อำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐาน ที่เป็นข้อมูลอิเล็กทรอนิกส์ ศึกษาเปรียบเทียบระหว่างประเทศไทยกับสหรัฐอเมริกา

The Authority Of Investigated Officer In Collecting The Electronic Information Evidence: Comparing Between Thailand And United State Of America

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต มหาวิทยาลัยกรุงเทพ
พ.ศ. 2550

อำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐาน ที่เป็นข้อมูลอิเล็กทรอนิกส์ ศึกษาเปรียบเทียบระหว่างประเทศไทยกับสหรัฐอเมริกา

The Authority Of Investigated Officer In Collecting The Electronic Information Evidence: Comparing Between Thailand And United State Of America

โดย
นายวิศรุต อนุศาสนนันทน์

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต มหาวิทยาลัยกรุงเทพ
พ.ศ. 2550

บัณฑิตวิทยาลัย
มหาวิทยาลัยกรุงเทพ

สารนิพนธ์

โดย

นายวิศรุต อนุศาสนนันทน์

เรื่อง

อำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ศึกษาเปรียบเทียบระหว่างประเทศไทยกับสหรัฐอเมริกา

ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต

อาจารย์ที่ปรึกษา _____
(ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ)

อาจารย์ที่ปรึกษาร่วม _____
(อาจารย์อำนาจ เนตยสุภา)

กรรมการผู้ทรงคุณวุฒิ _____
(รองศาสตราจารย์ ดร.พันธุ์ทิพย์ ก.สายสุนทร)

ชื่องานวิจัยภาษาไทย : อำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ศึกษาเปรียบเทียบระหว่างประเทศไทยกับสหรัฐอเมริกา

ชื่องานวิจัยภาษาอังกฤษ : The authority of investigated officer in collecting the electronic Information evidence: Comparing between Thailand and United State of America

ชื่อผู้วิจัยภาษาไทย : นายวิศรุต อนุศาสนนันทน์

ชื่อผู้วิจัยภาษาอังกฤษ : Mr. Visarut Anusasananant

ชื่อคณะ : คณะนิติศาสตร์

สาขา : กฎหมายธุรกิจระหว่างประเทศและธุรกรรมทางอิเล็กทรอนิกส์

ชื่อสถาบัน : มหาวิทยาลัยกรุงเทพ

รายชื่อที่ปรึกษา : ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ

ปีการศึกษา : 2550

คำสำคัญ : ข้อมูลอิเล็กทรอนิกส์ อาชญากรรมคอมพิวเตอร์

บทคัดย่อ

สังคมในปัจจุบันเข้าสู่ยุคเทคโนโลยีสารสนเทศที่ใช้ข้อมูลอิเล็กทรอนิกส์เป็นการสื่อสาร ทำให้สามารถส่งผ่านข้อมูลได้ง่ายและรวดเร็ว อีกทั้งยังช่วยให้การติดต่อสื่อสารเป็นอย่างสะดวกยิ่งขึ้นด้วย แต่ระบบคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์ ซึ่งเ ป็นสิ่งที่อำนวยความสะดวกในการติดต่อสื่อสารกลับไม่ได้คุ้มครองทางกฎหมาย เนื่องจากกฎหมายในการที่จะเข้ามาดูแลสังคมให้ปลอดภัยจากการกระทำความผิดนั้นอย่างเป็นไปอย่างเชื่องช้าและไม่ทันต่อสถานการณ์ อีกทั้งพนักงานสอบสวนยังไม่มีอำนาจเพียงพอที่จะเข้าไปดูแลอาชญากรรมทาง คอมพิวเตอร์ ทำให้เกิดช่องว่างมากมายในการป้องกันและปราบปรามอาชญากรรมประเภทนี้

สารนิพนธ์ฉบับนี้มีจุดหมายที่จะศึกษาเกี่ยวกับอำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เนื่องจากการในปัจจุบันได้มีอาชญากรรมเกิดขึ้นมากมาย แต่หน่วยงานที่ดูแลยังไม่มีศักยภาพในการทำงานเพียงพอ เช่น พนักงานสอบสวนยังไม่มีความรู้ความสามารถในการที่จะหาข้อมูลและพยานหลักฐานที่เป็นอิเล็กทรอนิกส์ อีกทั้งยังอาจจะเป็นผู้ทำลายพยานหลักฐานแบบรู้เท่าไม่ถึงการณ์ได้ นับว่าปัญหาดังกล่าวเป็นปัญหาที่สำคัญ เนื่องจากปัญหาอาชญากรรมทางคอมพิวเตอร์ ได้พัฒนารูปแบบที่สลับซับซ้อน และยากต่อการที่จะเข้าไปควบคุมกำกับดูแลและปราบปรามได้อย่างมีประสิทธิภาพ หากบทบัญญัติของกฎหมาย เจ้าหน้าที่ และหน่วยงานของรัฐที่เกี่ยวข้องยังไม่มีศักยภาพที่เพียงพอ

จากการศึกษาข้อมูลพบว่า ในหลายประเท ศก็พบกับปัญหาในลักษณะนี้เช่นกัน และได้มีความพยายามที่จะใช้มาตรการทางกฎหมายที่ออกมาใช้บังคับเฉพาะกับการกระทำความผิดทางคอมพิวเตอร์ รวมถึงมาตรการต่างๆ ที่เข้ามาควบคุมดูแลปัญหานี้ สำหรับประเทศไทยขณะนี้มี

พระราชบัญญัติเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ออกมาใช้บังคับกับปัญหาดังกล่าว และเพื่อที่จะทำให้กฎหมายออกมามีประสิทธิภาพมากขึ้น ประเทศไทยควรจำเป็นต้องจัดตั้งหน่วยงานที่มีอำนาจหน้าที่ โดยการสรรหาและพัฒนาบุคลากรจากกลุ่มผู้มีประสบการณ์ด้านการสอบสวนคดีอาญา ที่มีความรู้ทางคอมพิวเตอร์และอิเล็กทรอนิกส์ เพื่อฝึกอบรมในด้านวิธีการตรวจค้นและยึดพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์เพื่อให้พนักงานสอบสวนมีศักยภาพในการทำงาน เพื่อที่จะจัดการกับอาชญากรรมคอมพิวเตอร์ในประเทศไทยต่อไป

Abstract

Today, our society is stepping into the information technology age which using the electronic information to communicate among our society. The information will be transferred faster and easier. It will facilitate our way of life, though these facilities have never been appropriately protected by the enforceable law. The lack of aggressive and adaptability in our law will jeopardize our safety. Especially, the lack of authority to watch over the offence on the internet. This defect in our system will give the opportunity to the criminal to commit a crime.

This Independent study will concentrate on the authority of the investigator who has a duty to collect the electronic information evidence. Because of the incompetent government agency the illegal action is continuously increase such incompetent as the authority did not have a capability to collecting and searching for the electronic information. The information will be damaged by the incompetent officer. This was a big problem for the government agency because the offence on the computer is much more complicated and infeasibility to contained and suppressed by the inefficient law, incapability officer, incompetent government agency.

The author founded that many country were facing this kind of problem after researched the information. The legal actions were created to deal with crime on computer. Thailand has put a lot of effort deliberately draft the law which will be used to enforce the crime, though the authority government agency will be needed to select and develop people who has an experience in investigating criminal case and computer and electronic knowledge. These people will be given an effectively method in searching and confiscating the evidence in the computer criminal case. We expect that this method will prepare the officer who has an ability to productively dealing with the offence on the computer.

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้ สำเร็จลุล่วง ไปได้โดยความอนุเคราะห์เป็นอย่างดียิ่ง จากบุคคลต่างๆ ที่กรุณาให้คำปรึกษา ให้ข้อมูล และความช่วยเหลือในด้านต่างๆ ที่เป็นประโยชน์ในการศึกษาและการทำสารนิพนธ์ ข้าพเจ้าขอกล่าวขอบคุณไว้ดังนี้

ท่านอัยการอำนาจ เนตยสุภา ที่กรุณารับเป็นที่ปรึกษา และ กรุณาให้คำชี้แนะแนวความคิดที่ถูกต้องอันเป็นประโยชน์อย่างสูง โดย ท่านได้สละเวลาอันมีค่ายิ่ง ให้ความรู้ คำแนะนำ แนวคิดต่างๆ ในการทำสาร นิพนธ์ ตลอดจนแก้ไขข้อบกพร่องให้สารนิพนธ์ฉบับนี้ให้สมบูรณ์ ผู้เขียนจึงขอกราบขอบพระคุณท่านอาจารย์อย่างสูงไว้ ณ ที่นี้

ท่านอัยการวิพล กิติทัศนาสรชัย ที่กรุณาให้คำแนะนำที่เป็นประโยชน์ โดยเสียสละเวลาอันมีค่ายิ่ง อีกทั้งกรุณาให้หนังสือเพื่อใช้ประกอ บการทำสารนิพนธ์ ผู้เขียนจึงขอ กราบขอบพระคุณท่านอาจารย์อย่างสูงไว้ ณ ที่นี้

ผู้เขียนขอกราบขอบพระคุณบิดา มารดา ผู้มีพระคุณอันยิ่งใหญ่ของผู้เขียน ซึ่งท่านได้ให้การสนับสนุนในทุกๆ ด้าน ตลอดจนเป็นกำลังใจให้กับผู้เขียน และขอกราบขอบพระคุณ ครูบาอาจารย์ทุกๆท่านที่ได้ประสิทธิประสาทวิชาความรู้ต่างๆ ให้กับผู้เขียน

นอกจากนี้ผู้เขียนขอขอบคุณ พี่ๆ และเพื่อนนักศึกษามหา วิทยาลัยกรุงเทพ ที่ให้คำปรึกษา แนะนำ แลกเปลี่ยนข้อมูลความรู้ ประสบการณ์ต่างๆ รวมทั้งการติดต่อประสานงานในการศึกษาครั้งนี้ ส่วนความผิดพลาดใด ๆ ผู้เขียนขอน้อมรับแต่เพียงผู้เดียว

วิศรุต อนุศาสนนันทน์

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันการพัฒนาเทคโนโลยีคอมพิวเตอร์ก้าวหน้าไปอย่างรวดเร็ว ทำให้การติดต่อสื่อสารส่งผ่านข้อมูลสารสนเทศเป็นไปได้ง่ายและสะดวก มากขึ้น แต่ในทางกลับกันการก้าวหน้าไปอย่างรวดเร็วนี้กลับ ทำให้มีผลเสียตามมาเช่นกัน อาทิเ ช่น กฎหมายที่จะเข้ามาดูแลสังคมให้ปลอดภัยจากการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์นั้นเป็นไปอย่างเชื่องช้า และไม่ทันต่อสถานการณ์ อีกทั้งพนักงานสอบสวนยังไม่มีอำนาจเพียงพอที่จะเข้าไปดูแลอาชญากรรมคอมพิวเตอร์ ทำให้เกิดช่องว่างมากมายในการป้องกันและปราบปรามอาชญากร รมประเภทนี้ อีกทั้งการดำเนินคดีกับอาชญากรรมทางคอมพิวเตอร์มีความยากลำบากกว่าการดำเนินคดีกับอาชญากรรมทั่วไป เนื่องจากพยานหลักฐานส่วนใหญ่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ดังนั้นการป้องกันและปราบปรามอาชญากรรมประเภทนี้ต้องอาศัยบุคลากรที่มีความรู้พิเศษเฉพาะด้าน รวมถึงมีการวางแนวทางปฏิบัติที่ชัดเจนให้กับเจ้าหน้าที่ ดังนั้น จึงจำเป็นต้องมีกฎหมายพิเศษเป็นการเฉพาะ ในการค้นหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ไม่ว่าจะเป็นเรื่องของการตรวจค้น ทั้งนี้เพื่อเป็นการคุ้มครองสิทธิส่วนบุคคลไม่ให้ถูกละเมิดโดยเจ้าหน้าที่ รัฐจนทำให้เกิดความเสียหายแก่เจ้าของระบบด้วย

ในการดำเนินคดีทางอาชญากรรมทางคอมพิวเตอร์ กฎหมายที่ให้อำนาจหน้าที่แก่พนักงานสอบสวนในการค้นหาพยานหลักฐานทางอิเล็กทรอนิกส์ ปัจจุบันยังไม่ครอบคลุมประเด็นดังกล่าว จึงทำให้เกิดความขัดข้องในการรวบรวมพยานหลักฐานและการรับ ฟังพยานหลักฐาน มาตราการทางกฎหมายของประเทศไทยในปัจจุบันมักให้ความสำคัญเฉพาะอาชญากรรมลักษณะทั่ว ๆไป มากกว่าอาชญากรรมทางคอมพิวเตอร์ ซึ่งแตกต่างกับกฎหมายของประเทศสหรัฐอเมริกาที่ให้อำนาจหน้าที่แก่พนักงานสอบสวนอย่างเต็มที่ ในการรวบรวมพยานหลักฐานและการรับฟังพยาน หลักฐานทางอิเล็กทรอนิกส์

ปัจจุบันประเทศไทยมีหลายหน่วยงานที่ดูแล แต่ยังไม่มีหน่วยงานใดที่รับผิดชอบแก้ไขปัญหานี้โดยตรง ดังนั้น สารนิพนธ์ฉบับนี้ จึงทำการศึกษาถึงอำนาจหน้าที่ของพนักงานสอบสวนสอบสวนที่ขึ้นตรงต่อสำนักงานตำรวจแห่งชาติ และเปรียบเทียบอำนาจหน้าที่ของพ นักงานสอบสวนของ ประเทศไทยและประเทศสหรัฐอเมริกา เพื่อให้ทราบ ถึงอำนาจหน้าที่ของพนักงานสอบสวนในประเทศไทย ว่ายังมีข้อบกพร่องประการใดที่เป็นอุปสรรคต่อการปฏิบัติหน้าที่ ของ พนักงานสอบสวนบ้าง และมีแนวทางใดที่จะสามารถนำมาปรับใช้กับอำนาจ หน้าที่ของพนักงานสอบสวนของ ประเทศ ไทยได้บ้าง เพื่อให้การดำเนินคดีอาชญากรรมคอมพิวเตอร์มีประสิทธิภาพมากยิ่งขึ้น

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อให้ทราบถึงรูปแบบและประเภทของอาชญ ากรรมคอมพิวเตอร์ที่ก่อให้เกิดความเสียหายที่แตกต่างกันออกไป
2. เพื่อได้ทราบความหมาย อำนาจหน้าที่ของพนักงานสอบสวนในคดีอาญา ว่าปัจจุบันเป็นไปในทิศทางใด
3. เพื่อได้ทราบถึงปัญหาในการรวบรวมพยานหลักฐาน การค้นและยึด ทางคดีอาชญากรรมทางคอมพิวเตอร์
4. เพื่อให้ทราบถึงหลักกฎหมายในการสืบสวนสอบสวนค้นและยึดพยานหลักฐานของประเทศไทยและประเทศสหรัฐอเมริกา

1.3 สมมุติฐานของการศึกษา

งานวิจัยฉบับนี้ มีสมมุ ติฐานว่า กฎหมาย ของประเทศไทย โดยเฉพาะอย่างยิ่งเรื่องอำนาจหน้าที่ของพนักงานสอบสวนที่จะเข้าทำการค้นและยึดพยานหลักฐานที่บังคับใช้อยู่ในปัจจุบัน มีปัญหาในการปรับใช้ในคดีเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ตั้งแต่การรวบรวมพยานหลักฐานของพนักงานสอบสวน จนถึงการค้นและยึดพย านหลักฐานยังไม่มีความชัดเจนเท่าที่ควร กล่าวคือ เทคโนโลยีและสารสนเทศนำความเจริญก้าวหน้า และเข้ามามีบทบาทสำคัญต่อสังคมโลก และประเทศไทยอย่างมาก มีการก่ออาชญ ากรรมโดยใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ซึ่งเป็นอาชญากรรมรูปแบบใหม่ ที่สลับซับซ้อนและยากแก่ การสืบสวนสอบสวนดำเนินคดี เนื่องจากเจ้าหน้าที่ยังไม่มีความรู้ความชำนาญ และไม่เข้าใจลักษณะผลกระทบที่เกิดขึ้นดังกล่าว จึงต้องศึกษามาตรการกฎหมายของต่างประเทศ เพื่อเป็นแนวทางแก้ไขปัญหากฎหมายของประเทศไทยให้พัฒนามากยิ่งขึ้นต่อไป

1.4 ขอบเขตของการศึกษา

การศึกษาวิจัยในเรื่องอำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานที่เป็นอิเล็กทรอนิกส์นี้ จะศึกษาเฉพาะอำนาจหน้าที่ของพนักงานสอบสวนที่ขึ้นตรงต่อสำนักงานตำรวจแห่งชาติ ตลอดจนปัญหาในการค้น ยึดและรักษาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ โดยศึกษาเปรียบเทียบระหว่างประเทศไทย กับประเทศสหรัฐอเมริกา พร้อมทั้งเสนอแนวทางแก้ไขปัญหาดังกล่าว

1.5 วิธีการศึกษา

การดำเนินการวิจัยนี้เป็นการศึกษาวิจัยเชิงคุณภาพ โดยวิธีวิจัยจากเอกสารโดยศึกษาจากอินเตอร์เน็ต ตำรา ตัวบทกฎหมายทั้งของประเทศไทยและต่างประเทศ รายงานการวิจัย บทความ ระเบียบข้อบังคับ คำพิพากษาของศาล และนำข้อมูลเอกสารนั้นมาเรียบเรียงและวิเคราะห์

1.6 นิยามศัพท์

ข้อมูลอิเล็กทรอนิกส์ หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษาหรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทร อนิกส์ โทรเลข โทรพิมพ์หรือโทรสาร

ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

อาชญากรรมทางคอมพิวเตอร์ คือ การใช้คอมพิวเตอร์เพื่ออำนวยความสะดวกหรือนำไปสู่การกระทำผิดทางอาญา

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ทราบถึงรูปแบบ และวิธีการรวบรวมพยานหลักฐานในคดีอาญาทั่วไปและคดีอาชญากรรมคอมพิวเตอร์
2. ทำให้ทราบถึงปัญหาในการรวบรวมพยานหลักฐานของประ เทศไทย และข้อจำกัดในการปรับปรุงแก้ไขกฎหมายที่มีผลบังคับใช้อยู่นั้น สามารถที่จะป้องกันและแก้ไขปัญหาที่มีอยู่ในปัจจุบันว่ามีประสิทธิภาพเพียงพอหรือไม่ อีกทั้งยังสามารถที่จะรองรับกับปัญหาที่จะเกิดขึ้นตามมาในอนาคตได้ชัดเจนมากน้อยเพียงใด
3. เพื่อศึกษาหา แนวทางและมา ตราการทางด้านกฎหมาย ของประเทศไทยที่ จะใช้กับผู้ที่กระทำผิดทางอิเล็กทรอนิกส์ให้มีประสิทธิภาพมากยิ่งขึ้น เพื่อที่จะทำให้ ปัญหาอาชญากรรมทางคอมพิวเตอร์ลดลง
4. ทำให้ทราบถึงอำนาจหน้าที่ของพนักงานสอบสวนในคดีอาชญากรรมทางคอมพิวเตอร์ของประเทศไทยและประเทศสหรัฐอเมริกา
5. ทำให้ ทราบถึงแนวคิดในการที่จะปรับปรุงและพัฒนาบุคลากร โดยเฉพาะพนักงานสอบสวนทางคดีอาชญากรรมคอมพิวเตอร์ให้มีประสิทธิภาพในการทำงานมากยิ่งขึ้น เพื่อที่จะยับยั้งการกระทำความผิดทางอิเล็กทรอนิกส์ที่จะแผ่ขยายวงกว้างและรุนแรงในอนาคต

บทที่ 2

ความหมาย อำนาจหน้าที่และวิธีการของพนักงานสอบสวน ในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์

2.1 ความหมาย รูปแบบและประเภทของอาชญากรรมคอมพิวเตอร์

วิวัฒนาการทางเทคโนโลยีสารสนเทศในโลกปัจจุบันได้ก้าวไปอย่างไม่หยุดยั้ง อันทำให้สังคมเกิดความเปลี่ยนแปลงไปอย่างมากมาย โดยเฉพาะเครื่องคอมพิวเตอร์ก่อให้เกิดความสะดวกสบายขึ้นในชีวิตประจำวัน ไม่ว่าจะเป็นทางด้านการศึกษา สุขภาพ ความบันเทิง การค้า และการประยุกต์ในเชิงสร้างสรรค์ในรูปแบบต่างๆ แต่ ในขณะเดียวกันหากนำไปใช้ในทางก่อความเสียหายให้กับบุคคลอื่น โดยเฉพาะอย่างยิ่งในการก่ออาชญากรรมทางคอมพิวเตอร์ ซึ่งนับวันจะทวีความรุนแรงและสร้างความเสียหายเป็นอย่างมาก ความเสียหายที่เกิดขึ้นจากอาชญากรรมทางคอมพิวเตอร์ไม่ได้ส่งผลกระทบต่อความมั่นคงของบุคคลใดบุคคล หนึ่งเท่านั้น แต่ยังส่งผลกระทบไปยังความมั่นคงของประเทศชาติ ทั้งความมั่นคงภายในและความมั่นคงภายนอกประเทศ นอกจากนั้นอาชญากรรมทางคอมพิวเตอร์ยังแตกต่างจากอาชญากรรมรูปแบบเดิม ๆ อย่างสิ้นเชิง เนื่องจากผู้กระทำความผิดเป็นผู้มีความรู้ความสามารถเกี่ยวกับเทคโนโลยีค อมพิวเตอร์ทำให้การตรวจสอบการกระทำความผิดกระทำได้ลำบาก อีกทั้งไม่ค่อยจะหลงเหลือพยานหลักฐานให้เจ้าหน้าที่ใช้สำหรับการสืบสวนสอบสวน และติดตามจับกุมตัวผู้กระทำความผิดมาลงโทษ

2.1.1 ความหมายของอาชญากรรมทางคอมพิวเตอร์

หากกล่าวถึงอาชญากรรมทางคอมพิว เตอร์ จะพบว่าเกิดจากบุคคลหรือคณะบุคคลกระทำความผิดทางอาญา โดยใช้เครื่องคอมพิวเตอร์เป็นเครื่องมือกระทำความผิด และมีผู้ได้รับความเสียหายหรืออาจได้รับความเสียหายจากการที่มีผู้บุกรุกหรือพยายามที่จะเข้าไปในระบบคอมพิวเตอร์ หรือกล่าวอีกนัยหนึ่งคือการกระทำความผิดกฎ หมายอาญาใดเกี่ยวกับความรู้ทางเทคโนโลยีสารสนเทศ เพื่อวัตถุประสงค์ลักลอบเข้าไป ลักลอบเข้าถึงข้อมูลคอมพิวเตอร์เพื่อฉกฉวยประโยชน์อันก่อให้เกิดความเสียหายต่อเจ้าของข้อมูล บางครั้งส่งผลกระทบต่อระบบเศรษฐกิจของประเทศ หรือระบบเศรษฐกิจของโลก

เนื่องจากอาชญากรรมคอมพิ วเตอร์เกิดจากอาชญากรที่มีความรู้หรือที่เราเรียกว่า “โจรเสื้อนอก” หรือ “โจรเสื้อขาว” (White Collar Crime)[1] ซึ่งเกิดขึ้นโดยการนำเอาเทคโนโลยีคอมพิวเตอร์หรือเทคโนโลยีสารสนเทศไป ใช้ในการทุจริต จึงถือ ได้ว่าอาชญา กรรมทางคอมพิวเตอร์ เป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่ง

---

[1] สุปรียา อภิวัฒนากร, “อาชญากรรมทางคอมพิวเตอร์: ศึกษากรณีการหลอกลวงทางอินเตอร์เน็ต” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยจุฬาลงกรณ์, 2545 หน้า 39)

อาชญากรรมทางคอมพิวเตอร์เป็นคำที่มีความหมายกว้างมากและมีนักก ฎหมายหรือหน่วยงานต่างๆ ได้ให้คำนิยามแตกต่างกันดังนี้

สำนักงานตำรวจแห่งชาติได้ให้คำนิยามของคำ ว่า “อาชญากรรมทางคอมพิวเตอร์ ” ไว้ดังนี้ [2]

1. การกระทำใดๆ ก็ตามที่เกี่ยวกับการใช้คอมพิวเตอร์อันทำให้เหยื่อได้รับความเสียหายและผู้กระทำได้รับผลประโยชน์ตอบแทน
2. การทำผิดกฎหมายใดๆ ซึ่งใช้เทคโนโ ลยีคอมพิวเตอร์เป็นเครื่องมือ และในการสืบสวนสอบสวนของเจ้าหน้าที่ เพื่อนำตัวผู้กระทำผิดมาดำเนินคดี ก็ต้องใช้ความรู้ทางเทคโนโลยีทางคอมพิวเตอร์เช่นกัน

พันตำรวจเอก ญาณพล ยั่งยืน ได้ให้ความหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ไว้ว่า “การกระทำใดๆ ก็ตามที่เกี่ยวกับการใช้คอมพิวเตอร์ อันทำให้เหยื่อได้รับความเสียหายและทำให้ผู้กระทำผิดได้รับผลตอบแทน และการกระทำผิดกฎหมายใดๆ ซึ่งจะต้องใช้ความรู้เกี่ยวข้องกับคอมพิวเตอร์มาประกอบการกระทำผิดและต้องใช้ผู้มีความรู้ทางคอมพิวเตอร์ในการสืบสวน ติดตาม รวบรวมหลักฐานเพื่อการดำเนินคดีและจับกุม” [3]

กระทรวงยุติธรรม ประเทศสหรัฐอเมริกา (Department of Justice) ได้ให้คำนิยามคำว่า “อาชญากรรมคอมพิวเตอร์” ไว้ว่าเป็นการกระทำที่ต้องอาศัยประสบการณ์ทางคอมพิวเตอร์ โดยทั่วไปอาชญากรรมประเภทนี้จะเกิดขึ้นภายในเครื่องคอมพิวเตอร์ คำว่า “อาชญากรรมที่เกี่ยวกับคอมพิวเตอร์” เป็นคำที่กว้างกว่าหมายความถึงการกระทำความผิดทางอาญาที่อาศัยความรู้ทางเทคโนโลยีสารสนเทศเพื่อกระทำความผิด รวมทั้งการสืบสวนสอบสวน และฟ้องร้อง คำว่า “การใช้คอมพิวเตอร์กระทำความผิด ” เป็นการรวมความหมายที่กว้างคือ การกระทำโดยเจตนาที่เป็นความผิดทางอา ญา ซึ่งเป็นการกระทำโดยเจตนาใดๆ ที่อาศัยความรู้ทางด้านเทคโนโลยีสารสนเทศกระทำความผิด โดยบุคคลหนึ่งหรือมากกว่านั้น เพื่อที่จะให้เหยื่อได้รับความเสียหาย [4]

---

[2] http://www.ecid.police.go.th

[3] ญาณพล ยั่งยืน, อาชญากรรมทางคอมพิวเตอร์, (ศูนย์ข้อมูลข้อสนเทศ : สำนักงานตำรวจแห่งชาติ), หน้า 4 (อัดสำเนา)

[4] สุปรียา อภิวัฒนากร , “อาชญากรรมทางคอมพิวเตอร์ : ศึกษากรณีการหลอกลวงทางอินเตอร์เน็ต ” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยจุฬาลงกรณ์, 2545 หน้า 39)

องค์การสหประชาชาติยอมรับว่าไม่สามารถบัญญัตินิยามศัพท์ให้ยอมรับเป็นสากลได้ ซึ่งในทางปฏิบัติจำแนกออกเป็น 2 ส่วนคือ

ส่วนที่ 1 อาชญากรรมดั้งเดิม ซึ่งโดยทั่วไปมีกฎหมายระบุฐานความผิดและบทลงโทษไว้อยู่แล้ว เช่น การโจรกรรม การฉ้อโกง การปลอมแปลง และการก่อกวน ซึ่งมี กฎหมายหลักบัญญัติความผิดและบทลงโทษไว้

ส่วนที่ 2 การฝ่าฝืนกฎหรือข้อห้าม และพฤติกรรมเบี่ยงเบนต่างๆ ในการใช้คอมพิวเตอร์ ซึ่งยังไม่มีกฎหมายบัญญัติไว้เป็นความผิด [5]

จากที่ได้กล่าวมาข้างต้นจะเห็นได้ว่านิยามของคำว่าอาชญากรรมทางคอมพิวเตอร์มีผู้ได้ให้คำนิยามไว้มากมายหลากหลาย ผู้วิจัยพอจะสรุปคำนิยามของคำว่า “อาชญากรรมทางคอมพิวเตอร์ได้ดังนี้” คือการกระทำผิดกฎหมาย โดยใช้เทคโนโลยีคอมพิวเตอร์เป็นส่วนสำคัญ เป็นการกระทำใดๆ ที่เกี่ยวกับการใช้การเข้าถึงข้อมูล โดยที่ผู้กระทำไม่ได้รับอนุญาตหรือการลักลอกแก้ไขทำลาย คัดลอกข้อมูลหรือทำให้คอมพิวเตอร์ทำงานผิดพลาด แม้บางกรณีอาจไม่ถึงกับเป็นการกระทำที่ผิดกฎหมายแต่เป็นการกระทำที่ผิดระเบียบกฎเกณฑ์ จรรยาบรรณของการใช้คอมพิวเตอร์นั้นๆ

2.1.2 รูปแบบของอาชญากรรมคอมพิวเตอร์

รูปแบบของอาชญากรรมคอมพิวเตอร์ สามารถแบ่งออกได้เป็น 4 รูปแบบ ดังนี้ [6]

รูปแบบที่ 1 การเจาะระบบรักษาความปลอดภัยทางกายภาพ ได้แก่ ตัวอาคาร อุปกรณ์และสื่อต่างๆ

รูปแบบที่ 2 การเจาะเข้าไปในระบบสื่อสารและการรักษาความปลอดภัยของซอฟต์แวร์ ข้อมูลต่างๆ

รูปแบบที่ 3 เป็นการเจาะเข้าสู่ระบบรักษาความปลอดภัยของระบบปฏิบัติการ

รูปแบบที่ 4 เป็นการเจาะผ่านระบบรักษาความปลอดภัยส่วนบุคคล อินเตอร์เน็ต เพื่อเป็น ช่องทางในการกระทำความผิด

รูปแบบของอาชญากรรมคอมพิวเตอร์ที่ได้กล่าวมาข้างต้นนั้น เป็นรูปแบบเบื้องต้นที่กล่าวถึงอาชญากรรมคอมพิวเตอร์ โดยแต่ละรูปแบบนั้นจะก่อให้เกิดความเสียหายที่แตกต่างกันออกไป ซึ่งผู้ที่ได้รับผลกระทบจากอาชญากรรมคอมพิวเตอร์นั้นก็คือ ภาครัฐ ภาคเอกชน และองค์กรต่างๆ ซึ่งรวมไปถึงบุคคลโดยทั่วไปด้วย

---

[5] สุรพันธ์ มั่นคงดี, “พยานหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์,” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2541 น.30

[6] http://www.ecid.police.go.th/page/Thai/th_knows02.html

โดยธรรมชาติของอาชญากรรมทางคอมพิวเตอร์ ผู้กระทำผิดมักจะพยายามปรับรูปแบบ เพื่อให้ง่ายต่อการกระทำผิด และยากต่อการสืบสวนติดตามจับกุม ในส่วนของอาชญากรรมทางคอมพิวเตอร์นั้นก็เช่นเดียวกัน ผู้กระทำผิดก็จะพยายามหาช่องโอกาสที่เทคโนโลยีสมัยใหม่ได้เอื้ออำนวย ประกอบกับมีช่องว่างทางกฎหมาย บางประการ ดังนั้นจะเห็นได้ว่า ในช่วงที่ผ่านมา จะเกิดคดีอาชญากรรมทางคอมพิวเตอร์ มีความถี่มากขึ้น รูปแบบการกระทำผิดก็มีความหลากหลายมากขึ้น และนับวันจะเป็นปัญหามากยิ่งขึ้น ผู้วิจัยได้พยายามติดตามและรวบรวมกรณีปัญหาเฉพาะที่เกิดในประเทศหรือเกี่ยวพันกับบุคคลในชาติไว้ เพื่อประโยชน์ในการศึกษาหาแนวทางป้องกันปราบปราม โดยยกตัวอย่างเป็นบางกรณีดังนี้ [7]

ปัญหากรณี แอบใช้ Account Internet ของผู้อื่น

การแอบลักลอบใช้ Account Internet ของผู้อื่น ทำให้ผู้นั้นต้องจ่ายค่าชั่วโมงมากขึ้นหรือเสียเวลาชั่วโมงการใช้งาน (คล้ายกับการจูนโทรศัพท์มือถือของผู้อื่น) จากการสืบสวนบางรายทราบว่า ใครเป็นผู้ใช้ บางรายทราบเพียงหมายเลขโทรศัพท์ที่ใช้ในการติดต่อ (จาก Caller ID) และบางรายใช้หมายเลขโทรศัพท์เดียวกัน กับ Account หลาย ๆราย ปัญหาผู้กระทำผิดรู้ Account และ รหัสลับได้อย่างไร เจ้าของเป็นผู้บอกเอง หรือมี Hacker เข้ามาในระบบแล้วนำข้อมูลไป,ใครเป็นผู้เสียหาย ISP หรือ ผู้ใช้บริการ, ฐานความผิดข้อหาใด แพ่ง หรือ อาญา, สิทธิในการใช้บริการ ชั่วโมงใช้งาน เป็นทรัพย์หรือไม่, หลักฐานที่ต้องใช้ บันทึกหมายเลขโทรศัพท์ที่ติดต่อใช้บริการ Caller ID ได้หรือไม่, ใครที่ต้องถือว่าเป็นผู้กระทำผิด คนในบ้านหรือเจ้าบ้าน ถ้าไม่มีใครรับจะทำอย่างไร, ที่เกิดเหตุเป็นที่ใด เป็นที่ตั้ง ISP หรือที่บ้านผู้กระทำผิด หรือที่บ้านขอเจ้าของ Account, การประเมินค่าความเสียหาย

ปัญหากรณี เว็บที่ส่งเสริมการขายสินค้าของไทย 3 แห่ง ถูกใส่ร้าย

มีเว็บที่ส่งเสริมเผยแพร่สินค้าไทยสู่ตลาดโลก 3 เว็บไซต์ ได้ถูกกลุ่มผู้ไม่หวังดี ปลอมอีเมล์ ของเว็บดังกล่าว แล้วส่งไปยังผู้ใช้อินเทอร์เน็ตทั่วโลกประมาณ 4 ล้านฉบับ เป็นลักษณะ Spam Mail และได้ใส่ร้ายเว็บดังกล่าวว่า " เป็นเว็บที่ฉ้อโกง จะนำชื่อและหมายเลขบัตรเครดิตของผู้ที่สนใจเข้ามาซื้อของ ไปใช้ในทางที่ผิด ขอให้อย่าเข้าเว็บไทยทั้ง 3 ดังกล่าว " ผลร้ายที่เกิดขึ้น นอกจากจะทำให้คนทั้งโลกไม่เข้าไปชมเว็บดังกล่าวแล้ว ยังทำให้องค์กรต่อต้าน Spam Mail สั่งให้ Web Hosting ยุติ ปิดการให้บริการ เว็บไทยทั้ง 3 อีกด้วย

ปัญหากรณี อาจารย์ในสถานศึกษา ถูกแอบขโมยข้อมูลตำราและข้อสอบ

มีอาจารย์ในสถานศึกษาแห่งหนึ่ง ได้ใช้เวลากว่า 3 ปี เขียนตำราไว้ รวมเกือบ 1,000 ไฟล์ รวมทั้งข้อสอบ ข้อเฉลย และคะแนนสอบ เก็บไว้ในเครื่อง PC ของตนในห้องทำงานส่วนตัว แต่เนื่องจากได้มีการต่อเชื่อมโยงเป็นเครือข่าย LAN ไว้ทั้งสถานศึกษา จึงทำให้มีบุคคลอื่นสามารถเข้ามาดึงข้อมูลในเครื่อง PC ทั้งหมดที่มีไปได้

[7] ศูนย์ข้อมูลสารสนเทศ สำนักงานตำรวจแห่งชาติ

2.1.3 ประเภทของอาชญากรรมคอมพิวเตอร์

อาชญากรรมทางคอมพิวเตอร์ (Cyber-Crime) เป็นการกระทำที่ผิดกฎหมายโดยใช้วิธีการทางอิเล็กทรอนิกส์เพื่อโจมตีระบบคอมพิวเตอร์และข้อมูลที่อยู่บนระบบดังกล่าว ส่วนในมุมมองที่กว้างขึ้น “อาชญากรรมที่เกี่ยวเนื่องกับคอมพิวเตอร์ ” หมายถึงการกระทำที่ผิดกฎหมายใด ๆ ซึ่งอาศัยหรือมีความเกี่ยวเนื่อง กับระบบคอมพิวเตอร์หรือเครือข่า ย อย่างไรก็ตาม อาชญากรรมประเภทนี้ไม่ถือเป็นอาชญากรรมทางคอมพิวเตอร์โดยตรง

ในการประชุมสหประชาชาติครั้งที่ 10 ว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อ ผู้กระทำผิด (The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders) ซึ่งจัดขึ้นที่กรุงเวียนนา เมื่อวันที่ 10 -17 เมษายน 2543 ได้มีการจำแนกประเภทของอาชญากรรมทางคอมพิวเตอร์ โดยแบ่งเป็น 5 ประเภท คือ [8]

1. การเข้าถึงโดยไม่ได้รับอนุญาต
2. การสร้างความเสียหายแก่ข้อมูลหรือโปรแกรมคอมพิวเตอร์
3. การก่อกวนการทำงานของระบบคอมพิวเตอร์หรือเครือข่าย
4. การยับยั้งข้อมูลที่ส่งถึง/จากและภายในระบบหรือเครือข่ายโดยไม่ได้รับอนุญาต
5. การจารกรรม ข้อมูลบนคอมพิวเตอร์

โครงการอาชญากรรมทางคอมพิวเตอร์และการโจรกรรมทรัพย์สินทางปัญญา (Cyber-Crime and Intellectual Property Theft) พยายามที่จะเก็บรวบรวมและเผยแพร่ข้ อมูล และค้นคว้าเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ 6 ประเภท ที่ได้รับความนิยม ซึ่งส่งผลกระทบโดยตรงต่อประชาชนและผู้บริโภค นอกจากนี้ยังทำหน้าที่เผยแพร่ความรู้เกี่ยวกับขอบเขตและความซับซ้อนของปัญหา รวมถึงนโยบายปัจจุบันและความพยายามในการ แก้ปัญหานี้ อาชญากรรม 6 ประเภทดังกล่าวได้แก่ [9]

1. การเงิน อาชญากรรมที่ขัดขวางความสามารถขององค์กรธุรกิจในการทำธุรกรรมอีคอมเมิร์ซ (หรือพาณิชย์อิเล็กทรอนิกส์)
2. การละเมิดลิขสิทธิ์ การคัดลอกผลงานที่มีลิขสิทธิ์ ในปัจจุบันคอมพิวเตอร์ส่วนบุคคลและอินเทอร์เน็ตถูกใช้เป็นสื่อในการก่ ออาชญากรรม แบบเก่า โดยการโจรกรรมทางออนไลน์หมายรวมถึง การละเมิดลิขสิทธิ์ใดๆ ที่เกี่ยวข้องกับการใช้อินเทอร์เน็ตเพื่อจำหน่ายหรือเผยแพร่ผลงานสร้างสรรค์ที่ได้รับการคุ้มครองลิขสิทธิ์

---

[8] อ้างถึง บทความ : กลุ่มพันธมิตรธุรกิจซอฟต์แวร์ ผลการจับกุมทางอินเตอร์เน็ต, 2548

[9] เพิ่งอ้าง

3. การเจาะระบบ การให้ได้มาซึ่งสิทธิในการเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายโดยไม่ได้รับอนุญาต และในบางกรณีอาจหมายถึงการใช้สิทธิการเข้าถึงนี้โดยไม่ได้รับอนุญาต นอกจากนี้การเจาะระบบยังอาจรองรับอาชญากรรมทางคอมพิวเตอร์ในรูปแบบอื่นๆ (เช่น การปลอมแปลง การก่อการร้าย ฯลฯ)
4. การก่อการร้ายทางคอมพิวเตอร์ ผลสืบเนื่องจากการเจาะระบบ โดยมีจุดมุ่งหมายเพื่อสร้างความหวาดกลัว เช่นเดียวกับการก่อการร้ายทั่วไป โดยการกระทำที่เข้าข่าย การก่อการร้ายทางอิเล็กทรอนิกส์ (e-terrorism) จะเกี่ยวข้องกับการเจาะระบบคอมพิวเตอร์เพื่อก่อเหตุรุนแรงต่อบุคคลหรือทรัพย์สิน หรืออย่างน้อยก็มีจุดมุ่งหมายเพื่อสร้างความหวาดกลัว
5. ภาพอนาจารทางออนไลน์ ตามข้อกำหนด 18 USC 2252 และ 18 USC 2252A การประมวลผลหรือการเผยแพร่ภาพอนาจารเด็กถือเป็นการกระทำที่ผิดกฎหมาย และตามข้อกำหนด 47 USC 223 การเผยแพร่ภาพลามกอนาจารในรูปแบบใดๆ แก่เยาวชนถือเป็นการกระทำที่ขัดต่อกฎหมาย อินเทอร์เน็ตเป็นเพียงช่องทางใหม่สำหรับอาชญากรรม แบบเก่า อย่างไรก็ดี ประเด็นเรื่องวิธีที่เหมาะสมที่สุดในการควบคุมช่องทางการสื่อสารที่ครอบคลุมทั่วโลกและเข้าถึงทุก กลุ่มอายุนี้ได้ก่อให้เกิดการถกเถียงและการโต้แย้งอย่างกว้างขวาง
6. ภายในโรงเรียน ถึงแม้ว่าอินเทอร์เน็ตจะเป็นแหล่งทรัพยากรสำหรับการศึกษาและสันทนาการ แต่เยาวชนจำเป็นต้องได้รับทราบเกี่ยวกับวิธีการใช้งานเครื่องมืออันทรงพลังนี้อย่างปลอดภัยและมีความรับผิดชอบ โดยเป้าหมายหลักของโครงการนี้คือ เพื่อกระตุ้นให้เด็กได้เรียนรู้เกี่ยวกับข้อกำหนดทางกฎหมาย สิทธิของตนเอง และวิธีที่เหมาะสมในการป้องกันการใช้อินเทอร์เน็ตในทางที่ผิด

จากรูปแบบข้างต้นนี้ จะเห็นได้ว่าอาชญากรรมทางคอมพิวเตอร์ หรือ การกระทำผิดต่อข้อมูลคอมพิวเตอร์มีด้วยกั นหลายประเภท แตกต่างกันไปซึ่งนั บวันจะมีความสลับซับซ้อนกันมากขึ้น การนำกฎหมายที่มีอยู่มาจัดการกับการกระทำผิดประเภทนี้ เกิดปัญหาที่ไม่สามารถจะปรับใช้ได้อย่างสมบูรณ์ ดังนั้น การแก้ไขเพิ่มเติมหรือการบัญญัติกฎหมายขึ้นมาใหม่ให้สามารถครอบคลุมถึงการกระทำผิดในลักษณะดังกล่าว เพื่อที่จะได้นำตัวผู้ กระทำผิดมาลงโทษจึงเป็นเรื่องที่ควรให้ความสำคัญอย่างยิ่ง ดังนั้น ผู้วิจัย จึงสรุปประเภทของอาชญากรรมทางคอมพิวเตอร์ได้ดังนี้

2.1.3.1 การลักขโมยบริการ (Theft of Service)

การใช้ประโยชน์จากคอมพิวเตอร์บางอย่างจะต้องมีค่าใช้จ่ายเกิดขึ้น นอกเหนือจากตัวเครื่อง หรือแม้กระทั่งตัวเครื่องเองก็มีการให้เช่า การให้เช่าเครื่องหรือการให้บริการโดย

ปกติแล้ว จะมีผู้เกี่ยวข้องอยู่สองฝ่ายคือ ฝ่ายให้บริการกับผู้ใช้บริการโดยทำเป็นข้อตกลงหรือสัญญาระหว่างกัน ผู้ให้บริการจะได้รับผลประโยชน์ในรูปของค่าบริการ ส่วนผู้ใช้บริการก็จะได้รับ ผลประโยชน์เป็นการใช้บริการนั้นๆ โดยจะต้องชำระค่าบริการให้กับผู้ให้บริการ อาชญากรรมประเภทนี้จะเกิดขึ้นเมื่อมีผู้มาลักลอบใช้บริการ โดยไม่ชำระค่าบริการ ทำให้ผู้ให้บริการต้องเสียรายได้เป็นมูลค่ามหาศาล เรียกกันว่าการลักขโมยบริการ อาจจะเปรียบเทียบได้กับความผิดฐานลักทรัพย์ แต่จะแตกต่างกันตรงที่สิ่งที่ถูกลักขโมยเป็นสิ่งที่ไม่มีรูปร่าง

2.1.3.2 การจารกรรมข้อมูล (Theft of Information)

ในกรณีที่ข้อมูลในคอมพิวเตอร์ที่ต้องการจัดเก็บไว้เป็นความลับหรือกำหนดการใช้เฉพาะบุคคลหรือกลุ่มบุคคล หากถูกบุคคลที่ปราศจากอำนาจหน้าที่ในการเรียกใช้ข้อมูลและทำการแก้ไขเปลี่ยนแปลงข้อมูลชุดดังกล่าว ย่อมจะก่อให้เกิดความเสียหายรุนแรงกว่ากรณีที่เป็นข้อมูลประเภทที่เปิดให้บุคคลอื่นสามารถให้ใช้ได้

กรณีดังกล่าวสามารถเห็นได้จากคดีที่เกิดในประเทศอังกฤษ คือคดีออกซฟอร์ด กับ มอส (Oxford vs. Moss) คือมีนักศึกษาคนหนึ่งได้พบเอกสารที่เป็นข้อสอบซึ่งเขาจะต้องทำการทดสอบวิชาดังกล่าวด้วย เขาได้นำเอาเอกสารชุดดังกล่าวไปเพื่อถ่ายสำเนาเอกสาร โดยเขาตระหนักดีว่าถ้าผู้ที่ดำเนินการจัดสอบทราบว่าได้มีการสูญหายของต้นฉบับข้อสอบแล้ว ทางมหาวิทยาลัยจะดำเนินการออกข้อสอบชุดใหม่แ ทนดังนั้น เขาจึงพยายามที่จะนำเอกสารต้นฉบับส่งคืนไปยังที่จัดเก็บข้อสอบ นักศึกษาผู้นี้ถูกจับได้ในระหว่างที่พยายามจะเอาเอกสารชุดดังกล่าวไปคืน

ภายใต้กฎหมายว่าด้วยการลักทรัพย์ปี 1968 (The Theft Act 1968) มีสาระสำคัญว่าผู้เสียหายนั้นจะต้องถูกลักทรัพย์ไปอย่างถาวร กรณีของนักศึกษารายนี้ไม่ได้เป็นการนำเอาทรัพย์ไปเป็นการถาวร ดังนั้นได้มีการตั้งข้อหาว่านักศึกษารายนี้ได้กระทำการลักพาความลับของข้อมูลที่ปรากฏอยู่ในเอกสารหรือไม่ อย่างไรก็ตามคดีดังกล่าวได้ถูกยกฟ้องในศาลแขวง ซึ่งได้ชี้ประเด็นที่ว่าความลับของข้อมูลไม่สามารถยึ ดถือเป็นทรัพย์สินได้ ภายใต้กฎหมายว่าด้วยเรื่องการลักทรัพย์

จากกรณีดังกล่าวได้มีข้อสังเกตว่านักวิชาการ กฎหมาย ยังคงไม่ได้ให้ความสำคัญกับการพิจารณามูลค่าของทรัพย์สินที่ไม่ถาวร เมื่อเทียบกับสิ่งที่เป็นทรัพย์สินที่ถาวร ภาย ใต้กฎหมายเพื่อความปลอดภัยของข้อมูลทางกา ร (The Official Secrets Acts) ถ้าข้อมูลที่มีอยู่เป็นความลับได้ถูกเขียนไว้บนเอกสารที่วางไว้บนโต๊ะ และเอกสารชิ้นดังกล่าวได้ถูกวางไว้ในตำแหน่งที่บุคคลอื่นสามารถมองเห็นได้ ไม่ถือว่าบุคคลที่ได้อ่านหรือทราบข้อมูลที่เป็นความลับจากการเห็นเอกสารนั้น ถูกระบุว่าได้กร ะทำความผิด ไม่สามารถแม้แต่จะเอาผิดกับผู้ที่ได้ถ่ายรูปเอกสารชิ้นนั้น พร้อมข้อความที่ปรากฏในเอกสาร ซึ่งอาจจะมีความผิดเกิดขึ้นภายใต้เรื่องการละเมิดลิขสิทธิ์ แต่ไม่สามารถที่จะดำเนินคดีอาชญากรรมในข้อหาลักทรัพย์ได้ เพราะ

การกระทำที่จะถูกระบุว่าเป็นการลักทรัพย์นั้ นต้องเป็นการกระทำที่มีผลต่อการทำลายระบบการป้องกัน หรือก่อให้เกิดความเสียหายต่อทรัพย์สินนั้น

2.1.3.3 การยักยอกข้อมูล ชุดคำสั่งหรือโปรแกรม

(ก) การเข้าถึงข้อมูลโดยปราศจากอำนาจหรือฉ้อฉล

ผู้กระทำจะแสวงหาประโยชน์จากการเข้าถึงข้อมูลหรือชุดคำสั่ง โดยไม่มีเจตนาหวังผลประโยชน์ทางการค้าเช่นการแสดงความสามารถว่าตนเองสามารถเข้าสู่ระบบได้ อาจจะแก้ไขเปลี่ยนแปลงหรือทำลายข้อมูล รวมทั้งการแพร่ไวรัสคอมพิวเตอร์

(ข) การเปิดเผยข้อมูลที่มีเจ้าของโดยปราศจากอำนาจหรือโดยฉ้อฉล

กรณีผู้กระทำจะหวังผลประโยชน์มากกว่า โดยมากจะเป็นข้อมูลทางธุรกิจ โดยเฉพาะความลับทางการค้าที่มีมูลค่ามหาศาล เช่น ฐานข้อมูลลูกค้า แผนการตลาด หรือแม้กระทั่งวิธีการผลิตสินค้าอันเป็นทรัพย์สินทางปัญญาชนิดหนึ่ง รวมถึงการทำให้ระบบคอมพิวเตอร์ของคู่แข่งทางการค้าขัดข้อง อย่างไรก็ตามยังมีการเปิดเผยหรือแสวงหาผลประโยชน์จากข้อมูลประเภทอื่น เช่น ข้อมูลทางด้านการทหารข้อมูลความลับข้าราชการ และข้อมูลอื่นๆ

2.2 ความหมายและอำนาจหน้าที่ของพนักงานสอบสวนในคดีอาญา

คำนิยามของพนักงานสอบสวน หมายถึง “ เจ้าพนักงานซึ่งกฎ หมายให้มีอำนาจและหน้าที่สำหรับทำการสอบสวน รวบรวมหลักฐานทุกอย่างเท่าที่สาม ารถจะทำได้ เพื่อประสงค์จะทราบข้อเท็จจริงและ พฤติการณ์ต่างๆ อันเกี่ยวกับความผิดที่กล่าวหา และเพื่อจะรู้และเอาตัวผู้กระทำความผิดมาดำเนินการสอบสวน ฟ้องร้องตามกฎหมาย ” [10]

อำนาจพนักงานสอบสวน

เพื่อให้พนักงานสอบสวนมีอำนาจปฏิบัติงานสอบสวนในคดีอาญา ตลอดจนการรวบรวมพยานหลักฐานได้ครบถ้วนและรวดเร็วขึ้น จึงได้บัญญัติอำนาจของพนักงานสอบสวนไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา ดังนี้

1. **ให้อำนาจสำหรับค้น** เพื่อพบสิ่งของซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำผิดหรือได้ใช้หรือสงสัยว่า ได้ใช้ในการกระทำผิดมาแล้ว หรือซึ่งอาจใช้เป็ นพยานหลักฐานในคดีได้ แต่การปฏิบัติในเรื่องนี้ต้องปฏิบัติ ให้เป็นไปตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความทางอาญา ว่าด้วยการค้น (มาตรา 132 อนุมาตรา 2)

---

[10] ยุทธพงษ์ พงษ์สวัสดิ์ , คำบรรยายวิชาการสืบสวนสอบสวน , คณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ , 2513 หน้า 38

1.1 การค้นข้อมูลในที่รโหฐาน

การค้นในที่รโหฐานต้องมีหมายค้น

กฎหมายไทยให้ความคุ้มครองแก่ประชาชนในการครอบครองอสังหาริมทรัพย์โดยปกติสุขปราศจากการรบกวน แม้จากเจ้าหน้าที่ของรัฐเองจะเข้าไปรบกวนการครอบครองดังกล่าวจะต้องมีกฎหมายให้อำนาจไว้อย่างชัดแจ้งและต้องมีคำสั่ง หรือหมายของศาลดังบทบัญญัติแห่งรัฐธรรมนูญ มาตรา 35 และมาตรา 238 [11]

การเข้าไปค้นข้อมูลคอมพิวเตอร์ที่เก็บไว้ในที่รโหฐานต้องมีหมายค้น กล่าวอีกนัยหนึ่งก็คือการค้นในที่รโหฐานจะกระทำมิได้เว้นแต่มีคำสั่งหรือหมายของศาล เพื่อให้การค้นชอบด้วยกฎหมาย สิ่งนี้แสดงให้เห็นว่ารัฐธรรมนูญฉบับปัจจุบันต้องการให้หลักประกันในความคุ้มครองความเป็นส่วนตัวและสิทธิส่วนบุคคลของประชาชน เมื่อเจ้าพนักงานจำเป็นต้องล่วงล้ำ หรือรบกวนสิทธิดังกล่าว ก็ต้องมีการกำหนดขอบเขตอำนาจในการปฏิบัติหน้าที่ของเจ้าพนักงาน หมายค้นจะเป็นตัวกำหนดขอบเขตการค้นให้สามารถค้นได้เฉพาะที่ระบุไว้ในหมายเท่านั้น เป็นการตรวจสอบการไม่ให้ปฏิบัติหน้าที่เกินความจำเป็น เพราะมิฉะนั้นแล้วจะถือเป็นการปฏิบัติหน้าที่ที่มิชอบ

สำหรับเหตุที่จะออกหมายค้นได้ ต้องพิจารณาประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 69 นั่นคือ 1. เพื่อพบและยึดสิ่งของซึ่งเป็นพยานหลักฐานประกอบการสอบสวนไต่สวนมูลฟ้องหรือพิจารณา 2. เพื่อพบและยึดสิ่งของซึ่งมีไว้เป็นความผิดหรือได้มาโดยผิดกฎหมาย หรือมีเหตุอันควรสงสัยว่าได้ใช้หรือตั้งใจใช้ในการกระทำความผิด 3. เพื่อพบและช่วยบุคคลซึ่งได้ถูกหน่วงเหนี่ยวหรือกักขังโดย มิชอบด้วยกฎหมาย 4. เพื่อพบบุคคลซึ่งมีหมายจับ 5.เพื่อพบและยึดสิ่งของตามคำพิพากษาหรือตามคำสั่งศาลในกรณีที่จะพบหรือจะยึดโดยวิธีอื่นไม่ได้แล้ว

ประเด็นที่ต้องวิเคราะห์คือข้อมูลคอมพิวเตอร์ที่ต้องการค้นนั้นเป็น “สิ่งของ” ที่เจ้าพนักงานจะทำการรวบรวมหลักฐานได้หรือไ ม่ ซึ่งเมื่อพิจารณานิยามตามประมวลกฎหมายวิธีพิจารณาความอาญาแล้ว สิ่งของ หมายถึง สังหาริมทรัพย์ซึ่งอาจใช้เป็นพยานหลักฐานในคดีได้ รวมทั้งจดหมาย โทรเลขและเอกสารอื่นๆ แต่ข้อมูลคอมพิวเตอร์เป็นสิ่งไม่มีรูปร่าง อยู่ในรูปแม่เหล็กไฟฟ้า ไม่เป็นทรัพย์ จะเกิดปัญหาหรือไม่

ในเรื่องนี้ เนื่องด้วยประมวลกฎหมายวิธีพิจารณาความอาญาไม่ต้องตีความเคร่งครัดเหมือนประมวลกฎหมายอาญา จึงใช้วิธีการตีความเทียบเคียงได้ นอกจากนี้ พระราชบัญญัติว่า

---

[11] รัฐธรรมนูญ มาตรา 35 บัญญัติว่า “การเข้าไปในเคหสถาน โดยปราศจากการยินยอมของผู้ครอบครองหรือการตรวจค้นเคหสถานจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย” และมาตรา 238 บัญญัติว่า “ในคดีอาญา การค้นในที่รโหฐานจะกระทำมิได้ เว้นแต่จะมีคำสั่งหรือหมายของศาล หรือมีเหตุให้ค้นได้โดยไม่ต้องมีคำสั่งหรือหมายศาล ทั้งนี้ตามที่กฎหมายบัญญัติ”

ด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ .ศ.2544 ก็ได้รับรองสถานะข้อมูลอิเล็กทรอนิกส์เทียบเท่าพยานวัตถุ และพยานเอกสารอีกทางหนึ่งด้วย

อย่างไรก็ตาม อีกประเด็นที่ต้องวิเคราะห์คือ เมื่อการค้นในที่รโหฐานจำต้องมีหมายค้น อาจเป็นอุปสรรคและเกิดปัญหาในทางปฏิบัติ เนื่องจากการขอหมายศาลเป็นกระบวนการที่ต้องใช้ระยะเวลา ในระหว่างรอการออกหมายค้นจากศาล หรือระหว่างแสดงหมายค้นให้ เจ้าของบ้านหรือผู้ต้องสงสัยทราบ ผู้ต้องสงสัยอาจทำลายหลักฐาน แก้ไขข้อมูล หรือลบข้อมูลได้ในเวลาเพียงเสี้ยวนาที ในความจำเป็นเร่งด่วนเช่นนี้จะสามารถค้นโดยไม่มีหมายค้นได้หรือไม่

ในมาตรา 92 ระบุว่า ห้ามมิให้มีการค้นในที่รโหฐานโดยไม่มีหมายค้น เว้นแต่พนักงานฝ่ายปกครองหรือตำรวจเป็นผู้ค้น และในกรณี 1.เมื่อมีเสียงร้องให้ช่วยมาจากข้างในที่รโหฐาน 2.เมื่อปรากฏความผิดซึ่งหน้า กำลังกระทำลงในที่รโหฐาน 3.เมื่อบุคคลที่ได้กระทำผิดซึ่งหน้าขณะที่ถูกไล่จับหนีเข้าไปหรือมีเหตุอันแน่นแฟ้นควรสงสัยว่าได้เข้าไปซ่อนตัวอยู่ในที่รโหฐา นนั้น 4.เมื่อมีความสงสัยตามสมควรว่าสิ่งของที่ได้มาโดยการกระทำผิดได้ซุกหรืออยู่ในนั้น ประกอบกับต้องมีเหตุอันควรเชื่อว่า เนื่องจากการเนิ่นช้ากว่าจะเอาหมายค้นมาได้ สิ่งของนั้นจะถูกโยกย้ายเสียก่อน 5.เมื่อที่รโหฐานนั้น ผู้จะต้องถูกจับเป็นเจ้าของบ้านและการจับนั้ นมีหมายจับ หรือจับตามมาตรา 78

รัฐธรรมนูญ ฉบับปัจจุบัน ได้สร้างหลักประกันเพื่อให้ความคุ้มครองสิทธิเสรีภาพของประชาชนโดยมีบัญญัติให้หมายค้นต้องออกโดยศาลเท่านั้น เพื่อให้พ้นจากการถูกตรวจค้นที่ไม่เป็นธรรม แต่กระนั้นก็ยังมีข้อยกเว้นที่สงวนไว้ให้รัฐสามารถจำกัดสิทธิ เสรีภาพประชาชนได้บางประการตามความจำเป็นเพื่อประโยชน์ของประชาชนส่วนใหญ่ แต่ทั้งนี้ก็ต้องอาศัยอำนาจตามที่กฎหมายบัญญัติไว้เท่านั้น

ในกรณีการค้นข้อมูลคอมพิวเตอร์ เจ้าพนักงานอาจสามารถอ้างเหตุตามมาตรา 92(2) และ92(4) แต่ก็ไม่ใช่ทุกครั้งที่การเข้าค้นพยานหลักฐานจะ อ้างมาตราดังกล่าวได้เสมอ เพราะต้องวิเคราะห์ข้อเท็จจริงเป็นกรณีๆไปด้วย

1.2 การค้นต้องระบุสิ่งของ และสถานที่ที่จะค้น

กฎหมายได้กำหนดไว้ว่า กรณี ออกหมายค้น ให้ระบุสิ่งของที่ และสถานที่ที่จะค้น ซึ่งเกิดปัญหาว่าจะระบุอย่างไร เพราะข้อมูลคอมพิวเตอร์ไม่สามารถระบุ ได้ว่าอยู่ในรูปแบบใดและประกอบด้วยสิ่งใดบ้าง เนื่องจากมีลักษณะเป็นเพียงคลื่นแม่เหล็กไฟฟ้า ไม่สามารถจับต้องได้ ส่วนสถานที่ที่จะค้นนั้น ก็เป็นการยากที่จะระบุว่าเก็บไว้ที่ใด โดยเฉพาะอย่างยิ่งหากเป็นการค้นข้อมูลที่ต้องเจาะเข้าไปในระบบข้อมูล เช่น ในเครือข่ายอิน เตอร์เน็ต ซึ่งอาจมีแหล่งข้อมูลต้นทางอยู่ในต่างประเทศ จึงเป็นปัญหาว่าหมายค้นจะระบุอย่างไรและจะค้นไปในข้อมูลที่ต่างประเทศได้หรือไม่

1.3 การค้นในที่รโหฐานต้องจำกัดสิ่งของและบุคคล

การค้นจะกระทำได้แต่เฉพาะเพื่อหาตัวบุคคล หรือสิ่งของที่ต้องการเท่านั้น ซึ่งปัญหาก็คือ หากในการค้นได้พบการกระทำความผิดฐานอื่น ซึ่งไม่เกี่ยวกับความผิดที่มีการออกหมายค้น จะสามารถดำเนินการกับสิ่งที่พบในขณะนั้นได้หรือไม่ เพราะอาจถือเป็นการดำเนินการเกินกว่าที่กำหนดในหมายค้นซึ่งขัดต่อรัฐธรรมนูญ

1.4 การค้นในที่รโหฐานต้องกระทำเวลากลางวัน

ตามมาตรา 96 การค้นในที่รโหฐานต้องทำในเวลากลางวัน คือ ระหว่างพระอาทิตย์ขึ้นและตก ทั้งนี้เพราะที่รโหฐานควรเป็นที่ที่ทุกคนอยู่ได้อย่างสงบ และปลอดจากการรบกวนจากภายนอกรวมทั้งจากอำนาจรัฐ อีกทั้งการค้นในเวลากลางคืนอาจนำผลร้ายมาให้ประชาชนที่ถูกค้นได้ เช่น อาจเอาของร้ายมาซุกซ่อนโดยเจ้าของบ้านไม่รู้เห็นก็ได้ ยกเว้น

(1) เมื่อลงมือค้นแต่ในเวลากลางวัน ถ้ายังไม่เสร็จจะค้นต่อไปในเวลากลางคืนก็ได้

(2) ในกรณีฉุกเฉินอย่างยิ่ง [12] หรือซึ่งมีกฎหมายอื่นบัญญัติให้ค้นได้เป็นพิเศษ

แต่อาชญากรรมคอมพิวเตอร์นั้น สามารถกระทำได้ตลอด 24 ชั่วโมง และผลของการกระทำผิดก็สามารถสร้างความเสียหายให้แก่บุคคลได้โดยไม่เลือกเวลา ในขณะที่การปราบปรามอาชญากรรมคอมพิวเตอร์ก็ต้องใช้ความรวดเร็วให้ทันกับการกระทำผิด เพื่อป้องกันความเสียหายที่จะเกิดขึ้นได้ทันท่วงทีเช่นกัน ดังนั้นการต้องรอให้พระอาทิตย์ขึ้น จึงกลายเป็นอุปสรรคอีกข้อหนึ่งที่ทำให้การปราบปรามไม่มีประสิทธิภาพ เพราะหากในขณะที่มีกระทำความผิดเป็นเวลากลางคืนซึ่งตำรวจ ไม่สามารถเข้าไปค้นได้ ต้องรออยู่ก่อน ผู้ต้องสงสัยอาจรู้ตัว และอาจลบ ทำลาย แก้ไข หรือ เปลี่ยนแปลงพยานหลักฐานได้โดยใช้เวลาอันสั้น ยากที่จะเหลือร่องรอย ไว้ให้ติดตามได้ และหากเจ้าพนักงานจะอ้างมาตรา 96 (2) มาใช้ด้วยเกรงว่าพยานหลักฐานที่สำคัญจะสูญหายและส่งผลเสียต่อคดีอย่างมากก็ไม่แน่นอนเสมอไปว่าจะใช้ได้ทุกครั้ง เนื่องจากต้องวิเคราะห์ข้อเท็จจริงเป็นกรณีๆไปเช่นเดียวกับการพิจารณาเรื่องการค้นโดยไม่ต้องมีหมายค้น

1.5 การค้นข้อมูลส่วนบุคคล

ข้อมูลบางอย่าง เจ้าหน้าที่ต้องการเข้าถึงเพื่อประโยชน์ในการรวบรวมพยานหลักฐาน อาจเป็นข้อมูลที่เป็นความลับส่วนบุคคล หรือข้อมูลที่เป็นความลับทางธุรกิจของบริษัทสำนักงานต่างๆ ดังนั้น การพยายามเข้าถึงข้อมู ลนั้นๆ โดยเจ้าของไม่ยินยอม อาจถือเป็นการละเมิดสิทธิส่วนบุคคลได้

---

[12] กรณีฉุกเฉินอย่างยิ่ง หมายความว่า ถ้าไม่กระทำการค้นในเวลากลางคืนจะเกิดอันตรายแก่ชีวิตหรือร่างกายของบุคคลที่ต้องการค้นให้พบตัว หรือบุคคลนั้นอาจจะหลบหนีไปเสียก็ได้ หรือพยานหลักฐานอาจถูกทำลาย ทั้งคดีนั้นจะต้องมีลักษณะร้ายแรงไม่ใช่คดีเล็กๆน้อยๆด้วย ดูในหยุด แสงอุทัย, ประมวลกฎหมายวิธีพิจารณาความอาญา ศึกษาทางคำพิพากษาศาลฎีกา (กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2538), น. 706.

2. **ให้มีอำนาจออกหมายเรียกบุคคล** ซึ่งครอบครองสิ่งของที่อาจใช้เป็นพยานหลักฐานได้ แต่บุคคลผู้ได้รับหมายดังกล่าวไม่จำเป็นต้องมาเอง เมื่อได้จัดส่งสิ่งของนั้นมาตามหมายเรียกแล้ว (มาตรา 132 อนุ 3)
3. **ให้มีอำนาจยึดไว้ซึ่งสิ่งของที่ค้นพบหรือส่งมาดังกล่าว** (มาตรา 132 อนุ 2 และ อนุ 3)

การยึดของให้ปฏิบัติให้เป็นไปตามระเบียบที่กรมตำรวจและกระทรวงมหาดไทยได้วางไว้ จะต้องพิจารณาถึงความจำเป็นที่จะต้องยึดไว้ (ประกอบด้วย) และต้องเก็บรักษาสิ่งของนั้นให้เป็นไปตามระเบียบ (มาตรา 132 อนุ 4)

4. **ให้มีอำนาจ " หมายเรียกผู้เสียหาย หรือบุคคลใด** ซึ่งมีเหตุอันควรเชื่อว่าถ้อยคำของเขาอาจเป็น ประโยช น์แก่คดี ให้มาตามเวลาและสถานที่ในหมาย และให้ถามปากคำบุคคลนั้นไว้ "

ทั้งนี้ เนื่องจากผู้เสียหายบางคนไม่ยอมไปให้การต่อพนักงานสอบสวน หรือบุคคลผู้รู้เห็นไม่อยากไปเป็นพยานจึงจำ เป็นต้องให้ช่วยรักษาประโยชน์ ของส่วนรวมไว้ ผู้ที่ไม่มาตามหมายเรียกย่อมมีความผิดฐานขัดคำสั่งเจ้าพนักงานตามประมวลกฎหมายอาญา และผู้ที่มีอำนาจออกหมายเรียกต้องเป็นหัวหน้าพนักงานสอบสวนท้องที่นั้น (มาตรา 133)

5. **ให้มีอำนาจในการที่จะจัดการแก่ผู้กระทำความผิดหรือเชื่อว่ าได้กระทำผิด (จับ, ควบคุมและปล่อย) ดังนี้**
    ก. จับหรือจัดการให้จับบุคคลนั้น จะจับด้วยตนเองหรือจัดการให้เจ้าพนักงานอื่นจับก็ได้
    ข. ควบคุมหรือจัดการให้ควบคุมผู้นั้นไว้หรือสั่งให้ผู้อื่นควบคุมแทน
    ค. ในระหว่างที่ควบคุมผู้กระทำผิดไว้ ให้มีอำนาจปล่อยชั่วคราว (โดยไม่มีประกัน มีประกัน และมีหลักประกัน) หรือปล่อยไปตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาในเรื่องนั้น ๆ (มาตรา 136)
6. **ให้มีอำนาจ " ที่จะสั่งมิให้บุคคลออกไปจากสถานที่ "**

อำนาจนี้เพื่อประโยชน์ในเวลาที่พนักงานสอบสวนออกไปสอบสวน ณ ที่เกิดเหตุบางกรณีมีความจำเป็นอย่างยิ่งที่จะต้องสั่งบุคคลใดอยู่ประจำที่ หรือมิให้ออกไปที่อื่น เพื่อประโยชน์แห่งการสอบสวนก็ให้มีอำนาจในการปฏิบัติได้เท่าที่จำเป็น (มาตรา 137)

7. **ให้มีอำนาจ " ที่จะสอบสวนความเป็นมาแห่งชีวิตและความประพฤติอันเป็นอาจินของผู้ต้องหา " ได้**

ทั้งนี้ เนื่องจากในการสอบสวน คดีบางเรื่อง เช่นการสอบสวนคดีที่มีความผิดในทางการเมืองหรือการสอบสวนคนต่างด้าวกระทำความผิดอันต้องดำเนินการพิจารณาเนรเทศด้วย ตามข้อบังคับการสอบสวนจะต้องสอบสวนประวัติความเป็นมาแห่งชีวิต และความประพฤติประกอบไว้ในการสอบสวนนั้นด้วย ก็มีความจำเป็นเกิดขึ้นหรือแม้แต่คดีอาญาธรรมดาบางเรื่อง

หากผู้สอบสวนได้สอบถึงความประพฤติและประวัติความเป็นมาแห่งชีวิตแต่หนหลังก็อาจทำให้การวินิจฉัย หรือดำเนินคดีนั้นได้ถูกทาง หรือใกล้เคียงมาก จึงมีความจำเป็นต้องรับอำนาจนี้ด้วย (มาตรา 138)

2.3 การรับฟังหรือการอ้างพยานหลักฐานในคดีอาญา

พยานหลักฐานสามารถแสดงและอธิบายหรือชี้ให้เห็นข้อเท็จจริง พยานหลักฐานจึงเป็นสิ่งที่สำคัญที่สุด มีวิธีการอย่างไร ศาลจึงจะเชื่อว่าพยานหลักฐานที่นำมาเสนอนั้น เป็นข้อมูลหรือหลักฐานที่มิได้เปลี่ยนแปลงแก้ไข และทำให้พยานประเภทนี้มีความหน้าเชื่อถือเพียงพอที่ศาลจะลงโทษจำเลยได้ ซึ่งพยานหลักฐานที่รับฟังได้จะต้องเป็นพยานที่ได้มาโดยสุจริต ศาลจะไม่รับฟังก็ต่อเมื่อพยานหลักฐานนั้นได้มาโดยวิธีการที่มิชอบ อาทิ เกิดจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง [13] ดังนั้นในส่วนของการนำเสนอพยานหลักฐานที่ได้มาโดยมิชอบของศาลไทย สามารถสรุปได้ดังนี้

2.3.1 การค้น การจับกุม และการได้หลักฐานมาใช้เป็นพยานหลักฐานในคดี แต่เดิมศาลไทยเคร่งครัดมากกับหลักการรับฟังพยานหลักฐานที่ได้มาโดยการตรวจค้นที่ไม่ชอบด้วยกฎหมาย โดยถึงกับพิพากษายกฟ้อง เพียงเพราะมีเหตุว่าการค้นทำให้ได้ทรัพย์ที่ทำหรือมีไว้เป็นความผิดนั้นไม่ชอบด้วยกฎหมายเพราะเหตุไม่มีหมายค้น และไม่ใช่กรณีฉุกเฉิน ผู้ ทำการตร วจค้นก็ไม่ใช่นายตำรวจชั้นผู้ใหญ่ [14] ต่อมาศาลฎีกาเปลี่ยนแนววินิจฉัยเป็นในทางตรงข้ามกับแนวเดิม เช่น ว่าข้อปฏิบัติการค้นนั้นเป็นแต่กำหนดวิธีการอันหนึ่งที่เจ้าพนักงานจะต้องทำ มิได้บังคับว่าถ้าไม่ปฏิบัติตามแล้วจะไม่ให้เสียเลยว่าได้ค้นของกลางคือจักรยาน 3 ล้อที่ถูกลักไปได้ที่บ้านจำเลย และลงโทษจำเลย [15] และศาลวินิจฉัยอีกคดีว่า การจับกุมกับการสอบสวนเป็นการดำเนินการคนละชั้นตอนกัน เมื่อการสอบสวนได้ดำเนินการไปโดยชอบด้วยกฎหมายแล้ว แม้ข้อเท็จจริงจะฟังได้ว่า การจับกุมมิชอบด้วยกฎหมายก็เป็นเรื่องจะว่ากล่าวกันอีกส่วนหนึ่งต่างหาก หาทำให้การสอบสวนซึ่งชอบด้วย กฎหมาย แล้วนั้นกระทบกระเทือนถึงการฟ้องคดีอาญา ไม่ [16]

---

[13] ดูประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 234 วรรคสอง

[14] ดูคำพิพากษาฎีกาที่ 857/2482

[15] ดูคำพิพากษาฎีกาที่ 837/2483

[16] ดูคำพิพากษาฎีกาที่ 2699/2516

2.3.2 การได้หลักฐานมาโดยการหลอกลวงและล่อซื้อ ศาลไทยไม่เคร่งครัดกรณีดังกล่าว เพราะปรากฏแนววินิจฉัยของศาลสูงเสมอมาว่า แม้เป็นการล่อลวงซื้อหรือถึงขั้นให้เจ้าพนักงานตำรวจปลอมตัวเป็นผู้ใช้บริการแล้วเข้าร่วมประเวณีกับจำเลย ศาลไทยยอมรับฟังพยานหลักฐานลงโทษ จำเลย โดยมีแนววินิจฉัยดังต่อไปนี้

คำพิพากษาฎีกาที่ 1163/2518 การที่ตำรวจนายหนึ่งขอร่วมประเวณีกับจำเลยที่ 2 เพื่อพิสูจน์คำร้องเรียนว่ามีการค้าประเวณีในสถานที่เกิดเหตุจริงหรือไม่ จำเลยที่ 2 ยอมร่วมประเวณีและรับเงินจากตำรวจ ผู้นั้น ไม่เป็นการแสวงหาพยานหลักฐานมาโดยไม่ชอบ

คำพิพากษาฎีกาที่ 2572 /2540 การล่อซื้อเป็นเพียงวิธีการแสวงหาพยานหลักฐานมิใช่พยานหลักฐานที่เกิดขึ้นโดยมิชอบ

2.4 ความหมายและรูปแบบของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

ข้อมูลอิเล็กทรอนิกส์มีประโยชน์ในหลาย ๆ ด้านในทางกฎหมายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ .ศ. 2544 สรุปได้ว่า “ข้อมูลอิเล็กทรอนิกส์ [17]” เป็นเรื่องราวข้อเท็จจริงไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้ ที่ได้สร้าง ส่ง รับ เก็บรักษา หรือปร ะมวลผลด้วยวิธีประยุกต์ ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้าหรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็กหรืออุปกรณ์ที่เกี่ยวกับการประยุกต์ใช้วิธีต่างๆ ทำให้ความหมายของข้อมูลอิเล็กทรอนิกส์กว้างข วางครอบคลุมไปถึงข้อมูลทุกชนิดที่ทำขึ้นด้วยวิธีการทางอิเล็กทรอนิกส์ ไม่ใช่เพียงข้อความตัวอักษร รหัสหรือตัวเลขเท่านั้นที่จะเป็นข้อมูลอิเล็กทรอนิกส์ แต่ครอบคลุมไปถึงเสียงด้วย อย่างไรก็ตามข้อมูลอิเล็กทรอนิกส์ต้องมีความหมายและได้สร้าง ส่ง รับ เก็บรักษา หรือประม วลผลด้วยวิธีทางอิเล็กทรอนิกส์ ได้ยอมรับให้ข้อมูลอิเล็กทรอนิกส์สามารถใช้เป็นพยานหลักฐาน การจัดเก็บข้อมูลในระบบอิเล็กทรอนิกส์เป็นประโยชน์ในการประมวลผลข้อมูลด้วยคอมพิวเตอร์ นอกจากนี้ด้วยลักษณะเฉพาะของข้อมูลอิเล็กทรอนิกส์ที่ปรากฏข้อความขึ้นได้นั้น จำต้องใช้อุปกรณ์คอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ประกอบกัน ในปัจจุบันมีการใช้ข้อมูลอิเล็กทรอนิกส์กันอย่างแพร่หลาย ข้อมูลอิเล็กทรอนิกส์ที่ไม่มีระบบป้องกันที่ดีเพียงพออาจถูกบุคคลอื่นนำไปใช้ก่อให้เกิดความเสียหายได้ โดยเฉพาะอย่างยิ่งข้อมูลอิเล็กทรอนิกส์ที่ใช้

---

[17] พรทิพย์ ตัณฑวนันท์, “อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์ .” วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ ธรรมศาสตร์, 2548 น. 7

ประมวลผลในธุรกรรมต่างๆ จึงมีผู้ที่ใช้ข้อมูลอิเล็กทรอนิกส์ไม่ว่าจะเป็นการเข้าถึงข้อมูลอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต การเปิดเผยข้อมูล อิเล็กทรอนิกส์ การฉ้อโกงทางข้อมูลอิเล็กทรอนิกส์

2.4.1 รูปแบบของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

2.4.1.1 การใช้ข้อมูลเป็นพยานหลักฐาน

ข้อความที่ทำให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ได้มีการรับรองสถานะหรือผลทางกฎหมาย โดยมาตรา 7 แห่งพระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ .ศ.2544 บัญญัติว่า ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปข้อมูลอิเล็กทรอนิกส์ โดยเป็นการกำหนดหลักการพื้นฐานมิให้มีการเลือกปฏิบัติระหว่างสิ่งที่จัดทำขึ้นในรูปขอ งกระดาษทั้งในรูปของหนังสือ หลักฐานเป็นหนังสือหรือต้นฉบับกับสิ่งที่จัดทำขึ้นรูปของข้อมูลอิเล็กทรอนิกส์

อย่างไรก็ตาม แม้จะมีบทบัญญัติในมาตรา 7 รับรองสถานะของข้อมูลอิเล็กทรอนิกส์ไว้อยู่แล้วก็ตาม แต่หากในกรณีที่ต้องมีการจัดทำหนังสือ หลักฐานเป็นหนังสือหรือเอกส ารให้อยู่ในรูปของ ข้อมูลอิเล็กทรอนิกส์ การจัดทำให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์จะต้องอยู่ภายใต้เงื่อนไขของมาตรา 8 ด้วยว่า เมื่อได้มีการจัดทำหนังสือ หลักฐานเป็นหนังสือหรือเอกสารให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ข้อมูลอิเล็กทรอนิกส์นั้น จะต้องสามารถเข้า ถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง หลักการที่กำหนดให้ต้องสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง คำว่า “สามารถเข้าถึงได้” หมายความรวมถึงข้อความที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ที่สามารถอ่านออกได้โดยการใช้โปรแกรมหรือซอฟต์แวร์ และรวมถึงข้อมูลอิเล็กทรอนิกส์ที่จำเป็นต้องแปลงข้อมูลนั้นให้สามารถอ่านเข้าใจได้ด้วย นอกจากนั้นคำว่า “นำกลับมาใช้ได้ ” นั้นมิได้ครอบคลุมเฉพาะมนุษย์เท่านั้น ที่ใช้ได้แต่ยังหมายความรวมถึงการใช้โดยการประมวลผลด้วยเครื่องคอมพิวเตอร์ด้วย ส่วนความหมายของคำว่า “ความหมายไม่เปลี่ยนแปลง ” ต้องมีลักษณะถาวรไม่มีการแก้ไขเปลี่ยนแปลง กล่าวคือ ข้อมูลนั้นต้องไม่สร้างขึ้นโดยใช้มาตรฐานที่ต่ำเกินไปและข้อมูลอิเล็กทรอนิกส์นั้น ต้องสามารถอ่านและเข้าใจได้ [18] โดยแบ่งข้อมูลที่เป็นพยานหลักฐานได้ 2 ข้อ ดังนี้

---

[18] ชัยวัฒน์ วงศ์วัฒนศานต์, ทวีศักดิ์ กออนัตกูล, สุรางคณา แก้วจำนงค์, คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, (กรุงเทพ, สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ , 2545) หน้า 16

2.4.1.1.1 ข้อมูลอิเล็กทรอนิกส์ในสถานะพยานเอกสาร

พยานเอกสาร หมายถึง ข้อความหรือเครื่ องหมายใดๆ ที่ปรากฏอยู่บนกระดาษหรือวัตถุอื่นใด ซึ่งคู่ความเสนอต่อศาลเพื่อใช้ความหมายของข้อความหรือเครื่องหมายนั้นพิสูจน์ข้อเท็จจริง [19]

กฎหมายแม่บทของ UNCITRAL แม้จะเป็นกฎหมายเกี่ยวกับพาณิชย์อิเล็กทรอนิกส์ แต่จะนำมาเปรียบเทียบและวิเคราะห์ในคดีอาญาได้บ้าง เพราะสถานะของข้อมูลอิเล็กทรอนิกส์ในคดีแพ่ง และในคดีอาญานี้ไม่แตกต่างกันในเรื่องของประเภท แตกต่างกันตรงวิธีการนำเสนอเท่านั้น ในแม่บทของ UNCITRAL ไม่แต่วางหลักไว้ชัดเจนว่าข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลข่าวสารตามนัยมาตรา 2 ที่กล่าวมาแล้วเป็นพยานเอกสารหรือวัตถุ เพียงแต่มาตรา 5 ของ Model law บัญญัติเป็นหลักว่าข้อมูลข่าวสาร (data message) จะต้องไม่ปฏิเสธความสมบูรณ์หรือปฏิเสธการบังคับใช้ในทางกฎหมาย โดยที่มันเป็นเพียง data message ซึ่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ก็บัญญัติไว้ตรงกันเป็นมาตรา 11 ดังนี้

Article 5. Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

มาตรา 11 ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายเพียงเพราะว่าเป็นข้อมูลอิเล็กทรอนิกส์

นอกจากนี้ในมาตรา 9 ของ Model law ย้ำความในมาตรา 5 ที่ห้ามมิให้รับฟังพยานหลักฐานอันเกิดจากสื่ออิเล็กทรอนิกส์ โดยเหตุผลเพียงว่าเป็น data message ซึ่งมาตรา 9 บัญญัติว่า

(1) ในการดำเนินกระบวน พิจารณาตามกฎหมาย มิให้นำข้อกำห นดว่าด้วยพยานหลักฐานมาใช้บังคับ เพื่อปฏิเสธมิให้รับฟังข้อมูลข่าวสารเป็นพยานหลักฐาน

(ก) เพราะเหตุว่าพยานหลักฐานที่นำเสนอนั้นเป็นสารสนเทศ หรือ

(ข) เพราะเหตุว่าไม่ได้อยู่ในรูปต้นฉบับ หากข้อมูลข่าวสารนั้นเป็นพยานหลักฐานที่ดีที่สุดที่นำเสนออาจจะหาได้ตามสมควร

(2) ให้ข้อมูลที่อยู่ในรูปของข้อมูลข่าวสารได้รับน้ำหนักในฐานะพยานหลักฐานตามสมควร ในการชั่งน้ำหนักพยานหลักฐานของข้อมูลข่าวสาร ในคำนึงถึงความน่าเชื่อถือของวิธีการในการสร้าง เก็บรักษา หรือสื่อสารข้อมูลข่าวสารนั้น ความน่าเชื่อถือของวิธีการรักษาความแท้จริงของข้อมูล วิธีการแสดงถึงตัวผู้ส่ง และปัจจัยที่เกี่ยวข้องอื่นๆ

---

[19] เพิ่งอ้าง, หน้า 52

มาตรา 9 นี้เป็นเพียงบทบัญญัติว่าข้อมูลจากสื่ออิเล็กทรอนิกส์ต้องใช้เป็นพยานหลักฐานได้ และข้อมูลประเภทนี้มีน้ำหนัก แต่การจะทำลายน้ำหนักข้อมูลประเภทนี้ขึ้นอยู่กับวิธีการเกิดขึ้น การเก็ บรักษา และการส่งต่อข้อมูล แต่อย่างไรก็ตามก็ดี มาตรา 9 ไม่ได้กระทบถึงอำนาจของศาลที่จะปฏิเสธไม่รับฟังพยานหลักฐานประเภทนี้โดยเหตุอื่น เช่น โดยที่เป็นพยานบอกเล่า (Hearsay) เพราะข้อมูลจากสื่ อิเล็กทรอนิกส์ทุกประเภท แม้ไม่ ได้เป็นพยานบอกเล่าเสมอไป แต่ก็มีข้อมูลไ ม่น้อยที่มีลักษณะเป็นพยานบอกเล่า สำหรับประเทศที่มีกฎหมายห้ามรับฟังพยานบอกเล่าก็ดี ย่อมมีปัญหาที่ต้องพิจารณาในประเด็นข้อนี้

ปัจจุบันข้อกำหนดว่าด้วยการรับฟังข้อ มูลคอมพิวเตอร์ตามข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศข้อ 33- 36 วางหลักให้ศาลรับฟัง พยานหลักฐานอิเล็กทรอนิกส์ได้ แต่ต้องเป็นข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์ หรือประมวลผลโดยเครื่องคอมพิวเตอร์ พยานหลักฐานประเภทนี้จะจำกัดเฉพาะข้อมูลที่บันทึกไว้ หรือข้อมูลที่ประมวลผลได้ คำว่า “บันทึก” ย่อมหมายถึง การบันทึกข้อมูลข่าวสารเก็บไว้ในลักษณะที่สามารถตรวจสอบหรือนำกลับมาดูได้อีกครั้งหนึ่ง ส่วนคำว่า “ประมวลผล ” ย่อมหมายถึง การคำนวณทางคณิตศาสตร์จากข้อมูลที่ใส่เข้าไปให้ประมวล การรับฟังข้อมูล ลักษณะนี้จึงมีความหมายเท่ากับการยอม รับการประมวลผล โดยเครื่องมือทางวิทยาศาสตร์ และการเสนอข้อมูลนั้นเป็นการเสนอเพื่อ พิสูจน์สิ่งที่บันทึกไว้หรือสิ่งที่ประมวลผลได้ ดังนั้นหากมีการส่ง PrintOuts หรือ Computer Print-Outs ของคอมพิวเตอร์เพื่อการพิสูจน์ยืนยันว่าได้มีการบันทึกข้อมูลไว้ในคอมพิวเตอร์ เพื่อสนับสนุนข้อมูลที่ได้สื่อสารไปแล้ว ย่อมอยู่ในบังคับของข้อกำหนดคดีทรัพย์สินทางปัญญาฯ ข้อ 33 นั้นเอง [20]

แนวความคิดของนัก กฎหมายไทยในส่วนที่เกี่ยวกับพยานเอกสารนั้นจะหมายถึง การพิสูจน์ของข้อความที่เป็นภาษาหนังสือเป็นหลัก โดยไม่ต้องพิจารณาว่าสิ่งที่บันทึกไว้นั้นจะเป็นกระดาษหรือวัตถุอื่นใด ดังนั้น การพิสูจน์ข้อความที่บันทึกไว้ในเครื่องคอ มพิวเตอร์เป็นการนำเสนอพยานเอกสาร อย่างไรก็ตามแนวความคิดนี้ใช้ไม่ได้เมื่อเป็นกรณีที่เป็นการบันทึกภาพหรือภาพวิ่งซึ่งไม่ได้สื่อภาษาหนังสือ

จากที่กล่าวมานี้ ไม่ว่าพยานที่บันทึกโดยเครื่องคอมพิวเตอร์จะมุ่งพิสูจน์ข้อความที่เป็นภาษาหนังสือ หรือพิสูจน์การประมวลผลข องเครื่องคอมพิวเตอร์ พยานที่บันทึกโดยเครื่องคอมพิวเตอร์ก็มีลักษณะที่แตกต่างจากพยานเอกสาร ทั้งในเรื่องของต้นฉบับและสำเนาของพยานที่บันทึกโดยเครื่องคอมพิวเตอร์ แม้จะมีการ Printout ออกมาจากเครื่องคอมพิวเตอร์ได้อย่างพยานเอกสารก็ตาม

---

[20] พรเพชร วิชิตชลชัย, “บทวิเคราะห์เรื่อง : การรับฟังข้อมูลจากสื่ออิเล็กทรอนิกส์เป็นพยานหลักฐานในคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ,” วารสารกฎหมายทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ , (รวบรวมโดยศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ), หน้า 222

2.4.1.1.2 ข้อมูลอิเล็กทรอนิกส์สถานะพยานวัตถุ

พยานวัตถุ หมายถึง สิ่งของใดๆ ที่คู่ความอ้างอิงให้ศาลตรวจดู เพื่อประโยชน์แก่คดีของตน สิ่งที่เป็นพยานวัตถุ โดยมากเป็นวัตถุที่อาจรับรู้ได้โดยการเห็น หรือโดยประสาทตา แต่ความจริงสิ่งที่เป็นพยานวัตถุอาจเป็นสิ่งรับรู้ได้โดยประสาทสัมผัสอื่น ๆ ก็ได้ เช่น สัมผัสรูปโดยการตรวจดูขนาด รูปทรง สี สัมผัสกลิ่น สัมผัสเสียง เป็นต้น

การเสนอพยานหลักฐานต่อศาลในกรณีข้อมูลนั้นเป็นข้อมูลจากสื่ออิเล็กทรอนิกส์หรือมีการบันทึกบนสื่ออิเล็กทรอนิกส์ ซึ่งความจริงแล้วสื่ออิเล็กทรอนิกส์มิได้จำกัดเฉพาะคอมพิวเตอร์เท่านั้น เพราะมีการบันทึกข้อมูลในสื่ออื่นๆ มาแล้ว เช่น กล้องถ่ายรูป กล้องถ่ายภาพยนต์ วีดีทัศน์ ฟิลม์ เครื่องบันทึกเสียง ซึ่งนับได้ว่าเป็นวัตถุพยาน แต่สื่ออิเล็กทรอนิกส์คอมพิวเตอร์มีลักษณะพิเศษและยังมีประสิทธิภาพมากกว่าเดิม เพราะการเดินทางของสื่อนั้นไม่มีขอบเขตจำกัดไร้พรมแดนและมีผลในทันที นอกจากนี้ยังมีประสิทธิภาพในการประมวลผลโดยเฉพาะในทางคณิตศาสตร์และในทางวิทยาศาสตร์อื่นๆ โดยสามารถแสดงคำตอบและผลลัพธ์ออกมาซึ่งอาจค้นดูได้ และอ่านเป็นภาษามนุษย์ได้ด้วย

ตัวอย่างคดีที่ศาลฎีกาไทยเคยมีคำวินิจฉัยว่าพยานหลักฐานที่เป็นข้อมู ลที่บันทึกไว้ในสื่อที่ใช้อิเล็กทรอนิกส์บางอย่างเป็นพยานวัตถุ เช่น แถบบันทึกเสียงเป็นพยานวัตถุ จากคำพิพากษานี้ แถบบันทึกเสียงอาจตรวจดูด้วยการใช้ประสาทหูรับฟังจึงเป็นพยานวัตถุ เทปบันทึกเสียง ฟิลม์ที่ถ่ายภาพแล้ว และภาพถ่าย ซึ่งบางกรณีอาจถือว่าเป็นเอกสาร เพราะสามารถถ่ายทอดข้อความทำ นองเดียวกับเอกสารนั้น แต่ปกติ จะถือเป็นพยานวัตถุ โดยเฉพาะอย่างยิ่งเทปบันทึกเสียงที่แสดงให้เห็นถึงการพูดของบุคคลว่าเขามีสำเนียงหรือน้ำเสียงอย่างไรนั้นถือว่าเป็นพยานวัตถุ

นอกจากนี้ศาลฎีกาไทยเคยมีคำวินิจฉั ยรับฟังพยานหลักฐานที่เป็นภาพถ่าย บันทึกความจำที่มีลักษณะเหมือนโพยสลากกินรวบที่คนเดินโพยหรือเจ้ามือเป็นผู้กระทำ เพื่อส่งต่อเจ้ามือเหนือขึ้นไปอีกทอด แม้รับฟังเป็นพยานเอกสารไม่ได้ แต่ก็ฟังเป็นพยานวัตถุเกี่ยวกับการเล่นพนันได้ นั้นเป็นการแสดงให้เห็นว่าการนำเอกสารมาสืบหากประสงค์จะแสดงให้เป็นว่ า ได้มีการทำเอกสารนั้นขึ้นก็ดี หรือสืบถึงควา มมีอยู่ของเอกสารโดยไม่เกี่ยวข้องกับข้อความในเอกสารก็ดี หรือนำสืบให้เห็นว่าเอกสารมีลักษณะอย่างไรก็ดี ย่อมต้องถือว่าเอกสารนั้นเป็นพยานวัตถุ

2.5 วิธีและรูปแบ บการรวบรวมของพยานหลักฐานในคดีอาญาและคดีอาชญากรรมคอมพิวเตอร์

ในการรวบรวมพยานหลักฐานในการดำเนินคดีอาญา แก่ผู้กระทำความผิดโดยเจ้าพนักงานตำรวจนั้น จะอยู่ในขั้นตอนก่อนการฟ้องคดีอาญา ซึ่งประเทศต่างๆ จะกำหนดขอบเขตของการแสวงหาพยานหลักฐานไว้ในกฎหมายวิธีพิจารณาความอาญาไว้คล้าย ๆ กัน

ได้แก่ การสืบสวน การสอบสวน การจับ ก ารค้น การยึด ซึ่งถือว่าเป็นมาตรการสำคัญที่เจ้าพนักงานตำรวจได้ใช้ในการแสวงหาพยานหลักฐานเพื่อดำเนินคดีแก่ผู้กระทำความผิด ซึ่งรูปแบบการรวบรวมพยานหลักฐานในคดีอาญามีดังนี้

2.5.1 การสืบสวน สอบสวน (Investigation) ถูกใช้เป็นเครื่องมือของรัฐในการรักษาความสงบเรียบร้ อยของประชาชนเพื่อป้องกันและปราบปรามอาชญากรรมรวมถึงการอำนวยความยุติธรรมให้แก่ประชาชน ในการดำเนินคดีอาญาของพนักงานสอบสวนทั้งนี้ เนื่องจากเมื่อมีอาชญากรรมเกิดขึ้นย่อมทำให้เกิดความเสียหายแก่ชีวิต ร่างกายและทรัพย์สินของประชาชน [21] โดยที่การสืบสวนสอบสวนเป็นภาร กิจที่มีความสัมพันธ์เกี่ยวเนื่องกันอย่างใกล้ชิด เพราะต่างอยู่ในฐานะที่เป็นอุปกรณ์ที่เกื้อกูลต่อการสืบเสาะหาตัวผู้กระทำความผิดที่แท้จริงมาลงโทษอย่างยุติธรรม

สำหรับประเทศไทยตามประมวลกฎหมายวิธีพิจารณาความอาญา จะเน้นสาระสำคัญของการปฏิบัติ โดยแยกการสืบสวนสอบสวนออกจากกันอย่างชัดเจนในบทกฎหมาย แต่ในทางปฏิบัติวัตถุประสงค์ส่วนหนึ่งของการสืบสวนคือ เพื่อที่ทราบรายละเอียดแห่งความผิด [22] จะสอดคล้องกับการสอบสวนที่ว่า เพื่อที่จะทราบข้อเท็จจริงหรือพิสูจน์ความผิด [23] และยิ่งกว่านั้นประมวลกฎหมายวิธีพิจารณาความอาญาของไทยไม่ได้กำหน ดรูปแบบของการสืบสวนไว้ ซึ่งต่างกับการสอบสวนที่ได้มีการระบุแบบไว้อย่างชัดเจน ทั้งนี้เพื่อประโยชน์ในการนำคดีเสนอต่อศาล นั่นเอง

2.5.2 การจับ

การจับเป็นการกระทำขั้นต้นเพื่อจำกัดเสรีภาพในการเคลื่อนไหวเปลี่ยนที่ทางของบุคคล [24] จากการใช้อำนาจของรัฐ ดังนั้นการจั บหมายถึง การทำให้เสรีภาพในการเคลื่อนไหวโดยอิสระสิ้นสุดลงหรือการยึดตัวบุคคลและหน่วงเหนี่ยวไว้ภายใต้การควบคุมอำนาจของกฎหมาย [25]

---

[21] สุโขทัยธรรมาธิราช, มหาวิทยาลัย. เอกสารการสอนชุดวิชากฎหมายวิธีสบัญญัติ 3 หน่วยที่ 4. พิมพ์ครั้งที่ 12. กรุงเทพมหานคร : มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2539, หน้า 239

[22] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (10)

[23] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (11)

[24] คณิต ณ นคร. กฎหมายวิธีพิจารณาความอาญา . พิมพ์ครั้งที่ 3 แก้ไขเพิ่มเติม. กรุงเทพมหานคร : นิติบรรณาการ, 2539, หน้า 216

[25] วีระวุธ ชัยชณะมงคล เรื่องเดียวกัน. หน้า 58

2.5.3 การค้น การยึด

การค้นและการยึด หมายถึง การค้นหาและการเสาะหาสิ่งของที่ถูกซ้อนเร้น เพื่อค้นพบและยึดสิ่งของโดยเจ้าพนักงานตำรวจผู้มีอำนาจ เพื่อสืบสวบรวบรวมประจักษ์พยานหลักฐานข้อเท็จจริงประกอบการพิจารณาดำเนินคดี ให้เห็นอาจชัดแจ้งว่าการค้นเป็นอำนาจของเจ้าพนักงานผู้มีอำนาจโดยเฉพาะ ซึ่งการตรวจค้นมี 2 แบบคือ การตรวจค้นหาตัวบุคคลและการตรวจค้นหาเพื่อพบสิ่งของ การค้นหาตัวบุคคลหมายถึง การค้นสถานที่หรือเคหสถานเพื่อจะพบตัวบุคคลหรือเพื่อจับบุคคลนั้นเอง ส่วนการค้นหาเพื่อพบสิ่ งของอาจจะเป็นการค้นสถานที่เพื่อพบสิ่งของที่ต้องการค้นนั้น หรืออาจจะเป็นการค้นตัวบุคคลเพื่อพบสิ่งของก็ได้

ดังที่ได้กล่าวจากข้างต้นเป็นรูปแบบการรวบรวมพยานหลักฐานในคดีอาญาโดยทั่วไป แต่ในปัจจุบันอาชญากรรมทางคอมพิวเตอร์ได้เกิดขึ้นมากมายและไม่สามารถควบคุมได้ ทำให้เจ้าหน้าที่ตำรวจจำเป็นต้องหาวิธีและรูปแบบ การรวบรวมพยานหลักฐานเข้ามาใช้ เพื่อทำการแสวงหาพยานหลักฐาน ซึ่งจะในที่นี้จะกล่าวถึงวิธีและรูปแบบในการรวบรวมพยานหลั กฐานในคดีอาชญากรรมทางคอมพิวเตอร์ ดังต่อไปนี้ [26]

2.5.3.1 การวางแผนในการตรวจค้น (Search Planning)

การวางแผนในการตรวจค้นเป็นสิ่งจำเป็นในคดีอาชญากรรมคอมพิวเตอร์ การวางแผนที่ดีจะนำไปสู่ความสำเร็จในการรวบรวมพยานหลักฐาน เนื่องจากการจัดเก็บพยานหลักฐานที่เป็นเทคโนโลยีคอมพิวเตอร์ต้องใช้วิธีพิเศษโดยเฉพาะ ในการตรวจค้นประการแรกที่จะต้องพิจารณาในการวางแผนคือ ต้องทราบรูปแบบของอาชญากรรมคอมพิวเตอร์ว่าเป็นรูปแบบของอาชญากรรมที่เกี่ยวข้องกับฮาร์ดแวร์ (Hardware) ซอฟท์แวร์ (Software) หรือการสื่อสารโทรคมนาคม (Telecommunication) ซึ่งอาจแยกพิจารณาได้ดังนี้

---

[26] สุรพันธ์ มั่งคงดี , “พยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ .” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยา, 2541 หน้า 66

2.5.3.1.1 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับฮาร์ดแวร์ (Hardware) หากเป็นอาชญากรรมคอมพิวเตอร์ที่เกี่ยวข้องกับฮาร์ดแวร์ จะต้องพิจารณาว่ าเป็นฮาร์ดแวร์คอมพิวเตอร์ขนาดใด เช่นเป็นฮาร์ดแวร์ไมโครคอมพิวเตอร์ มิ นิคอมพิวเตอร์ เมนเฟรมคอมพิวเตอร์หรือซุปเปอร์คอมพิวเตอร์ โดยเฉพาะเครื่องขนาดใหญ่ หากทราบถึงข้อมูลถึงระบบปฏิบัติการ (OS) โปรแกรมของตัวแทนจำหน่ายหรือบริษัทผู้ผลิตย่อมเป็นประโยชน์ต่อการตรวจค้นเป็นอย่างมาก เพราะคอมพิวเตอร์ขนาดใหญ่ไม่สามารถตรวจยึดเข้าไปสู่ห้องป ฏิบัติการได้ การวางแผนและการตรวจค้นจึงต้องมีนักวิเคราะห์ระบบ โปรแกรมเมอร์ หรือวิศวกรของบริษัทผู้ผลิตเข้าร่วมดำเนินการในการแก้ไขปัญหาและอุปสรรคของการตรวจค้นด้วย

2.5.3.1.2 รูปแบบของอาชญากรรมที่เกี่ยวข้องกันซอฟท์แวร์ (Software) อาชญากรรมที่เกี่ยวข้องกับซอฟท์แวร์จะต้องพิ จารณาว่าเป็นการกระทำผิดในลักษณะใด เช่น การละเมิดลิขสิทธิ์ (Copyright) ซอฟท์แวร์ หรือการใช้ซอฟท์แวร์เพื่อประกอบอาชญากรรมโดยตรง (Criminal Tools) เช่น การถอดรหัสผ่าน (Password) การคัดลอกข้อมูล ในการเข้าตรวจค้นซอฟท์แวร์เป้าหมายจะต้องมีโปรแกรมเมอร์ของบริษัทผู้ผลิตเข้าดำเนินการด้วย

2.5.3.1.3 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับการสื่อสารโทรคมนาคม (Telecommunication)

อาชญากรรมคอมพิวเตอร์อาศัยระบบการสื่อสารโทรคมนาคมจึงต้องพิจารณาว่า การทำงานของเครื่องคอมพิวเตอร์เป็นการทำงานแบบอิสระ (Stand Alone) หรือเป็นคอมพิวเตอร์ที่เชื่อมกับระบบเครือข่าย เช่น ระบบ LAN (Local Area Network) ระบบ WAN (Wide Area Network) ระบบอินเตอร์เน็ต (Internet) การวางแผนในการตรวจค้นจึงต้องมีการเตรียมการสำหรับการตรวจค้นระบบเครือข่ายด้วย เช่น การหาข้อมูลเกี่ยวกับผู้ให้บริการ (ISP) ข้อมูลที่ใช้ในการเชื่อมต่อระบบ เช่น ชื่อผู้ใช้ (User Name), รหัสผ่าน (Password), หมายเลขโทรศัพท์ของ ISP, ชื่อเครื่องบริการของ ISP และหมายเลขประจำเครื่อง (IP Address) และชุดโปรแกรมสำหรับติดตั้งพร้อมคู่มือ

วัตถุประสงค์ของการทราบรูปแบบอาชญากรรมก็เพื่อที่จะได้มีข้อมูลในการดำเนินการขอหมายค้นต่อศาล การเตรียมบุคลากรและเครื่องมือในการปฏิ บัติงานและวิธีการรวบรวมพยานหลักฐานในขั้นตอนต่อไป

2.5.3.2 อำนาจในการตรวจค้น

เนื่องจากการตรวจค้นพยานหลักฐานที่เป็นเทคโนโลยีคอมพิวเตอร์นั้นจะต้องเกี่ยวข้องกับสิทธิส่วนบุคคล ข้อมูลที่เป็นความลับทางด้านเศรษฐกิจ การ เมือง การทหารและความเจริญก้าวหน้าทางวิทยาศาสตร์ ในการตรวจค้นจึงต้องอาศัยอำนาจของศาลเข้าดำเนินการ ทั้งนี้ เพื่อเป็นการคุ้มครองสิทธิส่วนบุคคลไม่ให้ถูกละเมิดโดยเจ้าหน้าที่ของรัฐจนทำให้เกิดความเสียหายแก่เจ้าของระบบ (David Icove, 1995 : 185) กฎหมายของประเทศสหรัฐอเมริการ 18 USC, Ch 119, Section 2522 กำหนดว่าในการบังคับการใช้กฎหมายเกี่ยวกับระบบสื่อสารโทรคมนาคมของเจ้าพนักงานจะต้องได้รับอนุญาตจากศาล ส่วน Ch 206, Section 3121 การใช้อุปกรณ์ดักฟังอุปกรณ์ติดตามและอุปกรณ์บันทึกเลขหมาย (Pen Register) จะต้องดำเนินการโดยได้รับอนุญาตจากศาล และ 42 USC, Ch 21A, Section 2000aa กำหนดว่าเพื่อเป็นการคุ้มครองสิทธิส่วนบุคคล การตรวจค้นยึดพยานหลักฐานในการสืบสวนดำเนินคดีจะต้องได้รับอนุญาตจากศาลจึงจะดำเนินการได้ (David Icove, 1995 : 78) ส่วนกฎหมาย Computer Misuse Act 1990 ของประเทศอังกฤษ Section 14 กำหนดให้การตรวจค้นพยานหลักฐานจะต้องได้รับอนุญาตจากศาล โดยให้มีอำนาจในการตรวจค้นจำนวน 28 วัน และระบุให้อำนาจเจ้าพนักงานที่จะเข้าไปในอสังหาริมทรัพย์ , สิ่งปลูกสร้าง, วัตถุที่เคลื่อนไหวได้ทั้งที่มีรูปร่างและไม่มีรูปร่าง ยานพาหนะ, เรือ, อากาศยาน และยานสะเทินน้ำสะเทินบก (David Icove, 1995 : 347)

การรวบรวมพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์จะต้องดำเนินการโดยมีหมายหรือคำสั่งอนุญาตจากศาล จะต้องระบุบริเวณข่ายงานหรือคอมพิวเตอร์ที่จะทำการตรวจ ค้นอุปกรณ์เครื่องมือที่จะใช้ พยานหลักฐานที่จะตรวจยึดและกำหนดระยะเวลาที่จะต้องปฏิบัติให้ชัดเจนและเมื่อได้รับอนุญาตแล้วจึงจะเข้าดำเนินการได้

2.5.3.3 วิธีการตรวจค้นสถานที่เกิดเหตุ

การตรวจค้นสถานที่เกิดเหตุในคดีอาชญากรรมคอมพิวเตอร์จะต้องระมัดระวังเป็นพิเศษในการรักษาอุปกรณ์และวัสดุที่เกี่ยวข้องนั้นไว้เป็นพยานหลักฐาน และเพื่อที่จะรักษาไว้ซึ่งสภาพที่มีความสมบูรณ์ของพยานหลักฐานเหล่านั้น

ถ้าอุปกรณ์คอมพิวเตอร์ปิดอยู่ขณะเข้าตรวจค้นที่เกิดเหตุ “อย่าเปิดโดยเด็ดขาด” มิฉะนั้นคอมพิวเตอร์จะถูกโปรแกรมทำลายพยานหลักฐานทั้งหมด ให้ดำเนินการถ่ายภาพหรือวิดีโอไว้แล้วตรวจยึดสู่ห้องปฏิบัติการ แต่ถ้าคอมพิวเตอร์เหล่านั้นเปิดและปฏิบัติการอยู่ขณะที่เข้าตรวจค้นในที่เกิดเหตุให้ดำเนินการดังนี้

2.5.3.3.1 การปิดกั้นสถานที่เกิดเหตุ (Control Area) เมื่อเจ้าหน้าที่เข้าไปถึงในสถานที่เกิดเหตุ จะต้องแยกตัวบุคคลออกจากเครื่องคอมพิวเตอร์หรือส่วนประกอบให้เร็วที่สุด เพื่อป้องกันการทำลายพยานหลักฐาน

2.5.3.3.2 ปลดสายโทรศัพท์ (Disconnect any Phone Line) ปลดเส้นทางการสื่อสารกับคอมพิวเตอร์ที่เชื่อว่าเป็นเครื่องมือที่ใช้ในการกระทำผิด เช่น สายโทรศัพท์หรือเครื่องมือสื่อสารอื่นๆ เพื่อป้องกันการควบคุมเครื่องจากระยะไกล

2.5.3.3.3 ถ่ายวิดีโอ (VDO) สถานที่เกิดเห ตุ รูปภายนอกของระบบ สภาพทำเลที่ตั้งของสถานที่เกิดเหตุ รวมทั้งสภาพอุปกรณ์ทุกอย่างในที่เกิดเหตุ

2.5.3.3.4 การวาดผังการต่อสายและผูกป้ายกำกับสายเชื่อม /ช่องเสียบ (Make a Diagram/Label) ให้ทำการวางผังของการต่อเชื่อมสายเครื่องมืออุปกรณ์ในห้องที่เกิดเหตุไว้อย่างละเอียด พร้อ มทั้งติดป้ายกำกับพยานหลักฐานทุกชิ้น รวมทั้งสายเชื่อม /ช่องเสียบและอุปกรณ์ต่อพ่วงทุกอย่างในที่เกิดเหตุ

2.5.3.3.5 ทำการถ่ายภาพสถานที่เกิดเหตุ (Photograph) เน้นให้เห็นบริเวณสายเชื่อมต่อ ช่องเสียบที่ทำป้ายผูกกำกับไว้ และที่สำคัญคือถ่ายภาพข้อมูลที่ปรากฏบนจอภาพ (Screen Displays) ของเครื่องคอมพิวเตอร์ทุกเครื่องขณะที่เข้าทำการตรวจค้นหรือยึดก่อนการถอดประกอบสายเชื่อมต่อ

2.5.3.3.6 อย่าสัมผัสบอร์ด เพราะในระบบเครือข่าย การสัมผัสกับคีย์บอร์ดอาจจะเป็นการเข้าสู่โปรแกรม (Run Programs) และถ่ายเทข้อมูลที่ต้องการออกไป และอย่าสัมผัสทุกสิ่ง ทุกอย่าง โดยปราศจากความเข้าใจว่ากำลังทำอะไร ห้ามปลดสายไฟหรือแหล่งพลังงานและห้ามเปลี่ยนแปลงคอมพิวเตอร์ขณะปฏิบัติงานอยู่ ควรดำเนินการดังนี้

- ให้ผู้เชี่ยวาญดำเนินการคัดลอกทุกสิ่งทุกอย่างที่แสดงผลอยู่บนจอคอมพิวเตอร์ในลักษณะคำต่อคำ

- ถ้าตรวจพบแฟ้มข้อมูลที่สามารถใช้เป็นพยาน หลักฐานในการกระทำผิดแล้วจะต้องสำรอง (Back up) ข้อมูลเหล่านั้นไว้ เพราะข้อมูลที่เก็บไว้ในสภาพแม่เหล็ก อาจเสื่อมหรือสูญหายได้ง่าย
- ควรเก็บรายละเอียดที่เกี่ยวข้อง เช่น หมายเลขโทรศัพท์ คู่มือการใช้เครื่องและเครื่องมือสื่อสารที่ใช้กับเครื่องคอมพิวเตอร์ พร้อมกับบันทึกลักษณะการต่อสายไฟฟ้าระหว่างอุปกรณ์ต่างๆ ในที่เกิดเหตุ นอกเหนือจากตัวกลางซึ่งใช้บันทึกข้อมูล เช่น เทป ดิสก์, ซีดี, เอกสารจากเครื่องพิมพ์
- การอ่านข้อมูลในจานบันทึกออก (Floppy Disk) หรือจานบันทึกแข็ง (Hard Disk) ควรใช้โปรแกรมของผู้ตรวจพิสูจน์เอง เพราะโปรแกรมในเครื่องคอมพิวเตอร์ที่ยึดมาอาจมีหลุมพลางซ่อนอยู่ เช่น คำสั่ง DIR อาจกลายเป็นคำสั่งลบทิ้ง (Delete) หลักฐานต่างๆ ก็อาจถูกทำลายไปโดยไม่รู้เท่าทัน
- บางครั้งทีมสอบสวนพยายามที่จะเข้าสู่โปรแกรม (Run Program) ในที่เกิดเหตุ เพื่อที่จะได้รายละเอียดเกี่ยวกับแฟ้มข้อ มูลและระบบปฏิบัติการของคอมพิวเตอร์ จะต้องระมัดระวังอย่างยิ่งเมื่อจะกระทำการดังกล่าวนั้น เพราะว่าโปรแกรมคอมพิวเตอร์บางชนิดอาจจะสร้างขึ้นมาเพื่อแก้ไขเปลี่ยนแปลงข้อมูลในจานบันทึกแข็ง หรือข้อมูลบนจานบันทึกอ่อน ทำให้พยานหลักฐานอาจจะถูกเปลี่ยนแปลงไป ส่งผลให้พยาน หลักฐานเหล่านั้นฟังไม่ขึ้น จึงเป็นเรื่องสำคัญมากที่จะต้องรักษาพยานหลักฐาน ตามเงื่อนไขในการ เข้าตรวจค้นก่อนจะทำการเข้าสู่โปรแกรม (Run Program) ทุกๆ สิ่ง ต้องมั่นในว่าผู้เชี่ยวชาญด้านเทคนิคได้ตรวจพิสูจน์ทุกโปรแกรมหมดแล้ว
- ให้ผู้เชี่ยวชาญตรวจสอบหน่วยความจำของค อมพิวเตอร์แบบชั่วคราว (RAM Drive) ว่ามีข้อมูลที่ต้องสงสัยหรือไม่ ก่อนปิดไฟฟ้าที่เครื่องคอมพิวเตอร์

2.5.3.3.7 การกู้ข้อมูลคอมพิวเตอร์บางลักษณะจะต้องอาศัยผู้เชี่ยวชาญทางคอมพิวเตอร์โดยเฉพาะ จึงจะสามารถแยกรายละเอียดข้อมูลที่ต้องการออกมาได้

2.5.3.3.8 การตรวจยึดพยานหลักฐานในที่เกิดเหตุ

- ตรวจยึดฮาร์ดแวร์ทั้งหมดที่พบในที่เกิดเหตุ
- ตรวจยึดโปรแกรมทั้งหมดในที่เกิดเหตุ
- แผ่นดิสก์, เทปหรือสื่อบันทึกชนิดอื่นๆ
- เอกสารทั้งหมดที่พบในที่เกิดเหตุ
- อุปกรณ์ต่อพ่วงทั้งหมดที่ค้นพบ เช่น เครื่องพิมพ์ , อุปกรณ์สื่อสาร, สายเชื่อม, ลำโพง เป็นต้น
- เอกสารที่ถูกทิ้ง เอกสารจากคอมพิวเตอร์และเอกสารพิมพ์ต่อเนื่องจากเครื่องพิมพ์ที่สำคัญจะต้องตรวจดูเอกสารในถังขยะในระหว่างการตรวจค้นด้วย

2.5.3.3.9 ในกรณีของการหลอกล่อคนร้ายที่ชอบขโมยข้อมูล เจ้าหน้าที่อาจสร้างกับดัก เช่น โปรแกรม Virus ชนิดพิเศษไว้ในข้อมูลที่คนร้ายต้องการ เพื่อเป็นหลักฐานในการจับกุมคนร้ายและฟ้องร้องต่อศาล

2.5.3.3.10 การตรวจหาและเก็บลายพิมพ์นิ้วมือแฝงในที่เกิดเหตุ รวมทั้งการดำเนินในกรณีอื่นๆ เช่น การวิเคราะห์แยกแยะพยานบุคคลที่เกี่ยวข้อง

2.5.3.4 วิธีการตรวจยึดพยานหลักฐานทางคอมพิวเตอร์

2.5.3.4.1 การตรวจยึดฮาร์ดแวร์ (Hardware) ไมโครคอมพิวเตอร์

A. หน่วยประมวลผลกลาง (CPU)

การตรวจยึดฮาร์ดแวร์ของไมโครคอมพิวเตอร์ ถ้าเครื่องเปิดอยู่และกำลังประมวลผลหรือปฏิบัติงานใดอยู่ปล่อยให้เครื่องทำงานจนเสร็จ แล้วดำเนินการถ่ายภาพหรือ V.D.O. ภาพข้อมูลที่ปรากฏบนจอภาพ นำดิสก์ออกจากหน่วยขับ เก็บข้อมูลจากความจำของ RAM โดยใช้ดิสก์ที่เตรียมมาให้ผู้เชี่ยวชาญทางการรักษาความปลอดภัยตรวจสอบระบบและรหัสผ่านถ้าสามารถเข้าไปสู่จานบันทึกแข็ง (Hard Disk) และเปิดแฟ้มข้อมูลได้จะต้องสำรองข้อมูลเหล่านั้นไว้โดยใช้ดิสก์ที่เตรียมมาเช่นกัน เมื่อเก็บข้อมูลเรียบร้อยแล้วจึงปิดเครื่องคอมพิวเตอร์ ห้ามเคลื่อนย้ายส่วนประกอบภายในออกจากเครื่องคอมพิวเตอร์ ให้ถอดสายเชื่อมระหว่างอุปกรณ์ต่อพ่วงออก ผูกป้ายกำกับบริเวณปลายสายและบันทึกไว้ที่ป้ายเรียงตามตัวอักษรหรือตัวเลข เช่น CPU 1 หมายถึง CPU ที่ตรวจยึดเป็นตัวที่ 1 เป็นต้น และจะต้องบันทึกวันและเวลาที่ตรวจยึดลงบนป้าย กำกับด้วย การเคลื่อนย้ายให้หีบห่อฮาร์ดแวร์โดยใช้พลาสติกและบรรจุลงกล่องสำหรับส่งสู่ห้องปฏิบัติการตรวจหาข้อมูลอีกครั้งหนึ่ง

B. จอภาพ (Monitor)

ให้ผูกป้ายกำกับที่ปลายสายและบันทึกรายละเอียด เพื่อแสดงว่าเป็นสายเชื่อมหรือช่องเสียบเข้าออกอย่างไร ติดป้ายกำกับลงบนจอภาพ และบันทึกว่าเป็นจอภาพที่ใช้กับ CPU เครื่องใด ระบุวันเวลาที่ตรวจยึด การเค ลื่อนย้าย หีบห่อจอภาพด้วยพลาสติกและบรรจุลงกล่องสู่ห้องปฏิบัติการ

C. แป้นพิมพ์ (Keyboard)

ให้ผูกป้ายกำกับที่ปลายสายและบันทึกรายละเอียดเพื่อแสดงว่าเป็นช่องเสียบเข้า/ออกอย่างไร ติดป้ายกำกับล งบนแป้นพิมพ์และบันทึกว่าเป็นแป้นพิมพ์ที่ใช้กับ CPU เครื่องใด ระบุวันเวลาที่ตรวจยึด การเคลื่อนย้ายหีบห่อแป้นพิมพ์ด้วยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

D. หน่วยขับจานบันทึกแข็งจานภายนอก (External/Removable Hard Drives)

ให้ผู้เชี่ยวชาญตรวจสอบข้อมู ลที่บรรจุอยู่ในจานบันทึกแข็ง (Hard Disk) ถ้าตรวจพบให้สำรองข้อมูลไว้ หน่วยขับจานบันทึกแข็งจากภายนอกในการเชื่อมกับคอมพิวเตอร์อาจจะต่อพ่วง โดยใช้คำสั่ง จากโปรแกรมหรือไม่ต้องใช้โปรแกรม ได้ ดังนั้นในการจัดเก็บจึงต้องตรวจสอบก่อนว่าการต่อพ่วงต้องใช้โปรแกรมหรือไม่ หากใช้ให้ปิดโปรแกรมให้เรียบร้อยก่อนแล้วจึงถอดสายเชื่อม ผูกป้ายกำกับสายเชื่อมเพื่อแสดงว่าเป็นสายเชื่อมที่เสียบเข้า /ออก อย่างไร ติดป้ายกำกับลงบนหน่วยขับและบันทึกว่าเป็นหน่วยขับที่ใช้กับคอมพิวเตอร์เครื่องใด การกำกับอาจจะใช้ลำดับอักษรและหมายเลข ส่วนการเคลื่อนย้ ายหีบห่อด้วยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

E. หน่วยขับจานบันทึกอ่อนจากภายนอก (External Floppy Diskette Drive)

เคลื่อนย้ายดิสก์ออกจากหน่วยขับ ให้ผู้เชี่ยวชาญคัดลอกข้อมูลโดยใช้ดิสก์ที่เตรียมมาตรวจสอบว่าในการเชื่อมกับคอมพิวเตอร์ต้องใช้โปรแกรมหรื อไม่ หากใช้ให้ปิดโปรแกรมให้เรียบร้อยแล้วจึงถอดสายเชื่อม ผูกป้ายกำกับสายเชื่อมเพื่อแสดงว่าเป็นสายเชื่อมที่เสียบเข้า/ออกอย่างไร ติดป้ายกำกับลงบนหน่วยขับและบันทึกว่าเป็นหน่วยขับที่ใช้คอมพิวเตอร์เครื่องใด การกำกับอาจจะใช้ลำดับอักษรและหมายเลข ส่วนการเคลื่อนย้ายหีบห่อด้วยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

F. หน่วยขับเทปจากภายนอก (External Tape Drive)

ดำเนินการถ่ายภาพและวาดผังระบบติดตั้งสวิตช์ DIP (Dual In Line) โดยเน้นให้เห็นการทำงานของระบบว่าหมุนจากด้านใดไปทางใด ตรวจสอบว่าต้องใช้โปรแกรมในการเปิด-ปิดหน่วยขับหรือไม่ หากใช้ให้ปิดโปรแกรมให้เรียบร้อยแล้วจึงปลดแหล่งพลังงาน เคลื่อนย้ายตัวเทปออกจากหน่วย ขับถอดสายเชื่อม ติดป้ายสายเชื่อมเพื่อแสดงทิศทางการเชื่อมต่อ ติดป้ายกำกับหน่วยขับและบันทึกว่าเป็นหน่วยขับถอดสายเชื่อม ติดป้ายสายเชื่อมเพื่อแสดงทิศทางการเชื่ อมต่อ ติดป้ายกำกับหน่ วยขับและบันทึกว่าเป็นหน่วยขับที่ใช้กับคอมพิวเตอร์เครื่องใด การกำกับอาจจะใช้ลำดับอักษรและหมายเลข ส่วนการเคลื่อนย้ายหีบห่อด้วยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

G. เครื่องพิมพ์ (Printer/Plotters)

ดำเนินการถ่ายภาพและวาดผังระบบติ ดตั้งสวิตช์ DIP แล้วเคลื่อนย้ายกล่องบรรจุผงห มึก (เครื่องพิมพ์ที่ใช้แบบผ้าหมึ กบางชนิ ดสามารถอ่านได้) ออกจากเครื่องพิมพ์ ติดป้ายกำกับเครื่องพิมพ์และกล่องบรรจุผงหมึกว่าใช้กับคอมพิวเตอร์เครื่องใด การกำกับอาจจะใช้ลำดับอักษรและหมายเลข ส่วนการเคลื่อนย้ายหีบห่อด้ว ยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

H. โมเด็ม (Modem)

โมเด็มจะต้องตัดการติดต่อจากโทรศัพท์ให้ผู้เชี่ยวชาญตรวจสอบที่โปรแกรมใช้งานโทรศัพท์อัตโนมัติว่าได้มีการติดต่อไปยังที่ใดบ้าง คัดลอกหมายเลขโทรศัพท์ที่คอมพิวเตอร์ติดต่อผ่านโมเด็มเข้ามายังระบบ เพื่อ นำมาใช้เป็นพยานหลักฐานและเชื่อมโยงกับแนวทางการสืบสวนสอบสวน ติดป้ายสายเชื่อมเพื่อแสดงทิศทางการเชื่อมต่อ ติดป้ายกำกับที่โมเด็มและบันทึกรายละเอียดว่าใช้กับคอมพิวเตอร์เครื่องใด การกำกับอาจจะใช้ลำดับอักษรและหมายเลข ส่วนการเคลื่อนย้ายหีบห่อด้วยพลาสติกและบรรจุลงกล่องเพื่อส่งสู่ห้องปฏิบัติการ

I. อุปกรณ์ต่อพ่วง/สายเชื่อม (Acoustic Couplers/Cables)

จัดเก็บอุปกรณ์ต่อพ่วงและสายเชื่อมทุกชนิดไว้เป็นพยานหลักฐานจะต้องดำเนินการถ่ายภาพและวาดผังการเชื่อมต่อแล้วจึงถอดสายเชื่อมนั้น ติดป้ายกำกับที่ปลายสายและที่อุปกรณ์ต่อพ่วง โดยบรร ยากาศสภาพการต่อเชื่อมสายไปสู่ PC เครื่องพิมพ์หรืออุปกรณ์อื่นๆ การเคลื่อนย้ายอุปกรณ์ต่อพ่วงหีบห่อด้วยพลาสติกบรรจุลงกล่อง ส่วนสายเชื่อมไม่จำเป็นต้อง บรรจุลง หีบห่อให้บรรจุลงกล่องไปสู่ห้องปฏิบัติการ

2.5.3.4.2 สื่อบันทึก (Magnetic Media) คอมพิวเตอร์

A. แผ่นดิสก์ (Floppy Diskettes)

การเก็บพยานหลักฐานที่เป็นแผ่นดิสก์ติดป้ายกำกับลงบนแผ่นดิสก์บันทึกลำดับตามตัวอักษรหรือตัวเลข วันเวลาที่ทำการตรวจยึด นอกจากนี้ให้บันทึกชื่อแฟ้มข้อมูลที่ถูกค้นพบ คำสั่งที่ใช้ในการเข้าถึงชื่อของระบบปฏิบัติการหรือรายละเอียดปลีกย่อยอื่นๆ หากเนื้อที่บนป้ายกำกับแผ่นดิสก์ไม่พออาจจะบันทึกไว้ต่างหากอีกส่วนก็ได้ เก็บรักษาแผ่นดิสก์ให้ห่างจากสนามแม่เหล็กไฟฟ้าและบรรจุไว้ในกล่องบรรจุแผ่นดิสก์ ห้ามใช้พลาสติกหุ้มเพราะพลาสติกเป็นอันตรายต่อการระบายออกของระบบไฟฟ้าสถิตย์ให้ติดป้ายกำกับแผ่นดิสก์ว่า “ห้ามเอ็กซเรย์” เพื่อเตือนว่าพยานหลักฐานชิ้นนี้จะต้องเก็บรักษาให้ห่างจากสนามแม่เหล็ก รวบรวมนำไปส่งห้องปฏิบัติการ

B. ม้วนเทป (Tape)

การเก็บพยานหลักฐานที่เป็นม้วนเทป ติดป้ายกำกับลงบนม้วนเทป บันทึกลำดับตามตัวอักษรหรือตัวเลข วันเวลาที่ทำการตรวจยึด เก็บรักษาแผ่นดิสก์ให้ห่างจากสนาม แม่เหล็กไฟฟ้า ห้ามใช้พลาสติกหุ้ม ติดป้ายกำกับที่ม้วนเทปว่า “ห้ามเอ็กซเรย์” เช่นกัน เพื่อรวบรวมนำส่งไปห้องปฏิบัติการ

2.5.3.4.3 พยานเอกสาร (Documentation)

A. คู่มือการปฏิบัติงานต่างๆ (Manuals/Hand Written Note)

การเก็บพยานหลักฐานที่เป็นเอกสาร เจ้าหน้าที่ผู้ปฏิบัติจะต้ องสวมถุงมือเพื่อรักษาลายพิมพ์นิ้วมือแผงในการตรวจพิสูจน์ ตรวจเก็บเอกสารทุกชนิดที่ต้องสงสัยว่าจะเกี่ยวข้องกับคดี เช่น สมุดคู่มือการใช้เครื่องคอมพิวเตอร์ การใช้โปรแกรมหรือเอกสารที่เป็นการจดบันทึกหรือบันทึกช่วยจำ อาจจะมีรหัสผ่านหรือข้อความที่ใช้เป็นพยานหลักฐา นบรรจุลงกล่องติดป้ายกำกับบนกล่อง ระบุวันที่ทำการตรวจค้นแล้วส่งไปสู่ห้องปฏิบัติการ เพื่อตรวจหาลายพิมพ์นิ้วมือแฝงและใช้เป็นพยานหลักฐานในชั้นศาล

B. เอกสารจากเครื่องพิมพ์/รายการบันทึก (Printout/Listings)

เก็บเอกสารที่ได้จากคอมพิวเตอร์เหล่านั้น โดยใช้ถุงมือเช่น กันบรรจุใส่กล่องแยกออกมาเป็นพิเศษจากเอกสา รชนิดอื่นๆ ติดป้ายกำกับบนกล่องและบันทึกรายละเอียดว่าเป็นเอกสารจากเครื่องพิมพ์และคอมพิวเตอร์เครื่องใด เป็นข้อมูลที่เกี่ยวข้องในเรื่องใด ระบุเวลาที่ทำการตรวจค้นแล้วส่งไปสู่ห้องปฏิบัติกา ร เพื่อประมวลผลข้อมูลและพิมพ์ซ้ำ ข้อมูลออกมาเปรียบเทียบและใช้เป็นพยานหลักฐานในชั้นศาล

2.5.3.4.4 การตรวจยึดพยานหลักฐานที่ไม่สามารถเคลื่อนย้ายได้

พยานหลักฐานที่เป็นเทคโนโลยีคอมพิวเตอร์บางประเภทที่ลักษณะทางกายภาพของพยานหลักฐานนั้นไม่อาจเคลื่อนย้ายไปได้ เช่น คอมพิวเตอร์ข นาดมินิหรือเมนเฟรมคอมพิวเตอร์ขึ้ นไป การตรวจค้นจะต้องได้รับความยินยอมจากเจ้าของเครื่องโดยคำสั่งศาลเข้าดำเนินการตรวจค้น การตรวจ คันคอมพิวเตอร์ขนาดใหญ่จึงต้องมีนักวิเคราะห์ระบบ โปรแกรมเมอร์และวิศวกรของบริษัทผู้ผลิตเครื่องคอมพิวเตอร์นั้นเข้าดำเนินการตรวจค้น โดยขณะตรวจค้นจะต้องถ่ายภาพหรือถ่าย วิดีโอ (V.D.O.) ไว้ทุกขั้นตอนโดยวิธีปฏิบัติดังนี้คือ

A. การเข้าสู่ระบบ (Initial Approach)

การเข้าสู่ระบบอาจจะใช้เครื่องปลายทาง ซึ่งเป็นเครือข่ายของเมนเฟรมนั้นหรือใช้คอมพิวเตอร์ของทีมสืบสวนที่เตรียมไป การเข้าสู่ระบบหากต้องใช้หมายเลขโทรศัพท์ผ่านโมเด็มและรหัสผ่า นจะต้องบันทึก หมายเลขโทรศัพท์และรหัสผ่านนั้นไว้เป็นพยานหลักฐาน เมื่อเข้าสู่ระบบได้แล้วให้ค้นหาสิ่งที่ต้องการถ่ายทอดข้อมูลออกมาทางเครื่องพิมพ์และสำรองเก็บใส่ดิสก์ ให้ผู้เกี่ยวข้องลงชื่อรับรองเอกสารจากเครื่องพิมพ์และลงชื่อบนป้ายกำกับแผ่นดิสก์ด้วยเช่นกัน

B. พยานหลักฐานที่ต้องตรวจยึด

- เอกสารจากเครื่องพิมพ์และดิสก์ที่ได้สำรองข้อมูลไว้
- ข้อมูลที่ต้องใช้เป็นพยานหลักฐานซึ่งอยู่ในรายการบันทึกของเครื่อง เช่น ชื่อผู้ใช้ รหัสผ่าน หมายเลขโทรศัพท์ที่ติดต่อเข้าระบบที่เป็นของผู้ต้องสงสัยหรือผู้กระทำความผิด และข้อมูลปลีกย่อยๆ อื่ นที่ใช้เป็นพยานหลักฐาน ถ่ายทอดออกมาทางเครื่องพิมพ์และให้ผู้เกี่ยวข้องลงชื่อรับรองไว้เป็นพยานหลักฐาน

C. การตรวจยึดพยานหลักฐานจากการใช้โปรแกรม BBS

ตามที่ได้กล่าวมาแล้วว่าโปรแกรม BBS (Bulletin Board System) เป็นโปรแกรมที่อาชญากรคอมพิวเตอร์ใช้รับส่งข้อมูลข่าวสารแ ละลักลอบเข้าไปในโปรแกรม BBS เพื่อค้นหาข้อมูลที่ต้องการ เช่น ข้อมูลเกี่ยวกับผู้ถือบัตรเครดิต รายนามผู้ใช้โทรศัพท์และเลขหมายโทรศัพท์ ในทางธุรกิจมีโปรแกรม BBS มากมายที่ผู้ก่อตั้งได้รวบรวมข้อมูลที่น่าสนใจไว้เพื่อให้ผู้ที่สนใจคัดลอกไปโดยเสียค่าใช้จ่าย สำหรับข้อมู ลนั้น เนื่องจากโปรแกรม BBS มีขนาดใหญ่และมีข้อมูลที่บรรจุไว้จำนวนมาก เป็นการยุ่งยากและไม่เกิดประโยชน์ที่ทีมสืบสวนสอบสวนจะตรวจยึดไปทั้งหมด

บทที่ 3

มาตรการทางกฎหมายที่ให้อำนาจพนักงานสอบสวนในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์

3.1 มาตรการทางกฎหมายที่ให้อำนาจพนักงานสอบสวนในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ในประเทศไทย

จากสถานการ ณ์ในประเทศไทยปัจจุบันได้เกิดคดีเกี่ยวกับอาชญากรรมคอมพิวเตอร์มากมายในหลาย ๆ รูปแบบ อย่างไรก็ตาม การกระทำความผิดทางคอมพิวเตอร์ในบางครั้งก็อาจส่งผลกระทบหรือก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ดังนั้น การพิจารณาเกี่ยวกับอำนาจหน้าที่ของพนักงาน เพื่อให้เกิดความสมดุลในการใช้อำนาจและปกป้องคุ้ม ครองสังคมได้อย่างเหมาะสม จึงเป็นสิ่งสำคัญอย่างยิ่งที่ หน่วยงานภาครัฐต้องเข้ามามีบทบาทสำคัญในการควบคุมดูแลอย่างจริงจัง

เนื่องจากการก่ออาชญากรรมทางคอมพิวเตอร์นั้น ยากต่อการตรวจพบและยากต่อการพิสูจน์ความรับผิด และกระทำได้อย่างรวดเร็วโดยอาจส่งผลเสียหายในวงกว้าง ในการพัฒนากฎหมายอาชญากรรมทางคอมพิวเตอร์ขึ้นใช้บังคับจึงน่าจะพิจารณาในเรื่องที่เกี่ยวกับการสืบสวน สอบสวนและการดำเนินคดี ซึ่งต้องอาศัยพนักงานสอบสวนหรือบุคคลที่เกี่ยวข้องในกระบวนการยุติธรรมที่ต้องมีความเชี่ยวชาญอย่างยิ่ง ดังนั้น จึงกำหนดอำนาจหน้าที่ของเจ้าพนักงานไว้ใน พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 18 เพื่อให้ง่ายต่อการรวบรวมพยา นหลักฐานและทันการกับลักษณะการกระทำความผิดดังกล่าว ดังนั้น จึงสมควรกำหนดมาตรการเพื่อป้องกัน และปราบปรามการกระทำดังกล่าว

3.1.1 กฎหมายประเทศไทยในปัจจุบัน

เนื่องจากกฎหมาย พระราชบัญญัติ ธุรกรรมทางอิเล็ก ทรอนิกส์ ที่ได้ประกาศบังคับใช้ตั้งแต่ปี พ.ศ. 2544 ในปัจจุบันเวลาผ่านมา 6 ปี ทางภาครัฐได้มีความพยายามในการผลักดันในการใช้กฎหมาย พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ โดยได้พยายามออกก ฎหมายลูกหรือ พระราชกฤษฎีกาออกมาในหลายมาตรา ซึ่งในวันที่ 10 มกราคม พ.ศ. 2550 ที่ผ่านมาทางรัฐบาลได้ประกาศใช้ พระราชกฤษฎีกา "กำหนดห ลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ .ศ.2549" อาศัยอำนาจตามความในมาตรา ๑๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พ.ศ. 2549 และมาตรา ๓๕ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งมีผลกระทบกับภาครัฐโด ยตรง โดยหน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ

หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ หน่วยงานภาครัฐมีความจำเป็นต้องทำตามหลั กธรรมาภิบาลในการใช้งานระบบสารสนเทศ หรือ "IT Governance" ตลอดจนปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยระดับโลกในบางส่วน ซึ่งได้แก่มาตรฐาน ISO / IEC 27001 (Information Security Management System) ซึ่งแนวนโยบายและแนวปฏิบัติบางส่วนของ มาตรฐาน ISO / IEC 27001 ตามพระราชกฤษฎีกา "กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ .ศ.2550" ในมาตรา 5 แบ่งออกเป็น 3 หัวข้อ ดังนี้[27]

1. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)
2. การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ (Business Continuity Planning & Disaster Recovery Planning)
3. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ (IT Risk Assessment)

โดยหน่วยงานรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ ซึ่งเหตุผลในการประกาศใช้พระราชกฤษฎีกา ฉบับนี้ คือ เนื่องจากประเทศไทยได้เริ่มเข้าสู่ยุคสังคมสารสนเทศ ซึ่งมีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาค รัฐมากขึ้น สมควรสนับสนุนให้หน่วยงานของรัฐมีระบบการบริการของตนโดยการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว อันเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ พร้อมกับให้หน่วยงานของรัฐสามารถพัฒนาการทำธุร กรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน และสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ ประกอบกับมาตรา 35 วรรคหนึ่งแห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ .ศ. 2544 บัญญัติว่า คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาแล้วให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนดจึงจำเป็นต้องตราพระราชกฤษฎีกานี้

---

[27] หนังสือ eLeader Thailand (เมษายน 2550 Update Information : 12 เมษายน 2550)

ในส่วนของ พระราชบัญญัติ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้แต่งตั้งคณะกรรมาธิการสภานิติบัญญัติแห่งชาติ ขึ้นมาพิจารณา พระราชบัญญัติ ดังกล่าว ความซึ่งมีทั้งสิ้น 30 มาตรา โดยในสาระที่คณะกรรมาธิการ สภานิติบัญญัติแห่งชาติ ให้ความสำคัญเป็นพิเศษทั้งหมด 3 ข้อ ได้แก่

1. การทำความเข้าใจเกี่ยวกับประเด็นทางเทคนิคทั้งในลักษณะของการกระทำ ความผิด และลักษณะของการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่
2. การสร้างความสมดุลระหว่างการคุ้มครองสังคมและคุ้มครองสิทธิความเป็นส่วนตัวของประชาชน
3. การควบคุมการใช้อำนาจของพนักงานเจ้าหน้าที่ให้อยู่ในระดับที่เหมาะสม ทั้งนี้ เพื่อให้กฎหมายนั้นสามารถใช้บังคับได้อย่างมี ประสิทธิภาพ โดยไม่ก่อให้เกิดภาระกับผู้ให้บริการ/ผู้ประกอบการมากเกินไป โดยมีจุดยืนสำคัญในการให้ความคุ้มครองความเป็นส่วนตัวของประชาชน

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ในปัจจุบันคอมพิวเตอร์เป็นส่วนสำคัญต่อชีวิตของมนุษย์ หากมีผู้กระทำการใด ทำให้คอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดหรือทำให้การทำงานผิดพลาด หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้คอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จ ย่อมก่อให้เกิดความเสียหายต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ จึงสมควรกำหนดมาตรการเพื่อป้องกัน และปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้ คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

หมวด ๒ พนักงานเจ้าหน้าที่

อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการรวบรวมพยานหลักฐาน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 [28]

กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจในการเข้าตรวจข้อมูลคอมพิวเตอร์ในกรณีมีเหตุอันควรสงสัยว่าน่าจะมีการกระทำความผิดตามพระราชบัญญัติโดยมีอำนาจ ดังนี้

[28] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวน ในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำ ความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ คำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงาน เจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้อง ต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับ อุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ประกอบคำร้อง ด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

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

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการ ให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

โดยสาระสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้แก่

1) ฐานความผิด

ในการพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในส่วนของฐานความผิดนั้น อันครอบคลุมถึงการกระทำความผิดที่สำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในลักษณะต่างๆ ที่กระทบต่อความลับ (confidentiality), ความครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ เช่น การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) การล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 6) การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) การดักรับข้อมูลคอมพิวเตอร์ (มาตรา 8) การรบกวนระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ (มาตรา 9 และมาตรา 10) การรบกวนระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข (มาตรา 11) การรบกวนระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่กระทบต่อความมั่นคงของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ และการบริการ

สาธารณะ (มาตรา 12) การเผยแพร่ชุดคำสั่งชั่วร้ายที่ใช้ในการกระทำความผิดตามมาตราก่อนหน้านี้ (มาตรา 13) การเผยแพร่เนื้อหาอันไม่เหมาะสมหรือเป็นเท็จ เช่น ปลอมแปลงข้อมูลคอมพิวเตอร์หรือทำข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือก่อให้เกิดความเสียหายหรือก่อให้เกิดความตื่นตระหนกกับประชาชน หรือเนื้อความที่กระทบต่อสถาบันหรือการก่อการร้าย รวมทั้งข้อมูลคอมพิวเตอร์อันลามกทั้งหลาย และการ Forward หรือส่งต่อข้อมูลคอมพิวเตอร์ข้างต้น (มาตรา 14)ผู้ให้บริการ ผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการทำความผิดตามมาตรา 14 ต้องรับโทษด้วย (มาตรา 15) กำหนดฐานความผิดในเรื่องการตัดต่อภาพของบุคคลอื่น อันอาจให้เกิดความอับอายหรือเสียหาย ยกเว้นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด (มาตรา 16) และรวมถึงการกระทำความผิดและกำหนดบทลงโทษในกรณีความผิดเกิดนอกราชอาณาจักร (มาตรา 17)

2) อำนาจของพนักงานเจ้าหน้าที่

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้อำนาจหน้าที่ทั่วไปแก่พนักงานเจ้าหน้าที่ไว้อย่างเต็มที่ เพื่อเอื้อประโยชน์ต่อการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ เช่น อำนาจในการค้นหรือเข้ายึด หรือตรวจสอบ ระบบคอมพิวเตอร์ที่ต้องสงสัยว่าได้มีการใช้ในการกระทำความผิด ,การถอดรหัสลับของข้อมูลคอมพิวเตอร์, หรือการเรียกข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น อย่างไรก็ตาม โดยที่มีการให้อำนาจแก่พนักงานเจ้าหน้าที่ไว้อย่างกว้างขวาง และเพื่อไม่ให้การใช้อำนาจนั้นเกิดผลกระทบกับผู้ให้บริการหรือกระทบกับสิทธิของประชาชนมากเกินไป ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงได้มีการกำหนดเงื่อนไขการใช้อำนาจไว้อย่างเข้มงวด เช่น ให้ใช้พยานหลักฐานที่รวบรวมได้เพียงเฉพาะในคดีเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เท่านั้น หรือห้ามไม่ให้พนักงานเจ้าหน้าที่ส่งมอบพยานหลักฐานที่ได้มา ให้กับพนักงานเจ้าหน้าที่ซึ่งมีอำนาจหน้าที่ตามกฎหมายฉบับอื่น เพื่อให้นำพยานหลักฐานดังกล่าวไปใช้ในการดำเนินคดีอื่นที่เกี่ยวข้องอันอาจกระทบกับสิทธิของประชาชนได้โดยง่ายหากพนักงานเจ้าหน้าที่ ใช้อำนาจหน้าที่ในทางมิชอบ หรือแม้กระทั่งการกำหนดให้พนักงานเจ้าหน้าที่ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ต้องรับผิดแม้กระทั่งกระทำให้พยานหลักฐานรั่วไหลโดยประมาท และกำหนดให้พยานหลักฐานที่รั่วไหลจากการกระทำโดยประมาทนั้น ไม่สามารถอ้างเป็นพยานหลักฐานในชั้นศาล เป็นต้น

นอกจากนั้น ยังได้กำหนดให้มีการตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่โดยศาลนั้น มีความชัดเจนมากขึ้น เช่น การกำหนดให้พนักงานเจ้าหน้าที่ระบุเหตุอันควรเชื่อว่าทำไมจึงต้องใช้อำนาจตาม พระราชบัญญัติ , ลักษณะการกระทำความผิด , รายละเอียดของอุปกรณ์ที่ใช้ในการกระทำความผิดเท่าที่จะกระทำได้

3) ความยืดหยุ่นและการเตรียมความพร้อมในการบังคับใช้กฎหมาย

โดยที่ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น ได้กำหนดเกี่ยวกับบุคคลซึ่งเกี่ยวข้องในหลายส่วน เช่น ผู้ให้บริการซึ่งอาจหมายถึง ผู้ประกอบกิจการทางด้านโทรคมนาคม , ผู้ให้บริการอินเทอร์เน็ต , ผู้ให้บริการอื่นๆ เช่น Web Hosting หรือหน่วยงานต่างๆ ที่ต้องกำหนดให้เจ้าหน้าที่หรือพนักงานผู้ดูแลระบบของตน เป็นต้น ทำหน้าที่ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (traffic data) ซึ่งเป็นข้อมูลสำคัญที่ใช้ในการสืบสวนหรือสอบสวนเป็นระยะเวลา 90 วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่คอมพิวเตอร์ แต่ในกรณีจำเป็นเจ้าหน้าที่จะสั่งให้ผู้ให้บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ได้เกิน 90 วัน แต่ไม่เกิน 1 ปี เป็นกรณีพิเศษเฉพาะราย จากเดิมที่กำหนดให้เก็บ traffic data ไว้เพียง 30 วัน ไม่เกิน 90 วัน เท่านั้น อันเป็นระยะที่เหมาะสมและสอดคล้องกับความจำเป็นในการนำไปใช้เพื่อประโยชน์ในการสืบสวนและสอบสวนทางปฏิบัติมากกว่า แต่เพื่อไม่ให้เป็นภาระกับผู้ให้บริการมากเกินสมควร ในกฎหมายจึงได้กำหนดให้รัฐมนตรีกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จัดทำประกาศว่า ใครบ้าง คือ "ผู้ให้บริการ" อันจะก่อให้เกิดภาระกับบุคคลหรือหน่วยงานดังกล่าวเมื่อมีการประกาศหลังกฎหมายบังคับใช้ต่อไป โดยในเบื้องต้นการกำหนดว่าใครบ้าง คือ ผู้ให้บริการนั้น ในเบื้องต้นไม่น่าจะหมายถึงผู้ให้บริการทุกประเภท แต่น่าจะกำหนดให้หมายถึงแต่เพียงผู้ให้บริการกลุ่มใหญ่ๆ เท่านั้น เช่น ผู้ประกอบกิจการทางด้านโทรคมนาคม หรือผู้ให้บริการอินเทอร์เน็ต เป็นต้น

นอกจากนั้น เพื่อให้รับกับประกาศเกี่ยวกับ "ผู้ให้บริการ" ในกฎหมายจึงได้กำหนดให้รัฐมนตรี กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จัดทำประกาศเกี่ยวกับ "Traffic data" ว่า หมายถึงอะไรบ้าง เพื่อผู้ให้บริการจะได้ไม่ต้องเก็บ traffic data ที่ไม่จำเป็นอันเป็นภาระโดยใช่เหตุแต่อย่างใด

อย่างไรก็ตาม ในการปฏิบัติหน้าที่ของ "พนักงานเจ้าหน้าที่" ซึ่งมีอำนาจหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น จำเป็นต้องมีความรู้ความเข้าใจในลักษณะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรืออาชญากรรมทางคอมพิวเตอร์เป็นอย่างดี ในกฎหมายจึงได้กำหนดให้ "พนักงานเจ้าหน้าที่" ต้องมีคุณสมบัติซึ่งต้องผ่านการอบรมหลักสูตรที่กำหนดขึ้นเป็นพิเศษเพื่อให้สามารถทำหน้าที่ตามกฎหมายฉบับนี้ได้อย่างแท้จริงต่อไป

3.1.2 มาตรการด้านกฎหมาย

มาตรการด้านกฎหมายเป็นนโยบายของรัฐบาลไทยประการหนึ่งที่นำมาใช้ในการต่อต้านอาชญากรรมคอมพิวเตอร์ โดยการ บัญญัติหรือตรากฎหมายเพื่อกำหนดว่าการกระทำใดบ้างที่มีโทษทางอาญา ในปัจจุบัน ประเทศไทยมีกฎหมายที่เกี่ยวข้องหลายฉบับ ดังนี้

(1) กฎหมายเทคโนโลยีสารสนเทศ

กฎหมายอาชญากรรมทางคอมพิวเตอร์ หรือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับค อมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายหนึ่งในหกฉบับที่อยู่ภายใต้ความรับผิดชอบของโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยี อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ โดยมีสาระสำคัญของกฎหมายแบ่งออกได้เป็น 2 ส่วนหลัก คือ [29]

ก) การกำหนดฐานความผิดและบทลงโทษ เกี่ยวกับการกระทำที่เป็นอาชญากรรมทางคอมพิวเตอร์ เช่น ความผิดเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยไม่มีอำนาจ (Illegal Access) ความผิดฐานลักลอบดักข้อมูลคอมพิวเตอร์ (Illegal Interception) หรือ ความผิดฐานรบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์โดยมิชอบ (Interference computer data and computer system) ความผิดฐานใช้อุปกรณ์ในทางมิชอบ (Misuse of Devices) เป็นต้น

ข) การให้อำนาจพิเศษแก่เจ้าพนักงานในการปราบปรามการกระทำความผิดนอกเหนือเพิ่มเติมไปจากอำนาจโดยทั่วไป ที่บัญญัติไว้ในกฎหมายอื่นๆ อาทิ การให้อำนาจในการสั่งให้ถอดรหัสข้อมูลคอมพิวเตอร์ อำนาจในการเรียกดูข้อมูลจราจร (Traffic data) หรืออำนาจค้นโดยไม่ต้องมีหมายในบางกรณี

จากการที่ได้ศึกษาข้อมูลเกี่ยวกับ มาตรการทางกฎหมายที่ให้อำนาจพนักงานสอบสวนในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ของประเทศไทยนั้น พบว่าประเทศไทยยังต้องพยายามพัฒนาบุคลากรในสายนี้ โดยการฝึกอบรมให้เกิดความรู้อย่างแท้จริงในการปฏิบัติงานตลอดจนควรจัดสัมมนาหรือเผยแพร่ข้อมูลให้ประชาชนเกิดความเข้าใจถึงวัตถุประสงค์ที่แท้จริงของ พระราชบัญญัติ ธุรกรรมอิเล็ก ทรอนิกส์ และ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้บรรลุวัตถุประสงค์ในเรื่องความมั่นคงของชาติ และเพื่อให้เกิดเสถียรภาพของระบบสารสนเทศในหน่วยงานทั้งภาครัฐ และเอกชนทั่วไป ไม่ให้เกิดความล้าหลังเมื่อเปรียบเทียบกับประเทศเพื่อนบ้าน ยกตัวอย่าง เช่น ประเทศเวียดนาม ที่กำลังพัฒนาด้านสารสนเทศแข่งกับประเทศไทยของเราอย่างน่ากลัว เราจึงควรหันมาจริงจังกับเรื่องความปลอดภัยข้อมูลให้มากกว่านี้ ไม่เช่นนั้นประเทศไทย จะเกิดคดีอาชญากรรมทางคอมพิวเตอร์ มีความถี่มากขึ้น รูปแบบการกระทำผิดก็มีความหลากหลายมากขึ้น และนับวันจะ

[29] http://thaicert.nectec.or.th

เป็นปัญหามากยิ่งขึ้น ด้วย กรณีตัวอย่าง อาชญากรรมทางคอมพิวเตอร์ ในประเทศไทย ที่จะกล่าวต่อไปนี้ เป็นเพียงการยกตัวอย่างรูปแบบในการกระทำผิด หรื อ แผนประทุษกรรม ของคนร้ายที่ใช้ในการกระทำผิดในแต่ละรูปแบบ ซึ่งไม่ได้หมายความว่าแต่ละรูปแบบจะเกิดขึ้นเพียง 1 ราย โดยแต่ละรูปแบบอาจเกิดขึ้นหลายครั้ง ทั้งจากผู้กระทำผิดคนเดียวกันหรือหลายคน โดยจะขอยกตัวอย่างดังต่อไปนี้ [30]

ปัญหากรณี ความผิดตามกฎหมาย ดั้งเดิม บน Internet

การจัดทำเว็บการพนันเป็นภาษาไทย ทั้งการพนันทายผลฟุตบอล และคาสิโน โดยเป็นส่วนหนึ่งของ เว็บการพนันที่มีชื่อเสียงและถูกต้องตามกฎหมายในต่างประเทศ ผู้จัดทำและผู้เล่น รวมทั้งสถาบันการเงินที่ให้บริการ มีความผิดอย่างไร

การเผยแพร่ภาพลามกอนาจาร ซึ่งเครื่อง Server อยู่ต่างประเทศ บางรายผู้จดทะเบียนโดเมนเนม แจ้งว่ามีที่อยู่ในประเทศไทย บางรายใช้ฟรีเว็บ และบางเว็บใช้ภาษาไทย บางเว็บมีการตัดต่อภาพดารา เป็นภาพลามกอนาจาร บางเว็บเสมือนเป็นธุรจัดหา หญิง-ชาย เพื่อการค้าประเวณี

การโฆษณาเป็นภาษาไทย ขาย เทป วิดีโอ CD ละเมิดลิขสิทธิ์ หรือเป็นภาพลามกอนาจาร บางรายให้โอนเงินเข้าบัญชีธนาคาร มีทั้งในประเทศและต่างประเทศ โดยระบุเลขที่บัญชี ไว้ชัดเจน

เผยแพร่ข้อมูล หมิ่นประมาท ใส่ร้าย บุคคลอื่น ส่งภาพลามก ภาพตัดต่อ ทาง E-Mail ในห้อง Chat หรือใน Web board

การจัดทำเว็บ เพื่อฉ้อโกงหลอกลวง โดยมีชายชาวต่างชาติ ทำเว็บแล้วปลอมตัวว่าเป็นหญิงไทย อ้างว่ามีความเดือดร้อน เสนอตัวไปเป็นภรรยา โดยขอให้ส่งเงินมาเป็นค่าเดินทาง โอนเข้าบัญชีธนาคารในประเทศไทย เมื่อได้เงินแล้ว ก็ลบเว็บนั้นออ ก จนไม่อาจตรวจสอบได้ว่าใช้ข้อความเพื่อชักจูงอย่างไร แล้วไปสร้างเว็บใหม่ เพื่อหลอกลวงคนอื่นๆ ต่อไป กรณีนี้ได้ทำการจับกุมแล้ว โดยใช้ข้อหาฉ้อโกงประชาชน

เผยแพร่ข้อมูล หรือใน Web board ที่ไม่ได้หมิ่นประมาท ไม่ได้ใส่ร้ายผู้อื่น แต่อ้างว่าบ้านนั้นจะขาย ทีวี โทรศัพท์มือถือ พระเครื่อง เครื่องเพชร ฯลฯ ในราคาถูก ทำให้มีผู้อื่นโทรศัพท์มาติดต่อทั้งวันทั้งคืน สร้างความเดือดร้อนรำคาญ

---

[30] ญาณพล ยั่งยืน “อาชญากรรมทางคอมพิวเตอร์.” ศูนย์ข้อมูลข้อสนเทศ : สำนักงานตำรวจแห่งชาติ

3.1.3 หน่วยงานที่เกี่ยวข้องกับคดีอาชญากรรมทางคอมพิวเตอร์

ซึ่งเมื่อเกิดปัญหาคดีอาชญากรรมคอมพิวเตอร์มากมายหลายรูปแบบ ในประเทศไทยจึงมีหน่วยงานที่รับผิดชอบหลัก ๆ อยู่ 2 หน่วยงาน คือ [31]

1. ศูนย์เทคโนโลยีสารสนเทศกลาง สังกัดสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ตามกฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการที่เรียกชื่ออย่างอื่นในสำนักงานตำรวจแห่งชาติ พ.ศ. ๒๕๔๘ ลงวันที่ ๓๐ มิถุนายน ๒๕๔๘ จนถึงปัจจุบัน มีอำนาจหน้าที่ดังต่อไปนี้

(1) จัดทำยุทธศาสตร์แผนแม่บทและแผนปฏิบัติการเทคโนโลยีสารสนเทศของสำนักงานตำรวจแห่งชาติให้สอดคล้องกับมาตรฐานกลางและนโยบายเทคโนโลยีสารสนเทศและ การสื่อสารของชาติ

(2) ดำเนินการเกี่ยวกับการวางระบบหรือพัฒนาระบบข้อมูลและประมวลผลข้อมูลข้อสนเทศของสำนักงานตำรวจแห่งชาติ

(3) ส่งเสริม ประสานงาน เผยแพร่ ให้คำปรึกษาแนะนำเกี่ยวกับการ พัฒนาระบบสารสนเทศและการบริหารงานของสำนักงานตำรวจแห่งชาติ

(4) ดำเนินการเกี่ยวกับการเผยแพร่การให้บริการข้อมูลข้อสารสนเทศต่าง ๆ รวมทั้งการให้คำปรึกษาแนะนำหรือฝึกอบรมการใช้เครื่องคอมพิวเตอร์และการใช้ โปรแกรมคอมพิวเตอร์

(5) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติ งานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

ส่วนราชการของศูนย์เทคโนโลยีสารสนเทศกลาง แบ่งออกได้เป็น 2 กลุ่มงาน ดังนี้

1. ฝ่ายประมวลผลข้อมูล
2. กลุ่มงานเทคโนโลยีสารสนเทศ แบ่งออกเป็น 3 กลุ่มย่อย ดังนี้

---

[31] http://thaicert.nectec.or.th

(1) กลุ่มงานเทคโนโลยีสารสนเทศ

หน้าที่ความรับผิดชอบ

1. งานบริหารจัดการและพัฒนาระบบสารสนเทศ มีหน้าที่รับผิดชอบ ดังนี้

1.1 ศึกษาวิเคราะห์ ออกแบบระบบสารสนเทศ

1.2 พัฒนาโปรแกรม (Coding)

1.3 ติดตั้ง บำรุงรักษา แก้ไขระบบสารสนเทศ

1.4 ดูแลรับผิดชอบในการตรวจสอบและทดสอบระบบก่อนการใช้งานจริง

1.5 กำหนดมาตรฐานข้อมูล

1.6 วิเคราะห์ ออกแบบและพัฒนาระบบสารสนเทศภูมิศาสตร์

1.7 งานอื่น ๆ ที่ผู้บังคับบัญชามอบหมาย

2. งานบริหารจัดการระบบเครื่อข่าย มีหน้าที่รับผิดชอบ ดังนี้

2.1 บริหารระบบเครือข่ายการเชื่อมโยงระหว่างคอมพิวเตอร์แม่ข่าย (Server) ส่วนกลางกับเครื่องลูกข่าย (Client) ในหน่วยงานอื่น ๆ ของสำนักงานตำรวจแห่งชาติ

2.2 ควบคุม ดูแล รักษาความปลอดภัยและแก้ปัญหาการใช้งานระบบเครือข่าย

2.3 วางแผน ดำเนินการจัดตั้งและขยายระบบเครือข่าย

2.4 บำรุงรักษาและปรับปรุงประสิทธิภาพของระบบเครือข่าย

2.5 งานอื่น ๆ ที่ผู้บังคับบัญชามอบหมาย

3. งานบริหารจัดการระบบฐานข้อมูล มีหน้าที่รับผิดชอบ ดังนี้

3.1 การบริหารจัดการ แก้ไขปรับปรุง รวมทั้งบำรุงรักษาฐานข้อมูล

3.2 ควบคุมเข้าถึงข้อมูล ดูแลรักษาความปลอดภัย ความถูกต้องของฐานข้อมูล

3.3 สนับสนุนการสืบค้นข้อมูลความต้องการของผู้ใช้งานและผู้บริหาร

3.4 วางแผนและดำเนินการเพิ่มประสิทธิภาพของระบบจัดการฐานข้อมูล

3.5 งานอื่น ๆ ที่ผู้บังคับบัญชามอบหมาย

4. งานบริหารจัดการระบบเครื่องคอมพิวเตอร์ มีหน้าที่รับผิดชอบ ดังนี้

4.1 ควบคุม ดูแล การทำงานของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ส่วนกลางกับเครื่องลูกข่าย (Client) รวมทั้งอุปกรณ์ที่เกี่ยวข้อง

4.2 ดูแลรักษาความปลอดภัยของระบบเครื่องคอมพิวเตอร์ทางด้านกายภาพและด้านระบบซอฟต์แวร์

4.3 ปรับปรุงประสิทธิภาพการใช้งานระบบซอฟต์แวร์

4.4 ปรับปรุง และปรับแต่งระบบเครื่องคอมพิวเตอร์แม่ข่าย ให้สามารถทำงานได้อย่างมีประสิทธิภาพ

4.5 งานอื่นๆ ที่ผู้บังคับบัญชามอบหมาย

5. งานวิจัยและพัฒนาเทคโนโลยีสารสนเทศ

5.1 ศึกษาค้นคว้าเทคโนโลยีที่เหมาะสมกับงานมาพัฒนาองค์กร

5.2 งานอื่นๆ ที่ผู้บังคับบัญชามอบหมาย

6. งานอำนวยการทางเทคนิค มีหน้าที่รับผิดชอบ ดังนี้

6.1 ธุรการทั่วไปของกลุ่มงาน

6.2 งานอื่นๆ ที่ผู้บังคับบัญชามอบหมาย

7. งานอื่นๆ ที่ผู้บังคับบัญชามอบหมาย

(2) กลุ่มงานเทคโนโลยีสารสนเทศ

หน้าที่ความรับผิดชอบ

งานดูแลและพัฒนาเว็บไซต์ มีหน้าที่รับผิดชอบ ดังนี้

1. ดูแลและพัฒนาเว็บไซต์ของสำนักงานตำรวจแห่งชาติ
2. ให้บริการเกี่ยวกับขอใช้ระบบอินเทอร์เน็ตของสำนักงานตำรวจแห่งชาติ
3. งานอื่นๆ ที่ผู้บังคับบัญชามอบหมาย

(3) กลุ่มงานเทคโนโลยีสารสนเทศ

หน้าที่ความรับผิดชอบ

งานสนับสนุนเทคนิคส่วนกลางและส่วนภูมิภาค มีหน้าที่รับผิดชอบ ดังนี้

1. ติดตั้งและบำรุงรักษาระบบคอมพิวเตอร์ และซอฟต์แวร์ที่เกี่ยวข้องกับระบบสารสนเทศที่ได้รับมอบหมายส่วนกลางและส่วนภูมิภาค

2. บริการให้ความรู้ ตอบข้อซักถามและแก้ปัญหาให้กับผู้ใช้งานในระบบสารสนเทศที่อยู่ในความรับผิดชอบ

3. งานอื่นๆ ที่ผู้บังคับบัญชามอบหมาย

2. สำนักงานเทคโนโลยีและสารสนเทศ

สำนักงานคดีเทคโนโลยีและสารสนเทศ เป็นหน่วยงานในสังกัด กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม มีภาระหน้าที่ดังต่อไปนี้ [32]

[32] www.dsi.go.th

1. ปฏิบัติงานด้านการป้องกัน ปราบปรามและสืบสวนผู้กระทำความผิดทางคดีเทคโนโลยีและสารสนเทศ
2. ปฏิบัติงานด้านการสอบสวนและดำเนินคดีกับผู้กระทำความผิดทางคดีเทคโนโลยีและสารสนเทศ
3. ปฏิบัติงานวิเคราะห์และพิสูจน์ความผิดทางเทคโนโลยีและสารสนเทศ
4. ปฏิบัติงานด้านการป้องกัน ปราบปราม สืบสวนและสอบสวนผู้กระทำความผิดในคดีอื่นที่ได้รับมอบหมาย
5. ดำเนินการวิเคราะห์ วิจัย วางแผนงาน บริหารจัดการและประสานงานเพื่อป้องกันและปราบปรามการกระทำความผิดทางคดีเทคโนโลยีและสารสนเทศ
6. ดำเนินการเก็บรักษาพยานหลักฐานและของกลางในคดี
7. ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย
8. ดำเนินการเกี่ยวกับข้อมูลและสถิติคดีในงานที่รับผิดชอบ

แบ่งส่วนราชการออกเป็น

1. ฝ่ายบริหารทั่วไป
2. ส่วนคดีเทคโนโลยีและสารสนเทศ 1
3. ส่วนคดีเทคโนโลยีและสารสนเทศ 2
4. ส่วนคดีเทคโนโลยีและสารสนเทศ 3

ปัจจุบันได้มี พันตำรวจเอกญาณพล ยั่งยืน เป็นผู้บัญชาการสำนักงานคดีเทคโนโลยีและสารสนเทศ

3.1.4 สภาพปัญหากับมาตรการทางกฎหมายวิธีบัญญัติในประเทศไทย

ประเทศไทยไม่มีกฎหมายสารบัญญัติเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์โดยเฉพาะซึ่งหากมีกระทำผิดเกิดขึ้น ก็ต้องพยายามปรับใช้กฎหมายอาญาที่มีอยู่ไปพลางก่อน ส่วนสิ่งที่สำคัญที่สุด คือ การนำตัวผู้กระทำความผิดมาลงโทษ ซึ่งมีปัญหาเกี่ยวข้อง ได้แก่ [33]

---

[33] วัลลิกา อุ่นศรี. “ ปัญหาการรวบรวมและพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีอาญา.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2544. น. 60

1. ปัญหาการค้นและยึด

กฎหมายวิธีพิจารณาความอาญาของไทยบัญญัติถึงหลักการออกหมายค้นว่าจะต้องสามารถระบุได้ว่าจะค้นสิ่งใด ซึ่งอยู่ที่ใด แต่ข้อมูลคอมพิวเตอร์บางกรณีไม่อาจระบุได้ว่าอยู่ในรูปแบบใด เก็บไว้ที่ใด ประกอบด้วยสิ่งใดบ้าง ตลอดจนหากในการค้นตามหมายค้น พบการกระทำความผิดอื่น ซึ่งไม่เกี่ยวกับความผิดที่มีการออกหมายค้น จะสามารถดำเนินการกับสิ่งที่พบในขณะนั้นได้หรือไม่ การค้นข้อมูลในระบบเครือข่ายมีขอบเขตเพียงใด กล่าวคือสามารถค้นเข้าไปในข้อมูลที่อยู่ต่างประเทศได้หรือไม่ จะสามารถทำสำเนาข้อมูลได้หรือไม่ การยึดพยานหลักฐานที่เป็นข้อมูลในคอมพิวเตอร์ ซึ่งเป็นสิ่งไม่มีรูปร่าง จะทำได้โดยวิธีใด หากข้อมูลที่จะยึดมาจากระบบเครือข่ายคอมพิวเตอร์ของผู้อื่น และมีอยู่มากมายหลายแห่ง จะสามารถยึดทั้งระบบได้หรือไม่ จึงน่าคิดว่าควรมีกฎหมายให้อำนาจพิเศษแก่เจ้าพนักงานในการตรวจค้นยึด หลักฐานพยานหรือไม่

2. ปัญหาอำนาจ และความสามารถของเจ้าพนักงานที่บังคับใช้กฎหมาย

เทคโนโลยีคอมพิวเตอร์เป็นเ รื่องใหม่ เจ้าพนักงานบังคับใช้กฎหมายยังขาดความรู้ความเข้าใจ บุคลากรที่มีความรู้ความสามารถยังมีอยู่จำกัด ทำให้การป้องกันอาชญากรรมคอมพิวเตอร์ยังขาดประสิทธิภาพ จึงน่าคิดว่าควรมีการจัดตั้งหน่วยงานเฉพาะกิจเกี่ยวกับอาชญากรรมคอมพิวเตอร์ เพื่อให้มีเจ้าหน้าที่ที่มี ความรู้ความชำนาญเฉพาะในการดำเนินคดีอาชญากรรมประเภทนี้ นอกจากนี้จึงควรปรับปรุงกฎหมายวิธีสบัญญัติในเรื่องการให้อำนาจพนักงานเจ้าหน้าที่ให้เหมาะสม เพื่อประสิทธิภาพในการบังคับใช้กฎหมาย

3. ปัญหาพยานหลักฐาน

ปัญหาพยานหลักฐานนี้น่าวิเคราะห์ว่าในชั้นสอบสวน พนักงานสอบ สวนได้รวบรวมพยานหลักฐานได้แล้วพนักงานอัยการจะใช้ดุลยพินิจอย่างไรในการพิจารณาส่งฟ้อง เพราะถ้าหากพนักงานสอบสวนได้มาด้วยความยากลำบาก แต่พนักงานอัยการสั่งไม่ฟ้อง ก็จะทำให้เกิดความสิ้นเปลืองทางเศรษฐกิจ บุคลากร และเวลาในการปฏิบัติหน้าที่อย่างน่าเสียดาย แต่เมื่อถึงชั้นศาลแล้ว ข้อมูลคอมพิวเตอร์เป็นพยานอิเล็กทรอนิกส์ จะจัดเป็นพยานเอกสารหรือพยานวัตถุตามกฎหมายเรื่องพยานหลักฐาน และศาลจะรับฟังพยานอิเล็กทรอนิกส์ได้หรือไม่ หากทำสำเนาข้อมูลคอมพิวเตอร์เพื่อเป็นพยานหลักฐานจะเกิดปัญหาว่าศาลจะรับฟังสำเนาพยานหลักฐานหรือไม่ กฎหมายของไทยควรกำหนดให้มีพยานผู้เชี่ยวชาญในเรื่องนี้

4. สภาพปัญหาระหว่างประเทศ

แต่ละประเทศมีภูมิหลังทางประวัติศาสตร์ ศีลธรรม จารี ตประเพณีต่างกัน ทำให้ส่งผลถึงกฎหมายบางเรื่องแตกต่างกัน ซึ่งทำให้กฎหมายอาญาแต่ละประเทศแตกต่างกันได้ อันทำให้เป็นอุปสรรคอยู่แล้ว ในกรณี ที่ว่าการกระทำอย่างหนึ่งอันเกิดในประเทศที่บางเรื่องไม่ถือว่า

เป็นความผิดแต่อีกประเทศหนึ่งถือว่าเป็นความผิด แม้แต่กฎหมายของแต่ละประเทศจะบัญญัติการกระทำใดบนเครือข่ายอินเตอร์เน็ตว่าเป็นความผิดเหมือนกัน ก็ยังคงมีปัญหาที่พบอีกคือ

ปัญหาเขตอำนาจศาล

ปัญหาเรื่องเขตอำนาจศาลนี้เกิดเพราะอาชญากรรมคอมพิวเตอร์มีลักษณะ ไร้พรมแดน เกี่ยวพันกันได้หลายประเภท ผู้กระทำความผิด ผู้เสียหาย สถานที่เกิดการกระทำความผิด และสถานที่เกิดผลแห่งการกระทำ ไม่จำเป็นต้องอยู่ในประเทศเดียวกัน ทำให้เกิดปัญหาว่าความผิดที่เกิดขึ้นในประเทศใด แล ะจะสรุปได้อย่างไรว่าประเทศใดมีอำนาจสอบสวน จะสอบสวนในมลรัฐหรือ สถานีตำรวจใด

ปัญหาความร่วมมือระหว่างประเทศในการดำเนินการคดี

สืบเนื่องมาจากปัญหาเขตอำนาจศาล หากต้องสืบสวน สอบสวน และดำเนินคดีในประเทศหนึ่ง จะขอความร่วมมือกับประเทศที่เกี่ยวข้องได้หรือไม่ และอยู่ในขอบเขตมากน้อยเพียงใด

อาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมในรูปแบบใหม่ที่เข้าไปเกี่ยวข้องในทุกพื้นที่มนุษย์ใช้ชีวิต ในอนาคตต้องพัฒนากฎหมายให้ทันต่อการปราบปรามอาชญากรพวกนี้ เพราะเป็นอันตรายมากต่อบุคคล และทำลายสังคมร้ายแรง จึงเป็นเรื่องที่ทุกหน่วยต้องให้ ความร่วมมือกันต่อไป

3.2 มาตรการทางกฎหมายที่ให้อำนาจพนักงานสอบสวนในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ในประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกานับว่าเป็นประเทศเสรีประชาธิปไตยที่มีการต่อสู้เพื่อประสิทธิและเสรีภาพของประชาชนมายาวนาน แนวความคิด ในเรื่องสิ ทธิและเส รีภาพของปัจเจกชนของสหรัฐอเมริกา จึงเป็นแนวความคิดทาง กฎหมาย ธรรมชาติที่ให้ความคุ้มครองสิทธิและเสรีภาพของประชาชนเป็นอย่างสูง และเนื่องจากประเทศสหรัฐอเมริกาเป็นประเทศผู้นำทางด้านเทคโนโลยี ทั้งคอมพิวเตอร์และระบบอินเตอร์เน็ตที่มีการแพร่ขยายอย่างกว้างขวาง เทคโนโลยีดังกล่าวนำความสะดวกสบายมาสู่ชีวิตประจำวันทำให้สังคมของปร ะเทศสหรัฐเป็นสังคมที่มีการใช้เทคโนโลยีสารสนเทศนี้อย่างมากมายแทบทุกสาขาอาชีพ

อาชญากรรมไซเบอร์ที่เกิดอย่างแพร่หลายก่อให้เกิดความเสียหายอย่างมหาศาลนับประการ ประเทศสหรัฐ อเมริกา จึงเริ่มตื่นตัวหวนกลับมาพิจ ารณา ทบทวนจุดสมดุลแห่งความขัดแย้งระหว่างการให้ความคุ้มครองสิทธิส่วนบุคคลกับอำนาจใช้กฎหมายของรัฐอีกครั้ง

การศึกษากฎหมายเกี่ยวกับประเทศที่ประสบปัญหามาก่อน และได้หาหาทางแก้ไขแล้ว เช่นประเทศสหรัฐอเมริกาซึ่งเผชิญกับปัญหาอาชญากรรมคอมพิวเตอร์มากที่สุดได้มีการจัดตั้ งหน่วยงานที่มีทั้งภาครัฐและเอกชน เช่น National Computer Crimes Squad ซึ่งสังกัดอยู่ใน F.B.I. ทำหน้าที่สืบสวนสอบสวนและจัดตั้ง Computer Analysis and Response Team ชื่อย่อ CART ทำหน้าที่ตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ จึงเป็นทางลัดในการนำไปสู่แนวทางการปรับปรุงกฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ที่จะเกิดขึ้นในประเทศไทยได้เป็นอย่างดี

ประเทศสหรัฐอเมริกา ในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มีมาตั้งแต่ปี ค .ศ. 1984 คือกฎหมาย Computer fraud and abuse act (CFAA) [34] ซึ่งมีแนวความคิดในการบัญญัติกฎหมายเพื่อใช้ดำเนินคดีกับการกระทำความผิดต่อคอมพิวเตอร์รูปแบบต่างๆ การที่สภาคองเกรสเห็นว่า การกระทำรู ปแบบใหม่นี้มีลักษณะพิเศษที่แตกต่างไปจากความผิดรูปแบบเดิม เพราะเป็นการกระทำที่เกี่ยวข้องกับสิ่งที่ไม่มีรูปร่างทำให้การจะดำเนินคดี โดยอาศัยความผิดฐาน Theft และ Larceny ตามกฎหมายเดิมเป็นเรื่องที่ยากลำบาก เพื่อแก้ปัญหาเรื่องนี้ก็ควรที่จะบัญญัติกฎหมายใหม่ขึ้นมามากกว่าพยายามจะนำกฎหมายเก่ามาใช้ดำเนินคดีกับความผิดรูปแบบใหม่

CFAA 18 U.S.C. มาตรา 1030 กำหนดให้การเข้าถึงข้อมูลคอมพิวเตอร์ในกรณีดังต่อไปนี้เป็นการกระทำความผิด [35]

1. ผู้ใด โดยรู้หรือเข้าถึงคอมพิวเตอร์ โดยอำนาจ หรือเกินขอบเขต และด้วยวิธีดังกล่าวได้ไปซึ่งข้อมูล ที่รัฐบาล สหรัฐอเมริกา โดยคำสั่งของฝ่ายบริหารหรือกฎหมายลายลักษณ์อักษรกำหนดให้มีการคุ้มครอง เพื่อป้องกันการเปิดเผยข้อมูลนั้นโดยปราศจากอำนาจ เนื่องจากเหตุผลเกี่ยวกับความ ปลอดภัยของประเทศหรือเกี่ยวกับการต่างประเทศ หรือเป็นข้อมูล ใด ๆ ที่เป็นความลับตามความหมายของมาตรา 11 แห่ง Atomic enegy Act of 1954 ซึ่งมีเหตุผลอันเชื่อได้ว่าข้อมูลที่ได้รับมานั้น อาจถูกนำไปใช้เพื่อสร้างความเสียหายให้กับสหรัฐอเมริกา หรือเพื่อก่อให้เกิดประโยชน์กับรัฐต่างชาติใด ๆ บุคคลนี้โดยเจตนาติดต่อสื่ อสาร ส่ง รับส่ง หรือเป็นเหตุผล ให้มีการติดต่อสื่อสาร ส่ง รับ หรือพยายามที่จะติดต่อสื่อสาร ส่ง รับส่ง ข้อมูล ดังกล่าวไปยังบุคคลใด ซึ่งไม่มีสิทธิได้รับข้อมูลนั้น หรือเจตนาเก็บข้อมูลนั้นไว้โดยไม่ยอมส่งข้อมูลดังกล่าวไปให้แก่เจ้าหน้าที่ของรัฐผู้มีสิทธิที่จะรับข้อมูลนั้นได้

---

[34] โปรดดู Adams, Jo-Ann M. “CONTROLLING CYBERSPACE: APPLYING THE COMPUTER FRAUD AND ABUSE ACT TO

[35] พรทิพย์ ตันฑวนันท์ , “อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์ :” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548 หน้า 68

2. ผู้ใดเข้าถึงคอมพิวเตอร์ โดยปราศจากอำนาจ หรือเกินอำนาจ เข้าถึงโดยชอบโดยเจตนา และเพื่อให้ได้รับไปซึ่ง
    a. ข้อมูลซึ่งเก็บไว้ในบันทึกทางการเงินของสถาบันการเงิน หรือของผู้ออกบัตร ตามที่กำหนดไว้ในมาตรา 1602 (n) ของหมวด 15 หรือข้อมูลซึ่งเก็บไว้ในแฟ้มของสำนักงานข้อมูลของผู้บริโภค ซึ่งมีข้อความอย่างเดียวกันกับที่กำหนดไว้ใน Fair Credit Reporting Act (15 U.S.C1681 et seg)
    b. ข้อมูลจากหน่วยงาน หรือสำนักงานใด ๆ ของสหรัฐอเมริกา หรือ
    c. ข้อมูลจากคอมพิวเตอร์ที่ได้รับความคุ้มครอง ถ้าการกระทำนั้น เกี่ยวข้อง กับการติดต่อสื่อสารระหว่างมลรัฐ หรือการติดต่อสื่อสารกับต่างประเทศ
3. ผู้ใด โดยเจตนาเข้าถึงคอมพิวเตอร์ของหน่วยงาน หรือสำนักงานของสหรัฐอเมริกาโดยปราศจากอำนาจ ซึ่งคอมพิวเตอร์นั้นมีไว้เพื่อการใช้งานสำหรับรัฐบาลสหรัฐอเมริกาโดยเฉพาะ หรือในกรณีที่คอมพิวเ ตอร์มิได้ถูกใช้สำหรับสหรัฐอเมริกา แต่ถูกใช้โดย หรือสำหรับรัฐบาลสหรัฐอเมริกา และการกระทำดังกล่าวส่งผลกระทบต่อการใช้งานของรัฐบาลสหรัฐอเมริกา หรือการใช้งานสำหรับรัฐบาลสหรัฐอเมริกา
4. ผู้ใด โดยรู้ และโดยเจตนาที่จะฉ้อโกง เข้าถึงคอมพิวเตอร์ที่ได้รับการคุ้มครองโดยปราศจากอำนาจ หรือเกินขอบอำนาจการเข้าถึงโดยชอบ และด้วยวิธีการดังกล่าวทำให้เกิดการฉ้อโกงโดยเจตนา และได้รับไปซึ่งสิ่งมีค่าใด ๆ เว้นแต่วัตถุของการฉ้อโกงและสิ่งของที่ได้มา รวมเฉพาะการใช้คอมพิวเตอร์ และมูลค่าของการใช้ดังกล่าวนั้นไม่เกิน 5,000 เหรียญสหรัฐในช่วงเวลา 1 ปี
5. ผู้ใด โดยรู้ และโดยเจตนาที่จะฉ้อโกงทางการค้า (ตามที่กำหนดไว้ในมาตรา 1029) ในรหัสผ่านใด ๆ หรือข้อมูลอื่นที่มีลักษณะคล้ายคลึงกัน โดยการใช้คอมพิวเตอร์ซึ่งอาจถูกเข้าถึงโดยปราศจากอำนาจถ้า
    a. การพาณิชย์นั้นส่งผลกระทบต่อการพาณิชย์ระหว่างรัฐ หรือระหว่างประเทศหรือ
    b. คอมพิวเตอร์ดังกล่าวถูกใช้โดยรัฐบาลของสหรัฐอเมริกา หรือถูกใช้สำหรับรัฐบาลของสหรัฐอเมริกา
6. ผู้ใด โดยเจตนาที่จะกรรโชกเอาเงิน หรือสิ่งมีค่าอื่นใดจากผู้อื่น ส่งการติดต่อสื่อสารใด ๆ ในทางการค้าระหว่างมลรัฐหรือระหว่างประเทศ ที่มีลักษณะเป็นการข่มขู่ว่าจะก่อให้เกิดความเสียหายต่อคอมพิวเตอร์ที่ได้รับการคุ้มครอง

การไม่มีอำนาจเข้าสู่ระบบคอมพิวเตอร์ตามกฎหมายของประเทศสหรัฐอเมริกานั้นถือว่าเป็น Theft of Computer Service[36] เพราะเป็นการเข้าไปใช้บริการโดยไม่มีอำนาจ ทั้งที่ไม่ได้ก่อให้เกิดความเสียหายอย่างใดเลยต่อระบบการทำงานของเครื่อง ทั้งนี้นักกฎหมายอเมริกันให้ความเห็นว่า ถือว่าเป็นความเสี่ยงต่อการก่อให้เกิดผลเสียหายต่อข้อมูลสารสนเทศได้และผู้กระทำย่อมรู้ดีว่าความเสียหายในอนาคตจะปรากฏขึ้น และการเข้าไปโดยไม่มีอำนาจเช่นนี้อาจทำให้เจ้าของสิทธิไม่อาจเข้าสู่ระบบได้

เนื่องจากกฎหมาย Computer fraud and abuse act (CFAA) ในปี ค.ศ. 1984 ไม่สามารถครอบคลุมความผิดได้ทั้งหมด จึงมีการแก้ไขเรื่อยมาในปี ค .ศ. 1988, 1989 และ 1990 ตามลำดับ จนกระทั่งสภาคองเกรสได้มีมติให้ผ่านกฎหมายใหม่ ๆ ออกมาเสริม เช่น The National Information Infrastructure Protection Act of 1996 (NIPA) และเพิ่มเติมการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ใน U.S. Code title 18 มาตรา 1030 (18 U.S.C.A. section 1030)

รัฐธรรมนูญของประเทศมีบทบัญญัติที่เป็นหลักประกันสิทธิของประชาชนมิให้ถูกละเมิดโดยรัฐบาลที่เรียกว่า Bill of Rights ถึง 10 บท ซึ่งเป็นการกำหนดมาตรฐานขั้นต่ำหรือจำกัดขอบเขตการใช้อำนาจของเจ้าหน้าที่ทั้งหลายที่เกี่ยวข้องในกระบวนยุติธรรมทั้งในระดับสหพันธรัฐและมลรัฐ โดยเฉพาะเจ้าหน้าที่ตำรวจและอัยการที่จะต้องปฏิบัติตามกฎเกณฑ์ที่ศาลสูงสุดได้วางไว้เท่านั้น

3.2.1 โครงสร้างทางกฎหมาย สหรัฐอเมริกา ด้านการก่อการร้ายและอาชญากรรมทางไซเบอร์

บรรดากฎหมายต่างๆ ของรัฐบาลสหรัฐอเมริกา ที่ครอบคลุมเกี่ยวกับ การสืบสวนและดำเนินคดีกับบุคคล ซึ่งได้กระทำ การก่อการร้ายและอาชญากรรมทางไซเบอร์ ที่น่าสนใจมีดังนี้

Title 18, USC 1029

กฎหมายของสหรัฐอเมริกา Title 18, USC 1029, Fraud and Related Activity in Connection with Access Devices ว่าด้วยการฉ้อฉลและกิจกรรมที่เกี่ยวเนื่องกับกลไกการเข้าถึง [ระบบเครือข่ายอินเทอร์เน็ต]

---

[36] See Edward M. Wise, United States Computer Crimes and Other Crimes against Information Technology in U.S.A. Review of penal Law 1992

- กฎหมายนี้ครอบคลุม การดำเนินคดีกับบุคคลซึ่งลักลอบค้า รหัสหรือ หมายเลขบัตรเครดิตทางอินเทอร์เน็ต
- กฎหมายนี้ครอบคลุม การดำเนินคดีบุคคลซึ่งใช้ซอฟท์แวร์หรือฮาร์ดแวร์ ในการผลิต หรือแพร่กระจายรหัสหรือหมายเลขบัตรเครดิต
- Title 18, USC 1029 Penalties (บทลงโทษ)

Title 18, USC 1030

กฎหมายของสหรัฐอเมริกา Title 18, USC 1030, Fraud and Related Activity in Connection with Computers ว่าด้วยการฉ้อฉลและกิจกรรมที่เกี่ยวเนื่องกับคอมพิวเตอร์

- กฎหมายนี้ใช้ดำเนินคดีกับบุคคลซึ่งจงใจบุกเข้าไปในคอมพิวเตอร์โดยไม่ได้รับอนุญาต อันเป็นคอมพิวเตอร์ซึ่งอยู่ในการปกป้องของรัฐบาลสหรัฐอเมริกา U.S. protected computer
- คอมพิวเตอร์ซึ่งอยู่ในการปกป้องของรัฐบาลสหรัฐอเมริกา หมายถึง คอมพิวเตอร์ของ รัฐบาล รวมทั้งคอมพิวเตอร์ซึ่งได้ถูกระบุไว้โดยรัฐบาลว่าเป็นคอมพิวเตอร์ที่เกี่ยวข้องกับการพาณิชย์ระหว่างมลรัฐ
- จะต้องเป็นกรณีที่ก่อให้เกิดความเสียหายที่เกินกว่าจำนวนเงิน $5,000 หรือก่อให้เกิดผลร้ายต่อความปลอดภัยของมหาชนและความมั่นคงของชาติ
- อีกทั้งกฎหมายนี้จะครอบคลุมการดำเนินคดีกับบุคคลซึ่งจงใจปล่อยไวรัส หรือหนอน worms เข้าไปในคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเพื่อก่อให้เกิดความเสียหาย Title 18, USC 1030 Penalties (บทลงโทษ)

Title 18, USC 1362

กฎหมายของสหรัฐอเมริกา Title 18, USC 1362, Communications Lines, Stations, or Systems. ว่าด้วยสายเคเบิ้ล, สถานี หรือ ระบบในการสื่อสาร

- กฎหมายนี้ใช้ในการดำเนินคดีกับบุคคลซึ่ง จงใจสร้างผลร้าย หรือทำลายระบบการสื่อสาร คมนาคม
- อีกทั้งกฎหมายนี้อาจใช้ในการดำเนินคดีกับบุคคลซึ่ง วางแผนที่จะดำเนินการละเมิดกฎหมายดังกล่าวนี้ Title 18, USC 1362 Penalties (บทลงโทษ)
- บุคคลซึ่งถูกตัดสินว่าได้ละเมิดกฎหมาย มาตราที่ 1362 อาจถูกลงโทษจำคุก 10 ปี การทำความผิดครั้งแรก

Title 18, USC 2511

กฎหมายของสหรัฐอเมริกา Title 18 USC 2511, Interception and Disclosure of Wire, Oral, or Electronic Communications. ว่าด้วยการดักเอาและเปิดเผยการสื่อสารโดยทางสาย ไม่ว่าจะเป็นการสื่อสารทางเสียง หรือข้อความ แบบอิเล็กทรอนิกส์

- กฎหมายนี้ใช้ในการดำเนินคดีกับบุคคลซึ่งจงใจดักจับการสื่อสารโดยทางสาย ทั้งที่เป็นการสื่อสารแบบเสียงและแบบอิเล็กทรอนิกส์
- อีกทั้งกฎหมายนี้ สามารถใช้ดำเนินคดีกับบุคคลซึ่งใช้เครื่องมือใดๆเพื่อดักเอาการสื่อสาร Title 18, USC 2511 Penalties (บทลงโทษ)
- บุคคลซึ่งถูกตัดสินว่าได้ละเมิดกฎหมาย มาตราที่ 2511 อาจถูกลงโทษจำคุก 5 ปี สำหรับการทำความผิดครั้งแรก

Title 18, USC 2701

- กฎหมายของสหรัฐอเมริกา Title 18, USC 2701, Unlawful Access to Stored Communication.ว่าด้วยการเข้าถึง โดยไม่ถูกต้องตามกฎหมาย เพื่อลักลอบเอาการสื่อสารที่ได้ถูกเก็บไว้
- กฎหมายนี้ใช้ในการดำเนินคดีกับบุคคลซึ่งจงใจเข้าไปในที่ใดซึ่งเป็น ศูนย์ให้บริการและเก็บการสื่อสาร โดยไม่ได้รับอนุญาต Title 18, USC 2701 Penalties (บทลงโทษ)
- บุคคลซึ่งถูกตัดสินว่าได้ละเมิดกฎหมาย มาตราที่ 2701 อาจถูกลงโทษจำคุก 2 ปี สำหรับการทำความผิดครั้งแรก

Title 18, USC 2702

กฎหมายของสหรัฐอเมริกา Title 18, USC 2702, Disclosure of Contents ว่าด้วยการเปิดเผยเนื้อหา

- กฎหมายนี้ใช้ในการดำเนินคดีกับบุคคลซึ่งจงใจ เปิดเผยหรือแฉการสื่อสารหรือข้อมูลแบบอิเล็กทรอนิกส์ซึ่งได้มีการเก็บไว้ ณ ที่ใด
- กฎหมายนี้เป็นการให้อำนาจในการดำเนินคดีแก่บุคคลซึ่ง มอบข้อมูลให้แก่ผู้รับคนใดที่ไม่ได้รับอนุญาตให้มีข้อมูลนั้นไว้ในครอบครอง

Patriot Act รัฐบัญญัติว่าด้วยความรักชาติ

- รัฐบัญญัตินี้ ได้ผ่านออกมา โดยนัยหนึ่งเป็นการตอบโต้การโจมตีโดยผู้ก่อการร้าย ถล่มอาคารเวิลด์เทรด ในกรุงนิวยอร์ค และอาคารเพนตากอน ในกรุงวอชิงตัน เมื่อวันที่ 11 กันยายน 2001

Patriot Act รัฐบัญญัติว่าด้วยความรักชาติ

- รัฐบัญญัตินี้ เป็นการเสริมกฎหมายที่มีอยู่ในขณะนั้น โดยการขยายและเพิ่มโทษสำหรับอาชญากรรมซึ่งกระทำโดยการใช้คอมพิวเตอร์เป็นเครื่องมือ
- รัฐบัญญัติฉบับนี้ มีบทเฉพาะซึ่งว่าด้วยการก่อการร้ายโดยทางไซเบอร์
- รัฐบาลสหรัฐอเมริกา จะต้องขยายขีดความสามารถทางด้านการพิสูจน์หลักฐานคดี แบบไซเบอร์ Patriot Act บัญญัติว่าด้วยความรักชาติ

รัฐบัญญัติปี 2002 ของสหรัฐอเมริกา ว่าด้วยความรักชาติ United States Patriot Act of รัฐบัญญัตินี้ ให้อำนาจในการที่จะ :

- ดักฟังการสื่อสารในรูปแบบเสียงทางอินเทอร์เน็ต
- ขยายคำจำกัดความของคำว่า คอมพิวเตอร์ที่อยู่ในความคุ้มครอง “Protected Computer” ให้รวมถึงคอมพิวเตอร์ในต่างประเทศด้วย
- เพื่อชี้ให้เห็นถึงการขึ้นต่อกันและกัน ในบรรดาคอมพิวเตอร์ ทั้งหมดที่อยู่ในระบบเครือข่ายอินเทอร์เน็ต

3.2.2 โครงสร้างทางกฎหมายระหว่างประเทศ

- ปัญหาสำคัญในการสืบสวนอาชญากรรมและการก่อการร้ายโดยทางไซเบอร์ คือการขาดโครงสร้างทางกฎหมายที่มิได้มีการกำหนดไว้รองรับ
- ปัญหาเรื่องเขตอำนาจศาล และ การขาดกฎหมายที่จะครอบคลุมเรื่องนี้ในบางประเทศ ทำให้เป็นงานยากอย่างยิ่งในการดำเนินงานสืบสวนข้ามพรมแดน
- อาชญากรและผู้ก่อการร้ายประเภทไซเบอร์ อาศัยความได้เปรียบจากช่องว่างนี้
- คนร้ายสามารถ“โดดข้าม”จากระบบคอมพิวเตอร์หนึ่งไปอีกระบบหนึ่ง ในหลายประเทศซึ่งไม่มีกฎหมายที่เหมาะสมในการแก้ปัญหาหรือรับมือกับอาชญากรรมและการก่อการร้ายโดยทางไซเบอร์

สหรัฐอเมริกา ได้เรียนรู้จากประสบการณ์ในอดีตว่า ในการที่จะป้องกันปราบปรามอาชญากรรม และการก่อการร้าย โดยทางไซเบอร์ จะต้องสร้างกฎหมายซึ่ง พร้อมที่จะปรับเปลี่ยน ให้เหมาะสมกับเทคโนโลยีใหม่ๆ ซึ่งมีเข้ามาในวงการนี้อยู่เสมออย่างต่อเนื่อง การต่อต้านการก่อการร้าย โดยทางไซเบอร์ ที่จะมีประสิทธิผล จะต้องมีโครงสร้างทางกฎหมาย ซึ่งจะให้อำนาจและเครื่องมือแก่พนักงานสืบสวนสอบสวน และอัยการ สามารถอาศัยอำนาจทางกฎหมายที่จะใช้ในการต่อสู้การก่อการร้ายโครงสร้างทางกฎหมายจะเปิดโอกาสให้บรรดาประเทศต่างๆสามารถแลกเปลี่ยนข้อมูลระหว่างกันและกัน ได้อย่างรวดเร็วในเรื่องที่เกี่ยวกับอินเทอร์เน็ต

บทที่ 4

วิเคราะห์เปรียบเทียบปัญหาของพนักงานสอบสวนในการรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ระหว่างประเทศไทยกับประเทศสหรัฐอเมริกา

4.1 เปรียบเทียบอำนาจหน้าที่ในการค้นและการเข้าถึงข้อมูลอิเล็กทรอนิ กส์ของพนักงานสอบสวน

เทคโนโลยีคอมพิวเตอร์เป็นเรื่องใหม่ที่เจ้าพนักงานบังคับใช้กฎหมายยังขาดความรู้ความเข้าใจ บุคลากรที่มีความรู้ความชำนาญยังมีอยู่จำกัด ทำให้การ ปราบอาชญากรรมคอมพิวเตอร์ยังขาดประสิทธิภาพ ซึ่งเป็นธรรมดาเมื่อผู้ปฏิบัติไม่มีความรู้เกี่ยวกับเทคโนโลยีคอมพิวเตอร์แต่มีความจำเป็นที่จะต้องปฏิบัติงานในสิ่งที่ตนเองไม่รู้จัก และยังไม่มีขั้นตอนที่ชัดเจนให้ปฏิบัติตาม ผู้ปฏิบัติก็ขาดความกล้าที่จะเข้าไปทำการสื บสวน สอบสวน และหากว่าผู้นั้นเข้าไปดำเนินการสืบสวน สอบสวนด้วยความจำเป็นเพราะสถานการณ์บังคับ เขาผู้นั้นอาจกลายเป็นผู้ก่อให้เกิดความเสียหายต่อรูปคดีหรือเป็นผู้ที่ทำลายพยานหลักฐานสำคัญทางคดีเสียเอง เนื่องจากความรู้เท่าไม่ถึงการณ์ได้

ซึ่งในประเทศไทยยังไม่มีหน่วยงานใดโดยเฉพาะ เจ้าหน้าที่ผู้ปฏิบัติขาดความรู้ความเข้าใจในด้านวิธีการตรวจค้นพยานหลักฐานที่เกี่ยวข้องกับคอมพิวเตอร์ แต่สำหรับประเทศสหรัฐอเมริกาซึ่งเผชิญกับปัญหาอาชญากรรมคอมพิวเตอร์มากที่สุด ได้มีการจัดตั้งหน่วยงานที่มีทั้งภาครัฐและเอกชน เช่น National Computer Crimes Squad ซึ่งสังกัดอยู่ใน F.B.I. ทำหน้าที่สืบสวนสอบสวนและจัดตั้ง Computer Analysis and Response Team ชื่อย่อ CART ทำหน้าที่ตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ ส่วนในภาคเอกชนก็จะอยู่ในรูปแบบของสมาคมหรือชมรม หรืออยู่ในสถานศึกษาในระดับมหาวิทยาลัย หรือจัดตั้งหน่วยงานขึ้นมาศึกษาและติดตามอาชญากรรมคอมพิวเตอร์โดยเฉพาะ

สำหรับประเทศไทยการใช้ อำนาจหน้าที่ในการค้นและการเข้าถึงข้อมูลอิเล็กทรอนิกส์ของพนักงานสอบสวนพอจะสรุปได้ ดังนี้

4.1.1. กรณีการค้นโดยมีหมายค้น

ปัญหาการออกหมายค้นโดยศาล

หมายค้นของศาล ถือ เป็นหลักประกันการคุ้มครองสิทธิและเสรีภาพของประชาชนที่ดีที่สุดในยุคหนึ่ง เพราะกระบวนการออกหมายค้นเป็นการตรวจสอบการใช้ดุลพินิจของเจ้าพนักงานมิให้กระทำการเกินเลยไปกว่าความจำเป็น ดังได้กล่าวไปแล้วว่าบทบัญญัติแห่งรัฐธรรมนูญมาตรา 238 [37] มีผลให้ต้องยกเลิกประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 58[38] และมาตรา 92 วรรคท้าย[39] ซึ่งหมายถึงยกเลิกการให้อำนาจเจ้าพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ในการออกหมายค้น โดยกำหนดให้ศาลแต่ฝ่ายเดียวที่มีอำนาจออกหมายค้น ผลของรัฐธรรมนูญข้อนี้ทำให้เจ้าพนักงานเกิดปัญหาในทางปฏิบัติในเรื่อ งการขอหมายค้นจากศาล คือ

ประการแรก เนื่องจากการค้นในที่รโหฐานต้องขอหมายค้นจากศาลเท่านั้น ในขณะที่สำนักงานเกี่ยวกับกระบวนการยุติธรรมต่าง ๆ ของไทย มีเขตที่ตั้งอยู่อย่าง กระจัดกระจายมิได้อยู่ภายในขอบเขตเดียวกันเช่นต่างประเทศ การขอหมายศาลจึงต้องใช้เวลาในการเดินท าง และช่วงระยะเวลาในการเดินทางไปขอหมายจากศาลนี้ อาจมีการแก้ไขเปลี่ยนแปลงหรือทำลายพยานหลักฐานไปทั้งหมดแล้วก็เป็นได้ นอกจากนี้อาจกล่าวได้ว่า หมายค้นของศาลในคดีอาชญากรรมไซเบอร์จะมีได้เพียงครั้งเดียวเท่านั้น เพราะเมื่อคนร้ายหรือผู้สบคบกันกระทำความผิดรู้ตัวว่าจะถูกค้นก็จะทำลายพยานหลักฐานทั้งหมดได้ในพริบตาเดียว

ประการที่สอง ความรู้ความเข้าใจของศาลในคดีเกี่ยวกับอาชญากรรมไซเบอร์มีผลต่อการออกหมายค้นของศาลเป็นอย่างยิ่ง หากศาลไม่เข้าใจลักษณะคดีว่ามีความละเอียดอ่อนและจำเป็นต้องใช้ความรวดเร็วดังกล่าว อาจทำให้ศาลไม่เห็นความสำคัญในการต้องออกหมายค้น

ดังนั้น ควรกำหนดให้ผู้มีอำนาจค้นในคดีอาชญากรรมคอมพิวเตอร์ คือคณะทำงานสืบสวนคดีอาชญากรรมคอมพิวเตอร์โดยเฉพาะ เพื่อความปลอดภัยในการค้นข้อมูลทางอิเล็กทรอนิกส์ โดยคณะทำงานฯ ชุดหนึ่งต้องประกอบด้วยทีมสอบสวนของเจ้าพนักงานตำรวจและทีมผู้เชี่ยวชาญด้านคอมพิวเตอร์ โดยแต่ละทีมต้องมีลูกทีมคือ [40]

---

[37] รัฐธรรมนูญ มาตรา 238 บัญญัติว่า “ในคดีอาญา การค้นในที่รโหฐานจะกระทำมิได้ เว้นแต่มีคำสั่งหรือหมายของศาล หรือมีเหตุให้ค้นโดยไม่ต้องมีคำสั่งหรือหมายศาล ทั้งนี้ตามที่กฎหมายบัญญัติ

[38] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 58 “เจ้าพนักงานและศาลมีอำนาจออกหมายอาญาได้ภายในเขตอำนาจดังต่อไปนี้

[39] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92 วรรคท้าย “เมื่อพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ค้นด้วยตัวเอง ไม่ต้องมีหมายค้นก็ได้ แต่ต้องเป็นในกรณีที่อาจออกหมายค้น หรือค้นได้ตามประมวลกฎหมายนี้

[40] อณิญพิไล เงินวิจิตร , “ปัญหาในการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์ .” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2544 หน้า 101

ทีมสอบสวนของเจ้าพนักงานตำรวจอย่างน้อยที่สุดต้องประกอบด้วย

- หัวหน้าพนักงานสอบสวน ทำหน้าที่หัวหน้าคณะทำงานฯ
- เจ้าหน้าที่ประสานงานระหว่างตำรวจ อัยการ และศาล เพื่อทำหน้าที่ประสานงานเรื่องต่าง ๆ เช่นการขอหมายค้น การรับคำสั่งปฏิบัติการจากหัวหน้าพนักงานสอบสวน รวมทั้งการประสานงานกับบุคคลภายนอกผู้เกี่ยวข้องกับการค้นหลักฐานเช่น ISP

ทีมผู้เชี่ยวชาญอย่างน้อยที่สุดต้องประกอบด้วย

- ชุดผู้เชี่ยวชาญด้านการค้นหา ประกอบด้วย ผู้เชี่ยวชาญด้านคอมพิวเตอร์ด้านตรวจสอบข้อมูลทางอิเล็กทรอนิกส์ หรือนักวิเคราะห์ระบบ อย่างใดอย่างหนึ่งหรือทั้งสอง อย่างน้อย 1 คน และผู้เชี่ยวชาญทางการรักษาความปลอดภัย อีกอย่างน้อย 1 คน เพื่อทำการค้นหาและป้องกันความเสียหายของข้อมูลในขณะค้นหาและจัดเก็บ
- ชุดผู้เชี่ยวชาญการรับรองความถูกต้องแท้จริงของพยานหลักฐานทางอิเล็กทรอนิกส์ในห้องปฏิบัติ

ปัญหาเกี่ยวกับการระบุรายละเอียดในหมายค้น[41]

หมายค้น ถือเป็นหลักประกันการปฏิบัติหน้าที่ของเจ้าพนักงานมิให้ กระทำการล่วงอำนาจตามอำเภอใจหรือลุแก่อำนาจ การที่ศาลจะออกหมายค้นในกรณีใดจะต้องปรากฏเหตุที่จะออกหมายค้นได้ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 69 คือ เพื่อหาพยานหลักฐาน เพื่อหาขอกลาง เพื่อช่วยบุคคล เพื่อจับบุคคล และเพื่อพบและยึดสิ่งของตามคำพิพากษา เหตุจะออกหมายค้นส่วนหนึ่งปรากฏแก่ศาลจากคำร้องขอของเจ้าพนักงาน โดยเจ้าพนักงานผู้จะทำการค้นมีเหตุอันควรเชื่อ (Probable Cause) ว่าสิ่งของที่จะใช้เป็นหลักฐานจะอยู่ในสถานที่ที่จะเข้าไปค้น

ปัญหาคือ Probable Cause หรือเหตุอันควรเชื่อเช่นนั้น ต้องปรากฏให้เห็นในหมายค้นด้วย ตามแบบของหมายค้นที่กำหนดในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 60 (3) และ (4) (ค) คือการให้ระบุสถานที่ที่จะค้น และลักษณะสิ่งของที่ต้องการค้น กำหนดวันเวลาที่จะทำการค้น และชื่อกับตำแหน่งของเจ้าพนักงานผู้จะทำการค้นนั้น

---

[41] อณิญพิไล เงินวิจิตร , “ปัญหาในการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์ .” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2544 หน้า 69

ในกรณีของการขอหมายค้นจึงมีปัญหา 2 ประการ

1. การระบุสิ่งของที่จะค้น

2. การระบุสถานที่ที่จะค้นในคำร้องขอหมายค้นจากศาล

ข้อมูลคอมพิวเตอร์บ างกรณีไม่อาจระบุได้ว่าอยู่ในรูปแบบใด ประกอบด้วยสิ่งใดบ้าง เพราะข้อมูลดังกล่าวมีลักษณะเป็นเพียงคลื่นกระแสไฟฟ้า และรหัสโปรแกรมที่ไม่สามารถจับต้องได้ทางกายภาพ และไม่สามารถระบุได้ว่าเก็บไว้ที่ใด ในระบบอินเทอร์เน็ตข้อมูลดังกล่าวอาจอยู่ต่างประเทศ หรือมีการบันทึก ข้อมูลต้นทางที่ต่างประเทศ แต่สถานที่ Down Load ข้อมูลอาจอยู่ที่ประเทศไทยก็เป็นได้

ปัญหาเกี่ยวกับเงื่อนเวลาที่ทำการค้น

ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 96 บัญญัติไว้ว่า “การค้นในที่รโหฐานต้องกระทำระหว่างพระอาทิตย์ขึ้นและตก ” หรืออีกนัยหนึ่งคือการค้นกระ ทำได้เฉพาะเวลากลางวันเท่านั้น ซึ่งมีข้อยกเว้นเพียง 2 ประการ คือ

1. เมื่อลงมือค้นแต่ในเวลากลางวัน ถ้ายังไม่เสร็จจะค้นต่อในเวลากลางคืนก็ได้

2. ในกรณีฉุกเฉินอย่างยิ่ง หรือซึ่งมีกฎหมายอื่นบัญญัติให้ค้นได้เป็นพิเศษจะทำการค้นในเวลากลางคืนก็ได้

แต่อาชญากรรมไซเบอร์มีการกระทำความผิดได้ตลอด 24 ชั่วโมง และผลของการกระทำความผิดสร้างความเสียหายให้แก่บุคคลที่ตกเป็ นเหยื่อได้โดยไม่เลือกเวลา และดั งที่กล่าวแล้วว่าการปราบปรามอาชญากรรมไซเบอร์นี้ต้องใช้ความรวดเร็วให้ทันกับการกระทำความผิด เพื่อป้องกันความเสียหายที่ จะเกิดขึ้นอย่างรวดเร็วเช่นกัน ดังนั้นการต้องรอให้พระอาทิตย์ขึ้นมีอำนาจทำการค้นได้ จึงเป็นปัญหาอีกประการหนึ่งที่ทำให้การปราบปรามการกระทำความผิดอาชญากรรมไซเบอร์ไม่มีประสิทธิภาพ

กรณีการค้นโดยไม่มีหมายค้น

ปัญหาเรื่องการกระทำความผิดซึ่งหน้าและขอบเขตในการค้น

ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92 วางหลักว่า ห้ามมิให้ค้นในที่รโหฐานโดยไม่มีหมายค้น เว้นแต่พนักงานฝ่ายปกครองหรือตำรวจเป็นผู้ค้น โดย ได้กำหนดข้อยกเว้นไว้ในอนุมาตรา (1) – (5) ที่ให้พนักงานฝ่ายปกครองหรือตำรวจสามารถเข้าทำการค้นในที่รโหฐานได้โดยไม่ต้องมีหมายค้น ในส่วนที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์ ใช้อนุมาตรา (2), (4) และ (5) คือ

(2) เมื่อปรากฏความผิดซึ่งหน้ากำลังกระทำลงในที่รโหฐาน

การที่เจ้าพนักงานพบอาชญากรรมไซเบอร์โดยบังเอิญขณะใช้บริการอินเทอร์เน็ตอยู่นั้น ถือเป็นความผิดซึ่งหน้าที่จะก ระทำการค้นในทันทีได้หรือไม่ เช่น เข้าไปในห้องสนทนา (Chat Room) แล้วพบข้อความเชิญชวนในลักษณะเสนอขายบริการทางเพศอย่างโจ่งแจ้ง ดังนี้

โดยหลักธรรมดาแล้วไม่ถือว่าเป็นความผิดซึ่งหน้า เพราะเจ้าพนักงานมิได้พบในขณะลงมือกระทำความผิด แต่พบเมื่อความผิดได้เกิดขึ้นแล้ว ก รณีเช่นนี้ถ้าต้องดำเนินการตามปกติคือเดินทางไปขอหมายค้นต่อศาลก่อน ซึ่งมีทางเป็นไปได้ เมื่อเจ้าพนักงานกลับมายัง Chat Room ดังกล่าวแล้วพบว่าข้อความดังกล่าวถูกลบทิ้งไปเสียแล้ว

(4) เมื่อมีความสงสัยตามสมควรว่าสิ่งของที่ได้มาโดยการกระทำความผิดได้ซ่อนหรืออยู่ในนั้นประกอบทั้งต้อง มีเหตุอันควรเชื่อว่าเนื่องจากการกระทำนั้นช้ากว่าจะเอาหมายค้นมาได้สิ่งของนั้นจะถูกโยกย้ายเสียก่อน

ข้อยกเว้นการเข้าค้นตามอนุมาตรานี้จะต้องปรากฏความจริงทั้งสองประการ คือ

1. มีความสงสัยว่าสิ่งของได้ซ่อนหรืออยู่ในนั้น และ

2. มีเหตุ อันควรเชื่อว่าการที่จะดำเนินการในการออกหมายค้นจะเกิดความชักช้าอันอาจทำให้มีการโยกย้ายสิ่งของจากที่รโหฐานนั้นเสียก่อนได้

ซึ่งข้อยกเว้นตามมาตรา 92 (4) นี้จำกัดเฉพาะกรณี “สิ่งของที่ได้มาโดยการกระทำผิด ” เท่านั้น อันหมายถึงทรัพย์ที่ได้มาจากการกระทำผิด เช่น ทรัพย์ที่ถูกลักหรือปล้นมา ถ้าเป็นอาชญากรรมคอมพิวเตอร์อาจเป็นข้อมูลความลับทางการค้ า หรือข้อมูลส่วนตัวของบุคคลอื่นที่ลักลอบคัดลอกมาเก็บไว้ใช้ประโยชน์โดยมิชอบ ส่วนสิ่งของที่มีไว้เป็นความผิด และสิ่งของที่ได้ใช้ในการกระทำผิด เช่น เครื่องคอมพิวเตอร์ที่ใช้ในการนัดหม ายเพื่อประกอบอาชญากรรม หรือใช้คอมพิวเตอร์ในการเข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ แม้จะเป็นสิ่งของที่จำเป็นต้องยึดเพื่อประกอบไว้ในสำนวน แต่ไม่ทำให้เจ้าพนักงานสามารถเข้าค้นได้โดยไม่มีหมายค้น อย่างไรก็ตามอาจเป็นเหตุให้ออกหมายค้นได้ตามมาตรา 69 (2)

ส่วนประเทศสหรัฐอเมริกา ในการกำหนดขอบเขตของการแสวงหาพยานหลักฐานของเจ้าหน้าที่ตำรวจ ได้กำหนดบทบัญญัติเกี่ยวข้องโดยตรงกับการปฏิบัติหน้าที่ของเจ้าพนักงานในการค้นและยึดพยานหลักฐานคือ บทแก้ไขที่ 4 (The Fourth Amendment) ซึ่งว่าด้วยสิทธิส่วนบุคคลของเอกชนที่บัญญัติว่า “สิทธิของบุคคลที่จะมีความปลอดภัยมั่นคงในร่างกาย เคหสถาน เอกสารและวัตถุสิ่งของต่อการค้น และยึด การจับที่ไม่มีเหตุอันควร ซึ่งได้มาโดยการสาบาน หรือการปฏิญาณตน และหมายนั้นจะต้องระบุเฉพาะเจาะจงถึงสถานที่ที่จะถูกค้น ตัวบุคคลที่จะถูกจับ และสิ่งของที่จะถูกยึด [42]

---

[42] “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”

The Fourth Amendment นี้เกิดมาจากความตั้งใจของคณะผู้ร่างบทบัญญัติว่าด้วยสิทธิต่างๆ ที่จะป้องกันมิให้รัฐบาลใช้อำนาจผิดๆ ในการค้นและจับเอกชนค้นบ้านและทรัพย์สินของเขา[43] โดยตั้งเป็นแนวความคิดเกี่ยวกับสิทธิส่วนบุคคล อันได้แก่สิทธิที่จะปลอดภัยจากการรุกล้ำเสรีภาพความมั่งคงและทรัพย์สินโดยไม่มีเหตุผลและไม่จำเป็น [44] ซึ่งถือเป็นสิ่งที่สำคัญมากสำหรับประชาชนชาวสหรัฐอเมริกา

The Fourth Amendment คุ้มครองทรัพย์สินของบุคคลให้พ้นจากการค้นและยึดที่ ไม่มีเหตุผล และไม่มีความหมาย แต่ไม่ได้ห้ามการค้นและการยึดเสียทั้งหมด และไม่ได้บังคับให้มีหมายในทุกกรณี แต่ถ้าจะมีการค้นหรือยึดทรัพย์สินโดยไม่มีหมาย The Fourth Amendment บังคับว่าการกระทำเหล่านี้จะต้องมีเหตุผลและมีหลักฐานเพียงพอ [45]

อย่างไรก็ตามการพัฒนากฎหม ายที่ใช้สำหรับการค้นและยึดคอมพิวเตอร์ของประเทศสหรัฐอเมริกาคงไม่สิ้นสุดลงอยู่เพียงเท่านี้ เพราะโครงร่างกฎหมายของอเมริกาส่วนใหญ่มีหลักแตกต่างกันระหว่างเทคโนโลยีการสื่อสารใช้เสียง เช่น โทรศัพท์ กับการสื่อสารที่ไม่ใช้เสียง เช่น Fax หรือ E-mail จึงมีหลักการในก ารควบคุมและคุ้มครองสิทธิส่วนบุคคล (Privacy Rights) แตกต่างกัน แต่ปัจจุบันปรากฏว่าข้อมูลและเสียงอาจปรากฏอยู่ร่วมกันในการสื่อสารหนึ่งในระบบเครือข่ายอินเตอร์เน็ต ซึ่งกฎหมายเดิมไม่ได้ครอบคลุมถึง ดังนั้นกฎหมายของอเมริกาจึงต้องมีการปรับเปลี่ยนต่อไปเช่นที่ได้มีกา รแก้ไขเปลี่ยนแปลงใน The USA Patriot Act of 2001 เพื่อให้อำนาจพนักงาน มีอำนาจในการดักฟังการสื่อสารในเทคโนโลยีรูปแบบใหม่นั้นเอง

การค้นตามแนวของประเทศสหรัฐอเมริกา [46]

1. พนักงานสอบสวน ผู้ค้นหาพยานหลักฐานจะต้องมีเจ้าหน้าที่ที่ได้รับการอบรมทางเทคนิค เช่นโปรแกรมเมอร์ หรือผู้เชี่ยวชาญอย่างน้อย 1 คน เพราะทีมค้นเป็นพนักงานสอบสวนอาจไม่มีความเชี่ยวชาญทางวิทยาการคอมพิวเตอร์ จึงจำเป็นที่ต้องใช้บุคลากรที่แปลความหมายของภาษาคอมพิวเตอร์ได้ ช่วยไล่ตรวจสอบข้อมูล ในเครื่องคอมพิวเตอร์นั้นว่ามีมากน้อยเพียงใดเพื่อการค้นจะได้พบข้อมูลที่จะใช้เป็นพยานหลักฐานได้ครบถ้วน

---

[43] กระมล ทองธรรมชาติ , สมบูรณ์ สุขสำราญ , เรื่องน่ารู้เกี่ยวกับการปกครองและรัฐธรรมนูญของสหรัฐอเมริกา, 2546 หน้า 94

[44] เพิ่งอ้าง, หน้า 94

[45] กระมล ทองธรรมชาติ , สมบูรณ์ สุขสำราญ , เรื่องน่ารู้เกี่ยวกับการปกครองและรัฐธรร มนูญของสหรัฐอเมริกา, 2546 หน้า 98

[46] ฉัทปณัย รัตนพันธ์, “อาชญากรรมคอมพิวเตอร์: ศึกษาการกำหนดฐานความผิด และการดำเนินอาชญากรรมทางคอมพิวเตอร์.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2547 น. 24

2. พนักงานสอบสวนต้องมีเครื่องมือในการป้องกันความเสียหาย เพราะขณะส่งไปยังห้องวิจัยอาจทำให้เกิดความสูญเสียของข้อมูล ทำให้ระบบการทำงานของคอมพิวเตอร์คลาดเคลื่อน

3. ก่อนค้นหาหัวหน้าทีม พนักงานสอบสวน ควรวางแผนที่ละเอียดรอบครอบเพื่อค้นและเก็บหลักฐานอิเล็กทรอนิกส์ แต่ไม่ควรลืมการรวบรวมพยานหลักฐานแบบดั้ง เดิม เช่น ลายพิมพ์นิ้วมือของผู้ต้องสงสัยบนคีย์บอร์ด

4. ผู้เชี่ยวชาญคอมพิวเตอร์บางคน ไม่ควรสอบหลักฐานที่คนอื่นพยายามค้นหาหรือจัดการข้อมูลแล้ว เพราะอาจทำให้เกิดการแก้ไขเปลี่ยนแปลงข้อมูล

5. คณะผู้ค้นหาต้องเตรียมแผนผังการเดินสายไฟ และทำเอกสารประกอบแสดงระบบเครื่องมือถูกจัดวางตำแหน่งใด ติดป้ายแสดงชื่ออย่างละเอียดและเชื่อมต่อสายเคเบิ้ลโดยระมัดระวังไม่ให้ใครก็ตามเข้าไปเปลี่ยนแปลงยุ่งเกี่ยวกับข้อมูลระหว่างค้นหาพยานหลักฐาน

6. คณะผู้ค้นหาหลีกเลี่ยงไม่ให้วัตถุที่ยึดไว้เข้าใกล้สนามแม่เหล็ก เช่น เครื่องส่งวิทยุ เครื่องส่งโทรศัพท์ เครื่องถ่ายเอกสาร เครื่องจักรกลต่าง ๆ เพราะจะเกิดสนามแม่เหล็กทำให้ฮาร์ดแวร์เสียหาย

7. คณะผู้ค้นหาไม่ควรตั้งฮาร์ดแวร์และซอฟต์แวร์ในสิ่งแวดล้อมที่ร้อนจัด และมีความชื้น เพราะอิทธิพลของอุณหภูมิจะทำให้หลักฐานอิเล็กทรอนิกส์เสียหาย[47]

นอกจากนี้ในการออก หมายค้นข้อมูลโดยศาลนั้น ก็มีการวางหลักให้บรรยายถึงลักษณะข้อมูลที่ถูกค้น โดยในการบรรยายนี้ให้ผู้เชี่ยวชาญคอมพิวเตอร์ช่วยศาลในการแสดงรายละเอียดในหมาย[48]

จาก ปัญหาดังกล่าวข้างต้น ผู้วิจัยได้ ทำการวิเคราะห์ปัญหาระหว่างประเทศไทยและประเทศสหรัฐอเมริกาได้ ดังนี้

สำหรับประเทศไทย เมื่อกลับมาทบทวน กฎหมายวิธีพิจารณาความอาญาที่ใช้ปัจจุบันพบว่าประเทศไทยยังมีปัญหาในเรื่องความล่าช้าในการเข้าค้นหาพยานหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากความประสงค์ของรัฐที่มุ่งจะให้ความคุ้มครองสิทธิส่วนบุคคล จึงสร้างหลักประกันสิทธิของประชาชนด้ วยการกำหนดมาตรการตรวจสอบการใช้ดุล ยพินิจของเจ้าพนักงานโดยองค์กรศาล และในส่วนของอำนาจในการออกหมายค้นกำหนดให้ศาลแต่ผู้เดียวเท่านั้นที่มีอำนาจ แม้แต่การค้นข้อมูลอิเล็กทรอนิกส์ที่ใช้อุปกรณ์เชื่อมต่อคอมพิวเตอร์เข้าไป

---

[47] www.usdou.gov

[48] วัลลิกา อุ่นศรี , “ปัญหาการรวบรวมและพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีอาญา , “(วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2544), น. 115

ค้นหาหลักฐานข้อมูลในเครื่องคอมพิวเตอร์ผู้ต้องสงสัยโดยไม่มีการรุกล้ำเข้าไปในที่รโหฐานก็ใช้หมายค้นเช่นเดียวกัน เพราะถือว่ามีการล่วงล้ำเข้าไปในพื้นที่อันสงวนไว้เป็นสิทธิส่วนตัว “กระบวนการออกหมายค้นโดยศาล ” จึงเป็นขั้นตอนหนึ่งที่ก่อให้เกิดปัญหาความล่าช้า เนื่องจากเจ้าพนักงานขาดความคล่องตัวในการปฏิบัติหน้าที่ นอกจากนี้ปัญหาในเงื่อนเวลาในการค้นก็เกิดความล่าช้าอีก เพราะก ฎหมายวิธีพิจารณาความอาญากำหนดให้เจ้าพนักงานทำการค้นได้เฉพาะเวลากลางวัน แต่บริการบนอินเตอร์เน็ตเปิดให้บริการตลอด 24 ชั่วโมง ดังนั้นการกระทำความผิดจึงอาจเกิดได้ตลอด 24 ชั่วโมง เช่นกัน ในขณะที่เจ้าหน้าที่ต้องรอจนกว่าพระอาทิตย์ขึ้นจึงจะทำการค้นได้ และข้อกฎหมาย ที่กำหนดให้ผู้มีอำนาจค้นต้องเป็นเจ้าพนักงานฝ่ายปกครองหรือตำรวจเท่านั้น โดยไม่เปิดช่องให้ผู้อื่นสามารถเข้ามาช่วยเจ้าพนักงานทำการตรวจค้นได้เลย นอก จากทำให้ค้นหาพยานหลักฐานทางอิเล็กทรอนิกส์ล่าช้า เพราะปัญหาจากเจ้าหน้าที่ยังขาดความรู้ความชำนาญในเรื่องคอมพิวเตอร์ แล้ว พนักงานผู้ค้นเองที่อาจกลายเป็นผู้ทำลายพยานหลักฐานโดยรู้เท่าไม่ถึงการณ์ด้วย

สำหรับประเทศสหรัฐอเมริกาพนักงานสืบสวนสอบสวนจะมีความรู้ความชำนาญในด้านเทคโนโลยีคอมพิวเตอร์ โดยเจ้าหน้าที่ต้องได้รับการอบรมทางเทคนิค เช่นโปรแกรมเมอร์ เพื่อการค้นพบข้อมูลที่จะใช้ เป็นพยานหลักฐานได้ครบถ้วน สหรัฐอเมริกาก็ยังคงมีปัญหาลักษณะใกล้เคียงกับประเทศไทย คือ การค้นหาพยานหลักฐานจากเครื่องคอมพิวเตอร์ที่อยู่ในบ้าน หรือการเข้าไปในเครือข่ายอินเตอร์เน็ตเพื่อค้นหาพยานหลักฐานจากแฟ้มข้อมูลส่วนบุคคล โดยไม่มีการบุกรุกเข้าไปในเคหสถานเลยก็ ต้องใช้หมายค้นด้วย เพราะกรณีนี้ศาลสูงสุดได้ให้ความคุ้มครองสิทธิส่วนบุคคล ทำให้เกิดความล่าช้าในการค้นหาพยานหลักฐาน ซึ่งทำให้บางครั้งข้อมูลที่เป็นพยานหลักฐานทางอิเล็กทรอนิกส์อาจจะถูกลบทำลายได้อย่างรวดเร็ว เพราะเทคโนโลยีที่ก้าวหน้า แต่ประเทศอเมริกาได้มีกฎหมาย The Fourth Amendment ไม่ได้บังคับว่าการค้นต้องมีหมายค้นทุกกรณีจะแตกต่างกับประเทศไทย เพราะประเทศสหรัฐอเมริกาได้รับทราบถึงสถานการณ์บางอย่างที่จะต้องทำให้มีเหตุผลเพียงพอที่จะทำการค้นโดยไม่มีหมายได้ เช่นการได้รับความยินยอมจากผู้ครอบครองทรัพย์ การค้นบันทึกสาธ ารณะและในสภาพการณ์ที่มีเหตุผลความจำเป็นอื่นๆ เช่น การค้นทรัพย์ที่เคลื่อนที่ได้ ซึ่งสภาพดังกล่าวประเทศสหรัฐอเมริกาได้พบปัญหาอาชญ ากรรมประเภทนี้เป็นจำนวนมากขึ้นตามเทคโนโลยีที่เจริญก้าวหน้า เหตุจะทำการค้นโดยไม่มีหมายค้นจึงเพิ่มขึ้นทุกที ตามกระแสการวิวัฒนาการทางเทคโนโลยี ซึ่งสถานการณ์ดังกล่าวนี้ทำให้รัฐบาลสามารถลุกล้ำสิทธิส่วนบุคคลของประชาชนมากขึ้นทุกที โดยที่ไม่รู้สึกว่าเป็นการคุกคามสิทธิส่วนบุคคลดังกล่าว

4.2. เปรียบเทียบอำนาจหน้าที่ในการยึดและรักษาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ของ พนักงานสอบสวน

พยานหลักฐานที่ดีจะต้องสามารถทำให้ศาลเชื่อจนสิ้นข้อสงสัยว่าจำเลยได้กระทำผิดจริงและ “พยานหลักฐานที่ศาลจะรับฟังได้ต้องเป็นพยานหลักฐานที่ได้มาโดยชอบด้วยกฎหมายและสามารถพิสูจน์ความผิดหรือความบริสุทธิ์ของจำเลยได้” [49]

เมื่อพบข้อมูลที่จะใช้เป็นพยานหลักฐานแล้ว กฎหมา ยกำหนดวิธีการในการยึดและรักษาพยานหลักฐานไว้ว่า ต้องคงสภาพให้ตรงตามความเป็นจริงมากที่สุด ไม่ให้มีการแก้ไขเปลี่ยนแปลงใดๆ เพราะหากในทางปฏิบัติของเจ้าหน้าที่ขัดกับหลักการที่กฎหมายบัญญัติไว้ ก็จะทำให้การได้มาซึ่งพยานหลักฐานเป็นการมิชอบด้วยกฎหมาย และศาลสามารถไม่รับฟ้องได้

ดังนั้น สิ่งที่ต้องพิจารณาคือ ทำอย่างไรจะทำให้พยานหลักฐานอยู่ในสภาพที่เป็นจริงที่สุด เพื่อให้พยานมีน้ำหนัก น่าเชื่อถือ เนื่องจากข้อมูลสามารถลบ แก้ไขได้ง่ายโดยใช้เวลาเพียงสั้นๆและมักไม่เหลือร่องรอย จะทราบได้อย่างไรว่าข้อมูลดังกล่าวไม่ได้ถูกแก้ไข แต่งเติมมาก่อนเพื่อสร้างความเชื่อถือให้ศาลมั่นใจว่าสิ่งที่นำเสนอต่อศาลมีความถูกต้องเป็นสิ่งเดียวกับที่ยึดมาได้จากที่เกิดเหตุ กฎหมายได้ให้อำนาจพนักงานสอบสวนยึดไว้ซึ่งสิ่งของที่ค้นพบหรือบุคคลส่งมาให้ ไว้ได้ เพื่อประโยชน์แก่การรวบรวมพยานหลักฐาน ได้แก่ สิ่งของที่ค้นพบว่ามีไว้เป็นความผิดหรือได้มาโดยการกระทำผิดหรือได้ใช้หรือสงสัยว่าได้ใช้ในการกระทำความผิด แต่การยึดพยานหลักฐานที่เป็นข้อมูลในคอมพิวเตอร์ ซึ่งเป็นสิ่งที่ไม่มีรูปร่างจะทำด้วยวิธีการใด

ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 101 บัญญัติว่า สิ่งของที่ยึดได้ในการค้นให้ห่อหรือบรรจุหีบห่อตีตราไว้ หรือทำเครื่องหมายไว้เพื่อป้องกันการสับเปลี่ยนพยานหลักฐาน แต่ข้อมูลคอมพิวเตอร์ไม่มีรูปร่าง ไม่สามารถบรรจุหีบห่อได้ ดังนั้น อาจใช้วิธียึดเครื่องคอมพิวเตอร์ที่มีข้อมูลนั้นอยู่ไว้แทน หรืออาจนำฮาร์ดดิสก์ที่มีข้อมูลนั้นเ สนอต่อศาลก็ได้ อย่างไรก็ตาม การจะรู้ว่าฮาร์ดดิสก์นั้นมีข้อมูลอันเกี่ยวกับการกระทำผิดหรือไม่ ลำพังพนักงานสอบสวนเองอาจไม่สามารถเข้าใจ อาจทำให้ได้ข้อมูลไม่ครบถ้วน ถ้าไม่อาศัยผู้เชี่ยวชาญ นอกจากนี้ หากเป็นการพบข้อมูลที่ยึดในระบบเครือข่ายคอมพิวเตอร์ของผู้อื่น และมีอยู่มากมายหลายแห่ง ก็เกิดปัญหาในการปฏิบัติงานว่าจะสามารถยึดทั้งระบบได้หรือไม่

---

[49] ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 บัญญัติไว้ว่า “พยานวัตถุ พยานเอกสารหรือพยานบุคคล ซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานที่มิได้เกิดขึ้นจากการจูงใจมี คำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน”

ประมวลกฎหมายวิธีพิจารณาความอาญา บัญญัติให้พนักงานสอบสวนมีอำนาจยึดไว้ซึ่งสิ่งของที่พ บ หลักกฎหมายดังกล่าวมีประเด็นที่ต้องวิเคราะห์ว่า เมื่อพนักงานสอบสวนพบเครื่องคอมพิวเตอร์ส่วนบุคคลตามหมายค้น สิ่งที่พนักงานสอบสวนต้องการคือข้อมูลภายในเครื่องคอมพิวเตอร์นั้น ซึ่งเมื่อพนักงานสอบสวนสามารถเข้าถึงข้อมูลที่ต้องสงสัยได้แล้ว จะต้องปฏิบัติการด้วยความ ระมัดระวังโดยคำนึงถึงกรรมวิธีที่ถูกต้อง เพื่อกักหรือล๊อคข้อมูลนั้นไว้ให้อยู่และยึดพยานหลักฐานที่เกี่ยวข้องอย่างอื่นให้อยู่ในสภาพที่เป็นจริงที่สุด เพื่อให้สิ่งทั้งหลายที่ยึดมานั้นมีน้ำหนักน่าเชื่อถือ ประมวลกฎหมายวิธีพิจารณาความอาญาได้กำหนดวิธีการเก็บรักษาสิ่งของที่จะใช้เป็นพยานหลักฐานในคดีอาญา คือ

ปัญหาเรื่องความน่าเชื่อถือของพยานหลักฐาน

กรณีอาชญากรรมไซเบอร์ สภาพที่แท้จริงของสิ่งที่ใช้เป็นพยานหลักฐานคือคลื่นแม่เหล็กไฟฟ้าที่เคลื่อนไหวอยู่ภายในเครื่องคอมพิวเตอร์ ซึ่งไม่สามารถมองเห็นได้แต่มีความละเอียดอ่อนและไม่เสถียรภาพดังกล่าว นอกจากนี้การรวบรวมพยานหลักฐานทางคอมพิวเตอร์จำเป็นต้องมีการเปลี่ยนแปลงรูปลักษณะของข้อมูล เช่น การถ่ายโอนข้อมูลมาเก็บไว้ในแผ่นดิสก์ การพิมพ์ออกมาบนกระดาษโดยใช้เครื่องพิมพ์ ปัญหาในขั้นตอนการยึด ทำอย่างไรจึงจะสร้างความเชื่อถือได้ว่า [50]

1. สิ่งที่เจ้าพนักงานนำเสนอนั้นถูกต้องแท้จริงและเป็นสิ่งเดียวกันกับที่ยึดมาได้ในสถานที่เกิดเหตุ

2. สิ่งที่เจ้าพนักงานนำเสนอนั้นมีความครบถ้วนบริบูรณ์เช่นเดียวกับวันที่ทำการยึด

ฉะนั้นปัญหาในการยึดข้อมูล ซึ่งบรรจุอยู่ในเครื่องคอมพิวเตอร์การยึดพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ปัญหาสำคัญในการยึดรวบรวมพยานหลักฐาน ก็คือข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ ซึ่งเป็นข้อมูลที่ถูกจัดเก็บไว้ในสื่อบัน ทึกโดยอาศัยการจัดระเบียบของกระแสแม่เหล็กไฟฟ้า ซึ่งเจ้าหน้าที่ของรัฐมีอำนาจในการตรวจยึดได้มากน้อยแค่ไหน ความสำคัญของข้อมูลในเครื่องคอมพิวเตอร์จะเป็นสิ่งยืนยันได้ว่ามีการใช้คอมพิวเตอร์จึงเป็นพยานหลักฐานในการบ่งชี้ว่าผู้ต้องหาหรือจำเลยได้กระทำความผิดจริงหรือไม่ แต่ข้อมูลที่จัดเก็บในเครื่องคอมพิวเตอร์นั้นจะเป็นสิ่งที่ไม่มีรูปร่าง ทำให้เกิดปัญหาที่เจ้าหน้าที่ของรัฐอาศัยอำนาจทางกฎหมายอย่างไรในการยึดข้อมูลเหล่านั้น

---

[50] อณิญพิไล เงินวิจิตร, “ปัญหาในการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2544 หน้า 73

สำหรับประเทศสหรัฐอเมริกา การบังคับใช้กฎหมาย การยึดพยานหลักฐานทางอิเล็กทรอนิกส์นั้น อาจกล่าวได้ว่ามีแนวโน้มที่จะผ่อนคลายจากหลัก The Exclusionary Rule ซึ่งเป็นหลักฐานเกณฑ์ที่ศาลสูงไว้วางไว้เพื่อให้ The Fourth Amendment มีประสิทธิภาพในการเป็นหลักประกันสิทธิส่วนบุคคลของประชาชนชาวสหรัฐอเมริกาให้พ้นจากการล่วงละเมิดจากการปฏิบัติหน้าที่ของเจ้าพนักงานโดยไม่มีเหตุผลและไม่จำเป็น โดยการที่ศาลจะไม่ยอมรับพยานหลักฐานที่ได้มาจากการยึดอันมิชอบด้วยกฎหมายรวมทั้งพยานหลักฐานโดยอ้อมอันสืบเนื่องมาจากพยานหลักฐานที่มิชอบนั้น

The Fourth Amendment เป็นบทบัญญัติที่ว่าด้วยสิทธิส่วนบุคคลของเอกชน อันได้แก่ สิทธิที่จะปลอดภัยจากการรุกล้ำเสรีภาพ ความมั่นคงและทรัพย์สินโดยไม่มีเหตุผลและไม่จำเป็นซึ่งถือเป็นเรื่องที่สำคัญมากสำหรับประชาชนชาวสหรัฐอเมริกา “กระบวนการการออกหมาย” จึงถือเป็นหลักประกันการคุ้มครองสิทธิส่วนบุคคลที่ดีได้ส่วนหนึ่ง เพราะจะต้องผ่านการตรวจสอบจากผู้พิพากษามาจิสเตรด ในเรื่อง “มีเหตุอันควรเชื่อ” (Probable Cause) ภายใต้คำสาบานของเจ้าพนักงานผู้ที่จะทำการยึด

ในประเทศสหรัฐอเมริกา การยึดมีวัตถุประสงค์เพื่อที่จะรวบรวมพยานหลักฐาน ซึ่งบทบัญญัติใน Title 18 แห่ง Federal Rules of Criminal Procedure Rule 41 [51] ได้บัญญัติเกี่ยวกับเหตุในการยึดสิ่งของไว้ 4 กรณี ดังนี้

1. ทรัพย์สินซึ่งเป็นพยานหลักฐานในการกระทำความผิด
2. สิ่งของผิด กฎหมาย สิ่งของที่ได้มาจากการกระทำความผิด หรือสิ่งของอื่นใดที่ครอบครองไว้เป็นความผิด
3. ทรัพย์สินที่ทำขึ้นเพื่อใช้ หรือเจตนาที่จะใช้ หรือ ได้ใช้เป็นเครื่องมือในการกระทำความผิด
4. บุคคลซึ่งจะต้องถูกจับกุมตามหมายจับหรือบุคคลซึ่งถูกควบคุมโดยมิชอบด้วยกฎหมาย

จากบทบัญญัติในรัฐธรรมนูญดังกล่าวเห็นได้ว่า คำว่า “Probable Cause” เป็นเงื่อนไขในการยึด หากปราศจาก Probable Cause แล้ว ย่อมมีผลให้การออกหมายไม่ถูกต้อง และเมื่อไม่มีการออกหมายแล้ว การยึดที่จะกระทำไปโดยปราศจากหมายย่อมเป็นการดำเนินการที่ไม่ถูกต้องเช่นกัน สำหรับความหมายของคำว่า Probable Cause มีความหมายว่าอย่างไรนั้น Black’s Law Dictionary ได้ให้นิยามคำว่า Probable Cause ไว้เป็นสองนัยด้วยกัน

---

[51] อณิญพิไล เงินวิจิตร , “ปัญหาในการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์ .” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2544 หน้า 73

นัยแรกหมายความว่า เหตุอันควรสงสัยว่ามีบุคคลได้กระทำหรือกำลังกระทำความผิดอาญา หรือสถานที่นั้นมีสิ่งของที่สัมพันธ์กับความผิดอาญา (A reasonable ground to suspect that a person has committed or is committing a crime or that a place contains specific items commented with a crime)

นัยที่สอง พิจารณาตามเจตนารมณ์ของรัฐธรรมนูญแก้ไขเพิ่มเติมครั้งที่ 4 หมายความว่า ข้อสรุปที่มากกว่า าความส งสัยลอย ๆ แต่น้อยกว่าพยานหลักฐานที่ใช้พิสูจน์การกระทำความผิด (Which amounts to more than a bare suspicion but less than evidence that would justify a conviction) [52]

อย่างไรก็ตาม จากคำอธิบายดังกล่าวก็ยังไม่ได้ข้อสรุปถึงความหมายของคำว่า probable cause เป็นที่ยุติแต่อย่างใด ดังนั้น การหาความหมายของถ้อยคำดังกล่าวจึงอาจพิจารณาได้จากคำตัดสินของศาลฎีกาสหรัฐอเมริกาในคดี Carroll v. United States (267 U.S. 132 (1925)) ซึ่งศาลได้วินิจฉัยไว้ว่า Probable Cause เกิดขึ้นเมื่อข้อเท็จจริงและพฤติการณ์แวดล้อมต่าง ๆ ของตัวเจ้าหน้าที่ตำรวจที่ทราบเองและโดยที่เจ้าหน้าที่ตำรวจมีข้อมูลข่าวสารที่เพียงพอออกหมายยึดสิ่งของที่เชื่อว่าอยู่ในสถานที่นั้นหรืออยู่ที่บุคคลนั้นโดยความเชื่อที่ชอบด้วยเหตุผล ต่อมาในคดี Brinegar v. United States (338 U.S. 160 (1949)) ได้วินิจฉัยไว้ว่า Probable Cause ปรากฏเมื่อข้อเท็จจริงและพฤติการ ณ์แวดล้อมจากการสืบทราบของเจ้าหน้าที่ตำรวจและเจ้าหน้าที่ตำรวจมีข้อมูลข่าวสารที่หน้าเชื่อถือโดยมีเหตุผลเพียงพอที่จะออกหมายยึด โดยที่วิญญูชนเชื่อว่ามีความผิดอาญาเกิดขึ้นหรือกำลังกระทำตามความหมายที่ศาลฎีกาของสหรัฐอเมริกา ได้วินิจฉัยไว้ในคดีดังกล่าวเป็นที่เห็นได้ว่า Probable Cause มีความหมายทางภาวะวิสัย (objective) และไม่ได้เกิดขึ้นเองแต่ขึ้นอยู่กับการพิจารณาของเจ้าหน้าที่ผู้ทำการยึดสิ่งของหรือผู้พิพากษาผู้มีอำนาจ [53]

---

[52] Black's Law Dictionary, 7 e.d.(St.Paul, Minn: West Group, 1999), p.1219.

[53] Charles H.Whitebread and Christopher Slobogin, supra note 5, p.141.

ในส่วนของการให้ความหมายของคำว่า Probable Cause ซึ่งเป็นถ้อยคำในบทบัญญัติรัฐธรรมนูญแก้ไขเพิ่มเติมครั้งที่ 4 อันเป็นเงื่อนไขในการยึดสิ่งของ เมื่อนำมาเทียบเคียงกับหลักการที่กำหนดไว้ในประมวลวิธีพิจารณาความอาญาแล้วน่าจะมีความหมายเทียบเคียงได้กับบทบัญญัติตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 59/1 ที่ว่า “ก่อนออกหมายจะต้องปรากฏพยานหลักฐานตามสมควรที่ทำให้ศาลเชื่อได้ว่ามีเหตุที่จะออกหมาย เพราะในการพิจารณาการยึดสิ่งของ ย่อมมาจากข้อเท็จจริงและพฤติการณ์แวดล้อมต่าง ๆ ที่น่าเชื่อถือและมีเหตุผลเพียงพอที่จะยึดได้หรือไม่ ซึ่งเมื่อพิจารณาตามบทบัญญัติในมาตรา 59/1 แล้วหมายความได้ว่าบทบัญญัติดังกล่าวกำหนดให้มีการเสนอพยานหลักฐานที่เพียงพอที่ทำให้ที่ทำให้น่าเชื่อว่ามีวัตถุสิ่งของที่ต้องการยึด ดังนั้นหากจะแปลความหายของคำว่า Probable Cause ตามนัยของประเทศไทยแล้ว เห็นว่าถ้อยคำว่า “เหตุอันควรเชื่อ” น่าจะใกล้เคียงกับความหมายดังกล่าวได้

จาก ปัญหาดังกล่าวข้างต้น ผู้วิจัยได้ทำการวิเคราะห์ปัญหาระหว่างประเทศไทยและประเทศสหรัฐอเมริกาได้ ดังนี้

สำหรับปัญหาเรื่องการยึดพยานหลักฐานทางอิเล็กทรอนิกส์ของประเทศไทย จะประสบปัญหากับเรื่องความน่าเชื่อถือของพยานหลักฐาน เพราะธรรมชาติของข้อมูลอิเล็กทรอนิกส์มีความไม่คงทนถาวร ทั้งสภาพที่แท้จริงของพยานหลักฐานเป็นคนละเรื่องกับสภาพที่ปรากฏแก่สายตา ความไม่ไว้วางใจจึงเกิดในทุกขั้นตอนที่มีการโอนข้อมูล และการเก็บรักษา ดังนั้นปัญหาสำหรับขั้นตอนการยึดคือทำอย่างไรจึงจะสร้างความเชื่อถือได้ว่า สิ่งที่เจ้าพนักงานนำเสนอนั้นถูกต้องแท้จริง และเป็นสิ่งเดียวกันกับที่ยึดมาในสถานที่เกิด และสิ่งนั้นยังคงสภาพครบถ้วนสมบูรณ์อยู่ จนถึงวันที่นำเสนอต่อศาล ปัญหาอีกเรื่องที่เห็นว่าสำคัญ คือพนักงานสอบสวนยังขาดอำนาจในการยึดพยานหลักฐานอิเล็กทรอนิกส์ในที่เกิดเหตุได้ทันที ในกรณีที่พบการกระทำความผิดซึ่งหน้า หรือกรณีที่ข้อมูลอิเล็กทรอนิกส์นั้นได้มาโดยผิดกฎหมาย เช่น กำลังตั้งใจที่จะใช้คอมพิวเตอร์ในทางที่ผิด โดยมีเครื่องมืออุปกรณ์ที่ใช้ในการกระทำความผิดอยู่ในการครอบครองด้วยเช่น ดิส์เก็ตต์ที่ใช้เก็บข้อมูล ในขณะที่ทำการยึด กรณีต่าง ๆ นี้พนักงานสืบสวนสอบสวนอาจจะมีอำนาจยึดข้อมูลไว้ก่อน โดยไม่ต้องรอหมายค้นข้อมูลได้ โดยอ้างเหตุฉุกเฉิน ส่วนประเทศสหรัฐอเมริกาได้มีกฎหมาย The Fourth Amendment เป็นบทบัญญัติที่ว่าด้วยสิทธิส่วนบุคคลของเอกชน อันได้แก่สิทธิที่จะปลอดภัยจากการรุกล้ำเสรีภาพของประชาชน เจ้าหน้าที่ตำรวจต้องมีหลักฐานที่น่า เชื่อถือ โดยมีเหตุผลเพียงพอที่จะออกหมายยึดได้จะคล้าย ๆ กับประเทศไทย เพราะเมื่อก ว่าที่จะเข้าไปทำการยึดหลักฐาน ผู้ที่กระทำความผิดอาจจะสามารถรู้ล่วงหน้าก่อน ทำให้ผู้กระทำความผิดทำลายข้อมูลไปแล้วก็ได้

4.3 ปัญหาในเรื่องอำนาจและความสามารถของพนักงานสอบสวนในการรวบรวมพยานหลักฐานที่ เป็นข้อมูลอิเล็กทรอนิกส์

โลกปัจจุบันเป็นโลกของเทคโนโลยีข่าวสาร ถ้าใช้เทคโนโลยีให้เกิดประโยชน์ก็จะเกิดการพัฒนาสังคมในทุก ๆ ด้าน แต่อย่างไรก็ตามในขณะที่เทคโนโลยีคอมพิวเตอร์และสารสนเทศได้ถูกพัฒนาให้มีความรุดหน้าไปอย่างรวดเร็วด้วยต้นทุนที่น้อยลง ทำให้บุคคลทั่วไปสามารถมีเครื่องคอมพิวเตอร์ที่มีสมรรถนะสูงมาใช้ในราคาที่ไม่แพ ง จึงทำให้บุคคลหรือองค์กรต่าง ๆ ซึ่งรวมถึง บรรดาอาชญากรทั้งหลายต่างมุ่งหน้าเข้าสู่ปริมณฑลแห่งเครือข่ายข้อมูลคอมพิวเตอร์โดยพร้อมเพียงกัน ผลลบจากการพัฒนาอย่างรวดเร็วของคอมพิวเตอร์ทำให้อาชญากรรมที่ กระทำบ นอินเตอร์เน็ตมีองค์ประกอบความผิดทางอาญาที่ไม่ชัดเจน เป็นอาชญากรรมรูปแบบใหม่ที่ไม่สามารถปรับให้เข้ากับกฎหมายอาญาได้ในปัจจุบัน ทั้งการกระทำความผิดดังกล่าวมีความยุ่งยากซับซ้อนยากแก่การสืบสวนดำเนินคดี นอกจากนี้ยังมีแนวโน้มที่จะเพิ่มจำนวนสูงขึ้นอย่างรวดเร็วและทวีความรุนแรงขึ้นเรื่อย ๆ

ในคดีอาชญากรรมทางคอมพิวเตอร์ต้อ งใช้ความระมัดระวังอย่างมากในเรื่องความน่าเชื่อถือของพยานหลักฐานทางอิเล็กทรอนิกส์ ดังนั้นจะต้องกำหนดหลักเกณฑ์ให้แน่นอนว่าพยานหลักฐานนั้นมีความน่าเชื่อถือมากพอที่ศาลจะรับฟัง เพื่อมิให้เกิดปัญหาความไม่แน่นอนของดุลพินิจของศาล ปัญหาจึงอยู่ที่ความน่าเชื่อถือของพ ยานหลักฐาน เพราะข้อมูลอิเล็กทรอนิกส์มีธรรมชาติที่ถูกจำกัด ทำลาย แก้ไขได้ง่าย จึงมีเหตุที่ศาลจะเคลือบแคลงสงสัยทำอย่างไรให้มีการบันทึก เก็บข้อมูล ทันต่อเหตุการณ์ และครบถ้วน นำไปพิสูจน์ต่อศาลได้ว่าไม่มีการแก้ไข ตัดต่อ ให้ศาลเชื่อถือพอที่จะฟังลงโทษจำเลยได้ จึงจำเป็นที่ต้องใช้ผู้ชำนาญการพิเศษเฉพาะด้านคอมพิวเตอร์ ช่วยในด้านแปลข้อความหรือความหมายของข้อมูลที่อยู่ในระบบคอมพิวเตอร์ สำหรับกฎหมายของประเทศไทย ผู้ชำนาญการพิเศษมีความสำคัญอย่างไรนั้นตามแนวทางความเชื่อถือของศาลที่มีความมั่นใจในการให้ความเห็นของผู้เชี่ยวชา ญ ถ้าให้ความเห็นถูกต้องแน่นอน พยานหลักฐานย่อมมีน้ำหนักมาก เหตุผลประกอบการลงความเห็นของผู้เชี่ยวชาญนี้ต้องอธิบายเหตุผลประกอบการตรวจพิสูจน์หรือให้ความเห็น เช่น ผู้เชี่ยวชาญในสาขาคอมพิวเตอร์มาให้ความเห็นเกี่ยวกับระบบข้อมูลคอมพิวเตอร์ หรือพฤติกรรมการกระทำความผิดของอาชญากรคอมพิวเตอร์ทำอย่างไรกับข้อมูลคอมพิวเตอร์ด้วยวิธีใด อย่างใด เป็นต้น

ดังนั้นความสามารถของผู้สอบสวนจึงมีความสำคัญมากในคดีอาชญากรรมทางคอมพิวเตอร์ เพราะในการพิสูจน์ข้อมูลอิเล็กทรอนิกส์ที่อยู่ในลักษณะเลขฐานสองในฮาร์ดดิสก์นั้น พนักงานสอบสวน พนักงานอัย การและศาล เมื่อตรวจดูฮาร์ดดิสก์แล้วก็มีข้อจำกัดที่ว่าแปลข้อความหรือความหมายของข้อมูลที่เป็นสัญลักษณ์ของระบบคอมพิวเตอร์ไม่ได้ เพราะฉะนั้นผู้สอบสวนจะต้องมีความรู้ความสามารถเฉพาะด้าน ซึ่งจะทำให้มีบทบาทมากใน

การช่วยแปลข้อความหรือความหมาย แต่ประเทศไทยยังขาดบุคค ลากรที่มีความชำนาญมีความรู้ความสามารถและประสบการณ์ด้านการวิเคราะห์พิสูจน์ข้อมูลคอมพิวเตอร์อย่างแท้จริง จึงทำให้ความเชื่ อถือของศาลที่มีต่อพยานหลักฐานน้อยลงไปด้วย ดังนั้นจะกล่าวถึงปัญหาในเรื่องอำนาจและความสามารถของพนักงานสอบสวนในการรวบรวมพยานหลักฐานที่เป็นข้ อมูลอิเล็กทรอนิกส์

4.4 ปัญหาในเรื่องอำนาจในการปฏิบัติงานของพนักงานสอบสวนในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์

1. ปัญหาการสืบหาตัวผู้กระทำผิด

การสืบหาตัวผู้กระทำความผิดในระบบอินเตอร์เน็ตซึ่งเป็นระบบ Cyberspace นั้น เป็นระบบที่เป็นการเชื่อมโยงเครือข่ายคอมพิวเตอร์หลาย ๆ เครือข่ายทั่วโลกซึ่งเชื่อมโยงถึงกันและกันแบบไร้พรมแดน การติดต่อสื่อสารจึงไม่จำเป็นต้องเห็นหน้ากัน และด้วยเหตุนี้เองจึงไม่สามารถที่จะระบุได้อย่างชัดเจนได้ว่าผู้กระทำความผิดนั้นเป็นใครและอยู่ที่ไหน เพราะผู้กระทำความผิดสามารถกระทำความผิดได้อย่างรวดเร็ วโดยอาศัยเครือข่ายอินเตอร์เน็ตและสามารถกระทำได้ในทุกสถานที่ไม่ว่าจะที่ใดก็ตาม ทำให้ยากต่อการสืบหาตัวผู้กระทำความผิด และหากผู้กระทำความผิดดำเนินการกระทำในที่พักอาศัย ก็ยากที่จะสืบหาข้อมูลได้ และก็มักจะไม่ทิ้งหลักฐานใด ๆ ไว้ให้ค้นหาหรือสืบหาตัวได้ ดังนั้น ก ารสืบสวนสอบสวนของเจ้าหน้าที่ตำรวจจึงจำเป็นต้องอาศัยการติดตามอย่างละเอียดและต่อเนื่อง การพิสูจน์ทราบตัวบุคคลผู้ส่งและรับข้อมูลที่แน่นอนเป็นเรื่องยาก ซึ่งโอกาสจับกุมมีน้อยเพราะกระทำผิดในลักษณะนี้จะกระทำให้สถานที่ปกปิดมิดชิด เจ้าหน้าที่ตำรวจจึงจำเป็นต้องมีหมา ยค้นเข้าไปตรวจสอบกระทำความผิด โดยกระบวนการในการขอหมายค้นจากศาลก็ต้องอาศัยระยะเวลานานพอสมควร และเป็นเวลาที่มากพอที่ผู้กระทำความผิดจะลบข้อมูลที่พยานหลักฐานได้

ดังนั้น ในการแก้ไขปัญหาส่วนหนึ่งก็ต้องอาศัยผู้ที่มีความรู้ทางด้านคอมพิวเตอร์และอินเตอร์เน็ต เพราะ ในการใช้อินเตอร์เน็ตส่วนใหญ่จะมีการทิ้งร่องรอยการกระทำความผิดไว้ แต่ก็มีในบางกรณีที่ผู้กระทำความผิดมีความเชี่ยวชาญและชำนาญจะไม่มีการทิ้งร่องรอยใด ๆ ไว้เลย

2. ปัญหาการขาดแคลนบุคลากรและงบประมาน

เทคโนโลยีคอมพิวเตอร์และอินเตอร์เน็ตเป็นเรื่องใหม่ที่เจ้า พนักงานผู้ บังคับใช้กฎหมายยังขาดความรู้และความเข้าใจ ประกอบกับบุคคลากรที่มีความรู้ความสามารถในด้านเทคโนโลยีคอมพิวเตอร์และอินเตอร์เน็ตยังมีอยู่จำกัด ทำให้การป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ยังขาดประสิทธิภาพ ซึ่งในส่วนของผู้ปฏิบัติงานที่เกี่ยวข้องกับ

อำนวยความ ยุติธรรมในทุกระดับ นับตั้งแต่เจ้าหน้าที่ตำรวจ พนักงานอัยการไปจนถึงผู้พิพากษา นอกจากจะต้องมีความรู้ความเข้าใจพื้นฐานในหลักการ วิธีการ และองค์ประกอบแห่งความผิดประเภทต่าง ๆ แล้ว ผู้ปฏิบัติงานที่เกี่ยวข้องกับคดีในทุกระดับยังจะต้องมีความรู้ความเข้าใจถึงหลักการพื้ นฐานของการเชื่อมโยงของระบบเครือข่ายและวิธีการทำงานของอินเตอร์เน็ต และหลักการที่คอมพิวเตอร์ใช้ในการรับส่งข้อมูล แต่ปรากฏว่าในปัจจุบันผู้ปฏิบัติหน้าที่ที่เกี่ยวข้องกับ คดีประเภทนี้ มีความรู้ความสามารถด้านเทคโนโลยีคอมพิวเตอร์ยังมีอยู่น้อย ประกอบกับอาชญากรหรือผู้กระทำความผิดมักใช้เครื่องคอมพิวเตอร์ที่มีเทคโนโลยีและมีความเร็วสูงในการรับส่งข้อมูล มีการเปลี่ยนแปลงการใช้อุปกรณ์คอมพิวเตอร์อยู่เสมอ เพื่อให้มีความสามารถป้องกันการสืบหาของเจ้าพนักงาน ทำให้เจ้าพนักงานของรัฐต้องมีการปรับปรุงเปลี่ยนแปลงอุปกรณ์คอมพิวเตอร์ เ พื่อให้สามารถสืบหาการกระทำความผิดได้ ซึ่งราคาของอุปกรณ์คอมพิวเตอร์ส่วนมากมีราคาแพง แต่งบประมาณที่ใช้ในการจัดซื้ออุปกรณ์คอมพิวเตอร์นั้นมีไม่เพียงพอ ทำให้ขาดแคลนงบประมาณในการจัดซื้ออุปกรณ์คอมพิวเตอร์ที่ทันสมัย ทำให้เป็นอุปสรรคต่อการปฏิบัติงานของเจ้าพนักงาน แ ละทำให้การป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ขาดประสิทธิภาพ

3. ปัญหาการขาดหน่วยงานพิเศษในการสอบสวน ดำเนินคดีและรวบรวมพยานหลักฐาน

ปัญหาการขาดหน่วยงานพิเศษที่มีอำนาจหน้าที่และความชำนาญเฉพาะด้านในการสืบสวน สอบสวน และดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ รวมทั้งมี หน้าที่ในการรวบรวมพยานหลักฐานเกี่ยวกับอาชญากรรมทางคอมพิ วเตอร์ เนื่องจากการกระทำความผิด ทางอินเตอร์เน็ตมีลักษณะที่แตกต่างไปจากอาชญากรรมหรือความผิดทั่วไป จึงต้องอาศัยบุคคลากรที่มีความเชี่ยวชาญเฉพาะด้าน ดังนั้ น สำนักงานตำรวจแห่งชาติควรจะมี การตั้งหน่วยงานตำรวจอินเตอร์เน็ต (Cybercop) หรือหน่วยงานพิเศษที่มีอำนาจหน้าที่ในการสืบสวนสอบสวนในคดีอาชญากรรมทางคอมพิวเตอร์มิใช่เรื่องง่ายที่เจ้าหน้าที่คนใดคนหนึ่งจะกระทำได้เหมือนคดีอาชญากรรมธรรมดาทั่ว ๆ ไป จึงจำเป็นที่จะต้องจัดตั้งหน่วยงานที่มีอำนาจหน้าที่โดยเฉพาะ มีองค์ประกอ บของสมาชิกหรือคณะทำงานที่เป็นผู้มีความรู้ความเชี่ยวชาญทั้งในด้านคอมพิวเตอร์และการสืบสวนสอบสวนคดีอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีคอมพิวเตอร์ ซึ่งในประเทศไทยยังไม่มีหน่วยงานดังกล่าวเป็นการเฉพาะ นอกจากนี้เจ้าหน้าที่ผู้ปฏิบัติงานยังขาดความรู้ความเข้าใจในด้าน วิธีการตรวจค้นและยึดพยานหลักฐานที่เกี่ยวข้องกับคอมพิวเตอร์ด้วย

4.5 ปัญหาและข้อจำกัดของการสอบสวนของเจ้าพนักงานตำรวจ

การป้องกัน ปราบปรามและแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์ซึ่งอยู่ในความรับผิดชอบของเจ้าหน้าที่ตำรวจไม่มีประสิทธิภาพและประสิทธิผลเท่าใดนัก ทั้งนี้สืบเนื่องมาจากปัญหาอุปสรรคหลายประการ กล่าวคือ

1. การกำหนดตำแหน่งพนักงานสอบสวนให้เป็นผู้ที่จบการศึกษาจากโรงเรียนนายร้อยตำรวจและผู้มีวุฒิการศึกษาสาขานิติศาสตร์หรือรัฐศาสตร์เท่านั้น ดังนี้ทำให้ขาดผู้ที่มีความรู้ ทักษะความชำนาญเฉพาะด้านที่เกี่ยวข้องกับการดำ เนินการเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์
2. การขาดพนักงานสอบสวนที่มีความรู้ความชำนาญในการสอบสวนอย่างแท้จริง เนื่องจากเจ้าหน้าที่ตำรวจที่ทำหน้าที่ด้านการสอบสวน ได้แก่ พนักงานสอบสวน ซึ่งมียศระหว่างร้อยตำรวจตรีถึงพันตำรวจโทเท่านั้น เมื่อพนักงานสอบสวนเหล่านี้ได้รับการเลื่อนตำแหน่งสูงขึ้นเป็นระดับ รองผู้กำกับการขึ้นไปแล้ว ก็จะต้องทำหน้าที่ด้านการบริการ มิได้ทำหน้าที่ด้านการสอบสวนแต่อย่างใด การที่พนักงานสอบสวนสามารถโยกย้ายสลับไปมาระหว่างหน่วยงานในสำนักงานตำรวจแห่งชาติได้ทำให้ขาดการเชื่อมต่อในการทำงานด้านการสอบสวนคดี อาชญากรรมคอมพิวเตอร์ และขาดพนักงานสอบสวนที่มีความรู้ความชำนาญและทักษะเกี่ยวกับการสอบสวนคดีอาชญากรรมคอมพิวเตอร์
3. ภารกิจในการป้องกันและปราบปรามอาชญากรรมของเจ้าหน้าที่ตำรวจเป็นภารกิจที่กว้างขวางและหลากหลายลำพังเพียงการควบคุมปัญหาอาชญากรรมพื้นฐาน ซึ่งได้แก่อาชญ ากรรมที่เกี่ยวกับการประทุษร้ายต่อทรัพย์ ชีวิต และร่างกาย และคดีเล็กน้อยอื่น ๆ ก็มิอาจปฏิบัติได้อย่างสัมฤทธิ์ผลเท่าที่ควร ทำให้ต้องทุ่มเททรัพยากรไปกับการดำเนินการดังกล่าวส่วนการดำเนินการกับอาชญากรรมทางคอมพิวเตอร์มิอาจจะกระทำได้เต็มที่

ดังนั้น การจัดตั้งกรม สอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ขึ้น เพื่อปฏิบัติภารกิจในการป้องกันปราบปรามและควบคุม อาชญากรรมทางคอมพิวเตอร์อย่างมีทิศทางที่ชัดเจนย่อมส่งผลต่อการลดและป้องกันความเสียหายที่จะเกิดต่อระบบเศรษฐกิจ สังคมและความมั่งคงของประเทศ ทำให้สังคมได้รับการป้องกันให้ปลอดภั ยจากอาชญากรรมคอมพิวเตอร์ ทั้งนี้โดยการปฏิบัติงานทั้งในเชิงรุกและเชิงรับด้วยการสืบสวนทั้งก่อนและหลังการกระทำความผิด และการสอบสวนดำเนินคดีกับผู้กระทำผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์โดยที่พนักงานสอบสวนประกอบด้วยผู้ซึ่งมีความรู้ความชำนาญด้านคอมพิวเตอร์ ทำให้สา มารถมีความรู้เท่าทันผู้กระทำความผิด สถานภาพและแนวโน้มของอาชญากรรมคอมพิวเตอร์ การสร้างความ

เชี่ยวชาญเฉพาะด้านการสอบสวน ทั้งนี้โดยการที่พนักงานสอบสวนคดีพิเศษสามารถปฏิบัติหน้าที่การสอบสวนได้อย่างต่อเนื่อง มีความก้าวหน้าในสายงาน โดยไม่มีการโยกย้ายข้ามสา ยงานการมี คณะกรรมการที่ปรึกษาบริห ารงานบุคคลในส่วนของพนักงานสอบสวนคดีอาชญากรรมคอมพิวเตอร์ การมีหลักประกันความมั่นคงและความเป็นอิสระในวิชาชีพโดยไม่ให้มีการโยกย้ายพนักงานสอบสวนในคดีอาชญากรรมคอมพิวเตอร์ได้โดยมิชอบ การมีเงินเดือนและค่าตอบแทนอย่างเหมาะสม เพื่อให้สามารถดำ รงอยู่ในความยุติธรรมได้อย่างมีเกียรติ เพื่อจะได้มิต้องใช้อำนาจหน้าที่แสวงหาผลประโยชน์ในทางไม่สุจริต [54]

กรมสอบสวนคดีอาชญากรรมคอมพิวเตอร์ จึงเป็นหน่วยงานที่มีหน้าที่ในการป้องกันปราบปราม สืบสวนคดีอาชญากรรมคอมพิวเตอร์ที่มีความซับซ้อน มีการใช้เทคนิคสูงในการกระทำความผิด ผู้กระทำความผิดเป็นผู้ที่มีความรู้เชี่ยวชาญในการประกอบอาชญากรรม มีการพัฒนารูปและวิธีการในการกระทำความผิดต่อเนื่องตลอดเวลามีการใช้เทคนิคสูง ทำให้จะต้องมีพนักงานสอบสวนที่มีความรู้ความสามารถเฉพาะด้าน ดังนั้นประเทศไทยควรจะให้ความสำคัญในคดีอาชญากรรมท างคอมพิวเตอร์ให้มากขึ้น เพื่อที่จะได้ลดปัญหาที่จะเกิดขึ้นและขยายวงกว้างต่อไป

---

[54] www.dsi.go.th

บทที่ 5

บทสรุปและข้อเสนอแนะ

ปัจจุบันเทคโนโลยีสารสนเทศถูกนำมาใช้ในสังคมมากขึ้นเรื่อย ๆ ข้อมูลต่าง ๆ ถูกจัดทำขึ้นในรูปแบบของข้อมูลอิเล็กทรอนิกส์แทนการบันทึกข้อมูลลงในกระดาษตามปกติ เนื่องจากความสะดวกในการบันทึก การเก็บรักษาและการติดต่อสื่อสารในขณะเดียวกันข้อมูลอิเล็กทรอนิกส์เหล่านี้ก็ถูกเข้าถึงได้โดยง่ายด้วยอุปกรณ์อิเล็กทรอนิกส์ และคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์อาจเป็นข้อมูลประเภทใดก็ได้ ซึ่งก็มีความสำคัญไม่แตกต่างกับข้อมูลที่บันทึกอยู่ในเอกสาร แต่ปัญหาสำคัญคือข้อมูลอิเล็กทรอนิกส์ยังมีสถานะที่ไม่แน่นอนในทางกฎหมาย เนื่องจากกฎหมายเน้นให้ความสำคัญให้ความคุ้มครองแก่วัตถุที่มีรูปร่าง เมื่อข้อมูลอิเล็กทรอนิกส์เป็นสิ่งที่ไม่มีรูปร่างการกระทำความ ผิดต่อข้อมูลอิเล็กทรอนิกส์และการนำข้อมูลอิเล็กทรอนิกส์ไปใช้กระทำความผิดจึงอยู่นอกเหนือความรับผิดอาญาและทำให้การกระทำเหล่านั้นไม่เป็นความผิด ทั้งยังก่อให้เกิดความเสียหายต่อสังคม

สำหรับประเทศไทยนั้น อาชญากรรมคอมพิวเตอร์ยังอยู่ในระยะเริ่มแรก แต่ก็มีแนวโน้มว่าจะมีการขยายตัวอย่างรวดเร็ว จึงควรที่จะศึกษาและเตรียมตัวรับมือกับปัญหาให้ทันกับสถานการ ณ์โดยเฉพาะอย่างยิ่งการศึกษาถึงกฎ หมายที่มีในปัจจุบันว่าจะสามารถลงโทษผู้กระทำ ความผิดได้เพียงใดไม่ว่าจะเป็นกฎ หมายสารบัญญัติที่กำ หนดฐานความผิดหรือกฎหมายวิธีส บัญญัติที่กำหนดวิธี การรวบรวมพยานหลักฐานและการนำผู้ก ระทำความผิดมาลงโทษ จากการศึกษากฎ หมายสารบัญญัติของไทย พบว่าบทบัญญั ติที่กำหนดฐานความผิดตามประมวลกฎหมายอาญามีความเพียงบางฐานที่สามารถนำมาใช้ลงโทษผู้กระทำผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ได้ แต่ยังไม่ครอบคลุมในทุกความผิดที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ เช่นความผิดฐานเข้าถึงโดยไม่มีอำนาจและการลักลอบดักข้อมูลเป็นต้น ซึ่งควรจะมีการบัญญัติ กฎหมายเพิ่มเติมไม่ว่าจะเป็นในรูปแบบของการแก้ไขเพิ่มเติมประมวล กฎหมายอาญาหรือในรูปแบบของการบัญญัติกฎหมายพิเศษขึ้นมาใหม่

ภัยจากอาชญากรรมคอมพิวเต อร์ในประเทศไทยมีอยู่จริง มูลค่าความเสียหายมีมากน้อยเพียงใดยังไม่อาจประเมินได้ เนื่องจากยังไม่มีการเก็บข้อมูลรวบรวมเป็นสถิติอาจกล่าวได้สภาพปัญหาอาชญากรรมคอมพิวเตอร์ของประเทศไทยในอนาคตจะรุนแรงขึ้นตามกระแสของการปฏิวัติเทคโนโลยีเหมือนเช่นเดียวกับต่างประเทศ เช่น ประเทศสหรัฐอเมริกาได้ประสบมาแล้ว เมื่ออาชญากรรมที่เกิดขึ้นเป็นอาชญากรรมรูปแบบใหม่ ซึ่งเกี่ยวข้องกับเทคโนโลยีคอมพิวเตอร์ผลกระทบที่ตามมาก็คือผลกระทบในทางกฎหมายโดยเฉพาะอย่างยิ่งกฎหมายวิธีสบัญญัติเรื่องพยานหลักฐานที่ใช้บังคับใช้อยู่ในปัจจุบัน มีปัญหาตั้งแต่ชั้ นการรวบรวมพยานหลักฐานของพนักงงานสอบสวนจนถึงชั้นการพิจารณาคดีของศาลว่ายังมีเนื้อหาที่ไม่

ครอบคลุมถึงอาชญากรรมชนิดใหม่เหล่านี้ ได้ทำให้เกิดความขัดข้องในการรวบรวมพยานหลักฐานและการรับฟังพยานหลักฐาน

จากคำนิยามของคำว่าอาชญากรรมทางคอมพิวเตอร์พอจะสรุปได้ดังนี้คือก ารทำผิดกฎหมายโดยใช้เทคโนโลยีคอมพิวเตอร์เป็นส่วนสำคัญ เป็นการกระทำใด ๆ ที่เกี่ยวกับการใช้การเข้าถึงข้อมูล โดยที่ผู้กระทำไม่ได้รับอนุญาตหรือการลักลอบแก้ไขทำลาย คัดลอกข้อมูลหรือทำให้คอมพิวเตอร์ทำงานผิดพลาดแม้บางกรณีอาจไม่ถึงกับเป็นการกระทำที่ผิดกฎหมายแต่เป็นการกระทำที่ผิดระเบียบกฎเกณฑ์ จรรยาบรรณของการใช้คอมพิวเตอร์นั้น ๆ

การรวบรวมพยานหลักฐาน

การสืบสวนสอบสวนในคดีอาชญากรรมทางคอมพิวเตอร์ไม่ใช่เรื่องง่ายที่เจ้าหน้าที่คนใดคนหนึ่งจะกระทำได้เหมือนคดีอาชญากรรมธรรมดา แต่ต้องเป็นเจ้าหน้าที่มีความรู้ความเข้าใจในระบบต่าง ๆ ของคอมพิวเตอร์ เครื่องมือและอุปกรณ์ในการตรวจสถานที่เกิดเหตุย่อมมีความแตกต่างจากคดีอาชญากรรมธรรมดาทั่วไป จึงจำเป็นที่จะต้องจัดตั้งหน่วยงานที่มีอำนาจหน้าที่โดยเฉพาะมีองค์ประกอบของสมาชิกหรือคณะทำงานที่เป็นผู้มีความรู้เชี่ยวชาญทั้งใดด้านคอมพิวเตอร์และการ สืบสวนคดีอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีคอมพิวเตอร์ ซึ่งในประเทศไทยยังไม่มีหน่วยงานใดโดยเฉพาะเจ้าหน้าที่ผู้ปฏิบัติขาดความรู้ความเข้าใจในด้านวิธีการตรวจค้นและยึด พยานหลักฐานที่เกี่ยวข้องกับคอมพิวเตอร์ ประเทศสหรัฐอเมริกาซึ่งเผชิญกับปัญหาอาชญากรรมคอมพิวเตอ ร์มากที่สุดได้มีการจัดตั้งหน่วยงานที่มีทั้งภาครัฐและเอกชน เช่น National Computer Crimes Squad ซึ่งสังกัดอยู่ใน F.B.I. ทำหน้าที่สืบสวนสอบสวนและจัดตั้ง Computer Analysis and Response Team ชื่อย่อ CART ทำหน้าที่ตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์

ในการตรวจค้ นและยึดพยานหลักฐานทางคอมพิวเตอร์ที่สามารถ เคลื่อนย้ายได้ควรตรวจยึดฮาร์ดแวร์,โปรแกรม, สื่อบันทึกทุกชนิด, อุปกรณ์ต่อพ่วง, เอกสารจากเครื่องพิมพ์และเอกสารที่เกี่ยวข้องกับคดี ส่งไปห้องปฏิบัติการเพื่อตรวจพิสูจน์หาข้อมูลใช้เป็นพยานหลักฐานเชื่อมโยงกับการกระทำความผิ ด ส่วนพยานหลักฐานทางคอมพิวเตอร์ที่ไม่สามารถเคลื่อนย้ายได้ เช่นคอมพิวเตอร์ขนาดเมนเฟรม ในการตรวจค้นหาข้อมูลที่ใช้เป็นพยานหลักฐานอาจต้องให้ผู้เชี่ยวชาญ ซึ่งเป็นตัวแทนของบริษัทผู้ผลิตเข้าร่วมในการตรวจค้น เพื่อช่วยแก้ไขปัญหาอุปสรรค ในระหว่างการตรวจค้น จึงเห็นได้ ว่าการดำเนินการรวบรวมพยานหลักฐานทางคอมพิวเตอร์จะต้องมีวิธีปฏิบัติต่อพยานหลักฐานโดยเฉพาะเจ้าหน้าที่ธรรมดาทั่วไปจะไม่สามารถดำเนินการได้

ซึ่งการรับฟังหรือการอ้างพยานหลักฐานในคดีอาญา พยานหลักฐานต้องสามารถแสดงและอธิบายหรือชี้ให้เห็นข้อเท็จจริง ดังนั้นพยานหลักฐา นจึงเป็นสิ่งที่สำคัญที่สุด ซึ่งจะมีวิธีการ

อย่างไร ที่ทำให้ศาลเชื่อว่าพยานหลักฐานที่นำมาเสนอนั้นเป็นข้อมูลหรือหลักฐานที่มิได้เปลี่ยนแปลงแก้ไข และทำให้พยานประเภทนี้มี ความน่าเชื่อถือเพียงพอที่ศาลจะลง โทษจำเลยได้ ซึ่งพยานหลักฐานที่รับฟังได้ต้องเป็นพยานที่ได้มาโ ดยสุจริต ศาลจะไม่รับฟังก็ต่อเมื่อพยานหลักฐานนั้นได้มาโดยวิธีการที่มิชอบเช่น พยานหลักฐานที่ยึดมาโดยไม่มีหมายตรวจค้น การจูงใจ มีค่ำ มั่น สัญญา ขู่เข็ญ หลอก ลวง ดังนั้นหากพนักงานสอบสวนสืบหาหรือได้มาซึ่งพยานหลักฐานที่มิชอบ ด้วยกฎหมาย เช่นอาจได้พยานหลักฐานมาโดยการจู งใจ ขู่เข็ญหรือหลอกลวง ซึ่งผลที่ได้พยานหลักฐานมาโดยมิชอบ จะให้ศาลไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบนั้น ซึ่งอาจทำให้ใช้ยันหรือลงโทษจำเลยไม่ได้

มาตรการด้านกฎหมาย

มาตรการด้านกฎ หมาย ของประเทศไทย เป็นนโยบายของรัฐบาลที่นำมาใช้ในการต่อต้านอาชญากรรมทางคอ มพิวเต อร์ โดยการบัญญัติหรือตรากฎ หมายเพื่อกำหนดว่าการกระทำใดบ้างที่มีโทษทางอาญ า ซึ่งในปัจจุบันประเทศไทยได้มีกฎ หมายเกี่ยวข้องหลายฉบับ และจากการ ที่ได้ศึกษาเกี่ยวกับมาตรการทางกฎ หมายที่ให้อำนาจสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ พบว่าประเทศไทยขาดแคลนบุคลากรสายงานในด้านนี้ ควรให้มีการจัดอบรมให้เกิดความรู้แก่พนักงานอย่างจริงจังเพื่อที่จะให้เกิดเสถียรภาพของระบบสารสนเทศในหน่วยงานของภาครัฐและภาคเอกชน

สำหรับแนวทางการบังคับกฎหมายทางอิเล็กทรอนิกส์ของประเทศสหรัฐอเมริกานั้น อาจกล่าวได้ว่ามีแนวโน้มที่จะผ่อนคลายจากหลัก The Exclusionary Rule ซึ่งเป็นหลักเกณฑ์ที่ศาลสูงได้วางไว้เพื่อให้ The Fourth Amendment มีประสิทธิภาพในการเป็นหลักประกันสิทธิส่วนบุคคลของประชาชนชาวสหรัฐอเมริกาให้พ้นจากการล่วงละเมิดจากการปฏิบัติหน้าที่ของเจ้าพนักงานโดยไม่มีเหตุผลและไม่จำเป็น โดยการที่ศาลจะไม่ยอมรับพยาน หลักฐานที่ได้มาจากการค้นและการยึดอันมิชอบด้วยกฎหมายรวมทั้งพยานหลักฐานโดยอ้อมอันสืบเนื่องมาจากพยานหลักฐานที่มิชอบนั้น

The Fourth Amendment เป็นบทบัญญัติที่ว่าด้วยสิทธิส่วนบุคคลของเอกชน อันได้แก่ สิทธิที่จะปลอดภัยจากการรุกล้ำเสรีภาพความมั่นคงและทรัพย์สินโดย ไม่มีเหตุผลและไม่จำเป็น ซึ่งถือเป็นเรื่องที่สำคัญมาก สำหรับประชาชนชาวสหรัฐอเมริกา

ปัญหาเรื่องการค้น

“หมายค้น” แม้จะเป็นหลักประกันการคุ้มครองสิทธิและเสรีภาพของประชาชนที่ดีที่สุด เพราะเป็นกลไกการตรวจสอบดุลยพินิจของเจ้าพนักงานมิให้กระทำการเกิน เลยไปกว่าความ จำ

เป็น แต่กระบว นการออกหมายค้นที่นอกจากจะทำให้เสียเวลาเดินทางไปศาลแล้ว ปัญหาในเรื่องการระบุรายละเอียดในหมายค้นก็เป็นปัญหาใหญ่ที่ควรคำนึงถึง เพราะการที่จะร้องขอหมายค้นจะต้องทำให้ศาลเชื่อว่ามีสิ่งของที่จะใช้เป็นพยานหลักฐานอยู่ในสถานที่นั้น การแสดง “เหตุอันควร เชื่อ ” เช่นในคดีอาชญากรรมไซเบอร์ถือว่าเป็นเรื่องที่ทำได้ยาก เพร าะพยานหลักฐาน อิเล็กทรอนิกส์เป็นสิ่งที่มองไม่เห็นได้ด้วยตา จะแสดงให้ศาลเชื่อได้อย่างไรว่าพยานหลักฐานอิเล็กทรอนิกส์ที่จะต้องการนั้นอยู่ในสถานที่นั้น

เจตนารมณ์ของ “หมายค้น” อีกประการหนึ่งคือ เป็นตั วกำหนดขอบเขตในการค้นของเจ้าพนักงานเพราะ “หมายค้น” เป็นทั้งสิ่งที่ให้อำนาจเจ้าพนักงานล่วงละเมิดสิทธิส่วนบุคคลได้ด้วยการค้น แต่ขณะเดียวกันก็เป็นกรอบในกา รใช้อำนาจของเจ้าพนักงานมิให้เกิน เลยไปกว่าที่กำหนดไว้ในหมายสิ่งที่ ต้องกำหนดไว้ในหมายคือ ลักษณะ สิ่งของที่จะ ค้น และสถานที่ที่จะทำการค้น แต่อย่างที่กล่าวแล้วว่าพยานหลักฐานทางอิเล็กทรอนิกส์ เป็นเพียงคลื่นแม่เหล็กไฟฟ้า ไม่สามารถระบุได้ว่าอยู่ในรูปแบบใด และเก็บอยู่ที่ใด ซึ่งแม้จะรู้ว่าอยู่ที่ใด แต่การที่พยานหลักฐานดังกล่าวมีการเคลื่อนไหวโยกย้ายที่ได้รวดเร็วทำให้กระบ วนการค้นอาจกินวงกว้างเกินกว่าจะระบุในหมายได้ นอกเหนือจากปัญหาเรื่องหมายค้นแล้ว ยังมีข้อกฎหมายที่ทำให้การค้นมีความล่าช้าอีกคือ “เงื่อนไขเวลาในการค้น” เพราะกฎหมายวิธีพิจารณา ความอาญากำหนดให้เจ้าพนักงานทำการค้นได้เฉพาะในเวลากลางวัน แต่บริการบนอินเตอร์เน็ตเปิดให้บริการตลอด 24 ชั่วโมง เป็นไปได้ว่าผู้กระทำความผิดทางอาชญากรรมคอมพิวเตอร์อาจทำในเวลากลางคืน ทำให้เจ้าหน้าที่ต้องรอจนกว่าพระอาทิตย์ขึ้น จึงจะทำการค้นได้ แล ะข้อกฎหมายที่กำหนดให้ผู้มีอำนาจค้นต้องเป็น “เจ้าพนักงานฝ่ายปกครองหรือตำรวจ” เท่านั้น โดยไม่เปิดช่องให้ผู้อื่นสามารถเข้ามาช่วยเข้าพนักงานทำการค้นได้เลย

ปัญหาเรื่องการยึด

การยึดพยานหลักฐานทางอิเล็กทรอนิกส์จะประสบปัญหากับเรื่องความน่าเชื่อถือของพยานหลักฐาน เพราะธรรมชาติของข้อมูลอิเล็กทรอนิกส์มีความไม่คงทนถาวร ทั้งสภาพที่แท้จริงของพยานหลักฐานเป็นคนละเรื่องกั นกับสภาพที่ปรากฏแก่สายตา ความไม่ไว้วางใจจึงเกิดในทุกขั้นตอนที่มีการถ่ายโอนข้อมูล และการเก็บรักษา ดังนั้นปัญหาสำหรับขั้นตอนการยึดคือ ทำอย่างไรจึงจะสร้างความเชื่อถือได้ว่า สิ่งที่เจ้าพนักงานนำเสนอนั้นถูกต้ องแท้จริงและเป็นสิ่งเดียวกันกับที่ยึดมาในสถานที่เกิด เหตุ และสิ่งนั้นยังคงสภาพครบถ้วนสมบูรณ์อยู่จนถึงวันที่นำเสนอต่อศาล

ปัญหาในเรื่องอำนาจและความสามารถของพนักงานสอบสวน

จากการศึกษา กฎหมาย สารบัญญัติของไทย พบว่าบทบัญญัติที่กำหนดฐานความผิดตามประมวล กฎหมาย อาญา มีความผิดเพียงบางฐานที่สามารถนำมาใช้ลงโทษผู้กระทำผิด เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ได้ โดยเฉพาะอำนาจในการเข้าถึงผู้ที่กระทำความผิด ของพนักงานยังใช้ระยะเวลานาน เจ้าหน้าที่ต้องขออำนาจจากศาลก่อนจึงจะทำการตรวจค้นได้ อาจทำให้หลักฐานถูกทำลายไปก่อนแล้ว อีกทั้งความชำนาญในการสืบสวนของพนักงานยังไม่มีประสบการณ์มากนัก ในคดีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ พนักงานสืบสวน ยังไม่มีความรู้ความสามารถในด้านคอมพิวเตอร์ เพราะผู้ที่กระทำความผิดส่วนใหญ่เป็นผู้ที่มีความรู้ความชำนาญ มีการศึกษาที่ดี ดังนั้นจำเป็นมากที่พนักงานควรมีความรู้เฉพาะด้านจะได้สามารถเข้าถึงหลักฐานและตัวผู้กระทำความผิดได้

แนวทางในการแก้ไขปัญหาในประเทศไทย จึงจำเป็นต้องจัดตั้งหน่วยงานที่มีอำนาจหน้าที่ โดยเฉพาะสรรหาและพัฒนาบุคลากรจากกลุ่มผู้มีประสบการณ์ด้านการสืบสวนสอบสวนคดีอาญา ที่มีความรู้พื้นฐานทางคอมพิวเตอร์และอิเล็กทรอนิกส์และกลุ่มวิชาชีพทางด้านคอมพิวเตอร์ เพื่ อฝึกอบรมในด้านวิธีการตรวจค้นและยึดพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ โดยเฉพาะเพื่อเตรียมการที่จะจัดการกับอาชญากรรมคอมพิวเตอร์ในประเทศไทยต่อไป

แนวทางแก้ไข และข้อเสนอแนะ

จากการวิเคราะห์กฎหมายที่มีโทษทางอาญาของไทยที่ใช้บังคับอยู่ จะเห็นว่ายังไม่เพียงพอต่ อการแก้ไขปัญหาการกระทำความผิดที่ผู้กระทำได้มีการพัฒนารูปแบบโดยอาศัยเทคโนโลยีใหม่ๆมาใช้เป็นช่องทางทางแก้ที่ดีที่สุดจึงควรที่จะมีการบัญญัติกฎหมายใหม่ที่เกี่ยวกับการกระทำผิดต่อข้อมูลคอมพิวเตอร์โดยตรง มีการกำหนดนโยบายรัฐที่ชัดเจน ฯลฯ ทั้งนี้ แม้จะต้องมีการล่ว งล้ำสิทธิส่วนบุคคลเพิ่มขึ้นก็ตาม แต่เมื่อการกระทำดังกล่าวเป็นการกระทำเพื่อประโยชน์ในการรักษาความสงบเรียบร้อยและความปลอดภัยของสังคมส่วนรวมก็ถือเป็นสิ่งที่ควรจะพึงกระทำ ซึ่งสามารถสรุปข้อเสนอแนะเพื่อใช้เป็นแนวทางได้ดังนี้

1. ด้านนโยบายของรัฐบาล
   1.1) ภาครัฐควรกำหนดนโยบายระดับชาติให้ชัดเจน ทั้งในเรื่องนโยบายด้านการรักษาความมั่นคงของระบบคอมพิวเตอร์และเครือข่าย และการปราบปรามอาชญากรรมคอมพิวเตอร์ รวมทั้งผลักดันกฎหมาย และมาตรการต่างๆที่จะช่วยให้การป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์สัมฤทธิ์ผลในทางปฏิบัติอย่างเร่งด่วน อาทิ

จัดตั้งองค์กรที่รับผิดชอบในระดับชาติ เพื่อกำหนดนโยบายในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

1.2) ภาครัฐควรกำหนดนโยบายด้านความมั่นคงของเครือข่ายคอมพิวเตอร์ และความปลอดภัยของข้อมูลให้สอดคล้องกับหลักสิทธิเสรีภาพของประชาชน ทั้งในด้านการติดต่อสื่อสาร สิทธิความเป็นส่วนตัว และดำเนินการด้วยความโปร่งใส ชอบธรรม

2. ด้านกฎหมาย

2.1)ในส่วนของกฎหมายสารบัญญัติ ต้องมีการบัญญัติกฎหมายเฉพาะ คือ กฎหมายอาชญากรรมคอมพิวเตอร์ มาบังคับใช้ มีการกำหนดฐานความผิดและบทลงโทษโดยเฉพาะเพื่อแก้ไขความล้าสมัยและการตีความโดยเคร่งครัดของกฎหมายอาญา ทั้งนี้ ควรมีขอบเขต ที่กว้างขวางพอที่จะครอบคลุมการกระทำความผิด แต่ขณะเดียวกันก็ต้องคำนึงถึงจุดดุลยภาพระหว่างผลประโยชน์ของสาธารณชนและสิทธิเสรีภาพของประชาชนที่อาจต้องเสียไปด้วย เพราะการใช้อำนาจรัฐและการบัญญัติกฎหมายใดๆย่อมมีผลกระทบต่อสิทธิเสรีภาพของประชาชนเสมอ

2.2)ในส่วนของกฎหมายวิธีสบัญญัติ ควรกำหนดหลักเกณฑ์หรือแนวทางปฏิบัติให้ชัดเจน ทั้งในเรื่องอำนาจหน้าที่เจ้าพนักงาน , วิธีสืบสวนสอบสวน , การรวบรวมและการตรวจสอบพยานหลักฐาน เพื่อให้หน่วยงานที่เกี่ยวข้องและเจ้าพนักงานผู้ปฏิบัติหน้าที่สามารถบังคับใช้กฎหมายได้อย่างมีป ระสิทธิภาพ และเป็นไปในทิศทางเดียวกัน อาทิ

- วางหลักกฎหมายในเรื่องสถานะของข้อมูลคอมพิวเตอร์ให้ชัดเจนว่า จัดเป็น “สิ่งของ” หรือไม่ เพราะแม้กฎหมายวิธีพิจารณาความอาญาจะให้สามารถตีความเทียบเคียงได้ แต่ก็ควรมีกฎหมายพิเศษบัญญัติให้ชัดเจนเพื่อที่ว่าเจ้าพนักงานจะสามารถรวบรวมเป็นพยานหลักฐานได้
- ควรมีกฎหมายพิเศษหรือกฎหมายวิธีสบัญญัติ ที่กำหนดถึงขั้นตอนต่างๆในการนำตัวผู้กระทำผิดมาลงโทษ อาทิ ให้อำนาจเจ้าพนักงาน สามารถกู้พยานหลักฐานที่ถูกกำจัด ทำล ายคืนมาได้ ฯลฯ เพิ่มเติมไว้ใน พระราชบัญญัติดังกล่าว นอกเหนือจากการมุ่งบัญญัติแต่เ ฉพาะในส่วนของการกระทำผิดหรือกฎหมายสารบัญญัติเท่านั้น ซึ่งน่าจะให้ผลในทางปฏิบัติกว่าการแก้ไขประมวลกฎหมายวิธีพิจารณาความอาญา ดังเช่น พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 ที่มีการบัญญัติกฎหมายทั้งในส่วนสารบัญญัติและวิธีสบัญญัติไว้ในกฎหมายฉบับเดียวกัน

- แต่งตั้งบุคลากรที่มีความรู้ความเชี่ยวชาญในวิทยาการคอมพิวเตอร์ เข้าร่วมในทีมตรวจค้นพยานหลักฐานกับเจ้าพนักงานด้วยและวางหลักหรือขอบเขตอำนาจให้เหมาะสม
- จัดตั้งหน่วยงานพิเศษเพื่อรับผิดชอบคดีอาชญากรรมคอมพิวเตอร์โดยเฉพาะ โดยมีเจ้าหน้าที่ในองค์กรที่ได้รับการอ บรมในแง่เทคนิควิทยาการคอมพิวเตอร์ มีความรู้ความชำนาญ ในการสอบสวนและ รวบรวมพยานหลักฐาน

3. ด้านบุคลากร

3.1)ควรมีการจัดโปรแกรมฝึกอบรมทั้งในส่วนเทคนิค และประเด็นกฎหมายที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ เพื่อเตรียมความพร้อมของบุคลากรในส่วนของกระบวนการยุติธรรมทุกระ ดับ ทั้งระดับผู้บริหาร ผู้ปฏิบัติการ องค์กรตำรวจ อัยการ และศาล

4. ด้านสังคม

4.1) นอกเหนือจากการออกมาตรการต่าง ๆ มาใช้แล้ว องค์กรทั้งภาครัฐและเอกชน รวมถึงสถาบันทางสังคมต่างๆ ควรร่วมกันรณรงค์ปลูกฝังคุณธรรม จริยธรรม จิตสำนึก และจรรยาบรรณ เพื่อสร้างแนวทางปฏิบัติที่ ดีของการใช้เทคโนโลยีที่ถูกต้องให้แก่คนในสังคม

อย่างไรก็ตาม แม้ว่าปัจจุบันหน่วยงานต่างๆจะเริ่มมีความตื่นตัวต่อปัญหาอาชญากรรมคอมพิวเตอร์กันมากขึ้น แต่ปัญหานี้ไม่สามารถแก้ไขได้ด้วยองค์กรใดเพียงองค์เดียว จำเป็นต้องได้รับความร่วมมือจากทุกๆ ฝ่ายในสังคม เพราะแท้ ที่จริงแล้วปัญหาอาชญากรรมคอมพิวเตอร์ ก็ขึ้นอยู่กับมนุษย์ทุกคนที่อยู่ในสังคมนั่นเอง

บรรณานุกรม

หนังสือ

กระมล ทองธรรมชาติ, สมบูรณ์ สุขสำราญ, เรื่องน่ารู้เกี่ยวกับการปกครองและรัฐธรรมนูญของสหรัฐอเมริกา, 2546

คณิต ณ นคร. กฎหมายวิธีพิจารณาความอาญา. พิมพ์ครั้งที่ 3 แก้ไขเพิ่มเติม. กรุงเทพมหานคร : นิติบรรณาการ, 2539

ชัยวัฒน์ วงศ์วัฒนศานต์, ทวีศักดิ์ กออนัตกูล, สุรางคณา แก้วจำนงค์, **คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทาง อิเล็กทรอนิกส์ พ.ศ. 2544**, (กรุงเทพ, สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, 2545)

ยุทธพงษ์ พงษ์สวัสดิ์, **คำบรรยายวิชาการสืบสวนสอบสวน**, คณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2513

สุโขทัยธรรมาธิราช, มหาวิทยาลัย. เอกสารการสอนชุดวิชากฎหมายวิธีสบัญญัติ 3 หน่วยที่ 4. พิมพ์ครั้งที่ 12. กรุงเทพมหานคร : มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2539

หยุด แสงอุทัย, **ประมวลกฎหมายวิธีพิจารณาความอาญา ศึกษาทางคำพิพากษาศาลฎีกา** (กรุงเทพมหานคร: สำนักพิมพ์ มหาวิทยาลัยธรรมศาสตร์, 2538)

หนังสือ eLeader Thailand (เมษายน 2550 Update Information : 12 เมษายน 2550)

บทความ

กลุ่มพันธมิตรธุรกิจซอฟต์แวร์ บริษัทพีซีแอนด์ เอสโซซิเอทส์คอนซัลติ้ง จำกัด , ผลการจับกุมทางอินเตอร์เน็ต, 2548

ญาณพล ยั่งยืน, อาชญากรรมทางคอมพิวเตอร์, (ศูนย์ข้อมูลข้อสนเทศ: สำนักงานตำรวจแห่งชาติ), หน้า 4 (อัดสำเนา)

พรเพชร วิชิตชลชัย, “บทวิเคราะห์เรื่อง :การรับฟังข้อมูลจากสื่ออิเล็กทรอนิกส์เป็นพยานหลักฐานในคดีทรัพย์สินทางปัญญา และการค้าระหว่างประเทศ,” **วารสารกฎหมายทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ,** (รวบรวมโดยศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ), หน้า 222

Adams, Jo-Ann M. “CONTROLLING CYBERSPACE: APPLYING THE COMPUTER FRAUD AND ABUSE ACT TO

“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”

วิทยานิพนธ์

ฉัทปณัย รัตนพันธ์, “อาชญากรรมคอมพิวเตอร์: ศึกษาการกำหนดฐานความผิด และการดำเนินอาชญากรรมทางคอมพิวเตอร์.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2547

พรทิพย์ ตัณฑวนันท์, “อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์.” วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต คณะนิติศาสตร์ ธรรมศาสตร์, 2548

วัลลิกา อุ่นศรี. “ ปัญหาการรวบรวมและพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีอาญา.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2544.

สุปรียา อภิวัฒนากร, “อาชญากรรมทางคอมพิวเตอร์: ศึกษากรณีการหลอกลวงทางอินเตอร์เน็ต” วิทยานิพนธ์มหาบัณฑิต คณะ นิติศาสตร์ มหาวิทยาลัยจุฬาลงกรณ์, 2545

สุรพันธ์ มั่นคงดี, “พยานหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์,” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์ มหาวิทยาลัย, 2541

อณิญพิไล เงินวิจิตร, “ปัญหาในการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2544

พระราชบัญญัติ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

Book

Black’s Law Dictionary, 7 e.d.(St.Paul, Minn: West Group, 1999)

Charles H.Whitebread and Christopher Slobogin, supra note 5

See Edward M. Wise, United States Computer Crimes and Other Crimes against Information Technology in U.S.A. Review of penal Law 1992

Internet

http://www.ecid.police.go.th
http://thaicert.nectec.or.th
www.dsi.go.th
www.mict.go.th
www.usdou.gov

ภาคผนวก

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๕๐

เป็นปีที่ ๖๒ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของ

ระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

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

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและ

ข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

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

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

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

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือ บุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษจะต้องรับโทษภายในราชอาณาจักร

หมวด ๒
พนักงานเจ้าหน้าที่

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐาน

อื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

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

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

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

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา ๒๐ ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้อง พร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา ๒๑ ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครองหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวงทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจมีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับไม่เกินสองแสนบาทและปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๒๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

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

ที่มา : ราชกิจจานุเบกษา
เล่มที่ ๑๒๔ ตอนที่ ๒๗ ก หน้า ๔ – ๑๓
ประกาศ ณ วันที่ ๑๘ มิถุนายน ๒๕๕๐

ประวัติผู้เขียน

ชื่อ – สกุล : นายวิศรุต อนุศาสนนันทน์

วัน เดือน ปี : 5 มิถุนายน 2525

วุฒิการศึกษา :

ปี 2547 นิติศาสตรบัณฑิต มหาวิทยาลัยกรุงเทพ

ประสบการณ์ทำงาน :

ปี 2549 - ปัจจุบัน ฝ่ายบังคับคดี บริษัท กฤตธีกรกฎหมายและบัญชี จำกัด