ปัญหาการใช้อำนาจหน้าที่ของเจ้าพนักงานในการขอหลักฐานที่เกี่ยวข้องกับการกระทำความผิดตามมาตรา 18 และมาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

แพรวนภา กองทิพย์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
คณะนิติศาสตร์
สถาบันบัณฑิตพัฒนบริหารศาสตร์
2558

ปัญหาการใช้อำนาจหน้าที่ของเจ้าพนักงานในการขอหลักฐานที่เกี่ยวข้องกับการกระทำความผิดตามมาตรา 18 และมาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

แพรวนภา กองทิพย์
คณะนิติศาสตร์

ผู้ช่วยศาสตราจารย์.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ดร.วราภรณ์ วนาพิทักษ์)

คณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาแล้วเห็นสมควรอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรนิติศาสตรมหาบัณฑิต

รองศาสตราจารย์.....ประธานกรรมการ
(ดร.สราวุธ ปิติยาศักดิ์)

ผู้ช่วยศาสตราจารย์.....กรรมการ
(ดร.วริยา ล้ำเลิศ)

ผู้ช่วยศาสตราจารย์.....กรรมการ
(ดร.วราภรณ์ วนาพิทักษ์)

ศาสตราจารย์.....คณบดี
(ดร.บรรเจิด สิงคะเนติ)
เมษายน 2559

บทคัดย่อ

ชื่อวิทยานิพนธ์ ปัญหาการใช้อำนาจหน้าที่ของเจ้าพนักงานในการขอหลักฐานที่เกี่ยวข้องกับการกระทำความผิดตามมาตรา 18 และมาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ชื่อผู้เขียน นางสาวแพรวนภา กองทิพย์

ชื่อปริญญา นิติศาสตรมหาบัณฑิต

ปีการศึกษา 2558

ปัญหาการใช้อำนาจหน้าที่ของเจ้าพนักงานในการขอหลักฐานที่เกี่ยวข้องกับการกระทำความผิด ตามมาตรา 18 และ มาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มีวัตถุประสงค์เพื่อศึกษาถึงปัญหาการใช้อำนาจหน้าที่ของเจ้าพนักงานในการขอหลักฐานที่เกี่ยวข้องกับการกระทำความผิดตามมาตรา 18 และ มาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ของประเทศไทยเปรียบเทียบกฎหมายของต่างประเทศ ตลอดจนความร่วมมือระหว่างประเทศ และมาตรการอื่นๆ ที่เกี่ยวข้องกับปัญหาดังกล่าว เพื่อนำเสนอแนวทางในการปรับปรุงแก้ไขปัญหาเกี่ยวกับอำนาจหน้าที่ของเจ้าพนักงานในการขอหลักฐานที่เหมาะสมกับประเทศไทย

จากการศึกษาพบว่าการบังคับใช้กฎหมายเกี่ยวกับการใช้อำนาจหน้าที่ของเจ้าพนักงานในการขอหลักฐานที่เกี่ยวข้องกับการกระทำความผิดตามมาตรา 18 และ มาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ยังไม่มีบทบัญญัติที่เกี่ยวข้องกับการใช้อำนาจหน้าที่ของเจ้าพนักงานในการขอหลักฐานไว้โดยตรง แต่ได้มีการกำหนดให้มีพนักงานเจ้าหน้าที่ที่เป็นบุคคลที่มีความรู้และความชำนาญเกี่ยวกับคอมพิวเตอร์มาทำหน้าที่ในการกระทำความผิดตามพระราชบัญญัตินี้ ซึ่งพนักงานเจ้าหน้าที่ควรที่จะมีอำนาจหน้าที่ในการเข้าถึงข้อมูลคอมพิวเตอร์ของประชาชนได้โดยไม่ต้องขอหมายจากศาลเมื่อเปรียบเทียบกับอำนาจของเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญาและพนักงานเจ้าหน้าที่ของต่างประเทศแล้ว พนักงานเจ้าหน้าที่มีอำนาจเพียงพอหรือไม่

แนวทางในการแก้ไขปัญหาการใช้อำนาจหน้าที่ของเจ้าพนักงานในการขอหลักฐานที่เกี่ยวข้องกับการกระทำความผิดตามมาตรา 18 และ มาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มีความจำเป็นอย่างมากในประเทศไทย ต้องมีบทบัญญัติกฎหมายเพื่อควบคุมการใช้อำนาจของเจ้าหน้าที่ไว้เป็นการเฉพาะ โดยมีข้อยกเว้นในเรื่องของการยึดและค้นข้อมูลคอมพิวเตอร์ไว้ให้ชัดเจน และกำหนดให้ผู้ครอบครอง ที่ได้ทำการยึดถือหรือครอบครองคอมพิวเตอร์อยู่ในขณะนั้นให้มีอำนาจให้ความยินยอมแก่เจ้าหน้าที่สามารถทำการค้นและ

ยึดข้อมูลคอมพิวเตอร์ได้โดยไม่ต้องมีหมายค้นหรือเพียงมีข้อสงสัย แต่การค้นและยึดข้อมูลคอมพิวเตอร์จะต้องไม่เกินขอบเขตของความยินยอมและในการให้ความยินยอมในการทำการค้นหาอาจถูกเพิกถอนได้จากเจ้าของข้อมูลคอมพิวเตอร์เอง เพื่อให้กฎหมายเป็นไปอย่างมีประสิทธิภาพมากยิ่งขึ้น

ABSTRACT

Title of Thesis	The Problem of Exercising Power and Duties of the Authority in Requesting Evidences about the Offences Subject to Section 18 and Section 19 of Computer Crime Act B.E. 2550
Author	Miss Praewnapa Kongthip
Degree	Master of Laws
Year	2015

This article is a part of the thesis “problems of exercising power and duties of the authorities for requesting evidences about offences subject to section 18 and section 19 of Computer Crime Act B.E.2550”, aimed to study the problems of exercising power and duties of the authorities for requesting evidences about offences subject to section 18 and section 19 of Computer Act B.E. 2550 of Thailand in comparison with foreign laws as well as international cooperation and measures involved in such problems. It was conducted for suggestions on the appropriate guideline to resolve the issues about power and duties of the authorities in requesting evidences for Thailand.

The study was found that legislation pertaining to power and duties of the authorities in requesting evidences about offences subject to section 18 and section 10 of Computer Crime Act B.E. 2550 has not been directly regulated with the provisions regarding to exercising power and duties of authorities in requesting evidences. However, it has been stipulated that the authority should be knowledgeable and proficient about computer to perform duties inspecting the offences subject to this act. The authorities should have power to access computer data of people without court warrant. When comparing the power of authorities according to the code of laws on criminal proceedings and foreign authorities, do the authorities have adequate power?

The guidelines to solve the problems of exercising power and duties of authorities in requesting the evidences about offences subject to section 18 and section 19 of Computer Crime Act B.E.2550 wax that it was extremely necessary for Thailand to specifically provide legal provision to control power and duty exercising

of the authorities with obvious exceptions about computer data seizure and searching. Furthermore, it should be legislated that the owner who holds or possesses the computer should have power to allow the authority to search and acquire computer data without search warrant but only suspects. However, computer data search and seizure shall not be beyond the extent of consent and permission. The search could be withdrawn by the computer data owner so that the law was exercised with more effectiveness.

กิตติกรรมประกาศ

ความสำเร็จของวิทยานิพนธ์ฉบับนี้มีบุคคลหลายท่านเข้ามาเกี่ยวข้อง ผู้เขียนจึงขอกล่าวถึงและขอขอบคุณในความเมตตาของท่านไว้ ที่นี้ อันดับแรก ผู้เขียนขอขอบพระคุณท่าน ผู้ช่วยศาสตราจารย์ ดร.วราภรณ์ วนาพิทักษ์ ที่ให้เกียรติเป็นที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้ให้คำแนะนำและข้อคิดเห็นต่างๆ อันเป็นประโยชน์อย่างยิ่งในการจัดทำวิทยานิพนธ์ อีกทั้งยังช่วยแก้ไขปัญหาต่างๆ ที่เกิดขึ้นระหว่างการจัดทำวิทยานิพนธ์ ขอขอบพระคุณท่านรองศาสตราจารย์ ดร.สราวุธ ปิติยาศักดิ์ และผู้ช่วยศาสตราจารย์ ดร.วริยา ล้ำเลิศ กรรมการผู้สอบวิทยานิพนธ์ ที่ท่านได้กรุณาเสียสละเวลาอันมีค่าเป็นกรรมการสอบวิทยานิพนธ์และได้กรุณาให้คำแนะนำในการแก้ไขเนื้อหาเพื่อให้มีความสมบูรณ์เป็นประโยชน์ทั้งในเชิงวิชาการและต่อผู้ที่สนใจ

ผู้เขียนขอขอบพระคุณ ร.ต.อ.พงษ์เทพ กองทิพย์ บิดาของผู้เขียน สำหรับการเลี้ยงดูด้วยความรักและการเป็นแบบอย่างที่ดีให้ผู้เขียนเจริญรอยตาม นางคำมั่น กองทิพย์ ซึ่งสนับสนุนในด้านการเงินและให้ความรัก ให้กำลังใจ ให้ความห่วงใย แก่ผู้เขียนมาโดยตลอด นายกัญจน์ กองทิพย์ สำหรับกำลังใจและความห่วงใยที่มีให้พี่เสมอ

ผู้เขียนขอขอบคุณมิตรภาพที่ดีจากพี่ๆ นิติศาสตรมหาบัณฑิต ภาคพิเศษ รุ่นที่ 4 และรุ่นที่ 5 ที่น่ารักทุกคน เพื่อนโรงเรียนสาธิตมหาวิทยาลัยรามคำแหง โดยเฉพาะนางสาวกมลชนก มีสมสิบ และ นางสาววิมลรัตน์ สงขำ ขอบคุณคณะเจ้าหน้าที่คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ ที่ดูแลด้านการศึกษาและให้คำแนะนำต่างๆ และกราบขอบพระคุณคณาจารย์ทุกท่านที่ประสิทธิประสาทวิชาความรู้มาตลอดหลักสูตร

และขอขอบคุณพี่มารุตพงศ์ มาสิงห์ ผู้ทำหน้าที่เติมเต็มความสมบูรณ์ให้กับวิทยานิพนธ์ฉบับนี้

หากวิทยานิพนธ์ฉบับนี้พอจะสามารถให้ความรู้และก่อให้เกิดประโยชน์แก่ท่านผู้อ่านอยู่บ้าง ผู้เขียนขอให้เป็นบุญกุศลแก่ทุกท่านที่ได้กล่าวมาทั้งหมด และอีกหลายๆ ท่านที่เป็นส่วนหนึ่งในชีวิตของผู้เขียนแต่ไม่อาจกล่าวได้ครบถ้วน ณ ที่นี้ แต่หากมีความผิดพลาดประการใดผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

แพรวนภา กองทิพย์

เมษายน 2559

สารบัญ

สารบัญตาราง

ตารางที่ **หน้า**

บทที่ 1

บทนำ

1.1 ที่มาและความสำคัญของปัญหา

เนื่องจากในปัจจุบันคอมพิวเตอร์ได้เข้ามามีบทบาทและหน้าที่ในชีวิตการทำงานของเราเพิ่มมากขึ้น ซึ่งคอมพิวเตอร์นั้นถือได้ว่าเป็นเทคโนโลยีที่ได้รับการยอมรับในยุคปัจจุบันของสังคมไทยและสังคมทั่วโลกเมื่อคอมพิวเตอร์ได้เริ่มเข้ามามีบทบาทในชีวิตการทำงานของเราเป็นประจำเพิ่มมากขึ้น ทำให้พฤติกรรมการดำรงอยู่ของเราเปลี่ยนแปลงไป อีกทั้งคอมพิวเตอร์ยังได้มีการพัฒนาอย่างต่อเนื่องให้ทันกับความเหมาะสมกับยุคดิจิตอลหรือยุคไอทีในปัจจุบันนี้ด้วย คอมพิวเตอร์จึงถือได้ว่าเป็นส่วนสำคัญอย่างหนึ่งของการทำกิจกรรมไม่ว่าจะเป็นในด้านของการทำงาน การเรียนรู้ การติดต่อสื่อสาร การจัดเก็บข้อมูล การทำธุรกรรมทางอิเล็กทรอนิกส์ ในการทำกิจกรรมเช่นว่านี้โดยการใช้ระบบคอมพิวเตอร์ผ่านการเชื่อมต่อทางอินเตอร์เน็ต จึงพูดได้ว่าคอมพิวเตอร์ได้เริ่มเข้ามามีบทบาทในชีวิตประจำวันของมนุษย์อย่างมากและไม่สามารถที่จะหลีกเลี่ยงได้ ดังจะเห็นได้ว่าคอมพิวเตอร์นั้น ได้เข้ามาแทนที่ เครื่องพิมพ์ดีด โทรสาร โทรศัพท์ ดังเช่นในปัจจุบันที่เราพบเห็นกันอยู่

เมื่อพัฒนาการทางเทคโนโลยีและการติดต่อสื่อสารมีการพัฒนาเพื่อให้เกิดความเหมาะสมกับยุคปัจจุบันโดยการนำเอาสื่อต่างๆ มาใช้ประกอบกันในแง่ของการเป็นอุปกรณ์ เครื่องมือ ในการทำงาน โดยมีเครื่องคอมพิวเตอร์เป็นตัวเชื่อมระหว่างกันโดยการเชื่อมโยงระหว่างกันนั้นได้ติดต่อเชื่อมโยงผ่านทางระบบอินเตอร์เน็ต (Internet) ดังนั้นในยุคปัจจุบันของข้อมูลข่าวสาร (Information Age) ระบบนเทอร์เน็ตนับว่าเป็นระบบเครือข่ายคอมพิวเตอร์ที่ประชาชนให้ความสนใจเป็นอย่างมาก ถือว่าเป็นปัจจัยที่หกเลยก็ว่าได้ และได้ขยายไปในวงกว้างอย่างแพร่หลาย และยังมีความสำคัญต่อระบบเศรษฐกิจ กล่าวคือ เพราะระบบอินเทอร์เน็ตนั้นเป็นการติดต่อสื่อสารในรูปแบบใหม่ที่มีความสะดวก รวดเร็ว เมื่อนำไปเปรียบเทียบกับการติดต่อสื่อสารในรูปแบบอื่นๆ ปัจจุบันระบบอินเทอร์เน็ตไม่เพียงแต่เป็นที่สร้างข้อมูล รับ-ส่ง หรือแลกเปลี่ยนข้อมูลต่างๆ จากทั่วทุกมุมโลก แต่ยังเปรียบเสมือนคลังข้อมูล ที่ทุกคนสามารถค้นหาสิ่งที่ตนเองต้องการได้ตลอดเวลา นับว่าระบบอินเทอร์เน็ตนั้นเป็นสื่อในการประกอบธุรกิจรูปแบบใหม่ ที่ให้ทั้งความสะดวกและรวดเร็ว อีกทั้งยังเป็นแหล่งข้อมูลเพื่อทำการศึกษาค้นคว้าในการติดต่อสื่อสาร แลกเปลี่ยนความคิดเห็นระหว่างกันและกัน และยังเป็นแหล่งรวบรวมความบันเทิงเต็มรูปแบบประเภทหนึ่งอีกด้วยระบบอินเทอร์เน็ต ถือว่าเป็นสื่อที่มีการถูกนำไปใช้ในทางที่สร้างสรรค์ ย่อมส่งผลให้เกิดประโยชน์ต่อสังคมอย่างมาก แต่ในยุคปัจจุบันระบบอินเทอร์เน็ต ได้ถูกใช้เป็นเครื่องมือในการกระทำความผิดโดยเฉพาะกับระบบ โซเชียลมีเดียซึ่งในการกระทำความผิดในรูปแบบต่างๆ นั้น อาจจะส่งผลกระทบในวงกว้างในด้านต่างๆ ได้ ดังเช่น ในทางอาชญากรรมทางเศรษฐกิจ การคุกคามในการละเมิดสิทธิส่วนบุคคล การแสวงหาผลประโยชน์โดยการหลอกลวง การสร้างความเกลียดชัง หรือ การละเมิดสถาบัน เป็นต้น

ในปัจจุบันการกระทำความผิดบนเครือข่ายระบบอินเทอร์เน็ต มีหลากหลายรูปแบบจึงง่ายต่อการกระทำความผิด และมีความรวดเร็ว และนับวันยิ่งจะทวีความรุนแรงเพิ่มมากขึ้นตามลำดับ โดยเฉพาะปัญหาของการใช้ระบบเครือข่ายอินเทอร์เน็ตในการล่วงละเมิดสิทธิส่วนบุคคล การอให้เกิดอาชญากรรม การก่อให้เกิดการกระทำความผิดบนโลกไซเบอร์เป็นต้น และด้วยประสิทธิภาพของระบบคอมพิวเตอร์ทำให้มีการนำเอาคอมพิวเตอร์มาใช้ในการปฏิบัติงานเพิ่มมากขึ้นอีกด้วย

ซึ่งในปัจจุบันประเทศไทยนั้นได้มีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบในการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย มีการรวบรวม จัดเก็บ และนำเอาอกมาใช้หรือนำเอาออกมาเผยแพร่ข้อมูลที่เป็นในส่วนบุคคลของผู้ที่ใช้บริการในรูปแบบของข้อมูลทางอิเล็กทรอนิกส์ อันเป็นการป้องกันจากการละเมิดข้อมูลข่าวสารส่วนบุคคล ซึ่งถือเป็นสิทธิขั้นพื้นฐานที่สำคัญในความเป็นส่วนตัว (Privacy Right) ของประชาชน ที่จะต้องได้รับการคุ้มครอง มีความมั่นคงในการจัดทำธุรกรรมทางอิเล็กทรอนิกส์ซึ่งถือเป็นการคุ้มครองการเข้าถึงข้อมูลส่วนบุคคล (Data Privacy) ซึ่งเป็นข้อมูลที่เกี่ยวข้องกับสิ่งเฉพาะบุคคล เช่น เรื่องของการศึกษา ฐานะทางการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้นหรือมี เลขหมาย รหัส หรือสิ่งอื่นที่สามารถทำให้รู้ตัวบุคคลนั้นได้ ไม่ว่าจะเป็นลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับเฉพาะสิ่งเฉพาะตัวของผู้ถึงแก่กรรมแล้วด้วย

ผู้คนทั่วโลกสามารถที่จะทราบและรู้ถึงข้อมูลและเข้าถึงข้อมูลข่าวสารได้โดยง่าย และรวดเร็วด้วยยุคสมัยของเทคโนโลยีทางการสื่อสารสมัยใหม่ที่มีการเชื่อมโยงติดต่อสื่อสารกันทั่วโลก ทำให้รับรู้ข้อมูลข่าวสารทั่วโลกได้อย่างรวดเร็ว แต่ทั้งนี้ทั้งนั้นข้อมูลข่าวสารที่ผู้คนทั่วโลกได้มีการรับรู้ หากนำมาพิจารณาแล้วจะพบว่ามีทั้งข้อมูลทั่วไป และข้อมูลส่วนบุคคลอื่นๆ รวมปะปนอยู่ด้วยกัน ซึ่งมีทั้งข้อมูลส่วนบุคคลที่สามารถเปิดเผยได้ซึ่งถือได้ว่าเป็นข้อมูลส่วนบุคคลโดยทั่วไป และข้อมูลส่วนบุคคลที่ห้ามทำการเปิดเผย ถือได้ว่าเป็นผลกระทบต่อการละเมิดความเป็นส่วนตัว หากข้อมูลส่วนบุคคลดังกล่าว มีการเผยแพร่และมีการเปิดเผยด้วยระบบเทคโนโลยี ที่มีการพัฒนาไปอย่างรวดเร็วแบบก้าวกระโดด อาจจะก่อให้เกิดผลทั้งทางด้านดีและด้านเสียควบคู่กันไปในเวลาเดียวกัน ด้วยตัวของผู้ที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้น อาจจะไม่ให้ความยินยอมที่จะทำการเปิดเผยข้อมูลส่วนบุคคลของตนเองให้บุคคลอื่นรับรู้ หากมีการทำการเปิดเผยออกสู่สาธารณะชน รับรู้จะส่งผลกระทบ ในด้านความปลอดภัย ในชีวิต ทรัพย์สิน ชื่อเสียง เกียรติยศ หน้าที่การงาน รวมถึงความสัมพันธ์ภายในสถาบันครอบครัว ซึ่งถือว่าเป็นสถาบันหลักทางสังคมที่มีผลกระทบต่อการดำรงชีวิตมากที่สุด การเปิดเผยข้อมูลส่วนบุคคลของบุคคลอื่นนั้น ถือได้ว่าเป็นเรื่องที่มีความละเอียด เรื่องเฉพาะตัวบุคคลที่มีความสำคัญอย่างมากและเป็นการไม่สมควรที่จะทำการเปิดเผยสู่สาธารณะชน

ดังนั้น เพื่อให้ประเทศไทยสามารถป้องกันหรือรับมือกับสถานการณ์ด้านภัยคุกคามทางด้านไซเบอร์ที่อาจจะส่งผลกระทบหรืออาจที่จะก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายผ่านทางระบบคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายทางคมนาคม หรือการให้บริการโดยปกติของดาวเทียม ซึ่งการกระทำดังกล่าวนั้น อาจจะเป็นการกระทบต่อความมั่นคงของชาติในด้านต่างๆ อันครอบคลุมไปถึงความมั่นคงทางการรักษาความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจได้อย่างเหมาะสม หากมีการดำเนินการที่รวดเร็วและมีความเป็นเอกภาพ สมควร

ที่จะกำหนดให้มีคณะกรรมการขึ้นเพื่อกำหนดมาตรการด้านความมั่นคงปลอดภัยด้านไซเบอร์ของประเทศ ให้เป็นไปอย่างมีประสิทธิภาพ และเกิดผลสัมฤทธิ์

ถึงแม้ว่าจะได้มีการนำเอาเทคโนโลยีสารสนเทศที่ทันสมัยมาใช้ในสังคมที่มีการพัฒนาตลอดเวลาอย่างเช่นในยุคปัจจุบัน ซึ่งการพัฒนานั้นให้เกิดการกระทำความผิดเพิ่มมากขึ้นตามไปด้วย ถึงแม้ว่าการกระทำบางอย่างจะก่อให้เกิดความเสียหายตามกฎหมายอาญาแต่ก็ไม่สามารถที่จะนำตัวผู้กระทำความผิดมาลงโทษได้อาจจะเป็นเพราะการเข้าถึงข้อมูลหรือการเข้าไปขอหลักฐานนั้น จึงได้มีการบัญญัติกฎหมายที่เกี่ยวกับความรับผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ขึ้นตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

สำหรับประเทศไทยนั้นได้มีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ขึ้นเพื่อรับมือกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เฉกเช่นเดียวกับต่างประเทศ โดยการกระทำความผิดตามพระราชบัญญัตินี้ให้ถือว่าเป็นความผิดทางอาญา อาจจะกล่าวได้ว่า การจะดำเนินคดีกับผู้กระทำความผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ในความผิดที่เกี่ยวกับการจับ การค้น การยึด หรือ อายัด ย่อมเป็นไปตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอื่นที่เกี่ยวข้อง แต่การกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีลักษณะที่แตกต่างไปจากความผิดอาญาทั่วๆ ไป กล่าวคือ การจะดำเนินคดีอาญาในขั้นตอนต่างๆ ได้นั้นจะต้องทำการรวบรวมพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดตามประเภทนี้

แต่เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่าหากมีการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ตามมาตรา 18 ที่ได้บัญญัติไว้ว่า

> ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะเท่าที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด
>
> (1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้
>
> (2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง
>
> (3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่
>
> (4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใดหรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้[1]

และในการใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 19 ที่ได้กล่าวไว้ว่าให้พนักงานเจ้าหน้าที่มีอำนาจตามมาตรา 18 (4) (5) (6) (7) และ (8) โดยการให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจในลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบกับคำร้องด้วย

ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็วที่สุดเมื่อศาลมีคำสั่งอนุญาตแล้วก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) และ (8) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐานการทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา 18 (4) และให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น การยึดหรืออายัดตามมาตรา 18 (8) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้อง

[1]มาตรา 18 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน ตามหนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง[2]

ดังจะเห็นได้จากร่างประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 131/2 ประกอบร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. .... ที่บัญญัติขึ้นเพื่อเพิ่มอำนาจให้แก่พนักงานเจ้าหน้าที่ในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ของประชาชน โดยการที่ให้พนักงานเจ้าหน้าที่รัฐเข้าสู่บัญชีข้อมูลส่วนบุคคลในเครือข่ายโซเชียลมีเดียต่างๆ ได้ แต่การกำหนดหลักเกณฑ์การใช้อำนาจ ความรับผิดในร่างประมวลกฎหมายวิธีพิจารณาความอาญานี้ ยังมีจุดบกพร่องอยู่หลายประการ ไม่ว่าจะเป็นการเพิ่มอำนาจให้กับพนักงานเจ้าหน้าที่ที่จะทำการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์การใช้งานการให้อำนาจพนักงานเจ้าหน้าที่ ในการที่จะทำการค้น ยึด อายัด ขอ เข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดยไม่มีหลักฐานเกี่ยวกับการกระทำความผิดในการที่จะกระทำการดังกล่าวได้ หากมีการแก้ไขหลักเกณฑ์ ให้สอดคล้องกับลักษณะการกระทำความผิดความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทย และหลักเกณฑ์สากลก็จะเป็นประโยชน์อย่างยิ่งต่อการบังคับใช้กฎหมายต่อความผิดประเภทนี้ในประเทศไทยต่อไป

ด้วยเหตุนี้ ข้าพเจ้าจึงมีเหตุจูงใจในการที่จะได้ทำการศึกษาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในความผิดเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ โดยวิทยานิพนธ์ฉบับนี้ ผู้เขียนมุ่งที่จะศึกษาว่าอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมีความหมายครอบคลุมเพียงใด ในกรณีใดที่จะขอออกหมาย และการกระทำใดที่ไม่ต้องขอหมายจากศาล เนื่องจากผู้เขียนมีความเห็นว่าความรับผิดทางวิธีพิจารณาความอาญาในการค้น การยึด ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์เป็นการกระทำความผิดทางคอมพิวเตอร์ที่เกิดขึ้น เพราะการกระทำความผิดทางด้านคอมพิวเตอร์ส่วนใหญ่จะเริ่มจากในการเข้าไปในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ซึ่งเมื่อเข้าไปแล้วจะทำให้เกิดการกระทำความผิดเกิดขึ้น

ดังนั้น ผู้เขียนจึงมุ่งที่จะทำการศึกษาเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอพยานหลักฐานในการกระทำความผิดตามมาตรา 18 และมาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ว่ามีองค์ประกอบในการใช้อำนาจหน้าที่เช่นใดตามกฎหมาย และการกำหนดองค์ประกอบดังกล่าวมีความเหมาะสมกับการกระทำความผิดที่เกิดขึ้นในปัจจุบันแล้วหรือไม่ และมีขอบเขตในอำนาจเพียงใด การกระทำเช่นใดที่จะขอหมายตามกฎหมายได้ เพื่อไม่ให้เกิดปัญหาในการขอหมายตามที่กฎหมายกำหนด ซึ่งถ้าจะมีการบังคับใช้ก็ต้องมีการศึกษาเพื่อให้มีขอบเขตในการใช้กฎหมายที่ชัดเจนต่อไป

---

[2]มาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาวิเคราะห์ถึงแนวความคิดและทฤษฎีของการกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในการกระทำความผิดตามมาตรา 18 และมาตรา 19
2. เพื่อศึกษาวิเคราะห์ถึงมาตรการทางกฎหมายที่เกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในการเข้าถึงข้อมูลคอมพิวเตอร์
3. เพื่อศึกษาวิเคราะห์ถึงลักษณะอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในการกระทำความผิด และ
4. เพื่อเสนอแนะแนวทางในการปรับปรุงกฎหมายที่เกี่ยวข้องในการขอหมายจากศาล

1.3 สมมติฐานของการศึกษา

ความรับผิดทางอาญาในการเข้าถึงข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ยังมีปัญหาในการใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอพยานหลักฐานอย่างยากลำบาก ซึ่งมีผลมาจากประมวลกฎหมายของบ้านเรายังไม่ชัดเจน ดังนั้น จึงควรมีการแก้ไขเพิ่มเติมไว้ใน มาตรา 19/1 โดยการกำหนดให้พนักงานเจ้าหน้าที่สามารถเข้าถึงข้อมูลคอมพิวเตอร์ได้โดยไม่ต้องขอหมายจากศาล หากเข้ากรณีใดกรณีหนึ่งดังต่อไปนี้ คือ กรณีที่ได้รับความยินยอม (Consent) หรือ กรณีที่เป็นการอันจำเป็นเร่งด่วน Exigent Circumstances หรือ กรณีที่การยึดค้นข้อมูลคอมพิวเตอร์ที่ได้มาจากการจับกุมโดยชอบ (Search Incident to a Lawful Arrest)

1.4 ขอบเขตของการศึกษา

การศึกษาด้านกฎหมายในครั้งนี้เป็นการศึกษาที่มุ่งศึกษาเกี่ยวกับปัญหาทางกฎหมายที่เป็นเรื่องเกี่ยวกับการเข้าถึงข้อมูลทางคอมพิวเตอร์ในการกระทำความผิดอันเกิดจากการใช้อำนาจในการค้น การยึด ข้อมูล ในระบบคอมพิวเตอร์ของพนักงานเจ้าหน้าที่ ในเรื่องที่ว่าด้วยการเข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์โทรเลข โทรศัพท์โทรสาร คอมพิวเตอร์เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ในการปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ในส่วนที่เป็นมาตรการในการป้องกันการเข้าถึงข้อมูล อีกทั้งมาตรการในการคุ้มครองในการขอหมายจากศาลและจะต้องมีการแจ้งให้ทราบ ในการค้นคว้าในครั้งนี้ได้ทำการรวบรวมเอกสารจากหนังสือ วารสาร บทความ สาระนิพนธ์ วิทยานิพนธ์ และข้อมูลต่างๆ จากเว็บไซต์ โดยทำการสืบค้นและศึกษาจากแหล่งข้อมูลภายในประเทศและต่างประเทศที่มีความเกี่ยวข้อง ได้แก่ ร่างประมวลกฎหมายวิธีพิจารณาความอาญา ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และกฎหมายอื่นๆ ที่เกี่ยวข้อง โดยได้ทำการศึกษาเปรียบเทียบกับกฎหมาย

ของประเทศสหรัฐอเมริกา และประเทศสิงคโปร์ เนื่องจากทั้งสองประเทศมีกฎหมายที่ให้ความคุ้มครองในการเข้าถึงข้อมูลในด้านการค้นและยึดข้อมูลทางคอมพิวเตอร์ไว้โดยตรง

1.5 วิธีการดำเนินการศึกษา

วิทยานิพนธ์ฉบับนี้เป็นการทำการศึกษาค้นคว้า โดยใช้วิธีการศึกษาค้นคว้าจากเอกสาร (Documentary Research) เป็นหลัก ทั้งภาคภาษาไทยและภาคภาษาต่างประเทศจากห้องสมุดและจากระบบฐานข้อมูลในเว็บไซต์บนเครือข่ายอินเทอร์เน็ต บทความ ของนักกฎหมายที่ได้แสดงความคิดเห็นในทางวิชาการจากวารสารกฎหมายไทยและกฎหมายต่างประเทศ วิทยานิพนธ์ตลอดจนแนวคำพิพากษาของศาลในส่วนที่เกี่ยวข้อง โดยได้ทำการศึกษาแล้วนำมาวิเคราะห์แล้วจึงนำมาสรุปเป็นประเด็นข้อมูล มีการจัดข้อมูลเป็นระบบ เพื่อทำการเปรียบเทียบให้เกิดความเข้าใจเกี่ยวกับกฎหมาย ของรัฐหรือเจ้าหน้าที่รัฐ ในการใช้อำนาจหน้าที่ในการเข้าถึงข้อมูลคอมพิวเตอร์ตามกฎหมายของประเทศต่างๆ เพื่อเป็นการนำไปสู่การวิเคราะห์ในประเด็นปัญหาและผลกระทบที่เกิดขึ้น เพื่อเป็นการหาข้อเสนอแนะ หลักเกณฑ์และแนวทางในการแก้ไขปัญหานั้น

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้เข้าใจแนวความคิดและทฤษฎีของการกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในการกระทำความผิด
2. ทำให้เห็นถึงแนวทางในการกำหนดมาตรการทางกฎหมายที่เกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในการเข้าถึงข้อมูลคอมพิวเตอร์ของประเทศต่างๆ และการบังคับใช้กฎหมาย เพื่อเป็นแนวทางในการกำหนดและบังคับใช้ตามกฎหมายไทย ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
3. ทำให้เข้าใจถึงลักษณะอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในการกระทำความผิดว่าเป็นเช่นไร การกระทำเช่นใดจึงควรที่จะขอหมาย
4. ทำให้เห็นถึงแนวทางในการที่จะขอหมายจากศาลว่ามีกรณีใดบ้างที่จะต้องขอหมายจากศาลในการเข้าถึงข้อมูลคอมพิวเตอร์ของผู้ที่กระทำความผิด

บทที่ 2

แนวคิดและทฤษฎีเกี่ยวกับการใช้อำนาจของพนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลคอมพิวเตอร์

เนื่องมาจากในปัจจุบันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้น ถือได้ว่าเป็นการกระทำที่ผู้กระทำความผิดจะต้องมีความรู้ความเชี่ยวชาญในการที่จะกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ได้ และการที่จะสืบสวนฟ้องร้องดำเนินคดีก็จะต้องกระทำโดยอาศัยองค์ความรู้ดังกล่าวมาพิจารณาประกอบกัน[3] หากจะกล่าวได้ว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นั้น ได้นำเอาแนวทางมาจากอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime) ของคณะมนตรียุโรป (Council of Europe) ที่นำเอาอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรียุโรปมาเป็นแนวทางนั้น เพราะอนุสัญญาดังกล่าวนั้นได้มีการกำหนดหลักเกณฑ์ในการที่จะรับมือกับปัญหาอาชญากรรมทางคอมพิวเตอร์ไว้อย่างชัดเจน กล่าวคือ ได้มีการกำหนดหลักเกณฑ์ในลักษณะของการกระทำความผิด และยังได้กำหนดหลักเกณฑ์ในการให้อำนาจกับพนักงานเจ้าหน้าที่ในการใช้กฎหมายอีกด้วย และเพื่อปรับปรุงการสืบสวนและการฟ้องร้องดำเนินคดีในด้านอาชญากรรมทางคอมพิวเตอร์ต่อไป

แต่อย่างไรก็ตามสิ่งที่เป็นปัญหาสำหรับการใช้อำนาจของพนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลคอมพิวเตอร์ในการที่จะขอหลักฐานในกรณีทีผู้กระทำความผิดได้กระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ลงไปแล้วนั้นเป็นสิ่งที่ไม่สามารถที่จะกระทำเลยจึงเป็นกระบวนการที่มีความยุ่งยากซับซ้อน กล่าวคือ ควรที่จะต้องมีการบัญญัติกฎหมายที่เกี่ยวกับการใช้อำนาจของพนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลคอมพิวเตอร์ขึ้น แต่เนื่องด้วยคำว่า “คอมพิวเตอร์” เป็นศัพท์เทคนิคเฉพาะที่เกี่ยวกับคอมพิวเตอร์จึงมีความจำเป็นอย่างมากที่จะต้องทำความเข้าใจในความหมายของคอมพิวเตอร์ที่ได้บัญญัติไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ว่ามีความหมายเป็นเช่นไรและในทางกฎหมายมีความหมายว่าเช่นไรในการที่จะนำเอามาปรับใช้กับกฎหมายต่อไป

---

[3] Donn B. Paker, S. Nycum and S. Aura, **Computer Abuse** (California: Stanford Reseacher, n.d.) quoted in Martin Wasik, **Crime and the Computer** (Oxford: Clarendon Press, 1991), p. 1 อ้างถึงใน องอาจ เทียนหิรัญ, **อาชญากรรมทางคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2546), หน้า 12.

2.1 ข้อมูลคอมพิวเตอร์

ข้อมูลคอมพิวเตอร์เป็นองค์ประกอบที่สำคัญอย่างหนึ่งในระบบคอมพิวเตอร์เป็นสิ่งที่ต้องมีการเขียนลงไปในคอมพิวเตอร์พร้อมกับโปรแกรมที่นักคอมพิวเตอร์ได้เขียนขึ้น เนื่องจากการทำงานของคอมพิวเตอร์นั้นจะเป็นการทำงานในด้านประมวลผลข้อมูลเพื่อที่จะได้นำส่งเข้าไปในคอมพิวเตอร์ เพราะฉะนั้น จะต้องทำความเข้าใจเกี่ยวกับความหมายของข้อมูลคอมพิวเตอร์เพื่อนำมาพิจารณาความหมายในทางกฎหมายต่อไป

2.1.1 ความหมายของข้อมูลคอมพิวเตอร์

คำว่า “ข้อมูลคอมพิวเตอร์” ไม่มีการให้ความหมายไว้ในทางกฎหมาย[4] มีแต่คำว่า “ข้อมูล” ที่ให้ความหมายไว้ว่า ข้อเท็จจริง ที่เกิดขึ้นในชีวิตประจำวัน อาจจะเกี่ยวข้องไปถึงบุคคล สิ่งของ การกระทำต่างๆ ซึ่งอาจจะอยู่ในรูปแบบของตัวเลข (Numeric) หรือเป็นข้อความที่ไม่ใช่ตัวเลขก็ได้ (Non-Numeric) รูปภาพ (Image) สัญลักษณ์ (Symbol) หรือ เหตุการณ์ต่างๆ เป็นต้น ซึ่งข้อมูลคอมพิวเตอร์ ก็จะมีความหมายคล้ายคลึงกันกับความหมายของข้อมูล (Data) ดังที่ได้กล่าวมาแล้วข้างต้น คำว่าข้อมูล (Data) ในทางทางคอมพิวเตอร์นั้น หมายถึงกลุ่มอักขระ (Character) ที่นำมารวมกันแล้วมีความหมายอย่างใดอย่างหนึ่งอาจจะหมายถึง คำ (Word) ข้อความ (Message) ที่กล่าวถึงสิ่งใดสิ่งหนึ่ง โดยที่ข้อความนั้นอาจเป็นตัวเลข (Numeric) สัญลักษณ์ (Symbol) หรืออื่นๆ ที่สามารถนำไปประมวลผลด้วยคอมพิวเตอร์ได้[5]

จึงอาจจะกล่าวได้ว่าอาจจะมีการให้ความหมายที่แตกต่างกันออกไปตามความต้องการในด้านการใช้งาน เพราะฉะนั้น ไม่ว่าจะเป็นคำว่า “ข้อมูลคอมพิวเตอร์” หรือคำว่า “ข้อมูลอิเล็กทรอนิกส์” ก็ไม่ได้ให้ความหมายไว้ในด้านคอมพิวเตอร์แต่อาจจะกล่าวได้ว่า ข้อมูลอิเล็กทรอนิกส์นั้นมีความหมายกว้างกว่าข้อมูลคอมพิวเตอร์ในความหมายทั่วๆ ไป

2.1.2 ประเภทของคอมพิวเตอร์

คอมพิวเตอร์สามารถแบ่งออกได้เป็น 2 ประเภท คือ แบ่งตามลักษณะของข้อมูล และแบ่งตามสมรรถนะและขนาดของคอมพิวเตอร์

2.1.2.1 การแบ่งตามลักษณะของข้อมูล

สามารถแบ่งออกได้เป็น 3 ประเภท ได้แก่[6]

---

[4]ธงชัย โรจน์กังสดาล, อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, จุฬาลงกรณ์มหาวิทยาลัย, 30 มกราคม 2551, สัมภาษณ์.

[5]โรงเรียนเชียงคำวิทยาคม, **อินเตอร์เน็ตและการสื่อสารในชีวิตประจำวัน**, ค้นวันที่ 9 ธันวาคม 2558 จาก http://www.krunee.com

[6]มหาวิทยาลัยราชภัฏสวนดุสิต, **วิชาเทคโนโลยีสารสนเทศเพื่อชีวิต**, ค้นวันที่ 9 ธันวาคม 2558 จาก http://dusithost.dusit.ac.th/~librarian/it107/C2.htm.

1) อนาลอกคอมพิวเตอร์ (Analog Computer) เป็นเครื่องคอมพิวเตอร์ที่ถูกสร้างขึ้นเป็นกรณีพิเศษ เพื่อให้เหมาะสมกับงานในด้านนั้นๆ มีการทำงานโดยการรับข้อมูลแบบวัดจำนวนที่ต่อเนื่องกัน ซึ่งจะนำข้อมูลที่วัดได้มาแปลงเป็นค่าตัวเลข เช่น การวัดอุณหภูมิของอากาศ การวัดแรงดันไฟฟ้า การวัดความดังของเสียงเครื่องยนต์ การวัดปริมาณอากาศที่เป็นพิษ เป็นต้น ซึ่งผลจากการวัดที่ได้จะมีความละเอียดค่อนข้างมากเหมือนกับดิจิทัลคอมพิวเตอร์ จึงเหมาะกับงานทางด้านวิทยาศาสตร์ วิศวกรรม และทางด้านคณิตศาสตร์ เนื่องจากงานเหล่านี้จะต้องใช้ค่าตัวเลขที่ละเอียด มีจุดทศนิยมหลายตำแหน่ง ซึ่งผลลัพธ์ที่ได้จะออกมาในรูปแบบของกราฟ

2) ดิจิทัลคอมพิวเตอร์ (Digital Computer) เป็นเครื่องคอมพิวเตอร์ชนิดดิจิตอลเป็นเครื่องคอมพิวเตอร์ที่มีการคำนวณโดยการนับจำนวนโดยตรงและมีความแม่นยำมากกว่าอนาลอกคอมพิวเตอร์ ข้อมูลที่นับได้จะเก็บเป็นรหัสตัวเลขฐาน 2 คือ มีเลข 0 กับเลข 1 การประมวลผลจะทำงานต่อเนื่องกันไป และมีการเก็บข้อมูลได้เป็นจำนวนมากได้อย่างถูกต้องแม่นยำจึงต้องใช้สื่อในการบันทึกข้อมูล เช่น จานแม่เหล็กและเทปแม่เหล็ก เป็นต้น ซึ่งต่อมาได้มีการพัฒนาให้สามารถนำไปใช้กับงานที่เหมาะสมได้ ซึ่งการนำไปใช้นั้นจะต้องขึ้นอยู่กับประเภทงานที่นำไปใช้ด้วย เช่น งานพิมพ์เอกสาร งานคำนวณ งานวิจัยเปรียบเทียบค่าทางสถิติ งานบันทึกนัดหมาย งานส่งข้อความในรูปแบบของเอกสาร การจองสายการบิน การควบคุมการยิงขีปนาวุธ การพยากรณ์สภาพภูมิอากาศ ตลอดไปถึงงานทางด้านกราฟิกเพื่อการนำเสนอในรูปแบบอื่นๆ เป็นต้น

3) ไฮบริดคอมพิวเตอร์ (Hybrid Computer) เป็นเครื่องคอมพิวเตอร์แบบผสม ที่มีลักษณะการใช้งานเฉพาะด้านโดยการนำเอาการทำงานแบบดิจิตอลและแบบอนาลอกมาผสมกัน เพื่อให้มีประสิทธิภาพสูงและสามารถทำงานที่ซับซ้อนได้ เนื่องจากลักษณะการทำงานของคอมพิวเตอร์ในลักษณะนี้จะมีการรับข้อมูลเข้าเครื่องหรือมีการแสดงผลข้อมูลออกมาอย่างต่อเนื่อง นอกจากนั้นคอมพิวเตอร์แบบนี้ยังมีความสามารถในด้านการคำนวณที่ถูกต้องแม่นยำ และสามารถทำงานตามโปรแกรมที่ซับซ้อนได้ สำหรับงานที่จะใช้คอมพิวเตอร์แบบผสม หรือ ไฮบริดจ์นั้น มักจะเป็นงานเฉพาะด้าน เช่น งานทางด้านวิทยาศาสตร์ การส่งยานอวกาศโดยจะใช้การควบคุมการหมุนของตัวยานอวกาศผ่านอนาลอกคอมพิวเตอร์ การฝึกนักบิน ใช้ในการควบคุมการทำงานด้านอุตสาหกรรม หรืออาจจะใช้ในวงการแพทย์ เป็นต้น

ดังนั้น การแบ่งคอมพิวเตอร์ให้เป็นไปตามลักษณะข้อมูลนั้นเป็นสิ่งที่ทำได้ยาก ส่วนการแบ่งตามสมรรถนะและขนาดของคอมพิวเตอร์นั้นสามารถทำได้ง่ายกว่า[7]

2.1.2.2 การแบ่งตามสมรรถนะและขนาดของคอมพิวเตอร์

1) ซูเปอร์คอมพิวเตอร์ (Supercomputer) เป็นคอมพิวเตอร์ที่มีขนาดใหญ่ที่สุด รุ่นแรก สร้างในปี ค.ศ.1960 ที่องค์การทหารของสหรัฐอเมริกาสร้างขึ้น สามารถประมวลผลได้กว่า 100 ล้านคำสั่งต่อวินาที จึงทำให้ทำงานได้รวดเร็วและมีประสิทธิภาพสูง เป็นเครื่องคอมพิวเตอร์ที่เหมาะกับงานคำนวณที่ต้องคำนวณตัวเลขจำนวนมหาศาลให้เสร็จภายในระยะเวลาอันสั้น โดยต้องอยู่ในห้องที่มีการควบคุมอุณหภูมิและปราศจากฝุ่นละออง มักใช้กับองค์กรที่มีขนาดใหญ่เท่านั้น เนื่องจากสามารถรองรับการใช้งานของผู้ใช้จำนวนมากพร้อมๆ กันได้ เรียกว่า

[7] *เรื่องเดียวกัน.*

มัลติโปรเซสซิ่ง (Multiprocessing) อันเป็นการใช้หน่วยประมวลผลหลายตัว เพื่อให้คอมพิวเตอร์สามารถทำงานหลายงานพร้อมๆ กันได้ จึงนิยมใช้กับงานที่การคำนวณที่ซับซ้อน เช่น การพยากรณ์อากาศ การทดสอบทางอวกาศ การคำนวณทางวิทยาศาสตร์ การบิน อุตสาหกรรมน้ำมัน ตลอดจนการวิจัยในห้องปฏิบัติการ ทั้งของภาครัฐบาลและเอกชน เป็นต้น ซูเปอร์คอมพิวเตอร์ที่รู้จักกันดีในปัจจุบันได้แก่ Cray Supercomputer

2) เมนเฟรมคอมพิวเตอร์ (Mainframe Computer) เป็นเครื่องคอมพิวเตอร์ขนาดใหญ่มีความเร็วในการประมวลผลสูงรองลงมาจากซูเปอร์คอมพิวเตอร์ ต้องอยู่ในห้องที่ควบคุมอุณหภูมิและปราศจากฝุ่นละออง และได้รับการพัฒนาให้มีหน่วยประมวลผลหลายหน่วยทำงานพร้อมๆ กัน เช่นเดียวกับซูเปอร์คอมพิวเตอร์ แต่มีจำนวนหน่วยประมวลผลที่น้อยกว่า จึงทำให้สามารถประมวลผลคำสั่งได้หลายสิบล้านคำสั่งต่อวินาที ระบบคอมพิวเตอร์ของเครื่องเมนเฟรมส่วนมากจะมีระบบคอมพิวเตอร์ย่อยๆ ประกอบอยู่ด้วย เพื่อช่วยในการทำงานบางประเภทให้กับเครื่องหลัก มีราคาแพงมาก (แต่น้อยกว่าซูเปอร์คอมพิวเตอร์) เหมาะกับงานที่มีข้อมูลที่มีปริมาณมากต้องประมวลผลพร้อมกันโดยผู้ใช้นับพันคน (Multi-User) ใช้กับองค์กรใหญ่ๆ ทั่วไป เช่น งานด้านวิศวกรรมคอมพิวเตอร์ วิทยาศาสตร์ การควบคุมระบบเครือข่าย งานพัฒนาระบบ งานด้านธุรกิจ ธนาคาร งานสำมะโนประชากร งานสายการบิน งานประกันชีวิต และมหาวิทยาลัย เป็นต้น

3) มินิคอมพิวเตอร์ (Minicomputer) เป็นเครื่องคอมพิวเตอร์ที่มีขนาดกลางที่มีประสิทธิภาพในการทำงานน้อยกว่าเมนเฟรมแต่สูงกว่าไมโครคอมพิวเตอร์ สามารถรองรับการทำงานจากผู้ใช้หลายร้อยคน (Multi-User) ในการทำงานที่แตกต่างกัน (Multi Programming) เช่นเดียวกับเครื่องเมนเฟรม แต่สิ่งที่แตกต่างกันระหว่างเครื่องเมนเฟรมและเครื่องมินิคอมพิวเตอร์ คือ ความเร็วในการทำงาน เนื่องจากมินิคอมพิวเตอร์ทำงานได้ช้ากว่า และควบคุมผู้ใช้งานต่างๆ ในจำนวนที่น้อยกว่า รวมทั้งสื่อที่เก็บข้อมูลมีความจุน้อยกว่าเมนเฟรม จึงเหมาะกับองค์กรขนาดกลาง เพราะมีราคาถูกกว่าเครื่องเมนเฟรมมาก ทำงานเฉพาะด้าน เช่น การคำนวณทางด้านวิศวกรรม การจองห้องพักของโรงแรม การทำงานด้านบัญชีขององค์การธุรกิจ เป็นต้น ในสถานศึกษาต่างๆ และบางหน่วยงานของรัฐนิยมใช้คอมพิวเตอร์ประเภทนี้

4) เวิร์คสเตชันคอมพิวเตอร์ (Workstation Computer) เป็นเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ ที่สนับสนุนการทำงานของคอมพิวเตอร์เครือข่าย ซึ่งใช้ในการจัดสรรและใช้ทรัพยากรร่วมกัน เช่น แฟ้มข้อมูลโปรแกรมประยุกต์ อุปกรณ์คอมพิวเตอร์ เช่น เครื่องพิมพ์และอุปกรณ์อื่นๆ โดยการเชื่อมโยงกับเทอร์มินัล (Terminal) หลายๆ เครื่อง อีกทั้งได้ถูกออกแบบมาให้มีความสามารถในการคำนวณด้านวิศวกรรม สถาปัตยกรรม หรืองานอื่นๆ ที่เน้นการแสดงผลด้านกราฟิก เช่น การนำมาช่วยออกแบบภาพกราฟิกที่มีความละเอียดสูง ทำให้เวิร์คสเตชันใช้หน่วยประมวลผลที่มีประสิทธิภาพสูงและมีหน่วยเก็บข้อมูลสำรองจำนวนมากด้วย ผู้ใช้บางกลุ่มจะเรียกเครื่องระดับเวิร์คสเตชันนี้ว่า ซูเปอร์ไมโคร (Supermicro) เพราะถูกออกแบบให้ใช้งานแบบตั้งโต๊ะ แต่ชิปที่ใช้ทำงานนั้นแตกต่างกันมาก เนื่องจากเวิร์คสเตชันส่วนมากใช้ชิปที่ลดจำนวนคำสั่งที่สามารถใช้สั่งงานให้เหลือเฉพาะที่จำเป็น เพื่อให้สามารถทำงานได้ด้วยความเร็วสูง

5) ไมโครคอมพิวเตอร์ (Microcomputer) เป็นเครื่องคอมพิวเตอร์ขนาดเล็ก ราคาถูกสามารถเรียกได้อีกอย่างหนึ่งว่าเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer:

PC) มีการพัฒนาขึ้นในปี ค.ศ.1975 ซึ่งได้รับความนิยมเป็นอันมาก เมื่อ IBM ได้สร้างเครื่อง IBM PC ออกมา ซึ่งความแตกต่างระหว่างเวิร์คสเตชันคอมพิวเตอร์ และไมโครคอมพิวเตอร์ได้ลดน้อยลงเรื่อยๆ เนื่องจากเครื่องไมโครคอมพิวเตอร์ระดับสูงในปัจจุบันมีประสิทธิภาพ และมีความเร็วในการแสดงผลที่ดีกว่าเวิร์คสเตชันคอมพิวเตอร์มาก สามารถใช้งานโดยใช้คนเดียว (Stand-Alone) หรือเชื่อมต่อเป็นเครือข่ายเพื่อติดต่อสื่อสารกับคอมพิวเตอร์เครื่องอื่นได้ จากการที่เทคโนโลยีที่ก้าวนำสมัยทำให้ PC สามารถเชื่อมโยงเข้ากับระบบเครือข่ายอินเทอร์เน็ตติดต่อสื่อสารกับคนอื่นได้ทั่วโลก เหมาะกับงานทั่วไป เช่น การประมวลผลคำ (Word Processing) การคำนวณ (Spreadsheet) การบัญชี (Accounting) จัดทำสิ่งพิมพ์ (Desktop Publishing) และงานที่เกี่ยวข้องกับฐานข้อมูล เป็นต้น โดยอาจจะแบ่งคอมพิวเตอร์ส่วนบุคคลได้ ดังนี้

(1) คอมพิวเตอร์แบบตั้งโต๊ะ (Desktop Computer) หรือเดสก์ท็อป เป็นคอมพิวเตอร์ส่วนบุคคล (Personal Computer: PC) ที่มีขนาดเล็กเหมาะกับโต๊ะทำงานในสำนักงาน สถานศึกษา และที่บ้าน รูปทรง ของตัวเครื่องคอมพิวเตอร์จะมีทั้งแบบวางนอน และแบบแนวตั้งที่เรียกว่าทาวเวอร์ (Tower) เพื่อประหยัดเนื้อที่เป็นการวางทั้งบนโต๊ะและที่พื้น โดยสามารถใช้งานได้เพียงคนเดียว (Stand-alone) หรือ เชื่อมต่อเป็นเครือข่ายเพื่อติดต่อสื่อสารกับคอมพิวเตอร์เครื่องอื่น

(2) โน๊ตบุ๊คคอมพิวเตอร์ (Notebook Computer) หรือบางครั้งเรียกว่า แลปท็อปคอมพิวเตอร์ (Laptop Computer) เป็นเครื่องคอมพิวเตอร์ที่มีขนาดเล็กกว่าเครื่องพีซีแบบตั้งโต๊ะน้ำหนักเบาประมาณ 2-4 กิโลกรัมและบางกว่าแบบตั้งโต๊ะ จึงสามารถนำติดตัวไปยังสถานที่ต่างๆ ได้สะดวก เครื่องโน้ตบุ๊คมีสมรรถนะในการทำงานเทียบเท่าเครื่องพีซีแบบตั้งโต๊ะ และมีแผงแป้นพิมพ์และจอภาพติดกับตัวเครื่องรวมทั้งมีแบตเตอรี่ภายในเครื่อง จึงสามารถทำงานได้ในช่วงเวลาหนึ่งโดยไม่ต้องใช้ไฟบ้าน เหมาะกับงานส่วนบุคคลและงานสำนักงานที่จำเป็นต้องออกนอกสถานที่ และในปัจจุบันได้มีการพัฒนาให้มีขนาดเล็กลงกว่าเดิมในขนาดที่สามารถที่จะวางบนตักได้

(3) ซับโน๊ตบุ๊ค (Subnotebook Computer) เป็นคอมพิวเตอร์พกพาที่มีขนาดเล็กกว่าคอมพิวเตอร์โน๊ตบุ๊ค มีน้ำหนักประมาณ 1 - 2.7 กิโลกรัม เพื่อเป็นการลดขนาดและน้ำหนักของตัวเครื่อง ในบางครั้ง Subnotebook จะไม่มีเครื่องอ่านแผ่นดิสก์ และจะใช้การ์ดสำหรับบันทึกและจะใช้การ์ดบันทึกสำหรับงานเฉพาะแทน[8]

(4) คอมพิวเตอร์แทปเลท (Tablet Computer) เป็นคอมพิวเตอร์ที่รวมการทำงานทุกอย่างไว้ในจอสัมผัสโดยใช้ปากกาดิจิตอลหรือปลายนิ้ว เป็นอุปกรณ์อินพุตพื้นฐานแทนการใช้คีย์บอร์ดและเมาส์ แต่มีอยู่หรือไม่มีก็ได้ มีอุปกรณ์ไร้สายสำหรับการเชื่อมต่ออินเทอร์เน็ตและระบบเครือข่ายภายในสามารถเคลื่อนย้ายและพกพาได้สะดวก มีลักษณะคล้ายโน้ตบุ๊คแต่จะมีความแตกต่างกันตรงที่แทปเลทสามารถป้อนข้อมูลทางจอภาพได้ตามเทคโนโลยีของผู้ผลิต

(5) คอมพิวเตอร์พกพา (Handheld Computer) หรือ ปาล์มท็อป (Palmtop Computer) หรือ เครื่องพีซีขนาดมือถือ หรือ เครื่องพีดีเอ (Personal Digital Assistant-

---

[8] *เรื่องเดียวกัน.*

PDA) เป็นเครื่องคอมพิวเตอร์ที่มีขนาดเท่ากับเครื่องคิดเลขขนาดเล็ก น้ำหนักเบามาก จึงสามารถวางบนฝ่ามือได้โดยมีสมรรถนะในการทำงานเฉพาะกับโปรแกรมสำหรับงานส่วนบุคคล เช่น การรับส่งอี-เมล์ การบันทึกตารางนัดหมาย และการเข้าถึงข้อมูลบนอินเตอร์เน็ต เครื่อง PDA (Personal Digital Assistant) บางครั้งก็เรียกว่า Pen-Based Computer

เนื่องจากเป็นคอมพิวเตอร์แบบพกพาที่ใช้ปากกาที่เรียกว่า สไตลัส (Stylus) เป็นอุปกรณ์ในการบันทึกข้อมูล ในบางครั้งก็จะใช้ปากกาในการเขียนข้อมูลด้วยลายมือลงบนหน้าจอ และในบางครั้งอาจจะใช้ปากกานี้สำหรับเป็นอุปกรณ์เพื่อเลือกการทำงานบนจอภาพ ซึ่ง Personal Digital Assistant ในปัจจุบันนอกจากจะทำหน้าที่พื้นฐานทั่วไปแล้วยังสามารถรับ-ส่งอีเมลล์ และส่งโทรสาร (Fax) ได้ด้วย

เพราะฉะนั้น จึงเห็นได้ว่าไม่ว่าคอมพิวเตอร์จะมีชื่อเรียกในแบบใด แต่ก็มีรูปลักษณ์และลักษณะการใช้งานที่แตกต่างกันออกไปเพื่อจุดประสงค์ของผู้ผลิตและความต้องการของผู้บริโภค และยิ่งในปัจจุบันได้มีการนำเอาคอมพิวเตอร์มาใช้มากขึ้นเท่าไหร่ ก็ยิ่งทำให้คอมพิวเตอร์มีการพัฒนาให้มีรูปแบบและการทำงานให้มีประสิทธิภาพมากขึ้นเท่านั้น

2.1.3 การให้คำนิยามในด้านกฎหมาย

หากพิจารณาถึงความหมายของคำว่า “ข้อมูล” ในด้านความหมายทางคอมพิวเตอร์แล้วสิ่งที่จะต้องทำการพิจารณาต่อมาคือความหมายที่จะนำมาใช้ในด้านกฎหมาย โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้ให้คำนิยามคำว่า “ข้อมูลคอมพิวเตอร์” ไว้ในมาตรา 3 ว่า “ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย กล่าวคือ ข้อมูลทุกอย่างที่อยู่ในระบบคอมพิวเตอร์รวมทั้งชุดคำสั่งด้วยหากอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้นอกจากนั้นยังให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย[9] เมื่อพิจารณาถึงนิยามของคำว่า “ข้อมูลคอมพิวเตอร์” แล้วนั้น สิ่งที่จะต้องทำการพิจารณาต่อไปคือ ความหมายของคำว่า “ข้อมูลอิเล็กทรอนิกส์” เพราะในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้ให้ความหมายครอบคลุมไปถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์อีกด้วย แต่ความจริงแล้ว “ข้อมูลอิเล็กทรอนิกส์” ย่อมอยู่ในความหมายของข้อมูลคอมพิวเตอร์อยู่แล้วแต่เพื่อให้ครอบคลุมถึงข้อมูลประเภทอื่นๆ ที่อาจสร้างด้วยวิธีการทางอิเล็กทรอนิกส์อื่นๆ ในอนาคตที่ไม่ใช่เทคโนโลยีคอมพิวเตอร์ก็ได้

อย่างไรก็ตาม “ข้อมูลอิเล็กทรอนิกส์” ตามที่บัญญัติไว้ในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ได้ให้ความหมายคำว่า “ข้อมูลอิเล็กทรอนิกส์” ไว้ว่า “ข้อความที่ได้สร้างส่งเก็บรักษาหรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์เช่นวิธีการแลกเปลี่ยนข้อมูล

---

[9]พรเพชร วิชิตชลชัย, **คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550** (กรุงเทพฯ: โรงพิมพ์ดอกเบี้ย, 2550), หน้า 4.

อิเล็กทรอนิกส์จดหมายอิเล็กทรอนิกส์โทรเลขโทรพิมพ์หรือ โทรสาร” ดังนั้น ความหมายจึงกว้างรวมออกไปถึงโทรเลข โทรพิมพ์ โทรสาร อย่างไรก็ตาม องค์ประกอบความผิดตามพระราชบัญญัตินี้ส่วนใหญ่จะเชื่อมโยงองค์ประกอบความผิด “ข้อมูลคอมพิวเตอร์” กับ “ระบบคอมพิวเตอร์” เข้าด้วยกัน ดังนั้น กรณีของโทรเลข โทรพิมพ์ หรือโทรสารหากเป็นความผิดที่ต้องเชื่อมโยงกับระบบคอมพิวเตอร์ เช่น การดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์โดยมิชอบตามมาตรา 8 นั้น จะต้องเป็นกรณีที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์เป็นต้น ดังนั้น การดักรับโทรเลขโทรพิมพ์หรือโทรสารที่ไม่ได้ส่งในระบบคอมพิวเตอร์ย่อมไม่เป็นความผิดตามมาตราดังกล่าวเป็นต้น[10]

เมื่อพิจารณาถึงความหมายของคำว่า “ข้อมูลคอมพิวเตอร์” แล้วนั้น สิ่งที่จะต้องศึกษาต่อมาคือการกระทำผิดทางอาญาที่เกี่ยวกับข้อมูลคอมพิวเตอร์ที่เกิดขึ้น โดยการกระทำทางอาญาที่เกี่ยวกับคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้น ถูกเรียกว่า “อาชญากรรมทางคอมพิวเตอร์” ซึ่งมีรายละเอียด ดังต่อไปนี้

อาชญากรรมทางคอมพิวเตอร์ หมายถึง การกระทำผิดทางอาญาในระบบคอมพิวเตอร์ หรือการใช้คอมพิวเตอร์เพื่อกระทำผิดทางอาญา เช่น ทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลต่างๆ เป็นต้น ระบบคอมพิวเตอร์ในที่นี้ หมายรวมไปถึง ระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ที่เชื่อมกับระบบดังกล่าวด้วยสำหรับอาชญากรรมในระบบเครือข่ายคอมพิวเตอร์ เช่น อินเทอร์เน็ตอาจเรียกได้อีกอย่างหนึ่ง คือ อาชญากรรมไซเบอร์ (Cybercrime) อาชญากรที่ก่ออาชญากรรมประเภทนี้ มักถูกเรียกว่า แครกเกอร์

แต่เมื่อได้พิจารณาการกระทำความผิดทางคอมพิวเตอร์นั้นแล้ว ส่วนมากจะเป็นการคุกคามหรือลักลอบเข้าไปในระบบโดยไม่มีอำนาจ หรือ ไม่ได้รับอนุญาตให้กระทำการดังกล่าวได้ และการกระทำเช่นนั้นย่อมนำไปสู่การกระทำความผิดอื่นๆ ต่อไป เมื่อได้พิจารณาถึงความเป็นมาในการกระทำความผิดเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์แล้ว จะเห็นได้ว่าโปรแกรมคอมพิวเตอร์และข้อมูลจัดเก็บลงในแผ่นการ์ดที่เจาะรูเอาไว้ หากมีบุคคลบุกรุกเข้ามากระทำการไม่ว่าจะเป็นการจะทำลายหรือลักเอาแผ่นการ์ดเหล่านี้ บุคคลที่กระทำเช่นว่านี้ สามารถที่จะถูกลงโทษในกฎหมายอาญาในแบบเดิมได้ในฐานความผิดบุกรุก ทำลาย หรือลักทรัพย์ได้ แต่เมื่อปี ค.ศ.1975 ได้มีการเข้าสู่โปรแกรมและข้อมูลจากเครื่องคอมพิวเตอร์ที่อยู่ในระยะไกลโดยใช้โมเด็มและสายโทรศัพท์ การเปลี่ยนแปลงทางเทคโนโลยีเช่นนี้ทำให้อาชญากรสามารถเปลี่ยนแปลงข้อมูลทางกายภาพได้ ทำให้กฎหมายอาญาในรูปแบบเดิมไม่สามารถที่จะลงโทษเอาผิดกับอาชญากรได้อีกต่อไป จึงมีความจำเป็นที่จะต้องกำหนดกฎหมายเฉพาะขึ้นเพื่อที่จะลงโทษผู้กระทำความผิดต่อไป

ในขณะที่สำนักงานตำรวจแห่งชาติได้ให้ความหมายของคำว่า “อาชญากรรมคอมพิวเตอร์” ไว้ ดังนี้[11]

---

[10] *เรื่องเดียวกัน,* หน้า 4-5.

[11] สำนักงานตำรวจแห่งชาติ, **อาชญากรรมคอมพิวเตอร์**, ค้นวันที่ 9 ธันวาคม 2558 จาก http://www.royalthaipolice.go.th.

1. การกระทำใดๆ ที่เกี่ยวกับการใช้คอมพิวเตอร์ก็ตามทำให้มีผู้ได้รับความเสียหายและบุคคลที่กระทำนั้นได้รับผลประโยชน์ตอบแทน

2. การกระทำผิดกฎหมายใดๆ ที่ใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือและในการสืบสวนสอบสวนของเจ้าหน้าที่เพื่อนำตัวผู้กระทำความผิดมาดำเนินคดีก็ต้องใช้ความรู้ทางเทคโนโลยีคอมพิวเตอร์มาใช้เช่นกัน

ในปัจจุบันทั่วโลกนั้นได้แบ่งประเภทอาชญากรรมทางคอมพิวเตอร์ไว้ 9 ประเภท ดังนี้[12]

1. การขโมยข้อมูลทางอินเตอร์เน็ต รวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ
2. การปกปิดความผิดของตัวเอง โดยใช้ระบบการสื่อสาร
3. การละเมิดลิขสิทธิ์ ปลอมแปลงรูปแบบ เลียนแบบระบบซอฟแวร์โดยมิชอบ
4. การเผยแพร่ภาพ เสียง ลามก อนาจาร และข้อมูลที่ไม่เหมาะสม
5. การฟอกเงิน
6. การก่อกวนระบบคอมพิวเตอร์ เช่น ระบบจ่ายค่าน้ำ ค่าไฟ จราจร
7. การหลอกลวงให้ร่วมค้าขาย หรือ ลงทุนปลอม (การทำธุรกิจที่ไม่ชอบด้วยกฎหมาย)
8. การลักลอบการใช้ข้อมูลเพื่อแสวงหาผลประโยชน์ในทางที่มิชอบ เช่น การขโมยรหัสบัตรเครดิต
9. การใช้คอมพิวเตอร์ในการโอนบัญชีของผู้อื่นเป็นของตนเอง

ซึ่งลักษณะของอาชญากรทางคอมพิวเตอร์อาจจำแนกได้ดังต่อไปนี้[13]

1. พวกเด็กหัดใหม่ (Novice) เป็นพวกที่เริ่มเข้าสู่วงการ หัดใช้คอมพิวเตอร์ หรืออาจจะเป็นพวกที่เพิ่งเข้าสู่ตำแหน่งที่มีอำนาจหรือเพิ่งได้รับความไว้วางใจให้เข้าสู่ระบบเครือข่ายคอมพิวเตอร์

2. พวกจิตวิปริต (Deranged Persons) เป็นพวกที่มีจิตวิปริต ผิดปกติ มีลักษณะที่เป็นพวกชอบความรุนแรง และอันตราย มักเป็นผู้ที่ชอบทำลายไม่ว่าจะเป็นการทำลายข้าวของหรือบุคคล เนื่องจากจำนวนอาชญากรในประเภทนี้มีไม่มากนัก กฎหมายจึงไม่ได้ให้ความสนใจ

3. เป็นกลุ่มที่ประกอบอาชญากรรมในลักษณะองค์กร (Organized Crime) เป็นองค์กรอาชญากรรมที่ใช้คอมพิวเตอร์ในรูปแบบที่แตกต่างกันออกไป โดยบางส่วนอาจจะใช้เป็นเครื่องมือในการหาข่าวสาร หรือ อาจจะใช้เทคโนโลยีของคอมพิวเตอร์เป็นตัวประกอบสำคัญในการก่ออาชญากรรม หรือ อาจใช้เทคโนโลยีของคอมพิวเตอร์นี้เป็นตัวประกอบสำคัญในการก่ออาชญากรรม หรืออาจจะใช้เทคโนโลยีคอมพิวเตอร์นี้ในการที่ทำให้เจ้าหน้าที่ตามไม่ทันอาชญากรรมที่เกิดขึ้น

---

[12] ข้อมูลอนุกรรมการเฉพาะกิจร่างกฎหมายอาญาอาชญากรรมทางคอมพิวเตอร์

[13] ญาณพล ยั่งยืน, “อาชญากรรมคอมพิวเตอร์,” ใน **เอกสารประกอบการสัมมนาโครงการเพิ่มศักยภาพข้าราชการฝ่ายตุลาการศาลอุทธรณ์ภาค 9 ประจำปี พ.ศ.2550**, ค้นวันที่ 20 กรกฎาคม 2558 จาก http://elearning.aru.ac.th/4000108/hum07/topic3/linkfile/print5.htm

4. อาชญากรมืออาชีพ (Carrier Criminal) เป็นกลุ่มอาชญากรรมคอมพิวเตอร์ที่มีเพิ่มมากขึ้นเรื่อยๆ เป็นผู้ก่ออาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์นี้ โดยอาชญากรประเภทนี้ อาจจะเคยถูกจับกุมในความผิดประเภทนี้มาก่อนแล้ว เป็นผู้กระทำผิดโดยสันดาน แบ่งเป็น 4 ประเภท
1. ทำลายเว็บคู่แข่ง 2. เจาะระบบเพื่อขโมยข้อมูล 3. พยายามเจาะระบบของผู้ว่าจ้างเพื่อหาจุดอ่อน 4. เจาะระบบก่อนเสนอขายระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์

5. พวกหัวพัฒนา มีความก้าวหน้า (Conartists) เป็นพวกที่ชอบใช้ความก้าวหน้าทางด้านคอมพิวเตอร์เพื่อให้ได้มาเพื่อผลประโยชน์มาสู่ตนเอง อาชญากรประเภทนี้จะใช้ความรู้ทางด้านเทคโนโลยีและระบบคอมพิวเตอร์ที่ตนมีอยู่ในการที่จะหาเงินให้กับตนเองในทางที่ไม่ชอบด้วยกฎหมาย

6. พวกคลั่งลัทธิ หรือ พวกช่างคิดช่างฝัน เป็นพวกกระทำความผิดเนื่องมาจากมีความเชื่อถือสิ่งหนึ่งสิ่งใดอย่างรุนแรง

7. ผู้ที่มีความรู้และทักษะด้านคอมพิวเตอร์เป็นอย่างดี (Hacker/Cracker) โดย Hacker หมายถึง บุคคลผู้ที่เป็นอัจฉริยะ มีความรู้ในระบบคอมพิวเตอร์เป็นอย่างดี สามารถเข้าไปถึงข้อมูลในคอมพิวเตอร์โดยเจาะผ่านระบบ รักษาความปลอดภัยของ คอมพิวเตอร์ได้ แต่อาจไม่แสวงหาผลประโยชน์ได้

และอีกคำหนึ่งคือ Cracker หมายถึง ผู้ที่มีความรู้และทักษะทางคอมพิวเตอร์เป็นอย่างดีจนสามารถเข้าสู่ระบบได้ เพื่อเข้าไปทำลายหรือลบแฟ้มข้อมูล หรือ ทำให้เครื่องคอมพิวเตอร์เสียหาย รวมทั้งการทำลายระบบปฏิบัติการของเครื่องคอมพิวเตอร์

เพราะฉะนั้นจึงเห็นได้ว่าอาชญากรรมทางคอมพิวเตอร์มีหลายประเภท โดยวิทยานิพนธ์เล่มนี้จะขอพูดถึงอาชญากรรมทางคอมพิวเตอร์ที่เกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์เท่านั้น โดยการเข้าถึงข้อมูลคอมพิวเตอร์ทางด้านกฎหมายอาญา สามารถแบ่งเป็น 4 ลักษณะได้ดังนี้

1. การเจาะระบบรักษาความปลอดภัยทางกายภาพ ได้แก่ ตัวอาคาร อุปกรณ์และสื่อต่างๆ
2. การเจาะเข้าไปในระบบสื่อสารและการรักษาความปลอดภัยของซอฟแวร์ข้อมูลต่างๆ
3. เป็นการเจาะเข้าสู่ระบบรักษาความปลอดภัยของระบบปฏิบัติการ
4. เป็นการเจาะผ่านระบบรักษาความปลอดภัยส่วนบุคคลโดยใช้อินเทอร์เน็ตเป็นช่องทางในการกระทำความผิด

2.2 การเข้าถึงข้อมูลคอมพิวเตอร์

การเข้าถึงข้อมูลคอมพิวเตอร์เป็นการกระทำความผิดที่ใช้คอมพิวเตอร์เป็นเป้าหมายหรือวัตถุแห่งการกระทำความผิด (Computers as the Target of the Crime) โดยผู้ที่กระทำความผิดมีวัตถุประสงค์อยู่ที่ข้อมูลคอมพิวเตอร์เป็นสำคัญ ทั้งนี้อาจจะเป็นการเข้าถึงโดยการไปทำลาย เปลี่ยนแปลง หรือกระทำด้วยประการใดๆ เพื่อให้ข้อมูลดังกล่าวได้รับความเสียหาย หรือ มีการเปลี่ยนแปลงไปจากเดิม โดยผู้ที่กระทำอาจจะได้รับผลประโยชน์จากการกระทำดังกล่าวด้วยหรือไม่ก็ตาม

ซึ่งจะกล่าวไปว่าการกระทำนั้นเป็นการกระทำที่มีลักษณะในรูปแบบใหม่ที่อาศัยเทคโนโลยีที่ได้มีการพัฒนาไปเป็นเครื่องมือส่งเสริมการกระทำความผิดโยมีรูปแบบในการกระทำความผิดในรูปแบบใหม่ทั้งหมด จนไม่สามารถที่จะเอากฎหมายเดิมที่มีอยู่มากำหนดขอบเขตได้ และจำเป็นที่จะต้องมีการบัญญัติกฎหมายใหม่เพื่อกำหนดฐานความผิดขึ้นใหม่

2.2.1 ความหมายของการเข้าถึงข้อมูลคอมพิวเตอร์

การเข้าถึง (Access) คอมพิวเตอร์นั้น แบ่งได้เป็น 2 กรณี คือ การเข้าถึงในความหมายอย่างแคบ กล่าวคือ การเข้าไปโดยเทียบเคียงกับลักษณะของการบุกรุกที่เกิดขึ้นในโลกทางกายภาพ หรือ มีการเข้าไป (Inside) ในคอมพิวเตอร์ โดยได้มีการรุกล้ำเข้าไปโดยเทียบกับการบุกรุกที่มีการเข้าถึงสถานที่นั้น แต่ในการเข้าถึงคอมพิวเตอร์ได้มีความหมายอย่างกว้างมีแนวคิดที่อ้างอิงกับการทำงานของคอมพิวเตอร์เป็นหลัก โดยมุ่งเน้นไปที่การทำงานของคอมพิวเตอร์ที่เกิดขึ้นโดยเห็นว่าการเข้าถึงนั้น คือการทำให้คอมพิวเตอร์ทำงาน หากการกระทำเช่นนั้นทำให้เครื่องคอมพิวเตอร์มีการตอบสนองกับคำสั่งที่ได้มีการสั่งนั้น

นอกจากนี้ยังได้มีคำนิยามของคำว่า “การเข้าถึง” (Access) ไว้ว่าเป็นการเข้าถึงข้อมูลคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ เพราะฉะนั้นอาจจะหมายถึง การเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่างๆ ของคอมพิวเตอร์ หรือ ข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่ง หรือโอนไปยังบุคคลอีกคนหนึ่ง เช่น ข้อมูลจราจรทางคอมพิวเตอร์[14] เป็นต้น

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่าข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิดต้นทางปลายทางเส้นทางเวลาวันที่ปริมาณระยะเวลาชนิดของบริการหรืออื่นๆที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น กล่าวคือ ความหมายของ “ข้อมูลจราจรทางคอมพิวเตอร์” หมายถึง ข้อมูลที่แสดงรายการให้เห็นถึงการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ซึ่งจะแสดงถึงแหล่งกำเนิดเช่น IP Address ของเครื่องชื่อที่อยู่ของผู้ใช้บริการที่มีการลงทะเบียนข้อมูลของผู้ให้บริการ (Service Provider) ลักษณะของการให้บริการว่าผ่านระบบใดหรือเครือข่ายใดวันเวลาของการส่งข้อมูลและข้อมูลทุกประเภทที่เกิดจากการสื่อสาร (Communication) ผ่าน “ระบบคอมพิวเตอร์” การสื่อสารผ่านระบบคอมพิวเตอร์นั้นจะต้องมีระบบเครือข่ายคอมพิวเตอร์และมีผู้ให้บริการซึ่งผู้ให้บริการจะมีข้อมูลจราจรทางคอมพิวเตอร์อยู่ในระบบคอมพิวเตอร์ของตนและตามพระราชบัญญัตินี้กำหนดว่าผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ใช้บริการได้ใช้บริการในระบบคอมพิวเตอร์ของตนดังกล่าว

โดย “การเข้าถึง” ยังหมายความรวมไปถึง การเข้าถึงผ่านทางเครือข่ายสาธารณะอีกด้วย กล่าวคือ ผ่านทางอินเตอร์เน็ตที่เป็นการเชื่อมต่อระหว่างเครือข่ายหลายๆ เครือข่ายเข้าด้วยกัน และยังหมายความรวมไปถึงการเข้าถึงโดยผ่านการเชื่อมต่อกับเครือข่ายเดียวกันอีกด้วย เช่น ระบบ LAN (Local Area Network) ที่เป็นเครือข่ายที่มีการเชื่อมต่อกับคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆ เข้าไว้ด้วยกัน

---

[14] *เรื่องเดียวกัน,* หน้า 5.

การที่ได้มีการกำหนดให้การเข้าถึงโดยปราศจากอำนาจหรือกระทำการโดยการฝ่าฝืนต่อกฎหมาย ในการใช้คอมพิวเตอร์ไปในทางที่มิชอบในการเข้าถึงโดยไม่มีอำนาจหรือโดยฝ่าฝืนต่อกฎหมาย และการใช้คอมพิวเตอร์ในทางที่มิชอบนั้น ถือได้ว่าเป็นการกระทำที่คุกคามหรือเป็นภัยต่อความปลอดภัย (Security) ของระบบคอมพิวเตอร์และระบบข้อมูลที่มีผลกระทบต่อความครบถ้วน การรักษาความลับ และความมีเสถียรภาพในการใช้งาน ของระบบข้อมูล ซึ่งอาจจะนำมาซึ่งความเสียหายหรือการกระทำวามผิดในรูปแบบอื่นอีก เพราะฉะนั้น ในหลายๆ ประเทศจึงได้มีการกำหนดให้การเข้าถึงโดยมิชอบเป็นความผิดขึ้น การเข้าถึงโดยไม่ได้รับความยินยอมนี้จะเกิดเป็นความผิดได้ต่อเมื่อผู้กระทำสามารถเข้าถึงข้อมูลคอมพิวเตอร์นั้นได้ ซึ่งการเข้าถึงนั้นอาจจะเข้าโปรแกรมหรือไฟล์คอมพิวเตอร์ ผู้ที่กระทำอาจจะเป็นบุคคล หรือ คอมพิวเตอร์ที่ถูกสั่งการให้กระทำโดยการวางโปรแกรม การเข้าถึงจะสำเร็จได้โดยการใช้อิเล็กทรอนิกส์ เช่น ผ่านทางรหัส และโดยวิธีอื่นๆ หรืออาจทำสำเร็จโดยการเข้าถึงโดยทางกายภาพ เช่น การขโมยรหัสประจำตัว[15]

การเข้าถึงข้อมูลโดยมิชอบนั้น สามารถก่อให้เกิดความเสียหายแก่บุคคลเป็นส่วนตัว หรือแก่องค์กรโดยรวม เช่น การเข้าถึงข้อมูลส่วนบุคคลย่อมเป็นอันตรายต่อสิทธิส่วนบุคคล แต่ถ้าหากว่าผู้กระทำนำข้อมูลส่วนบุคคลนั้นไปเผยแพร่หรือจำหน่ายต่อให้แก่บุคคลอื่น

2.2.2 ลักษณะของการเข้าถึงข้อมูลคอมพิวเตอร์

ลักษณะการเข้าถึงโดยปราศจากอำนาจ อาจจะกล่าวได้ว่า ผู้กระทำส่วนใหญ่ไม่ได้มีความประสงค์ในการที่จะกระทำความผิด เช่น การเปลี่ยนแปลงเพื่อหลอกลวงข้อมูล ทำลายระบบ หรือจารกรรมข้อมูล เพียงแต่ผู้กระทำต้องการที่จะทดลองหรือทดสอบความสามารถของตนเพียงเท่านั้นในการที่จะฝ่าฝืนระบบรักษาความปลอดภัยของผู้อื่นเพียงเท่านั้น

2.2.3 ประเภทของการเข้าถึงข้อมูลคอมพิวเตอร์

แต่เดิมเครื่องคอมพิวเตอร์แต่ละเครื่องมีการทำงานที่แตกต่างแยกออกจากกัน แต่เมื่อได้พัฒนาการติดต่อสื่อสารให้มากขึ้นการเคลื่อนย้ายข้อมูลจำนวนมากจากที่หนึ่งไปยังอีกที่หนึ่งกลายเป็นสิ่งที่จำเป็น จึงได้เกิดเอาแนวความคิดที่ว่าจะนำเอาเครื่องคอมพิวเตอร์มาเชื่อมต่อกันผ่านสายสัญญาณ (Signal Cable)ที่ทำให้เกิดการส่งผ่านข้อมูลระหว่างเครื่องคอมพิวเตอร์ที่เร็วกว่าการบันทึกข้อมูลใส่อุปกรณ์บันทึกข้อมูลแล้วนำไปยังเครื่องอื่นๆ โดยการทำเช่นนี้เรียกว่าการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ “ระบบเครือข่ายคอมพิวเตอร์” ซึ่งการพัฒนานี้ทำให้การเจาะระบบคอมพิวเตอร์สามารถทำได้ง่าย รวดเร็ว และเกิดผลกระทบเป็นลูกโซ่

แต่เนื่องจากในอดีตคอมพิวเตอร์นั้นทำงานแยกออกจากกัน การเจาะระบบก็จะทำได้เฉพาะเครื่องเท่านั้นมักจะเป็นการทำทางกายภาพไม่สามารถที่จะทำในระยะไกลได้ อาจจะทำให้เกิดความเสียหายหากแต่ผลของความเสียหายนั้นไม่ได้ขยายเป็นวงกว้างและการเจาะระบบก็มีข้อจำกัดทั้งใน

---

[15]นพมาศ ประสิทธิ์มณฑล, **อาชญากรรมคอมพิวเตอร์ ตามกฎหมายสหรัฐอเมริกา กฎหมายอิเล็กทรอนิกส์เพื่อการศึกษา,** ค้นวันที่ 11 ธันวาคม 2558 จาก http://www.geocities.com/elaw007

เรื่องของเวลาและระยะทาง แต่เทคโนโลยีในระบบของเครือข่ายก็สามารถทำให้การเจาะระบบสามารถเกิดได้ทุกที่และสามารถใช้เวลาเท่าไหร่ก็ได้โดยไม่มีเวลาจำกัด เมื่อทำการเจาะระบบได้แล้วการที่จะเชื่อมต่อไปยังเครื่องคอมพิวเตอร์เครื่องอื่นก็สามารถทำได้เช่นกัน

ในระบบเครือข่ายคอมพิวเตอร์นั้น หมายถึง การนำเอาเครื่องคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไปมาเชื่อมโยงต่อเข้าด้วยกันโดยอาศัยสายเคเบิลชนิดต่างๆ และมีเครื่องคอมพิวเตอร์ขนาดใหญ่เป็นศูนย์กลางในการจัดเก็บและประมวลผลข้อมูลของเครื่องและเพื่อประโยชน์ในการใช้โปรแกรมซอฟแวร์และข้อมูลร่วมกันในการติดต่อสื่อสารและการแลกเปลี่ยนข้อมูลข่าวสารระหว่างผู้ใช้คอมพิวเตอร์ในเครือข่ายเดียวกันอีกด้วย โดยผู้ใช้คอมพิวเตอร์สามารถที่จะใช้งานผ่านคอมพิวเตอร์เครื่องใดๆก็ได้ในเครือข่าย

หากจะจำแนกระบบเครือข่ายคอมพิวเตอร์ตามระยะทางการเชื่อมต่อระหว่างอุปกรณ์การสื่อสาร สามารถที่จะแบ่งได้เป็น 3 ลักษณะ ดังต่อไปนี้

1. Local Area Network (LAN) คือ เป็นระบบเครือข่ายคอมพิวเตอร์ที่ได้มีการเชื่อมต่อสื่อสารกับอุปกรณ์ในระยะทางที่จำกัด ซึ่งการเชื่อมต่อดังกล่าวนั้นจะมีความเร็วในการแลกเปลี่ยนข้อมูลที่แตกต่างกันไปในเฉพาะกลุ่มของหน่วยงาน ดังนั้น จึงเป็นเครือข่ายแบบปิด (Close Network) เชื่อมระบบอินเตอร์เน็ต เป็นต้น

2. Metropolitan Area Network (MAN) เป็นระบบเครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่และครอบคลุมพื้นที่มากกว่าระบบเครือข่ายแบบ LAN เครือข่ายนี้มีการเชื่อมต่อระหว่างเครือข่ายคอมพิวเตอร์แบบ LAN 2 เครื่อง เข้าด้วยกัน

3. Wide Area Network (WAN) เป็นระบบเครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่ประกอบด้วยระบบเครือข่ายคอมพิวเตอร์ทั้งแบบ LAN และเครือข่ายคอมพิวเตอร์แบบ MAN พื้นที่เครือข่ายสามารถที่จะครอบคลุมพื้นที่ได้ในระดับประเทศหรือระดับโลก และเป็นระบบเครือข่ายแบบเปิด (Open Network) ซึ่งระบบนี้ก็ถือว่าเป็นเครือข่ายอินเตอร์เน็ตในรูปแบบ WAN เช่นเดียวกัน

เพราะฉะนั้นจะเห็นได้ว่า เมื่อได้มีการพัฒนาเทคโนโลยีให้มีความทันสมัยตามแต่ละยุคสมัย รูปแบบการกระทำความผิดก็ย่อมมีการพัฒนาตามไปด้วย การเจาะระบบก็เช่นเดียวกัน ในยุคปัจจุบันนั้นไม่ได้เฉพาะแต่ระบบคอมพิวเตอร์เท่านั้นที่มีการกระทำความผิด ระบบการให้บริการแบบอื่นๆ ก็มีการกระทำความผิดเกิดขึ้นด้วยเช่นกัน เช่น บริการโทรศัพท์ทางอินเตอร์เน็ต โทรศัพท์ทางไกล บริการจดหมายเสียง เป็นต้น และการเข้าถึงต่างๆ ไม่ใช่เพียงแต่เข้าไปทำลายระบบป้องกัน หรือรักษาความปลอดภัยเพียงอย่างเดียวเท่านั้น แต่ผู้กระทำต้องการที่จะลักลอบใช้บริการเหล่านั้นโดยไม่ต้องเสียเงินอีกด้วย ฉะนั้น จากเดิมการกระทำความผิดในรูปแบบนี้ไม่ได้เป็นภัยต่อเศรษฐกิจมากนัก แต่ในปัจจุบันการกระทำความผิดดังกล่าวได้สร้างความเสียหายที่เกิดขึ้นในรูปแบบอื่นๆ อีกมากมาย[16]

ในรูปแบบของการกระทำความผิดที่เกิดขึ้นเยอะที่สุด คือ การเจาะข้อมูล (Hacking And Cracking) คือ การเข้าไปในระบบคอมพิวเตอร์โดยที่ไม่มีอำนาจ กล่าวคือ ในกรณีที่ผู้กระทำความผิดกระทำการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้มาซึ่งรหัสผ่านโดยอาจจะเป็นการใช้เครื่องคอมพิวเตอร์ของผู้อื่น

---

[16]สาวิตรี สุขศรี, **ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์**, ค้นวันที่ 13 ธันวาคม 2558 จาก http://www.siamsewana.org

โดยตรงหรืออาจจะเป็นกรณีที่มีการเข้าถึงโดยผู้กระทำอยู่ห่างโดยระยะทาง อย่างเช่น การเจาะข้อมูลผ่านทางเครือข่ายอินเตอร์เน็ต อินทราเน็ต หรือ ระบบ LAN โดยการเข้าถึงข้อมูลคอมพิวเตอร์นั้นผู้กระทำไม่ได้มีเหตุจูงใจในการกระทำ หรือ ต้องการทำให้เกิดความเสียหายต่อระบบแต่อย่างใด เรียกว่า Hacking แต่ในกรณีที่เข้าไปเพื่อทำลาย หรือ ก่อให้เกิดความเสียหายต่อข้อมูล จะเรียกว่า Cracking

2.2.4 รูปแบบของการเข้าถึงข้อมูลคอมพิวเตอร์

การเข้าถึง (Access)[17] หมายถึง การเข้าถึงทั้งในระดับกายภาพเช่นกรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์และผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเองและหมายความรวมถึงการเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้

นอกจากนั้นยังหมายถึง การเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนอีกด้วย ดังนั้นจึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์หรือส่วนประกอบต่างๆ ของคอมพิวเตอร์ข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น

ส่วนวิธีการเข้าถึงนั้นรวมทุกวิธีการไม่ว่าจะเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตอันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆ เครือข่ายเข้าด้วยกันและยังหมายถึง การเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้เช่นระบบ LAN (Local Area Network) อันเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆ เข้าด้วยกันนอกจากนี้ยังหมายความรวมถึง การเข้าถึงโดยการติดต่อสื่อสารแบบไร้สาย (Wireless Communication) อีกด้วย การเจาะเข้าไปในระบบนั้นมีขั้นตอนที่หลากหลายซึ่งในนี้จะขอกล่าวถึงการเจาะระบบแบบทั่วไป ดังนี้

1.การแกะรอย (Foot Printing) เป็นวิธีการในการค้นหา และดึงข้อมูลมาใช้เพื่อหาช่องว่างในสิ่งที่ต้องการ เช่น ชื่อโดเมน หมายเลขเครือข่าย รูปแบบการติดต่อเครือข่าย เพื่อรวบรวมข้อมูล โดยจะทำการตรวจสอบในสิ่งต่างๆไม่ว่าจะเป็นในเรื่องของความปลอดภัยหรือพฤติกรรมการใช้งาน กระบวนการตรวจสอบนี้จะตรวจสอบโดยการแยกทั้งในเครือ และนอกเครือข่าย

2.การตรวจสอบหรือสแกน (Scan) เป็นวิธีการแกะรอยโดยผู้เจาะระบบได้ทำการตรวจสอบข้อมูลก่อนที่จะเริ่มการโจมตี และในการสแกนนี้เป็นการตรวจสอบเพื่อเข้าไปดูข้อมูล หรือรายละเอียดภายในอีกขั้นตอนหนึ่ง ซึ่งอาจจะทำได้โดยกา Ping Sweeps, ICMP Queries หรือ Port Scanning

3.การเจาะระบบ (Hacking) เป็นการเจาะระบบที่สามารถทำได้ง่ายที่สุด กล่าวคือ การเข้าไปถึงตัวเครื่องในวิธีส่วนใหญ่ผู้เจาะระบบเริ่มจากการลวงข้อมูลในเครื่องก่อน ซึ่งจะทำการรวบรวมรหัสผ่านจากไฟล์ PW หรือ การแฮกรหัสผ่านจากโปรแกรมสำเร็จรูปผ่านเครือข่ายภายใน หรือจากเครื่องอื่นๆ

---

[17] *เรื่องเดียวกัน,* หน้า 8-9.

ซึ่งพบว่าผู้ใช้ได้มีการล็อครหัสผ่านเครือข่าย ซึ่งการล็อคนั้นจะมี User Name และ Password ซึ่งด้วยระบบคอมพิวเตอร์นั้นเมื่อผู้ใช้ได้ทำการเข้าสู่ระบบจะมีไฟล์ PW ขึ้นมาจากเครือข่ายหลัก และตรงจุดนี้จะเป็นการเปิดโอกาสให้มีการเจาะระบบปฏิบัติการ เช่น Microsoft Network Unix เป็นต้น ซึ่งไฟล์ PW จะถูกเข้ารหัสด้วยอัลกอรึทึมที่เข้ารหัสนี้ไม่ยากต่อการถอดรหัสทั้ง Unix และ Windows NT ซึ่งผู้กระทำสามารถทำได้เพียงแค่ Copy ไฟล์ดังกล่าว ในเครื่องหลัก และ Copy ไฟล์ลงแผ่นดิสก์ หรือส่งไฟล์ผ่าน E-Mail เท่านั้น และบุคคลทั่วไปสามารถที่จะแฮกโปรแกรม PW ที่บ้าน หรือจะทำผ่านเว็บก็ได้ ซึ่งถ้าได้ไฟล์ PW ก็สามารถแฮกหรือควบคุมระบบใดๆ ก็ได้

ในเครื่องคอมพิวเตอร์ส่วนตัวที่ถูกแฮกนั้นผู้กระทำสามารถที่จะดูได้ทั้งจากการล็อคอิน หรือเกิดจากการพูดคุยกันผ่านคีบอร์ด (กรณีที่เจ้าของเครื่องไม่อยู่) ถ้าผู้เจาะระบบได้รับ Root หรือ Administrator ผู้เจาะระบบสามารถติดตั้งโปรแกรมที่อนุญาตให้คีย์บนเครื่องลูกข่าย และส่งผ่านทางไกลได้ด้วย

นอกจากนี้วิธีการแฮกแบบทั่วไป การแฮกที่เป็นที่นิยมทำกันในปัจจุบันคือการแฮกโดยผ่านระบบสืบค้นข้อมูล โดยเฉพาะ Google สาเหตุที่ Google เป็นระบบค้นหาที่แฮกเกอร์นิยมใช้กันก็เพราะ Google มีฐานข้อมูลเป็นเว็บไซต์ต่างๆ ที่ระบบค้นหาสมบูรณ์มากที่สุด สามารถใส่เงื่อนไขหรือพารามิเตอร์ในการค้นหาได้อย่างละเอียด ทำให้ผลลัพธ์ที่ได้คือข้อมูลที่มีความถูกต้องตรงกับความต้องการมากที่สุด

สำหรับแฮกเกอร์แล้วนั้น การได้มาซึ่งข้อมูลเป็นสิ่งที่สำคัญที่สุดโดยเฉพาะอีเมลล์แอดเดรส หากแฮกเกอร์ต้องการที่จะเจาะเข้าไปในระบบของหน่วยงานราชการหรือองค์กรธุรกิจ ประการแรกที่ต้องทำคือ ค้นหาอีเมล์แอ็คเคาต์ ของบุคคลากรในหน่วยงานนั้นๆ ให้ได้ หากแฮกเกอร์สามารถเจาะเข้าไปเพื่ออ่านข้อมูลในอีเมล์ได้จะเป็นช่องทางที่ทำให้เกิดความเสียหายได้อย่างมากมาย เพราะฉะนั้นจึงเห็นได้ว่า Google หรือแม้แต่เว็บอื่นๆ มีความสามารถหรือมีสมรรถนะในการสืบค้นหาข้อมูลได้อย่างละเอียดและถูกต้องมากขึ้นเท่าไร การนำวิธีของแฮกเกอร์ไปใช้ก็เพื่ออำนวยผลประโยชน์ให้มีมากขึ้นเท่านั้น

2.3 แนวคิดเกี่ยวกับการคุ้มครองสิทธิ

สิทธิในการได้รับความคุ้มครองเป็นสิทธิส่วนตัว และเสรีภาพในการสื่อสาร ต่างก็เป็นสิทธิและเสรีภาพขั้นพื้นฐานของมนุษย์ ประกอบกับปัจจุบันในประเทศไทยนั้นได้ให้ความสำคัญกับสิทธิเป็นอย่างมาก ไม่ว่าบุคคลใดจะกระทำอะไรก็จำเป็นที่จะต้องคำนึงถึงสิทธิของบุคคลอื่นอีกด้วย กล่าวคือ จะต้องคำนึงว่าการกระทำของตนจะไปกระทบหรือละเมิดสิทธิของผู้อื่นหรือไม่ ด้วยประการเช่นนี้ ในประเทศต่างๆ จึงได้มีแนวความคิดที่จะรับรองในสิทธิขั้นพื้นฐานของมนุษย์ ที่มนุษย์ควรจะได้รับการคุ้มครองสิทธิไม่ให้ถูกละเมิดโดยบุคคลหรือหน่วยงานใด

ต่อมาแนวความคิดเกี่ยวกับการคุ้มครองสิทธิได้มีการเผยแพร่เป็นอย่างมาก จนทำให้หลายๆ ประเทศพัฒนาการคุ้มครองสิทธิ และเมื่อประเทศต่างๆ ได้ปฏิบัติตามกฎเกณฑ์ในการคุ้มครองสิทธิจนกลายเป็นแนวทางปฏิบัติ องค์กรระหว่างประเทศจึงได้ริเริ่มและพัฒนาแนวทางในการปฏิบัติให้เป็นกฎหมายหรือกฎเกณฑ์ระหว่างประเทศ ด้วยการวางและพัฒนากรอบทางกฎหมาย ทั้งนี้ เพื่อให้

ประเทศสมาชิกได้ใช้เป็นแนวทางในการพัฒนากฎหมายหรือกำหนดให้เป็นกฎเกณฑ์ภายในประเทศของตน เพื่อให้กฎหมายนี้มีมาตรฐานในการให้ความคุ้มครองสิทธิในระดับที่ดีและให้เป็นไปในทิศทางเดียวกันต่อไป

2.3.1 ความหมายของสิทธิและเสรีภาพ

คำว่า “สิทธิ” ศาสตราจารย์ ดร.หยุด แสงอุทัย ได้อธิบายความหมายไว้ว่า อำนาจที่กฎหมายให้แก่บุคคลในอันที่จะมีเจตจำนงเพื่อประโยชน์อย่างใดอย่างหนึ่งซึ่งบุคคลมุ่งประสงค์ ตามความเห็นของนักกฎหมายชาวเยอรมันสองคน คือ Windscheid และ Jhering

ดร.โภคิน พลกุล ได้ให้ความเห็นไว้ว่า อำนาจหรือประโยชน์ที่กฎหมายรับรองและคุ้มครองให้

Alex Well ได้ให้ความหมายไว้ว่า อำนาจที่กฎหมายรับรองให้แก่บุคคลในอันที่จะกระทำการเกี่ยวข้องกับทรัพย์หรือบุคคลอื่น

จึงอาจกล่าวได้ว่า สิทธิ (Right) คือ อำนาจที่กฎหมายรับรองให้แก่บุคคลในอันที่จะกระทำการเกี่ยวข้องกับทรัพย์หรือผู้อื่น โดยมีเจตนาเพื่อประโยชน์อย่างใดอย่างหนึ่ง

ถึงอย่างไรก็ตามถึงแม้ว่ากฎหมายจะให้การรับรองหรือคุ้มครองให้มีสิทธิที่จะกระทำการใดอันเกี่ยวข้องกับทรัพย์หรือผู้อื่นไว้ก็ตาม แต่การกระทำดังกล่าวหากมีขึ้นเพื่อประโยชน์อย่างใดๆ ตามที่กฎหมายให้สิทธิไว้ จะต้องเป็นการกระทำที่ไม่ขัดหรือแย้งหรือไม่ชอบด้วยกฎหมาย

คำว่า “เสรีภาพ” หมายความว่า ความคิดของมนุษย์ที่ไม่ได้ตกอยู่ภายใต้การครอบงำของบุคคลอื่น หรือภาวะที่ปราศจากการหน่วงเหนี่ยว ขัดขวาง หรือสถานภาพของมนุษย์ที่จะไม่ตกอยู่ภายใต้การบังคับบัญชาของบุคคลใด หรืออำนาจที่จะกระทำการอย่างใดอย่างหนึ่ง หรือไม่กระทำอย่างใดอย่างหนึ่ง[18]

ศาสตราจารย์ ดร.หยุด แสงอุทัย ได้ให้ความหมายคำว่า “เสรีภาพ” ไว้ว่า อิสระที่จะกระทำหรืองดเว้นที่จะไม่กระทำตามที่กฎหมายได้บัญญัติไว้[19]

เพราะฉะนั้น จากความหมายดังกล่าวจะเห็นได้ว่า บุคคลย่อมมีเสรีภาพในการที่เขาจะไม่ถูกบังคับให้กระทำในสิ่งที่เขาไม่ต้องการจะกระทำ หรือ ถูกหน่วงเหนี่ยว ขัดขวางไม่ให้เขากระทำในสิ่งที่เขาต้องการที่จะกระทำ อาจกล่าวได้ว่า เสรีภาพ คือ อำนาจของคนที่จะตัดสินด้วยตนเองในการที่จะเลือกกระทำการใดๆในการที่จะดำเนินพฤติกรรมใดๆ ของตนเองโดยบุคคลอื่นไม่มีอำนาจที่จะมาบังคับเกี่ยวข้องในการตัดสินใจ กล่าวคือ เรามีอำนาจในการที่จะกำหนดได้ด้วยตนเอง มีอำนาจที่จะเลือกวิถีการดำเนินการชีวิตด้วยตนเอง เมื่อพิจารณาแล้วเห็นความหมายของเสรีภาพในทางกฎหมายหมายถึง อำนาจของบุคคลที่จะตัดสินใจกระทำการหรือไม่กระทำการใดๆ ที่ไม่เป็นการฝ่าฝืนต่อกฎหมาย

---

[18]วีระ โลจายะ, “สิทธิเสรีภาพของประชาชน,” ใน **เอกสารการสอนวิชากฎหมายมหาชน เล่มที่ 2**, พิมพ์ครั้งที่ 9 (นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2545), หน้า 462.

[19]หยุด แสงอุทัย, **กฎหมายอาญา 1**, พิมพ์ครั้งที่ 20 แก้ไขเพิ่มเติม (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2551.

2.3.2 การคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัวหรือสิทธิส่วนบุคคล

แนวคิดความเป็นส่วนตัว (โดย Samuel D. Warren และ Louis D. Brandeis ปี ค.ศ. 1890) ความเป็นส่วนตัวหมายถึง “สิทธิที่จะอยู่โดยลำพัง” (The Right to be let Alone) “ความเป็นส่วนตัว” หรือ “Privacy” เป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์ที่สังคมยุคใหม่เกือบทุกประเทศให้ความสำคัญอย่างมากดังจะเห็นได้จากการรับรองหลักการดังกล่าวไว้ในรัฐธรรมนูญหรือแม้บางประเทศจะไม่ได้บัญญัติรับรองไว้โดยตรงในรัฐธรรมนูญแต่ก็ได้ตราบทบัญญัติรับรองไว้ในกฎหมายเฉพาะ “ความเป็นส่วนตัว” ได้รวมถึงการคุ้มครองสิทธิส่วนบุคคลซึ่งเป็นการตีความคำว่า “ความเป็นส่วนตัว” ในด้านการจัดการสิทธิส่วนบุคคลในความเป็นส่วนตัวเกี่ยวกับสิทธิเป็นการให้ความคุ้มครองสิทธิ

โดยหลักการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right of Privacy) จากการกระทำละเมิดประกอบด้วย

1. ความรับผิดฐานบุกรุก (Trespass)
2. การก่อให้เกิดความเดือดร้อนรำคาญ (Nuisance)
3. หมิ่นประมาท (Defamation)
4. ความรับผิดต่อความไว้วางใจต่อกัน (Breach of Confidence)
5. การกระทำโดยประมาทเป็นเหตุให้ผู้อื่นได้รับความเสียหาย (Negligence)[20]
6. การคุ้มครองสิทธิส่วนบุคคลในเรื่องการค้นและการยึดทรัพย์สิน (Searches and Seizures)

สิทธิในความเป็นส่วนตัว หรือ สิทธิส่วนบุคคล (Right of Privacy) ในที่ประชุม ICJ (International Commission of Jurists) ได้ให้ความหมายไว้ในที่ประชุมว่า “สิทธิที่จะอยู่โดยลำพังโดยมีการรบกวนการแทรกแซงในระดับที่น้อยที่สุด” ซึ่งต่อมาได้มีการขยายให้มีความหมายกว้างขึ้นคือ “สิทธิของปัจเจกชนที่จะดำเนินชีวิตโดยได้รับการคุ้มครองจากสิ่งเหล่านี้” คือ[21]

1. การแทรกแซงในชีวิตความเป็นส่วนตัว ครอบครัว และเคหะสถาน
2. การแทรกแซงในทางกายภาพ หรือในทางจิตใจ หรือศีลธรรมและเสรีภาพในทางความคิด
3. การกระทำต่อเกียรติยศและชื่อเสียง
4. การไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนความจริง ซึ่งทำให้เป็นที่เสื่อมเสียในสายตาของสาธารณชน

---

[20]สกล อดิศรประเสริฐ, **มาตรการทางกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเฉพาะกรณีการแยะแยะประเภทข้อมูลส่วนบุคคล** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์, 2552.

[21]วีระพงษ์ บึงไกร, **การเปิดเผยข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2543.

5. การเปิดเผยข้อเท็จจริงที่ไม่ถูกต้องที่ไม่ถูกต้องอันเป็นที่น่าอับอายเกี่ยวกับชีวิตความเป็นส่วนตัว

6. การใช้ชื่อหรือเครื่องหมายชี้เฉพาะหรือภาพโดยไม่มีอำนาจ

7. การสืบความลับ การสอดรู้สอดเห็น การติดตามเฝ้าดู และการรบกวน

8. การแทรกแซงการติดต่อสื่อสารระหว่างกัน

9. การเปิดเผยข้อมูลข่าวสารที่เป็นความลับ ซึ่งผู้กระทำได้รับมาอันเนื่องมาจากการประกอบอาชีพนั้น

10. การใช้งานในทางที่มิชอบซึ่งการติดต่อสื่อสารส่วนบุคคล

ดังนั้น บุคคลควรได้รับการคุ้มครองและให้ความเคารพในสิทธิความเป็นส่วนตัวคือการมีอิสรเสรีภาพในการดำรงชีวิตอยู่ในสังคม มีสิทธิที่จะหาความสุขในชีวิตให้กับตัวเองตามวิถีทางที่พอจะเป็นไปได้และการดำรงชีวิตนั้นจะต้องไม่ขัดต่อหลักกฎหมาย ไม่ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน

2.3.3 การคุ้มครองตามหลักสากลและการคุ้มครองตามหลักกฎหมายไทย

การคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัวหรือสิทธิส่วนบุคคลของประเทศสหรัฐอเมริกานั้นได้ให้คำนิยามของ “ส่วนบุคคล” ไว้หมายถึงข้อมูลรายบุคคลที่สามารถระบุได้เกี่ยวกับบุคคลที่เก็บรวบรวมแบบออนไลน์รวมทั้งชื่อและนามสกุลที่อยู่ที่บ้านหรือที่อยู่เชิงกายภาพอื่นๆ รวมทั้งชื่อถนนและชื่อเทศบาลนครหรือเทศบาลเมืองที่อยู่อีเมล์หมายเลขโทรศัพท์หมายเลขประกันสังคมหรือตัวระบุอื่นใดที่คณะกรรมาธิการกำหนดใบอนุญาตการติดต่อทางกายภาพหรือออนไลน์ของแต่ละบุคคลที่เจาะจงหรือข้อมูลเกี่ยวข้องกับบุคคลเหล่านั้นที่เว็บไซต์เก็บรวบรวมบนเว็บไซต์และในเวลาต่อมายังได้มีการแก้ไขเพิ่มเติมนิยามคำว่า “ข้อมูลส่วนบุคคล” ให้หมายความรวมถึงข้อมูลเกี่ยวกับที่อยู่ทางกายภาพ (Geo Location Information) ภาพถ่าย (Photograph) และวิดีโอด้วยซึ่งในการให้ความหมายของข้อมูลส่วนบุคคลตามกฎหมายในประเทศสหรัฐอเมริกานั้นครอบคลุมถึงข้อมูลต่างๆ ของบุคคลที่ออนไลน์หรือข้อมูลของบุคคลบนอินเทอร์เน็ตด้วย

การคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัวหรือสิทธิส่วนบุคคลของประเทศอังกฤษได้ให้คำนิยาม “ข้อมูลส่วนบุคคล” ไว้ว่าหมายถึง ข้อมูลซึ่งเกี่ยวกับบุคคลที่มีชีวิตอันสามารถระบุตัวได้จากข้อมูลนั้นหรือจากข้อมูลนั้นและข้อมูลอื่นซึ่งอยู่ในความครอบครองหรือกำลังจะอยู่ในความครอบครองของผู้ควบคุมข้อมูล

นิยามการคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัวหรือสิทธิส่วนบุคคลตามกฎหมายของประเทศไทยดังกล่าวนั้น ยังไม่ครอบคลุมถึงข้อมูลส่วนบุคคลในด้านอื่นๆ อีกเป็นจำนวนมาก เช่น ข้อมูลเกี่ยวกับพฤติกรรมทางเพศ ข้อมูลเกี่ยวกับกิจกรรมส่วนตัวใดๆ ที่ควรปกปิดเป็นความลับ และความเป็นอยู่ส่วนตัวอันไม่พึงเปิดเผย เป็นต้น ส่งผลให้มีการล่วงละเมิดสิทธิของบุคคลเป็นจำนวนมาก ประกอบกับปัจจัยเทคโนโลยีสารสนเทศและการสื่อสารได้มีการพัฒนาและมีการส่งผ่านข้อมูลส่วนบุคคลระหว่างประเทศ ซึ่งเมื่อเทียบกับนิยามการคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัวหรือสิทธิส่วนบุคคลของต่างประเทศ ซึ่งสามารถระบุตัวบุคคลนั้นได้ไม่ว่าโดยทางตรงหรือทางอ้อม การกำหนดให้ข้อมูลส่วนบุคคลรวมถึงข้อมูลที่สามารถระบุตัวบุคคลนั้นได้แม้ว่าในเบื้องต้นนั้น

จะมาสามารถระบุตัวบุคคลดังกล่าว หากที่สุดแล้วก็สามารถระบุตัวบุคคลได้โดยอยู่ภายใต้กฎหมายเช่นเดียวกัน และต่างประเทศได้มีกฎหมายกลางว่าด้วยการคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัวหรือสิทธิส่วนบุคคลไว้

เนื่องจากการคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัว หรือ สิทธิส่วนบุคคลนั้นมีหลายประเด็นที่ควรให้ความสำคัญและในประเทศไทยได้มีการกล่าวถึงข้อมูลส่วนบุคคลอันเป็นสิทธิมนุษยชนขั้นพื้นฐานอย่างกว้างขวาง เช่น

ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2540 มาตรา 34 สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครองการกล่าวหรือไขข่าวแพรหลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัวเกียรติยศ ชื่อเสียง หรือความเป็นอยู่สวนตัวจะกระทำมิได้ เว้นแต่ กรณีที่เป็นประโยชน์ต่อสาธารณชน[22]

ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550 มาตรา 4 ศักดิ์ศรีความเป็นมนุษย์สิทธิเสรีภาพ และความเสมอภาคของบุคคลย่อมได้รับความคุ้มครอง[23] มาตรา 35 สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครองการกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ตามที่กฎหมายบัญญัติ[24]

จะเห็นได้จากรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550 มาตรา 35 เป็นบทบัญญัติเพิ่มเติมจากรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2540 มาตรา 34 เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลให้มีความเหมาะสมมากขึ้น

ถึงแม้ว่าจะมีบทบัญญัติของกฎหมายกำหนดให้การคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัวหรือ สิทธิส่วนบุคคลไว้ให้มีความเหมาะสมกันในแต่ยุคแต่ละสมัย แต่เนื่องจากในปัจจุบันเป็นยุคที่มีระบบการติดต่อสื่อสารผ่านทางเทคโนโลยีสารสนเทศ และเทคโนโลยีสารสนเทศนี้ได้มีพัฒนาการให้มีความสะดวก รวดเร็วมากขึ้น ทำให้การติดต่อสื่อสารระหว่างฐานข้อมูลมีความรวดเร็วมากขึ้นและยังสามารถเชื่อมต่อข้อมูลถึงกันได้ทั่วโลก แต่พัฒนาการของเทคโนโลยีสารสนเทศนั้นก็ได้ส่งผลไปกระทบถึงสิทธิในความเป็นส่วนตัวของบุคคล กล่าวคือ เมื่อสื่อยิ่งได้มีการพัฒนามากขึ้นการเข้าถึงข้อมูลก็มีมากขึ้นและการเข้าถึงข้อมูลของบุคคลก็จะเป็นการไปละเมิดสิทธิความเป็นส่วนตัวของบุคคลได้ง่ายขึ้น

ซึ่งจะเห็นได้จากการรับรู้และการเข้าถึงข้อมูลข่าวสารในปัจจุบันจะต้องอาศัยเทคโนโลยีสื่อสารสนเทศที่มีการเชื่อมต่อผ่านโครงข่ายแบบไร้สายที่สามารถเชื่อมต่อกันได้ทั่วโลก จึงทำให้สามารถรับรู้ข้อมูลข่าวสารได้แบบเสถียรภาพ แต่การรับรู้ข้อมูลข่าวสารของบุคคลหรือข้อมูลส่วนตัว

---

[22]มาตรา 34 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2540

[23]มาตรา 4 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550

[24]มาตรา 35 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550

(Right of Privacy) ข้อมูลเหล่านั้นอาจจะเป็นข้อมูลที่สามารถเปิดเผยได้ และไม่สามารถที่จะเปิดเผยให้สาธารณะชนได้ทราบได้ เนื่องจากการเปิดเผยข้อมูลในบางส่วนอาจจะไปกระทบต่อความรู้สึกของเจ้าของข้อมูลและอาจจะทำให้เจ้าของข้อมูลได้รับความเสียหายได้

กรอบในการคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัว หรือ สิทธิส่วนบุคคลมีกรอบตามหลักของสากลประเทศและประเทศไทยได้นำมาเป็นกรอบในการคุ้มครองในการเข้าถึงข้อมูลส่วนบุคคลผ่านทางข้อมูลอิเล็กทรอนิกส์ กรอบในการคุ้มครองข้อมูลในส่วนนี้จะรวมไปถึงองค์กรที่ให้ความร่วมมือทางด้านเศรษฐกิจอีกด้วย (Guidelines Governing the Protection of Privacy and Tran Border Data Flows of Personal Data) ซึ่งมีกรอบพื้นฐานดังต่อไปนี้ ประกอบไปด้วย

1. หลักข้อจำกัดในการเก็บรวบรวมข้อมูล

สาระสำคัญในการเก็บรวบรวมข้อมูลนั้น ต้องชอบด้วยกฎหมายและต้องใช้วิธีการที่เป็นธรรมและเหมาะสมโดยในการเก็บรวบรวมข้อมูลนั้นต้องให้เจ้าของข้อมูลรู้เห็น รับรู้หรือได้รับความยินยอมจากเจ้าของข้อมูล

2. หลักคุณภาพของข้อมูล

สาระสำคัญ ข้อมูลที่เก็บรวบรวมนั้น ต้องเกี่ยวข้องกับวัตถุประสงค์ที่กำหนดขึ้นว่า “จะนำไปใช้ทำอะไร” และเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานตามที่กฎหมายกำหนด นอกจากนั้นข้อมูลดังกล่าวจะต้องถูกต้อง สมบูรณ์หรือทำให้เป็นปัจจุบันหรือทันสมัยอยู่เสมอ

3. หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ

สาระสำคัญ ต้องกำหนดวัตถุประสงค์ว่าข้อมูลที่มีการเก็บรวบรวมนั้น เก็บรวมรวมไปเพื่ออะไร พร้อมทั้งกำหนดระยะเวลาที่เก็บรวบรวมหรือรักษาข้อมูลนั้น ตลอดจนกรณีที่จำเป็นต้องมีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเช่นว่านั้นไว้ให้ชัดเจน

4. หลักข้อจำกัดในการนำไปใช้

สาระสำคัญ ข้อมูลส่วนบุคคลนั้นจะต้องไม่มีการเปิดเผย ทำให้มีหรือปรากฏในลักษณะอื่นใดซึ่งไม่ได้กำหนดไว้โดยชัดแจ้งในวัตถุประสงค์ของการเก็บรวบรวมข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลหรือโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

5. หลักการรักษาความมั่นคงปลอดภัยข้อมูล

สาระสำคัญจะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมเพื่อป้องกันความเสี่ยงภัยใดๆ ที่อาจจะทำให้ข้อมูลนั้นสูญหายเข้าถึง ทำลาย ใช้ดัดแปลงแก้ไข หรือเปิดเผยโดยมิชอบ

6. หลักการเปิดเผยข้อมูล

สาระสำคัญ ควรมีการประกาศนโยบายฯให้ทราบโดยทั่วกัน หากมีการปรับปรุงแก้ไข หรือพัฒนาแนวนโยบายหรือแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคลก็ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้ข้อมูลใดๆ ที่สามารถระบุเกี่ยวกับหน่วยงานของรัฐผู้ให้บริการ ที่อยู่ผู้ควบคุมข้อมูลส่วนบุคคลด้วย

7. หลักการมีส่วนร่วมของบุคคล

สาระสำคัญ ให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับแจ้งหรือยืนยันจากหน่วยงานของรัฐที่เก็บรวบรวมหรือจัดเก็บข้อมูลทราบว่า “หน่วยงานของรัฐนั้นๆ ได้รวบรวมข้อมูลหรือจัดเก็บข้อมูลส่วนบุคคลดังกล่าวหรือไม่ ภายในระยะเวลาที่เหมาะสม”

8. หลักความรับผิดชอบ

สาระสำคัญ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

ดังนั้นจึงเห็นได้ว่า สิทธิส่วนบุคคล หมายถึงสิทธิประจำตัวของบุคคลประกอบด้วย เสรีภาพในร่างกาย การดำรงชีวิต มีความเป็นส่วนตัว ซึ่งได้รับการรับรองคุ้มครองตากกฎหมายมิให้ผู้ใดมาล่วงละเมิดได้

2.4 แนวคิดเกี่ยวกับกระบวนการยุติธรรม

การทำงานของคอมพิวเตอร์ทำให้การสืบสวนสอบสวนกระทำได้ยาก ข้อมูลหลักฐานเป็นสื่อที่มีผลโดยตรงต่อการรับฟังพยานหลักฐานในชั้นศาล เพราะคอมพิวเตอร์เป็นสิ่งที่มีความซับซ้อนละเอียดอ่อนมาก กล่าวคือ พยานหลักฐานทางอิเล็กทรอนิกส์เป็นหลักฐานประเภทที่ไม่สามารถมองเห็นได้เป็นประจักษ์ ทั้งสภาพที่แท้จริงของสื่ออิเล็กทรอนิกส์ที่ใช้เป็นพยานหลักฐานในคดีอาชญากรรมไซเบอร์เป็นคนละเรื่องกับสิ่งที่เห็นเป็นประจักษ์ในสิ่งที่เราสามารถเข้าใจได้ เพราะสื่ออิเล็กทรอนิกส์ในเครื่องคอมพิวเตอร์เป็นเพียงคลื่นแม่เหล็กที่ผ่านการแปลงสัญญาณเพื่อเปลี่ยนสภาพให้เป็นสื่อในลักษณะที่มนุษย์สามารถเข้าใจได้ การที่ต้องผ่านกระบวนการแปลงด้วยวิธีส่งสัญญาณด้วยเครื่องคอมพิวเตอร์ที่อยู่ในการควบคุมของเจ้าพนักงานอาจจะเชื่อถือไม่ได้ว่าพยานหลักฐานดังกล่าวจะไม่มีการเปลี่ยนแปลงแก้ไข หรือ ถูกทำให้สูญหายไปเสียก่อน

ดังนั้น ถ้าจะทำการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์นั้น มีหลักเกณฑ์ในการค้นและยึดตามประมวลกฎหมายวิธีพิจารณาความอาญา กล่าวคือ ถ้าจะทำการค้นจะต้องมีหมายค้นจากศาล ซึ่งการออกหมายค้นจะต้องมีเหตุที่จะออกหมายด้วย และการยึดสิ่งของที่ค้นพบของพนักงานสอบสวน ที่เป็นพยานอิเล็กทรอนิกส์ดังกล่าวทำอย่างไรกับพยานหลักฐานที่เกี่ยวข้องและสามารถที่จะรับฟังเป็นพยานหลักฐาน โดยมีหลักเกณฑ์ที่เกี่ยวข้อง ดังต่อไปนี้

2.4.1 การค้นหาพยานหลักฐาน

การค้นในที่รโหฐานต้องมีหมายค้น กล่าวคือ ตามเจตนารมณ์ของกฎหมายรัฐธรรมนูญแห่งราชอาณาจักรไทย ในประเด็นหนึ่งที่มุ่งประสงค์ต่อการให้ความคุ้มครองของประชาชนในการที่จะครอบครองอสังหาริมทรัพย์ กล่าวคือ เป็นการคุ้มครองสิทธิของเจ้าของบ้านไม่ให้ถูกรบกวนแม้แต่จากเจ้าหน้าที่ของรัฐก็ตาม เพราะฉะนั้น การที่พนักงานเจ้าหน้าที่จะเข้าไปทำการตรวจค้นที่พักของบุคคลใดอันเป็นการไปรบกวนการครอบครองดังกล่าว การจะเข้าไปตรวจค้นนั้นจะต้องมีหมายค้นจากศาลเพื่อเป็นการตรวจสอบไม่ให้การใช้อำนาจเข้าไปทำการตรวจค้นโดยพลการ หรือมีเหตุให้ค้น

ได้ภายใต้อำนาจกฎหมายวิธีพิจารณาความอาญา ซึ่งเป็นกฎหมายที่รองรับในการให้อำนาจไว้ในมาตรา 92(1)-(5)

การค้นที่รโหฐาน คำว่า “รโหฐาน” ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 2 (13) ได้ให้คำนิยามไว้ว่า หมายถึง ที่ต่างๆ ที่ไม่ใช่ที่สาธารณสถานดั่งที่บัญญัติไว้ในกฎหมายลักษณะอาญา และเมื่อพิจารณาคำว่า “สาธารณสถาน” ตามประมวลกฎหมายอาญามาตรา 1 (3) ได้ให้คำนิยามไว้ว่า หมายถึง สถานที่ใดๆ ที่ประชาชนมีความชอบธรรมที่จะเข้าไปได้ เพราะฉะนั้น ที่รโหฐานจึงหมายถึงสถานที่ใดๆ ที่ประชาชนไม่มีความชอบธรรมที่จะเข้าไปได้ ซึ่งอาจจะรวมไปถึง ที่ที่เป็นสถานที่ซึ่งมีเจ้าของอันเป็นสถานที่ส่วนตัว เช่น เคหสถาน สำนักงานหรืออสังหาริมทรัพย์ที่อยู่ในความครอบครองโดยปกติสุขของผู้อื่น โดยมีการแสดงให้เห็นชัดโดยการล้อมรั้วหรือสร้างกำแพง เป็นต้น หรืออาจจะเป็นการแสดงเจตนาโดยปริยายหรือโดยสภาพแห่งสถานที่นั้นๆ เช่น บริเวณเคหสถาน บ้านเรือนของบุคคลใดๆ ย่อมเป็นที่รโหฐานอยู่ในตัว

ในเรื่องของการค้นตามสถานที่กฎหมายมุ่งประสงค์ที่จะคุ้มครองสถานที่ที่เป็นที่อยู่อาศัยของบุคคลเป็นสำคัญ ทั้งนี้ก็เพื่อเป็นการเคารพสิทธิของบุคคลในการที่จะอยู่อาศัยในเคหสถานด้วยความปกติสุข ปราศจากการรบกวนจากบุคคลภายนอก เว้นแต่ การค้นนั้นจะได้รับความยินยอมจากผู้ครอบครองตามที่ได้บัญญัติไว้ในรัฐธรรมนูญ มาตรา 35 ที่ว่า “. . . การเข้าไปในเคหสถานโดยปราศจากความยินยอมของผู้ครอบครอง หรือ การตรวจค้นเคหสถานจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย” กล่าวคือ ถ้าบุคคลที่ครอบครองสถานที่นั้นได้ให้ความยินยอมให้ทำการตรวจค้นด้วยความสมัครใจ เพื่อแสดงเจตนาให้เห็นว่าไม่มีสิ่งผิดกฎหมายใดๆ ซ้อนอยู่ เจ้าพนักงานอาจเข้าไปตรวจค้นได้ แต่การตรวจค้นจะต้องมีหมายจากศาลด้วย แต่การยินยอมดังกล่าวต้องเป็นไปด้วยความสมัครใจจริงๆ หากความยินยอมนั้นเกิดขึ้นเพราะความเกรงกลัวเนื่องจากการข่มขู่ของเจ้าพนักงาน หรือ เป็นเพราะมีเหตุอย่างใดอย่างหนึ่งเกิดขึ้น โดยไม่ได้เกิดจากความสมัครใจดังนี้อาจถือไม่ได้ว่าเป็นความยินยอมตามรัฐธรรมนูญดังกล่าว

การค้นตามหมายค้น ในการที่จะออกหมายค้นได้นั้นจะต้องมีเหตุที่ออกหมายค้นได้ด้วย หมายค้นคือเครื่องมือในการที่จะทำการสืบพยานหลักฐานในคดีอาญาที่อยู่ในที่รโหฐาน เหตุที่ออกหมายค้นตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 69 กล่าวคือ เพื่อหาพยานหลักฐาน เพื่อหาของกลาง เพื่อช่วยบุคคล เพื่อจับบุคคล และเพื่อพบและยึดสิ่งของตามคำพิพากษาในการค้นหาพยานหลักฐานหรือหาของกลางนั้น เจ้าพนักงานผู้ที่จะทำการค้นสิ่งของดังกล่าวจะต้องมีเหตุอันควรเชื่อได้ว่าสิ่งของนั้นจะใช้เป็นหลักฐานที่อยู่ในเคหสถานที่จะเข้าไปค้นด้วย

ข้อยกเว้นในการค้นโดยไม่มีหมายค้น ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 238 ในตอนท้ายที่เปิดช่องให้เจ้าพนักงานสามารถทำการค้นได้โดยไม่มีหมายค้น แต่ทั้งนี้จะต้องกระทำภายใต้ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92[25] ที่บัญญัติว่า

[25] มาตรา 92 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

ห้ามมิให้ค้นในที่รโหฐานโดยไม่มีหมายค้นหรือคำสั่งของศาล เว้นแต่พนักงานฝ่ายปกครองหรือตำรวจเป็นผู้ค้น และในกรณี ดังต่อไปนี้

(1) เมื่อมีเสียงร้องให้ช่วยมาจากข้างในที่รโหฐาน หรือมีเสียงหรือพฤติการณ์อื่นใดอันแสดงได้ว่ามีเหตุร้ายเกิดขึ้นในที่รโหฐานนั้น

(2) เมื่อปรากฏความผิดซึ่งหน้ากำลังกระทำลงในที่รโหฐาน

(3) เมื่อบุคคลที่ได้กระทำความผิดซึ่งหน้า ขณะที่ถูกไล่จับหนีเข้าไปหรือมีเหตุอันแน่นแฟ้น ควรสงสัยว่าได้เข้าไปซุกซ่อนตัวอยู่ในที่รโหฐานนั้น

(4) เมื่อมีพยานหลักฐานตามสมควรว่าสิ่งของที่มีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิดหรือได้ใช้หรือมีไว้เพื่อจะใช้ในการกระทำความผิด หรืออาจเป็นพยานหลักฐานพิสูจน์การกระทำความผิดได้ซ่อนหรืออยู่ในนั้น ประกอบทั้งต้องมีเหตุอันควรเชื่อว่าเนื่องจากการเนิ่นช้ากว่าจะเอาหมายค้นมาได้สิ่งของนั้นจะถูกโยกย้ายหรือทำลายเสียก่อน

(5) เมื่อที่รโหฐานนั้นผู้จะต้องถูกจับเป็นเจ้าบ้าน และการจับนั้นมีหมายจับหรือจับตามมาตรา 78

กล่าวคือ ห้ามไม่ให้ทำการค้นในที่รโหฐานโดยไม่มีหมายค้น แต่ทั้งนี้ทั้งนั้นกฎหมายได้บัญญัติกำหนดข้อยกเว้นไว้ในอนุมาตรา (1)-(5) ที่ให้พนักงานฝ่ายปกครองหรือตำรวจสามารถเข้าทำการค้นในที่รโหฐานได้โดยไม่ต้องมีหมายค้น ในส่วนที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์ ให้ใช้อนุมาตรา (2) (4) และ (5) กล่าวคือ (2) เมื่อมีความผิดปรากฏซึ่งหน้าที่กำลังกระทำลงในที่รโหฐาน ความผิดซึ่งหน้าในที่นี้ไม่จำกัดว่าต้องเป็นความผิดประเภทใดก็ตามที่ระบุไว้ในบัญชีท้ายประมวลกฎหมายวิธีพิจารณาความอาญาแต่ต้องเป็นความผิดที่ปรากฏต่อหน้าเจ้าพนักงาน กล่าวคือ กำลังกระทำต่อหน้าเจ้าพนักงาน

ตามความหมายใน (4) กล่าวคือ เมื่อมีเหตุอันควรสงสัยว่าสิ่งของที่ได้มานั้นได้มาโดยการกระทำความผิดได้ซ่อนหรืออยู่ในนั้น ประกอบทั้งจะต้องมีเหตุอันควรเชื่อได้ว่าเนื่องจากการกระทำนั้นช้ากว่าจะไปขอหมายค้นจากศาลได้สิ่งของเหล่านั้นจะถูกโยกย้ายเปลี่ยนแปลงสถานที่เสียก่อน ข้อยกเว้นของการจะเข้าอนุมาตรานี้ได้จะต้องปรากฏความจริงให้เห็นเป็นที่ประจักษ์เสียก่อน คือ

1. มีความสงสัยว่าสิ่งของได้ถูกซ่อนหรืออยู่ในนั้น

2. มีเหตุอันควรเชื่อได้ว่าจะต้องดำเนินการออกหมายค้นจะทำให้เกิดความล่าช้า อาจจะทำให้มีการโยกย้ายสิ่งของจากที่รโหฐานนั้นก่อนได้ แต่ข้อยกเว้นตามมาตรา 92 (4) นี้จำกัดเฉพาะกรณี สิ่งของที่ได้มาโดยการกระทำความผิดเท่านั้น ไม่ได้หมายความรวมไปถึงการใช้คอมพิวเตอร์ในการเข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ แม้จะเป็นสิ่งของที่จำเป็นต้องยึดเพื่อประกอบไว้ในสำนวนแต่ก็ไม่ได้ทำให้เจ้าพนักงานสามารถเข้าค้นได้โดยไม่มีหมายค้น อย่างไรก็ตามอาจเป็นเหตุให้ออกหมายค้นได้ตามมาตรา 69 (2) ต่อไปก็ได้

ตามความหมายใน (5) กล่าวคือ เมื่อที่รโหฐานนั้นผู้เป็นเจ้าของบ้านจะต้องถูกจับและการจับนั้นมีหมายจับหรือจับตามมาตรา 78 เป็นการค้นภายหลังการจับกุมบุคคลฐานก่ออาชญากรรมโดยชอบแล้ว ซึ่งต้องเป็นการค้นทันทีทันใดเพื่อป้องกันการทำลายพยานหลักฐานในภายหลัง

ผู้ที่มีอำนาจค้นตามประมวลกฎหมายวิธีพิจารณาความอาญากำหนด ได้แก่

(1) พนักงานฝ่ายปกครอง หรือ ตำรวจ มาตรา 92

(2) พนักงานสอบสวน มาตรา 132 (2)

ผู้ที่จะทำการค้นได้จะต้องเป็นพนักงานฝ่ายปกครองหรือตำรวจนั้น ดั่งที่ปรากฏไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92 และถ้าหากว่าเป็นการค้นโดยมีหมายตามมาตรา 97 ได้บัญญัติไว้ว่า ในกรณีที่ค้นโดยมีหมาย เจ้าพนักงานผู้มีชื่อในหมายค้นหรือผู้รักษาการแทนซึ่งต้องเป็นพนักงานฝ่ายปกครองตั้งแต่ระดับสามหรือตำรวจซึ่งมียศตั้งแต่ชั้นร้อยตำรวจตรีขึ้นไปเท่านั้น มีอำนาจเป็นหัวหน้าไปจัดการให้เป็นไปตามหมายนั้น กล่าวคือ เจ้าพนักงานที่มีรายชื่ออยู่ในหมายค้นหรือผู้รักษาการแทนเท่านั้นที่จะมีอำนาจเป็นหัวหน้าไปจัดการตามหมายค้น ทั้งนี้ยังแสดงให้เห็นหมายค้นจะต้องระบุตัวเจ้าพนักงานว่าผู้ใดจะเป็นผู้ทำการค้น ดังนั้น เจ้าพนักงานอื่นๆ อาจค้นได้ในฐานะเป็นผู้ช่วยในการค้นเท่านั้นเอง

กรณีการค้นโดยไม่มีหมายค้น ผู้ที่มีอำนาจค้นคือพนักงานฝ่ายปกครองหรือตำรวจที่มีเหตุให้ค้นได้ตามมาตรา 92 (1)-(5) ซึ่งเป็นข้อยกเว้นของการค้นโดยไม่มีหมายค้น

ในกรณีที่เป็นพนักงานสอบสวนมีอำนาจค้นได้ในฐานะเป็นเจ้าพนักงานตำรวจตามที่บัญญัติไว้ในมาตรา 92 แต่มาตรา 132 (2) ยังให้อำนาจพนักงานสอบสวนทำการค้นสิ่งของที่มีไว้เป็นความผิดหรือได้มาโดยการกระทำผิด หรือได้ใช้ หรือสงสัยว่าได้ใช้ในการกระทำความผิด หรืออาจซึ่งใช้เป็นพยานหลักฐานได้ แต่จะต้องอยู่ภายใต้บทบัญญัติแห่งประมวลกฎหมายนี้ที่ว่าด้วยเรื่องของการค้น กล่าวคือ ถ้าหากจะค้นในที่รโหฐานจะต้องมีหมายค้นจากศาล

โดยทั่วไปแล้วนั้นการค้นกฎหมายไม่ได้ให้อำนาจราษฎรทำการค้นใดๆ ได้นอกจากกรณีที่จะค้นตัวผู้หญิง กับในกรณีค้นหาสิ่งของที่หายได้ที่ให้เจ้าของหรือผู้ครอบครองสิ่งนั้น หรือผู้แทนของเขาไปกับเจ้าพนักงานในการค้นนั้น เพื่อความสะดวกในการค้นและตรวจสอบว่าสิ่งของนั้นเป็นของของตนที่หายไปหรือไม่ แต่ในคดีอาชญากรรมทางคอมพิวเตอร์แม้จะมีความจำเป็นที่จะต้องให้บุคคลภายนอกในการช่วยสืบค้นหาข้อมูล ซึ่งบุคคลภายนอกดังกล่าวอาจอยู่ในฐานะเป็นผู้เกี่ยวข้องหรือใกล้ชิดข้อมูล หรือเป็นผู้เชี่ยวชาญพิเศษด้านคอมพิวเตอร์ แต่เมื่อกฎหมายไม่ได้บัญญัติให้อำนาจไว้ การค้นหาหลักฐานทางอิเล็กทรอนิกส์จึงต้องอาศัยความสามารถจากพนักงานสืบสวนแต่เพียงฝ่ายเดียวเวลาที่ทำการค้น ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 96 ที่บัญญัติไว้ว่า

> การค้นในที่รโหฐานต้องกระทำระหว่างพระอาทิตย์ขึ้นและตก กล่าวคือ จะทำการค้นในเวลากลางคืนไม่ได้ แต่การค้นในเวลากลางคืนนั้นก็ได้มีข้อยกเว้นไว้ว่า
>
> (1) เมื่อลงมือค้นแต่ในเวลากลางวัน ถ้ายังไม่เสร็จจะค้นต่อไปในเวลากลางคืนก็ได้ กล่าวคือ เมื่อเจ้าพนักงานได้ทำการค้นในเวลากลางวันแล้วยังหาบุคคลหรือสิ่งของที่เป็นที่สงสัยยังไม่พบ หรือค้นได้สิ่งของบางอย่างแล้วแต่ยังได้ไม่ครบตามที่ต้องการและเชื่อได้ว่าถ้าค้นต่อไปอาจจะพบหรือได้ข้อมูลจนครบ ถือได้ว่าการค้นยังไม่เสร็จเจ้าพนักงานมีอำนาจค้นต่อไปได้ในเวลากลางคืน แต่การค้นนั้นจะต้องกระทำโดยติดต่อกันด้วย หากการค้นในเวลากลางวันแล้วไม่พบแล้วกลับออกไปแล้วกลับเข้ามาค้นใหม่ในเวลากลางคืนย่อมไม่สามารถที่จะกระทำได้

(2) ในกรณีฉุกเฉินอย่างยิ่ง หรือซึ่งมีกฎหมายอื่นบัญญัติให้ค้นได้เป็นพิเศษ จะทำการค้นในเวลากลางคืนก็ได้ กล่าวคือ กรณีฉุกเฉินอย่างยิ่ง หมายความว่า ถ้าไม่ทำการค้นในเวลากลางคืนจะเกิดอันตรายแก่ชีวิตหรือร่างกายของบุคคลที่ต้องการค้นให้พบตัว หรือบุคคลนั้นอาจจะหลบหนีไปเสียก่อน หรือพยานหลักฐานอาจจะถูกทำลาย ทั้งคดีนั้นจะต้องมีลักษณะที่ร้ายแรงอีกด้วย

ในกรณีทีมีกฎหมายพิเศษเฉพาะให้อำนาจกับเจ้าพนักงานค้นในเวลากลางคืนได้ เจ้าพนักงานย่อมทำได้ตามเงื่อนไขของกฎหมายพิเศษนั้น

2.4.2 การยึดพยานหลักฐาน

จะต้องสามารถทำให้ศาลเชื่อโดยปราศจากข้อสงสัยว่าจำเลยได้กระทำความผิดจริง (Prove Beyond Reasonable Doubt) ซึ่งพยานหลักฐานที่ศาลจะรับฟังเพื่อลงโทษจำเลยได้จะต้องเป็นพยานหลักฐานที่ได้มาโดยชอบด้วยกฎหมายและสามารถพิสูจน์ความผิดหรือความบริสุทธิ์ของจำเลยได้ รวมถึงมาตรการในการยึดสิ่งของและกระบวนการในการเก็บรักษาสิ่งของที่จะใช้เป็นพยานหลักฐาน เพื่อให้ศาลเห็นว่าเป็นพยานหลักฐานที่ถูกต้องแท้จริงปราศจากการแก้ไข

ประมวลกฎหมายวิธีพิจารณาความอาญา บัญญัติให้พนักงานสอบสวนมีอำนาจยึดไว้ซึ่งสิ่งของที่ค้นพบ ดังเช่น เมื่อพนักงานสอบสวนพบเครื่องคอมพิวเตอร์ส่วนบุคคลตามหมายค้น แต่สิ่งที่พนักงานสอบสวนต้องการคือ ข้อมูลภายในเครื่องคอมพิวเตอร์นั้น ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์ ถือว่าเป็นสิ่งของที่อยู่ในอำนาจของพนักงานสอบสวนที่จะทำการยึดเพื่อรวบรวมไว้เป็นหลักฐานได้ เมื่อพนักงานสอบสวนสามารถเข้าถึงข้อมูลที่ต้องสงสัยได้แล้ว จะต้องคำนึงถึงวิธีที่ถูกต้องเพื่อกักหรือล็อคข้อมูลนั้นไว้ให้อยู่ และยึดพยานหลักฐานที่เกี่ยวข้องอย่างอื่นให้อยู่ในสภาพที่เป็นจริงที่สุด เพื่อให้สิ่งทั้งหลายที่ยึดมานั้นมีน้ำหนักน่าเชื่อถือตามประมวลกฎหมายวิธีพิจารณาความอาญาได้บัญญัติไว้ คือ

สิ่งของที่ยึดได้ในการค้นให้ห่อหรือบรรจุหีบห่อตราไว้ ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 101 ที่บัญญัติว่า สิ่งของที่ยึดได้ในการค้นให้ห่อหรือบรรจุหีบห่อตีตราไว้ หรือให้ทำเครื่องหมายไว้เป็นสำคัญ กล่าวคือ เพื่อป้องกันไม่ให้มีการสับเปลี่ยนสิ่งของที่ค้นได้ เพราะฉะนั้นจึงรวมไปถึงการยึดข้อมูลอิเล็กทรอนิกส์จากเครื่องคอมพิวเตอร์ด้วย

เมื่อมีการค้นสิ่งของที่ยึดไว้เป็นพยานหลักฐานจะต้องมีการบรรจุหีบห่อตีตรา และทำเครื่องหมายไว้เป็นสำคัญเพื่อป้องกันการสับเปลี่ยนพยานหลักฐาน และให้ทำการบันทึกรายละเอียดในการค้นเพื่อประกอบสำนวนและการบันทึกรายละเอียดนั้นจะต้องอ่านให้ผู้ที่เกี่ยวข้องตามที่กำหนดไว้ในมาตรา 103 ฟังด้วย และให้บุคคลดังกล่าวลงลายมือชื่อรับรองเป็นการยืนยันว่าเป็นพยานหลักฐานที่ได้ทำการยึดมาจริง จากนั้นให้รีบส่งไปยังผู้ออกหมาย คือ ส่งไปให้ศาล ในกรณีที่มีการตรวจพิสูจน์แล้ว ในกรณีที่เป็นข้อมูลอิเล็กทรอนิกส์หากมีความจำเป็นจะต้องส่งให้ตรวจพิสูจน์ก่อนเสมอ

2.4.3 การรับฟังพยานหลักฐาน

พยานหลักฐานที่ได้มาโดยกระบวนการต่างๆ ที่กล่าวมาข้างต้นจะต้องนำพยานหลักฐานที่ได้มานั้นมานำเสนอต่อศาลในกระบวนการนี้ ความถูกต้องแท้จริงของพยานหลักฐานเป็นสิ่งที่สำคัญที่สุด และอย่างไรศาลถึงจะเชื่อว่าพยานหลักฐานที่นำมาเสนอนั้นเป็นข้อมูลหรือหลักฐานที่ไม่ได้มีการเปลี่ยนแปลงแก้ไข และทำให้พยานประเภทนี้มีความน่าเชื่อถือพอที่ศาลจะฟังลงโทษจำเลยได้ หากพิจารณาหลักการและกฎหมายประกอบกันแล้วจะมีหลักดังต่อไปนี้ คือ ต้องเป็นพยานหลักฐานที่ได้มาโดยชอบ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 ที่อาจถือได้ว่าเป็นบทตัดพยานตามกฎหมายของไทย ที่ได้บัญญัติไว้ว่า พยานวัตถุ พยานเอกสาร หรือ พยานบุคคล ซึ่งอาจจะพิสูจน์ได้ว่าจำเลยผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานหลักฐานชนิดที่ไม่ได้เกิดจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบด้วยประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือ กฎหมายอื่นที่ว่าด้วยการสืบพยาน ประกอบกับประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 135 ที่บัญญัติไว้ว่า ห้ามมิให้พนักงานสอบสวนทำหรือทำการใดๆ ซึ่งเป็นการล่อลวง หรือขู่เข็ญ หรือให้สัญญากับผู้ต้องหาเพื่อจูงใจให้เขาให้การอย่างใดๆ ในเรื่องที่ต้องหานั้น

ในกรณีที่พนักงานสอบสวนได้พยานหลักฐานใดมาด้วยประการใดมาด้วยการกระทำที่ต้องด้วยสองมาตราดังกล่าวข้างต้น อาจถือได้ว่าสิ่งเหล่านั้นเป็นพยานหลักฐานที่ไม่ชอบ ซึ่งรวมไปถึงถ้าหากพยานหลักฐานเหล่านั้นได้มาโดยมิชอบแล้ว ศาลจะรับฟังพยานหลักฐานนั้นๆ ไม่ได้

ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227 ที่บัญญัติไว้ว่า ให้ศาลใช้ดุลพินิจวินิจฉัยชั่งน้ำหนักพยานหลักฐานทั้งปวง อย่าพิพากษาลงโทษจนกว่าจะแน่ใจว่ามีการกระทำผิดจริงและจำเลยเป็นผู้กระทำความผิดนั้น กล่าวคือ เมื่อมีความสงสัยตามสมควรว่าจำเลยได้กระทำความผิดหรือไม่นั้นให้ยกประโยชน์แห่งความสงสัยนั้นให้แก่จำเลย หมายถึง การแสดงให้ศาลเห็นด้วยพยานหลักฐานถึงการมีอยู่จริงของขอเท็จจริงโดยปราศจากความสงสัย หากมีความสงสัยแม้แต่เพียงเล็กน้อยจากพยานหลักฐานว่าจำเลยได้กระทำผิดจริงหรือไม่ก็ต้องยกฟ้องโจทก์โดยการปล่อยตัวจำเลยไป และการจะเป็นพยานหลักฐานซึ่งน่าจะพิสูจน์ได้ว่าจำเลยผิดหรือบริสุทธิ์ ให้หมายความรวมไปถึง ในคดีอาญานั้นไม่ว่าจะเป็นพยานวัตถุ พยานเอกสาร หรือ พยานบุคคล ที่อาจจะพิสูจน์ได้ว่าจำเลยผิดหรือบริสุทธิ์ คู่ความสามารถอ้างเป็นพยานหลักฐานได้ทั้งสิ้น ซึ่งเป็นการเปิดโอกาสที่จะให้โจทก์และจำเลยสามารถนำพยานเข้ามาในคดีได้อย่างเต็มที่

กล่าวคือการคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัวหรือสิทธิส่วนบุคคลของประเทศสหรัฐอเมริกานั้นหมายถึงข้อมูลรายบุคคลที่สามารถระบุได้เกี่ยวกับตัวบุคคลนั้นๆ และการคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัวหรือสิทธิส่วนบุคคลตามกฎหมายของประเทศไทยนั้นยังมีความหมายที่ไม่ชัดเจนเพราะการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว หรือสิทธิส่วนบุคคลยังมีหลายประเด็นที่ควรให้ความสำคัญและในประเทศไทยได้มีการกล่าวถึงข้อมูลส่วนบุคคลอันเป็นสิทธิมนุษยชนขั้นพื้นฐานไว้อย่างกว้างขวางถึงแม้ว่าจะมีบทบัญญัติของกฎหมายกำหนดให้การคุ้มครองของสิทธิในความเป็นอยู่ส่วนตัว หรือ สิทธิส่วนบุคคลไว้ให้มีความเหมาะสมกันในแต่ยุคแต่ละสมัย แต่เนื่องจากในปัจจุบันเป็นยุคที่มีระบบการติดต่อสื่อสารผ่านทางเทคโนโลยีสารสนเทศ และเทคโนโลยีสารสนเทศทำให้การติดต่อสื่อสารระหว่างฐานข้อมูลมีความสะดวกรวดเร็วมากยิ่งขึ้นและยังสามารถเชื่อมต่อ

ข้อมูลถึงกันได้ทั่วโลก และพัฒนาการของเทคโนโลยีสารสนเทศนั้นก็ได้ส่งผลไปกระทบถึงสิทธิในความเป็นส่วนตัวของบุคคล เช่น ในกรณีที่พนักงานเจ้าหน้าที่จะทำการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์ตามประมวลกฎหมายวิธีพิจารณาความอาญา ที่ได้มีการกำหนดหลักเกณฑ์ในการค้นและยึดไว้ว่าถ้าจะทำการค้นจะต้องมีหมายค้นจากศาล ซึ่งการจะออกหมายค้นจะต้องมีเหตุที่จะออกหมายด้วย ซึ่งกรณีใดบ้างที่จะต้องข้อหมายจากศาล ผู้เขียนจะทำการพิเคราะห์ในบทต่อไป

บทที่ 3

มาตรการทางกฎหมายที่เกี่ยวข้องกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในการเข้าถึงข้อมูลคอมพิวเตอร์ตามหลักกฎหมายไทยและกฎหมายต่างประเทศ

3.1 อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลคอมพิวเตอร์ในประเทศไทย

เพื่อให้การดำเนินคดีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เป็นไปอย่างมีประสิทธิภาพ จึงได้มีหลักเพิ่มขึ้นในพระราชบัญญัติเป็นกรณีพิเศษ มี 2 ประการ ดังนี้

1. การเพิ่มวิธีพิเศษในการสืบสวนและสอบสวน และ
2. การเพิ่มให้พนักงานเจ้าหน้าที่เข้ามามีอำนาจในการสืบสวนและสอบสวนความผิดตามพระราชบัญญัตินี้ นอกเหนือไปจากเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญา

แต่อย่างไรก็ตาม พระราชบัญญัตินี้ได้มีการกำหนดการใช้อำนาจของพนักงานเจ้าหน้าที่ว่าพนักงานเจ้าหน้าที่จะใช้อำนาจได้ก็ต่อเมื่อเป็นกรณีที่มีเหตุอันควรเชื่อได้ว่าได้มีการกระทำความผิดเกิดขึ้นตามพระราชบัญญัตินี้ หากความผิดที่เกิดขึ้นเป็นความผิดตามกฎหมายอื่นย่อมไม่เข้าเงื่อนไขที่พนักงานเจ้าหน้าที่จะใช้อำนาจตามพระราชบัญญัตินี้ได้[26] เนื่องมาจากในการใช้อำนาจหน้าที่ของพระราชบัญญัติเดิม ถึงแม้ว่าจะมีการตรวจสอบหรือควบคุมการใช้อำนาจของรัฐอยู่หลายมาตรา หากแต่การใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่นั้น ได้มีบัญญัติไว้ในลักษณะที่ให้พนักงานเจ้าหน้าที่สามารถใช้อำนาจได้ในบางกรณีเท่านั้น เช่น ในกรณีที่เจ้าหน้าที่ “เพียงแค่สงสัยเท่านั้น” ต่อมาเพื่อที่จะให้พนักงานเจ้าที่มีอำนาจเพิ่มมากขึ้นจึงได้มีการปรับแก้ให้มีการใช้อำนาจหน้าที่นั้นได้ก็ต่อเมื่อ “มีเหตุอันควรเชื่อ” แต่การใช้อำนาจของพนักงานเจ้าที่ยังคงต้องใช้เฉพาะเท่าที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานอันมีความเกี่ยวข้องกับการกระทำความผิด และต้องการหาตัวผู้กระทำความผิดเท่านั้น[27]

ตามมาตรา 18 แห่งพระราชบัญญัตินี้ ได้บัญญัติให้พนักงานเจ้าหน้าที่มีอำนาจเพื่อประโยชน์ในการสืบสวนและสอบสวนทั้งหมด 8 ประการ นอกเหนือจากอำนาจในการสืบสวนและสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา กล่าวคือ อำนาจในการสืบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาไม่ได้กำหนดหลักเกณฑ์เงื่อนไขหรือแบบที่มีความเกี่ยวข้องกับการสืบสวนไว้แต่

---

[26] พรเพชร วิชิตชลชัย, *เรื่องเดิม*, หน้า 60.

[27] *เรื่องเดียวกัน*, หน้า 25.

อย่างใด และรวมไปถึงไม่ได้กำหนดขอบเขตอำนาจของพนักงานเจ้าหน้าที่ในการสืบสวนไว้ และการสืบสวนนี้อาจจะมีขึ้นทั้งก่อนที่จะเกิดจากการกระทำความผิดและภายหลังการกระทำความผิดได้เกิดขึ้นแล้วก็ได้[28] เพราะการสืบสวนเป็นเรื่องของการดำเนินการของเจ้าพนักงานของรัฐ ไม่ได้มีผลกระทบต่อสิทธิเสรีภาพของเอกชนแต่อย่างใด แต่ในบางกรณีการสืบสวนจะต้องทำเป็นความลับด้วยเหตุนี้ ในการปฏิบัติหน้าที่ที่เกี่ยวกับความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 พนักงานเจ้าหน้าที่จึงมีอำนาจที่จะแสวงหาข้อเท็จจริงตามพฤติการณ์ที่แสดงได้ว่าความผิดอาจจะเกิดมีขึ้นการสอบสวนย่อมเป็นไปเพื่อช่วยให้พนักงานเจ้าหน้าที่หาทางป้องกันหรือระงับไม่ให้เกิดมีขึ้น ถ้ามีความผิดเกิดขึ้นแล้ว การสืบสวนย่อมเป็นมาตรการที่จะช่วยให้พนักงานเจ้าหน้าที่สามารถดำเนินการสอบสวนเกี่ยวกับความผิดนั้น โดยให้พนักงานเจ้าหน้าที่มีอำนาจสืบสวนคดีอันเกี่ยวกับการกระทำความผิดที่มีความเกี่ยวข้องกับคอมพิวเตอร์ได้โดยไม่จำกัดเขตอำนาจ

โดยปกติพนักงานสอบสวนจะมีอำนาจสอบสวนได้ก็ต่อเมื่อความผิดนั้นได้เกิดขึ้นในเขตอำนาจของตนในกรณีใดกรณีหนึ่งดังต่อไปนี้ คือ

ในกรณีปกติพนักงานสอบสวนจะมีอำนาจทำการสอบสวนได้ก็ต่อเมื่อ[29]

1. ความผิดอาญาได้เกิด อ้าง หรือเชื่อได้ว่าเกิดภายในเขตอำนาจของตน
2. ผู้ต้องหามีที่อยู่หรือถูกจับภายในเขตอำนาจของตน

หรือในกรณีที่การกระทำความผิดคาบเกี่ยวกับอีกท้องที่หนึ่งในลักษณะและสภาพดังต่อไปนี้ คือ[30]

1. เมื่อเป็นการไม่แน่ว่าการกระทำผิดอาญาได้กระทำในท้องที่ใด
2. เมื่อความผิดส่วนหนึ่งกระทำในท้องที่หนึ่ง แต่อีกส่วนหนึ่งในอีกท้องที่หนึ่ง
3. เมื่อความผิดนั้นเป็นความผิดต่อเนื่องและกระทำต่อเนื่องกันในท้องที่ต่างๆ
4. เกินกว่าท้องที่หนึ่งขึ้นไป
5. เมื่อเป็นความผิดที่มีหลายกรรมกระทำลงในท้องที่ต่างๆ กัน
6. เมื่อความผิดเกิดขึ้นขณะผู้ต้องหากำลังเดินทาง
7. เมื่อความผิดเกิดขึ้นขณะผู้เสียหายเดินทาง

ในกรณีใดกรณีหนึ่งดังกล่าวข้างต้น พนักงานสอบสวนแห่งท้องที่ที่เกี่ยวข้องทุกท้องที่มีอำนาจสอบสวนได้ เพราะฉะนั้นอำนาจสอบสวนในคดีความผิดเกี่ยวกับคอมพิวเตอร์ของพนักงานเจ้าหน้าที่จึงหมายความรวมไปถึงการรวบรวมพยานหลักฐาน ทั้งพยานบุคคล พยานเอกสาร และพยานวัตถุ และกระทำการใดเพื่อให้ได้มาซึ่งพยานหลักฐานเหล่านั้นโดยอำนาจสอบสวนในคดีความผิดเกี่ยวกับคอมพิวเตอร์นั้นให้มีอำนาจสอบสวนได้ทั่วราชอาณาจักร กล่าวคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ไม่ได้มีการแบ่งเขตอำนาจสอบสวนของ

---

[28]จุลสิงห์ วสันตสิงห์, **คำอธิบายประมวลกฎหมายวิธีพิจารณาความอาญา ภาค 1**, พิมพ์ครั้งที่ 2 (กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตสภา, 2553).

[29]มาตรา 18 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

[30]มาตรา 19 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

พนักงานเจ้าหน้าที่ไว้เหมือนเช่นประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 18 และมาตรา 19 แต่อย่างไรก็ตาม อำนาจในการดำเนินการค้นและยึดด้วยตนเอง พนักงานเจ้าที่ไม่มีอำนาจที่จะกระทำได้ กล่าวคือ ด้วยมีระเบียบว่าด้วยการค้นและยึดการทำสำนวนสอบสวนและการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ข้อ 6 ที่ได้กล่าวไว้ว่า กำหนดให้พนักงานเจ้าหน้าที่ต้องประสานงานมายังพนักงานสอบสวนผู้รับผิดชอบแล้วให้พนักงานสอบสวนผู้รับผิดชอบดำเนินการตามอำนาจหน้าที่ต่อไป

แต่มีข้อน่าสังเกตอยู่ว่า การสอบสวนอาจทำได้โดยสมบูรณ์โดยไม่ต้องอาศัยการสืบสวนเลย เช่น เมื่อการกระทำความผิดนั้นแจ้งชัดต่อหน้าพยานหลายคนและกระทำต่อหน้าพนักงานสอบสวนทั้งกฎหมายก็ไม่ได้มีข้อบังคับว่าจะต้องมีการสอบสืบสวนเสียก่อนจึงจะสอบสวนได้[31] พนักงานเจ้าหน้าที่จึงอาจใช้อำนาจในการสอบสวนความผิดเกี่ยวกับคอมพิวเตอร์ได้แต่เพียงอย่างเดียว โดยไม่ใช้อำนาจในการสืบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาก็ได้

3.1.1 อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

เพราะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นโดยส่วนตัวแล้วค่อนข้างมีปัญหาอย่างมากในการที่จะที่จะทำการตรวจพบและเป็นปัญหาอย่างยิ่ง หากจะทำการพิสูจน์ความรับผิดให้ทันถ่วงทีและกระทำได้อย่างรวดเร็ว ซึ่งการกระทำเช่นนี้ได้ส่งผลเสียหายอย่างมาก ในการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จึงได้มีการกำหนดอำนาจของพนักงานเจ้าหน้าที่ไว้เป็นกรณีพิเศษให้นอกเหนือไปจากอำนาจในการสืบสวนและสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ดังนั้น เพื่อให้พนักงานเจ้าหน้าที่สามารถรวบรวมพยานหลักฐานให้ตรงกับลักษณะของการกระทำความผิด จึงแบ่งออกเป็น 2 ประเภท กล่าวคือ

3.1.1.1 อำนาจที่ไม่ต้องขออนุญาตจากศาล

ตามมาตรา 18 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ที่ได้บัญญัติว่า

> ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้เฉพาะเท่าที่จำเป็นเพื่อประโยชน์ในการใช้เป็นพยานหลักฐานที่เกี่ยวกับการกระทำความผิดและการหาตัวผู้กระทำความผิด

---

[31] คะนึง ฤาไชย, **กฎหมายวิธีพิจารณาความอาญา เล่ม 1**, พิมพ์ครั้งที่ 9 (กรุงเทพฯ: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2551), หน้า 325.

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

กล่าวคือ ในการกำหนดดังกล่าวข้างต้นเป็นการให้พนักงานเจ้าหน้าที่สามารถใช้อำนาจได้เพียง 3 ประการ โดยไม่จำต้องขออนุญาตจากศาล คือ อนุมาตรา 1-3 กล่าว คือ

1) อำนาจในการมีหนังสือสอบถามหรือเรียกบุคคล

อำนาจตาม (1) เป็นเรื่องทั่วไปเกี่ยวกับการรวบรวมพยานหลักฐานซึ่งอาจทำได้โดยวิธีการเรียกให้บุคคลมาให้ถ้อยคำ หรือโดยการให้บุคคลส่งคำชี้แจงเป็นหนังสือ หรือโดยการส่งเอกสาร ข้อมูล หรือวัตถุอื่นใด ที่เป็นอำนาจหน้าที่ของเจ้าพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ ที่มีอยู่แล้วตามประมวลกฎหมายวิธีพิจาณาความอาญา[32] ตามมาตรา 52 ที่ได้บัญญัติเกี่ยวกับการออกหมายเรียกไว้

[32]พรเพชร วิชิตชลชัย, *เรื่องเดิม*, หน้า 44.

ตามประมวลกฎหมายวิธีพิจารณาความอาญาไม่ได้ให้ความหมายของ “หมายเรียก” ไว้แต่อย่างใดไม่ หากพิจารณาถึงมาตราที่เกี่ยวข้องจะเห็นได้ว่า “หมายเรียก” หมายถึง หนังสือบงการที่ออกโดยพนักงานสอบสวน พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือศาล โดยการสั่งให้บุคคลที่ถูกระบุไว้ในหมายนั้นมายังผู้ออกหมายเรียกเพื่อทำการสอบสวน ไต่สวนมูลฟ้อง หรือการพิจารณา หรือเพื่อการอื่นใดก็ตามแห่งบทบัญญัติตามกฎหมายนี้[33] เพราะเหตุนี้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ก็ไม่ได้บัญญัติแบบของหมายเรียกไว้เป็นการเฉพาะ การที่ให้บุคคลใดมาพบพนักงานเจ้าหน้าที่เพื่อทำการการสอบสวน จะต้องกระทำเป็นหนังสือและมีข้อความตามที่ได้บัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 53 ที่ระบุไว้ว่า

(1) สถานที่ที่ออกหมาย
(2) วันเดือนปีที่ออกหมาย
(3) ชื่อและตำบลที่อยู่ของบุคคลที่ออกหมายเรียกให้มา
(4) เหตุที่ต้องเรียกผู้นั้นมา
(5) สถานที่ วันเดือนปีและเวลาที่จะให้ผู้นั้นไปถึง
(6) ลายมือชื่อและประทับตราของศาล หรือลายมือชื่อและตำแหน่งเจ้าพนักงานผู้ออกหมาย

กล่าวคือ ในชั้นสอบสวนนี้บุคคลที่อาจถูกเรียกมาตามหมายนั้น อาจจะเป็น ผู้ต้องหา พยานบุคคล ผู้มีเอกสารหรือวัตถุใดไว้ในครอบครองที่อาจจะเป็นประโยชน์ในการสอบสวน แต่อย่างไรก็ตาม บุคคลที่ถูกเรียกจะต้องอยู่ในฐานะที่ต้องให้ความร่วมมือกับบ้านเมืองในการที่จะรักษาความยุติธรรมให้คงอยู่ ถึงแม้ว่าบุคคลผู้นั้นจะถูกเรียกมาในฐานะผู้ต้องหา หรือ จำเลยก็ตาม แต่ก็จะมาอยู่ในฐานะที่เป็นคู่ความที่มีสิทธิเหมือนคู่ความอีกฝ่ายหนึ่ง แต่ไม่มีฐานะเสมือนผู้กระทำความผิด

2) อำนาจในการเรียกข้อมูลจราจรทางคอมพิวเตอร์

ข้อมูลจราจรทางคอมพิวเตอร์เป็นข้อมูลอีกรูปแบบหนึ่งที่มีความสำคัญในการที่จะทำการรวบรวมพยานหลักฐานในการสืบสวนและสอบสวนในคดีอาญา กล่าวคือ ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิดต้นทางปลายทางเส้นทางเวลาวันที่ปริมาณระยะเวลาชนิดของบริการหรืออื่นๆที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้นที่เป็นข้อมูลคอมพิวเตอร์ที่เกิดขึ้นจากระบบคอมพิวเตอร์อันเป็นส่วนหนึ่งของ กล่าวคือ หมายถึงข้อมูลที่แสดงรายการให้เห็นถึงการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ซึ่งจะแสดงถึงแหล่งกำเนิดเช่น IP Address ของเครื่องชื่อที่อยู่ของผู้ใช้บริการที่มีการลงทะเบียนข้อมูลของผู้ให้บริการ (Service Provider) ลักษณะของการให้บริการว่าผ่านระบบใดหรือเครือข่ายใดวันเวลาของการส่งข้อมูลและข้อมูลทุกประเภทที่เกิดจากการสื่อสาร(Communication) ผ่าน “ระบบคอมพิวเตอร์”

---

[33]คะนึง ฦาไชย, *เรื่องเดิม*, หน้า 192.

การสื่อสารผ่านระบบคอมพิวเตอร์นั้นจะต้องมีระบบเครือข่ายคอมพิวเตอร์และมีผู้ให้บริการซึ่งผู้ให้บริการจะมีข้อมูลจราจรทางคอมพิวเตอร์อยู่ในระบบคอมพิวเตอร์ของตนและตามพระราชบัญญัตินี้กำหนดว่าผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ใช้บริการได้ใช้บริการในระบบคอมพิวเตอร์ของตนดังกล่าว[34]

ดังนั้น ข้อมูลจราจรทางคอมพิวเตอร์ที่เกิดขึ้นนั้น เกิดขึ้นจากระบบคอมพิวเตอร์ที่เป็นส่วนหนึ่งของการสื่อสาร เพราะการสื่อสารผ่านทางระบบคอมพิวเตอร์จะต้องมีเครือข่ายของคอมพิวเตอร์และมีผู้ให้บริการ ซึ่งผู้ให้บริการนั้นจะมีข้อมูลจราจรทางคอมพิวเตอร์อยู่ในระบบคอมพิวเตอร์ของตนและตามพระราชบัญญัตินี้ มาตรา 25 ได้กำหนดว่า ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ใช้บริการได้ใช้บริการไว้ในระบบคอมพิวเตอร์ของตนอีกด้วย

ซึ่งข้อมูลจราจรทางคอมพิวเตอร์ไม่ได้รวมไปถึงเนื้อหาสาระของข้อมูลที่บุคคลติดต่อสื่อสารกัน โดยให้ถือว่าเป็นข้อมูลที่มีความสำคัญต่อการรวบรวมพยานหลักฐานและการสืบสวนสอบสวนในคดีที่เป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น หมายเลขโทรศัพท์ เลขที่อยู่ไอพี หรือ IP Address ชื่อที่อยู่ของผู้ใช้ บริการที่มีการลงทะเบียน ข้อมูลของผู้ให้บริการ (Service Provider) เป็นลักษณะของการให้บริการว่าผ่านระบบใดหรือเครือข่ายใดของการให้บริการ การส่งข้อมูลทุกประเภทที่เกิดจากการสื่อสาร (Communication) โดยผ่านระบบคอมพิวเตอร์ เป็นต้น[35] ส่วนข้อมูลของปลายทางนั้น เช่น เลขที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (E-mail Address) หรือที่อยู่เว็ปไซร์ (URL) ของผู้ใช้อินเตอร์เน็ตที่เข้าไปดูข้อมูล เป็นต้น นอกจากข้อมูลจากต้นทางหรือปลายทางแล้วนั้นยังรวมไปถึงข้อมูลต่างๆ ที่เกี่ยวกับเวลาที่มีการติดต่อสื่อสารในลักษณะการใช้บริการหรือประเภทของการติดต่อสื่อสาร เช่น ติดต่อในรูปแบบของไปรษณีย์อิเล็กทรอนิกส์ หรือการโอนแฟ้มข้อมูล[36]

ดังนั้น การจะเรียกตามอนุมาตรานี้พนักงานเจ้าหน้าที่ไม่จำเป็นต้องมีหมายพนักงานเจ้าหน้าที่สามารถเรียกข้อมูลจราจรทางคอมพิวเตอร์ได้เลยจากผู้ให้บริการหรือบุคคลอื่นที่เกี่ยวข้องโดยทางโทรศัพท์ โทรสาร หรือทางอีเมลล์ก็ได้ เพราะอนุมาตรา 2 ก็ไม่ได้บัญญัติถึงวิธีการในการเรียกไว้ดังเช่นในอนุมาตรา 1

3) อำนาจในการสั่งให้ผู้ให้บริการส่งมอบข้อมูล

เป็นข้อมูลที่เกี่ยวกับผู้ใช้บริการ กล่าวคือ ข้อมูลที่บันทึกถึงตัวตนของบุคคลในการใช้บริการเครือข่ายของผู้ใช้บริการ เช่น ข้อมูลรหัสประจำตัวผู้ใช้บริการ (User ID) ข้อมูลเกี่ยวกับบุคคลที่ใช้บริการที่ได้มีการลงทะเบียนไว้ เป็นต้น[37]

นอกจากข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลเกี่ยวกับผู้ใช้บริการที่ผู้ให้บริการมีหน้าที่ต้องเก็บตามมาตรา 26 แล้วนั้น ถ้าหากผู้ให้บริการมีข้อมูลของผู้ใช้บริการที่อยู่ใน

---

[34]พรเพชร วิชิตชลชัย, *เรื่องเดิม*, หน้า 202.

[35]*เรื่องเดียวกัน*, หน้า 44.

[36]สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, **แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์** (กรุงเทพฯ: สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, 2547), หน้า 18.

[37]พรเพชร วิชิตชลชัย, *เรื่องเดิม*, หน้า 45.

ความครอบครองหรือควบคุมของผู้ให้บริการ ดังนั้น พนักงานเจ้าหน้าที่จะสั่งให้ผู้บริการส่งมอบก็ย่อมทำได้[38]

3.1.1.2 อำนาจที่ต้องขออนุญาตจากศาล

ตามมาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้บัญญัติไว้ว่า การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้

เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็วเมื่อศาลมีคำสั่งอนุญาตแล้ว

ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) และ (8) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐานการทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา 18 (4) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น การยึดหรืออายัดตามมาตรา 18 (8) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

กล่าวคือ การใช้อำนาจของพนักงานเจ้าหน้าที่ต้องปฏิบัติตามมาตรา 19 หากพิจารณาตามมาตรา 19 จะเห็นได้ว่าเป็นบทบัญญัติที่กำหนดถึงการให้อำนาจของพนักงานเจ้าหน้าที่รวม 5 อนุมาตรา คือ (4) (5) (6) (7) และ (8) ที่ให้พนักงานเจ้าหน้าที่จะต้องทำการยื่นคำร้องต่อศาลที่มีเขตอำนาจและศาลต้องมีคำสั่งอนุญาตตามคำร้องก่อน พนักงานเจ้าหน้าที่จึงจะสามารถดำเนินการได้ ดังนั้น จึงเป็นบทบัญญัติที่ให้อำนาจแก่ศาลที่จะควบคุมและตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่ และยังกล่าวรวมไปถึงการใช้กฎหมายเพื่อควบคุมการใช้อำนาจตามมาตรานี้ว่าจะ

---

[38] *เรื่องเดียวกัน,* หน้า 45.

ใช้ได้ต่อเมื่อเป็นกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้[39] แต่ในคำร้องจะต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างใดอย่างหนึ่งที่เป็นความผิดตามพระราชบัญญัตินี้ ลักษณะของเหตุการณ์กระทำความผิดที่ต้องใช้อำนาจ รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและตัวผู้กระทำความผิดที่สามารถจะระบุได้ไว้ในคำร้องด้วย

เพราะฉะนั้น พระราชบัญญัตินี้ได้วางหลักประกันไว้เพื่อคุ้มครองสิทธิเสรีภาพของประชาชน เช่น สิทธิเสรีภาพส่วนบุคคลในที่อยู่อาศัยและการครอบครองเคหสถานโดยปกติสุข ความเป็นอยู่ส่วนตัว การสื่อสารถึงกันตามรัฐธรรมนูญเพราะกฎหมายวิธีพิจารณาความอาญาบัญญัติขึ้นมาเพื่อรักษาสมดุลระหว่างอำนาจรัฐในการนำตัวผู้กระทำความผิดมาลงโทษ และหลักประกันสิทธิเสรีภาพของประชาชน จะต้องไม่ไปในทางใดทางหนึ่งมากจนเกินไป[40] และยังกล่าวไปอีกว่า หากศาลจะทำการไต่สวนให้ได้ชัดเจนก่อนว่าการใช้อำนาจของพนักงานเจ้าหน้าที่ในการดำเนินการตามคำสั่งของศาลนั้นจะต้องมีการเข้าไปในเคหสถานหรือสถานประกอบการของบุคคล หากพนักงานเจ้าหน้าที่จะต้องเข้าไปในสถานที่ดังกล่าวแล้วนั้น จะต้องให้ผู้ยื่นที่คำร้องระบุมาในคำร้องด้วยว่าให้พนักงานเจ้าหน้าที่เข้าไปในเคหสถานหรือสถานประกอบการเพื่อดำเนินการอย่างใดๆ โดยศาลจะมีคำสั่งอนุญาตให้เข้าดำเนินการตามคำร้องโดยไม่จำต้องให้ผู้ร้องยื่นคำร้องขอหมายค้นในสถานที่ดังกล่าวอีก[41] และในการที่จะสั่งคำร้องของพนักงานเจ้าหน้าที่ ได้กำหนดให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็วที่สุดที่ศาลจะมีคำสั่งอนุญาตหรือไม่อนุญาตโดยศาลจะต้องทำการพิจารณาจากคำร้องนั้นเสียก่อน ถ้าหากว่าศาลเห็นสมควร จะมีคำสั่งให้มีการไต่สวนคำร้องก่อนมีคำสั่งก็สามารถที่จะกระทำได้เพราะเป็นอำนาจทั่วไปของศาลตามประมวลกฎหมายวิธีพิจารณาความอาญา และถือได้ว่าเป็นการสั่งคำร้องคำขอในคดีอาญาที่มีผู้พิพากษาคนเดียวสามารถที่จะมีอำนาจตามพระธรรมนูญศาลยุติธรรม มาตรา 25[42]

หากจะทำการพิจารณาว่าศาลใดเป็นศาลที่มีเขตอำนาจที่มีลักษณะเป็นไปตามพระธรรมนูญศาลยุติธรรมและกฎหมายว่าด้วยการจัดตั้งศาล เช่น กฎหมายว่าด้วยการจัดตั้งศาลและเยาวชนและครอบครัว กฎหมายว่าด้วยการจัดตั้งศาลแขวง เป็นต้น กล่าวได้ว่า การยื่นคำร้องในคดีความผิดเกี่ยวกับคอมพิวเตอร์ตามพระราชบัญญัตินี้ที่เป็นคดีอาญา จะต้องทำการยื่นต่อศาลชั้นต้นที่มี

---

[39]พรเพชร วิชิตชลชัย, *เรื่องเดิม*, หน้า 43.

[40]ในสหรัฐอเมริกาเรียกเป้าหมายแรกว่า Crime Control Model และเป้าหมายที่สองว่า Due Process; Herbert L. Packer, **The Limits of the Criminal Sanction** (California: Stanford University Press, 1968), p. 153 อ้างถึงใน เกียรติขจร วัจนะสวัสดิ์, **คำอธิบายหลักกฎหมายวิธีพิจารณาความอาญาว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณา**, พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม (กรุงเทพฯ: หจก.จิรรัชการพิมพ์, 2551), หน้า 1.

[41]สำนักงานศาลยุติธรรม, **ผลสรุปจากการประชุมหารือของผู้แทนศาลเพื่อดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ระหว่างวันที่ 19 พฤศจิกายน 2550 ถึงวันที่ 20 ธันวาคม 2550** (กรุงเทพฯ: สำนักงานศาลยุติธรรม, 2550).

[42]พรเพชร วิชิตชลชัย, *เรื่องเดิม*, หน้า 51.

อำนาจที่จะพิจารณาพิพากษาคดีอาญาและมีเขตอำนาจในคดีที่บุคคลใดกระทำหรือกำลังจะกระทำความผิด[43]

ถ้าหากว่าศาลได้มีคำสั่งอนุญาตแล้ว ก่อนที่จะดำเนินการตามคำสั่งศาล พนักงานเจ้าหน้าที่จะต้องส่งสำเนาบันทึกเหตุอันควรเชื่อได้ว่าเพราะเหตุใดจึงต้องใช้อำนาจตามอนุมาตรา 4-8 มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน ถ้าหากว่าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวทันที และให้พนักงานเจ้าหน้าที่ที่เป็นหัวหน้าให้ดำเนินการตามอนุมาตรา 4-8 โดยการส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการต่อศาลที่มีเขตอำนาจภายใน 48 ชั่วโมง นับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

ดังนั้น การใช้อำนาจระงับการทำให้แพร่หลายหรือสั่งให้ผู้ใช้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจจะกระทบกระเทือนไปถึงความมั่นคงแห่งราชอาณาจักรตามที่ได้มีการกำหนดไว้แห่งประมวลกฎหมายอาญาในลักษณะ 1 หรือลักษณะ 1/1 แห่งภาคสอง หรือที่มีลักษณะที่เป็นการขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนตามมาตรา 20 ที่กำหนดไว้ว่า

ให้พนักงานเจ้าหน้าที่จะต้องยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ เพื่อขอให้ศาลออกคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้น โดยคำสั่งนั้นจะต้องได้รับความเห็นชอบจากรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเสียก่อน และการใช้อำนาจห้ามจำหน่ายหรือเผยแพร่หรือสั่งให้เจ้าของหรือผู้ที่ครอบครองข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ในนั้นด้วย ให้ระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์ หรือกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครองหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ตามมาตรา 21 นั้น ให้พนักงานเจ้าหน้าที่ยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจเพื่อขอให้ศาลมีคำสั่งห้ามจำหน่ายหรือเผยแพร่ ระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์ หรือกำหนดเงื่อนไขในการใช้ มีไว้เพื่อครอบครอง หรือเผยแพร่ชุดคำสั่งที่ไม่พึงประสงค์อีกด้วย

อำนาจของพนักงานเจ้าหน้าที่ที่ต้องขออนุญาตจากศาล มีกรณีดังต่อไปนี้

1) อำนาจในการทำสำเนาข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดในบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์สามารถประมวลผลได้ และได้ให้ความหมายรวมไปถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุระกรรมทางอิเล็กทรอนิกส์ด้วย[44] กล่าวคือ ข้อมูลทุกอย่างที่อยู่ในระบบคอมพิวเตอร์ รวมไปถึงชุดคำสั่งอีกด้วย หากอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจจะประมวลผลได้[45] ในคำว่า “ข้อมูลคอมพิวเตอร์” ให้หมายความรวมไปถึงข้อมูลดิจิตัลที่มีลักษณะหลากหลายแล้วแต่การสร้างและวัตถุประสงค์ในการใช้งาน ที่อาจจะไม่ได้หมายรวมไปถึงชุดคำสั่ง หรือโปรแกรมคอมพิวเตอร์ เพราะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้น อาจจะ

---

[43] *เรื่องเดียวกัน*, หน้า 51.

[44] มาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

[45] พรเพชร วิชิตชลชัย, *เรื่องเดิม*, หน้า 46.

เป็นการกระทำต่อ “ข้อมูล” ที่ไม่ได้หมายถึงเรื่องราวต่างๆในทำนองเดียวกับ “ข้อความ” ดังนั้น ข้อมูลดังกล่าวจะต้องอยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจจะประมวลผลได้เท่านั้นที่จะได้รับความคุ้มครองตามพระราชบัญญัตินี้ ทั้งนี้ ข้อมูลที่อยู่ในสื่อบันทึกข้อมูลที่ไม่ได้มีการเชื่อมต่อระบบคอมพิวเตอร์ไม่ได้อยู่ในความหมายของคำว่า “ข้อมูลคอมพิวเตอร์” และไม่ได้รับความคุ้มครองตามพระราชบัญญัตินี้ เช่น แผ่นดิส ซีดีรอม เพราะไม่ได้อยู่ในระบบคอมพิวเตอร์ในสภาพที่อาจจะประมวลผลได้

เมื่อได้ทำการพิจารณาความหมายของคำว่า “ข้อมูลอิเล็กทรอนิกส์” ตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2544 ที่ตราขึ้นเพื่อรับรองผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ที่เป็นการรับรองข้อความที่อยู่บนสื่ออิเล็กทรอนิกส์ให้เท่าเทียมกับข้อความที่อยู่บนกระดาษและได้ให้ความหมายคำว่า “ข้อมูลอิเล็กทรอนิกส์” โดยให้ความหมายไว้ว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร เป็นต้น ดังจะเห็นได้ว่าในการก่ออาชญากรรมทางคอมพิวเตอร์ อาจจะกระทำความผิดโดยการคุกคามหรือการก่อให้เกิดความเสียหายให้เกิดขึ้น อาจจะไม่ใช่เพียงแค่ข้อมูลอิเล็กทรอนิกส์ตามความหมายในพระราชบัญญัติดังกล่าวเท่านั้น เพราะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อาจจะเป็นการกระทำต่อ “ข้อมูล” ที่ไม่ได้มีการสื่อความหมายในทำนองเดียวกันกับข้อความ เช่น ข้อมูลที่เป็นรหัสผ่าน หรือลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น แต่อย่างไรก็ตาม ถึงแม้ว่าข้อมูลจะมีลักษณะที่หลากหลาย แต่การสร้างหรือวัตถุประสงค์ในการใช้งานจะเป็นไปในทิศทางเดียวกัน และนี่ก็เป็นอีกหนึ่งปัญหาที่พระราชบัญญัตินี้ต้องบัญญัติให้ข้อมูลคอมพิวเตอร์หมายความรวมไปถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์อีกด้วย

ดังนั้น ในกรณีของโทรเลข โทรพิมพ์ หรือโทรสารหากเป็นความผิดที่ต้องมีการเชื่อมต่อกับระบบคอมพิวเตอร์ เช่น การดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์โดยมิชอบตามมาตรา 8 นั้นจะต้องเป็นกรณีที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์นั้น เป็นต้น เพราะฉะนั้น การดับรับโทรเลข โทรพิมพ์ หรือโทรสารที่ไม่ได้ส่งในระบบคอมพิวเตอร์ย่อมไม่เป็นความผิดตามมาตราดังกล่าว[46]

การใช้อำนาจของพนักงานเจ้าหน้าที่ตามอนุมตรานี้คือการทำสำเนากล่าวคือ การที่พนักงานเจ้าหน้าที่จะเข้าไปตรวจสอบข้อมูลในข้อมูลคอมพิวเตอร์ใดๆก็ตาม เช่น การเจาะระบบคอมพิวเตอร์เพื่อให้ทราบถึงระบบคอมพิวเตอร์ที่ใช้ เข้าถึงข้อมูลคอมพิวเตอร์หรือข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งในส่วนใหญ่แล้วต้องใช้วิธีการทางคอมพิวเตอร์เพื่อการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ และข้อมูลจราจรทางคอมพิวเตอร์ย่อมทำให้พนักงานเจ้าหน้าที่ได้พยานหลักฐานที่เกี่ยวกับการกระทำความผิดที่กระทำผ่านระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ นอกจากนั้น การเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ย่อมเป็นประโยชน์ในการสืบสวนหาตัวผู้กระทำความผิดว่าผู้ใดกระทำความผิด และเมื่อวันที่ เวลาใดจากสถานที่ใด เป็นต้น[47] โดยสามารถกระทำได้

---

[46] *เรื่องเดียวกัน,* หน้า 45-46.

[47] *เรื่องเดียวกัน,* หน้า 46.

เฉพาะเมื่อมีเหตุอันสมควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

เมื่อพนักงานเจ้าหน้าที่ได้ตัวผู้กระทำความผิดมาแล้ว จะต้องมีอำนาจสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์หรือข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวข้องเท่าที่จำเป็นมาด้วย ในกรณีถ้าหากพนักงานเจ้าหน้าที่ได้ยึดหรืออายัดระบบคอมพิวเตอร์มาแล้วนั้นย่อมที่จะใช้อำนาจทำสำเนาข้อมูลคอมพิวเตอร์ได้เลยโดยไม่จำเป็นต้องขออนุญาตต่อศาลตามอนุมาตรานี้อีก[48] เพราะเป็นกรณีที่ระบบคอมพิวเตอร์อยู่ในความครอบครองของพนักงานเจ้าหน้าที่แล้ว

ในส่วนที่เป็นของพนักงานเจ้าหน้าที่ในการทำสำเนาข้อมูลคอมพิวเตอร์นั้น พระราชบัญญัติฉบับนี้ไม่ได้บัญญัติไว้โดยเฉพาะจึงถือได้ว่าเป็นเรื่องของพนักงานเจ้าหน้าที่ผู้ปฏิบัติที่จะต้องพยายามรักษาข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ให้คงสถาพเดิมที่สุด ทั้งนี้เพื่อให้มีความน่าเชื่อถือที่ศาลจะรับฟังเป็นพยานหลักฐานได้

เพราะฉะนั้นในการใช้อำนาจของพนักงานเจ้าหน้าที่ในอนุมาตรานี้เมื่อไปกระทำกับระบบคอมพิวเตอร์ จึงมีความแตกต่างจากอนุมาตรา 1-3 ที่พนักงานเจ้าหน้าที่ไม่ต้องกระทำจากระบบคอมพิวเตอร์ กล่าวคือ มีหนังสือสอบถามหรือเรียกบุคคลมาเพื่อให้ถ้อยคำ เรียกข้อมูลจราจรทางคอมพิวเตอร์และสั่งให้ผู้บริการส่งมอบข้อมูลตามลำดับ ดังนั้น พนักงานเจ้าหน้าที่จึงไม่ต้องขออนุญาตจากศาลก่อน

2) อำนาจในการสั่งให้บุคคลส่งข้อมูลหรืออุปกรณ์

พนักงานเจ้าหน้าที่สามารถสั่งให้บุคคลที่ครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ให้ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ได้ โดยบุคคลที่ครอบครองหรือควบคุมนั้นไม่ได้หมายถึงเฉพาะผู้กระทำความผิดเท่านั้น แต่ยังหมายความรวมไปถึงบุคคลใดๆที่ครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์หรืออุปกรณ์ด้วย

เพราะเหตุนี้จึงต้องบัญญัติให้รวมไปถึงอุปกรณ์ที่ใช้เก็บเครื่องมือคอมพิวเตอร์อีกด้วย เพราะว่าการเก็บข้อมูลคอมพิวเตอร์นอกจากจะมีการจัดเก็บในเครื่องคอมพิวเตอร์ที่ใช้งานแล้วนั้น ยังอาจจะนำไปเก็บไว้ที่อื่นอีกด้วย เช่น ศูนย์เก็บข้อมูล ซึ่งเป็นการเก็บไว้ภายนอกเครื่อง เพราะฉะนั้น จึงต้องกำหนดให้พนักงานเจ้าหน้าที่มีอำนาจสั่งให้ส่งอุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์นั้นได้ด้วย[49]

3) อำนาจในการตรวจสอบหรือเข้าถึง

เป็นสิ่งที่จะใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิดซึ่งบุคคลเหล่านั้นอาจจะเป็นพยานบุคคล พยานเอกสาร หรือพยานวัตถุ การที่จะนำพยานบุคคลมาพิสูจน์ย่อมสามารถที่จะกระทำได้ด้วยการทำเป็นหนังสือเรียกหรือออกหมายเรียกบุคคลนั้นมา แต่สำหรับพยานเอกสารแล้วนั้นหรือจะเป็นพยานวัตถุ ถึงแม้จะมีวิธีการที่ให้ออกหมายโดยการสั่งให้เจ้าของหรือผู้ครอบครองส่งเอกสารหรือวัตถุนั้นอาจจะไม่สามารถกระทำได้เพราะผู้ที่มีเอกสารหรือ

---

[48] *เรื่องเดียวกัน,* หน้า 45-46.

[49] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, *เรื่องเดิม*, หน้า 18.

วัตถุนั้นอาจจะปฏิเสธได้ และจะถือได้ว่าเป็นการขัดขืนหมายก็ไม่ได้ เพราะบุคคลนั้นอาจไม่มีพยานหลักฐานดังกล่าวจริงๆ ก็ได้ แต่อย่างไรก็ตาม แต่หากพนักงานเจ้าหน้าที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้และข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์นั้นมีอยู่จริง อาจจะขอให้ศาลทำการตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์นั้นมาได้

การตรวจสอบหรือการเข้าถึง หมายความว่า การเจาะระบบเพื่อให้ทราบถึงระบบคอมพิวเตอร์ที่ใช้ในการเข้าถึงข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ โดยการกระทำนั้นจะต้องกระทำโดยใช้คอมพิวเตอร์ เช่น พนักงานเจ้าหน้าที่สามารถ Hack หรือ เจาะระบบเพื่อดูอีเมลล์ หรือ Website โดยใช้อำนาจตามอนุมาตรานี้ พนักงานเจ้าหน้าที่จะต้องทำการยื่นคำร้องต่อศาลที่มีเขตอำนาจและได้รับอนุญาตให้ดำเนินการ แต่ถ้าหากว่าได้พบตัวผู้กระทำความผิด หากข้อมูลคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวนั้นอยู่ในความครอบครองหรือควบคุมของผู้กระทำความผิดนั้น พนักงานเจ้าหน้าที่ย่อมมีอำนาจที่จะสั่งให้บุคคลผู้กระทำความผิดนั้นส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่มีความเกี่ยวข้องให้กับพนักงานเจ้าหน้าที่ต่อไป

การใช้อำนาจตามอนุมาตรานี้ของพนักงานเจ้าหน้าที่ในการเจาะระบบคอมพิวเตอร์เหมือนกับอำนาจในการทำสำเนาข้อมูลก็ตาม แต่ต้องแยกอำนาจตามอนุมมาตรานี้ออกมาต่างหากจากกัน อำนาจตามอนุมาตรานี้เป็นการตรวจสอบหรือเข้าถึง และขยายไปถึงการเข้าถึงอุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์อีกด้วย

อำนาจของพนักงานเจ้าหน้าที่ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ และอุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์นี้ ดังนั้นพนักงานเจ้าหน้าที่จึงได้พยานหลักฐานเกี่ยวกับการกระทำความผิดที่กระทำผ่านระบบคอมพิวเตอร์และเป็นประโยชน์ในการที่จะทำการสืบสวนหาตัวผู้กระทำความผิดว่าผู้ใดเป็นผู้กระทำความผิดและการกระทำความผิดนั้นเกิดขึ้นเมื่อใด

4) อำนาจในการถอดรหัสลับ

การใช้อำนาจในการตรวจสอบหรือเข้าถึงตามอนุมาตราก่อนนี้ พนักงานเจ้าหน้าที่อาจพบปัญหาซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลคอมพิวเตอร์ได้เนื่องจากมีรหัสลับป้องกันการเข้าถึงข้อมูลนั้น อนุมาตรานี้จึงให้อำนาจพนักงานเจ้าหน้าที่ในการดำเนินการถอดรหัสลับ หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์[50] เช่นผู้ดูแลระบบ (Admin) หรือเจ้าของเครื่องคอมพิวเตอร์ เป็นต้น ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว[51] ซึ่งหากไม่มีการบัญญัติเป็นการเฉพาะให้มีอำนาจในการถอดรหัสในกฎหมายให้ชัดเจน การกระทำของพนักงานเจ้าหน้าที่ดังกล่าวอาจถือได้ว่าเป็นการล่วงละเมิดข้อมูลส่วนบุคคลได้

โดยปกติแล้วข้อมูลคอมพิวเตอร์ที่สำคัญ เช่น สถาบันการเงิน การซื้อขายหลักทรัพย์ หรือข้อมูลเกี่ยวกับความมั่นคงและความลับของประเทศจะต้องมีระบบป้องกันการเข้าถึง

---

[50]พรเพชร วิชิตชลชัย, *เรื่องเดิม*, หน้า 47.

[51]*เรื่องเดียวกัน*, หน้า 47.

ข้อมูลคอมพิวเตอร์เหล่านี้ด้วยรหัสลับ เพราะถ้าผู้ใดล่วงรู้หรือเข้าถึงข้อมูลดังกล่าวได้อาจทำความเสียหายให้แก่เจ้าของข้อมูลหรือความปลอดภัยสาธารณะเป็นอย่างมาก[52]

5) อำนาจในการยึดหรืออายัดระบบคอมพิวเตอร์

ระบบคอมพิวเตอร์ หมายถึง “อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ[53] จึงได้แก่ ฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่พัฒนาขึ้นเพื่อประมวลผลข้อมูลดิจิทัล (Digital Data) อันประกอบด้วยเครื่องคอมพิวเตอร์ และอุปกรณ์รอบข้าง (Peripheral) ต่างๆ ในการรับเข้าหรือป้อนข้อมูล (Input) หรือแสดงผลข้อมูล (Output) และบันทึกหรือเก็บข้อมูล (Store and Record) ดังนั้น ระบบคอมพิวเตอร์จึงอาจเป็นเพียงอุปกรณ์เพียงเครื่องเดียวหรือหลายเครื่องที่มีลักษณะเชื่อมต่อถึงกันได้ ดังนั้น อาจจะมีการเชื่อมต่อกันผ่านระบบเครือข่ายและมีลักษณะการทำงานโดยอัตโนมัติตามโปรแกรมที่ได้วางไว้และไม่มีการแทรกแซงการทำงานจากมนุษย์ ในส่วนที่เป็นโปรแกรมคอมพิวเตอร์จะหมายถึงชุดคำสั่งที่ทำหน้าที่สั่งการให้คอมพิวเตอร์ทำงาน[54]

ตามอนุมาตรานี้ พนักงานเจ้าหน้าที่มีอำนาจในการยึดหรืออายัด โดยการยึดระบบคอมพิวเตอร์นั้น หมายถึง การนำระบบคอมพิวเตอร์มาอยู่ในความครอบครองของพนักงานเจ้าหน้าที่ ในส่วนของการอายัดระบบคอมพิวเตอร์นั้น หมายถึง การที่พนักงานเจ้าหน้าที่สั่งระงับการใช้ระบบคอมพิวเตอร์นั้นและให้ระบบคอมพิวเตอร์นั้นมาอยู่ในความควบคุมของพนักงานเจ้าหน้าที่ต่อไป[55]

ถ้าหากว่าพนักงานเจ้าหน้าที่จะใช้อำนาจตามที่ได้บัญญัติไว้ในอนุมาตราก่อนๆ นั้น เช่น การเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ อุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ หรือการถอดรหัสลับ แต่ในบางครั้งก็อาจจะยังไม่ได้ข้อมูล เช่น ไม่อาจที่จะถอดรหัสได้ ดังนั้น อนุมาตรานี้จึงให้อำนาจกับพนักงานเจ้าหน้าที่ในการยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในรายละเอียดแห่งการกระทำความผิดนั้นและผู้กระทำความผิด[56]

โดยการยึดหรืออายัดตามพระราชบัญญัตินี้ นอกจากพนักงานเจ้าหน้าที่จะต้องทำการส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดให้เป็นไปตามกำหนดในกระทรวงมอบให้เจ้าของหรือผู้ที่ทำการครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นพยานหลักฐานแล้ว การจะสั่งยึดหรืออายัดดังกล่าวนี้จะเกิน 30 วันไม่ได้ ในกรณีที่มีเหตุจำเป็นที่จะต้องทำการยึดหรืออายัดไว้เป็นเวลานานกว่า 30 วัน ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัด ถ้าหากศาลได้อนุญาตให้ขยายเวลาได้ครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกิน 60 วัน และ

---

[52] *เรื่องเดียวกัน,* หน้า 48.

[53] มาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

[54] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หน้า, *เรื่องเดิม*, หน้า 16.

[55] พรเพชร วิชิตชลชัย, *เรื่องเดิม*, หน้า 48.

[56] *เรื่องเดียวกัน,* หน้า 48.

เมื่อหมดความจำเป็นที่จะทำการยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้วนั้น พนักงานเจ้าหน้าที่จะต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือทำการถอนการอายัดนั้นโดยฉับพลัน ในกรณีที่เป็นหนังสือที่แสดงการยัดหรืออายัดให้เป็นไปตามที่กำหนดในกฎกระทรวง

6) อำนาจในการระงับการทำให้แพร่หลาย

การระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามมาตรา 20 แห่งพระราชบัญญัตินี้ คือ การบล็อกไม่ให้ระบบคอมพิวเตอร์เผยแพร่ข้อมูลคอมพิวเตอร์ที่เป็นความผิดดังกล่าวในระบบคอมพิวเตอร์อีกต่อไป[57] โดยการที่ศาลจะอนุญาตให้พนักงานเจ้าหน้าที่ใช้อำนาจตามมาตรานี้ได้ต้องเป็นเรื่องที่พนักงานเจ้าหน้าที่ดำเนินการโดยได้รับความเห็นชอบจากรัฐมนตรีก่อน แล้วจึงยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจเพื่อขอให้ศาลมีคำสั่งระงับการทำให้เผยแพร่ซึ่งข้อมูลคอมพิวเตอร์นั้น

ในปัจจุบันนี้การกระทำใดๆ ในลักษณะที่เป็นการเข้าข่ายเป็นความผิดตามพระราชบัญญัติที่อาจจะไปกระทบกระเทือนถึงความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และกระทบต่อความรู้สึกร่วมของคนในสังคมเป็นอย่างมากและในการจัดการกับปัญหานี้ ต้องกระทำด้วยความรวดเร็ว หากการปิดกั้นเว็ปไซต์นั้นอาจจะส่งผลกระทบต่อการประกอบการของผู้ให้บริการด้วยเช่นกันและอาจจะมีการฟ้องกลับหรือเรียกร้องค่าเสียหายจากพนักงานเจ้าหน้าที่ได้เช่นกัน[58]

ดังนั้น การใช้อำนาจตามมาตรานี้จึงไม่ได้อยู่ในดุลพินิจของพนักงานเจ้าหน้าที่เท่านั้น แต่จะต้องได้รับความเห็นชอบจากรัฐมนตรีเสียก่อน เนื่องจากการบล็อคระบบคอมพิวเตอร์อาจจะไปกระทบถึงสิทธิเสรีภาพของบุคคลในการสื่อสารข้อมูล[59] เมื่อศาลมีคำสั่งให้ระงับการทำให้เผยแพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามคำร้องขอของพนักงานเจ้าหน้าที่แล้วนั้น พระราชบัญญัตินี้ได้กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจทำการระงับการทำให้เผยแพร่หลายนั้นเอง หรือพนักงานเจ้าหน้าที่ที่จะสั่งให้ผู้บริการระงับการให้บริการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ก็ได้ หากผู้ใดไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่จะต้องระวางโทษตามมาตรา 27

ในส่วนลักษณะของข้อมูลคอมพิวเตอร์ที่ศาลจะสั่งให้ระงับการเผยแพร่นั้นจะต้องเป็นข้อมูลคอมพิวเตอร์ที่มีองค์ประกอบของความผิดตามพระราชบัญญัตินี้ เช่น ความผิดตามมาตรา 14 และ มาตรา 15[60] และยังต้องเป็นข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่บัญญัติไว้ในภาค 2 ลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะเป็นการขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน เป็นต้น

---

[57] พรเพชร วิชิตชลชัย, *เรื่องเดิม,* หน้า 52.

[58] บันทึกการประชุมสภานิติบัญญัติแห่งชาติ, ครั้งที่ 6/2549, 15 พฤศจิกายน 2549.

[59] พรเพชร วิชิตชลชัย, *เรื่องเดิม,* หน้า 53.

[60] *เรื่องเดียวกัน,* หน้า 53.

7) อำนาจในการห้ามจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์

มาตรา 21 แห่งพระราชบัญญัตินี้เป็นบทบัญญัติที่กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจที่จะยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้ศาลมีคำสั่งห้ามจำหน่ายหรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ เพราะจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มีโอกาสเกิดขึ้นได้บ่อยและง่ายขึ้น กล่าวคือ การใช้ชุดคำสั่งไม่พึงประสงค์ (Malicious Code) ที่อาจจะเป็นชุดคำสั่งหรือโปรแกรมที่เป็นการทำลายทั้งหลาย เพื่อกระทำความผิดตามพระราชบัญญัติในรูปแบบต่างๆ[61]

ศาลที่มีเขตอำนาจตามมาตรานี้ หมายถึง ศาลที่มีอำนาจพิจารณาคดีอาญาที่เจ้าของหรือผู้ที่ครอบครองข้อมูลคอมพิวเตอร์อยู่ในเขตอำนาจ[62]

ในชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมให้เกิดความขัดข้อง หรือปฏิบัติงานไม่ตรงกับคำสั่งที่ได้ตั้งไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่ว่า ชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวนั้นตามที่รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารประกาศในราชกิจจานุเบกษา

นอกจากจะสั่งห้ามจำหน่ายหรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์แล้วนั้น พนักงานเจ้าหน้าที่อาจสั่งให้เจ้าของหรือผู้ที่ครอบครองข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วยนั้น ระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์ได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์นั้นก็สามารถกระทำได้

3.2 อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลคอมพิวเตอร์ในต่างประเทศ

การกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นได้ส่งผลกระทบไปถึงกฎหมายวิธีพิจารณาความอาญาของประเทศต่างๆ และในประเทศไทยเองก็ได้มีบทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ขึ้น เพื่อให้อำนาจแก่พนักงานเจ้าหน้าที่ในการดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ให้มีประสิทธิภาพมากยิ่งขึ้น และในหัวข้อนี้ผู้เขียนจะขอกล่าวถึงเรื่องอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ตามกฎหมายต่างประเทศ ที่ทำให้พนักงานเจ้าหน้าที่สามารถดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ในรูปแบบอื่นๆ ได้ เพื่อนำกฎหมายของต่างประเทศนั้นๆ มาใช้เป็นแนวทางในการปรับปรุง แก้ไข เพิ่มเติมกฎหมายของไทยต่อไป

---

[61] บันทึกการประชุมสภานิติบัญญัติแห่งชาติ, *เรื่องเดิม*, หน้า 58.

[62] พรเพชร วิชิตชลชัย, *เรื่องเดิม*, หน้า 54.

3.2.1 ประเทศสหรัฐอเมริกา

การที่ได้นำเอากฎหมายของประเทศสหรัฐอเมริกามาพิจารณาเปรียบเทียบไว้ในบทนี้ เพื่อที่จะใช้เป็นแนวทางในการเปรียบเทียบกับกฎหมายไทยให้มีความสอดคล้องกับกฎหมายไทยที่มีอยู่ในปัจจุบันที่เกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในการกระทำความผิดตามมาตรา 18 และมาตรา 19 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 หากจะกล่าวว่าเหตุใดต้องใช้กฎหมายของประเทศสหรัฐอเมริกามาทำการศึกษาเปรียบเทียบก็เพราะว่าประเทศสหรัฐอเมริกาเป็นประเทศที่ให้ความสำคัญในด้านวิทยาศาสตร์และเทคโนโลยี และในขณะเดียวกันก็เป็นประเทศที่ให้ความสำคัญกับด้านการให้ความคุ้มครองต่อสิทธิและเสรีภาพของประชาชนเป็นอย่างมากอีกด้วย ซึ่งความก้าวหน้าทางวิทยาศาสตร์และทางด้านเทคโนโลยีได้ส่งผลกระทบไปถึงสิทธิส่วนตัวของปัจเจกชนเป็นอย่างมากและในประเทศสหรัฐอเมริกาได้มีการออกกฎหมายไว้โดยเฉพาะเพื่อบังคับใช้กับการให้อำนาจของพนักงานเจ้าหน้าที่ในการใช้อำนาจ

หากจะกล่าวต่อไปอีกว่าในประเทศสหรัฐอเมริกา เป็นที่ทราบกันโดยทั่วไปว่าเป็นประเทศที่ให้ความคุ้มครองในเรื่องสิทธิและเสรีภาพของประชาชนเป็นสำคัญ โดยจะเห็นได้จากรัฐธรรมนูญของสหรัฐอเมริกา ที่บัญญัติว่า

> สิทธิของบุคคลที่จะมีความปลอดภัยมั่นคงในร่างกาย เคหสถาน เอกสาร และวัตถุสิ่งของต่อการค้น การยึด และการจับ ที่ไม่มีเหตุอันสมควร จะถูกล่วงละเมิดมิได้และห้ามมิให้มีการออกหมาย เว้นแต่จะโดยมีเหตุอันสมควร ซึ่งได้มาโดยการสาบานหรือปฏิญาณตน และหมายนั้นจะต้องระบุเฉพาะเจาะจงถึงสถานที่ซึ่งจะถูกค้น ตัวบุคคลที่จะถูกจับ และสิ่งของที่จะถูกยึด

กล่าวได้ว่า ความคุ้มครองถึงสิทธิในความเป็นส่วนตัว (Right of Privacy) ของบุคคลในการเข้าถึงข้อมูลทางคอมพิวเตอร์ ที่ได้กระทำโดยเจ้าพนักงานของรัฐ[63] อย่างไรก็ตามก็ได้กำหนดข้อยกเว้นที่ให้อำนาจเจ้าพนักงานของรัฐทำการเข้าถึงข้อมูลการใช้งานทางคอมพิวเตอร์ได้เพื่อประโยชน์ในการแสวงหาพยานหลักฐานในการดำเนินคดีกับผู้ที่กระทำความผิดทางอาญา โดยการกระทำของพนักงานเจ้าหน้าที่ให้อยู่ภายใต้การดูแลของศาลหรือดุลพินิจของศาล และวิธีพิจารณาที่บัญญัติไว้ในลักษณะ 3 (Title III) The Omnibus Crime Control and Safe Streets Act ปี 1968[64] ซึ่งในประเทศ สหรัฐอเมริกานั้นได้ให้ความสำคัญกับหลักการจำกัดเสรีภาพของบุคคลเป็นเรื่องที่สำคัญ ซึ่งจะมีปัญหาขัดแย้งกันระหว่างการให้ความคุ้มครองเสรีภาพในร่างกายของบุคคลเพื่อให้เห็นถึงการแก้ปัญหาความขัดแย้งดังกล่าวข้างต้น ประเทศสหรัฐอเมริกาจึงได้กำหนดหลักเกณฑ์ในการที่จะให้เจ้าพนักงานของรัฐสามารถที่จะใช้อำนาจ ไว้ในบทบัญญัติแห่งรัฐธรรมนูญของ

---

[63] Katz v. United States (United State Court, 1967)

[64] Olmstead v. United States (1928)

สหรัฐอเมริกา[65] กล่าวได้ว่า การจะจับนั้นจะต้องจับโดยอาศัยหมายจับ (Arrest Warrant) โดยศาลเป็นผู้ออกหมายให้โดยอาศัยเหตุอันสมควร (Probable Cause)[66]

การนำหลัก Probable Cause มาปรับใช้เพราะศาลสูงสุดในสหรัฐอเมริกาได้มีพัฒนาการเปลี่ยนแปลงไปตามแต่ละยุคสมัย ในทางวิชาการได้พยายามวางหลักเกณฑ์ หรือ ตั้งข้อสังเกตในการดุลพินิจของศาลสูงสุดว่าการปรับใช้หลัก Probable Cause นั้น ขึ้นอยู่กับการชั่งน้ำหนักระหว่างสิทธิในความเป็นส่วนตัวของบุคคล และ เป้าหมายของรัฐในการพิทักษ์รักษาความสงบเรียบร้อยในสังคมผ่านกระบวนการการบังคับใช้กฎหมาย ซึ่งศาลจะมีมุมมองแตกต่างกันไปตามแต่ละยุคสมัย เช่น ในข้อเท็จจริงในคดี Olmstead v. United States มีใจความว่า

> เจ้าหน้าที่ตำรวจได้ทำการดักฟังการสนทนาโทรศัพท์ของจำเลย โดยการดักฟังนั้นไม่ได้บุกรุกเข้าไปในสถานที่ที่จำเลยอยู่ แต่ได้ทำการพ่วงสายโทรศัพท์ของบ้านจำเลย คดีนี้จึงมีปัญหาที่จะต้องทำการพิจารณาว่า การที่มีการส่งข่าวสารผ่านทางสายโทรศัพท์นั้นจะได้รับความคุ้มครองหรือไม่ ซึ่งได้มีบทบัญญัติไว้ในรัฐธรรมนูญแห่งสหรัฐอเมริกาที่ว่า ห้ามการค้นและยึดโดยไม่มีเหตุอันสมควร ข้อเท็จจริงในคดีนี้ปรากฏว่าไม่มีการบุกรุกเข้าไปสถานที่ที่จำเลยอยู่จึงไม่มีสถานที่ให้ค้น กล่าวคือ ไม่ได้รับความคุ้มครองตามบทบัญญัติที่บัญญัติไว้ในรัฐธรรมนูญแห่งสหรัฐอเมริกา

การเข้าถึงข้อมูลการใช้งานอินเทอร์เน็ตทางคอมพิวเตอร์ในประเทศสหรัฐอเมริกาได้มีกฎหมายที่เกี่ยวข้องกัน อยู่ 4 ฉบับ คือ

3.2.1.1 The Federal Communications Act of 1934

รัฐสภาของประเทศสหรัฐอเมริกาได้ตรากฎหมาย The Federal Communications Act of 1934 ไว้ในมาตรา 605 มีหลักอยู่ว่า “ห้ามมิให้บุคคลใดโดยมิได้รับอนุญาตจากผู้ส่งข่าวสารกักการสื่อสารใดๆ และเปิดเผยความลับ หรือพิมพ์เผยแพร่ความมีอยู่ข้อความเนื้อหาสาระ หรือความหมายแห่งการสื่อสารที่กักนั้นต่อบุคคลอื่น” กล่าวคือ ห้ามทำการกักและการเปิดเผย หรือการใช้ประโยชน์จากการสื่อสารนั้น[67] หมายความว่า ข่าวสารที่ได้ผ่านการสื่อสารไม่ว่าจะทางใดๆ ถือว่าไม่ใช่การดักฟังหรือเป็นการดักข้อมูลการสื่อสารต่างๆ ได้ แต่ตามมาตรา 605 ก็ได้มีข้อยกเว้นที่กล่าวว่าเว้นแต่จะได้รับอนุญาตจากผู้ส่งข่าวสารและถ้อยคำดังกล่าวชัดเจนโดยตรงที่ว่าห้ามมิให้บุคคลใดเปิดเผย

---

[65] Olmstead v. United States (1928)

[66] สุเมธ ลิขิตธนานันท์, **เหตุในการจับกุม** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2542), หน้า 63.

[67] แปลจากภาษาอังกฤษว่า (N) o person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. . .

หรือพิมพ์เผยแพร่ข่าวสาร ข้อความแก่บุคคลอื่นและได้มีคำพิพากษาว่าบทบัญญัติดังกล่าวนี้ใช้บังคับกับกรณีการดักฟังทางโทรศัพท์หรือดักข้อมูลการสื่อสารโดยเจ้าหน้าที่

กล่าวโดยสรุปบทบัญญัติมาตรา 605 แห่ง The Federal Communications Act ปี ค.ศ.1934 ทำให้มีปัญหาในการบังคับใช้กฎหมายของเจ้าพนักงานเพราะในการทำหน้าที่เจ้าพนักงานจะใช้วิธีการดักฟังทางโทรศัพท์ หรือ ดักรับข้อมูลสื่อสารต่างๆ ในการสืบสวนคดี

3.2.1.2 The Omnibus Crime Control and Safe Streets Act of 1968

การที่เจ้าพนักงานของรัฐทำการดักฟังโทรศัพท์ หรือ ดักรับข้อมูลสื่อสารต่างๆ เป็นการล่วงละเมิดในสิทธิส่วนตัว (Right of Privacy) แต่เนื่องจาก The Federal Communications Act ปี ค.ศ.1934 มาตรา 605 ที่วางหลักไว้ว่า “ห้ามมิให้บุคคลใดโดยมิได้รับอนุญาตจากผู้ส่งข่าวสารกักการสื่อสารใดๆ และเปิดเผยความลับ หรือพิมพ์เผยแพร่ความมีอยู่ข้อความเนื้อหาสาระ หรือความหมายแห่งการสื่อสารที่กักนั้นต่อบุคคลอื่น” ซึ่งหลักกฎหมายดังกล่าวนี้ ทำให้เกิดปัญหาในการปฏิบัติงานของเจ้าพนักงาน เพราะในประเทศสหรัฐอเมริกาจะแสวงหาพยานหลักฐานโดยวิธีการดักฟังทางโทรศัพท์เพื่อนำมาประกอบในการพิจารณาดำเนินคดีกับผู้ที่กระทำความผิด ดังนั้น จึงมีการออกกฎหมาย The Omnibus Crime Control and Safe Streets Act of 1968 ขึ้น เพื่อแก้ไขเพิ่มเติมในมาตรา 605 แห่ง The Federal communications Act ปี ค.ศ.1934 เพื่อให้อำนาจแก่ศาลที่จะอนุญาตให้เจ้าพนักงานที่มีอำนาจหน้าที่สามารถบังคับใช้กฎหมายฉบับนี้ต่อไป กล่าวคือทางรัฐบาลได้ห้ามการดักฟังทางโทรศัพท์และการดักรับข้อมูลผ่านเครื่องมืออิเล็กทรอนิกส์โดยที่ไม่ได้รับอนุญาตจากศาล และได้มีบทลงโทษหากมีการฝ่าฝืนบทบัญญัตินี้อีกด้วย เว้นแต่ คู่กรณีจะให้ความยินยอมในการดักฟังทางโทรศัพท์และการดักรับข้อมูลผ่านเครื่องมืออิเล็กทรอนิกส์ต่างๆ แต่จะเป็นเช่นไรก็ตาม เจ้าพนักงานมีสิทธิที่จะขออนุญาตจากศาลต่อการที่จะกระทำการดักฟังโทรศัพท์หรือดักรับข้อมูลการใช้งานอินเตอร์เน็ตทางคอมพิวเตอร์ของประชาชนได้ แต่การที่เจ้าหน้าที่จะมีสิทธิดังกล่าวได้นั้นเจ้าหน้าที่จะต้องแสดงเหตุผลอันสมควรให้ศาลเห็นได้ว่าเจ้าหน้าที่มีเหตุอันสมควรที่ศาลจะอนุญาตให้กระทำการดังกล่าวได้

ได้วางหลักไว้ในมาตรา 2518 จะเป็นเรื่องที่เกี่ยวกับการใช้ในพิจารณาในการดักฟังโทรศัพท์หรือดักรับข้อมูลการใช้งานอินเตอร์เน็ตทางคอมพิวเตอร์ของประชาชนในการสื่อสารผ่านทางสาย ทางคำพูด หรือทางอิเล็กทรอนิกส์ ดังต่อไปนี้ เช่น[68]

> (A) มีคำร้องให้ศาลมีคำสั่งอนุญาต หรือมีคำสั่งให้รับรองการดักฟังโทรศัพท์หรือดักรับข้อมูลการใช้งานอินเตอร์เน็ตทางคอมพิวเตอร์ของประชาชนทางคำพูด หรือทางอิเล็กทรอนิกส์ ในคำร้องที่ยื่นต่อศาลนั้นจะต้องประกอบไปด้วยรายละเอียด ดังต่อไปนี้
>
> a. ระบุตัวเจ้าหน้าที่ที่จะทำการสืบสวนสอบสวนหรือเจ้าพนักงานที่มีหน้าที่ในการใช้กฎหมายที่เกี่ยวกับคำร้องนั้น และเจ้าพนักงานผู้อนุญาตตามคำร้องนั้น

[68]The Omnibus Crime Control and Safe Streets Act of 1968, Sec. 2518 (1),(3)

b. รายละเอียดข้อเท็จจริงและพฤติการณ์ที่เกี่ยวกับคำร้องโดยการแสดงเหตุให้ศาลเชื่อว่าควรอนุญาตรวมไปถึง (1) รายละเอียดเกี่ยวกับความผิดที่ระบุไว้ โดยเฉพาะที่ได้เกิดขึ้นจากการกระทำ หรือ จะกระทำ (2) เว้นแต่ตามที่ได้บัญญัติไว้ในอนุมาตรา (11) รายละเอียดที่เกี่ยวกับลักษณะและสถานที่ที่จะติดเครื่องดักฟังหรือเครื่องดักข้อมูล (3) รายละเอียดเกี่ยวกับประเภทของการใช้งานการสื่อสาร (4) ระบุตัวบุคคลที่กระทำความผิดและการใช้งานของเขาที่จะถูกดักรับข้อมูล

c. ถ้อยคำที่ได้มีการสืบสวนสอบสวนโดยวิธีอื่น หรือ จะเป็นอันตรายมากเกินไป

d. ระบุระยะเวลาที่อนุญาตให้ดักรับข้อมูลถ้าในลักษณะของการสืบสวนมีว่า การอนุญาตนั้นเพื่อให้การดักรับข้อมูลไม่อาจจะหยุดลงโดยอัตโนมัติ รายละเอียดแห่งข้อเท็จจริงโดยเฉพาะจะต้องระบุเหตุอันสมควรที่จะเชื่อได้ว่า สามารถเพิ่มเติมรายละเอียดได้ในภายหลัง

e. ข้อเท็จจริงที่มีข้อความสมบูรณ์ในเนื้อหาที่เกี่ยวกับคำร้องทั้งหมดที่เกี่ยวข้องกับบุคคลผู้ที่ให้อนุญาตและทำคำร้องยื่นต่อผู้พิพากษาเพื่อขออนุญาตให้มีการดักรับข้อมูล หรือ เพื่อขอให้มีการรับรองในการดักฟังโทรศัพท์หรือดักรับข้อมูลการใช้งานอินเตอร์เน็ตทางคอมพิวเตอร์ของประชาชนทางคำพูด หรือทางอิเล็กทรอนิกส์กับบุคคลที่มีส่วนเกี่ยวข้อง

f. หากมีการขยายระยะเวลาจะต้องระบุถึงเหตุผลที่ขอขยายระยะเวลานั้นด้วย

(B) หากศาลได้รับคำร้องดังกล่าวแล้ว ให้ศาลทำการพิจารณาโดยให้ผู้พิพากษามีคำสั่งไปฝ่ายเดียวได้ตามที่ระบุมาในคำร้องขอภายในเขตที่ศาลมีอำนาจหน้าที่ที่ผู้พิพากษานั้นนั่งพิจารณาอยู่ หากผู้พิพากษาพิจารณาแล้วเห็นว่า ข้อเท็จจริงที่พิจารณาได้นั้นมีรายละเอียด ดังต่อไปนี้

1. มีเหตุอันควรเชื่อได้ว่ามีบุคคลได้กำลังกระทำความผิดตามที่ระบุไว้ในมาตรา 2516

2. มีเหตุอันควรเชื่อได้ว่ามีการสื่อสารที่เกี่ยวกับความผิดนั้นที่จะได้รับจากการดักฟัง หรือ ดักรับข้อมูลจากการใช้งานนั้น

3. การสืบสวนสอบสวนด้วยวิธีธรรมดาไม่ประสบผลสำเร็จ

4. หรือมีเหตุตามที่ได้บัญญัติไว้ในอนุมาตรา (11) ที่กล่าวว่า หากเครื่องดักฟัง หรือดักรับข้อมูล ที่จะอำนวยความสะดวกในการให้ได้มาซึ่งข้อมูลดังกล่าวนั้น ได้กำลังใช้ หรือถูกใช้ในการกระทำความผิดในลักษณะดังกล่าว หรือ เป็นผู้เช่ามีชื่อเป็นเจ้าของ

กล่าวคือ การที่พนักงานเจ้าหน้าที่จะกระทำการถึงข้อมูลการใช้งานอินเทอร์เน็ตของประชาชนได้นั้น จะต้องขออนุญาตจากศาลเสียก่อน โดยการขออนุญาตนั้นจะต้องทำเป็นลาย

ลักษณ์อักษรโดยทำเป็นคำร้อง การทำเป็นคำร้องนั้นจะต้องระบุเหตุผลอันสมควรที่จำเป็นที่จะต้องใช้วิธีการดังกล่าวด้วย ตามหลักเกณฑ์ที่ได้กล่าวมาแล้วข้างต้น และถ้าศาลเห็นสมควรให้ศาลพิจารณาพิพากษาอนุญาตคำร้องดังกล่าวได้ หากศาลได้มีคำสั่งอนุญาตในคำร้องดังกล่าวแล้ว ศาลจะต้องระบุรายละเอียดไปถึงบุคคล สถานที่ ความผิดที่เกี่ยวข้อง หน่วยงาน ระยะเวลา ที่จะมีการเข้าถึงข้อมูล และจะต้องแจ้งให้ทราบถึงการสิ้นสุดการ ที่จะเข้าถึงข้อมูล เมื่อทราบรายละเอียดที่จะถูกเข้าถึงข้อมูลในโอกาสแรก[69] หากศาลมีคำสั่งอนุญาตให้ทำการดังกล่าวได้ การกระทำนั้นจะต้องไม่เกินระยะเวลาที่มีความจำเป็น และหากมีกรณีใดๆ เกิดขึ้นก็ตามจะขอขยายระยะเวลาได้ไม่เกิน 30 วัน

แต่อย่างไรก็ตาม ยังได้มีการกำหนดข้อยกเว้นให้พนักงานเจ้าหน้าที่สามารถทำการเข้าถึงข้อมูล ได้ก่อนที่จะได้รับอนุญาตจากศาลในกรณีที่มีเหตุฉุกเฉิน ดังต่อไปนี้

1. จะมีอันตรายถึงแก่ชีวิต หรือ จะมีอันตรายต่อร่างกายอย่างสาหัส
2. การกระทำความผิดที่ร่วมกันกระทำซึ่งอาจจะเป็นอันตรายต่อความมั่นคงของประเทศชาติ
3. การกระทำความผิดที่ร่วมกันก่อให้เกิดเป็นอาชญากรรม

ในกรณีที่กล่าวมานี้จะต้องเป็นกรณีที่ศาลได้มีคำสั่งอนุญาตให้มีการเข้าถึงข้อมูลนั้นๆ และจะต้องทำการร้องขอต่อศาลภายใน 48 ชั่วโมง หลังจากที่ได้มีการเข้าถึงข้อมูลการใช้งานนั้น[70]

แต่อย่างไรก็ตาม ศาลสหรัฐอเมริกาได้เคยว่าวินิจฉัยไว้ในคดี Unites States v. Whitaker ว่า Title III แห่ง The Omnibus Crime Control and safe Streets Act ปี 1968 เป็นคดีที่ขัดต่อรัฐธรรมนูญ ในเรื่องของการขยายระยะเวลาในการดักฟังหรือดักรับข้อมูลเพราะเป็นการกระทำที่นานเกินสมควร และยังจำกัดในการใช้ดุลพินิจของเจ้าพนักงานที่จะกระทำการดังกล่าวจนกว่าจะได้ข้อมูลที่เพียงพอ และบทบัญญัติแห่งมาตรานี้ ยังถือได้ว่าเป็นการให้อำนาจกับเจ้าพนักงานในการค้นและยึดอันเป็นการฝ่าฝืนต่อบทบัญญัติแห่งรัฐธรรมนูญ

และในปี ค.ศ. 1973 ศาลสหรัฐอเมริกาได้วินิจฉัยพิพากษาคดี United States v. Cafero ซึ่งเป็นคดีที่มีการกลับคำวินิจฉัย โดยได้ปฏิเสธว่าบทบัญญัติดังกล่าวนั้นขัดต่อกฎหมายรัฐธรรมนูญ และนอกจากจะเป็นการขัดต่อรัฐธรรมนูญแล้ว คดีนี้ศาลยังเห็นว่าระยะเวลาที่ได้มีคำสั่งอนุญาตให้มีการดักฟัง หรือดักรับข้อมูล ให้เป็นเวลา 30 วัน เป็นบทบัญญัติที่ได้กำหนดไว้ตามกฎหมายแห่ง Title III แต่ในคดีดังกล่าวได้ตีความไปว่าศาลได้อนุญาตให้ดักฟังต่อไปได้อีก 30 วัน และจะสิ้นสุดลงโดยอัตโนมัติ หรือ ขึ้นอยู่กับดุลพินิจของศาลผู้ออกคำสั่งอนุญาต กล่าวคือ ศาลได้อนุญาตให้มีการดักฟังต่อไปได้โดยที่ไม่ต้องแสดงเหตุอันสมควรซึ่งไม่เห็นด้วย เพราะกำหนดเวลาในการสิ้นสุดการดักฟัง หรือ ดักรับข้อมูล ภายใน 30 วัน เป็นข้อจำกัดตามที่กฎหมายได้อนุญาตให้กระทำได้ภายในระยะเวลาดังกล่าว โดยที่ไม่จำเป็นต้องได้รับอนุญาตให้ดักฟัง หรือ ดักรับข้อมูลนั้นแล้วหรือไม่

ดังนั้น ศาลในสหรัฐอเมริกาได้ถือเอาตามคำวินิจฉัยในคดี United States v. Cafero ว่าด้วยบทบัญญัติ แห่ง Title III ที่ได้อนุญาตให้เจ้าพนักงานบังคับใช้กฎหมายด้วยวิธีการดักฟัง หรือ

---

[69]The Omnibus Crime Control and Safe Streets Act of 1968, Sec. 2518 (4)

[70]The Omnibus Crime Control and Safe Streets Act of 1968, Sec. 2518 (7)

ดักรับข้อมูล ตามที่ศาลได้มีคำสั่งอนุญาต ถือว่าไม่ขัดต่อรัฐธรรมนูญแก้ไขเพิ่มเติม ฉบับที่ 4 (The Fourth Amendment) ซึ่งถือว่าเป็นบทบัญญัติที่คุ้มครองไปถึงประชาชนที่จะไม่ถูกค้นและยึด โดยไม่มีเหตุอันสมควร

สรุป ในประเทศสหรัฐอเมริกาได้ให้อำนาจเจ้าพนักงานในการดักฟัง หรือ ดักรับข้อมูล เพื่อรักษาความปลอดภัยในการป้องกันและปราบปรามอาชญากรรม เพื่อรักษาผลประโยชน์และรักษาความสงบเรียบร้อยภายในประเทศ แต่ในการกระทำดังกล่าวนั้น ไปกระทบถึงสิทธิเสรีภาพของประชาชน ในการที่รัฐออกกฎหมาย The Omnibus Crime Control and Safe Streets Act of 1968 มานั้น มีวัตถุประสงค์เพื่อคุ้มครองถึงสิทธิเสรีภาพของประชาชนและได้วางหลักเกณฑ์ในการใช้อำนาจของเจ้าพนักงาน ในการใช้วิธีการดักฟัง หรือดักรับข้อมูลการใช้งาน เพื่อให้ได้ข้อมูลที่มีความจำเป็นอันสมควรในการบังคับใช้กฎหมาย กล่าวคือ กฎหมายนั้นจะต้องไม่ขัดต่อรัฐธรรมนูญ ที่เป็นกฎหมายอันสูงสุดของประเทศสหรัฐอเมริกา

3.2.2.3 The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA)

กฎหมาย CFAA มีหลักเกณฑ์อยู่ 3 หลักเกณฑ์[71] ที่ให้ความคุ้มครองครอบคลุมไปถึงการรักษาความลับ ให้มีความครบถ้วนและสามารถนำข้อมูลนั้นมาใช้ให้เกิดประโยชน์ได้ กล่าวคือ CFAA ได้กำหนดให้กฎเกณฑ์ดังต่อไปนี้เป็นการกระทำที่ถือว่าเป็นความผิดอาญาและได้มีการแก้ไขเปลี่ยนแปลงให้กฎหมายคุ้มครองการกระทำให้มากขึ้น เช่น

1) หากผู้ใด กระทำการโดยรู้ หรือเข้าถึง คอมพิวเตอร์โดยการกระทำนั้นกระทำโดยปราศจากอำนาจ หรือเกินขอบอำนาจหรือโดยวิธีอื่นใด และได้ไปซึ่งข้อมูล และข้อมูลที่ได้มานั้นเป็นข้อมูลที่เกี่ยวกับความปลอดภัยในประเทศหรือต่างประเทศ หรือเป็นข้อมูลที่ไม่อาจจะเปิดเผยได้ และมีเหตุอันควรคาดหมายได้ว่าข้อมูลที่ได้มานั้นหากนำไปใช้อาจก่อให้เกิดความเสียหายให้กับประเทศสหรัฐอเมริกาได้

2) หากผู้ใดเจตนาที่จะเข้าถึงคอมพิวเตอร์เพื่อให้ได้ข้อมูลโดยปราศจากอำนาจ หรือเกินขอบอำนาจเพื่อให้ได้รับข้อมูลไป เช่น

(1) ข้อมูลที่เก็บไว้ในแฟ้มของสำนักงาน

(2) ข้อมูลของหน่วยงาน หรือสำนักงานใดๆในประเทศสหรัฐอเมริกา

(3) ข้อมูลที่มีความเกี่ยวข้องในการติดต่อสื่อสารระหว่างมลรัฐ หรือการติดต่อกับประเทศต่างๆ

3) หากผู้ใดมีเจตนาที่จะเข้าถึงข้อมูลทางคอมพิวเตอร์ที่รัฐบาลมีไว้เพื่อใช้งาน

4) หากผู้ใดรู้และมีเจตนาที่จะฉ้อโกงในการเข้าถึงข้อมูลที่ได้รับความคุ้มครองทางคอมพิวเตอร์โดยปราศจากอำนาจ หรือเข้าถึงข้อมูลโดยมิชอบ

---

[71] องอาจ เทียนหิรัญ, **อาชญากรรมทางคอมพิวเตอร์:การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2546).

5)

(1)

(1.1) ผู้ใด ส่งโปรแกรมข้อมูล หรือ คำสั่ง โดยมีเจตนาที่จะทำให้เกิดความเสียหายต่อคอมพิวเตอร์

(1.2) มีเจตนาเข้าถึงข้อมูลทางคอมพิวเตอร์ที่ได้รับการคุ้มครองและการเข้าถึงข้อมูลคอมพิวเตอร์นั้นกระทำไปโดยปราศจากอำนาจและเป็นการกระทำที่ประมาทโดยรู้ตัว

(1.3) มีเจตนาเข้าถึงข้อมูลทางคอมพิวเตอร์ที่ได้รับการคุ้มครองและการเข้าถึงข้อมูลคอมพิวเตอร์นั้นทำให้เกิดความเสียหาย

(2) จากการกระทำที่ได้กล่าวมาแล้วข้างต้นนั้นถ้าความผิดนั้นเป็นเหตุให้เกิด

(2.1) ความเสียหายได้เกิดขึ้นกับบุคลหึ่งหรือมากกว่าในระยะเวลา 1 ปี

(2.2) การแก้ไขเปลี่ยนแปลง หรือ การทำให้เกิดความเสียหายกับคำวินิจฉัยในการแพทย์ การรักษาพยาบาล หรือ อนามัยของบุคคลใด บุคคลหนึ่ง หรือ มากกว่านั้น

(2.3) การทำให้บุคคลได้รับบาดเจ็บทางร่างกาย

(2.4) มีการข่มขู่ว่าจะทำให้เกิดอันตรายต่อสุขภาพและอนามัยของสาธารณะ หรือ

(2.5) ความเสียหายที่ส่งผลกระทบไปถึงคอมพิวเตอร์ของหน่วยงานของรัฐในด้านความมั่นคงของประเทศชาติ

6) หากผู้ใดรู้และมีเจตนาที่จะทำการฉ้อโกงในเชิงพาณิชย์ที่มีผลระหว่างรัฐหรือระหว่างประเทศโดยการใช้รหัสผ่านหรือข้อมูลที่ทำให้เข้าถึงข้อมูลทางคอมพิวเตอร์ได้โดยปราศจากอำนาจ

7) ผู้ใดเจตนาที่จะกระทำการกรรโชกเอาไปซึ่งทรัพย์ของผู้อื่นโดยการส่งข้อมูลที่เป็นไปในลักษณะข่มขู่ว่าจะก่อให้เกิดความเสียต่อข้อมูลทางคอมพิวเตอร์[72] เป็นต้น

3.2.2.4 The Electronic Communications Privacy Act (ECPA)

กฎหมาย ECPA เป็นกฎหมายที่คุ้มครองในด้านการสื่อสารทางอิเล็กทรอนิกส์เป็นกฎหมายที่ห้ามการแทรกแซงการติดต่อสื่อสารทางสายไฟและอิเล็กทรอนิกส์ (Federal Wiretapping Statute 18 U.S.C. มาตรา 2510) ที่ใช้บังคับดำเนินคดีที่เกี่ยวกับการดักรับข้อมูลจากการติดต่อสื่อสารโดยทางสายและการสื่อสารโดยข้อความเสียง (Wire and Oral Communications) เท่านั้น ไม่ได้หมายความรวมไปถึงการดักรับข้อมูลในรูปแบบต่างๆ ต่อมาสภาคองเกรสได้บัญญัติกฎหมาย ECPA ขึ้นเพื่อคุ้มครองในความเป็นส่วนตัวที่จะทำการติดต่อสื่อสารในรูปแบบใหม่ๆ เช่น

---

[72]ฉัทปณัย รัตนพันธ์, **อาชญากรรมทางคอมพิวเตอร์: ศึกษาการกำหนดฐานความผิดและการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์** (สารนิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), หน้า 12-13.

เครื่องมือที่สามารถรับส่งข้อความทางคลื่นวิทยุ จดหมายอิเล็กทรอนิกส์ โทรศัพท์เคลื่อนที่ การติดต่อสื่อสารในส่วนที่เป็นบุคคล และการรับส่งข้อมูลผ่านทางคอมพิวเตอร์

กฎหมาย ECPA ฉบับนี้บัญญัติขึ้นเพื่อกำหนดให้การลักลอบการดักฟัง หรือการสื่อสารที่ถูกรบกวนโดยบุคคล ทางอิเล็กทรอนิกส์ให้เป็นการกระทำที่ไม่ชอบด้วยกฎหมายและได้กำหนดให้การกระทำนั้นได้รับโทษทางอาญา กล่าวคือ ห้ามมิให้บุคคลใดเปิดเผยข้อมูลที่เป็นข้อความที่ได้รับมาโดยละเมิดต่อกฎหมาย ECPA และห้ามผู้ดูแลระบบ (System Operator) เปิดเผยข้อความที่ได้มาให้แก่บุคคลอื่นนอกจากบุคคลที่ที่มีอำนาจตามคำสั่งให้สามารถรับรู้ถึงข้อมูลทางคอมพิวเตอร์นั้นๆ ได้ เว้นแต่ ในมาตรา 2511(2) (a) (ii) ที่ได้บัญญัติอนุญาตให้ผู้บริการที่ทำการสื่อสารผ่านทางอิเล็กทรอนิกส์ ได้ให้ความยินยอมกับเจ้าหน้าที่ให้มีอำนาจ ทำการติดเครื่องมือดักฟังได้อย่างถูกต้องตามกฎหมาย หากได้ปฏิบัติตามขั้นตอนที่กำหนดไว้ กล่าวคือ ได้รับอนุญาตจากศาลตามคำร้องขอของบุคคลที่กำหนดไว้ในกฎหมาย อย่างเช่น พนักงานอัยการ รองอัยการ เพื่อให้พนักงานสอบสวนสามารถทำการดักฟังและอัดเทปข้อความที่ดักฟังได้ อย่างเช่นในคดีที่มีความผิดร้ายแรงตามที่กฎหมายได้กำหนดไว้ กล่าวคือ การจารกรรม กบฏ ปล้น ฆาตกรรม หรือจะเป็นการติดสินบนเจ้าพนักงาน ทำการฟอกเงิน เป็นต้น[73]

ในการที่จะกำหนดขอบเขตของการแสวงหาพยานหลักฐานของตำรวจนั้นได้กำหนดบทบัญญัติที่เกี่ยวข้องไว้กับมาตรการ การปฏิบัติหน้าที่ของเจ้าพนักงานในการค้นและยึดพยานหลักฐานกล่าวคือได้บัญญัติไว้ในบทแก้ไขที่ 4 (The Fourth Amendment) ที่ว่าด้วยสิทธิส่วนบุคคลของเอกชนที่บัญญัติว่า “สิทธิของบุคคลที่จะมีความปลอดภัยมั่นคงในร่างกายเคหสถาน เอกสารและวัตถุสิ่งของต่อการค้นและยึดที่ไม่มีเหตุอันควรซึ่งได้มาโดยการสาบานหรือการปฏิญาณตน และหมายนั้นจะต้องระบุเฉพาะเจาะจงถึงสถานที่ที่จะถูกค้นตัวบุคคลและสิ่งของที่จะถูกยึด”[74]

อย่างไรก็ตามกฎหมายของประเทศสหรัฐอเมริกา ได้บัญญัติในเรื่องของข้อยกเว้นในเรื่องของการยึดค้นและรวมรวมพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์ไว้ซึ่งปรากฏอยู่ในบทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญสหรัฐอเมริกาที่ 14 (Fourth Amendment to the U.S. Constitution) และกฎหมาย Electronic Communications Privacy Act of 1986 (ECPA)[75] กฎหมาย The Stored Communications Act1989[76] และคำพิพากษาของศาลสหรัฐอเมริกา

---

[73]เลอสรร ธนสุกาญจน์, จิตตภัทร เครือวรรณ์ และสุธรรม อยู่ในธรรม, **กฎหมายสำหรับบริการอินเตอร์เน็ตในประเทศไทย** (กรุงเทพฯ: นิติธรรม, 2541), หน้า 148-150.

[74]“The right to be secured in their persons, their house, their papers, and their other property from all unreasonable searches and seizures, shall not be violated by warrants issued without probable cause, supported by oath or affirmation, or not particularly describing the places to be searched, or the persons or things to be seized”

[75]18 U.S.C. §§ 2510-22

[76]18 U.S.C. §§ 2701-12, and 18 U.S.C. §§ 3121-27

ในส่วนที่เกี่ยวกับการคุ้มครองสิทธิของประชาชนจากการยึดค้นและรวมรวมพยานหลักฐาน จะบัญญัติไว้ในบทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญสหรัฐอเมริกาที่ 14 ว่า สิทธิของประชาชนจะมีความปลอดภัยในร่างกาย เคหสถาน และทรัพย์สิ่งของจากการถูกตรวจค้น หรือยึดโดยไม่มีเหตุอันควร จะละเมิดมิได้ และจะออกหมายเพื่อกระทำการดังกล่าวใดๆ ไม่ได้ เว้นแต่จะมีเหตุอันควรเชื่อ ซึ่งได้รับการยืนยันด้วยคำสาบาน หรือคำปฏิญาณ และโดยเฉพาะต้องระบุสถานที่ที่จะค้น หรือบุคคลที่จะจับกุมหรือสิ่งที่จะยึดไว้ในหมายนั้น โดยบทบัญญัติดังกล่าวมีเจตนารมณ์เพื่อคุ้มครองสิทธิส่วนบุคคล (Right to Privacy) และเสรีภาพของบุคคลจากการถูกล่วงละเมิดโดยเจ้าหน้าที่ของรัฐซึ่งต่อมาในปี ค.ศ.1868 มลรัฐต่างๆ ได้มีการให้สัตยาบันบทบัญญัติ

โดยหลักของการยึดค้นและรวมรวมพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์ จะต้องกระทำโดยมีหมายค้น (Search Warrant) แต่เนื่องจากปัจเจกชนย่อมมีสิทธิในความเป็นอยู่ส่วนตัว (A Reasonable Expectation of Privacy) และการค้นโดยไม่มีหมายอาจเป็นการกระทำที่ขัดกับหลักกฎหมายดังกล่าว อย่างไรก็ตามการยึดค้นและรวบรวมพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์โดยไม่มีหมายอาจจะกระทำได้ในบางกรณีเท่านั้น ซึ่งจะเป็นไปตามข้อยกเว้นในบทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญสหรัฐอเมริกาที่ 14 และคำพิพากษาของศาลสหรัฐอเมริกา ซึ่งข้อยกเว้นของการยึดค้นและรวมรวมพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์โดยไม่ต้องมีหมายซึ่ง ได้แก่

1) กรณีที่ได้รับความยินยอม (Consent)

ตามกฎหมายของประเทศสหรัฐอเมริกา เจ้าหน้าที่สามารถทำการค้นหาสถานที่หรือวัตถุโดยไม่ต้องมีหมายค้นหรือเพียงมีข้อสงสัย โดยบุคคลที่มีอำนาจได้ให้ความยินยอมสมัครใจในการที่จะทำการค้นหาเช่นในคดี Schneckloth v. Bustamonte[77] และคดี United States v. Buckner[78] ที่กล่าวว่าผู้ที่มีอำนาจอาจจะให้ความยินยอมในการทำการค้นโดยได้รับความยินยอมอย่างชัดเจนหรือโดยนิตินัยเช่น คดี United States v. MilianRodriguez[79] ที่ไม่ว่าจะได้รับความยินยอมด้วยความสมัครใจหรือไม่ ศาลจะต้องตัดสินโดยพิจารณาจากปัญหาข้อเท็จจริงที่เกิดขึ้นใน แต่ในขณะที่ศาลสูงสุดสหรัฐอเมริกาได้มีการระบุเหตุที่สำคัญต่อไปนี้ในเรื่องของอายุ การศึกษา สติปัญญาสภาพร่างกายและจิตใจของบุคคลที่ให้ความยินยอม ว่าบุคคลเหล่านี้อาจจะปฏิเสธในการให้ความยินยอมก็สามารถที่จะกระทำได้เช่น คดีของ Schneckloth ที่รัฐบาลจะต้องทำการดำเนินการภาระการพิสูจน์ว่าได้รับความยินยอมโดยความสมัครใจหรือไม่ ดังเช่นในคดี United States v. Matlock[80]

ในกรณีที่เป็นการยึดค้นและรวมรวมพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์ มีสองประเด็นที่จะต้องได้รับความยินยอม ดังนี้

(1) การค้นหานั้นจะต้องไม่เกินขอบเขตของความยินยอม กล่าวคือ เจ้าหน้าที่มีสิทธิยึดค้นและรวมรวมพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์ได้เฉพาะในกรณีที่ได้รับ

---

[77] Schneckloth v. Bustamonte (1973)

[78] United States v. Buckner (2007)

[79] United States v. MilianRodriguez (1985)

[80] United States v. Matlock (1974)

ความยินยอมให้มีการค้นในสถานที่ (Search of a Location) ซึ่งเป็นที่ตั้งของเครื่องคอมพิวเตอร์ที่ได้มีการจัดเก็บข้อมูลคอมพิวเตอร์นั้นไว้ และในการค้นจะต้องไม่เกินขอบเขตที่ได้รับอนุญาตในการเข้าถึง

ทั้งนี้ การให้ความยินยอมในการทำการค้นหาอาจถูกเพิกถอนได้ “ก่อนที่การค้นหานั้นจะเสร็จสิ้น”(prior to the time the search is completed) เช่นในคดี United States v. Lattimore[81] (quoting 3 Wayne R. LaFave, Search and Seizure § 8.2(f), at 674 (3d ed. 1996)) ซึ่งเมื่อเจ้าหน้าที่ได้รับความยินยอมในการที่จะเอาเครื่องคอมพิวเตอร์ไปทำการตรวจสอบความยินยอมนั้นอาจถูกเพิกถอนได้อยู่ตลอดเวลาก่อนที่จะมีการยึดค้นและรวมรวมพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์ ในกรณีที่เป็นพยานเอกสาร ศาลได้วางหลักไว้ว่า เจ้าหน้าที่มีอำนาจในการเก็บสำเนาของเอกสารที่จัดทำโดยของหน่วยงานรัฐก่อนที่จะมีการเพิกถอนการให้ความยินยอม โดยรัฐบาลอาจจะส่งคืนสำเนาหลังจากได้รับความยินยอมให้ถูกเพิกถอน

a. ขอบเขตของการได้รับความยินยอม

นอกจากนี้ ขอบเขตของการได้รับความยินยอมให้ทำการค้นข้อมูลคอมพิวเตอร์ยังมีข้อจำกัดบางประการในการให้ความยินยอมโดยในคดี United States v. Pena ศาลได้กำหนดขอบเขตของการได้รับความยินยอมภายใต้บทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญสหรัฐอเมริกาที่ 14 ที่ว่าต้องเป็นไปอย่างสมเหตุผลเพื่อให้บรรลุวัตถุประสงค์ของการยึดค้นข้อมูลคอมพิวเตอร์โดยการจะได้รับความยินยอมต้องมีการไต่สวนข้อเท็จจริงว่าการให้ความยินยอมนั้นให้ก่อนหรือระหว่างในการทำการค้น

กรณีปัญหาของการค้นข้อมูลคอมพิวเตอร์มักจะก่อให้เกิดคำถามที่ว่าเมื่อใดที่ได้รับความยินยอมที่จะทำการค้นหาได้หรือเมื่อใดที่ให้ความยินยอมในการค้นหน่วยความจำบนอุปกรณ์ในการจัดเก็บข้อมูลอิเล็กทรอนิกส์ในกรณีเช่นนี้ศาลมองว่าในกรณีที่เป็นการร้องขอความยินยอมจากบุคคลอื่นที่ไม่ได้เป็นเจ้าของข้อมูลคอมพิวเตอร์โดยตรง การให้ความยินยอมนั้นจะต้องชัดเจน มีขอบเขตและระยะเวลาในการค้นเพราะท้ายที่สุดของวิธีการค้นนี้จะต้องอาศัยสามัญสำนึก

ขอบเขตในการได้รับความยินยอมจะต้องระบุเกี่ยวกับวัตถุที่ต้องทำการค้น สถานที่ค้น และวัตถุประสงค์ของการค้นให้ชัดเจน ยกตัวอย่างเช่น คดี United States v. Brook ที่เจ้าหน้าที่จะต้องได้รับอนุญาตเพื่อให้สามารถดำเนินการค้นหาข้อมูลให้เสร็จสมบูรณ์ (Complete Search) ในเครื่องคอมพิวเตอร์ที่เป็นของจำเลยที่ต้องสงสัยว่าเกี่ยวข้องกับสื่อลามกอนาจารเด็กโดยเจ้าหน้าที่จะทำการค้นกับอุปกรณ์สำหรับเก็บข้อมูลในเบื้องต้น (Pre-Search) เพื่อค้นหาไฟล์ภาพว่ามีภาพใดบ้างที่เป็นภาพลามกอนาจารเด็ก ถึงแม้ว่าเจ้าหน้าที่จะได้ใช้วิธีการค้นหาที่แตกต่างจากที่ขอจากศาลและศาลได้อนุญาตให้ทำการค้นหานั้นได้ด้วยตนเองแล้วเพราะการค้นหานั้นไม่ได้เกินขอบเขตของการค้นหาที่ได้รับอนุญาต

การได้รับความยินยอมดังกล่าวควรอยู่ในรูปลายลักษณ์อักษรที่ระบุไว้อย่างชัดเจนถึงขอบเขตของการได้รับความยินยอมรวมไปถึงการได้รับความยินยอมในการ

[81] United States v. Lattimore (1996)

ค้นหาคอมพิวเตอร์และอุปกรณ์จัดเก็บข้อมูลอิเล็กทรอนิกส์อื่นๆ ด้วยเพราะการกำหนดขอบเขตของความยินยอมในการค้นหาข้อมูลคอมพิวเตอร์อาจทำให้เจ้าหน้าที่ไม่สามารถค้นหาหลักฐานจากอุปกรณ์จัดเก็บข้อมูลอิเล็กทรอนิกส์อื่นๆที่เกี่ยวข้อง จึงควรระบุขอบเขตของการค้นหาหลักฐานที่เป็นข้อมูลคอมพิวเตอร์อย่างชัดเจนตั้งแต่ในขณะที่ได้รับความยินยอมจากผู้ต้องสงสัยในการค้นหาคอมพิวเตอร์

(2) บุคคลที่จะให้ความยินยอมในการทำการค้นข้อมูลคอมพิวเตอร์ของบุคคลอื่นนอกจากบุคคลที่เป็นเจ้าของข้อมูลคอมพิวเตอร์เอง บุคคลที่ที่มีอำนาจให้ความยินยอมมีในการเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่น อาจเป็นบุคคลที่สาม ซึ่งได้แก่

(2.1) คู่สมรส (Spouses and Domestic Partners)

(2.2) ผู้ปกครอง (Parents)

(2.3) ช่างซ่อมคอมพิวเตอร์ (Computer Repair Technicians)

(2.4) ผู้ดูแลระบบ (System Administrators)

(3) การได้รับความยินยอมโดยนิตินัยกล่าวคือในการค้นหาพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์ บุคคลที่ให้ทำการค้นจะต้องสมัครใจยินยอมให้กระทำการนั้นได้ตลอดเวลาที่ทำการค้นเพื่อหาหลักฐานในการกระทำความผิดแม้ว่าจะเป็นการค้นโดยไม่มีหมายค้นจากศาล

2) กรณีที่เป็นการอันจำเป็นและเร่งด่วน Exigent Circumstances

เป็นข้อยกเว้นในกรณีที่มีเหตุจำเป็นและเร่งด่วนในการที่จะไม่ต้องมีหมาย ซึ่งโดยหลักแล้วจะใช้เมื่อมีกรณีใดกรณีหนึ่ง ดังต่อไปนี้

(1) หลักฐานอยู่ในสภาพที่ง่ายต่อการถูกทำลาย The Degree of Urgency Involved

(2) เป็นภัยคุกคามที่ทำให้ทั้งตำรวจหรือประชาชนตกอยู่ในอันตราย A Threat puts either the Police or the Public in Danger

(3) เป็นกรณีที่เจ้าหน้าที่ตำรวจพบพิรุธ หรือ The Police are in “Hot Pursuit” of a Suspect

(4) ผู้ต้องสงสัยมีโอกาสที่จะหนีไปก่อนที่เจ้าหน้าที่จะขอหมายค้นได้ The Suspect is Likely to Flee before the Officer can Secure a Search Warrant

เช่น กรณีที่ตำรวจมีอำนาจเข้าไปในบ้านเพื่อที่จะค้นหา เป็นกรณีที่ตำรวจมีสิทธิในการทำการค้นได้ภายใน 2 ชั่วโมง ตามหมายค้นซึ่งเป็นไปตามหลักของบทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญสหรัฐอเมริกาที่ 14 ที่บัญญัติเกี่ยวกับการค้นหาในกรณีที่มีความจำเป็นและเร่งด่วนเมื่อหลักฐานนั้นได้อยู่ในสภาพที่ง่ายต่อการถูกทำลายได้

ทั้งนี้ ในการพิจารณาว่าสถานการณ์ใดที่มีความจำเป็นและเร่งด่วน ศาลได้วางหลักในการพิจารณา ดังนี้

(1) ความจำเป็นเร่งด่วนที่เกี่ยวข้องกับการค้น (The Degree of Urgency Involved)

(2) ระยะเวลาที่จำเป็นในการที่จะขอหมายจากศาล (The amount of Time Necessary to Obtain a Warrant)

(3) หลักฐานที่เป็นเรื่องสำคัญจะถูกลบออกหรือถูกทำลายไปเสียก่อน (Whether the Evidence is about to be Removed or Destroyed)

(4) ความเป็นไปได้ที่จะเกิดอันตรายในขณะนั้น (The Possibility of Danger at the Site)

(5) มีการครอบครองสินค้าต้องห้ามในระหว่างชั้นการพิจารณาคดี (Whether those in Possession of the Contraband know that the Police are on their Trail)

(6) ความเร่งด่วนในการทำลายสินค้าต้องห้าม (The Ready Destructibility of the Contraband)

เช่น การยึดคอมพิวเตอร์โดยไม่มีหมายเมื่อหลักฐานถูกทำลายโดยการเผาเอกสารหลักฐานที่เกี่ยวข้องแล้วหลบหนีไปในสถานการณ์ที่มีความจำเป็นและเร่งด่วนที่อาจจะเกิดขึ้นได้กับเครื่องคอมพิวเตอร์ก่อนที่หลักฐานจะถูกส่งไปยังที่ที่ปลอดภัยเพราะการได้รับข้อมูลอิเล็กทรอนิกส์นั้นจะต้องมีการดูแลรักษาเป็นอย่างดีการบังคับใช้กฎหมายกับโปรแกรมเข้ารหัสเพื่อให้มีประสิทธิภาพ สามารถทำได้ด้วยการกดแป้นพิมพ์เพียงไม่กี่แป้นสามารถใส่ข้อมูลในคอมพิวเตอร์ได้อย่างมีประสิทธิภาพนอกจากนี้คำสั่งของคอมพิวเตอร์สามารถทำลายข้อมูลในเครื่องได้ภายในไม่กี่วินาที เช่น โดยผ่านแม่เหล็กที่แข็งแรงกว่าดิสก์ ที่เจ้าหน้าที่เห็นจำเลยลบไฟล์ในคอมพิวเตอร์ของเขาและเจ้าหน้าที่สามารถยึดคอมพิวเตอร์ได้ทันทีโดยศาลเห็นได้ว่าเจ้าหน้าที่ไม่จำเป็นต้องมีหมายในการที่จะทำการยึดคอมพิวเตอร์เพราะการกระทำของจำเลยถือได้ว่าเป็นสถานการณ์ฉุกเฉินที่ได้เกิดขึ้นแล้ว ที่มีการดาวน์โหลดโดยไม่มีข้อมูลจากคอมพิวเตอร์ โดยหมายในรัสเซียที่มีอยู่น่าจะเป็นสาเหตุที่จะเชื่อว่าคอมพิวเตอร์ของรัสเซียที่มีหลักฐาน ของอาชญากรรมที่มีอยู่เหตุผลที่ดีที่จะกลัวความล่าช้าที่อาจนำไปสู่การทำลายหรือการสูญเสียการเข้าถึงหลักฐานและที่เจ้าหน้าที่เพียงขอข้อมูลที่คัดลอกและหมายค้นที่ได้รับภายหลัง

ในอุปกรณ์อิเล็กทรอนิกส์บางประเภทอาจเกิดขึ้นในกรณีจำเป็นและเร่งด่วนที่อาจจะเกิดขึ้นเนื่องจากข้อมูลได้สูญหายไปในขณะเมื่อแบตเตอรี่ของอุปกรณ์หมดหรือข้อมูลใหม่อาจทำให้ข้อมูลเก่าหายไปอย่างถาวร ศาลให้ถือได้ว่าเจ้าหน้าที่ได้กระทำการอย่างถูกต้องในการเข้าถึงข้อมูลในเพจเจอร์อิเล็กทรอนิกส์ที่อยู่ในความครอบครองของบุคคลเหล่านั้นเพราะบุคคลเหล่านั้นมีเหตุอันควรเชื่อได้ว่าเป็นสิ่งที่จำเป็นเพื่อป้องกันการทำลายหลักฐานข้อมูลที่เก็บไว้ในวิทยุติดตามตัวได้ถูกทำลายได้อย่างง่ายดาย โดยศาลตั้งข้อสังเกตว่าข้อความที่เข้ามาสามารถลบข้อมูลที่เก็บไว้หรือในกรณีที่แบตเตอร์รี่หมดอาจจะลบข้อมูล ดังนั้น เจ้าหน้าที่มีอำนาจในการเข้าถึงวิทยุติดตามตัวได้โดยไม่ต้องมีหมายที่เป็นเหตุการณ์ที่เกิดขึ้นในการดำเนินการค้นหาเพื่อจับกุม เจ้าหน้าที่มีอำนาจในการเรียกดูตัวเลขจากเพจเจอร์เนื่องจากข้อมูลเพจเจอร์อาจถูกทำลายได้อย่างง่ายดายหรือศาลได้คำนึงถึงผลที่อาจจะเกิดขึ้นกับโทรศัพท์มือถือเช่นเดียวกับวิทยุติดตามตัว ถึงแม้ว่าการวิเคราะห์ของศาลอาจจะอยู่ในส่วนที่เกี่ยวข้องกับความเข้าใจผิดของวิธีการที่มือถือมีฟังก์ชั่นในโทรศัพท์ศาลถือได้ว่ามีเหตุจำเป็นและเร่งด่วน ที่มีอำนาจในการค้นหาโทรศัพท์มือถือเพราะโทรศัพท์มีหน่วยความจำที่ จำกัด

ความก้าวหน้าทางเทคโนโลยีล่าสุดที่มีอยู่ในวิทยุติดตามตัวโทรศัพท์มือถือและอุปกรณ์คอมพิวเตอร์แบบพกพาขนาดเล็ก (Personal Digital Assistant: PDA) อาจมีผลกระทบในกรณีที่จำเป็นและเร่งด่วน โดยให้เหตุผลในการค้นหาอุปกรณ์เหล่านี้โดยไม่มีหมายค้นในบางส่วนของความก้าวหน้าที่อาจจะบั่นทอนพื้นฐานในกรณีที่มีเหตุจำเป็นและเร่งด่วนเช่น ในปัจจุบันอุปกรณ์อิเล็กทรอนิกส์มีแนวโน้มที่จะพึ่งพากลไกในการจัดเก็บ (เช่น Flash Memory) ที่ไม่ต้องใช้พลังงานจากแบตเตอรี่ในการรักษาจัดเก็บข้อมูลแต่อย่างไรก็ตามความก้าวหน้าทางเทคโนโลยีอื่นๆ ได้สร้าง Exigencies ขึ้นใหม่ เช่น คำสั่ง "Kill Command" ที่สามารถส่งไปยังอุปกรณ์บางอย่างที่จะทำให้อุปกรณ์ในการเข้ารหัสตัวเองหรือข้อมูลที่เก็บไว้ในเครื่องและอุปกรณ์อื่นๆ สามารถตั้งค่าให้ลบข้อมูลที่จัดเก็บบนอุปกรณ์หลังจากช่วงระยะเวลาหนึ่งที่สถานการณ์จำเป็นและเร่งด่วนมีอำนาจการค้นหาโทรศัพท์มือถือสำหรับข้อความที่โทรศัพท์มือถือมีตัวเลือกสำหรับการลบข้อความโดยอัตโนมัติหลังจากวันที่ส่ง

เนื่องจากการค้นโดยไม่มีหมายจะต้องมีการกำหนดขอบเขตอย่างเคร่งครัดโดยการยกระดับซึ่งแสดงให้เห็นถึงการเริ่มต้น (การละเว้นโดยการอ้างหมาย) ในสถานการณ์ที่จำเป็นและเร่งด่วนในการยึด Warrantless ของคอมพิวเตอร์ อาจไม่สนับสนุนการค้นหาที่มาของคอมพิวเตอร์โดยการบังคับใช้กฎหมาย "เป็นการไปก้าวก่ายคำสั่งในการจับกุมที่ศาลได้อนุมัติให้ไม่ต้องมีการออกหมาย (Warrantless) ดังนั้นจึงจำเป็นที่จะต้องยึดอุปกรณ์เพื่อป้องกันการทำลายหลักฐานโดยไม่จำเป็นต้องมอบอำนาจให้กับเจ้าหน้าที่ในการทำตามขั้นตอนต่อไปโดยไม่ต้องมีหมายค้น (ในกรณีที่จำเป็นและเร่งด่วนที่มีอำนาจยึด แต่ไม่สามารถที่จะทำการค้นหาเครื่องคอมพิวเตอร์ เน้นว่าในขณะที่เกิดกรณีที่จำเป็นและเร่งด่วน อาจแสดงให้เห็นถึงการยึดวิทยุติดตามตัว (Pager)) ในการเข้าถึงข้อมูลคอมพิวเตอร์ในกรณีจำเป็นและเร่งด่วนในการเข้าถึงข้อมูลจะต้องอยู่บนพื้นของการยึด ผู้เชี่ยวชาญทางด้านคอมพิวเตอร์สามารถดึงข้อมูลรายละเอียดที่มีความเกี่ยวข้องกับข้อมูลคอมพิวเตอร์ที่ไม่สามารถกู้คืนได้โดยการค้นหา

3) กรณีที่การยึดค้นข้อมูลคอมพิวเตอร์นั้นได้มาจากการจับกุมโดยชอบ (Search Incident to a Lawful Arrest)

ส่วนการการจับกุมตามกฎหมายเจ้าหน้าที่อาจดำเนินการ “ค้นหา” (Full Search) บุคคลที่ถูกจับกุมและการค้นหาที่จำกัดขอบเขตโดยไม่ต้องมีหมายค้น ในบางกรณีเจ้าหน้าที่ตำรวจสามารถดำเนินทำการค้นในเหตุการณ์ที่เกิดขึ้นซึ่งนำไปสู่การจับกุมที่เป็นการกระทำความผิดตามกฎหมายจราจร (Traffic Offense) ที่ไม่ทราบว่าส่วนประกอบทั้งหมดที่มีเจ้าหน้าที่เปิดแพคเกจและพบสิบสี่แคปซูลเฮโรอีน ที่ศาลฎีกาถือได้ว่าการค้นหาของแพคเกจได้รับอนุญาตแม้ว่าเจ้าหน้าที่ก็ไม่มีเหตุผลที่จะเปิดแพคเกจ ดูแต่ในแง่ของความต้องการทั่วไปในการเก็บหลักฐานและป้องกันไม่ให้เกิดอันตรายต่อการจับกุมเจ้าหน้าที่ศาลให้เหตุผลก็คือว่าเป็นการกระทำที่เหมาะสมสำหรับเจ้าหน้าที่ที่จะดำเนินการค้นหาและเป็นการจับกุมถูกต้องตามกฎหมาย

การอนุญาตและขอบเขตของการค้นหาเพื่อจับกุมแตกต่างกันไปขึ้นอยู่กับสิ่งที่จะทำการค้นในกรณีที่เกี่ยวข้องกับการจับกุมของบุคคล เช่น เสื้อผ้าหรือกระเป๋าสตางค์หรือทรัพย์สินส่วนบุคคลอื่นๆ ใกล้กับ Arrestee ที่บริการรับฝากสัมภาระ ทั้งสองกรณีนี้ศาลฎีกาแสดงให้เห็นถึงความแตกต่างที่เกิดขึ้นที่แสดงให้เห็นถึงช่วงเวลาที่สำคัญในการได้รับอนุญาตสำหรับเหตุการณ์

ที่เกิดขึ้นเพื่อทำการค้นหาจับกุมสินค้าที่เกี่ยวข้องทันทีที่มีเจ้าหน้าที่ผู้มีอำนาจจับกุมโดยศาลยึดถือจากการค้นหาจากหลักฐานที่ได้ในทางตรงกันข้ามคดีของ Chadwick ศาลถือได้ว่าเจ้าหน้าที่อาจค้นตู้เก็บของ (Footlocker) ในบริเวณสถานที่อื่นได้แม้ว่าได้มีที่การจับกุมเกิดขึ้นแล้วเก้าสิบนาทีในคดี Chadwick ศาลระบุว่าเจ้าหน้าที่บังคับใช้กฎหมายได้เฉพาะทรัพย์สินของบุคคลอื่นๆ ที่ไม่เกี่ยวข้องทันทีที่มีคนถูกจับในการควบคุมและมีไม่อันตรายใดๆ ที่ถูกจับอาจเข้าไปถึงโรงแรม โดยการยึดอาวุธหรือทำลายหลักฐานการค้นทรัพย์สินที่ไม่มีเหตุการณ์ในการจับกุม

ศาลฎีกาได้ตัดสินคำพิพากษาในเรื่องของการค้นเพื่อทำการจับกุม ตามหลักของ Arizona v. Gant ที่ศาลอนุญาตให้มีการค้นห้องโดยสารของเหตุการณ์ที่เกิดขึ้นจากยานพาหนะเพื่อทำการจับกุม ในกรณีแรก การถูกจับในกรณีนี้คือการไม่มีหลักประกันและอยู่ในช่วงระยะเวลาของการค้นหา ในกรณีที่สอง เมื่อมีเหตุผลที่น่าจะเชื่อได้ว่ามีพยานหลักฐานที่เกี่ยวข้องกับอาชญากรรมที่อาจจะพบในรถแต่มีข้อจำกัดที่ว่า การค้นหาหลักฐานในรถจะต้องเป็นหลักฐานที่เกี่ยวข้องกับอาชญากรรมในเรื่องที่จะทำการจับกุม ข้อกำหนดนี้ควรใช้เฉพาะกับการค้นหาดังกล่าว แต่ Gant ระบุว่าข้อยกเว้นในกรณีที่สองจะขึ้นอยู่กับสถานการณ์ที่เกี่ยวข้องกับการใช้ยานพาหนะ (Circumstances unique to the vehicle context) เมื่อได้ทำการพิจารณาจากคดี Scalia's concurrence in Thornton v. United States เห็นตรงกันว่าการเสนอข้อยกเว้นในกรณีที่สองในเรื่องของการค้นหาหลักฐานภายในรถผู้ขับขี่อาจจะถูกจับสำหรับการกระทำผิดในกรณีอื่นที่ไม่มีพื้นฐานที่จะเชื่อได้ว่าหลักฐานที่เกี่ยวข้องที่อาจจะพบในรถ

การค้นหาหลักฐานภายในรถยนต์ในปัจจุบันได้ขยายไปถึงการค้นหาหลักฐานจากวิทยุติดตามตัวและโทรศัพท์มือถือและอุปกรณ์คอมพิวเตอร์พกพาขนาดเล็กใช้กับเหตุการณ์ที่เกิดขึ้นในการจับกุมการค้นหานำไปใช้กับอุปกรณ์อิเล็กทรอนิกส์แบบพกพาได้ ศาลได้วางหลักโดยทั่วไปว่าเหตุการณ์ที่เกิดขึ้นในการจับกุมในการทำการค้นสามารถนำไปใช้กับอุปกรณ์อิเล็กทรอนิกส์แบบพกพาได้ ซึ่งในกรณีนี้ศาลอุทธรณ์พิจารณาถึงปัญหานี้และวินิจฉัยว่าโทรศัพท์เคลื่อนที่ที่พบในตัวจำเลยให้ถือว่าเป็นทรัพย์สินส่วนตัวแต่อย่างไรก็ตามศาลแขวงได้เทียบเคียง (Analogized) ระหว่างโทรศัพท์เคลื่อนที่และตู้เก็บของที่ในคดี Chadwick และวางหลักว่าการค้นหาโทรศัพท์เคลื่อนที่ไม่สามารถกระทำได้ในที่มีการจับกุมการละเมิดตามบทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญสหรัฐอเมริกาที่ 14

ศาลได้ระบุได้ว่าสื่ออิเล็กทรอนิกส์ในปัจจุบันที่มีอยู่ในคอมพิวเตอร์แบบพกพา สามารถทำการค้นหาหลักฐานเพื่อทำการจับกุมได้แต่อย่างไรก็ตาม ศาลได้อนุญาตให้ทำการค้นหาอย่างละเอียดโดยจดรายละเอียดในการค้นตามที่กฎหมายได้ให้อำนาจในการจับไว้ ในทำนองเดียวกัน ศาลสามารถให้อำนาจแก่เจ้าหน้าที่เพื่อทำการค้นหาการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์และสื่อเก็บข้อมูลที่คล้ายกัน และถือได้ว่าเจ้าหน้าที่สามารถทำการจับได้ในกรณีที่การกระทำนั้นเป็นการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ โดยไม่ต้องมีหมายค้น

ในกรณีที่ทำการค้นได้โดยที่ไม่ต้องมีหมาย จากแนวคำพิพากษาของศาลสูงของประเทศสหรัฐอเมริกา การค้นจะต้องมีหมายเสมอ จะมีข้อยกเว้นเฉพาะกรณีที่จำเป็นจริงๆ เท่านั้น เช่น

(1) การค้นยานพาหนะโดยมีเหตุอันควรสงสัย (Probable Cause) เพื่อหาเครื่องมือและผลพวงจากการประกอบอาชญากรรม (Fruits and Instrumentality of Crime)

(2) การค้นที่สืบเนื่องจากการจับโดยชอบด้วยกฎหมาย (Search Incidentto a Valid Arrest) อำนาจค้นเกิดขึ้นโดยอัตโนมัติไม่จำต้องมีเหตุอันควรสงสัย (Probable Cause) เพราะเป็นเหตุผลของอีกหลักหนึ่ง กล่าวคือ หลักป้องกันไม่ให้คนร้ายเอื้อมไปหยิบอาวุธมาทำร้ายหรือทำลายพยานหลักฐาน

(3) การค้นในลักษณะที่เป็นการตรวจสอบเบื้องต้นในกรณีที่เรียกว่า Stop and Frisk

(4) การค้นที่เกิดจากเหตุฉุกเฉิน เช่น การค้นในกรณีติดตามอย่างกระชั้นชิด ทั้งนี้ตามหลักความจำเป็นเร่งด่วน (Exigent Circumstance) เนื่องจากไปขอหมายไม่ทัน แต่ไม่ได้ยกเว้นหลักเหตุอันควรสงสัย (Probable Cause)

(5) การค้นโดยความยินยอม (Consent of Search)[82]

(6) การค้นตามหลัก Plain View คือ การค้นได้เฉพาะเห็นอยู่ต่อหน้าต่อตา

(7) การค้นเพื่อทำบัญชีเก็บรักษาทรัพย์สินที่ยึดไว้ (Inventory Search)

แนวความคิดและทฤษฎีของหลัก Probable Cause นั้น ปรากฏอยู่ในหลักกฎหมายเกี่ยวกับการค้นของประเทศสหรัฐอเมริกา ซึ่งแนวความคิดนี้มีพื้นฐานมาจากการตีความตามบทบัญญัติของรัฐธรรมนูญของประเทศอเมริกา หรือ The Fourth Amendment ที่บัญญัติไว้ว่า

> สิทธิของบุคคลที่จะได้รับความปลอดภัยมั่นคงในร่างกาย เคหสถานเอกสาร และวัตถุสิ่งของต่อการค้น และการยึด และการจับที่ไม่มีเหตุผลอันควร (Unreasonable Search and Seizures) จะถูกล่วงละเมิดไม่ได้ และห้ามไม่ให้มีการออกหมาย เว้นแต่ จะมีเหตุอันควรสงสัย ซึ่งได้มาโดยการสาบานหรือปฏิญาณตน และหมายนั้นจะต้องระบุเฉพาะเจาะจงถึงสถานที่ซึ่งจะถูกค้น ตัวบุคคลที่จะถูกจับ และสิ่งของที่จะถูกยึด

บทบัญญัติใน The Fourth Amendment of United States Constitution เป็นการครอบคลุมการค้นโดยเจ้าพนักงานของรัฐไม่ว่ากรณีใดกรณีหนึ่ง แต่จะต้องเป็นการค้นที่กระทำโดยเจ้าพนักงานของสหรัฐอเมริกาเท่านั้น บทบัญญัติในรัฐธรรมนูญของประเทศสหรัฐอเมริกาดังกล่าวนี้ สามารถแยกออกได้ เป็น 2 ส่วน คือ

---

[82]จิรนิติ หะวานนท์, **สิทธิทางวิธีพิจารณาความอาญาตามรัฐธรรมนูญ** (กรุงเทพฯ: วิญญูชน 2543), หน้า 43.

1. ห้ามไม่ให้ทำการค้นโดยไม่มีเหตุอันสมควร
2. การออกหมายใดๆ ต้องมี Probable Cause

กล่าวคือ ถ้าตีความบทบัญญัติดังกล่าวตามตัวอักษรแล้วจะเห็นได้ว่า The Fourth Amendment นี้ ไม่ได้บัญญัติว่าการค้นในทุกๆ ครั้งจะต้องมีหมาย และไม่ได้บัญญัติว่าต้องมี Probable Cause ในการทำการค้นในทุกๆ ครั้งไป แต่อย่างไรก็ตามศาลสูงสุดของสหรัฐอเมริกา (The Supreme Court) ได้ตีความบทบัญญัติในส่วนนี้ว่าจะต้องมีเหตุอันสมควร (Reasonableness) ในการออกหมายค้น และถ้าจะทำการค้นโดยไม่มีหมายก็ต้องมี Probable Cause ด้วยจึงจะถือได้ว่าเป็นการค้นโดยมีเหตุอันสมควร (Reasonable) เพราะศาลสูงสุดของสหรัฐอเมริกานั้นถือได้ว่า การค้นโดยไม่มีหมายค้นนั้นถือว่าเป็นการค้นที่ไม่มีเหตุผลอันสมควรอยู่ในตัวเอง

เมื่อตำรวจทำการค้นหรือจับโดยไม่มีหมาย กล่าวคือ ตำรวจได้ทำการประเมิน Probable Cause ด้วยตัวเองแล้ว แต่จำเลยอาจพยายามให้มีประเด็นการพิสูจน์ถึง Probable Cause กันอีกครั้งเพื่อที่จะไม่ให้นำสิ่งที่ได้จากการค้นหรือจับมานั้นมาใช้เป็นพยานหลักฐานพิสูจน์ความผิด เช่นเดียวกับกรณีที่การจับหรือค้นโดยมีหมาย Magistrate ผู้ที่วิจัย Probable Cause ในการออกหมายจับหรือหมายค้นนั้น การวินิจฉัยนี้ยังไม่ถึงที่สุด เนื่องจากจำเลยสามารถอุทธรณ์ขึ้นสู่ศาลสูงเพื่อให้วินิจฉัยอีกครั้งหนึ่งได้ (Review de novo on Appeal) เหตุที่จำเลยต่อสู้ว่าการออกหมายค้นไม่ชอบไปด้วยกฎหมายนั้น ก็เพื่อไม่ให้นำสิ่งที่ได้จากการค้นโดยไม่ชอบมาใช้เป็นพยานหลักฐานตามหลัก Exclusionary Rules นั่นเอง

ข้อมูลที่จะนำมาสนับสนุน Probable Cause ในการออกหมายค้นนั้นจะต้องมีลักษณะเฉพาะ กล่าวคือ ตัวข้อมูลนั้นจะต้องมีความน่าเชื่อถือ และตัวข้อมูลนั้นจะต้องมีน้ำหนัก หากตัวข้อมูลเป็นคนก็ต้องเป็นคนที่น่าเชื่อถือก่อน แล้วจึงจะพิจารณาว่าสิ่งที่เขาพูดมีน้ำหนักหรือไม่ ถ้าตัวข้อมูลเป็นเอกสารตัวเอกสารนั้นจะต้องมีน้ำหนักที่พอจะรับฟังได้

ตัวอย่างเช่น มีคนบอกตำรวจว่ามีเฮโรอีนในรถคันนั้น กรณีเช่นนี้เพียงพอที่ตำรวจจะอ้างอิงขอหมายค้นรถนี้หรือไม่ กรณีเช่นนี้น่าจะไม่เพียงพอ เพราะอาจเป็นการแต่งเรื่องขึ้นมาเองก็ได้ ผู้ที่มาบอกข้อมูลให้ทราบนั้นจะต้องบอกที่มาที่ไปว่าได้ข้อมูลนั้นมาได้อย่างไรและรายละเอียดของเหตุการณ์จะทำให้เกิดน้ำหนักของตัวพยานขึ้นมา (Self-Verifying Detail) ความน่าเชื่อถือต้องมีรายละเอียด 2 ประการ คือ รายละเอียดของตัวพยาน และรายละเอียดในเนื้อหาของพยานหรือรายละเอียดในข้อเท็จจริงที่ต้องการการพิสูจน์[83]

หลักเกณฑ์การพิจารณา Probable Cause ในคดีของ Spinelli v. United States[84] ถูกตัดสินว่ามีความผิดฐานกระทำการพนันขันต่อโดยการเดินทางจากรัฐอิลลินอยส์ไปยังเมืองเซนหลุยส์ในรัฐมิซซูรีเพื่อทำการพนันขันต่อซึ่งเป็นความผิดตามกฎหมายของรัฐมิซซูรี ผู้ร้องได้ต่อสู้เรื่องความชอบธรรมด้วยรัฐธรรมนูญของหมายค้นที่ให้อำนาจ FBI เข้าทำการค้น ศาลจึงได้อธิบายหลัก ว่าในคดีของ Aguilar หมายค้นได้ออกโดยมีถ้อยคำภายใต้การสาบานของตำรวจ ที่

---

[83] *เรื่องเดียวกัน,* หน้า 27.

[84] Jerold H. Israel, Yale Kamisar and Wayne R. Lafave, **Criminal Procedure and the Constitution** (U.S.A.: West, 1995), pp. 97-100.

สาบานว่าตนได้รับข่าวที่เชื่อถือได้จากบุคคลที่น่าเชื่อถือและตนก็เชื่อตามนั้น แม้จะมีหลักว่า Probable Cause อาจพิสูจน์โดยพยานบอกเล่าก็ได้ แต่ศาลก็วินิจฉัยได้ว่า ถ้อยคำในการสาบานดังกล่าวนั้นยังไม่เพียงพอที่จะแสดงว่ามี Probable Cause ด้วยเหตุผล 2 ประการ คือ

1. ผู้ขอออกหมายไม่ได้บรรยายหรือให้การถึงรายละเอียดข้อเท็จจริงที่จำเป็น (Underlying Circumstances) แก่ศาล Magistrate ที่จะทำให้ศาลสามารถวินิจฉัยได้ว่าข่าวที่ผู้ให้ข่าวกล่าวอ้างมานั้นสามารถเชื่อถือได้เพียงใด และ

2. ตำรวจที่ให้ถ้อยคำไม่ได้พยายามสนับสนุนข้อกล่าวอ้างที่ว่าผู้ให้ข่าวของเขาน่าเชื่อถือ หรือข่าวที่เขาให้มานั้นเชื่อถือได้

ในประเทศสหรัฐอเมริกาได้มีนักวิชาการสรุปได้ว่า[85] หลักของ Probable Cause จะถูกนำมาปรับใช้ผ่านหลักจากแนวบรรทัดฐานคำพิพากษา โดยเรียกหลักนี้ว่า Aguilar-Spinelli Test ซึ่งวางหลักไว้ว่า ในการพิจารณาว่าเจ้าพนักงานของรัฐมี Probable Cause ในการที่จะขอให้ศาลหรือคณะลูกขุนออกหมายค้น หรือ Probable Cause ที่จะทำให้สามารถค้นได้โดยไม่มีหมายนั้น จะต้องพิจารณาข้อมูลที่มีนั้นใน 2 แง่มุม กล่าวคือ

1. ฐานที่มาแห่งข้อเท็จจริง (the basis of knowledge) กล่าวคือ เจ้าพนักงานของรัฐจะต้องแสดงให้เห็นว่าผู้ที่ให้ข้อเท็จจริงนั้น ได้รับรู้ข้อเท็จจริงนั้นมาอย่างไร โดยทางใด ซึ่งการตอบคำถามเหล่านี้จะต้องอาศัยข้อมูลที่ได้จากคำบอกกล่าวชี้แจงของผู้ให้ข้อเท็จจริงนั้น

2. ตัวผู้ให้ข้อเท็จจริง กล่าวคือ เจ้าพนักงานของรัฐจะต้องแสดงให้ปรากฏว่าเหตุใดผู้ให้ข้อเท็จจริงจึงเป็นบุคคลที่เชื่อถือได้หรือไว้ใจได้

นอกจากนั้นแล้ว รัฐหรือเจ้าพนักงานของรัฐ ควรจะพยานอื่นๆ ที่จะนำมาใช้สนับสนุนหลักเกณฑ์ทั้งสองดังกล่าวได้

จากกฎหมายที่เกี่ยวข้องของประเทศสหรัฐอเมริกาที่ได้กล่าวมาทั้งหมดข้างต้น จะเห็นได้ว่าประเทศสหรัฐอเมริกานั้นเป็นประเทศที่มีความทันสมัยและเป็นจุดกำเนิดของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ และยังมีแนวความคิดเพื่อนำไปพัฒนาเพื่อให้เกิดการควบคุมและแก้ไขปัญหาในการใช้อำนาจของพนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลคอมพิวเตอร์ให้ได้รับความคุ้มครองในเรื่องสิทธิและเสรีภาพของประชาชนตามกฎหมายรัฐธรรมนูญอีกด้วยสำหรับประเทศสหรัฐอเมริกาการบังคับใช้กฎหมายการยึดพยานหลักฐานทางอิเล็กทรอนิกส์นั้นอาจกล่าวได้ว่ามีแนวโน้มที่จะผ่อนคลายจากหลัก The Exclusionary Rule ซึ่งเป็นหลักฐานเกณฑ์ที่ศาลสูงไว้วางไว้เพื่อให้ The Fourth Amendment มีประสิทธิภาพในการเป็นหลักประกันสิทธิส่วนบุคคลของประชาชนชาวสหรัฐอเมริกาให้พ้นจากการล่วงละเมิดจากการปฏิบัติหน้าที่ของเจ้าพนักงานโดยไม่มีเหตุผลและไม่จำเป็นโดยการที่ศาลจะไม่ยอมรับพยานหลักฐานที่ได้มาจากการยึดอันมิชอบด้วยกฎหมายรวมทั้งพยานหลักฐานโดยอ้อมอันสืบเนื่องมาจากพยานหลักฐานที่มิชอบนั้น The Fourth

---

[85] Major Walter M. Hudson, “A Few New Developments in the Fourth Amendment,” **The Army Lawyer** (April 1999): 118, Retrieved July 31, 2015 from http://heinonline.org/HOL/LandingPage?handle=hein.journals/armylaw1999&div=21&id=&page=

Amendment เป็นบทบัญญัติที่ว่าด้วยสิทธิส่วนบุคคลของเอกชนอันได้แก่สิทธิที่จะปลอดภัยจากการรุกล้ำเสรีภาพความมั่นคงและทรัพย์สินโดยไม่มีเหตุผลและไม่จำเป็นซึ่งถือเป็นเรื่องที่สำคัญมากสำหรับประชาชนชาวสหรัฐอเมริกา “กระบวนการการออกหมาย” จึงถือเป็นหลักประกันการคุ้มครองสิทธิส่วนบุคคลที่ดีได้ส่วนหนึ่งเพราะจะต้องผ่านการตรวจสอบจากผู้พิพากษามาในเรื่อง “มีเหตุอันควรเชื่อ” (Probable Cause) ภายใต้คำสาบานของเจ้าพนักงานผู้ที่จะทำการยึดในประเทศสหรัฐอเมริกาการยึดมีวัตถุประสงค์เพื่อที่จะรวบรวมพยานหลักฐานซึ่งบทบัญญัติใน Title 18 แห่ง Federal Rules of Criminal Procedure Rule 41 ได้บัญญัติเกี่ยวกับเหตุในการยึดสิ่งของไว้ 4 กรณีดังนี้

1. ทรัพย์สินซึ่งเป็นพยานหลักฐานในการกระทำความผิด
2. สิ่งของผิดกฎหมายสิ่งของที่ได้มาจากการกระทำความผิดหรือสิ่งของอื่นใดที่ครอบครองไว้เป็นความผิด
3. ทรัพย์สินที่ทำขึ้นเพื่อใช้หรือเจตนาที่จะใช้หรือได้ใช้เป็นเครื่องมือในการกระทำความผิด
4. บุคคลซึ่งจะต้องถูกจับกุมตามหมายจับหรือบุคคลซึ่งถูกควบคุมโดยมิชอบด้วยกฎหมาย

อย่างไรก็ตามถึงแม้ว่าการยึดค้นและรวมรวมพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์ จะต้องกระทำโดยมีหมายค้น (Search Warrant) และการค้นโดยไม่มีหมายอาจเป็นการกระทำที่ขัดต่อหลักกฎหมายแต่ก็มีบางกรณีที่กฎหมายได้ให้อำนาจไว้ว่าสามารถกระทำได้โดยไม่มีหมาย เช่น

1. กรณีที่ได้รับความยินยอม (Consent)
2. กรณีที่เป็นการอันจำเป็นและเร่งด่วน (Exigent Circumstances) และ
3. กรณีที่การยึดค้นข้อมูลคอมพิวเตอร์นั้นได้มาจากการจับกุมโดยชอบ (Search Incident to a Lawful Arrest)

3.2.2 ประเทศสิงคโปร์

การที่ได้นำเอากฎหมายของประเทศสิงคโปร์มาพิจารณาเปรียบเทียบไว้ในบทนี้ เนื่องจากประเทศสิงคโปร์เป็นประเทศที่ได้ชื่อว่ามีความเป็นระเบียบเรียบร้อยและปลอดภัยในระดับที่ดีมากประเทศหนึ่งในโลก โดยสิงคโปร์มีกฎหมายที่เข้มงวดและมีบทลงโทษสูงในการกระทำผิดต่างๆ เพื่อรักษามาตรฐานคุณภาพชีวิตที่ดีของสังคม โดยเฉพาะอย่างยิ่งเกี่ยวกับเรื่องการค้ายาเสพติด การติดสินบนเจ้าพนักงานหรือเจ้าหน้าที่ และการลักลอบเข้าเมืองผิดกฎหมาย โดยบทลงโทษสูงสุดของสิงคโปร์คือ การประหารชีวิตและเพื่อที่จะใช้เป็นแนวทางในการเปรียบเทียบกับกฎหมายไทยให้มีความสอดคล้องกับกฎหมายที่มีอยู่ในปัจจุบันที่เกี่ยวกับการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในการกระทำความผิด หากจะกล่าวว่าเหตุใดต้องใช้กฎหมายของประเทศสิงคโปร์มาทำการศึกษาเปรียบเทียบก็เพราะว่าประเทศสิงคโปร์เป็นประเทศที่ได้บัญญัติการกระทำความผิด และอำนาจในการเข้าถึงข้อมูลเกี่ยวกับคอมพิวเตอร์ไว้ชัดเจนโดยการได้กำหนดขอบเขตของการกระทำความผิดไว้ในกฎหมาย Computer Misuse and Cyber

security Act (Chapter 50A)[86] ในประเทศสิงคโปร์นั้นได้รับอิทธิพลมาจากกฎหมายของประเทศอังกฤษ เพราะประเทศอังกฤษเป็นประเทศในเครือจักรภพจึงได้รับเอาอิทธิพลมาเช่นเดียวกับประมวลกฎหมายวิธีพิจารณาความอาญาของสิงคโปร์

ประเทศสิงคโปร์ได้กำหนดเรื่องการดำเนินการสอบสวนไว้ใน Computer Misuse and Cyber Security Act (Chapter 50A) มาตรา 14 ที่ได้บัญญัติไว้ว่า

> การสอบสวนของเจ้าหน้าที่ตำรวจและเจ้าหน้าที่ผู้ได้รับมอบอำนาจหน้าที่ตามกฎหมาย
>
> 14. ไม่มีข้อความใดในพระราชบัญญัตินี้ที่จะห้ามเจ้าหน้าที่ตำรวจ (Police Officer) หรือบุคคลที่ได้รับมอบอำนาจตามความหมายในมาตรา 39 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา หรือเจ้าหน้าที่ใดๆ ที่มีอำนาจบังคับใช้กฎหมายอื่นๆ ในการดำเนินการสอบสวนโดยชอบด้วยกฎหมายตามอำนาจของเขา ภายใต้กฎหมายลายลักษณ์อักษรใดๆ

มาตรา 15 A. ที่แก้ไขเพิ่มเติมแทน มาตรา 15 ว่าด้วยเรื่องอำนาจของเจ้าหน้าที่ตำรวจในการเข้าถึงเครื่องคอมพิวเตอร์และข้อมูล ที่ยกเลิกไปปี 2005 บัญญัติถึงเรื่องการป้องกันหรือต่อต้านภัยคุกคามต่อความมั่นคงของชาติ ซึ่งบัญญัติว่า

> การป้องกันหรือต่อต้านภัยคุกคามต่อความมั่นคงของชาติและอื่นๆ
>
> 15 A-(1) เมื่อรัฐมนตรี (Minister) เห็นว่ามีความจำเป็นเพื่อวัตถุประสงค์ในการป้องกัน หรือต่อต้านภัยคุกคามต่อความมั่นคงของชาติ บริการที่สำคัญ การป้องกันประเทศหรือความสัมพันธ์กับต่างประเทศของประเทศสิงคโปร์ รัฐมนตรี (Minister) อาจจะมอบอำนาจให้บุคคลใดๆ หรือองค์กรที่ระบุไว้ในหมาย (Certificate) โดยใช้มาตรการเท่าที่จำเป็นในการป้องกัน หรือ ต่อต้านคอมพิวเตอร์ หรือ บริการคอมพิวเตอร์ หรือ ประเภทคอมพิวเตอร์ใดๆ
>
> (1) มาตรการที่กล่าวถึงในอนุมาตรา (1) อาจจะรวมไปถึงแต่ไม่จำกัดเฉพาะการกระทำการโดยบุคคลที่ได้รับมอบอำนาจหรือองค์กรที่มีตามที่อ้างถึงในมาตรา 39 และมาตรา 40 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา
>
> (2) ความผิดที่มีการเปิดเผยในแนวปฏิบัติหรือการดำเนินการตามอำนาจใดๆ ภายใต้มาตรานี้
>
> (a) ไม่ให้ข้อมูลสำหรับการกระทำความผิดที่จะยอมรับในพยานหลักฐานในการดำเนินคดีทางแพ่งหรือทางอาญาใดๆและ
>
> (b) ไม่มีพยานในการดำเนินคดีทางแพ่งหรืออาญาใดๆ ที่จะมีหน้าที่

---

[86]Singapore Government, **Singapore Statutes Online,** Retrieved July 31, 2015 from http://statutes.agc.gov.sg

1.1 เปิดเผยชื่อ ที่อยู่ หรือรายละเอียดอื่นๆของสายสืบ (Informer) ความผิดใดๆ ที่ได้ให้ข้อมูลเกี่ยวกับการกระทำความผิด หรือ

1.2 ตอบคำถามใดๆ หากคำตอบจะก่อให้เกิดหรือมีแนวโน้มที่ค้นพบ ชื่อ ที่อยู่ หรือรายละเอียดอื่นๆ ของสายสืบ (Informer)

(3) หากหนังสือ เอกสาร ข้อมูล หรือคอมพิวเตอร์ที่ส่งออกเป็นที่ยอมรับในพยานหลักฐานหรือมีแนวโน้มในการตรวจสอบในการดำเนินคดีทางแพ่งหรือทางอาญาใดๆประกอบด้วยข้อมูลของสายสืบ (Informer) ที่เป็นชื่อหรือคำอธิบายหรือที่อาจทำให้การค้นพบของเขา ศาลจะทำให้ข้อมูลเหล่านั้นถูกปกปิดจากการสำรวจหรือถูกปกปิดจนไม่เห็นร่องรอยเท่าที่จำเป็นเพื่อป้องกันสายสืบ (Informer) จากการค้นพบ

(4) ในอนุมาตรา (1) บริการที่สำคัญ หมายถึง

(a) การบริการที่เกี่ยวข้องโดยตรงกับโครงสร้างพื้นฐานทางการสื่อสาร การเงินการธนาคาร ระบบสื่อประชาสัมพันธ์ของสาธารณะ ระบบการขนส่งสาธารณะ โครงสร้างพื้นฐานในการขนส่งทางบก การขนส่งทางอากาศยาน โครงสร้างการขนส่งที่สำคัญๆ และ

(b) การบริการเหตุฉุกเฉินของเจ้าหน้าที่ตำรวจ, การบริการเหตุฉุกเฉินป้องกันในส่วนของฝ่ายพลเรือน หรือ การบริการการเข้าถึงทางด้านการแพทย์

ในมาตรา 16 บัญญัติเรื่องการจับกุมไว้ว่า

การจับโดยไม่มีหมายจับ

16. เจ้าหน้าที่ตำรวจ (Police Officer) สามารถทำการจับกุมบุคคลใดๆ ได้โดยไม่มีหมายจับ หากมีเหตุอันเป็นการสงสัยว่า มีเหตุในการกระทำความผิดตามพระราชบัญญัตินี้ในประเทศสิงคโปร์ ได้บัญญัติเรื่องอำนาจในการเข้าถึงข้อมูลการถอดรหัสไว้ในThe Criminal Procedure Code (Chapter 68) มาตรา 40 ไว้ว่า

(1) เพื่อวัตถุประสงค์ในการสอบสวนความผิดประเภทจับกุมได้ (Arrestable Offence) พนักงานอัยการ (Public Prosecutor) มีอำนาจออกคำสั่งอนุญาจให้เจ้าหน้าที่ตำรวจสืบสวน หรือสั่งให้บุคคลใดกระทำการและใช้อำนาจตามมาตรา 39 ทั้งหมดหรืออำนาจอย่างใดอย่างหนึ่งตามมาตรานี้

(2) เจ้าหน้าที่ตำรวจ (Police Officer) หรือบุคคลที่ได้รับมอบหมายตามอนุมาตรา (1) จะมีสิทธิ

(a) เข้าถึงข้อมูลใดๆ รหัส หรือเทคโนโลยีที่มีความสามารถในการเข้ารหัส หรือไขรหัส ข้อมูลที่เข้ารหัสไว้เพื่อมีรูปแบบที่สามารถอ่านและเข้าใจได้หรือมีข้อความเพื่อการสอบสวนความผิดประเภทจับกุมได้นั้น

(b) ให้

(i) บุคคลใดๆ ที่มีเหตุอันควรสงสัยว่าใช้คอมพิวเตอร์เกี่ยวกับการกระทำความผิดประเภทจับกุมได้ หรือมีการใช้ในทำนองเดียวกันนี้ หรือ

(ii) บุคคลใดที่ถูกฟ้อง หรือที่เกี่ยวข้องกับการทำงานของคอมพิวเตอร์ดังกล่าวนั้น เพื่อให้บุคคลดังกล่าวช่วยเหลือทางด้านเทคนิคตามสมควรและความช่วยเหลืออื่นๆ เพื่อวัตถุประสงค์ในวรรค (a) และ

(c) เรียกร้องให้บุคคลใดๆ ที่มีเหตุอันควรสงสัยว่ามีข้อมูลการถอดรหัสอยู่ในความครอบครองเพื่อให้เขาสามารถเข้าถึงข้อมูลการถอดรหัสดังกล่าวซึ่งจำเป็นต้องถอดรหัสเพื่อวัตถุประสงค์ในการสืบสวนสอบสวนการกระทำความผิดประเภทจับกุมได้ดังกล่าว

(3) บุคคลใดๆ ที่ขัดขวางคำสั่งโดยอาศัยตามกฎหมายภายใต้อำนาจอนุมาตรา (2) (a) หรือผู้ไม่ปฏิบัติตามคำขอภายใต้อนุมาตรา (2) (b) หรือ (c) จะมีความผิดสำหรับการกระทำความผิดนั้นและจะต้องถูกปรับไม่เกิน $10,000 หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ

(4) ในกรณีที่ผู้ใดกระทำความผิดตามอนุมาตรา (3) และปรากฏว่ามีข้อมูลที่ถูกเข้ารหัสบรรจุไว้ในพยานหลักฐานที่เกี่ยวข้องกับการวางแผน เตรียมการ หรือคระกรรมการที่ระบุว่าเป็นความผิดร้ายแรง เขาจะมีความผิดดังต่อไปนี้แทนการลงโทษตามที่กำหนดไว้ในอนุมาตรา (3)

(a) ต้องระวางโทษเดียวกับที่กำหนดไว้สำหรับความผิดร้ายแรง เว้นแต่การลงโทษที่กำหนดไว้ว่าโทษปรับจะต้องไม่เกิน $50,000 หรือโทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับหรือ

(b) ต้องระวางโทษปรับไม่เกิน $50,000 หรือ โทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ซึ่งเป็นการกระทำความผิดร้ายแรงระบุโทษรุนแรงถึงประหารชีวิตหรือจำคุกตลอดชีวิต

(5) เพื่อวัตถุประสงค์ในอนุมาตรา (4) และอาจจะมีในอนุมาตรา (6) การกระทำความผิดร้ายแรง หมายถึง การกระทำความผิดใดๆ ภายใต้กฎหมายลายลักษณ์อักษร ต่อไปนี้

(a) กฎหมายที่เกี่ยวกับ (Written Law) การกระทำความผิดเกี่ยวกับการก่อให้เกิดการเสียชีวิตหรืออันตรายต่อร่างกาย

(b) กฎหมายที่เกี่ยวกับ (Written Law) การกระทำหรือการคุกคามซึ่งการดำเนินการเป็นผลร้ายต่อความมั่นคงของชาติ

(c) กฎหมายที่เกี่ยวกับ (Written Law) การสื่อสารหรืออาวุธรังสีหรือทางชีวภาพ

(d) กฎหมายที่เกี่ยวข้องกับอาวุธและวัตถุระเบิดที่บัญญัติไว้ (ในหมวด 13)

(e) กฎหมายที่เกี่ยวกับอาวุธทางเคมี ที่บัญญัติ (ในหมวด 37B)

(f) กฎหมายที่เกี่ยวข้องกับสารเคมีที่อาจก่อให้เกิดระเบิด (ในหมวด 65)

(g) กฎหมายที่เกี่ยวข้องกับการจี้และการป้องกันภัยของอากาศยานและสนามบินนานาชาติ (ในหมวด 124)

(h) กฎหมายที่ความผิดเกี่ยวข้อง การลักพาตัวเพื่อเรียกค่าไถ่ (ในหมวด 151)

(i) พระราชบัญญัติความผิดทางทะเล การเดินเรือ (ในหมวด 170B)

(j) พระราชบัญญัติเกี่ยวกับความลับของทางราชการ (ในหมวด 213)

(k) กฎหมายบัญญัติว่าด้วยพื้นที่ที่ได้รับความคุ้มครองเกี่ยวกับการการป้องกันความปลอดภัย (ในหมวด 256)

(l) กฎหมายว่าด้วยหน่วยงานตามกฎหมาย และหน่วยงานของรัฐ (คุ้มครองเกี่ยวกับเรื่องความลับ) (ในหมวด 319)

(m) พระราชบัญญัติเกี่ยวกับการควบการการค้าทางด้านกลยุทธ์ (ในหมวด 300)

(n) พระราชบัญญัติเกี่ยวกับการปราบปรามเกี่ยวกับแหล่งเงินทุนให้กับกลุ่มก่อการร้าย (ในหมวด 325)

(o) พระราชบัญญัติเกี่ยวข้องกับการต่อต้านการก่อการร้ายข้ามชาติ (ในหมวด 339, Rg 1) และ

(p) กฎหมายอื่นๆ ตามที่รัฐมนตรีประกาศหรือในพระราชกิจจานุเบกษากำหนดไว้

(6) การกระทำที่จะถือได้ว่าเป็นความผิดร้ายแรง จะต้องมีโทษสูงสุดดังต่อไปนี้ ไม่ว่าก่อนหรือหลังการพิสูจน์ว่ามีความผิด

(a) จำคุกตั้งแต่ 5 ปีขึ้นไป

(b) จำคุกตลอดชีวิต หรือ

(c) ประหารชีวิต

(7) ในการดำเนินคดีกับบุคลใดบุคคลหนึ่งที่กระทำความผิดตามมาตรานี้ หากปรากฏว่าบุคคลนั้นมีข้อมูลที่ถอดรหัสอยู่ในความครอบครองในเวลาใดก่อนที่จะร้องขอเพื่อเข้าถึงข้อมูลดังกล่าวให้สันนิษฐานว่าบุคคลนั้นได้ครอบครองข้อมูลถอดรหัสในเวลาต่อมา เว้นแต่ จะพิสูจน์ได้ว่าข้อมูลถอดรหัสนั้น

(a) ไม่ได้อยู่ในความครอบครองของเขาในเวลาที่ได้มีการร้องขอ และ

(b) ยังไม่ได้อยู่ในความครอบครองของเขาหลังจากที่มีการร้องขอ

(8) บุคคลที่ได้ปฏิบัติโดยสุจริต หรือ กระทำการตามคำสั่งให้เป็นไปตามอนุมาตรา (2)

บุคคลนั้นไม่ต้องรับผิดในการดำเนินทางอาญาใดๆ หรือ ความผิดในทางแพ่ง ในความเสียหายที่เกิดขึ้นจากการกระทำนั้นๆ

(9) เพื่อวัตถุประสงค์ของมาตรานี้

“ข้อมูล” หมายถึง การแสดงข้อมูลหรือ ความคิดที่ถูกจัดเก็บไว้ในรูปแบบที่เหมาะสมในการใช้งานทางระบบคอมพิวเตอร์

“การถอดรหัสข้อมูล” หมายถึง การแปลงข้อมูลอิเล็กทรอนิกส์จากรูปแบบที่เปลี่ยนแปลงไปจากเดิม (Cipher Text) นั้นให้กลับไปอยู่ในรูปของข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปแบบเดิมก่อนการเปลี่ยนแปลง (Plaintext)

“ข้อมูลที่เข้ารหัสไว้” หมายถึง การแปลงข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปหนึ่งที่อ่านได้ (Plaintext) ให้อยู่ในอีกรูปแบบหนึ่งที่เปลี่ยนแปลงไปจากเดิมซึ่งอ่านไม่ได้ (Cipher Text)

“ข้อมูลต้นฉบับ” หมายถึง ข้อมูลเดิมก่อนที่จะมีการปรับเปลี่ยนรูปแบบหรือ แปลงข้อมูลจนทำให้มีความไม่เข้าใจในข้อมูลนั้นมากขึ้น

และในประเทศสิงคโปร์ได้บัญญัติเรื่องการขัดขวางการเข้าถึงคอมพิวเตอร์ไว้ใน Criminal Procedure Code (Chapter 68) มาตรา 39 (3) ว่า บุคคลใดที่ขัดขวางการกระทำการตามกฎหมายภายใต้อำนาจอนุมาตรา (1) หรือ ผู้ที่ล้มเหลวในการจัดการตามคำขอภายใต้อนุมาตรา (2) จะมีความผิดสำหรับการกระทำความผิดนั้นและจะต้องถูกปรับไม่เกิน $ 5,000 หรือ จำคุกไม่เกิน 6 เดือน หรือทั้งจำทั้งปรับ

ส่วนการขัดขวางการเข้าถึงข้อมูลการถอดรหัสบัญญัติโทษไว้ในมาตรา 40 (3) (4) ไว้ว่า

(3) บุคคลใดๆ ที่ขัดขวางการกระทำการตามกฎหมายภายใต้อำนาจอนุมาตรา (2) (a) หรือผู้

ที่ล้มเหลวในการจัดการตามคำขอภายใต้อนุมาตรา (2) (b) หรือ (c) จะมีความผิดสำหรับการกระทำความผิดนั้นและจะต้องถูกปรับไม่เกิน $10,000 หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ

ในกรณีที่ผู้ใดถูกพิสูจน์ว่ามีความผิดตามอนุมาตรา (3) และปรากฏว่ามีข้อมูลที่ถูกเข้ารหัสบรรจุไว้ในพยานหลักฐานที่เกี่ยวข้องกับการวางแผน เตรียมการหรือคณะกรรมการที่ระบุว่าเป็นความผิดร้ายแรง เขาจะมีความผิดดังต่อไปนี้แทนการลงโทษตามที่กำหนดไว้ในอนุมาตรา (3)

จากการที่ได้ศึกษากฎหมายของประเทศสิงคโปร์ดังกล่าวมาแล้วข้างต้น จะเห็นได้ว่าประเทศสิงคโปร์นั้นจะให้อำนาจแก่บุคคลที่เป็นข้าราชการตำรวจหรือบุคคลที่ได้รับอนุญาตในการเข้าถึงการใช้งานด้านคอมพิวเตอร์ สามารถที่จะเข้าถึงข้อมูล หรือระบบข้อมูลในคอมพิวเตอร์ได้ตามที่กฎหมายให้อำนาจไว้และเจ้าหน้าที่ตำรวจสามารถทำการจับกุมได้โดยไม่มีหมาย หากมีเหตุอันเป็นการสงสัยว่า มีเหตุในการกระทำความผิดตามกฎหมายนี้โดยการศึกษาดังกล่าวผู้เขียนจะทำการวิเคราะห์ในประเด็นที่มีปัญหาในบทต่อไป

ตารางที่ 3.1 เปรียบเทียบหลักเกณฑ์ในการเข้าถึงข้อมูลคอมพิวเตอร์ที่เป็นหลักฐานเกี่ยวกับการกระทำความผิด

ประเทศ	กฎหมาย	หลักเกณฑ์ในการเข้าถึงข้อมูลคอมพิวเตอร์ที่เป็นหลักฐานเกี่ยวกับการกระทำความผิด	ผู้ที่มีอำนาจในการเข้าถึง
ประเทศไทย	- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	- จะต้องมีหมายจากศาล และในการออกหมายนั้นจะต้องมีเหตุที่จะออกหมายด้วยเว้นแต่ 1. มีหนังสือสอบถาม หรือเรียกบุคคลที่เกี่ยวข้อง กับการกระทำความผิดมาเพื่อให้ถ้อยคำ ส่งคำชี้แจง เป็นหนังสือหรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถข้าใจได้ 2. เรียกข้อมูลจราจรทางคอมพิว เตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง 3. สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่	- พนักงานเจ้าหน้าที่ - พนักงานสอบสวน
ประเทศสหรัฐอเมริกา	- The Electronic Communications Privacy Act (ECPA)	- จะต้องกระทำการโดยมีหมายค้น (Search Warrant) แต่อย่างไรก็ตาม การยึดและค้นข้อมูลคอมพิว เตอร์โดยไม่มีหมายอาจจะทำได้เพียงบางกรณีเท่านั้น ซึ่งข้อ ยกเว้นของการยึดและค้นข้อมูล คอมพิวเตอร์โดยไม่ต้องมีหมาย มีอยู่ด้วยกัน 3 ประการ คือ 1.กรณีที่ได้รับความยินยอม (Consent) 2.กรณีที่เป็นการอันจำเป็นและเร่งด่วน (Exigent Circumstances) และ 3. กรณีที่การยึดค้นข้อมูลคอมพิวเตอร์นั้นได้มาจากการจับกุมโดยชอบ (Search Incident to a Lawful Arrest)	- พนักงานสอบสวน - เจ้าพนักงาน

ตารางที่ 3.1 (ต่อ)

ประเทศ	กฎหมาย	หลักเกณฑ์ในการเข้าถึงข้อมูลคอมพิวเตอร์ที่เป็นหลักฐานเกี่ยวกับการกระทำความผิด	ผู้ที่มีอำนาจในการเข้าถึง
ประเทศสิงคโปร์	- Computer Misuse Act	- จะต้องมีหมาย เว้นแต่ หากมีเหตุอันควรสงสัยตามสมควรว่ามีการกระทำความผิดในกรณีนี้ไม่จำเป็นต้องมีหมาย	- เจ้าหน้าที่ตำรวจ - เจ้าหน้าที่ผู้ที่ได้รับมอบอำนาจ

บทที่ 4

วิเคราะห์ปัญหาทางกฎหมายว่าด้วยลักษณะอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐาน

ก่อนที่จะมีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ที่มีการบัญญัติความผิดเกี่ยวกับลักษณะอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในการใช้อำนาจของพนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลคอมพิวเตอร์นั้น โดยการเข้าถึงคอมพิวเตอร์โดยไม่ชอบด้วยกฎหมายไม่สามารถที่จะหาตัวผู้กระทำความผิดมาลงโทษในการกระทำนั้นได้ เพราะไม่มีกฎหมายใดบัญญัติให้การกระทำนั้นเป็นความผิดหรือไม่ และอำนาจที่มีอยู่ในกฎหมายอาญาในขณะนั้นก็ไม่สามารถที่จะนำมาเทียบเคียงหรือปรับใช้ได้

ลักษณะอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในความผิดอาญาในการเข้าถึงข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นี้ เป็นกฎหมายที่ได้มีการประกาศในราชกิจจานุเบกษามีผลใช้บังคับเป็นกฎหมาย และจากที่ได้ทำการศึกษาค้นคว้าและเห็นได้ว่าการกระทำดังกล่าว ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เป็นกฎหมายที่มีความเกี่ยวข้องกับเทคโนโลยีและศาสตร์ทางคอมพิวเตอร์ที่มีความซับซ้อนยุ่งยากและมีวิวัฒนาการไปตามแต่ละยุคสมัย และในขณะเดียวกันก็เป็นที่นิยมใช้กันอยู่ทั่วไป เพราะเป็นเทคโนโลยีที่ให้ความสะดวกสบายในการใช้คอมพิวเตอร์ในการทำงานในด้านต่างๆ เพราะฉะนั้น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นี้ จึงมีผลกระทบอย่างมากต่อบุคคลที่ใช้งานด้านคอมพิวเตอร์อยู่เป็นประจำ

และด้วยสภาพปัญหาในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในลักษณะที่เป็นกฎหมายพิเศษ เช่น ผู้กระทำความผิดอาจจะอยู่ ณ ที่ใดก็ได้ และได้ใช้เทคโนโลยีนั้นในการกระทำความผิด ซึ่งเป็นการยากต่อการตรวจสอบหาเหตุแห่งการกระทำความผิด และเป็นการยากต่อการค้นยึดที่จะนำตัวผู้กระทำความผิดมาลงโทษ และรวมไปถึงความเสียหายที่อาจจะกระทบไปถึงบุคคลอื่นๆ อีกด้วย[87] ดังนั้นเพื่อเป็นการป้องกันหรือรักษาคอมพิวเตอร์ของตนเองให้มีความเป็นส่วนตัวและความปลอดภัย จึงควรที่จะมีการติดตั้งระบบตรวจสอบการเข้าถึงหรือ การติดตั้งกำแพงไฟ (Firewall) และรัฐบาลควรที่จะขอความร่วมมือระหว่างหน่วยงานต่างๆ ที่เกี่ยวข้องกับภาครัฐและเอกชนเพื่อป้องกันอาชญากรรมทางคอมพิวเตอร์ โดยการบัญญัติหรือการตรากฎหมายเพื่อกำหนดมาตรการว่าการกระทำใดบ้างที่เป็นการกระทำความผิดและมีโทษ อีกทั้งในด้านการขอความร่วมมือระหว่างหน่วยงานก็ไม่ได้จำกัดเฉพาะหน่วยงานที่มีหน้าที่ตามกฎหมายแต่อย่างใด แต่ให้หมายความรวมไปถึงหน่วยงาน

---

[87] ทวีเกียรติ มีนะกนิษฐ, **เอกสารประกอบการสัมมนาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550** (กรุงเทพฯ: คณะกรรมการฝ่ายวิชาการ สถาบันวิจัยและพัฒนากฎหมาย สภาทนายความ, 2550).

ต่างๆ ที่อาจจะเกี่ยวข้องด้วย เช่น บุคคลที่อยู่ในประเทศหนึ่งอาจจะทำการเข้าถึงข้อมูลคอมพิวเตอร์ที่อยู่ในประเทศอีกประเทศหนึ่ง โดยกระทำการดังกล่าวอาจจะกระทำผ่านทางระบบเครือข่ายอินเตอร์เน็ต หรือการใช้คอมพิวเตอร์ที่อยู่อีกประเทศ ส่งผ่านระบบคอมพิวเตอร์ที่ได้มีการเชื่อมเข้าหากัน เป็นต้น เพราะฉะนั้น การป้องกันหรือแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์จึงไม่อาจที่จะจำกัดเฉพาะประเทศใดประเทศหนึ่งเท่านั้น

ในปัจจุบัน ประเทศไทยได้มีมาตรการทางกฎหมายที่เกี่ยวข้องกับคอมพิวเตอร์ไว้ โดยการบัญญัติหรือการตรากฎหมายโดยการกำหนดให้การกระทำใดบ้างที่ให้ถือว่าเป็นความผิดเกี่ยวกับคอมพิวเตอร์และให้การกระทำความผิดนั้นมีโทษทางอาญาด้วย เพื่อป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่อาจจะเกิดขึ้นอีกด้วย โดยการบัญญัติหรือตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ขึ้น ที่ได้มีการกล่าวไว้ว่า การกระทำใดเป็นความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจทำการสืบสวนสอบสวนเป็นกรณีพิเศษได้ตามประมวลกฎหมายวิธีพิจารณาความอาญาที่ว่าด้วยเรื่องอำนาจของเจ้าพนักงาน

จากการศึกษา พบว่าการใช้อำนาจของพนักงานเจ้าหน้าที่จะใช้อำนาจได้ก็ต่อเมื่อมีกรณีที่มีเหตุอันควรเชื่อได้ว่าได้มีการกระทำความผิดเกิดขึ้น และความผิดนั้นจะต้องเป็นความผิดที่ได้เกิดขึ้นตามพระราชบัญญัตินี้ด้วย หากความผิดที่เกิดขึ้นเป็นความผิดตามกฎหมายอื่นย่อมไม่เข้าเงื่อนไขหลักเกณฑ์ในการที่พนักงานเจ้าหน้าที่จะใช้อำนาจตามพระราชบัญญัตินี้ได้ เนื่องจากการใช้อำนาจของพนักงานเจ้าหน้าที่ ได้บัญญัติไว้เพียงว่าพนักงานเจ้าหน้าที่สามารถใช้อำนาจได้เพียงบางกรณีเท่านั้น เช่น ในกรณีที่ “เพียงแค่สงสัย” เท่านั้น และหากพนักงานเจ้าหน้าที่จะมีอำนาจเพิ่มมากขึ้นก็เพียงแต่ “มีเหตุอันควรเชื่อได้ว่า” เท่านั้น ที่จะทำให้พนักงานเจ้าหน้าที่มีอำนาจเพิ่มขึ้น แต่การจะใช้อำนาจนี้ได้พนักงานเจ้าหน้าที่ใช้เฉพาะเท่าที่จำเป็นเท่านั้นเพราะพนักงานเจ้าหน้าที่จะมีอำนาจเพียงเพื่อแสวงหาข้อเท็จจริงตามพฤติการณ์ที่คาดว่าอาจจะเกิดมีขึ้นถ้าหากความผิดได้เกิดขึ้นแล้วย่อมก่อให้เกิดอำนาจในการที่จะทำการสืบสวนเพื่อที่จะช่วยให้พนักงานเจ้าหน้าที่มีอำนาจในการดำเนินการสอบสวนในความผิดที่ได้เกิดขึ้น และเมื่อความผิดที่ได้เกิดขึ้นเป็นความผิดที่ได้มีความเกี่ยวข้องกับคอมพิวเตอร์ พนักงานเจ้าหน้าที่มีอำนาจที่จะสืบสวนคดีนี้ได้โดยไม่จำกัดเขตอำนาจ

นอกจากนี้ จากการที่ได้ทำการศึกษาทฤษฎีทางกฎหมายที่เกี่ยวข้องกับการบัญญัติหรือการตราพระราชบัญญัตินี้ ผู้เขียนเห็นว่าการบังคับใช้กฎหมายวิธีสบัญญัติในส่วนของพระราชบัญญัตินี้ไม่สามารถป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้อย่างชัดเจน เนื่องด้วยยังคงมีปัญหาในขั้นตอนของการดำเนินคดีในส่วนของการกระทำความผิดในส่วนที่เกี่ยวข้องกับคอมพิวเตอร์อยู่หลายประการ เพราะฉะนั้น ในบทนี้ผู้เขียนจะกล่าวถึงอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ตามมาตรา 18 ที่กำหนดไว้ว่า เมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ขึ้น ให้พนักงานเจ้าหน้าที่มีอำนาจตามอนุมาตรา 1 ถึง อนุมาตรา 8 แห่งพระราชบัญญัตินี้ ทำการสืบสวนสอบสวนเพื่อประโยชน์ในการใช้เป็นพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดและในการหาตัวผู้กระทำความผิด และได้มีบทบัญญัติได้กล่าวไว้ว่า ให้พนักงานเจ้าหน้าที่มีอำนาจทำการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้เท่านั้น เพราะเหตุนี้ พนักงานเจ้าหน้าที่จึงมีอำนาจ

หน้าที่ในการสืบสวนสอบสวนได้เฉพาะแต่ในความผิดที่เกี่ยวข้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เท่านั้น ความผิดในส่วนอื่นๆ ที่ไม่ได้บัญญัติไว้ในพระราชบัญญัตินี้ พนักงานเจ้าหน้าที่ไม่อาจที่จะมีอำนาจกระทำได้ ตามมาตรา 18 และ มาตรา 19 ถึงแม้ว่าความผิดนั้นจะมีความเกี่ยวข้องกับระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือจะเป็นอุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ก็ตาม ในกระบวนการของการสืบสวนสอบสวนการกระทำความผิดอาญานั้นได้เพราะการกระทำความผิดอาญาไม่ได้เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จึงไม่ได้อยู่ในอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ที่จะใช้อำนาจในการสืบสวนสอบสวน

ผู้เขียนเห็นว่า การบัญญัติมาตรา 18 ในลักษณะเช่นนั้น เป็นการจำกัดการใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่มากจนเกินไป เพราะพนักงานเจ้าหน้าที่เป็นผู้ที่มีความรู้ความเชี่ยวชาญเกี่ยวกับคอมพิวเตอร์ ด้วยการกระทำความผิดอาญาที่เกี่ยวข้องกับคอมพิวเตอร์ไม่ได้เป็นการกระทำความผิดที่เกิดกับระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เท่านั้น การกระทำความผิดอาญาอาจจะเกี่ยวข้องกับคอมพิวเตอร์ในประการอื่นๆ อีกด้วย เช่น การใช้คอมพิวเตอร์ที่เป็นวัตถุแห่งการกระทำความผิด เช่น การใช้โทรศัพท์เคลื่อนที่ส่ง SMS การขโมยเครื่องคอมพิวเตอร์ไป เป็นต้น หรือ การนำเอาเครื่องคอมพิวเตอร์มาใช้เป็นเครื่องมือในการกระทำความผิด หรือ การใช้คอมพิวเตอร์ในบางส่วนที่มีความเกี่ยวข้องกับการกระทำความผิด โดยการใช้คอมพิวเตอร์ในประเภทนี้อาจนำอุปกรณ์อย่างอื่นมาใช้แทนกันได้ เช่น การเก็บข้อมูลไว้ในเครื่องคอมพิวเตอร์ หรือ การเก็บข้อมูลการใช้โทรศัพท์เคลื่อนที่ไว้ในระบบจัดเก็บของคอมพิวเตอร์ เพราะถ้าไม่มีเครื่องคอมพิวเตอร์ ผู้กระทำความผิดสามารถที่จะนำข้อมูลดังกล่าวไปเก็บไว้ในอุปกรณ์ต่างๆ ได้ อย่างเช่น ในคดีนายอำพล ตั้งนพกุล ในการส่งข้อความหมิ่นสถาบัน ซึ่งรูปแบบของการส่งข้อความสั้น เป็นการทำงานโดยส่งข้อความไปที่ Short Message Service Centre (SMSC) และระบบจะทำการประมวลผล แล้วส่งไปยังเครือข่ายของเครื่องรับเข้าไปยังเครื่องโทรศัพท์เคลื่อนที่ที่ใช้กับโทรศัพท์ดังกล่าว ซึ่งเป็นการนำเข้าสู่ระบบคอมพิวเตอร์ เป็นต้น ดังนั้นควรแก้ไขในมาตรา 18 วรรคแรก ให้พนักงานเจ้าหน้าที่สามารถใช้อำนาจในการทำการสืบสวนสอบสวนการกระทำความผิดใดๆ ที่มีความเกี่ยวข้องกับระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ด้วย ถึงแม้ว่าการกระทำนั้นจะไม่ได้เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยตรงก็ตาม โดยเห็นควรแก้ไขดังต่อไปนี้ มาตรา 18

> ภายใต้บังคับแห่งมาตรา 19 เพื่อประโยชน์ในการสืบสวนสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือการกระทำความผิดใดที่มีต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ที่มีความเกี่ยวข้อง ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด เฉพาะเท่าที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาผู้กระทำความผิด

แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จะได้กำหนดหลักเกณฑ์พิเศษขึ้นมาโดยการให้พนักงานเจ้าหน้าที่ ซึ่งเป็นบุคคลที่มีความรู้ความชำนาญในด้าน

คอมพิวเตอร์เข้ามาทำหน้าที่ในการสืบสวนสอบสวนตามพระราชบัญญัตินี้ เพราะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นการยากต่อการตรวจสอบและยากต่อการพิสูจน์ในเรื่องความรับผิดและไม่สามารถที่จะกระทำได้อย่างรวดเร็ว ซึ่งได้ส่งผลอย่างมากในวงกว้าง ดังเช่น ในกฎหมายของประเทศสหรัฐอเมริกาที่ได้มีการกำหนดข้อยกเว้นที่ให้อำนาจเจ้าพนักงานของรัฐทำการเข้าถึงข้อมูลการใช้งานทางคอมพิวเตอร์ได้เพื่อประโยชน์ในการแสวงหาพยานหลักฐานในการดำเนินคดีกับผู้ที่กระทำความผิดทางอาญา โดยการกระทำของพนักงานเจ้าหน้าที่ให้อยู่ภายใต้การดูแลของศาลหรือดุลพินิจของศาล ดังนั้นผู้เขียนเห็นว่า เมื่อเปรียบเทียบกับหลักของกฎหมายต่างประเทศแล้วยังมีข้อพิจารณาอยู่หลายประการที่ควรนำมาศึกษาว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จะนำหลักต่างๆ มาปรับปรุง แก้ไขเพิ่มเติมพระราชบัญญัตินี้ต่อไปหรือไม่อย่างไร โดยผู้เขียนขอแบ่งออกเป็น 2 หัวข้อ ดังต่อไปนี้

4.1 อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในกรณีไม่มีหมาย

ตามมาตรา 18 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กำหนดให้ การใช้อำนาจของพนักงานเจ้าหน้าที่มีอยู่ด้วยกัน 3 ประการ และในอำนาจที่จะออกหมายไม่ว่าจะเป็นหมายจับ หมายขัง หมายจำคุก หมายค้น และหมายปล่อยนั้น ศาลจะเป็นผู้ออกคำสั่งตามที่ศาลเห็นสมควรหรือโดยมีผู้ร้องขอเท่านั้น

นอกจากนี้ หากเป็นกรณีจำเป็นเร่งด่วนที่มีเหตุอันสมควร หากผู้ร้องขอไม่อาจไปพบศาลได้ ผู้ร้องขออาจจะต้องร้องขอต่อศาลทางโทรศัพท์ โทรสาร สื่ออิเล็กทรอนิกส์ หรือสื่อเทคโนโลยีสารสนเทศเพื่อขอให้ศาลออกหมายจับหรือหมายค้นได้ ในกรณีเช่นว่านี้เมื่อศาลสอบถามจนปรากฏว่ามีเหตุที่จะออกหมายจับหรือหมายค้นได้ และศาลได้มีคำสั่งให้ออกหมายนั้นแล้ว ก็ให้ทำการจัดส่งสำเนาหมายไปยังผู้ร้องขอ

และเมื่อได้มีการออกหมายแล้ว ให้ศาลดำเนินการให้กับผู้ที่เกี่ยวข้องกับการขอหมายมาพบศาลเพื่อสาบานตัวโดยไม่ชักช้า โดยจดบันทึกถ้อยคำของบุคคลดังกล่าวและลงลายมือชื่อของศาลผู้ออกหมายไว้ หรือจะใช้เครื่องบันทึกเสียงก็ได้โดยจัดให้มีการถอดเสียง เป็นหนังสือและลงลายมือชื่อของศาลผู้ออกหมาย บันทึกที่มีการลงลายมือชื่อรับรองดังกล่าวแล้ว ให้เก็บไว้ในสาระบบของศาล หากความปรากฏต่อศาลในภายหลังว่าได้มีการออกหมายไปโดยฝ่าฝืนต่อบทบัญญัติแห่งกฎหมาย ศาลอาจมีคำสั่งให้เพิกถอนหรือแก้ไขเปลี่ยนแปลงหมายเช่นว่านั้นได้ ทั้งนี้ ศาลจะมีคำสั่งให้ผู้ร้องขอจัดการแก้ไขเพื่อเยียวยาความเสียหายที่เกิดขึ้นแก่บุคคลที่เกี่ยว ข้องตามที่เห็นสมควรก็ได้ ดังนั้นจะเห็นได้ว่า มีอยู่เพียง 3 อนุ เท่านั้น ที่ไม่ต้องขออนุญาตจากศาล คือ

1. มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

จากการศึกษา พบว่าอำนาจในการมีหนังสือสอบถามหรือเรียกเพื่อมาให้ถ้อยคำ หรือโดยการให้บุคคลส่งคำชี้แจงมาเป็นหนังสือ หรือโดยการส่งเอกสาร ข้อมูล หรือวัตถุอื่นใด มาให้แก่พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ สามารถกระทำได้

ผู้เขียนเห็นว่า อำนาจในการมีหนังสือสอบถามหรือเรียกเพื่อมาให้ถ้อยคำ หรือโดยการให้บุคคลส่งคำชี้แจงมาเป็นหนังสือ หรือโดยการส่งเอกสาร ข้อมูล หรือวัตถุอื่นใด เป็นอำนาจหน้าที่ของเจ้าพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ ที่มีอยู่แล้วตามประมวลกฎหมายวิธีพิจาณาความอาญา ตามมาตรา 52 ซึ่งได้บัญญัติเกี่ยวกับการออกหมายเรียกไว้ซึ่งในลักษณะเช่นนี้ เป็นการถูกเรียกมาตามหมาย และ บุคคลที่ถูกเรียกมาจะต้องอยู่ในฐานะที่ให้ความร่วมมือกับบ้านเมืองในการที่จะรักษาความยุติธรรม ถึงแม้ว่าบุคคลผู้นั้นจะถูกเรียกมาในฐานะผู้ต้องหา หรือ จำเลยก็ตาม และก็จะมาอยู่ในฐานะที่เป็นคู่ความที่มีสิทธิเหมือนคู่ความอีกฝ่ายหนึ่ง แต่ไม่มีฐานะเสมือนผู้กระทำความผิดเป็นต้น

2. เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

จากการศึกษา พบว่าอำนาจในการเรียกข้อมูลจราจรทางคอมพิวเตอร์ มีความสำคัญมากในการทำการรวบรวมพยานหลักฐานที่ใช้ในการสืบสวนสอบสวนที่เป็นส่วนหนึ่งของการติดต่อสื่อสาร

ผู้เขียนเห็นว่า ผู้ให้บริการได้มีข้อมูลจราจรทางคอมพิวเตอร์อยู่ในระบบคอมพิวเตอร์อยู่แล้ว ซึ่งเป็นหน้าที่ที่ผู้ให้บริการมีหน้าที่จะต้องทำการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้บริการไว้ เพราะข้อมูลจราจรทางคอมพิวเตอร์ถือได้ว่าเป็นข้อมูลที่มีความสำคัญ สามารถนำพยานหลักฐานดังกล่าวมาทำการสอบสวนในคดีที่เป็นความผิดเกี่ยวกับคอมพิวเตอร์ได้ เช่น เลขที่ไอพี หมายเลขโทรศัพท์ หรือ IP Address ชื่อที่อยู่ของผู้ใช้บริการ การใช้บริการโดยการลงทะเบียน ข้อมูลของผู้ให้บริการ ในลักษณะที่เป็นการให้บริการผ่านทางระบบหรือเครือข่ายใด เป็นต้น

3. สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

จากการศึกษา พบว่าอำนาจในการสั่งให้ผู้ใช้บริการส่งมอบข้อมูลนี้ เป็นบทบัญญัติที่มีข้อมูลเกี่ยวกับบุคคลที่ใช้บริการได้ลงทะเบียน (Register) ไว้ ซึ่งข้อมูลของผู้ใช้บริการผู้ให้บริการมีหน้าที่จะต้องเก็บรักษาไว้ ดังนั้น หากผู้ให้บริการมีข้อมูลของผู้ใช้บริการอยู่ในความครอบครองหรือควบคุมของผู้ให้บริการพนักงานเจ้าหน้าที่มีอำนาจที่จะสั่งให้ผู้ให้บริการส่งมอบให้ก็ได้

จากการศึกษาข้างต้น พบว่าการจะเรียกตามอนุมาตราที่ได้กล่าวมาแล้วข้างต้น พนักงานเจ้าหน้าที่มีอำนาจที่จะกระทำการดังกล่าวได้ โดยไม่ต้องขออนุญาตจากศาล และเมื่อไม่มีการขออนุญาตจากศาลก่อนที่จะกระทำการดังกล่าว การกระทำนั้นอาจจะเป็นการไปละเมิดสิทธิส่วนตัวและเสรีภาพในการสื่อสารนั้น ถึงแม้ว่ากฎหมายได้ให้การรับรองไว้หรือคุ้มครองให้มีสิทธิที่จะกระทำกับทรัพย์ของผู้อื่นได้ แต่การกระทำนั้นต้องกระทำขึ้นเพื่อประโยชน์ และจะต้องไม่ขัดหรือแย้งหรือไม่ชอบด้วยกฎหมาย และการจะกระทำการดังกล่าวจะต้องได้รับความยินยอมจากบุคคลดังกล่าวด้วย

เมื่อทำการศึกษาเปรียบเทียบกับกฎหมายของประเทศอเมริกาแล้วเห็นว่าทางรัฐบาลได้ห้ามการรับข้อมูลผ่านเครื่องมืออิเล็กทรอนิกส์โดยที่ไม่ได้รับอนุญาตจากศาลและได้มีบทลงโทษหากมีการกระทำที่ฝ่าฝืน เว้นแต่คู่กรณีจะให้ความยินยอมในการกระทำเช่นนั้น แต่อย่างไรก็ตาม เจ้าพนักงานมีสิทธิที่จะขออนุญาตจากศาลก่อนที่จะกระทำการดังกล่าว ดังนั้น เจ้าหน้าที่จึงไม่มีอำนาจที่จะทำการค้นได้หากไม่มีหมายค้นจากศาลและการค้นนั้นจะต้องแสดงเหตุผลอันสมควรให้

ศาลได้เห็นได้ว่าเจ้าหน้าที่มีเหตุอันสมควรที่ศาลจะอนุญาตให้กระทำการดังกล่าวได้ แต่ก็มีบางกรณีที่ได้รับการยกเว้นไว้ว่าให้ทำการค้นได้หากไม่มีหมายจากศาล แต่การค้นนั้นจะต้องได้รับความยินยอมจากเจ้าของข้อมูลคอมพิวเตอร์นั้นเสียก่อน แต่ถ้าหากว่าเจ้าของข้อมูลคอมพิวเตอร์ไม่อยู่ในขณะนั้น บุคคลอื่นอาจให้ความยินยอมแก่เจ้าหน้าที่ในการค้นหาข้อมูลคอมพิวเตอร์นั้นได้ โดยบุคคลที่สามารถให้ความยินยอมได้ คือ

1. คู่สมรส (Spouses and Domestic Partners)
2. ผู้ปกครอง (Parents)
3. ช่างซ่อมคอมพิวเตอร์ (Computer Repair Technicians)
4. ผู้ดูแลระบบ (System Administrators)

การที่พนักงานเจ้าหน้าที่จะกระทำการเข้าถึงข้อมูลของประชาชนได้ จะต้องขออนุญาตจากศาลเสียก่อน ในการขออนุญาตนั้นจะต้องกระทำเป็นลายลักษณ์อักษร โดยทำเป็นคำร้องในคำร้องนั้นจะต้องระบุเหตุอันสมควรที่จำเป็นที่จะต้องใช้วิธีการในการเข้าถึงดังกล่าวด้วย

ผู้เขียนเห็นว่า หลักการนี้น่าจะนำมาปรับใช้กับกฎหมายของประเทศไทยได้ และเมื่อมีความผิดปรากฏซึ่งหน้าที่กำลังจะกระทำลงในที่รโหฐาน เมื่อมีเหตุอันควรสงสัยว่าสิ่งของที่ได้มานั้นได้มาโดยการกระทำความผิดได้ซ่อนหรืออยู่ในนั้น ประกอบทั้งจะต้องมีเหตุอันควรเชื่อได้ว่าเนื่องจากการกระทำนั้นช้ากว่าจะไปขอหมายค้นจากศาลได้สิ่งของเหล่านั้นจะถูกโยกย้ายเปลี่ยนแปลงสถานที่เสียก่อน การจะเข้าข้อยกเว้นตามอนุมาตรานี้ได้จะต้องเป็นกรณีดังต่อไปนี้

1. มีความสงสัยว่าสิ่งของได้ถูกซ่อนหรืออยู่ในนั้น
2. มีเหตุอันควรเชื่อได้ว่าจะต้องดำเนินการออกหมายค้นจะทำให้เกิดความล่าช้า อาจจะทำให้มีการโยกย้ายสิ่งของจากที่รโหฐานนั้นก่อนได้ แต่ข้อยกเว้นตามมาตรา 92(4) นี้จำกัดเฉพาะกรณีสิ่งของที่ได้มาโดยการกระทำความผิดเท่านั้น ไม่ได้หมายความรวมไปถึงการใช้คอมพิวเตอร์ในการเข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ แม้จะเป็นสิ่งของที่จำเป็นต้องยึดเพื่อประกอบไว้ในสำนวนแต่ก็ไม่ได้ทำให้เจ้าพนักงานสามารถเข้าค้นได้โดยไม่มีหมายค้น จึงเป็นวิธีการที่เหมาะสมแล้ว

เนื่องมาจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีเพิ่มมากขึ้นเรื่อยๆ จึงถือเป็นเรื่องสำคัญที่จะนำเอากฎหมายของต่างประเทศมาใช้ในด้านของกฎหมายเพื่อช่วยศาลในการติดสินคดี เพราะคอมพิวเตอร์ได้เข้ามาเกี่ยวข้องกับการพิจารณาพิพากษาคดีมากขึ้น และในการสืบสวนหรือหาพยานหลักฐานทางคอมพิวเตอร์ดังกล่าวสามารถนำมารับฟังเป็นพยานหลักฐานได้

ดังนั้น เมื่อทำการศึกษาเปรียบเทียบกับกฎหมายของประเทศสิงคโปร์ ในกฎหมาย Computer Misuse and Cyber Security Act. จะเห็นได้ว่า ในมาตรา 15A ได้บัญญัติขึ้นมาเพื่อป้องกันหรือต่อต้านภัยคุกคามต่อความมั่นคงของชาติ ในการป้องกันประเทศหรือความสัมพันธ์กับต่างประเทศสิงคโปร์ โดยการกำหนดให้รัฐมนตรี มอบอำนาจให้แก่บุคคลหรือองค์ที่ได้ระบุไว้ในหมายมีอำนาจเท่าที่จำเป็นในการป้องกัน หรือ ต่อต้านทางด้านข้อมูลคอมพิวเตอร์ หรือบริการคอมพิวเตอร์ และในกฎหมายของประเทศสิงคโปร์ ได้ให้อำนาจเจ้าหน้าที่สามารถเข้าทำการจับ การค้นและยึด ได้โดยไม่ต้องขออนุญาตจากศาล หากกรณีนั้นเป็นการสงสัยว่าจะมีเหตุในการกระทำความผิดเกิดตามพระราชบัญญัตินี้

ฉะนั้นการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ที่เป็นการกระทำความผิดที่น่าจะก่อให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือเพื่อการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ การใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ก็ควรให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เช่นเดียวกับการกระทำความผิดในมาตราอื่นๆ กล่าวคือ มีการตรวจสอบการใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่จากศาลก่อน

ผู้เขียนเห็นว่า การกระทำความผิดตามมาตราใดในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 การใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ตามมาตรา 18 (1) (2) (3) ควรให้เป็นไปในทิศทางเดียวกัน

4.2 อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการขอหลักฐานในกรณีมีหมาย

ตามมาตรา 19 แห่งพระราชบัญญัตินี้ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ที่กำหนดว่า

> ให้อำนาจพนักงานหน้าที่รวม 5 อนุมาตรา โดยพนักงานเจ้าหน้าที่จะต้องยื่นคำร้องต่อศาลที่เขตอำนาจและศาลจะต้องมีคำสั่งอนุญาตตามคำร้องก่อน พนักงานเจ้าหน้าที่จึงจะมีอำนาจในการดำเนินการได้ แต่ในคำร้องดังกล่าวนั้นจะต้องระบุเหตุอันควรเชื่อได้ว่าได้มีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นี้ด้วย

จะเห็นได้ว่าเป็นบทบัญญัติที่ได้กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจรวม 5 อนุมาตรา คือ (4) (5) (6) (7) และ (8) ตามมาตรา 18 โดยการให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจและศาลจะต้องมีคำสั่งอนุญาตตามคำร้องนั้นเสียก่อนที่พนักงานเจ้าหน้าที่จะสามารถดำเนินการดังกล่าวได้ อำนาจของพนักงานเจ้าหน้าที่ที่ต้องขออนุญาตจากศาล มีดังต่อไปนี้

4.2.1 อำนาจในการทำสำเนาข้อมูล

จากการศึกษาพบว่าอำนาจในการทำสำเนาข้อมูล คือ ข้อมูลทุกอย่างที่อยู่ในระบบคอมพิวเตอร์ รวมไปถึงชุดคำสั่งด้วย หากอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจจะประมวลผล เพราะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้น เป็นการกระทำต่อ “ข้อมูล” ดังนั้น ข้อมูลดังกล่าวจะต้องอยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจจะประมวลผลได้เท่านั้นที่จะได้รับความคุ้มครองตามพระราชบัญญัตินี้

ทั้งนี้ ข้อมูลที่อยู่ในสื่อบันทึกข้อมูลที่ไม่ได้มีการเชื่อมต่อระบบคอมพิวเตอร์ไม่ได้อยู่ในความหมายของคำว่า “ข้อมูลคอมพิวเตอร์” และไม่ได้รับความคุ้มครองตามพระราชบัญญัตินี้ เช่น แผ่นดิส ซีดีรอม เพราะไม่ได้อยู่ในระบบคอมพิวเตอร์ในสภาพที่อาจจะประมวลผลได้

เมื่อได้ทำการพิจารณาความหมายของคำว่า “ข้อมูลอิเล็กทรอนิกส์” ตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2544 ที่ตราขึ้นเพื่อรับรองผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ที่เป็นการรับรองข้อความที่อยู่บนสื่ออิเล็กทรอนิกส์ให้เท่าเทียมกับข้อความที่อยู่บนกระดาษและได้ให้ความหมายคำว่า “ข้อมูลอิเล็กทรอนิกส์” โดยให้ความหมายไว้ว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร เป็นต้น

ดังจะเห็นได้ว่า ในการก่ออาชญากรรมทางคอมพิวเตอร์ อาจจะกระทำความผิดโดยการคุกคามหรือการก่อให้เกิดความเสียหายให้เกิดขึ้น อาจจะไม่ใช่เพียงแค่ข้อมูลอิเล็กทรอนิกส์ตามความหมายในพระราชบัญญัติดังกล่าวเท่านั้น เพราะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อาจจะเป็นการกระทำต่อ “ข้อมูล” ที่ไม่ได้มีการสื่อความหมายในทำนองเดียวกันกับข้อความ เช่น ข้อมูลที่เป็นรหัสผ่าน หรือลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น แต่อย่างไรก็ตาม ถึงแม้ว่าข้อมูลจะมีลักษณะที่หลากหลาย แต่การสร้างหรือวัตถุประสงค์ในการใช้งานจะต้องเป็นไปในทิศทางเดียวกัน ผู้เขียนเห็นว่านี่เป็นอีกหนึ่งปัญหาที่พระราชบัญญัตินี้ต้องบัญญัติให้ข้อมูลคอมพิวเตอร์หมายความรวมไปถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์อีกด้วย

ดังนั้น การใช้อำนาจของพนักงานเจ้าหน้าที่ตามอนุมตรานี้คือการทำสำเนา กล่าวคือ การที่พนักงานเจ้าหน้าที่จะเข้าไปตรวจสอบข้อมูลในข้อมูลคอมพิวเตอร์ใดๆ ก็ตาม เช่น การเจาะระบบคอมพิวเตอร์เพื่อให้ทราบถึงระบบคอมพิวเตอร์ที่ใช้ เข้าถึงข้อมูลคอมพิวเตอร์หรือข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งในส่วนใหญ่แล้วต้องใช้วิธีการทางคอมพิวเตอร์เพื่อการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ และข้อมูลจราจรทางคอมพิวเตอร์ย่อมทำให้พนักงานเจ้าหน้าที่ได้พยานหลักฐานที่เกี่ยวกับการกระทำความผิดที่กระทำผ่านระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ นอกจากนั้น การเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ย่อมเป็นประโยชน์ในการสืบสวนหาตัวผู้กระทำความผิดว่าผู้ใดกระทำความผิด และเมื่อวันที่ เวลาใดจากสถานที่ใด เป็นต้น โดยสามารถทำได้เฉพาะเมื่อมีเหตุอันสมควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้เท่านั้น และในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นต้องไม่เกินความจำเป็น

4.2.2 อำนาจในการสั่งให้บุคคลส่งข้อมูลหรืออุปกรณ์

จากการศึกษา พบว่าพนักงานเจ้าหน้าที่สามารถสั่งให้บุคคลที่ครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ให้ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ได้ โดยบุคคลที่ครอบครองหรือควบคุมนั้นไม่ได้หมายถึงเฉพาะผู้กระทำความผิดเท่านั้น แต่ยังหมายความรวมไปถึงบุคคลใดๆ ที่ครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์หรืออุปกรณ์ด้วย

เช่น ในคดีของ อากง ที่ได้มีการส่งข้อความหมิ่นเดชานุภาพไปยังรองเลขานุการของอดีตนายกรัฐมนตรี นายอภิสิทธิ์ เวชชาชีวะ ซึ่งการส่งข้อความดังกล่าวนั้น เป็นการส่งข้อความแบบสั้น (SMS) ซึ่งจะทำงานโดยส่งข้อความไปยัง Shot Message Service Centre (SMSC) จากนั้นระบบจะทำการประมวลผล แล้วส่งไปยังเครือข่ายของเครื่องรับเข้าไปยังเครื่องโทรศัพท์เคลื่อนที่ดังกล่าว โดยเจ้าหน้าที่ได้ทำการตรวจสอบข้อมูลการใช้โทรศัพท์เคลื่อนที่ผ่านระบบจัดเก็บของคอมพิวเตอร์ ซึ่งการ

กระทำความผิดนี้เป็นการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ อันเป็นการดูหมิ่น หมิ่นประมาทต่อราชวงศ์ และการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร และผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 อีกด้วย

เพราะเหตุนี้ จึงต้องบัญญัติให้รวมไปถึง อุปกรณ์ที่ใช้เก็บเครื่องมือคอมพิวเตอร์อีกด้วย เช่น ศูนย์เก็บข้อมูล ซึ่งเป็นการเก็บไว้ภายนอกเครื่อง เพราะฉะนั้นจึงต้องกำหนดให้พนักงานเจ้าหน้าที่มีอำนาจสั่งให้ส่งอุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์นั้นได้ด้วย

4.2.3 อำนาจในการตรวจสอบหรือเข้าถึง

จากการศึกษา พบว่าเป็นสิ่งที่จะใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิดซึ่งบุคคลเหล่านั้นอาจจะเป็นพยานบุคคล พยานเอกสาร หรือพยานวัตถุ และในการที่จะนำเอาพยานบุคคลมาพิสูจน์ย่อมสามารถที่จะกระทำได้ด้วยการทำเป็นหนังสือเรียกหรือออกหมายเรียกบุคคลนั้นมา แต่สำหรับพยานเอกสารแล้วนั้นหรือจะเป็นพยานวัตถุถึงแม้จะมีวิธีการที่ให้ออกหมาย โดยการสั่งให้เจ้าของหรือผู้ครอบครองส่งเอกสารหรือวัตถุนั้นอาจจะไม่สามารถกระทำได้ เพราะผู้ที่มีเอกสารหรือวัตถุนั้นอาจจะปฏิเสธได้ และจะถือได้ว่าเป็นการขัดขืนหมายก็ไม่ได้ เพราะบุคคลนั้นอาจไม่มีพยานหลักฐานดังกล่าวจริงๆ ก็ได้ แต่อย่างไรก็ตาม แต่หากพนักงานเจ้าหน้าที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้และข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์นั้นมีอยู่จริง อาจจะขอให้ศาลทำการตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์นั้นมาได้ โดยพนักงานเจ้าหน้าที่มีอำนาจที่จะสั่งให้บุคคลผู้กระทำความผิดนั้นส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่มีความเกี่ยวข้องให้กับพนักงานเจ้าหน้าที่จึงถือว่ามีความเหมาะสมแล้ว

การใช้อำนาจตามอนุมาตรานี้ของพนักงานเจ้าหน้าที่ในการเจาะระบบคอมพิวเตอร์เหมือนกับอำนาจในการทำสำเนาข้อมูลก็ตาม แต่ต้องแยกอำนาจตามอนุมมาตรานี้ออกมาต่างหากจากกัน อำนาจตามอนุมาตรานี้เป็นการตรวจสอบหรือเข้าถึง และขยายไปถึงการเข้าถึงอุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์อีกด้วย

อำนาจของพนักงานเจ้าหน้าที่ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ และอุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์นี้ เพราะฉะนั้น พนักงานเจ้าหน้าที่จึงได้พยานหลักฐานเกี่ยวกับการกระทำความผิดที่กระทำผ่านระบบคอมพิวเตอร์และเป็นประโยชน์ในการที่จะทำการสืบสวนหาตัวผู้กระทำความผิดว่าผู้ใดเป็นผู้กระทำความผิดและการกระทำความผิดนั้นเกิดขึ้นเมื่อใดอย่างเช่นในคดีอากงเป็นต้น

4.2.4 อำนาจในการถอดรหัสลับ

จากการศึกษา พบว่าการใช้อำนาจในการตรวจสอบหรือเข้าถึงตามอนุมาตราก่อนนี้ พนักงานเจ้าหน้าที่พบปัญหาซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลคอมพิวเตอร์ได้เนื่องจากมีรหัสลับป้องกันการเข้าถึงข้อมูลนั้น อนุมาตรานี้จึงให้อำนาจพนักงานเจ้าหน้าที่ในการดำเนินการถอดรหัสลับ หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ เช่นผู้ดูแลระบบ (Admin) หรือเจ้าของ

เครื่องคอมพิวเตอร์ เป็นต้น ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว[88] ซึ่งหากไม่มีการบัญญัติเป็นการเฉพาะให้มีอำนาจในการถอดรหัสในกฎหมายให้ชัดเจน การกระทำของพนักงานเจ้าหน้าที่ดังกล่าวอาจถือได้ว่าเป็นการล่วงละเมิดข้อมูลส่วนบุคคลได้

เพราะฉะนั้น โดยปกติแล้วข้อมูลคอมพิวเตอร์ที่สำคัญ เช่น สถาบันการเงิน การซื้อขายหลักทรัพย์ หรือข้อมูลเกี่ยวกับความมั่นคงและความลับของประเทศจะต้องมีระบบป้องกันการเข้าถึงข้อมูลคอมพิวเตอร์เหล่านี้ด้วยรหัสลับ เพราะถ้าผู้ใดล่วงรู้หรือเข้าถึงข้อมูลดังกล่าวได้อาจทำความเสียหายให้แก่เจ้าของข้อมูลหรือความปลอดภัยสาธารณะเป็นอย่างมาก

4.2.5 อำนาจในการยึดหรืออายัดระบบคอมพิวเตอร์

จากการศึกษาระบบคอมพิวเตอร์ คือ“อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ที่ได้มีการพัฒนาขึ้นเพื่อประมวลผลข้อมูลดิจิทัล (Digital Data) อันประกอบด้วยเครื่องคอมพิวเตอร์ และอุปกรณ์รอบข้าง (Peripheral) ต่างๆ ในการรับเข้าหรือป้อนข้อมูล (Input) หรือแสดงผลข้อมูล (Output) และบันทึกหรือเก็บข้อมูล (Store and Record) ดังนั้น ระบบคอมพิวเตอร์จึงอาจเป็นเพียงอุปกรณ์เพียงเครื่องเดียวหรือหลายเครื่องที่มีลักษณะเชื่อมต่อถึงกันได้ ดังนั้น อาจจะมีการเชื่อมต่อกันผ่านระบบเครือข่ายและมีลักษณะการทำงานโดยอัตโนมัติตามโปรแกรมที่ได้วางไว้และไม่มีการแทรกแซงการทำงานจากมนุษย์ ในส่วนที่เป็นโปรแกรมคอมพิวเตอร์จะหมายถึงชุดคำสั่งที่ทำหน้าที่สั่งการให้คอมพิวเตอร์ทำงาน

ตามอนุมาตรานี้ พนักงานเจ้าหน้าที่มีอำนาจในการยึดหรืออายัด โดยการยึดระบบคอมพิวเตอร์นั้น หมายถึง การนำระบบคอมพิวเตอร์มาอยู่ในความครอบครองของพนักงานเจ้าหน้าที่ ในส่วนของการอายัดระบบคอมพิวเตอร์นั้น หมายถึง การที่พนักงานเจ้าหน้าที่สั่งระงับการใช้ระบบคอมพิวเตอร์นั้นและให้ระบบคอมพิวเตอร์นั้นมาอยู่ในความควบคุมของพนักงานเจ้าหน้าที่ต่อไป

ผู้เขียนเห็นว่าถ้าหากว่าพนักงานเจ้าหน้าที่จะใช้อำนาจตามที่ได้บัญญัติไว้ในอนุมาตราก่อนๆ นั้น เช่น การเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ อุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ หรือการถอดรหัสลับ ในบางครั้งอาจจะยังไม่ได้ข้อมูล เช่น ไม่อาจที่จะถอดรหัสได้ ดังนั้น อนุมาตรานี้จึงให้อำนาจกับพนักงานเจ้าหน้าที่ในการยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในรายละเอียดแห่งการกระทำความผิดนั้นและผู้กระทำความผิด เช่น ในคดี ผอ.ประชาไท ที่ไม่ให้ความร่วมมือกับเจ้าหน้าที่โดยการไม่ส่งข้อมูล IP Address ของผู้ใช้บริการเว็บบอร์ดอื่นๆ ที่มีข้อความเข้าข่ายหมิ่นสถาบันให้แก่เจ้าหน้าที่เพื่อทำการสืบสวนสอบสวนหาตัวผู้กระทำความผิดมาลงโทษ เป็นต้น

นอกจากนี้ การยึดหรืออายัดตามพระราชบัญญัตินี้ นอกจากพนักงานเจ้าหน้าที่จะต้องทำการส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดให้เป็นไปตามกำหนดในกระทรวงมอบให้เจ้าของหรือผู้ที่ทำการครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นพยานหลักฐานแล้ว การจะสั่งยึดหรืออายัดดังกล่าว

---

[88] *เรื่องเดียวกัน,* หน้า 47.

นี้จะเกิน 30 วันไม่ได้ ในกรณีที่มีเหตุจำเป็นที่จะต้องทำการยึดหรืออายัดไว้เป็นเวลานานกว่า 30 วัน ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัด ถ้าหากศาลได้อนุญาตให้ขยายเวลาได้ครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกิน 60 วัน และเมื่อหมดความจำเป็นที่จะทำการยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้วนั้น พนักงานเจ้าหน้าที่จะต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือทำการถอนการอายัดนั้นโดยฉับพลัน ในกรณีที่เป็นหนังสือที่แสดงการยัดหรืออายัดให้เป็นไปตามที่กำหนดในกฎกระทรวง

4.2.6 อำนาจในการระงับการทำให้แพร่หลาย

การระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามมาตรา 20 แห่งพระราชบัญญัตินี้ คือ การบล็อกไม่ให้ระบบคอมพิวเตอร์เผยแพร่ข้อมูลคอมพิวเตอร์ที่เป็นความผิดดังกล่าวในระบบคอมพิวเตอร์อีกต่อไป โดยการที่ศาลจะอนุญาตให้พนักงานเจ้าหน้าที่ใช้อำนาจตามมาตรานี้ได้ต้องเป็นเรื่องที่พนักงานเจ้าหน้าที่ดำเนินการโดยได้รับความเห็นชอบจากรัฐมนตรีก่อนแล้วจึงยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจเพื่อขอให้ศาลมีคำสั่งระงับการทำให้เผยแพร่ซึ่งข้อมูลคอมพิวเตอร์นั้น

ในปัจจุบันนี้การกระทำใดๆ ในลักษณะที่เป็นการเข้าข่ายเป็นความผิดตามพระราชบัญญัติที่อาจจะไปกระทบกระเทือนถึงความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และกระทบต่อความรู้สึกร่วมของคนในสังคมเป็นอย่างมาก และในการจัดการกับปัญหานี้ ต้องกระทำด้วยความรวดเร็ว หากการปิดกั้นเว็ปไซร์นั้นอาจจะส่งผลกระทบต่อการประกอบการของผู้ให้บริการด้วยเช่นกันและอาจจะมีการฟ้องกลับหรือเรียกร้องค่าเสียหายจากพนักงานเจ้าหน้าที่ได้เช่นกัน

ดังนั้น การใช้อำนาจตามมาตรานี้จึงไม่ได้อยู่ในดุลพินิจของพนักงานเจ้าหน้าที่เท่านั้น แต่จะต้องได้รับความเห็นชอบจากรัฐมนตรีเสียก่อน เนื่องจากการบล็อคระบบคอมพิวเตอร์อาจจะไปกระทบถึงสิทธิเสรีภาพของบุคคลในการสื่อสารข้อมูล เมื่อศาลมีคำสั่งให้ระงับการทำให้เผยแพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามคำร้องขอของพนักงานเจ้าหน้าที่แล้วนั้น พระราชบัญญัตินี้ได้กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจทำการระงับการทำให้เผยแพร่หลายนั้นเอง หรือพนักงานเจ้าหน้าที่ที่จะสั่งให้ผู้บริการระงับการให้บริการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ก็ได้ หากผู้ใดไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่จะต้องระวางโทษตามมาตรา 27

ในส่วนลักษณะของข้อมูลคอมพิวเตอร์ที่ศาลจะสั่งให้ระงับการเผยแพร่นั้นจะต้องเป็นข้อมูลคอมพิวเตอร์ที่มีองค์ประกอบของความผิดตามพระราชบัญญัตินี้ เช่น ความผิดตามมาตรา 14 และ มาตรา 15 และยังต้องเป็นข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่บัญญัติไว้ในภาค 2 ลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะเป็นการขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน เป็นต้น

4.2.7 อำนาจในการห้ามจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์

มาตรา 21 แห่งพระราชบัญญัตินี้เป็นบทบัญญัติที่กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจที่จะยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้ศาลมีคำสั่งห้ามจำหน่ายหรือเผยแพร่ข้อมูลคอมพิวเตอร์

ที่มีชุดคำสั่งไม่พึงประสงค์ เพราะจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มีโอกาสเกิดขึ้นได้บ่อยและง่ายขึ้น กล่าวคือ การใช้ชุดคำสั่งไม่พึงประสงค์ (Malicious Code) ที่อาจจะเป็นชุดคำสั่งหรือโปรแกรมที่เป็นการทำลายทั้งหลาย เพื่อกระทำความผิดตามพระราชบัญญัติในรูปแบบต่างๆ

ศาลที่มีเขตอำนาจตามมาตรานี้ หมายถึง ศาลที่มีอำนาจพิจารณาคดีอาญาที่เจ้าของหรือผู้ที่ครอบครองข้อมูลคอมพิวเตอร์อยู่ในเขตอำนาจ

ในชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมให้เกิดความขัดข้อง หรือปฏิบัติงานไม่ตรงกับคำสั่งที่ได้ตั้งไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่ว่า ชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวนั้นตามที่รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารประกาศในราชกิจจานุเบกษา

นอกจากจะสั่งห้ามจำหน่ายหรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์แล้วนั้น พนักงานเจ้าหน้าที่อาจสั่งให้เจ้าของหรือผู้ที่ครอบครองข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วยนั้น ระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์ได้ หรือจะกำหนดเงื่อนไขในการใช้มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์นั้นก็สามารถกระทำได้

ดังนั้น จะเห็นได้ว่าการให้อำนาจนั้นเป็นการให้อำนาจในการควบคุมและตรวจสอบการใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่โดยศาล และ กฎหมายได้จำกัดขอบเขตการใช้อำนาจตามมาตรานี้ไว้ว่าจะใช้ได้ก็ต่อเมื่อเป็นกรณีที่มีเหตุอันสมควรอันเชื่อได้ว่าได้มีการกระทำความผิดตามพระราชบัญญัตินี้เกิดขึ้นและในคำร้องนั้นจะต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างใดอย่างหนึ่งซึ่งเป็นความผิดตามพระราชบัญญัตินี้

การใช้อำนาจของพนักงานเจ้าหน้าที่ในการดำเนินการตามคำสั่งของศาล จะต้องมีการเข้าไปในเคหสถานหรือสถานประกอบการ หากเป็นกรณีที่พนักงานเจ้าหน้าที่จะต้องเข้าไปในสถานที่พนักงานเจ้าหน้าที่จะต้องให้ผู้ที่ยื่นคำร้องระบุมาในคำร้องให้ชัดเจนว่าประสงค์จะให้พนักงานเจ้าหน้าที่เข้าไปในเคหสถานนั้นหรือสถานประกอบการเพื่อดำเนินการใด โดยที่ศาลนั้นจะมีคำสั่งอนุญาตให้เข้าไปและดำเนินการตามคำร้องได้โดยไม่จำเป็นที่จะต้องให้ผู้ร้องยื่นคำร้องขอหมายค้นในสถานที่ดังกล่าวและในการที่จะสั่งคำร้องของพนักงานเจ้าหน้าที่ กฎหมายก็ได้กำหนดให้ศาลพิจารณาคำร้องดังกล่าวโดยเร่งด่วน ซึ่งศาลอาจจะออกคำสั่งอนุญาตหรือไม่อนุญาตก็ได้โดยพิจารณาจากคำร้องได้เลย แต่ถ้าศาลเห็นสมควรจะสั่งให้มีการไต่สวนคำร้องก่อนมีคำสั่งก็สามารถกระทำได้เพราะเป็นอำนาจของศาลที่ได้บัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา

ศาลที่มีเขตอำนาจให้พิจารณาตามพระธรรมนูญศาลยุติธรรมและกฎหมายว่าด้วยการจัดตั้งศาลและด้วยว่าการยื่นคำร้องในคดีซึ่งเป็นความผิดเกี่ยวกับคอมพิวเตอร์ตามพระราชบัญญัตินี้ซึ่งถือว่าเป็นคดีอาญา จะต้องยื่นคำร้องต่อศาลชั้นต้นที่มีอำนาจพิจารณาพิพากษาคดีอาญาและมีเขตอำนาจในคดีที่บุคคลใดกระทำหรือกำลังจะกระทำความผิด

และเมื่อศาลมีคำสั่งอนุญาตแล้วก่อนที่จะดำเนินการตามคำสั่งศาล พนักงานเจ้าหน้าที่จะต้องส่งสำเนาบันทึกเหตุอันควรเชื่อที่จะต้องมีการใช้อำนาจตามอนุมาตรา 4-8 เพื่อที่จะได้ทำการมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นเพื่อเก็บไว้เป็นหลักฐาน ถ้าหากไม่มีเจ้าของหรือผู้ครอบครองให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่จะกระทำได้

ดังนั้น ผู้เขียนเห็นว่าตามมาตรา 19 แห่งพระราชบัญญัติที่ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในลักษณะเช่นนี้ เป็นการจำกัดขอบเขตการใช้อำนาจของพนักงานเจ้าหน้าที่ให้อยู่ในอำนาจของศาลที่จะทำการควบคุมและตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่มากจนเกินไปหากพนักงานเจ้าหน้าที่มีเหตุอันควรเชื่อได้ว่าได้มีการกระทำความผิดเกิดขึ้นตามพระราชบัญญัตินี้พนักงานเจ้าหน้าที่จะต้องทำคำร้องยื่นต่อศาลเพื่อขออนุญาตต่อศาลให้ศาลออกหมายให้

เพราะฉะนั้น ผู้เขียนเห็นว่าอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในกรณีนี้น่าจะหมายความรวมไปถึงการที่ให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้มีอำนาจในการค้นและยึดข้อมูลคอมพิวเตอร์ในคดีความผิดอันเกี่ยวกับคอมพิวเตอร์เพื่อทำการรวบรวมไว้เป็นพยานหลักฐาน เพราะพนักงานเจ้าที่ตามพระราชบัญญัตินี้เป็นผู้ที่มีความรู้และความเชี่ยวชาญเกี่ยวกับระบบคอมพิวเตอร์โดยเฉพาะ อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ที่สามารถกระทำได้แต่การกระทำนั้นต้องขออนุญาตจากศาลเสียก่อน

แต่อย่างไรก็ตาม การขอหมายจากศาลจะต้องใช้เวลา และในช่วงระยะเวลาที่ไปขอหมายจากศาล อาจจะมีการแก้ไขเปลี่ยนแปลง หรือ ทำลายพยานหลักฐานข้อมูลคอมพิวเตอร์นั้นแล้ว และจากการที่ได้ทำการศึกษา จะเห็นได้ว่าหมายของศาลในความผิดอันเกี่ยวกับคอมพิวเตอร์นี้ จะมีได้เพียงครั้งเดียวเท่านั้น และ หากศาลจะออกหมาย ศาลอาจจะไม่เข้าใจในลักษณะคดีที่เป็นความผิดอันเกี่ยวกับคอมพิวเตอร์ว่าความผิดนั้นมีความละเอียดอ่อนและจำเป็นต้องเป็นกรณีเร่งด่วนในการที่จะออกหมายนั้นด้วย และเมื่อศาลไม่มีความเข้าในความผิดดังกล่าว อาจจะทำให้ศาลไม่เห็นความสำคัญในการที่จะต้องออกหมายในกรณีนี้ด้วย

ด้วยสภาพแห่งพยานหลักฐานทางคอมพิวเตอร์ไม่สามารถบอกได้อย่างแน่นอนว่าอยู่ ณ ที่ใด การดำเนินการตามคำสั่งศาลอาจจะก่อให้เกิดปัญหาในทางปฏิบัติกับพนักงานเจ้าหน้าที่ได้ เมื่อพนักงานเจ้าหน้าที่ทำการตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์แล้ว ได้พบเจอผู้กระทำความผิดได้ส่งข้อมูลคอมพิวเตอร์ ที่สามารถใช้เป็นหลักฐานได้ไปยังระบบคอมพิวเตอร์อื่น พนักงานเจ้าหน้าที่ไม่สามารถทำการตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์นั้นได้เลย ถ้าหากพนักงานเจ้าหน้าที่จะทำการตรวจสอบหรือเข้าถึงข้อมูลคอมพิวเตอร์พนักงานเจ้าหน้าที่อาจจะมีความผิดตามพระราชบัญญัตินี้ได้

แนวทางกฎหมายในต่างประเทศซึ่งบัญญัติขึ้นมาเพื่อแก้ไขปัญหาดังกล่าว สามารถศึกษาได้จาก The Electronic Communications Privacy Act (ECPA) โดยได้กำหนดไว้ว่า เจ้าหน้าที่จะทำการค้นยึดโดยไม่มีเหตุอันควรไม่ได้ และจะออกหมายโดยไม่มีเหตุอันสมควรก็ไม่สามารถที่จะกระทำได้ โดยหลักแล้วการจะยึดค้นข้อมูลคอมพิวเตอร์ จะต้องกระทำโดยมีหมายค้น (Search Warrant) หากกระทำการค้นโดยไม่มีหมายอาจจะเป็นการกระทำที่ขัดต่อหลักกฎหมาย แต่อย่างไรก็ตาม การยึดและค้นข้อมูลคอมพิวเตอร์สามารถกระทำได้โดยไม่มีหมาย แต่อาจจะกระทำได้เพียงบางประการเท่านั้น

อย่างไรก็ตาม ผู้เขียนเห็นว่าหากจะมีการแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยบัญญัติเรื่องการใช้อำนาจของพนักงานเจ้าหน้าที่ไว้ทำนองเดียวกับ ECPA ตัวอย่างเช่น กำหนดให้พนักงานเจ้าหน้าที่สามารถตรวจสอบหรือเข้าถึงข้อมูลคอมพิวเตอร์ของบุคคลได้โดยไม่ต้องขอหมายจากศาล หากเป็นกรณีที่มีเหตุจำเป็นเร่งด่วน

จะเห็นได้ว่า การบัญญัติให้อำนาจแก่พนักงานเจ้าหน้าที่สามารถตรวจสอบหรือเข้าถึงข้อมูลคอมพิวเตอร์ได้โดยไม่ต้องขอหมายจากศาลก่อน

ปัญหานี้อาจจะมีการแก้ไขไว้ในขั้นตอนการค้นและยึดข้อมูลคอมพิวเตอร์โดยไม่ต้องขอหมายตามมาตรา 18 (4) (5) (6) (7) และ (8) โดยให้พนักงานเจ้าหน้าที่ที่ทำการตรวจสอบหรือเข้าถึงข้อมูลคอมพิวเตอร์ระบุรายละเอียดเกี่ยวกับระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือ อุปกรณ์ที่ใช้ในการกระทำความผิดอื่นๆ ไว้ นอกจากนั้น การตรวจสอบหรือการเข้าถึงในกรณีจำเป็นเร่งและด่วน (Exigent Circumstances) จะต้องเข้าเงื่อนไขดังต่อไปนี้ด้วย

1. หลักฐานอยู่ในที่เป็นอันตรายง่ายต่อการทำลาย The Degree of Urgency Involved
2. เป็นภัยคุกคามที่ทำให้ทั้งตำรวจหรือประชาชนตกอยู่ในอันตราย
3. เป็นกรณีที่เจ้าหน้าที่ตำรวจพบพิรุธ หรือ
4. ผู้ต้องสงสัยมีโอกาสที่จะหนีไปก่อนที่เจ้าหน้าที่จะขอหมายค้นได้

จะเห็นได้ว่า ถ้าไม่เข้าเงื่อนไขดังกล่าวข้างต้นพนักงานเจ้าหน้าที่ไม่มีอำนาจที่จะกระทำการตรวจสอบหรือเข้าถึงข้อมูลคอมพิวเตอร์ได้ เพราะหากเจ้าหน้าที่กระทำเช่นนั้นอาจจะไปกระทบถึงสิทธิเสรีภาพของประชาชนได้ ฉะนั้นเมื่อมีการกระทำความผิดเกิดขึ้นตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 แล้วความผิดนั้นจะต้องขอหมายจากศาล ซึ่งเมื่อจะทำการขอหมายจากศาลอาจจะก่อให้เกิดความเสียหาย ข้อมูลสูญหาย หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ การใช้อำนาจของพนักงานเจ้าหน้าที่ควรให้เป็นไปตามมาตรา 18 (1) (2) (3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กล่าวคือ สามารถตรวจสอบหรือเข้าถึงข้อมูลคอมพิวเตอร์ได้เลยโดยไม่ต้องขอหมายจากศาล

อย่างไรก็ตามควรพิจารณาเปรียบเทียบกับคำพิพากษาของประเทศอเมริกาด้วยว่ากรณีใดบ้างให้ถือเป็นกรณีจำเป็นและเร่งด่วน เช่น

1. หลักฐานที่เป็นเรื่องสำคัญจะถูกลบออกหรือถูกทำลายไปเสียก่อน (Whether the Evidence is about to be Removed or Destroyed)
2. ความเป็นไปได้ที่จะเกิดอันตรายในขณะนั้น (The Possibility of Danger at the Site)
3. ความเร่งด่วนในการทำลายสินค้าต้องห้าม (The Ready Destructibility of the Contraband)

ดังนั้น ผู้เขียนจึงเห็นว่าเมื่อพนักงานเจ้าหน้าที่ที่จะใช้อำนาจได้โดยไม่ต้องมีหมายไม่ใช่เจ้าพนักงานทั่วไปแต่เป็นพนักงานเจ้าหน้าที่ที่ได้มีการแต่งตั้งเป็นกรณีพิเศษโดยได้มีการกลั่นกรองคุณสมบัติและระดับตำแหน่งของผู้ที่ได้รับการแต่งตั้งแล้ว หากพนักงานเจ้าหน้าที่จะใช้อำนาจตามอนุมาตราที่ได้กล่าวมาแล้ว โดยไม่ต้องขออนุญาตจากศาลก่อน หรือจะบัญญัติเป็นข้อยกเว้นไว้สำหรับการใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 19 ที่ว่าด้วยการค้นไม่ต้องขอหมายจากศาลก็ย่อมที่จะกระทำได้

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

เมื่อในปัจจุบันคอมพิวเตอร์ได้เข้ามามีบทบาทและหน้าที่ในสังคมมากขึ้น คนในสังคมคงจะปฏิเสธบทบาทของคอมพิวเตอร์ที่มีเพิ่มมากขึ้นในชีวิตประจำวันไม่ได้ คอมพิวเตอร์ทำให้พฤติกรรมของบุคคลเกิดการเปลี่ยนแปลงไปทั้งในแง่ของการใช้ชีวิตในการทำงาน การผักผ่อน การเรียนรู้ หรือการติดต่อสื่อสาร จึงไม่แปลกใจที่คอมพิวเตอร์ได้เข้ามาแทนที่ เครื่องพิมพ์ดีด โทรสาร โทรศัพท์ เป็นต้น ดังนั้นคอมพิวเตอร์จึงได้กลายมาเป็นเครื่องมือที่ใช้ในการกระทำความผิดด้วยเช่นกัน คือการประกอบอาชญากรรมทางคอมพิวเตอร์ที่ไม่มีการกระทำทางกายภาพซึ่งเป็นการกระทำความผิดที่เกิดขึ้นเพียงอย่างเดียวที่จะนำมาเป็นพยานหลักฐานได้

นอกจากนี้คอมพิวเตอร์ยังก่อให้เกิดการกระทำความผิดในรูปแบบต่างๆ ขึ้นอีกมากมาย การกระทำความผิดที่เป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้นเป็นความผิดที่เกิดขึ้นในรูปแบบการกระทำความผิดต่างๆ ที่แตกต่างกันออกไป ทั้งในด้านของการกระทำความผิดและในด้านของการสืบสวนและสอบสวน และยังรวมไปถึงการรวบรวมพยานหลักฐานในการที่จะออกหมายดำเนินคดีกับผู้ที่กระทำความผิดดังกล่าวอีกด้วย

ในการแสวงหาพยานหลักฐานในคดีอาญาเพื่อจะพิสูจน์ให้ได้ว่าจำเลยเป็นผู้กระทำความผิดหรือไม่ ในด้านของการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ที่เป็นการกระทำความผิดที่เกิดขึ้นจากการพัฒนาเทคโนโลยีในด้านคอมพิวเตอร์ในยุคดิจิตอลหรือยุคไอทีในปัจจุบันนี้ ซึ่งเป็นการกระทำทางกายภาพไม่มีรูปร่าง ไม่ว่าจะเป็นในด้านการกระทำความต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ จึงเป็นข้อแตกต่างจากการกระทำความผิดในทางอาญาซึ่งการกระทำความผิดในทางอาญาเป็นการกระทำที่มีรูปร่าง

เพราะฉะนั้น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จึงได้กำหนดให้พนักงานเจ้าหน้าที่ซึ่งเป็นบุคคลผู้ที่มีความรู้ความเชี่ยวชาญในด้านระบบคอมพิวเตอร์เข้ามามีอำนาจในการสืบสวนและสอบสวนในพระราชบัญญัตินี้ เช่น การทำสำเนาข้อมูลคอมพิวเตอร์และข้อมูลจราจรคอมพิวเตอร์ การถอดรหัสลับ การยึดหรืออายัดระบบคอมพิวเตอร์ ซึ่งพยานหลักฐานทางคอมพิวเตอร์ในปัจจุบันได้มีการกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ไว้เพื่อรับรองการใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ กล่าวคือ พนักงานเจ้าหน้าที่เป็นผู้ที่ทำการรวบรวมพยานหลักฐานเกี่ยวกับคอมพิวเตอร์ไว้โดยเฉพาะ เมื่อพนักงานเจ้าหน้าที่ทำการรวบรวมพยานหลักฐานจนครบแล้วพนักงานเจ้าหน้าที่ก็ทำการส่งพยานหลักฐานดังกล่าวให้แก่เจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญาเพื่อดำเนินการต่อไป เพราะพระราชบัญญัติว่า

ด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ไม่ได้ให้อำนาจแก่เจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญาไว้

การค้นหรือการยึดพยานหลักฐานที่เป็นพยานหลักฐานทางอิเล็กทรอนิกส์มีความสำคัญอย่างมากต่อการพิสูจน์ถึงความผิดของจำเลยและเป็นหลักฐานที่มีลักษณะพิเศษ เมื่อผู้เขียนได้ทำการศึกษาพบว่ามีขั้นตอนหลายประการทำให้การค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์ล่าช้า เนื่องจากได้มีการให้ความคุ้มครองในเรื่องของสิทธิส่วนบุคคลจึงมีมาตราการในการตรวจสอบการใช้ดุลพินิจของเจ้าพนักงานโดยองค์กรของศาล

อำนาจในการที่จะออกหมายค้นนั้นได้กำหนดให้ศาลแต่เพียงผู้เดียวเท่านั้นที่จะมีอำนาจในการออกหมายค้น และให้รวมไปถึงการค้นข้อมูลอิเล็กทรอนิกส์ที่ได้มีการใช้อุปกรณ์เชื่อมต่อกับคอมพิวเตอร์เพื่อเข้าไปค้นหาฐานข้อมูลในเครื่องคอมพิวเตอร์ของผู้ต้องสงสัยโดยไม่มีการรุกล้ำเข้าไปในที่รโหฐานด้วย และในการจะทำการค้นในกรณีดังกล่าวนั้นจะต้องใช้หมายค้นเช่นเดียวกับความผิดในทางอาญาอื่นๆ ด้วย ดังนั้นกระบวนการที่ศาลจะออกหมายค้นจึงเป็นขั้นตอนที่ทำให้เกิดความล่าช้าทำให้พนักงานไม่มีอำนาจที่จะปฏิบัติตามหน้าที่ได้

ดังนั้น การที่มีบทบัญญัติให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญาในมาตรา 29 จึงเป็นเพียงการกำหนดให้พนักงานเจ้าหน้าที่สามารถปฏิบัติหน้าที่ร่วมกันกับพนักงานสอบสวนในการตรวจสอบพยานหลักฐานในคดีได้เท่านั้น

แต่อย่างไรก็ตามความผิดอาญาอื่นๆ ที่ไม่ได้บัญญัติไว้ในพระราชบัญญัตินี้ ถึงแม้จะมีความเกี่ยวข้องกับระบบคอมพิวเตอร์ แต่พนักงานเจ้าหน้าที่ก็ไม่มีอำนาจที่จะเข้าไปใช้อำนาจในการสืบสวนและสอบสวนตามพระราชบัญญัติว่าด้วยการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ได้ เช่น การละเมิดลิขสิทธิ์ การพนัน การกระทำความผิดที่เกี่ยวกับยาเสพติด เป็นต้น

กฎหมายของต่างประเทศก็ได้มีบทบัญญัติในเรื่องที่เกี่ยวกับอำนาจหน้าที่ของเจ้าพนักงานในการแสวงหาพยานหลักฐานทางด้านคอมพิวเตอร์ไว้ ซึ่งนำมาพิจารณาประกอบกับพระราชบัญญัตินี้ว่าจะมีการแก้ไขเพิ่มเติมหรือไม่ เช่น

กฎหมาย The Omnibus Crime Control and Safe Streets Act ปี 1968 ของประเทศสหรัฐอเมริกานั้นได้ให้ความสำคัญกับหลักการจำกัดเสรีภาพของบุคคลเป็นเรื่องที่สำคัญ โดยจะเน้นไปในเรื่องของการจับ ซึ่งจะมีปัญหาขัดแย้งกันระหว่างการให้ความคุ้มครองเสรีภาพในร่างกายของบุคคลและการใช้อำนาจของเจ้าพนักงานของรัฐในการจับ เพื่อให้เห็นถึงการแก้ปัญหาความขัดแย้งดังกล่าวข้างต้น ประเทศสหรัฐอเมริกาจึงได้กำหนดหลักเกณฑ์ในการที่จะให้เจ้าพนักงานของรัฐสามารถที่จะใช้อำนาจจับ ไว้ในบทบัญญัติแห่งรัฐธรรมนูญของสหรัฐอเมริกาไว้ว่า การจะจับนั้นจะต้องจับโดยอาศัยหมายจับ (Arrest Warrant) โดยศาลเป็นผู้ออกหมายให้โดยอาศัยเหตุอันสมควร (Probable Cause)

การที่พนักงานเจ้าหน้าที่ของรัฐใช้อำนาจในการจับโดยไม่มีหมายจับให้ถือได้ว่าเป็นข้อยกเว้นที่ใช้เฉพาะกรณีที่มีเหตุฉุกเฉิน หรือมีความจำเป็นอย่างยิ่ง ถึงแม้จะไม่ใช่ความผิดที่ได้กระทำซึ่งหน้าต่อพนักงานเจ้าหน้าที่ของรัฐ พนักงานเจ้าหน้าที่ของรัฐอาจจับได้ก่อนที่จะได้ขอออกหมายจับจากศาล แต่เมื่อจับแล้วจะต้องนำมามอบให้กับพนักงานอัยการพร้อมทั้งชี้แจงรายละเอียดต่างๆ ให้กับพนักงานอัยการทราบเพื่อที่จะขอให้พนักงานอัยการออกหมายจับย้อนหลังต่อไป (Post Arrest Warrant)

หรือจะเป็นกรณีที่กฎหมาย ECPA ของประเทศสหรัฐอเมริกาที่ได้กำหนดขอบเขตในการแสวงหาพยานหลักฐานในการที่จะให้เจ้าพนักงานมีอำนาจในการค้นและยึดได้โดยไม่ต้องมีหมาย ซึ่งหลักในการยึดและค้นข้อมูลคอมพิวเตอร์ จะต้องกระทำโดยมีหมายค้น (Search Warrent) เท่านั้น แต่อย่างไรก็ตามการยึดและค้นข้อมูลคอมพิวเตอร์โดยไม่มีหมายอาจจะทำได้เพียงบางกรณีเท่านั้น ซึ่งข้อยกเว้นของการยึดและค้นข้อมูลคอมพิวเตอร์โดยไม่ต้องมีหมาย มีอยู่ด้วยกัน 3 ประการ คือ

1. กรณีที่ได้รับความยินยอม (Consent)
2. กรณีที่เป็นการอันจำเป็นและเร่งด่วน (Exigent Circumstances) และ
3. กรณีที่การยึดค้นข้อมูลคอมพิวเตอร์นั้นได้มาจากการจับกุมโดยชอบ (Search Incident to a Lawful Arrest)

กฎหมาย Computer Misuse and Cyber Security Act (Chapter 50A) ของประเทศสิงคโปร์ ที่ได้กำหนดให้รัฐมนตรีสามารถที่จะมอบอำนาจให้กับบุคคลใดๆ หรือองค์กรที่ระบุไว้ในหมาย โดยการใช้มาตรการเท่าที่จำเป็นในการที่จะป้องกันหรือต่อต้านคอมพิวเตอร์ หรือ บริการคอมพิวเตอร์ หรือประเภทคอมพิวเตอร์ หรือบริการคอมพิวเตอร์ใดๆ เพื่อให้เป็นไปตามวัตถุประสงค์ในการป้องกันหรือต่อต้านภัยคุกคามต่อความมั่นคงของชาติ บริการที่สำคัญ การป้องกันประเทศหรือความสัมพันธ์กับต่างประเทศของประเทศสิงคโปร์

และในขณะเดียวกันประเทศสิงคโปร์ก็ได้มีการบัญญัติเรื่องการจับกุมไว้ว่าให้เจ้าหน้าที่ตำรวจ (Police Officer) สามารถทำการจับกุมบุคคลใดๆ ได้โดยไม่มีหมายจับ หากมีเหตุอันเป็นการสงสัยว่ามีเหตุในการกระทำความผิดตามพระราชบัญญัตินี้

อย่างไรก็ตาม เมื่อได้ทำการศึกษากฎหมายต่างประเทศดั่งที่ได้กล่าวมาแล้วนั้น ผู้เขียนเห็นว่าควรที่จะนำมาตราการดังกล่าวมาแก้ไขเพิ่มเติมไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในกรณีที่มีความจำเป็นเร่งด่วนในเรื่องการใช้อำนาจโดยไม่ต้องมีหมายจากศาลเพราะผู้ที่จะทำการค้นได้จะต้องเป็นพนักงานฝ่ายปกครองหรือตำรวจเท่านั้น ดั่งที่ปรากฏไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92 และถ้าหากว่าเป็นการค้นโดยมีหมายตามมาตรา 97 ที่ได้ได้บัญญัติไว้ว่า ในกรณีที่ค้นโดยมีหมาย เจ้าพนักงานผู้มีชื่อในหมายค้นหรือผู้รักษาการแทนซึ่งต้องเป็นพนักงานฝ่ายปกครองตั้งแต่ระดับสามหรือตำรวจซึ่งมียศตั้งแต่ชั้นร้อยตำรวจตรีขึ้นไปเท่า นั้นมีอำนาจเป็นหัวหน้าไปจัดการให้เป็นไปตามหมายนั้น กล่าวคือ เจ้าพนักงานที่มีรายชื่ออยู่ในหมายค้นเท่า หรือผู้รักษาการแทนเท่านั้นที่จะมีอำนาจเป็นหัวหน้าไปจัดการตามหมายค้น ทั้งนี้ยังแสดงให้เห็นหมายค้นจะต้องระบุตัวเจ้าพนักงานว่าผู้ใดจะเป็นผู้ทำการค้น ดังนั้นเจ้าพนักงานอื่นๆ อาจค้นได้ในฐานะเป็นผู้ช่วยในการค้นเท่านั้นเอง

5.2 ข้อเสนอแนะ

ถึงแม้ว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จะได้มีการกำหนดหลักเกณฑ์การใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เพื่อให้ทันต่อการพัฒนาของระบบคอมพิวเตอร์ก็ตาม แต่ก็ยังคงมีปัญหาในบางประการที่ควรจะต้องนำมาพิจารณาแก้ไขเพิ่มเติมหรือปรับปรุงเพื่อให้พระราชบัญญัติดังกล่าวมีความสมบูรณ์

มากยิ่งขึ้น และสามารถนำไปใช้ป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ให้เป็นไปอย่างมีประสิทธิภาพยิ่งขึ้น เพราะในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นการกระทำความผิดในรูปแบบที่มีการพัฒนาไปตามแต่ละยุคสมัยและการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์นั้นได้เข้ามาเกี่ยวข้องกับมนุษย์เพิ่มมากขึ้นทุกวัน และในอนาคตอาจจะต้องมีการพัฒนากฎหมายเพื่อให้ทันต่อการปราบปรามผู้กระทำความผิดนี้ จึงเป็นเรื่องที่ต้องวิเคราะห์ต่อไปถึงปัญหาของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และเพื่อศึกษาหาแนวทางในการแก้ไขปัญหาทั้งที่เกิดจากกฎหมายของประเทศไทยและกฎหมายของต่างประเทศ ที่อาจจะต้องนำมาปรับปรุงแก้ไขเพื่อใช้กับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ต่อไป ดังนั้นจึงมีข้อเสนอแนะให้มีการแก้ไข ดังนี้

5.2.1 ข้อเสนอแนะทางกฎหมาย

1. แก้ไขอำนาจหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ตามมาตรา 18 ที่ได้บัญญัติไว้ว่า

> ให้อำนาจกับพนักงานเจ้าหน้าที่ให้มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะเท่าที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด
>
> (1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้
>
> (2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง
>
> (3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่
>
> (4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่
>
> (5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่
>
> (6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวน

หาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใดหรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้และตามมาตรา 19 ที่ได้บัญญัติไว้ว่า ให้พนักงานเจ้าหน้าที่มีอำนาจตามมาตรา 18(4) (5) (6) (7) และ (8) โดยการให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง

ควรเพิ่มเป็น มาตรา 19/1 ในส่วนที่เป็นกรณีของการค้นและยึดข้อมูลคอมพิวเตอร์โดยไม่ต้องขอหมาย โดยให้เป็นไปตามกรณีของข้อยกเว้นในเรื่องของการยึดและค้นข้อมูลคอมพิวเตอร์โดยไม่ต้องมีหมาย คือ 1. กรณีที่ได้รับความยินยอม (Consent) 2. กรณีที่เป็นการอันจำเป็นและเร่งด่วน (Exigent Circumstances) และ 3. กรณีที่การยึดค้นข้อมูลคอมพิวเตอร์นั้นได้มาจากการจับกุมโดยชอบ (Search Incident to a Lawful Arrest) ดังนั้นในกรณีที่เป็นความผิด ตามมาตรา 18 (4)-(8) พนักงานเจ้าหน้าที่อาจจะทำการเข้าถึงหรือกระทำการตามมาตราดังกล่าวได้ โดยไม่ต้องขอหมายจากศาล หากว่าเป็นกรณีที่ได้รับความยินยอมจากเจ้าของหรือผู้ครอบครอง

2. มาตรา 19/2 กำหนดให้ผู้ครอบครอง ที่ได้ทำการยึดถือหรือครอบครองคอมพิวเตอร์อยู่ในขณะนั้นให้มีอำนาจให้ความยินยอมแก่เจ้าหน้าที่สามารถทำการค้นและยึดข้อมูลคอมพิวเตอร์ได้โดยไม่ต้องมีหมายค้นหรือเพียงมีข้อสงสัย แต่การค้นและยึดข้อมูลคอมพิวเตอร์จะต้องไม่เกินขอบเขตของความยินยอมและในการให้ความยินยอมในการทำการค้นหาอาจถูกเพิกถอนได้จากเจ้าของข้อมูลคอมพิวเตอร์เอง

3. มาตรา 19/3 กำหนดให้การเข้าถึงข้อมูลคอมพิวเตอร์ให้อำนาจเจ้าหน้าที่เข้าถึงข้อมูลคอมพิวเตอร์ได้โดยไม่ต้องมีหมายค้นในกรณีที่มีความเกี่ยวข้องกับโครงสร้างพื้นฐานของประเทศ เช่น การเงินการธนาคาร, ระบบสื่อประชาสัมพันธ์ของสาธารณะ, ระบบการขนส่งสาธารณะ, โครงสร้างพื้นฐานในการขนส่งทางบก, การขนส่งทางอากาศยาน, โครงสร้างการขนส่งที่สำคัญๆ ควรจะมีการร่วมมือประสานงานหรือศาลควรจะพิจารณาในเรื่องที่มีความจำเป็นและเร่งด่วน

5.2.2 ข้อเสนอแนะอื่นๆ

1. ในกรณีที่ไม่ต้องขอหมายจากศาลหากเป็นกรณีที่มีความจำเป็นเร่งด่วน ศาลควรจะพิจารณาจากสถานการณ์ว่าสถานการณ์ใดมีความจำเป็นและเร่งด่วนมากที่สุด หากระยะเวลาที่ขอหมายอาจจะทำให้ข้อมูลคอมพิวเตอร์นั้น ถูกเปลี่ยนแปลง หรือ ถูกทำลาย หรือสูญหายได้หรือเป็นภัยคุกคามที่ทำให้ทั้งตำรวจหรือประชาชนตกอยู่ในอันตราย หรือผู้ต้องสงสัยมีโอกาสที่จะหนีไปก่อนที่เจ้าหน้าที่จะขอหมายค้นได้เช่น 1.ระยะเวลาที่จำเป็นในการที่จะขอหมายจากศาล (The Amount of Time Necessary to Obtain a Warrant)

2. หลักฐานที่เป็นเรื่องสำคัญจะถูกลบออกหรือถูกทำลายไปเสียก่อน (Whether the Evidence is about to be Removed or Destroyed)

3. ความเป็นไปได้ที่จะเกิดอันตรายในขณะนั้น (The Possibility of Danger at the Site) ในกรณีที่ไม่ต้องขอหมายจากศาลหากเป็นกรณีที่เป็นภัยคุกคามต่อความมั่นคงของชาติที่อาจจะก่อให้เกิดความผิดที่ร้ายแรง ศาลจะต้องทำการพิจารณาจากบุคคลที่รัฐมนตรีได้มอบหมายหรือองค์กรที่ได้ระบุไว้ในหมาย ให้มีอำนาจในการที่จะกระทำการค้นและยึดได้ เพื่อเป็นการป้องกันหรือต่อต้านภัยคุกคามต่อความมั่นคงของชาติ การป้องกันประเทศหรือความสัมพันธ์กับต่างประเทศต่อไป

บรรณานุกรม

กระมล ทองธรรมชาติ และสมบูรณ์ สุขสำราญ. **เรื่องน่ารู้เกี่ยวกับการปกครองและรัฐธรรมนูญของสหรัฐอเมริกา.** พระนคร: โรงพิมพ์สังคมศาสตร์, 2546.

เกียรติขจร วัจนะสวัสดิ์. **คำอธิบายหลักกฎหมายวิธีพิจารณาความอาญาว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณา**. พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม. กรุงเทพฯ: หจก.จิรรัชการพิมพ์, 2551.

คะนึง ฦาไชย. **กฎหมายวิธีพิจารณาความอาญา เล่ม 1**. พิมพ์ครั้งที่ 9 แก้ไขเพิ่มเติม. กรุงเทพฯ: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2551.

จิรนิติ หะวานนท์. **สิทธิทางวิธีพิจารณาความอาญาตามรัฐธรรมนูญ.** กรุงเทพฯ: วิญญูชน, 2543.

จุลสิงห์ วสันตสิงห์. **คำอธิบายประมวลกฎหมายวิธีพิจารฯความอาญา ภาค 1.** พิมพ์ครั้งที่ 2. กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตสภา, 2553.

ฉัทปณัย รัตนพันธ์. **อาชญากรรมทางคอมพิวเตอร์: ศึกษาการกำหนดฐานความผิดและการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์.** สารนิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547.

ญาณพล ยั่งยืน. อาชญากรรมคอมพิวเตอร์. ใน **เอกสารประกอบการสัมมนาโครงการเพิ่มศักยภาพข้าราชการฝ่ายตุลาการศาลอุทธรณ์ภาค 9 ประจำปี พ.ศ.2550.** ค้นวันที่ 20 กรกฎาคม 2558 จาก http://elearning.aru.ac.th/4000108/hum07/topic3/linkfile/print5.htm

ณัฐวสา ฉัตรไพฑูรย์ และคณะ. **การค้นและยึดคอมพิวเตอร์และการได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์ในการสอบสวนคดีอาญา**. กรุงเทพฯ: แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา, 2545.

ทวีเกียรติ มีนะกนิษฐ. **เอกสารประกอบการสัมมนาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550.** กรุงเทพฯ: คณะกรรมการฝ่ายวิชาการ สถาบันวิจัยและพัฒนากฎหมาย สภาทนายความ, 2550.

ธงชัย โรจน์กังสดาล. อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 30 มกราคม 2551. สัมภาษณ์.

นพมาศ ประสิทธิ์มณฑล. **อาชญากรรมคอมพิวเตอร์ ตามกฎหมายสหรัฐอเมริกากฎหมายอิเล็กทรอนิกส์เพื่อการศึกษา.** ค้นวันที่ 11 ธันวาคม 2558 จาก http://www.geocities.com/elaw007

บันทึกการประชุมสภานิติบัญญัติแห่งชาติ. ครั้งที่ 6/2549. 15 พฤศจิกายน 2549.

พรเพชร วิชิตชลชัย. **คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550**. กรุงเทพฯ: โรงพิมพ์ดอกเบี้ย, 2550.

มหาวิทยาลัยราชภัฏสวนดุสิต. **วิชาเทคโนโลยีสารสนเทศเพื่อชีวิต.** ค้นหาวันที่ 9 ธันวาคม 2558. จาก http://dusithost.dusit.ac.th/~librarian/it107/C2.htm.

โรงเรียนเชียงคำวิทยาคม. **อินเตอร์เน็ตและการสื่อสารในชีวิตประจำวัน.** ค้นวันที่ 9 ธันวาคม 2558. จาก http://www.krunee.com

เลอสรร ธนสุกาญจน์, จิตตภัทร เครือวรรณ์ และสุธรรม อยู่ในธรรม. **กฎหมายสำหรับบริการอินเตอร์เน็ตในประเทศไทย**. กรุงเทพฯ: นิติธรรม, 2541.

วรุฬลักษณ์ แซ่ลี้. **อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550.** วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2554.

วัลลิกา เนติบันลือฤทธิ์. ปัญหาการรวบรวมและพิสูจน์พยานหลักฐานที่เป็ข้อมูลอิเล็กทรอนิกส์ในคดีอาญา. **วารสารยุติธรรมปริทัศน์**. 1, 9 (กันยายน 2550): 14-19.

วีรพงษ์ บึงไกร. **การเปิดเผยข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540.** กรุงเทพฯ: คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2543.

วีระ โลจายะ. สิทธิเสรีภาพของประชาชน. ใน **เอกสารการสอนวิชากฎหมายมหาชน เล่มที่ 2**. พิมพ์ครั้งที่ 9. นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2545.

สกล อดิศรประเสริฐ. **มาตรการทางกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเฉพาะกรณีการแยกแยะประเภทข้อมูลส่วนบุคคล.** วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์, 2552.

สาวิตรี สุขศรี. **ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์**. ค้นวันที่ 13 ธันวาคม 2558 จาก http://www.siamsewana.org

สำนักงานตำรวจแห่งชาติ. **อาชญากรรมคอมพิวเตอร์.** ค้นวันที่ 9 ธันวาคม 2558 จาก http://www.royalthaipolice.go.th.

สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. **แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์.** กรุงเทพฯ: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, 2547.

สำนักงานศาลยุติธรรม. **ผลสรุปจากการประชุมหารือของผู้แทนศาลเพื่อดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ระหว่างวันที่ 19 พฤศจิกายน 2550 ถึงวันที่ 20 ธันวาคม 2550**. กรุงเทพฯ: สำนักงานศาลยุติธรรม, 2550.

สุเมธ ลิขิตธนานันท์. **เหตุในการจับกุม**. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2529.

หยุด แสงอุทัย. **กฎหมายอาญา 1.** พิมพ์ครั้งที่ 20 แก้ไขเพิ่มเติม. กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2551.

องอาจ เทียนหิรัญ. **อาชญากรรมทางคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์.** วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2546.

Hudson, Major Walter M. A Few New Developments in the Fourth Amendment. **The Army Lawyer**. (April 1999). Retrieved July 31, 2015 from http://heinonline.org/HOL/LandingPage?handle=hein.journals/armylaw1999&div=21&id=&page=

Israel, Jerold H.; Kamisar, Yale and Lafave, Wayne R. **Criminal Procedure and the Constitution**. U.S.A.: West, 1995.

Jarrett, H. Marshall and Bailie, Michael W. **Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal.** Retrieved July 31, 2015 from https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

Kamisar, Yale and others. **Basic Criminal Procedure, Cases, Comments and Questions.** 12th ed. Eagan, Minnesota: Thomson West, 2008.

Packer, Herbert L. **The Limits of the Criminal Sanction**. California: Stanford University Press, 1968 อ้างถึงใน เกียรติขจร วัจนะสวัสดิ์. **คำอธิบายหลักกฎหมายวิธีพิจารณาความอาญาว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณา**. พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม. กรุงเทพฯ: หจก.จิรรัชการพิมพ์, 2551.

Paker, Donn B.; Nycum, S. and Aura, S. **Computer Abuse**. California: Stanford Reseacher, n.d. quoted in Wasik, Martin **Crime and the Computer**. Oxford: Clarendon,1991 อ้างถึงใน องอาจ เทียนหิรัญ. **อาชญากรรมทางคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์**. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2546.

Singapore Government. **Singapore Statutes Online.** Retrieved July 31, 2015 from http://statutes.agc.gov.sg

ประวัติผู้เขียน

ชื่อ ชื่อสกุล	นางสาวแพรวนภา กองทิพย์
ประวัติการศึกษา	นิติศาสตรบัณฑิต มหาวิทยาลัยรามคำแหง ปีที่สำเร็จการศึกษา พ.ศ.2554
ประสบการณ์ทำงาน	พ.ศ.2552-2555 เจ้าหน้าที่ผู้ช่วยทนายความ บริษัท ชื่นหทัยทนายความและบัญชี จำกัด พ.ศ.2558-ปัจจุบัน นิติกร กรมโยธาธิการและผังเมือง