

ปัญหากฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์
ในชั้นพนักงานสอบสวน

ปิ่นฤๅณัฐ ชันเขต

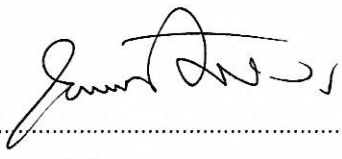
วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
คณะนิติศาสตร์
สถาบันบัณฑิตพัฒนบริหารศาสตร์

2559

ปัญหากฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์
ในชั้นพนักงานสอบสวน
ปิ่นตมัฐ ชันเขต
คณะนิติศาสตร์

ผู้ช่วยศาสตราจารย์..........อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ดร.วริยา ลำเลิศ)

คณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาแล้วเห็นสมควรอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรนิติศาสตรมหาบัณฑิต

รองศาสตราจารย์..........ประธานกรรมการ
(ดร.พินัย ณ นคร)

..........กรรมการ
(ดร.วัชร เนติวานิชย์)

ผู้ช่วยศาสตราจารย์..........กรรมการ
(ดร.วริยา ลำเลิศ)

ศาสตราจารย์..........คณบดี
(ดร.ประสิทธิ์ เอกบุตร)

กันยายน 2559

บทคัดย่อ

ชื่อวิทยานิพนธ์	ปัญหากฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ ในชั้นพนักงานสอบสวน
ชื่อผู้เขียน	ร้อยตำรวจเอกหญิงปณิณัฐ ชันเขต
ชื่อปริญญา	นิติศาสตรมหาบัณฑิต
ปีการศึกษา	2559

บทความนี้เป็นส่วนหนึ่งของวิทยานิพนธ์ “ปัญหากฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในชั้นพนักงานสอบสวน” มีวัตถุประสงค์เพื่อศึกษาถึงอำนาจหน้าที่ของพนักงานสอบสวนรวมถึงค้นหาปัญหากฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานในชั้นพนักงานสอบสวนของประเทศไทยนำมาเปรียบเทียบกับอำนาจหน้าที่ของพนักงานสอบสวนในต่างประเทศที่ใช้ระบบกฎหมายคอมมอนลอว์ การวิจัยได้เปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกา และประเทศอังกฤษ นอกจากนี้ ยังได้เปรียบเทียบกับอำนาจหน้าที่ของพนักงานสอบสวนในต่างประเทศที่ใช้ระบบกฎหมายซีวิลลอว์ โดยศึกษาเปรียบเทียบกับประเทศสหพันธ์สาธารณรัฐเยอรมนี จากนั้นจึงนำมาวิเคราะห์ถึงปัญหากฎหมายในแต่ละระบบกฎหมาย หาแนวทางและหามาตรการทางกฎหมายที่เกี่ยวข้องกับปัญหาดังกล่าว เพื่อนำเสนอแนวทางในการปรับปรุงแก้ไขปัญหาเกี่ยวกับอำนาจหน้าที่ของเจ้าพนักงานสอบสวนคดีทั่วไปของประเทศไทยให้มีอำนาจหน้าที่ตามกฎหมาย เพื่อให้สามารถรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพ แต่ในขณะเดียวกันก็อยู่ภายใต้กรอบของกฎหมายที่บัญญัติชัดเจนและเหมาะสมกับประเทศไทย

จากการศึกษา พบว่า ในปัจจุบันการใช้อำนาจของพนักงานสอบสวนคดีอาญาทั่วไป ในการแสวงหาพยานหลักฐานตามกฎหมายวิธีพิจารณาความอาญาซึ่งไม่ใช่พนักงานสอบสวนคดีพิเศษ และไม่ใช่พนักงานเจ้าหน้าที่ตามมาตรา 18 และมาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ที่มีอำนาจในการเข้าถึงพยานหลักฐานอิเล็กทรอนิกส์มากกว่า อีกทั้งยังมีกฎหมายให้อำนาจไว้ชัดเจน

พยานหลักฐานอิเล็กทรอนิกส์ส่วนใหญ่จะเป็นข้อมูลส่วนบุคคล หรืออยู่ในความครอบครองของผู้ให้บริการ เช่น ผู้ประกอบการด้านโทรศัพท์เคลื่อนที่ ผู้ประกอบการด้านการเงินการธนาคาร การปฏิบัติหน้าที่ของพนักงานสอบสวนจึงเป็นการละเมิดสิทธิส่วนบุคคลที่ได้รับการคุ้มครองตามรัฐธรรมนูญ การตรวจสอบข้อมูลส่วนบุคคลซึ่งอยู่ภายในเครื่องคอมพิวเตอร์ เครื่องมือสื่อสารหรือข้อมูลอันเกิดจากสื่ออิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นโดยบุคคลนั้นๆ หากไม่มีกฎหมายบัญญัติอำนาจไว้อย่างชัดเจนก็จะกระทำไม่ได้ การรวบรวมพยานหลักฐานอิเล็กทรอนิกส์โดยอาศัยกฎหมายวิธีพิจารณาความอาญาจึงยังไม่เพียงพอสำหรับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ จึงได้ศึกษากฎหมายต่างประเทศเพื่อทราบถึงอำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ เปรียบเทียบกับอำนาจของพนักงานสอบสวนของประเทศไทยต่อไป

แนวทางในการแก้ไขปัญหามีความจำเป็นอย่างยิ่งที่ประเทศไทย จะต้องบัญญัติกฎหมายในการใช้อำนาจของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา มีอำนาจในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ชัดเจน เพื่อให้การแสวงหาพยานหลักฐานอิเล็กทรอนิกส์มีประสิทธิภาพ ในเรื่องของการยึดและค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ควรเป็นความผิดซึ่งหน้าการยึดการค้นเพื่อตรวจสอบไม่จำเป็นต้องขออนุญาต เพียงอาศัยเหตุอันควรสงสัยว่ามีส่วนเกี่ยวข้องกับการกระทำความผิดก็เพียงพอแล้ว และกรณีที่ผู้ครอบครองให้ความยินยอมแก่เจ้าหน้าที่สามารถทำการค้นและยึดข้อมูลคอมพิวเตอร์หรือข้อมูลในเครื่องอิเล็กทรอนิกส์ได้ การใช้อำนาจต้องไม่เกินขอบเขตที่กฎหมายบัญญัติไว้ เพื่อให้กฎหมายมีความชัดเจนส่งผลให้การปฏิบัติหน้าที่มีประสิทธิภาพมากยิ่งขึ้น

ABSTRACT

Title of Thesis	Legal Problems on Electronic Evidence Collecting in the Investigator
Author	Pol. Capt. Pannat Khankhate
Degree	Master of Laws
Year	2016

This article is a part of the thesis “legal issues about electronic evidence and witness collection in investigator level” aims to study duties and power of investigators as well as ascertaining legal issues about evidence and witness collection in investigator level of Thailand to compare with power and duties of investigators in foreign countries that exercise common law. The research was conducted to compare with law in The United States of America and England. Furthermore, it included the comparison of power and duties of investigators in foreign countries that exercise common law by comparing with Federal Republic of Germany. The result would be analyzed in terms of legal issues in each law system to find guidelines and measures relating to such problems. After that, the researcher would apply the result to propose approaches for resolving issues about power and duties of general investigators in Thailand so that they have lawful power and duties to gather electronic evidence and witness effectively. Meanwhile, their actions should be consistent with the law which is obviously and properly enforced in Thailand.

The study result was found that currently, power of investigators in general criminal cases to seek evidences and witnesses according to criminal procedure was not performed by special investigators or the officials subject to section 18 and section 19 of Computer Crime Act B.E. 2550 who had more authority to access electronic witness and the law was clearly stipulated about their authorization.

Most electronic evidence and witness was personal information or under the possession of service providers such as mobile phone entrepreneurs, or finance and banking entrepreneurs. Therefore, duty performing of investigators was violating personal rights subject to the Constitution. To inspect personal information inside computers, communication devices or information in electronic media created by

such people, if the regulation on power was not obvious, could not be done. Gathering electronic evidence and witness subject to law on criminal procedure was not adequate. Accordingly, the researcher studied foreign laws to be aware of power and duties of investigators in the process of gathering electronic evidence and witness to compare with power and duties of investigators in Thailand.

For the guideline to solve such issues, it is extremely necessary that Thailand needs to regulate the law about power exercising of investigators according to the Criminal Procedure Code so that they have power to seek electronic evidence and witness conspicuously and effectively in terms of seizing and searching electronic data. Such action does not need search warrant but the investigators may claim doubtful cause that those who are examined are involved in the offence and the owner consents the officials to search and seize data on the computer or electronic devices. Power exercising should not be excessive according to the law with clear regulations so that their performance would be more productive and effective.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ไม่อาจสำเร็จลุล่วงได้หากไม่ได้รับโอกาส และความกรุณาจากบุคคลหลายฝ่าย ผู้เขียนขอกราบขอบพระคุณผู้ช่วยศาสตราจารย์ ดร.วริยา ล้ำเลิศ ซึ่งท่านได้เสียสละเวลาอันมีค่ายังเป็นอาจารย์ที่ปรึกษาและกรรมการในการสอบ ให้คำแนะนำ คำปรึกษา แก้ไขข้อบกพร่องต่าง ๆ ข้อคิดทางวิชาการ ตรวจสอบ รับรองการศึกษาวิจัยอิสระนี้จนสำเร็จได้ด้วยดี

ขอกราบขอบพระคุณรองศาสตราจารย์ ดร.พินัย ณ นคร ประธานกรรมการสอบการศึกษาอิสระ และอาจารย์ ดร.วัชร เนติวานิชย์ กรรมการสอบการศึกษาอิสระที่ได้ให้ความเมตตา ให้ความรู้ แนวคิด คำแนะนำในการปรับปรุงแก้ไขการศึกษาอิสระฉบับนี้ให้มีความถูกต้องสมบูรณ์มากยิ่งขึ้น และขอกราบขอบพระคุณผู้ช่วยศาสตราจารย์ ดร.วราภรณ์ วนาพิทักษ์ คณาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ให้กับผู้เขียน รวมถึงผู้เป็นเจ้านายงานเขียนในหนังสือ วารสาร บทความในเรื่องที่เกี่ยวข้องกับวิทยานิพนธ์ฉบับนี้ ทุกท่านที่ผู้เขียนได้ศึกษาค้นคว้าตลอดจนได้อ้างอิงถึงผลงานทางวิชาการซึ่งเป็นประโยชน์ในการเรียบเรียงวิทยานิพนธ์ฉบับนี้อย่างยิ่ง

นอกจากนี้ ผู้เขียนขอขอบคุณนางสาวจันทร์ทิพย์ แสงแปง และเพื่อนที่คอยให้กำลังใจ และให้ความช่วยเหลือ ผู้เขียนมาโดยตลอด

ผู้เขียนสำนึกในความเมตตากรุณาของบุคคลต่างๆ ที่ได้เอื้อนนามไว้ข้างต้นแล้ว และปิติยินดีอย่างยิ่งที่ได้มีโอกาสเผยแพร่ประกาศเกียรติคุณของท่านให้ปรากฏไว้เป็นลายลักษณ์อักษรควบคู่กับวิทยานิพนธ์นี้ตลอดไป

หากวิทยานิพนธ์ฉบับนี้มีคุณค่า และประโยชน์ต่อการศึกษาขอมอบเป็นเครื่องบูชาพระคุณ บิดา มารดา ครูบาอาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ให้แก่ข้าพเจ้า ส่วนถ้าเป็นความบกพร่องทั้งหลายผู้เขียนขอน้อมรับ และกราบขอภัยไว้ ณ ที่นี้ด้วย ขออาราธนาอำนาจคุณพระศรีรัตนตรัย และสิ่งศักดิ์สิทธิ์ทั้งหลายในสากลโลกนี้ ดลบันดาลให้ท่านมีแต่ความสุขสมปรารถนาทุกประการ

ปิ่นทณัฐ ชันเขต

กันยายน 2559

สารบัญ

	หน้า
บทคัดย่อ	(3)
ABSTRACT	(5)
กิตติกรรมประกาศ	(7)
สารบัญ	(8)
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการศึกษา	4
1.3 สมมติฐานของการวิจัย	4
1.4 ขอบเขตการศึกษา	5
1.5 วิธีการศึกษาวิจัย	5
1.6 ประโยชน์ที่คาดว่าจะได้รับ	5
บทที่ 2 แนวคิดและทฤษฎีเกี่ยวกับอำนาจหน้าที่ของพนักงานสอบสวน ในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์	6
2.1 ความหมายและความสำคัญของพยานหลักฐานอิเล็กทรอนิกส์	7
2.1.1 ความหมายของข้อมูลอิเล็กทรอนิกส์	8
2.1.2 การประมวลผลข้อมูล (Data Processing)	9
2.2 หลักเกณฑ์การคุ้มครองสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล	10
2.2.1 ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ.1948	11
2.2.2 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550	12
2.2.3 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547	12
2.2.4 กฎหมายวิธีพิจารณาความอาญา	15
2.3 การแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์ในคดีอาญา	17
2.3.1 การค้นพยานหลักฐานอิเล็กทรอนิกส์	18
2.3.2 รูปแบบและการวางแผนในการตรวจค้น (Search Planning)	21
2.4 การรับฟังพยานหลักฐานอิเล็กทรอนิกส์	22
บทที่ 3 หลักกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ ในต่างประเทศและประเทศไทย	24
3.1 หลักกฎหมายในต่างประเทศที่ใช้ระบบกฎหมาย Common Law	23

3.1.1	ประเทศสหรัฐอเมริกา	23
3.1.2	ประเทศอังกฤษ	31
3.2	หลักกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ใน ต่างประเทศที่ใช้ระบบกฎหมาย Civil Law	39
3.3	หลักกฎหมายที่เกี่ยวข้องกับพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทย	42
3.3.1	รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550	43
3.3.2	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550	44
3.3.3	พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	49
บทที่ 4	วิเคราะห์มาตรการทางกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์	53
4.1	วิเคราะห์กฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ ของประเทศไทย	54
4.1.1	ปัญหาในการออกหมายค้นโดยศาล	54
4.1.2	ปัญหาเกี่ยวกับการระบุรายละเอียดในการค้น	55
4.1.3	ปัญหาการรับฟังพยานหลักฐานอิเล็กทรอนิกส์	56
4.1.4	ปัญหาเกี่ยวกับเงื่อนไขที่จะทำการค้น	57
4.1.5	ปัญหาในการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ของศาล	58
4.2	วิเคราะห์กฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ ในต่างประเทศ	61
4.2.1	ประเทศสหรัฐอเมริกา	61
4.2.2	ประเทศอังกฤษ	64
4.2.3	ประเทศสหพันธ์สาธารณรัฐเยอรมนี	66
4.3	ปัญหาความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้อง	68
บทที่ 5	บทสรุปและข้อเสนอแนะ	69
5.1	บทสรุป	69
5.2	ข้อเสนอแนะ	71
5.2.1	อำนาจในการค้น	71
5.2.2	การแสวงหาและการรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ของพนักงานสอบสวน	72
	บรรณานุกรม	74
	ภาคผนวก	78
	ประวัติผู้เขียน	89

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

สังคมไทยในปัจจุบันมีความเจริญก้าวหน้าในการนำเทคโนโลยีและโทรคมนาคมเข้ามาใช้ ทำให้เกิดการเปลี่ยนแปลงสภาพสังคมไทยไปสู่สังคมสมัยใหม่ เป็นยุคของสังคมข่าวสารหรืออิเล็กทรอนิกส์โดยเฉพาะอย่างยิ่งการใช้คอมพิวเตอร์ ก่อให้เกิดการเปลี่ยนแปลงรูปแบบของการดำเนินชีวิต ในขณะที่เทคโนโลยีสารสนเทศได้รับการพัฒนาเพื่อใช้ประโยชน์ในหลาย ๆ ด้านนั้น การใช้เทคโนโลยีดังกล่าวเพื่อวัตถุประสงค์ทางการกระทำความผิด ก็ได้รับการพัฒนาการควบคู่กันไป ด้วย การกระทำความผิดที่เกี่ยวข้องกับเทคโนโลยีคอมพิวเตอร์มีแนวโน้มที่จะเพิ่มมากขึ้นเรื่อย ๆ และมีการพัฒนาวิธีการและรูปแบบในการกระทำความผิดให้มีความสลับซับซ้อนมากยิ่งขึ้น เช่น การลักทรัพย์ การฉ้อโกง การโอนเงินจากบัญชีธนาคารจากบัญชีหนึ่งไปสู่บัญชีหนึ่ง เหล่านี้ล้วนเป็นอาชญากรรมที่เกี่ยวกับข้อมูลอิเล็กทรอนิกส์ ที่ผ่านมาประเทศไทยประสบปัญหาว่าพนักงานสอบสวนไม่สามารถสืบสวนหาตัวผู้กระทำความผิดมาลงโทษได้ เพราะพยานหลักฐานมากมายที่เกี่ยวข้องกับพยานหลักฐานทางอิเล็กทรอนิกส์ แม้กระทั่งตัวของพนักงานสอบสวนเองก็ยังมีคำถามและข้อสงสัยว่า หากพบว่าเป็นพยานหลักฐานอิเล็กทรอนิกส์จะต้องขอหลักฐานอะไรบ้าง จากหน่วยงานที่เกี่ยวข้อง หรือจะต้องพิจารณาว่าพยานหลักฐานนั้นเป็นพยานหลักฐานทางอิเล็กทรอนิกส์หรือไม่ ควรสอบถามไปยังหน่วยงานใดบ้าง การตั้งคำถามผู้เชี่ยวชาญควรถามในประเด็นใดบ้าง เหล่านี้ล้วนแต่เป็นปัญหาของพนักงานสอบสวนทั้งสิ้น

ในอดีตพยานหลักฐานอิเล็กทรอนิกส์ส่วนใหญ่จะมุ่งไปที่เครื่องคอมพิวเตอร์เป็นหลักในการตีความว่าอุปกรณ์คอมพิวเตอร์ และสิ่งบันทึกไว้ในคอมพิวเตอร์นั้นเป็นพยานหลักฐานอิเล็กทรอนิกส์ แต่ในปัจจุบันไม่ใช่แค่คอมพิวเตอร์อีกต่อไป พยานหลักฐานอิเล็กทรอนิกส์ถูกพบในทุกหนทุกแห่งแทรกซึมมาอยู่ในการดำเนินชีวิตประจำวันของคนทั่วไป ซึ่งแทบจะไม่มีใครตัวด้วยซ้ำว่านั่นเป็นการสร้างพยานหลักฐานอิเล็กทรอนิกส์ เช่น การส่งอีเมลล์ การถ่ายภาพด้วยกล้องดิจิทัล การสืบค้นในเว็บไซต์ต่าง ๆ ล้วนเป็นการสร้างพยานหลักฐานทางอิเล็กทรอนิกส์ทั้งสิ้น

เนื่องจากมาตรการตามกฎหมายวิธีพิจารณาความอาญา ไม่สามารถครอบคลุมไปถึงอาชญากรรมทางอิเล็กทรอนิกส์ได้เท่าที่ควร การขอความร่วมมือกับหน่วยงานที่เกี่ยวข้องก็ยากลำบากไม่ค่อยให้ความร่วมมือแม้ว่าพนักงานสอบสวนจะออกหมายเรียก หรือแม้กระทั่งไปขอรับเองซึ่งต้องใช้ระยะเวลาอย่างมากที่จะนำพยานหลักฐานประเภทนี้เข้าสู่สำนวนการสอบสวนได้ จะเห็นได้ว่าการดำเนินคดีกับอาชญากรรมทางอิเล็กทรอนิกส์มีความยากลำบากในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ไม่เพียงแต่ยากต่อการระบุตัวผู้กระทำความผิดเท่านั้น แต่การแสวงหาพยานหลักฐานจากหน่วยงานที่ครอบครองพยานหลักฐานนั้น ๆ ยากยิ่งกว่า แม้จะได้พยานหลักฐานมาแล้วก็มีได้

หมายความว่าศาลจะรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์นั้น เนื่องจากข้อมูลอิเล็กทรอนิกส์ มีลักษณะเฉพาะแตกต่างจากพยานหลักฐานทั่วไป คือ เป็นข้อมูลที่ไม่มีรูปร่าง มองไม่เห็นด้วยตาเปล่า อีกทั้งข้อมูลอิเล็กทรอนิกส์ยังง่ายต่อการ ก๊อปปี้ ทำลาย แก้ไขเปลี่ยนแปลงได้ง่ายในเวลาอันสั้น จึงยากต่อการค้นและรวบรวมพยานหลักฐานเพื่อนำพยานหลักฐานอิเล็กทรอนิกส์เสนอต่อศาล

การค้น การยึดพยานหลักฐานอิเล็กทรอนิกส์ก็ต้องใช้อำนาจทางศาลเท่านั้น เพื่อไม่ให้กระทบต่อสิทธิส่วนบุคคลหรือความเป็นส่วนตัวตามกฎหมายรัฐธรรมนูญ ทำให้เกิดความล่าช้าในการเข้าถึงพยานหลักฐาน จึงเป็นช่องว่างที่จะทำให้ผู้กระทำความผิดทำลายพยานหลักฐานได้ พนักงานสอบสวนก็ยังมีข้อจำกัดในเรื่องความรู้ความชำนาญในการเก็บพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ รวมถึงอำนาจที่จะเข้าถึงข้อมูลอิเล็กทรอนิกส์ก็ยังมีข้อจำกัด และให้กระทำได้ตามประมวลกฎหมายวิธีพิจารณาความว่าด้วยอำนาจหน้าที่ของพนักงานสอบสวน เท่านั้น

แม้ว่าหลังจากที่ประเทศไทยจะประกาศใช้พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 แต่พนักงานสอบสวนก็ยังเป็นผู้รับผิดชอบรับคำร้องทุกข์ในคดีอาญาทั่วไป และหากพบว่าเกี่ยวข้องกับคอมพิวเตอร์ก็จะทำหนังสือประสานไปยังพนักงานเจ้าหน้าที่ตามพระราชบัญญัติคอมพิวเตอร์ ซึ่งรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแต่งตั้งเพื่อตรวจสอบข้อมูลรวมถึงพยานหลักฐานอื่นที่เกี่ยวข้อง เพื่อตรวจสอบวิเคราะห์การกระทำความผิดทางเทคโนโลยีรวบรวมเข้าสู่สำนวนการสอบสวนต่อไป

การดำเนินคดีอาญาใด ๆ ล้วนมีจุดเริ่มต้นที่พนักงานสอบสวนท้องที่ที่เกิดเหตุ ที่จะต้องรับผิดชอบในการรับคำร้องทุกข์จากผู้เสียหาย รวมถึงการรวบรวมพยานหลักฐานโดยต้องพิจารณาตามประมวลกฎหมายวิธีพิจารณาความอาญา ที่ให้อำนาจไว้ในส่วนที่เกี่ยวข้องกับพยานหลักฐาน หากเป็นพยานหลักฐานอิเล็กทรอนิกส์ ก็ให้เป็นอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ตามมาตรา 18-21 และหากเกี่ยวข้องกับผู้ใช้บริการตามมาตรา 26 พนักงานสอบสวนจะต้องประสานขอความร่วมมือจากพนักงานเจ้าหน้าที่ ซึ่งรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแต่งตั้ง โดยทำหนังสือ หรือขอคำปรึกษาได้จากศูนย์ตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี โดยเฉพาะความผิดตาม มาตรา 14 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.2550 ซึ่งมีลักษณะใกล้เคียงกับประมวลกฎหมายอาญา พนักงานสอบสวนจำเป็นจะต้องใช้ความระมัดระวังในการที่จะแจ้งข้อกล่าวหาเพิ่มเติมเพื่อไม่ให้กระทบสิทธิของผู้ต้องหาตามที่กฎหมายรัฐธรรมนูญคุ้มครองและรับรองไว้

ปัจจุบันการดำเนินคดีอาญาของพนักงานสอบสวน พยานหลักฐานล้วนเกี่ยวข้องกับพยานหลักฐานที่เป็นข้อมูลทางอิเล็กทรอนิกส์ทั้งสิ้น และมีแนวโน้มจะเพิ่มขึ้นอย่างต่อเนื่อง ผลอันเนื่องมาจากความเจริญก้าวหน้าทางเทคโนโลยีและการสื่อสาร การรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์จึงมีความสำคัญอย่างมากในยุคปัจจุบัน ในขณะที่ผู้เชี่ยวชาญเกี่ยวกับการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ยังมีไม่เพียงพอ พนักงานสอบสวนผู้รับผิดชอบคดีอาญาไม่มีอำนาจในการเข้าถึงพยานหลักฐานทางอิเล็กทรอนิกส์เท่าที่ควร อีกทั้งยังขาดความรู้ความชำนาญในการเก็บรวบรวมพยานหลักฐานประเภทนี้ รัฐก็ยังไม่ได้ให้ความสำคัญกับการเพิ่มบุคลากรที่มีความรู้ความชำนาญในการเก็บรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ ส่วนหน่วยงานที่มีอำนาจหน้าที่และมี

กฎหมายรองรับการปฏิบัติหน้าที่ สามารถเข้าถึงพยานหลักฐานทางอิเล็กทรอนิกส์ได้ง่ายกว่าพนักงานสอบสวนทั่วไป เช่น กรมสอบสวนคดีพิเศษ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ก็จะได้รับมอบหมายเฉพาะคดีสำคัญที่ผู้บังคับบัญชาระดับสูงมอบหมาย หรือคดีที่เกี่ยวข้องกับความมั่นคงของประเทศ

แม้ว่าพยานหลักฐานทางอิเล็กทรอนิกส์ถือเป็นพยานหลักฐานที่สำคัญในคดีที่เกี่ยวข้องกับอาชญากรรมทางอิเล็กทรอนิกส์ ในการที่จะติดตามตัวผู้กระทำความผิดมาดำเนินคดีตามกฎหมาย แต่ข้อมูลทางอิเล็กทรอนิกส์ที่จะใช้เป็นพยานหลักฐานก็มีลักษณะเฉพาะสามารถเปลี่ยนแปลงแก้ไขได้ง่าย จึงจำเป็นที่พนักงานสอบสวนผู้รับผิดชอบคดีจะต้องมีความรู้ความชำนาญและสามารถเข้าถึงพยานหลักฐานประเภทนี้ได้อย่างรวดเร็ว เพื่อให้ทันกับอาชญากรที่มีความชำนาญด้านเทคโนโลยี ที่พยายามจะทำลาย กลบเกลื่อนร่องรอยในการกระทำความผิดอยู่เสมอ เพื่อให้การดำเนินคดีที่เกี่ยวข้องกับอาชญากรรมทางอิเล็กทรอนิกส์ เป็นไปอย่างมีประสิทธิภาพสอดคล้องทันต่อการเปลี่ยนแปลงของโลกและเทคโนโลยีต่อไป

ดังนั้น ผู้วิจัยจึงทำการศึกษารายงานของพนักงานสอบสวนที่ขึ้นตรงต่อสำนักงานตำรวจแห่งชาติ รวมถึงค้นหาปัญหาในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ของพนักงานสอบสวนของประเทศไทย นำมาเปรียบเทียบกับอำนาจหน้าที่ของพนักงานสอบสวน ในกลุ่มประเทศที่ใช้ระบบกฎหมายคอมมอนลอว์ ซึ่งผู้วิจัยเปรียบกับ ประเทศสหรัฐอเมริกา และประเทศอังกฤษ ซึ่งมีการบัญญัติกฎหมายเกี่ยวกับอาชญากรรมทางอิเล็กทรอนิกส์ และการให้อำนาจพนักงานสอบสวนในการเข้าถึงพยานหลักฐานทางอิเล็กทรอนิกส์ได้อย่างเต็มที่ ให้ความสำคัญต่อการเข้าควบคุมข้อมูลทางอิเล็กทรอนิกส์ที่เป็นพยานหลักฐานทางอิเล็กทรอนิกส์ โดยอ้างเหตุผลฉุกเฉิน แต่ในขณะเดียวกันก็ต้องคำนึงถึงความเป็นส่วนตัวของพลเมือง การให้อำนาจของพนักงานตำรวจในการค้นจึงกระทำไม่ได้มากกว่าความจำเป็น โดยพิจารณาจาก “มีเหตุอันควรสงสัย (Probable Cause)” ว่าพยานหลักฐานนั้นเกี่ยวข้องกับการกระทำความผิดและจะก่อให้เกิดความเสียหายให้กับส่วนรวมเป็นหลัก

นอกจากนี้ ผู้วิจัยยังได้ศึกษาเปรียบเทียบถึงอำนาจหน้าที่ของพนักงานสอบสวน ในต่างประเทศที่ใช้ระบบกฎหมายซีวิลลอว์ ได้แก่ สหพันธสาธารณรัฐเยอรมนี ซึ่งได้มีการปรับแก้กฎหมายที่มีอยู่เดิมให้สอดคล้องทันกับอาชญากรรมทางอิเล็กทรอนิกส์ แม้ว่าสหพันธสาธารณรัฐเยอรมนี จะให้ความสำคัญในการคุ้มครองสิทธิเสรีภาพของประชาชนตามรัฐธรรมนูญเป็นสำคัญ แต่ศาลของสหพันธสาธารณรัฐเยอรมนีสามารถใช้ดุลพินิจได้อย่างกว้างขวางโดยศาลถือหลักว่าพยานหลักฐานสามารถได้มาโดยหมายหรือหมายนั้นมิชอบก็พร้อมก็ได้ ซึ่งจะเห็นว่ากฎหมายของสหพันธสาธารณรัฐเยอรมนี ไม่ได้ให้ความสำคัญกับกฎหมายเคร่งครัดนัก ในเรื่องหลักปฏิบัติในการใช้มาตรการบังคับของเจ้าพนักงานในการแสวงหาพยานหลักฐาน

ดังนั้น เพื่อหามาตรการทางกฎหมายและแนวทางแก้ไขปัญหาการรวบรวมพยานหลักฐานที่เป็นพยานหลักฐานอิเล็กทรอนิกส์ และข้อเสนอแนะในการแก้ไขกฎหมายวิธีพิจารณาความอาญาในการให้อำนาจพนักงานสอบสวนทั่วไปถึงพยานหลักฐานทางอิเล็กทรอนิกส์ให้มีความถูกต้องตามหลักการค้นหาความจริง สามารถดำเนินคดีได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาปัญหากฎหมายเกี่ยวกับอำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ในการค้นและการยึดหลักฐานทางคดี
2. เพื่อศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้องในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ตามกฎหมาย
3. เพื่อศึกษาถึงหลักกฎหมายในการสืบสวนสอบสวน การค้น การจับ และการยึดพยานหลักฐานอิเล็กทรอนิกส์ของไทยเปรียบเทียบกับประเทศสหรัฐอเมริกา ประเทศอังกฤษ และสหพันธ์สาธารณรัฐเยอรมนี
4. เพื่อศึกษาวิเคราะห์ถึงปัญหาข้อขัดข้องตามประมวลกฎหมายวิธีพิจารณาความอาญาและการใช้อำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ของในประเทศไทย
5. เพื่อเสนอแนะและหามาตรการทางกฎหมายปรับแก้ประมวลกฎหมายวิธีพิจารณาความอาญาในหมวดอำนาจของพนักงานสอบสวนทั่วไป ให้มีอำนาจเหมือนกับพนักงานสอบสวนคดีพิเศษในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์

1.3 สมมติฐานของการวิจัย

เนื่องจากรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550 มีบทบัญญัติที่ให้อำนาจรัฐตรากฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ภายใต้ขอบเขตที่รัฐธรรมนูญกำหนด เช่น มาตรา 36 บัญญัติรับรองคุ้มครองสิทธิความเป็นส่วนตัวของบุคคล ซึ่งเป็นสิทธิส่วนบุคคล รัฐจะกระทำการใด ๆ ก็ได้หากเป็นกรณีที่กระทำไปเพื่อประโยชน์สาธารณะ รัฐอาจอาศัยข้อยกเว้นดังกล่าวเพื่อให้อำนาจเจ้าหน้าที่ของรัฐเข้าไปตรวจสอบข้อมูลส่วนบุคคลใดบุคคลหนึ่งได้ตามสมควรโดยเฉพาะข้อมูลข่าวสารซึ่งจำกัอยู่ภายในเครื่องมือสื่อสารส่วนบุคคลหรือข้อมูลอันเกิดจากสื่ออิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นโดยบุคคลนั้น ๆ เช่น ข้อมูลที่ถูกบันทึกไว้ในเครื่องคอมพิวเตอร์ การแสวงหาพยานหลักฐานอิเล็กทรอนิกส์เพื่อมาดำเนินคดีกับผู้กระทำความผิด โดยนำประมวลกฎหมายวิธีพิจารณาความอาญามาปรับใช้จึงยังไม่เพียงพอ โดยเฉพาะพยานหลักฐานทางอิเล็กทรอนิกส์ มีลักษณะข้อมูลอิเล็กทรอนิกส์ มีความพิเศษแตกต่างจากพยานหลักฐานทั่วไป อีกทั้งยังง่ายต่อการทำลาย ยักย้ายถ่ายเท หากนำระบบการแสวงหาข้อเท็จจริง และการรวบรวมพยานหลักฐานว่าด้วยการค้น และยึดตามกฎหมายวิธีพิจารณาความอาญามาใช้กับพยานหลักฐานอิเล็กทรอนิกส์ ควรบัญญัติกฎหมายในเรื่องให้พนักงานสอบสวนมีอำนาจหน้าที่เข้าถึงพยานหลักฐานในคดีที่เกี่ยวข้องกับอาชญากรรมทางอิเล็กทรอนิกส์ ภายในขอบเขตที่ไม่กระทบสิทธิในข้อมูลข่าวสารส่วนบุคคล

ดังนั้น ต้องศึกษามาตรการกฎหมายของต่างประเทศ เพื่อนำมาเป็นแนวทางในการปรับแก้ประมวลกฎหมายวิธีพิจารณาความอาญาในส่วนที่เกี่ยวข้องกับอำนาจของพนักงานสอบสวนทั่วไปให้สามารถเข้าถึงพยานหลักฐานทางอิเล็กทรอนิกส์ต่อไป

1.4 ขอบเขตการวิจัย

การศึกษาวิจัยถึงข้อมูลที่เป็นพยานหลักฐานอิเล็กทรอนิกส์ วิเคราะห์หลักกฎหมายวิธีพิจารณาความอาญาที่ถือว่าน่าจะนำมาปรับใช้กับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ได้เพียงใด โดยจะทำการศึกษาเปรียบเทียบกับประเทศสหรัฐอเมริกา ประเทศอังกฤษ และสหพันธ์สาธารณรัฐเยอรมนี ที่เกี่ยวข้องกัอำนาจหน้าที่ของพนักงานพนักงานสอบสวนในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์เพื่อใช้เป็นพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์

1.5 วิธีการศึกษาวิจัย

การศึกษาคั้งนี้ใช้วิธีการศึกษาจากเอกสาร (Documentary Research) โดยศึกษาจากบทกฎหมายรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ประมวลกฎหมายวิธีพิจารณาความอาญารวมถึงบรรดาเอกสารกฎหมายที่เกี่ยวข้องกับพยานหลักฐานอิเล็กทรอนิกส์ โดยผู้ศึกษาได้ค้นคว้ารวบรวมจากเอกสารทางวิชาการ วิทยานิพนธ์ กฎ ระเบียบ คำสั่ง ข้อบังคับ เอกสารทางราชการ และเอกสารอื่น ๆ ที่เกี่ยวข้องนั้น นำมาวิเคราะห์และเรียบเรียง

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. เพื่อทราบถึงขอบเขตอำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในการค้นและการยึดหลักฐานทางคดี
2. เพื่อให้ทราบถึงแนวคิดและทฤษฎีที่เกี่ยวข้องในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ตามกฎหมาย
3. เพื่อศึกษาให้ทราบถึงหลักกฎหมายในการสืบสวนสอบสวน การค้น การจับ และการยึดพยานหลักฐานอิเล็กทรอนิกส์ของประเทศไทยเปรียบเทียบกับประเทศสหรัฐอเมริกา ประเทศอังกฤษ และสหพันธ์สาธารณรัฐเยอรมนี
4. เพื่อศึกษาวิเคราะห์หาปัญหาข้อขัดข้องตามประมวลกฎหมายวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ของพนักงานสอบสวนทั่วไปในประเทศไทย
5. เพื่อให้ทราบมาตรการทางกฎหมายแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความอาญาในหมวดอำนาจของพนักงานสอบสวนทั่วไป ให้มีกฎหมายรับรองอำนาจเหมือนกับพนักงานสอบสวนคดีพิเศษในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์รวมถึงอำนาจหน้าที่ของพนักงานสอบสวนในคดีอาชญากรรมทางคอมพิวเตอร์ของประเทศไทย กับประเทศสหรัฐอเมริกา ประเทศอังกฤษ และสหพันธ์สาธารณรัฐเยอรมนี

บทที่ 2

แนวคิดและทฤษฎีเกี่ยวกับอำนาจหน้าที่ของพนักงานสอบสวน ในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์

เนื่องจากประเทศไทยในปัจจุบันได้มีการนำเอาเทคโนโลยีและสารสนเทศ เข้ามาใช้ในการอำนวยความสะดวกสบายในชีวิตประจำวัน การดำเนินชีวิตของประชากรเปลี่ยนแปลงไปจากเดิม ส่วนใหญ่ล้วนเข้าไปเกี่ยวข้องกับการสื่อสารผ่านเครือข่ายอินเทอร์เน็ต การส่งอีเมลล์ ส่งแฟกซ์ การติดต่อสื่อสารผ่านโทรศัพท์เคลื่อนที่ การใช้คอมพิวเตอร์ในที่ทำงาน การทำธุรกรรมด้านการเงินการบัญชี เหล่านี้ล้วนเกี่ยวข้องกัพยานหลักฐานอิเล็กทรอนิกส์ทั้งสิ้น เทคโนโลยีสารสนเทศถูกนำมาใช้เพื่อเพิ่มประสิทธิภาพในการทำงานและการใช้ชีวิตประจำวันเพื่อสร้างความบันเทิง แม้แต่การศึกษา ค้นคว้าหาข้อมูลต่าง ๆ ก็จำเป็นต้องพึ่งพาอินเทอร์เน็ต

ในอีกด้านก็มีกลุ่มบุคคลที่นำเอาเทคโนโลยีมาใช้เพื่อแสวงหาผลประโยชน์โดยมิชอบ สำหรับตนเองและพวกพ้อง ก่อให้เกิดความเดือดร้อนให้กับประชาชนโดยทั่วไป ประเทศไทยกำลังประสบกับปัญหาอาชญากรรมทางอิเล็กทรอนิกส์เพิ่มมากขึ้น และทวีความรุนแรงมากขึ้นเป็นลำดับมีความซับซ้อนขึ้นในการก่ออาชญากรรม อาชญากรรมส่วนใหญ่มาจากการสื่อสารผ่านเครือข่ายอินเทอร์เน็ต ผ่านสื่ออิเล็กทรอนิกส์ โดยเฉพาะคอมพิวเตอร์และโทรศัพท์มือถือสามารถเข้าถึงเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ต่าง ๆ ได้อย่างง่ายดาย โดยไม่จำกัดเวลาและสถานที่

โครงสร้างทางกฎหมายทำให้เกิดปัญหาด้านการสืบสวนสอบสวนหาตัวผู้กระทำความผิดกฎหมายและการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ของพนักงานสอบสวน จึงต้องมีการพัฒนาให้ทันต่ออาชญากรรมทางอิเล็กทรอนิกส์ อาชญากรรมประเภทนี้เป็นลักษณะไร้พรมแดน รัฐและเจ้าหน้าที่ของรัฐจึงจำเป็นที่จะต้องศึกษาค้นหาความรู้และวิธีการเก็บรวบรวมพยานหลักฐานเพื่อให้เกิดความเชี่ยวชาญ เพราะการกระทำความผิดสามารถกระทำได้โดยไม่จำกัดเวลาสถานที่ อีกทั้งพยานหลักฐานประเภทนี้ถูกทำลายได้โดยง่าย จึงไม่ค่อยหลงเหลือให้พนักงานสอบสวนใช้เป็นหลักฐานในการดำเนินคดีกับผู้กระทำความผิด รวมถึงยากต่อการสืบสวนติดตามผู้กระทำความผิดมาดำเนินคดีตามกฎหมายได้

ดังนั้น จึงจำเป็นที่จะต้องศึกษาถึงแนวคิดในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ของพนักงานสอบสวน เพื่อหาวิธีการรับมือกับอาชญากรรมอิเล็กทรอนิกส์ ส่งเสริมให้มีการพัฒนาความรู้ให้มีความเชี่ยวชาญด้านเทคโนโลยี และกฎหมายเป็นเครื่องมือรองรับในการปฏิบัติหน้าที่ของพนักงานสอบสวน เพื่อที่จะเข้าถึงพยานหลักฐานอิเล็กทรอนิกส์และสามารถรวบรวมพยานหลักฐานอย่างถูกต้อง มีประสิทธิภาพ สอดคล้องกับสภาพการณ์ของโลกที่เปลี่ยนแปลงไปอย่างรวดเร็วสามารถนำตัวผู้กระทำความผิดมาฟ้องลงโทษต่อไป

ตามแนวคิดตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550 การดำเนินคดีพนักงานสอบสวนถือเป็นจุดเริ่มต้นของกระบวนการยุติธรรมทางอาญา การสอบสวนเป็นการดำเนินการของเจ้าพนักงานก่อนการยื่นฟ้อง การสอบสวนของพนักงานสอบสวนเป็นการดำเนินการก่อนการยื่นฟ้องของพนักงานอัยการ¹ การดำเนินการสอบสวนก็จะต้องเนื้อหาครอบคลุม 2 ประการ ได้แก่ การรวบรวมพยานหลักฐานและการใช้มาตรการบังคับ²

การแสวงหาและรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดจึงเป็นขั้นตอนก่อนการฟ้อง เมื่อมีการกระทำความผิดเกิดขึ้นการที่จะลงโทษผู้กระทำความผิดได้จำเป็นต้องมีการรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิด ถ้าไม่มีพยานหลักฐานก็ไม่สามารถที่จะดำเนินกระบวนการยุติธรรมทางอาญาได้ หากพยานหลักฐานที่จะนำมาพิสูจน์การกระทำความผิดเป็นส่วนสำคัญของกระบวนการยุติธรรมทางอาญา ผู้กระทำความผิดก็ยิ่งปกปิด ซ่อนเร้น หรือทำลายพยานหลักฐานซึ่งเป็นข้อมูลอิเล็กทรอนิกส์ต่าง ๆ ซึ่งเป็นข้อมูลจากสื่อต่าง ๆ ก็อาจจะต้องใช้เป็นพยานหลักฐานในคดีอาญาได้

ด้วยเหตุนี้ กฎหมายวิธีพิจารณาความอาญาจึงเป็นเครื่องมือสำคัญในการแสวงหาพยานหลักฐานซึ่ง ได้แก่ การค้น ถือเป็นมาตรการบังคับในการดำเนินคดีอาญา การค้นพยานหลักฐานอิเล็กทรอนิกส์จากสื่ออิเล็กทรอนิกส์ต่าง ๆ ซึ่งจะต้องรุกล้ำเข้าไปสู่ข้อมูลส่วนบุคคล ถือเป็นมาตรการที่รุนแรง ที่นำมาใช้บังคับ และผลของมาตรการบังคับนั้นจึงไปกระทบถึงสิทธิและเสรีภาพของบุคคล ดังนั้น พนักงานสอบสวนจึงจำเป็นที่จะต้องมีความเชี่ยวชาญและเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ อีกทั้งจะต้องมีเครื่องมือทางกฎหมายที่ให้อำนาจไว้อย่างชัดเจน เพื่อประโยชน์ต่อการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ต่อไป

2.1 ความหมายและความสำคัญของพยานหลักฐานอิเล็กทรอนิกส์

มาตรการทางกฎหมายที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ของพนักงานสอบสวน ถือเป็นสิ่งสำคัญเพื่อหาวิธีการรับมือกับอาชญากรรมอิเล็กทรอนิกส์ กฎหมายเป็นเครื่องมือรองรับในการปฏิบัติหน้าที่ของพนักงานสอบสวน เพื่อที่จะเข้าถึงพยานหลักฐานอิเล็กทรอนิกส์และสามารถรวบรวมพยานหลักฐานได้อย่างถูกต้อง พนักงานสอบสวนจึงจำเป็นที่จะต้องมีความเชี่ยวชาญและเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ อีกทั้งจะต้องมีเครื่องมือทางกฎหมายที่ให้อำนาจไว้อย่างชัดเจนเพื่อประโยชน์ต่อการปฏิบัติหน้าที่ที่ชอบด้วยกฎหมาย

¹ คณิต ณ นคร, กฎหมายวิธีพิจารณาความอาญา, พิมพ์ครั้งที่ 8 แก้ไขเพิ่มเติม (กรุงเทพฯ: วิญญูชน, 2555), หน้า 308.

² เรืองเดียวกัน, หน้า 313.

2.1.1 ความหมายของข้อมูลอิเล็กทรอนิกส์

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ให้ความหมายของคำว่า “ข้อมูลอิเล็กทรอนิกส์” หมายถึง ข้อความที่ได้ส่ง รับ เก็บรักษาหรือประมวลผลด้วยวิธีการอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรสาร โทรศัพท์หรือโทรสาร³ มาตรา 4 ยังให้คำนิยามคำว่า อิเล็กทรอนิกส์ ข้อความ ระบบข้อมูล การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ ผู้ส่งข้อมูล ผู้รับข้อมูล และบุคคลที่เป็นสื่อกลาง ไว้ดังนี้ “อิเล็กทรอนิกส์” หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ทาง ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น “อิเล็กทรอนิกส์” คือ โทรศัพท์ แฟกซ์ อีเมลล์ อินเทอร์เน็ต ก็ถือว่าเป็นอิเล็กทรอนิกส์ด้วย เพราะคำว่า “วิธีการทางอิเล็กทรอนิกส์นั้น” จะหมายความรวมถึงการส่งข้อมูลไปตามสายโทรศัพท์ สายแลน สายไฟเบอร์ หรือ แม้แต่การส่งข้อมูลผ่านดาวเทียมก็ล้วนแต่เป็นการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมด⁴

“อิเล็กทรอนิกส์” ยังปรากฏอยู่ในประมวลกฎหมายอาญาด้วย กล่าวคือ

มาตรา 1 “(14) แห่งประมวลกฎหมายอาญา “บัตรอิเล็กทรอนิกส์” หมายความว่า

(ก) เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใดทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า

(ข) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ ที่ผู้ออกให้แก่ผู้มีสิทธิใช้ โดยมีได้มีการออกเอกสารหรือวัตถุอื่นใดให้ แต่มีวิธีการใช้ในการทำงานเกี่ยวกับ หรือ

(ค) สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่าง

บุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ให้ความหมายของคำว่าระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ ไว้ดังนี้ “ระบบคอมพิวเตอร์” ตามกฎหมายฉบับนี้ไม่ได้หมายถึงเฉพาะเครื่องคอมพิวเตอร์

³ มาตรา 4 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

⁴ สุเนติ คงเทพ, คำอธิบายเกี่ยวกับกฎหมายคอมพิวเตอร์ (กรุงเทพฯ: ม.ป.พ., 2558), หน้า

ส่วนบุคคล หรือเครื่องคอมพิวเตอร์เซิร์ฟเวอร์เท่านั้น แต่ “ระบบคอมพิวเตอร์” ยังหมายความรวมถึง อุปกรณ์อิเล็กทรอนิกส์ หรืออุปกรณ์สื่อสารทุกประเภทที่มีโปรแกรมซอฟต์แวร์เฉพาะที่ทำให้อุปกรณ์ดังกล่าวสามารถประมวลผลข้อมูลคอมพิวเตอร์ได้เช่น โทรศัพท์มือถือ เครื่องโทรสาร เครื่องคอมพิวเตอร์แบบพกพา

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์⁵

ดังนั้น ข้อมูลคอมพิวเตอร์ จึงไม่ใช่เฉพาะตัวอักษร หรือข้อความที่สื่อความหมาย อ่านเข้าใจได้ที่หน้าจอภาพ (Monitor) เท่านั้น แต่เป็นข้อมูลดิจิทัลที่อยู่ในระบบคอมพิวเตอร์ และอยู่ที่ระบบคอมพิวเตอร์อาจประมวลผลได้

2.1.2 การประมวลผลข้อมูล (Data Processing)

เมื่อมีข้อมูลเกิดขึ้นหรือมีการรวบรวมข้อมูลต่าง ๆ ขึ้น วิธีการจัดการข้อมูลไม่ว่าการคำนวณ การเรียงลำดับ หรือการจัดกลุ่ม ต่างก็เป็นการประมวลผล (Processing) ทั้งสิ้น การประมวลผล จึงหมายถึง วิธีการจัดการกับข้อมูล โดยมีจุดมุ่งหมายเพื่อให้ได้ผลลัพธ์อย่างใดอย่างหนึ่ง ข้อสรุปที่ได้เรียกว่าข้อสนเทศ (Information) ซึ่งสามารถนำไปใช้ในการตัดสินใจต่าง ๆ ที่เกี่ยวข้อง ขึ้นอยู่กับการนำไปใช้ประโยชน์ของแต่ละบุคคล ขั้นตอนของการประมวลผลข้อมูล แบ่งเป็น 3 ขั้นตอน ได้แก่

2.1.2.1 การเตรียมข้อมูล (Input) คือ การเก็บรวบรวมข้อมูลเพื่อรอประมวลผล ซึ่งหมายรวมถึงการเปลี่ยนสภาพข้อมูลให้อยู่ในรูปแบบที่เหมาะสมและพร้อมที่จะประมวลต่อไป การเปลี่ยนสภาพข้อมูลประกอบด้วยการลงรหัสแทนข้อมูลจริง ซึ่งรหัสอาจเป็นตัวเลขหรือตัวอักษรย่อ การตรวจสอบความถูกต้อง การจัดประเภทข้อมูลให้เป็นกลุ่มตามลักษณะของข้อมูล และการบันทึกข้อมูลในสื่อ

2.1.2.2 การประมวลผล (Processing) หมายถึง วิธีการจัดการกับข้อมูล ซึ่งอาจเป็นการคำนวณการรวมข้อมูลมากกว่าหนึ่งชุดเข้าด้วยกัน (Merge) การดึงข้อมูลมาใช้ (Retrieve) หรือการเรียงลำดับ (Sort)

2.1.2.3 การนำเสนอผลลัพธ์ (Output) หมายถึง การนำผลลัพธ์ที่ได้จากการประมวลผลมาแสดงให้ทราบ เช่น แสดงผลสรุปในรูปของตาราง หรือกราฟ⁶

⁵ เรืองเดียวกัน, หน้า 117.

⁶ ไพบุลย์ อมรภิญโญเกียรติ, คำอธิบาย พ.ร.บ.คอมพิวเตอร์ พ.ศ.2550 (กรุงเทพฯ: โปรวิชั่น, 2553), หน้า 12-15.

ประเภทของการประมวลผลข้อมูล สามารถแบ่งออกเป็น 3 ประเภท ได้แก่ การประมวลผลข้อมูลด้วยมือ การประมวลผลข้อมูลด้วยเครื่องจักรกล และการประมวลผลข้อมูลด้วยเครื่องคอมพิวเตอร์ซึ่งเหมาะกับงานที่มีปริมาณมาก ประสิทธิภาพในการทำงานให้ผลลัพธ์ที่ถูกต้อง เป็นการคำนวณที่มีสูตรยุ่งยากซับซ้อน ทันสมัย⁷

ความหมายของข้อมูลจราจรทางคอมพิวเตอร์⁸ “ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารทางระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการหรืออื่น ๆ ที่เกี่ยวข้องกับ การติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

คำว่า “ข้อมูลจราจรทางคอมพิวเตอร์” บัญญัติอยู่ในมาตรา 18 มาตรา 22 มาตรา 23 มาตรา 24 มาตรา 25 มาตรา 26

ความหมายของผู้ให้บริการ “ผู้ให้บริการ” หมายความว่า ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น

ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น คำว่า “ผู้ให้บริการ” บัญญัติอยู่ในมาตรา 15 มาตรา 18 มาตรา 20 มาตรา 26

ความหมาย “ผู้ให้บริการ” หมายถึง ผู้ให้บริการคอมพิวเตอร์ เช่น บริการอินเทอร์เน็ต ตามหอพัก ตามคอนโดมิเนียม ตามอพาร์ทเมนท์ หรือร้านเกมออนไลน์ รวมถึงโรงแรมที่ให้บริการอินเทอร์เน็ตด้วย รวมถึงผู้ประกอบการโทรคมนาคม⁹

2.2 หลักเกณฑ์การคุ้มครองสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล

การคุ้มครองสิทธิเสรีภาพของประชาชนจากการละเมิดสิทธิเสรีภาพของเจ้าพนักงานของรัฐ ไม่ว่าจะเป็นการดำเนินการจับกุม หรือการตรวจค้น ก่อนศตวรรษที่ 18 เป็นเหตุให้เจ้าพนักงานของรัฐมีอำนาจมากในการปฏิบัติหน้าที่ ไม่มีหลักเกณฑ์ใดมาจำกัดอำนาจของเจ้าพนักงาน ในประเทศฝรั่งเศสสามารถจับบุคคลไปขังไว้โดยไม่แจ้งข้อกล่าวหา และสามารถขังไว้ได้โดยไม่มีกำหนดเวลา¹⁰ ในศตวรรษที่ 18 นักปราชญ์หลายท่าน เช่น มองเตสกีเออ จึงได้สร้างแนวคิดเกี่ยวกับสิทธิมนุษยชนขึ้น เป็นการนำไปสู่แนวคิดในการให้ความคุ้มครองสิทธิมนุษยชนมากขึ้นเห็นได้จากการจัดทำเอกสาร

⁷ วัชรภรณ์ สุริยาวัฒน์, คอมพิวเตอร์เบื้องต้นและเทคนิคการเขียนโปรแกรม (กรุงเทพฯ: ไทยเจริญการพิมพ์, 2543), หน้า 26-27.

⁸ เรื่องเดียวกัน, หน้า 28-29.

⁹ สุเนติ คงเทพ, เรื่องเดิม, หน้า 118.

¹⁰ จงรักษ์ จุฑานนท์, การคุ้มครองสิทธิของประชาชนต่อการถูกจับและตรวจค้นโดยไม่ชอบธรรม (กรุงเทพฯ: ม.ป.พ., 2525), หน้า 1.

ที่เกี่ยวกับการให้ความคุ้มครองสิทธิของบุคคล เช่น ในประเทศสหรัฐอเมริกา มีการจัดทำ The Declaration of Independence¹¹ และประเทศอังกฤษได้จัดทำ Magna Carta¹²

2.2.1 ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948

เดิมการให้ความคุ้มครองสิทธิ และเสรีภาพ ของบุคคลจะเป็นการให้ความคุ้มครองกันภายในรัฐใดรัฐหนึ่ง จนกระทั่งวันที่ 10 ธันวาคม ค.ศ.1948 องค์การสหประชาชาติได้มีการประชุมและประกาศปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ.1948 เป็นการให้ความร่วมมือกันระหว่างประเทศ เพื่อให้การคุ้มครองสิทธิและเสรีภาพของบุคคล และพัฒนาไปในทิศทางเดียวกัน¹³

หลักการของสัญญาประชาคม ดังกล่าว รัฐจะแทรกแซงสิทธิส่วนบุคคลหรือปัจเจกชนได้แต่ภายใต้บังคับบทบัญญัติของกฎหมายเท่านั้นปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ได้กำหนดหลักเกณฑ์ที่สำคัญเกี่ยวกับการคุ้มครองสิทธิในความเป็นอยู่ทั่วไปของประชาชน ดังนี้ “บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นอยู่ส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือการถูกลบหลู่ในเกียรติยศ และชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับการคุ้มครองจากกฎหมายต่อการแทรกแซงหรือการลบหลู่ดังกล่าวนี้”

จากบทบัญญัติดังกล่าวเป็นการให้ความคุ้มครองความเป็นอยู่ทั่วไปในชีวิตส่วนตัวของบุคคล ทั้งที่เป็นการดำเนินชีวิตประจำวัน การติดต่อสื่อสารเป็นหลัก และยกเว้น ในกรณีที่เพื่อประโยชน์สาธารณะ และมีกฎหมายอนุญาตให้ทำได้ แต่ก็ต้องมีการควบคุมมิให้มีการใช้อำนาจหน้าที่กระหอบกระเทือนต่อสิทธิของประชาชนมากเกินไป

สมัชชาสหประชาชาติจึงได้สร้างหลักการควบคุมการใช้อำนาจของรัฐขึ้นมาโดยประกาศใช้ “ประมวลจรรยาบรรณ สำหรับเจ้าหน้าที่ผู้มีหน้าที่โดยกฎหมาย” (Code of Conduct for Law Enforcement) ซึ่งข้อที่ 1 บัญญัติให้เจ้าพนักงานผู้มีหน้าที่รักษากฎหมายต้องปฏิบัติตามกฎหมาย โดยมุ่งที่จะให้บริการแก่ประชาชน และคุ้มครองให้ประชาชนปลอดภัยจากการกระทำที่ผิดกฎหมาย และข้อ 2 บัญญัติให้เจ้าพนักงานผู้มีหน้าที่รักษากฎหมายเมื่อมีการปฏิบัติตามกฎหมาย ที่เป็นการกระหอบกระเทือนถึงสิทธิดังกล่าว การกระทำนั้นต้องเคารพและคุ้มครองศักดิ์ศรีความเป็นมนุษย์ และจะต้องไม่ทำลายล้างหลักสิทธิมนุษยชน¹⁴

¹¹ กุลพล พลวัน, พัฒนาการแห่งสิทธิมนุษยชน, พิมพ์ครั้งที่ 3 (กรุงเทพฯ: วิญญูชน, 2538), หน้า 31.

¹² เรืองเดียวกัน, หน้า 74.

¹³ เรืองเดียวกัน, หน้า 36.

¹⁴ ศุภฤกษ์ ศุภรเศพย์, การค้นในทึรโธฐานของเจ้าพนักงานป้องกันและปราบปราม ยาเสพติด (วิทยานิพนธ์ปริญญาโทบริหารคดี สาขานิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์, 2545), หน้า 10.

2.2.2 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550

นับแต่ประเทศไทยเปลี่ยนแปลงการปกครองตั้งแต่นั้นการจัดทำรัฐธรรมนูญแห่งราชอาณาจักรไทยฉบับต่างก็เหมือนกับรัฐเสรีประชาธิปไตยอื่น ๆ คือได้รับแนวคิดของสิทธินี้สอนว่า “มนุษย์ทุกคนเกิดมามีศักดิ์ศรี” คือศักดิ์ศรีความเป็นมนุษย์ รัฐธรรมนูญของรัฐเสรีประชาธิปไตยทุกรัฐจึงได้บัญญัติรับรองและให้ความคุ้มครองศักดิ์ศรีความเป็นมนุษย์ของปัจเจกชนไว้อย่างชัดเจน เป็นสิทธิเสรีภาพขั้นพื้นฐาน รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550 มาตรา 4 บัญญัติว่า “ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาคของบุคคลย่อมได้รับความคุ้มครอง” มาตรา 26 บัญญัติว่า “การใช้อำนาจโดยองค์กรของรัฐทุกองค์กร ต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพ ตามบทบัญญัติแห่งรัฐธรรมนูญนี้” และมาตรา 27 บัญญัติว่า “สิทธิและเสรีภาพของบุคคลที่รัฐธรรมนูญรับรองไว้จะกระทำได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อการที่รัฐธรรมนูญนี้กำหนดไว้ และเท่าที่จำเป็นเท่านั้น และจะกระทบกระเทือนต่อสาระสำคัญของสิทธิและเสรีภาพนั้นมิได้” และมาตรา 37 วรรคแรกบัญญัติว่า “บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบด้วยกฎหมาย”¹⁵

จากบทบัญญัติดังกล่าวที่กำหนดขึ้นเพื่อปกป้องสิทธิและเสรีภาพของประชาชน มิให้ถูกล่วงละเมิด แม้กฎหมายจะให้การรับรองเสรีภาพอย่างใดอย่างหนึ่งให้แก่บุคคลใดบุคคลหนึ่ง ย่อมมีผลก่อให้เกิดหน้าที่แก่ผู้อื่นด้วยเช่นกัน แต่หน้าที่ที่เกิดขึ้นกับผู้อื่นอันเนื่องมาจากการที่กฎหมายบัญญัติรับรองเสรีภาพให้แก่บุคคลหนึ่งนี้ เป็นแต่เพียงหน้าที่ที่จะต้องเคารพเสรีภาพของผู้ทรงเสรีภาพ และผู้ทรงเสรีภาพเองก็มีอำนาจตามกฎหมายแต่เพียงที่จะเรียกร้องให้ผู้อื่นละเว้นจากการรบกวนขัดขวางการใช้เสรีภาพของตนเท่านั้น หากได้มีอำนาจ ที่จะเรียกร้องให้ผู้อื่นกระทำการอย่างใดอย่างหนึ่ง ซึ่งมีลักษณะเป็นการส่งเสริมหรือช่วยเหลือการใช้เสรีภาพของตนด้วย

สิทธิและเสรีภาพตามรัฐธรรมนูญนั้นมีผลผูกพันโดยตรงต่ออำนาจนิติบัญญัติ อำนาจบริหาร และอำนาจตุลาการ เพราะอำนาจนิติบัญญัติ อำนาจบริหาร และอำนาจตุลาการ ต่างก็เป็นอำนาจที่มาจากอำนาจอธิปไตย ซึ่งเป็นส่วนหนึ่ง que แสดงออกถึงความเป็นรัฐ นอกจากอาณาเขต และพลเมือง¹⁶

2.2.3 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547

มีบทบัญญัติบางประการ เกี่ยวกับการจำกัดสิทธิ และเสรีภาพของบุคคลซึ่งมาตรา 29 ประกอบกับมาตรา 31 มาตรา 34 มาตรา 35 มาตรา 36 มาตรา 37 มาตรา 48 มาตรา 58 มาตรา 237 และมาตรา 238 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายได้แก่ บทบัญญัติต่อไปนี้

¹⁵ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550

¹⁶ บรรเจิด สิงคะเนติ, **หลักพื้นฐานของสิทธิเสรีภาพ และศักดิ์ศรีความเป็นมนุษย์ตามรัฐธรรมนูญ พ.ศ.2540**, พิมพ์ครั้งที่ 2 (กรุงเทพฯ: วิญญูชน, 2547), หน้า 47.

มาตรา 24 บัญญัติว่าเพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ให้พนักงานสอบสวนคดีพิเศษมีอำนาจดังต่อไปนี้

(1) เข้าไปในเคหสถาน หรือสถานที่ใด ๆ เพื่อตรวจค้น เมื่อมีเหตุสงสัยตามสมควรว่ามี บุคคลที่มีเหตุสงสัยว่ากระทำความผิดที่เป็นคดีพิเศษหลบซ่อนอยู่ หรือมีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้ ประกอบกับมีเหตุอันควรเชื่อว่าเนื่องจากการเน้นซ้ำว่าจะเอาหมายค้นมาได้บุคคลนั้นจะหลบหนีไป หรือทรัพย์สินนั้นจะถูกโยกย้าย ซุกซ่อน ทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิม

(2) ค้นบุคคล หรือยานพาหนะที่มีเหตุสงสัยตามสมควรว่ามีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้

(3) มีหนังสือสอบถามหรือเรียกให้สถาบันการเงิน ส่วนราชการ องค์กร หรือหน่วยงานของรัฐ หรือรัฐวิสาหกิจ ส่งเจ้าหน้าที่ที่เกี่ยวข้องมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(4) มีหนังสือสอบถาม หรือเรียกบุคคลใด ๆ มาเพื่อให้ถ้อยคำใด ๆ ส่งคำชี้แจงเป็นหนังสือหรือส่งบัญชีเอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(5) ยึด หรืออายัดทรัพย์สินที่ค้นพบ หรือที่ส่งมาดังกล่าวไว้ใน (1) (2) (3) และ (4) การใช้อำนาจตามวรรคหนึ่งให้พนักงานสอบสวนคดีพิเศษปฏิบัติปฏิบัติตามข้อบังคับที่ กพค.กำหนดเฉพาะการใช้อำนาจตามวรรคหนึ่ง (1) นอกจากพนักงานสอบสวนคดีพิเศษต้องดำเนินการเกี่ยวกับ วิธีการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญา แล้วให้พนักงานสอบสวนคดีพิเศษแสดง ความบริสุทธิ์ก่อนการเข้าค้น รายงานเหตุผลและผลการตรวจค้นเป็นหนังสือต่อผู้บังคับบัญชาเหนือ ขึ้นไป และบันทึกเหตุสงสัยตามสมควรและเหตุอันควรเชื่อที่ทำให้สามารถเข้าค้นได้เป็นหนังสือให้ไว้แก่ผู้ครอบครองเคหสถานหรือสถานที่ค้นแต่ถ้าไม่มีผู้ครอบครองอยู่ ณ ที่นั้น ให้พนักงานสอบสวนคดีพิเศษส่งมอบสำเนาหนังสือนั้นให้แก่ผู้ครอบครองดังกล่าวในทันทีที่กระทำได้ และหากเป็นการเข้าค้นในเวลากลางคืนภายหลังอาทิตย์ตก พนักงานสอบสวนคดีพิเศษผู้เป็นหัวหน้าในการเข้าค้นต้องเป็นข้าราชการพลเรือนตั้งแต่ระดับ 7 ขึ้นไปด้วยให้พนักงานสอบสวนคดีพิเศษผู้เป็นหัวหน้าในการเข้าค้นส่งสำเนาบันทึกเหตุสงสัยตามสมควรและเหตุอันควรเชื่อตามวรรคสาม และสำเนาบันทึกการตรวจค้น และบัญชีทรัพย์สินที่ยึด หรืออายัดต่อศาลจังหวัดที่มีอำนาจเหนือท้องที่ที่ทำการค้น หรือศาลอาญาในเขตกรุงเทพมหานคร ภายในสี่สิบแปด ชั่วโมงหลังจากสิ้นสุดการตรวจค้นเพื่อเป็นหลักฐาน

พนักงานสอบสวนคดีพิเศษระดับใดจะมีอำนาจหน้าที่ตามที่ได้กำหนดไว้ตามวรรคหนึ่งทั้งหมดหรือแต่บางส่วน หรือจะต้องได้รับอนุมัติจากบุคคลใดก่อนดำเนินการให้เป็นไปตามที่ อธิบดีกำหนดโดยทำเอกสารให้ไว้ประจำตัวพนักงานสอบสวนคดีพิเศษผู้ได้รับอนุมัตินั้นและ พนักงานสอบสวนคดีพิเศษผู้นั้นต้องแสดงเอกสารดังกล่าวต่อบุคคลที่เกี่ยวข้องทุกครั้ง

มาตรา 25 ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการ กระทำความผิดที่เป็นคดีพิเศษพนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือ จะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษ ได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้

การอนุญาตตามวรรคหนึ่งให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

- (1) มีเหตุอันควรเชื่อว่าจะมีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ
- (2) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว
- (3) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกิน 90 วัน โดยกำหนดเงื่อนไขใด ๆ ก็ได้และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่า เหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

มาตรา 26 ห้ามมิให้บุคคลใดเปิดเผยข้อมูลข่าวสารที่ได้มาเนื่องจากการดำเนินการตามมาตรา 25 เว้นแต่เป็นข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษซึ่งได้รับอนุญาตตามมาตรา 25 และเป็นการปฏิบัติตามอำนาจหน้าที่หรือตามกฎหมายหรือตามคำสั่งศาล

จะเห็นได้ว่าอำนาจที่กฎหมายมอบให้กับพนักงานสอบสวนคดีพิเศษตามบทบัญญัติข้างต้นเป็นการกระทำที่กระทบต่อสิทธิเสรีภาพของประชาชน และจะทำให้เกิดการใช้อำนาจที่ไร้ ขอบเขต และประเทศไทยเองก็ยังไม่มียกเว้นของกฎหมายที่ให้การคุ้มครองสิทธิในชีวิตส่วนตัวของบุคคลโดยตรง แต่หากพิจารณาบทกฎหมายที่มีในปัจจุบันแล้วจะพบว่ากฎหมายที่ให้ความคุ้มครองสิทธิส่วนบุคคลมีมากมายพอสมควร โดยเฉพาะที่ปรากฏอยู่ในประมวลกฎหมายอาญาใน ความผิด

ฐานหมิ่นประมาท ความผิดฐานดูหมิ่น ความผิดฐานบุกรุก และความผิดฐานก่อความเดือดร้อนรำคาญเท่านั้น ในประมวลกฎหมายแพ่ง และพาณิชย์ ก็มีอยู่ในมาตรา 420 ซึ่งบัญญัติว่า “ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิด จำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น”¹⁷

ดังที่กล่าวมาแล้วจะเห็นได้ว่าบทบัญญัติรัฐธรรมนูญ ล้วนแฝงไว้ด้วยสิทธิในชีวิตส่วนบุคคลแทบทั้งสิ้น จึงไม่อาจปฏิเสธได้ว่าสิทธิส่วนบุคคลเป็นสิทธิประการหนึ่ง ซึ่งย่อมได้รับการรับรองโดยกฎหมายโดยชอบ หากผู้ใดละเมิดก็จะมีผิด และเมื่อพิจารณาถึงจุดสมดุระหว่างแนวคิดในเรื่องปัจเจกชนนิยม กับผลประโยชน์ของรัฐหรือสาธารณะ จึงจำเป็นต้องมีกฎหมายวิธีพิจารณาความอาญาที่สามารถรองรับการปฏิบัติหน้าที่ของพนักงานสอบสวน สามารถรักษาสมดุระหว่างอำนาจรัฐในการนำตัวผู้กระทำความผิดมาลงโทษ และหลักประกันสิทธิเสรีภาพของประชาชน การรวบรวมพยานหลักฐานอิเล็กทรอนิกส์อาจจะล่วงละเมิดความเป็นส่วนตัวของบุคคลแต่ควรกระทำได้เท่าที่จำเป็นและมีเหตุผล

2.2.4 กฎหมายวิธีพิจารณาความอาญา

บทบัญญัติสำคัญของกฎหมายวิธีพิจารณาความอาญาบัญญัติไว้เพื่อความสะดวกในการใช้อำนาจหน้าที่ของเจ้าพนักงานของรัฐ แนวทางการปฏิบัติหน้าที่ โดยคำนึงถึงสิทธิเสรีภาพส่วนบุคคล แต่จะเป็นส่วนน้อย ส่วนมากจะบัญญัติไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย ซึ่งในปัจจุบันรัฐให้ความสำคัญคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานของประชาชนเป็นสำคัญ การปฏิบัติหน้าที่จึงอยู่ภายใต้ของกฎหมาย

1. สถานะผู้กล่าวหา บทบัญญัติที่ให้ความสำคัญต่อสิทธิเสรีภาพส่วนบุคคลของผู้กล่าวหาได้แก่ มาตรา 165 วรรคสาม บัญญัติว่า “ก่อนที่ศาลประทับฟ้องมิให้ถือว่าจำเลยอยู่ในฐานะเช่นนั้น นั่นคือก่อนที่ผู้ที่ถูกผู้เสียหายฟ้อง ถูกศาลประทับฟ้องยังไม่ถือเป็น “จำเลย” ผู้ถูกกล่าวหาในปัจจุบันจึงไม่ถือเป็นวัตถุแห่งการซักพอรหรือเป็น “กรรมในคดี” (Prozess-objekt) อีกต่อ แต่เป็น “ประธานในคดี” (Prozess-subjekt) ซึ่งสอดคล้องกับบทบัญญัติในรัฐธรรมนูญ มาตรา 40 (7) บัญญัติว่า “ในคดีอาญาผู้ต้องหาหรือจำเลยมีสิทธิได้รับการสอบสวนหรือการพิจารณาคดีที่ถูกต้องรวดเร็วและเป็นธรรม การตรวจสอบหรือได้รับทราบพยานหลักฐานตามสมควร การได้รับความช่วยเหลือในทางคดีจากทนายความ และการได้รับการปล่อยตัวชั่วคราว”¹⁸

2. สิทธิของผู้ถูกกล่าวหา สิทธิของผู้ต้องหาที่จะไม่ให้เป็นสิทธิของผู้ถูกกล่าวหาในทางอยู่เฉย ซึ่งเป็นสิทธิที่จะตัดสินใจในคดีด้วยตนเอง ในมาตรา 134 บัญญัติว่า “เมื่อผู้ต้องหาเต็มใจให้การอย่างไร ก็ให้จดคำให้การไว้ ถ้าผู้ต้องหาไม่เต็มใจให้การเลยก็ให้บันทึกไว้” และในชั้นศาล มาตรา 174

¹⁷ พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547

¹⁸ คณิต ณ นคร, *เรื่องเดิม*, หน้า 31.

บัญญัติว่า “ถ้าจำเลยไม่ยอมให้การ ก็ให้ศาลจดรายงานไว้และพิจารณาต่อไป” และเพื่อประกันสิทธิในการให้การหรือไม่ให้การของจำเลย มาตรา 135 บัญญัติว่า “ห้ามมิให้พนักงานสอบสวนทำหรือจัดให้ทำการใด ๆ ซึ่งเป็นการล่อลวง หรือขู่เข็ญ หรือให้สัญญากับผู้ต้องหาเพื่อจงใจให้เขาให้การอย่างใด ๆ ซึ่งเป็นการล่อลวง หรือขู่เข็ญ หรือให้สัญญากับผู้ต้องหาเพื่อจงใจให้เขาให้การอย่างใด ๆ ในเรื่องที่ต้องหานั้น” การล่อลวง หรือขู่เข็ญ หรือให้สัญญา ซึ่งเป็นการกระทำที่มีขอบด้วยกฎหมายตามที่บัญญัติไว้ในมาตรา 135 นั้น เป็นเพียงการกระทำความผิดที่กฎหมายบัญญัติไว้เท่านั้นแต่ความหมายที่บทบัญญัติในมาตรานี้ต้องการแสดงให้ปรากฏก็คือ “การกระทำที่เป็นการละเมิดเสรีภาพในการตัดสินใจของผู้ต้องหา” ทุกสถาน¹⁹

บทบัญญัติที่ถือว่าขัดแย้งกันกับบทบัญญัติที่ให้ความคุ้มครองสิทธิของผู้ถูกกล่าวหาในทางอยู่เฉยได้แก่ มาตรา 132 บัญญัติว่า “เพื่อประโยชน์แห่งการรวบรวมพยานหลักฐาน พนักงานสอบสวนมีอำนาจตรวจค้นผู้ต้องหา จำเลยพิมพ์ลายนิ้ว ลายมือหรือลายเท้า” เป็นบทบัญญัติ ที่แสดงให้เห็นถึงอำนาจของรัฐในการแสวงหาพยานหลักฐานจากผู้ต้องหา หรือเพื่อประโยชน์ในการรวบรวมพยานหลักฐาน โดยไม่จำเป็นต้องได้รับความยินยอมจากผู้ต้องหา หรือจำเลยดังกล่าว เพียงแต่การตรวจค้นนั้น

มาตรา 85 วรรคหนึ่ง บัญญัติว่า “เจ้าพนักงานผู้จับหรือรับจับไว้ ตัวผู้ต้องหา” และวรรคสองบัญญัติว่า “การค้น นั้นโดยสุภาพ ถ้าค้นตัวผู้ต้องหาต้องให้หญิงอื่นเป็นผู้ค้น” ซึ่งแสดงถึงความเคารพสถานะความเป็นประธานในคดีของผู้ต้องหา²⁰

3. สถานะของผู้ต้องหา มาตรา 2 (2) นิยามคำว่า “ผู้ต้องหา” หมายความว่า บุคคลผู้ถูกหาว่าได้กระทำความผิด แต่ยังมีได้ถูกฟ้องต่อศาล จากคำนิยาม บุคคลที่จะมีสถานะเป็นผู้ต้องหาตามกฎหมายจึงต้องเป็นบุคคลที่มีผู้กล่าวหาบุคคลนั้นว่าได้กระทำความผิดอาญาต่อเจ้าพนักงาน หรือเจ้าพนักงานกล่าวหาเองในการกล่าวหาต่อเจ้าพนักงาน มาตรา 2 (7) อาจทำในรูปของคำร้องทุกข์ของผู้เสียหายหรือตามมาตรา 2 (8) คำกล่าวโทษโดยบุคคลอื่น

4. สถานะของจำเลย มาตรา 2 (3) นิยามคำว่า “จำเลย” หมายความว่า บุคคลซึ่งถูกฟ้องยังศาลแล้วโดยข้อหาหาได้กระทำความผิด ดังนั้นจะถือว่าบุคคลซึ่งถูกฟ้องยังศาลแล้วเป็นจำเลยในทันทีที่ยื่นฟ้องจะต้องพิจารณาจากผู้ฟ้องเป็นหลัก หากพนักงานอัยการเป็นผู้ฟ้อง ผู้ถูกฟ้องจะตกเป็นจำเลยทันทีโดยไม่ต้องมีการ ไต่สวนมูลฟ้องก่อนหรือไม่ แต่ในกรณีที่ผู้เสียหายเป็นผู้ฟ้อง มาตรา 165 วรรคสามตอนท้าย บัญญัติว่า “ก่อนที่ศาลจะประทับฟ้องมิให้ถือว่าจำเลยอยู่ในฐานะเช่นนั้น” ดังนั้นก่อนศาลประทับฟ้องผู้ถูกฟ้องจึงยังไม่ตกเป็นจำเลย²¹

5. การแสวงหาพยานหลักฐาน พยานหลักฐานเป็นเครื่องมือประการหนึ่งในการดำเนินคดีอาญาที่มีความสำคัญมาก ซึ่งในคดีอาญาพยานหลักฐานทุกชนิดรับฟังได้ ดังจะเห็นได้จาก มาตรา 226 บัญญัติว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพินิจได้ว่าจำเลยมีผิด หรือ

¹⁹ เรื่องเดียวกัน, หน้า 102.

²⁰ เรื่องเดียวกัน, หน้า 105.

²¹ มาตรา 2(3) แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

บริสุทธิ์ใช้อ้างเป็นพยานหลักฐานได้แต่ต้องเป็นพยานหลักฐานชนิดที่มีได้เกิดจากแรงจูงใจ มี คำมั่นสัญญา ชูเชิญ หลอกลวง หรือโดยมิชอบด้วยประการอื่น และให้สืบตามบทบัญญัติแห่ง ประมวลกฎหมายนี้ หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน”²²

การดำเนินคดีอาญา ได้แก่ การสืบสวนและการสอบสวน ซึ่งบทบัญญัติดังกล่าวถือเป็นหลักเบื้องต้นทั่วไปเกี่ยวกับพยานหลักฐานที่แสดงสถานะและความเป็นอิสระในการแสวงหาพยานหลักฐาน แต่สำหรับปัญหาอาชญากรรมทางอิเล็กทรอนิกส์ที่มีอยู่ในปัจจุบัน เพื่อให้การบังคับใช้กฎหมายป้องกันและปราบปรามอาชญากรรมนี้ให้มีประสิทธิภาพมากขึ้น จึงควรแสวงหามาตรการทางกฎหมายที่จะมารองรับการปฏิบัติหน้าของพนักงานสอบสวนในการเข้าถึงพยานหลักฐานอิเล็กทรอนิกส์ แต่ในขณะเดียวกันก็ต้องคำนึงถึงสิทธิขั้นพื้นฐานของประชาชนเป็นสำคัญ

เนื่องจากกระบวนการสอบสวนตามประมวลกฎหมายวิธีพิจารณาในปัจจุบัน ยังไม่สามารถแก้ไขปัญหาความบกพร่องของการรวบรวมพยานหลักฐานในคดีที่เกี่ยวข้องกับอาชญากรรมทางอิเล็กทรอนิกส์ ได้รวมทั้งการบริหารจัดการระบบงานสอบสวนของพนักงานสอบสวนที่มีอยู่เดิม อาชญากรรมมีความเชี่ยวชาญในการใช้เทคโนโลยีระดับสูงในการประกอบอาชญากรรมในขณะเดียวกันก็ใช้ความรู้ความเชี่ยวชาญนี้ ปกปิดซ่อนเร้นทำลายพยานหลักฐาน เพื่อการแสวงหาพยานหลักฐาน และนำตัวผู้กระทำความผิดมาลงโทษให้ได้ โดยอำนาจหน้าที่หลักของพนักงานสอบสวน ตามมาตรา 2 (6) นิยามว่า “พนักงานสอบสวน หมายความว่า เจ้าพนักงานซึ่งกฎหมายให้อำนาจและหน้าที่ทำการสอบสวน”²³ และมาตรา 121 วรรคหนึ่ง บัญญัติว่า “พนักงานสอบสวนมีอำนาจสอบสวนคดีอาญาทั้งปวง”²⁴ ซึ่งเป็นบทบัญญัติถึงอำนาจในการสอบสวนของพนักงานสอบสวน

2.3 การแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญา

การดำเนินคดีกับผู้กระทำความผิดนั้นไม่ว่าประเทศใดในโลกและความแตกต่างของระบบกฎหมายใดต่างก็จะค้นหาความจริงโดยมีข้อสันนิษฐานตามกฎหมายว่า จำเลยเป็นผู้บริสุทธิ์ เพียงแต่วิธีการค้นหาความจริงอาจแตกต่างกันออกไปตามสภาพสังคม แต่จุดประสงค์หลักก็เพื่อค้นหาข้อเท็จจริงในคดีอาญาของพนักงานสอบสวน จึงจำเป็นต้องรวบรวมพยานหลักฐานทุกชนิดเท่าที่จะสามารถรวบรวมได้ เพื่อจะทราบข้อเท็จจริงและพฤติการณ์ต่าง ๆ อันเกี่ยวข้องกับการกระทำความผิดที่ถูกกล่าวหาและเพื่อรู้ตัวผู้กระทำความผิดและพิสูจน์ให้เห็นความผิด เพื่อประโยชน์แห่งการรวบรวมหลักฐานให้พนักงานสอบสวนมีอำนาจตามกฎหมาย ตามบทบัญญัติประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 บัญญัติว่า “อำนาจตรวจตัวผู้เสียหาย เมื่อผู้เสียหายยินยอม ตรวจตัวผู้ต้องหา การตรวจตัวผู้เสียหายหรือตรวจตัวผู้ต้องหา หากผู้เสียหายหรือผู้ต้องหาเป็นหญิงให้จัดให้

²² มาตรา 226 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

²³ มาตรา 2(6) แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

²⁴ มาตรา 121 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

เจ้าพนักงานซึ่งเป็นหญิงหรือให้หญิงอื่นเป็นผู้ตรวจ ในการตรวจค้นผู้เสียหายหรือผู้ต้องหาจะขอ นำบุคคลใดมาอยู่ร่วมในการตรวจก็ได้ การตรวจสิ่งของหรือที่ทางอันสามารถใช้เป็นพยานหลักฐานได้ ทำ ภาพถ่าย แผนที่ หรือภาพวาด จำลองหรือพิมพ์ลายนิ้วมือ ลายมือ หรือลายเท้า บันทึกรายละเอียด ทั้งหลาย ซึ่งน่าจะทำให้คดีมีความกระจ่างชัดขึ้น”²⁵

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550 มาตรา 33 วรรคสาม บัญญัติว่า “การเข้าไป ในเคหสถาน โดยปราศจากการยินยอมของผู้ครอบครองหรือการตรวจค้นเคหสถานจะกระทำมิได้ เว้น แต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย”²⁶

ดังนั้น การใช้อำนาจค้นเพื่อพบสิ่งของซึ่งมีไว้เป็นความผิดหรือสิ่งของซึ่งได้มาจากการกระทำ ความผิดหรือได้ใช้หรือสงสัยว่าได้ใช้ในการกระทำความผิดหรือซึ่งอาจใช้เป็นพยานหลักฐานได้ โดย พนักงานสอบสวนจะต้องปฏิบัติตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาว่าด้วย การค้นกฎหมายไทยให้ความคุ้มครองแก่ประชาชนในการครอบครองสิ่งหาทรัพย์สินโดยปกติสุข ปราศจากการรบกวน แม้จากเจ้าหน้าที่ของรัฐเองจะเข้าไปรบกวนการครอบครองดังกล่าวจะต้องมี กฎหมายให้อำนาจไว้อย่างชัดแจ้ง

2.3.1 การค้นพยานหลักฐานอิเล็กทรอนิกส์

การค้นเป็นมาตรการบังคับ (Zwangsmassnahme หรือ Compulsory measures) ซึ่งเป็น เครื่องมือในการดำเนินคดีอาญาที่สำคัญและจำเป็นต้องมีหากขาดไปการดำเนินคดีอาญาก็ย่อมไม่อาจ กระทำได้โดย²⁷ กำหนดให้เจ้าพนักงานของรัฐ 2 ประเภทเป็นผู้ดำเนินการค้น ได้แก่ พนักงานฝ่าย ปกครองและเจ้าพนักงานตำรวจหรือพนักงานสอบสวน ประชาชนทั่วไปไม่สามารถค้นได้ไม่ว่ากรณีใด ก็ตาม และมีเหตุในการออกหมายค้นได้ตามมาตรา 69 (1)-(5) การค้นจึงเป็นการดำเนินการของเจ้า พนักงานของรัฐที่กฎหมายอนุญาตให้เข้าไปแสวงหาพยานหลักฐานได้ตามสถานที่ต่าง ๆ หรือจาก ตัวบุคคลก็ย่อมกระทำได้ เมื่อการค้นเป็นการแสวงหาพยานหลักฐานจากสถานที่ต่าง ๆ หรือจากตัว บุคคล การค้นของเจ้าพนักงานย่อมเป็นการกระทำที่กระทบกระเทือนต่อสิทธิส่วนบุคคล²⁸ เสรีภาพใน เคหสถาน และสิทธิเสรีภาพในชีวิต และร่างกาย กรณีที่พยานหลักฐานที่เจ้าพนักงานของรัฐแสวงหา มิใช่พยานวัตถุ พยาน เอกสารหรือพยานบุคคล เช่น ข้อมูลมูลอิเล็กทรอนิกส์ ซึ่งกฎหมายไทยมิได้มี การจัดเอาไว้ว่า เป็นพยานหลักฐานประเภทใด และยังมีการโต้แย้งกันอยู่ว่าจะเป็นพยานเอกสาร หรือพยานวัตถุพิจารณาจากการแสวงหาพยานหลักฐานดังกล่าวแล้วอาจทำได้ 2 วิธี ได้แก่

²⁵ มาตรา 132 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

²⁶ มาตรา 33 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550

²⁷ คณิต ญ นคร, *เรื่องเดียวกัน*, หน้า 190.

²⁸ คณิง ภาไชย, *กฎหมายวิธีพิจารณาความอาญา เล่ม 1. พิมพ์ครั้งที่ 6* (กรุงเทพฯ: ม.ป.พ., 2540), หน้า 252.

1. เป็นข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ส่วนบุคคลของบุคคลใดบุคคลหนึ่ง ไม่ว่าจะอยู่ที่ใดที่พนักงานของรัฐไม่สามารถใช้เครื่องมือใด ๆ เชื่อมเข้าไปในเครื่องคอมพิวเตอร์เพื่อเรียกดูข้อมูลที่ถูกจัดเก็บไว้ในฮาร์ดดิสก์ได้นอกจากเข้าไปค้นในที่ที่เครื่องคอมพิวเตอร์ นั้นอยู่ ซึ่งก็เป็นการบุกรุกเข้าไปในเคหสถานของผู้เป็นเจ้าของ จึงจะได้ข้อมูลที่เป็นพยานหลักฐานมา และ

2. เป็นการจัดเก็บข้อมูลในรูปของเครือข่าย เช่น เครือข่ายในระบบ LAN (Local Area Network) เป็นระบบเครือข่ายท้องถิ่นภายในอาคารเดียวกัน หรือระบบ WAN (Wide Area Network) เป็นเครือข่ายระยะไกล จำกัดเฉพาะกลุ่ม เช่น ระบบธนาคารเฉพาะกลุ่มธนาคารและรวมถึงระบบอินเทอร์เน็ต ซึ่งเจ้าพนักงานของรัฐไม่จำเป็นต้องเข้าไปในที่รโหฐานเพื่อค้นหาพยานหลักฐาน แต่อาจใช้เครื่องมือหรือเครื่องคอมพิวเตอร์อีกเครื่องเชื่อมไปที่แม่ข่าย หรือเซิร์ฟเวอร์ (Server) เพื่อเรียกข้อมูลมาตรวจดูก็ได้

2.3.1.1 การค้นพยานหลักฐานอิเล็กทรอนิกส์ที่อยู่ในที่รโหฐาน

ตามคำนิยามของคำว่า “รโหฐาน” ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (13) หมายถึงสถานที่ใด ๆ ซึ่งประชาชนไม่มีความชอบธรรมที่จะเข้าไปได้ หรือเป็นที่ส่วนตัว” (Private Place) ที่แสดงถึงเจตนาหวงกันของเจ้าของหรือผู้ครอบครอง การคุ้มครองเสรีภาพในเคหสถานของบุคคลตามการคุ้มครองเสรีภาพในเคหสถานของบุคคลตามรัฐธรรมนูญ มาตรา 33 การที่เจ้าพนักงานของรัฐเข้าไปค้นหาข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งอยู่ในที่รโหฐานได้จะต้องเป็นกรณีที่มีกฎหมายบัญญัติไว้ และจะต้องมีหมายค้น ดังที่บัญญัติไว้ตามรัฐธรรมนูญ มาตรา 33 วรรคสาม ซึ่งจะต้องมีเหตุในการออกหมายค้น ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 69 เว้นแต่เป็นกรณีกฎหมายบัญญัติให้มีการค้นได้โดยไม่ต้องมีหมาย

ตามมาตรา 92 หากเจ้าพนักงานของรัฐการตรวจค้นโดยไม่ต้องมีหมาย และไม่ต้องเข้ากรณียกเว้น การค้นดังกล่าวก็เป็นการค้นที่มีขอบเขตให้ศาลไม่สามารถรับฟังเป็นพยานหลักฐานได้ การค้นข้อมูลอิเล็กทรอนิกส์ที่เก็บไว้ในที่รโหฐานต้องมีหมายค้น กล่าวอีกนัยหนึ่งก็คือ การค้นในที่ค้นในที่รโหฐานจะกระทำมิได้เว้นแต่มีคำสั่งหรือหมายของศาลเพื่อให้การค้นชอบด้วยกฎหมายสิ่งนี้แสดงให้เห็นว่ารัฐธรรมนูญฉบับปัจจุบันต้องการให้หลักประกันในความคุ้มครองความเป็นส่วนตัวและสิทธิส่วนบุคคลของประชาชน

การตรวจค้นในที่รโหฐานเพื่อค้นคนหาพยานหลักฐานอิเล็กทรอนิกส์ในเครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์ที่เชื่อมโยงเครือข่ายในเคหสถานเดียวกันของผู้ต้องสงสัยซึ่งเป็น “สิ่งของที่ใช้ในการกระทำความผิด” เพื่อค้นหาข้อมูลอิเล็กทรอนิกส์ซึ่งเป็นพยานหลักฐานแสดงการกระทำ ความผิดของผู้ต้องสงสัย เจ้าพนักงานของรัฐจำเป็นต้องมีหมายค้นจากศาลในการรวบรวมพยานหลักฐาน²⁹ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132

พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งสามารถทำลายแก้ไขได้ง่ายโดยใช้เวลาเพียงสั้น ๆ แต่การออกหมายค้นจากศาลต้องใช้เวลาพอสมควร หากผู้กระทำความผิดทราบเหตุว่าจะถูกค้นก็สามารถทำลายหรือแก้ไขเปลี่ยนแปลงได้ง่ายดาย แม้กรณีเร่งด่วนอ้างเป็นข้อยกเว้นตาม

²⁹ มาตรา 132 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92 และใช้อำนาจตามมาตรา 92 วรรคสอง ซึ่งน่าจะนำมาเป็นเหตุยกเว้นได้ เพราะหลักการค้นจะต้องมีหมาย สำหรับการค้นตามมาตรา 92 เป็นการค้นในกรณีพิเศษจึงต้องมีกฎหมายบัญญัติเอาไว้อย่างชัดแจ้งประกอบคำวินิจฉัยของคณะกรรมการกฤษฎีกาที่ นร. 0601/6182 ให้ความเห็นว่าบทบัญญัติมาตรา 92 วรรคสอง แห่งประมวลกฎหมายวิธีพิจารณาความอาญาในส่วนที่บัญญัติให้พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ค้นด้วยตนเองโดยไม่ต้องมีหมายค้น ถ้าขัดต่อบทบัญญัติของรัฐธรรมนูญแห่งราชอาณาจักรไทยเป็นอันบังคับใช้ไม่ได้³⁰

กรณีที่เจ้าพนักงานของรัฐเข้าค้นข้อมูลอิเล็กทรอนิกส์ได้โดยไม่ต้องเข้าไปในที่รโหฐานแต่ใช้เครื่องคอมพิวเตอร์เชื่อมจากภายนอกไม่ว่าจะเป็นระบบ LAN WAN หรือ อินเทอร์เน็ต ลักษณะไม่เป็นการบุกรุกตามประมวลกฎหมายอาญาเพราะไม่ได้เข้าไปยังเคสสถานของผู้อื่นแต่เป็นการละเมิดสิทธิส่วนบุคคลตามรัฐธรรมนูญ มาตรา 34 โดยถือว่าเป็นการค้นเช่นกัน การใช้อำนาจของเจ้าพนักงานของรัฐ ย่อมจะต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของประชาชน ตาม ดังที่บัญญัติไว้ในรัฐธรรมนูญมาตรา 26

2.3.1.2 การยึดและการเก็บรักษาพยานหลักฐานอิเล็กทรอนิกส์

ด้วยความก้าวหน้าของเทคโนโลยี ทุกองค์กรต้องพึ่งพาเทคโนโลยีเพื่อให้ทันต่อโลกที่ก้าวหน้าไปสู่ยุคเทคโนโลยีสารสนเทศ จากเดิมที่มนุษย์ใช้การสื่อสารโดยใช้ภาษาและตัวอักษรเป็นหลักในการศึกษามาเป็นการสื่อสารด้วยภาษาอิเล็กทรอนิกส์ซึ่งมีประสิทธิภาพในการประมวลผลสื่ออิเล็กทรอนิกส์จึงถือเป็นพยานหลักฐานได้ในการพิจารณาคดี นอกเหนือจากพยานวัตถุ พยานเอกสาร หรือพยานบุคคล และพยานนิติวิทยาศาสตร์ ซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ถึงแม้ว่าข้อมูลอิเล็กทรอนิกส์จะมีลักษณะเป็นพยานเอกสารและพยานวัตถุ แต่ก็มีแตกต่างจากพยานทั่ว ๆ ไปในการนำสืบ จึงต้องอาศัยวิธีการพิเศษในการจัดทำ

พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานที่ไม่มีรูปร่างซึ่งจะทำการยึดอย่างเช่นพยานหลักฐานทั่วไปตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 101 ไม่ได้ โดยลักษณะของข้อมูลอิเล็กทรอนิกส์ การยึดสามารถกระทำได้โดยการยึดเครื่องคอมพิวเตอร์หรือเครื่องอิเล็กทรอนิกส์ที่มีข้อมูลนั้น หรือการนำฮาร์ดดิสก์ที่มีข้อมูลนั้นเสนอต่อศาล³¹ จะเห็นได้ว่าการตรวจค้น และการยึดพยานหลักฐานอิเล็กทรอนิกส์ เพื่อนำมาเป็นพยานหลักฐานในอาชญากรรมทางอิเล็กทรอนิกส์นั้น ไม่อาจกระทำได้หากไม่มีหมายค้น และในบางกรณีทำให้ไม่สามารถทำได้อย่างทันทั่วทั้งที่ จึงเป็นปัญหาในเรื่องของอำนาจหน้าที่ของพนักงานสอบสวนที่ยังไม่มีกฎหมายให้อำนาจเอาไว้เป็นเฉพาะการดำเนินการตามประมวลกฎหมายวิธีพิจารณาความอาญาจึงยังไม่เพียงพอกับสังคมในปัจจุบัน

³⁰ “คำวินิจฉัยของคณะกรรมการกฤษฎีกาตามหนังสือสำนักงานคณะกรรมการกฤษฎีกาที่ นร.0601/618 (2542),” วารสารอัยการนิเทศ 61, 1: 183-194.

³¹ มาตรา 101 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

ดังที่ได้กล่าวมาแล้วข้างต้น รูปแบบการรวบรวมพยานหลักฐานเหมือนกับคดีอาญาโดยทั่วไป แต่ในปัจจุบันอาชญากรรมทางคอมพิวเตอร์ได้เกิดขึ้นมากมายและไม่สามารถควบคุมได้ ทำให้เจ้าหน้าที่ตำรวจจำเป็นต้องหาวิธีการ และรูปแบบ การรวบรวมพยานหลักฐานใหม่ ๆ เข้ามาใช้เพื่อทำการ แสวงหาพยานหลักฐาน ซึ่งในที่นี้จะกล่าวถึงวิธีและรูปแบบในการรวบรวมพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ต่อไป ดังนั้น การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN WAN หรือ อินเทอร์เน็ตแม้ในปัจจุบันประเทศไทย ยังไม่มีกฎหมายบัญญัติไว้โดยเฉพาะ แต่เมื่อพิจารณาถึงสิ่งที่กฎหมายประสงค์จะให้ความคุ้มครองนั้นคือ สิทธิส่วนบุคคล การค้นจึงต้องมีหมายค้น เช่นเดียวกับการค้นโดยทั่วไป หากเป็นการค้นโดยไม่มีหมายค้น ถือว่าพยานหลักฐานที่ได้เป็นพยานหลักฐานที่ได้มาโดยมิชอบเช่นกัน และศาลก็ไม่สามารถนำมาใช้ประกอบการพิจารณาได้

2.3.2 รูปแบบและการวางแผนในการตรวจค้น (Search Planning)

ต้องมีการวางแผนในการตรวจค้นซึ่งเป็นสิ่งจำเป็นในคดีอาชญากรรมคอมพิวเตอร์ การวางแผน ที่ดีจะทำการทำงานบรรลุเป้าหมายในการรวบรวมพยานหลักฐาน เนื่องจากการรวบรวมพยานหลักฐานที่ข้อมูลคอมพิวเตอร์แล้วต้องใช้วิธีพิเศษโดยเฉพาะในการตรวจค้นประการแรกที่จะต้อง พิจารณาในการวางแผนคือ ต้องทราบรูปแบบของอาชญากรรมคอมพิวเตอร์ว่าเป็นรูปแบบของ อาชญากรรมที่เกี่ยวข้องกับฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) หรือการสื่อสารโทรคมนาคม (Telecommunication) ซึ่งอาจแยกพิจารณาได้ ดังนี้³²

2.3.2.1 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับฮาร์ดแวร์ (Hardware)

หากเป็นอาชญากรรมคอมพิวเตอร์ที่เกี่ยวข้องกับฮาร์ดแวร์ จะต้องพิจารณารวบรวมเป็นฮาร์ดแวร์คอมพิวเตอร์ขนาดใหญ่ เช่น เป็นฮาร์ดแวร์ ไมโครคอมพิวเตอร์ มินิคอมพิวเตอร์ เมนเฟรมคอมพิวเตอร์หรือ ซูเปอร์คอมพิวเตอร์ โดยเฉพาะเครื่องขนาดใหญ่ หากทราบถึง ข้อมูลถึงระบบปฏิบัติการ (OS) โปรแกรมของตัวแทนจำหน่ายหรือ บริษัทผู้ผลิตย่อมเป็นประโยชน์ต่อการตรวจค้นเป็นอย่างระบบ โปรแกรมเมอร์ หรือวิศวกรของบริษัทผู้ผลิตเข้าร่วมดำเนินการในการแก้ไขมาก เพราะคอมพิวเตอร์ขนาดใหญ่ไม่สามารถตรวจยึดเข้าไปสู่ห้องปฏิบัติการได้ การวางแผนและการตรวจค้นจึงต้องมีนักวิเคราะห์ปัญหาและอุปสรรคของการตรวจค้นด้วย

2.3.2.2 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับซอฟต์แวร์ (Software)

อาชญากรรมที่เกี่ยวข้องกับซอฟต์แวร์จะต้องพิจารณาว่าเป็นการกระทำความผิดในลักษณะใด เช่น การละเมิดลิขสิทธิ์ (Copyright) ซอฟต์แวร์หรือการใช้ซอฟต์แวร์ เพื่อประกอบอาชญากรรมโดยตรง (Criminal Tools) เช่น การถอดรหัสผ่าน (Password) การคัดลอกข้อมูล ในการเข้าตรวจค้นซอฟต์แวร์เป้าหมายจะต้องมี โปรแกรมเมอร์ของบริษัทผู้ผลิต เข้าร่วมดำเนินการด้วย

³² สุรพันธ์ มั่งคั่งดี, พยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ (วิทยานิพนธ์ปริญญา มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2541), หน้า 66.

2.3.2.3 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับการสื่อสารโทรคมนาคม (Telecommunication)

อาชญากรรมคอมพิวเตอร์อาศัยระบบการสื่อสารโทรคมนาคมจึงต้องพิจารณาว่าการทำงานของเครื่องคอมพิวเตอร์เป็นการทำงานแบบอิสระ (Stand Alone) หรือ เป็นคอมพิวเตอร์ที่เชื่อมกับระบบเครือข่าย เช่น ระบบ LAN (Local Area Network) ระบบ WAN (Wide Area Network) ระบบอินเทอร์เน็ต (Internet) การวางแผนในการ ตรวจค้นจึงต้องมีการเตรียมการในการตรวจค้นระบบเครือข่ายด้วย เช่น การหา ข้อมูลเกี่ยวกับผู้ให้บริการ (ISP) ข้อมูลที่ใช้ในการเชื่อมต่อระบบ เช่น ชื่อผู้ใช้ (User Name) รหัสผ่าน (Password) หมายเลขโทรศัพท์ของ ISP ชื่อเครื่องบริการของ ISP และหมายเลขเครื่อง (IP Address) และชุดโปรแกรมติดตั้งพร้อมคู่มือ³³

วัตถุประสงค์ของการทราบรูปแบบอาชญากรรมก็เพื่อที่จะได้มีข้อมูลในการ ดำเนินการ ขอหมายค้นต่อศาล การเตรียมบุคลากรและเครื่องมือต่าง ๆ และวิธีการรวบรวมพยานหลักฐานในขั้นตอนต่อไป

2.4 การรับฟังพยานหลักฐานอิเล็กทรอนิกส์

เนื่องจากพยานหลักฐานประเภทนี้หากจัดการไม่ถูกต้องจะทำให้พยานหลักฐานหรือของกลางนั้น ๆ อาจนำมาสู่การสันนิษฐานหรือลงความเห็นที่ผิดพลาด หากไม่สามารถทำให้พยานหลักฐานเกิดความน่าเชื่อถือได้ ก็จะไม่สามารถรับฟังเป็นพยานหลักฐานทางคดีได้ การรับฟังพยานหลักฐานอิเล็กทรอนิกส์นั้นมีหลักการที่ใช้ในการพิจารณาพยานหลักฐานอิเล็กทรอนิกส์นั้นสามารถยืนยันความแท้จริง (Authentication) ได้อย่างเหมาะสมหรือไม่ ซึ่งได้แก่ เนื้อหาของเอกสารไม่เปลี่ยนแปลง ข้อมูลในเอกสารเป็นไปตามเจตนาที่แท้จริงของผู้สร้างเอกสารนั้น ทั้งนี้ไม่ว่าผู้สร้างเอกสารจะเป็นมนุษย์ หรือคอมพิวเตอร์ ข้อมูลพิเศษในเอกสาร อันได้แก่ วันเดือนปีที่ถูกสร้าง นั้นถูกต้อง

การเสนอพยานหลักฐานต่อศาลในกรณีข้อมูลเป็นข้อมูลจากสื่ออิเล็กทรอนิกส์หรือมีการบันทึกบนสื่ออิเล็กทรอนิกส์ ซึ่งความจริงแล้วสื่ออิเล็กทรอนิกส์มิได้จำกัดเฉพาะคอมพิวเตอร์เท่านั้น เพราะมีการบันทึกข้อมูลในสื่ออื่น ๆ มาแล้ว เช่น กล้องถ่ายรูป กล้องถ่ายภาพยนตร์ วีดิทัศน์ फिल्म เครื่องบันทึกเสียง ซึ่งนับได้ว่าเป็นวัตถุพยาน แต่สื่ออิเล็กทรอนิกส์คอมพิวเตอร์มีลักษณะพิเศษและยังมีประสิทธิภาพมากกว่าเดิม เพราะการเดินทางของสื่ออื่นนั้นไม่มีขอบเขตจำกัด ไร้พรมแดนและมีผลในทันที นอกจากนี้ยังมีประสิทธิภาพในการประมวลผลโดยเฉพาะในทางคณิตศาสตร์และทางวิทยาศาสตร์อื่น ๆ โดยสามารถแสดงคำตอบและผลลัพธ์ออกมาซึ่งอาจค้นดูได้ และอ่านได้เป็นภาษามนุษย์ได้ด้วย

³³ พรเพชร วิชิตชลชัย, “การรับฟังข้อมูลคอมพิวเตอร์จากสื่ออิเล็กทรอนิกส์เป็นพยานหลักฐาน: ปัญหาและข้อเสนอแนะ,” *ตุลพาท* 42, 4 (ตุลาคม-ธันวาคม 2538): 87.

สรุปได้ว่าปัญหาในการรวบรวมและรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ตามประมวลกฎหมายวิธีพิจารณาความอาญาของพนักงานสอบสวนในประเทศไทยมี ดังนี้³⁴

1. ปัญหาการค้นหรือการเข้าถึงข้อมูลข้อมูลอิเล็กทรอนิกส์ จำทำอย่างไรพนักงานสอบสวนจะเข้าถึงพยานหลักฐานได้เร็วที่สุดเท่าที่จะทำได้ เพราะหลักฐานประเภทนี้มีธรรมชาติหรือลักษณะพิเศษ คือไม่มีรูปร่าง มองไม่เห็นและสัมผัสด้วยตาเปล่าไม่ได้ อีกทั้งยังถูกลบ กำจัด ทำลาย แก้ไขหรือเปลี่ยนแปลงง่ายในเวลาอันสั้น ทำให้ยากต่อการค้น รวบรวมเพื่อนำเสนอต่อศาล
2. ปัญหาการยึดและการเก็บรักษาพยานหลักฐานว่าจะทำอย่างไรให้ข้อมูลอยู่ในสภาพที่เป็นจริงมากที่สุด ไม่ถูกแก้ไขเปลี่ยนแปลง เพื่อนำเสนอต่อศาลให้มีความน่าเชื่อถือ
3. ปัญหาการนำเสนอพยานหลักฐานว่าจะนำเสนอในสถานะหรือฐานะเป็นพยานวัตถุหรือพยานเอกสาร และทำอย่างไรจึงจะมีน้ำหนักพอที่ศาลจะรับฟังได้โดยปราศจากความเคลือบแคลงสงสัย

³⁴ วัลลิกา เนติบันลือฤทธิ์, “ปัญหาการรวบรวมและพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีอาญา,” วารสารศาลยุติธรรมปริทัศน์ (กันยายน 2550): 14-19.

บทที่ 3

หลักกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ ตามกฎหมายต่างประเทศและประเทศไทย

จากสถานการณ์โลกในปัจจุบันพบว่าการก่ออาชญากรรมทางอิเล็กทรอนิกส์เพิ่มมากขึ้น หลากหลายรูปแบบ การกระทำความผิดประเภทนี้ส่งผลกระทบต่อประชาชนทั่วไป และยังก่อให้เกิด ความเสียหายต่อส่วนรวมต่อความมั่นคงของประเทศไทย ปัญหาอาชญากรรมทางอิเล็กทรอนิกส์มิได้ เกิดขึ้นกับประเทศไทยเท่านั้น ยังส่งผลกระทบต่อประเทศอื่น ๆ ด้วย ดังนั้น ในบทนี้จะศึกษาแนวคิด ในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ วิเคราะห์ถึงสภาพปัญหา และมาตรการทางกฎหมายที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของต่างประเทศ ในที่นี้จะกล่าวถึง ประเทศสหรัฐอเมริกา อังกฤษ และสหพันธ์รัฐเยอรมนี เพื่อศึกษาถึงแนวคิด เหตุผล ขั้นตอน วิธีการ และระยะเวลาในการค้น การยึด และการรับฟังพยานหลักฐานในศาลของ ต่างประเทศ เพื่อเป็นแนวทางในการแก้ไขปัญหากฎหมายเกี่ยวกับการรวบรวมพยานหลักฐาน อิเล็กทรอนิกส์ของประเทศไทยต่อไป

3.1 หลักกฎหมายในต่างประเทศที่ใช้ระบบกฎหมาย Common Law

จากปัญหาเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์จากปัญหาอาชญากรรมทาง เทคโนโลยีและการสื่อสารผ่านเครือข่ายอินเทอร์เน็ตและสื่ออิเล็กทรอนิกส์ได้สร้างความเสียหายกับ ระบบเศรษฐกิจและความมั่นคงกับนานาประเทศ การหามาตรการทางกฎหมายเพื่อควบคุมและ ปรามปรามการกระทำความผิดจึงเป็นสิ่งที่แต่ละประเทศได้เรียนรู้และปรับโครงสร้างทางกฎหมาย ภายในประเทศให้ทันต่อการเปลี่ยนแปลงไปของรูปแบบของอาชญากรรมและการเปลี่ยนแปลงของ สภาพการณ์โลก เจ้าหน้าที่ของรัฐจึงต้องปฏิบัติหน้าที่อยู่ภายใต้กฎหมายที่ให้อำนาจไว้เท่านั้น เพื่อ ไม่ให้กระทบต่อความเป็นส่วนตัวบุคคล การรวบรวมพยานหลักฐานการค้นข้อมูลอิเล็กทรอนิกส์ที่เป็น ข้อมูลส่วนบุคคลถือเป็นการละเมิดต่อสิทธิความเป็นส่วนตัวอย่างร้ายแรง จึงจำเป็นต้องมีกฎหมาย บัญญัติไว้อย่างชัดเจน

3.1.1 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาเป็นประเทศเสรีประชาธิปไตยที่มีการต่อสู้เพื่อสิทธิและเสรีภาพ ของประชาชนมายาวนาน แนวความคิดในเรื่องสิทธิและเสรีภาพของปัจเจกชนของสหรัฐอเมริกาจึง เป็นแนวความคิดทางกฎหมายธรรมชาติที่ให้ความสำคัญคุ้มครองสิทธิและเสรีภาพของประชาชนเป็นอย่าง สูง แต่ในขณะเดียวกันก็มีมาตรการทางกฎหมายที่จะใช้ดำเนินคดีกับอาชญากรรมทางอิเล็กทรอนิกส์ มากมายกว่า 40 ฉบับ เช่น National Stolen Property Act, Copyright Act ฯลฯ ประเทศ

สหรัฐอเมริกาเป็นสังคมที่มีการใช้เทคโนโลยีสารสนเทศมากมายแทบทุกสาขาอาชีพ อาชญากรรมไซเบอร์ที่เกิดขึ้นแพร่หลายก่อให้เกิดความเสียหายอย่างมาก

ในประเทศสหรัฐอเมริกา จึงเป็นที่มาของการพัฒนากฎหมายเพื่อทบทวนจุดสมดุลแห่งความขัดแย้งระหว่างการให้ความคุ้มครองสิทธิส่วนบุคคลกับอำนาจใช้กฎหมายของรัฐอีกครั้ง การศึกษากฎหมายเกี่ยวกับประเทศที่ประสบปัญหามาก่อนและได้หาทางแก้ไขแล้วเช่นประเทศสหรัฐอเมริกา ซึ่งเผชิญกับปัญหาอาชญากรรมคอมพิวเตอร์มากที่สุดได้มีการจัดตั้ง หน่วยงานที่มีทั้งภาครัฐและเอกชน เช่น National Computer Crimes Squad ซึ่งสังกัดอยู่ใน F.B.I. ทำหน้าที่สืบสวนสอบสวนและจัดตั้ง Computer Analysis and Response Team ชื่อย่อ CART ทำหน้าที่ตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ จึงเป็นน่าจะนำไปสู่แนวทางการปรับปรุงกฎหมายของประเทศไทย ได้เป็นอย่างดี ในประเทศสหรัฐอเมริการกระทำคามผิดเกี่ยวกับคอมพิวเตอร์ มีมาตั้งแต่ปี ค.ศ.1984 คือกฎหมาย Computer Fraud and Abuse Act (CFAA) ซึ่งมีแนวความคิดในการ บัญญัติกฎหมายเพื่อใช้ดำเนินคดีกับการกระทำคามผิดต่อคอมพิวเตอร์รูปแบบต่าง ๆ การที่สภากรรณเห็นว่าการกระทำรูปแบบใหม่นี้มีลักษณะพิเศษที่แตกต่างไปจากความผิดรูปแบบเดิม เพราะเป็นการกระทำที่เกี่ยวข้องกับสิ่งที่ไม่รูปร่างทำให้การจะดำเนินคดี โดยอาศัย ความผิดฐาน Theft และ Larceny ตามกฎหมายเดิม เป็นเรื่องที่ยากลำบาก เพื่อแก้ปัญหาเรื่องนี้ก็ควรที่จะบัญญัติกฎหมายใหม่ขึ้นมามากกว่าพยายามจะนำกฎหมายเก่ามาใช้ดำเนินคดีกับความผิดรูปแบบใหม่³⁵

CFAA 18 U.S.C. มาตรา 1030 กำหนดให้การเข้าถึงข้อมูลคอมพิวเตอร์ในกรณีดังต่อไปนี้ เป็นการกระทำคามผิด

1. Subsection 1030 (a) (1) เข้าสู่ระบบคอมพิวเตอร์โดยรู้ว่ามีอำนาจ และได้ไปซึ่งข้อมูลนั้น โดยมีเหตุอันควรเชื่อได้ว่าข้อมูลนั้นอาจใช้ไปเพื่อการอันเป็นภัยต่อความมั่นคงของรัฐ หรือเพื่อประโยชน์ของชาติอื่น ผู้กระทำความผิดตามอนุมาตรานี้จะถูกลงโทษปรับหรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 20 ปี³⁶

2. Subsection 1030 (a) (2) ผู้ใดเจตนาที่จะเข้าสู่ระบบคอมพิวเตอร์โดยปราศจากอำนาจ

³⁵ Jo-Ann M. Adams, "Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet," **Santa Clara High Technology Law Journal**. 12, 2 (January 1996), Retrieved March 10, 2016 from <http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1206&context=chtlj>

³⁶ CFAA 18 U.S.C. Subsection 1030(a)(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, of a financial institution, or of a card issuer as defined in section 1602(n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in

เพื่อให้ได้มาซึ่งข้อมูลทางการเงินหรือเข้าสู่ข้อมูลของสถาบันการเงิน ผู้กระทำความผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำความผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี³⁷

3. Subsection 1030 (a) (3) ผู้ใดมีเจตนาเข้าสู่คอมพิวเตอร์ของรัฐบาล โดยปราศจากอำนาจ และปลอมแปลง หรือสร้างทำเป็นว่าเป็นพนักงานของรัฐบาลเพื่อทำการเปิดระบบประมวลผลอันก่อให้เกิดความเสียหายต่อรัฐบาลสหรัฐ ผู้กระทำความผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำความผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี³⁸

4. Subsection 1030 (a) (4) ผู้ใดเข้าสู่ระบบคอมพิวเตอร์ของรัฐบาล โดยรู้ว่าไม่มีอำนาจเพื่อผลประโยชน์ใด ๆ ด้วยเจตนาที่จะฉ้อโกง หรือได้ไปซึ่งสิ่งมีค่าใด ๆ ผู้กระทำความผิดจะมีโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำความผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี เว้นแต่วัตถุประสงค์ของการ ฉ้อโกงและสิ่งของที่ได้มา รวมเฉพาะการใช้คอมพิวเตอร์และมูลค่าของการใช้ ดังกล่าวนั้น ไม่เกิน 5,000 เหรียญสหรัฐในช่วงเวลา 1 ปี³⁹

5. ผู้ใดเจตนาที่จะเข้าสู่ระบบคอมพิวเตอร์เพื่อผลประโยชน์ในคอมพิวเตอร์ของสหรัฐอเมริกาโดยปราศจากอำนาจและต่อแต่นั้นได้ทำการเปลี่ยนแปลง ทำลายข้อมูลสารสนเทศที่ได้เข้าไปสู่ นั่น ถ้าเพื่อฉ้อโกงทางการค้า (ตามที่กำหนดไว้ในมาตรา 1029) ในรหัสผ่านใด ๆ หรือข้อมูลอื่นที่มีลักษณะคล้ายคลึงกัน โดยปราศจากอำนาจ ก่อให้เกิดความเสียหาย⁴⁰

³⁷CFAA 18 U.S.C. Subsection 1030(a) (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—(A) information contained in a financial record

³⁸ CFAA 18 U.S.C. Subsection 1030(a) (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

³⁹CFAA 18 U.S.C. (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

⁴⁰ CFAA 18 U.S.C. section 1030 (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected

6. ผู้รู้และเจตนาที่จะโกงโดยการใช้ Password โดยปราศอำนาจ เพื่อที่จะเข้าไปยังข้อมูลคอมพิวเตอร์ของรัฐบาล เพื่อหาผลประโยชน์หรือเพื่อขายความลับนั้นให้กับต่างชาติ มีลักษณะเป็นการข่มขู่ว่าจะก่อให้เกิดความเสียหายต่อคอมพิวเตอร์ที่ได้รับการคุ้มครอง การไม่มีอำนาจเข้าสู่ระบบคอมพิวเตอร์ตามกฎหมายของประเทศสหรัฐอเมริกา นั่นคือ ว่าเป็น Theft of Computer Service เพราะเป็นการเข้าไปใช้บริการโดยไม่มีอำนาจ ทั้งที่ไม่ได้ก่อให้เกิดความเสียหายอย่างใดเลยต่อระบบการทำงานของเครื่อง ทั้งนี้กฎหมายอเมริกันให้ความเห็นว่า ถือว่าเป็นความเสี่ยงต่อการก่อให้เกิดผลเสียหายต่อข้อมูลสารสนเทศได้ และผู้กระทำความผิดรู้ดีว่าความเสียหายในอนาคตจะปรากฏขึ้น และการเข้าไปโดยไม่มีอำนาจเช่นนี้ อาจทำให้เจ้าของสิทธิไม่อาจเข้าสู่ระบบได้ เนื่องจากกฎหมาย Computer Fraud and Abuse Act (CFAA) ในปี ค.ศ.1984 ไม่สามารถครอบคลุมความผิดได้ทั้งหมด จึงมีการแก้ไขเรื่อยมาในปี ค.ศ.1988, 1989 และ 1990 ตามลำดับ จนกระทั่งสภาองเกรสได้มีมติให้ผ่านกฎหมายใหม่ ๆ ออกมาเสริม เช่น The National Information Infrastructure Protection Act of 1996 (NIIA) และเพิ่มเติมการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ใน U.S. Code title 18 มาตรา 1030 (18 U.S.C.A. Section 1030)⁴¹

รัฐธรรมนูญของประเทศมีบทบัญญัติที่เป็นหลักประกันสิทธิของประชาชนมิให้ถูกละเมิดโดยรัฐบาลที่เรียกว่า Bill of Rights ถึง 10 บท ซึ่งเป็นการกำหนดมาตรฐานขั้นต่ำ หรือจำกัดขอบเขตการใช้อำนาจของเจ้าหน้าที่ทั้งหลายที่เกี่ยวข้องในกระบวนการยุติธรรมทั้งในระดับ สหพันธรัฐและมลรัฐ โดยเฉพาะเจ้าหน้าที่ตำรวจและอัยการที่จะต้องปฏิบัติตามกฎเกณฑ์ที่ศาลสูงสุดได้วางไว้เท่านั้น โครงสร้างทางกฎหมาย สหรัฐอเมริกา ด้านการก่อการร้ายและอาชญากรรมทางไซเบอร์

บรรดากฎหมายต่าง ๆ ของรัฐบาลสหรัฐอเมริกา ที่ครอบคลุมเกี่ยวกับ การสืบสวน และดำเนินคดีกับบุคคล ซึ่งได้กระทำการก่อการร้ายและอาชญากรรมทางไซเบอร์ที่น่าสนใจ ได้แก่

1. Title 18, USC 1029 กฎหมายของสหรัฐอเมริกา Title 18, USC 1029, Fraud and Related Activity in Connection with Access Devices ว่าด้วยการฉ้อฉลและกิจกรรมที่เกี่ยวข้องเนื่องกับกลไกการเข้าถึง (ระบบเครือข่ายอินเทอร์เน็ต) ครอบคลุมการดำเนินคดีกับบุคคล ซึ่งลักลอบค้า รหัสหรือ หมายเลข บัตรเครดิตทางอินเทอร์เน็ต และการดำเนินคดีบุคคลซึ่งใช้ซอฟต์แวร์หรือฮาร์ดแวร์ในการผลิต หรือแพร่กระจายรหัสหรือหมายเลขบัตรเครดิต⁴² Title 18, USC 1029 Penalties (บทลงโทษ)

computer without authorization, and as a result of such conduct, causes damage and loss

⁴¹ CFAA 18 U.S.C. section 1030 (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if- (A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States;

⁴² พรทิพย์ ต้นทวนันท์, อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์ (วิทยานิพนธ์ปริญญาโทบริหารคดี คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), หน้า 68.

2. Title 18, USC 1030 กฎหมายของสหรัฐอเมริกา Title 18, USC 1030, Fraud and Related Activity in Connection with Computers ว่าด้วยการฉ้อฉลและกิจกรรมที่เกี่ยวข้องกับคอมพิวเตอร์ กฎหมายนี้ใช้ดำเนินคดีกับบุคคลซึ่งจงใจบุกรุกเข้าไปในคอมพิวเตอร์ โดยไม่ได้รับอนุญาตอันเป็นคอมพิวเตอร์ซึ่งอยู่ในการปกป้องของรัฐบาลสหรัฐอเมริกา U.S. Protected Computer คอมพิวเตอร์ซึ่งอยู่ในการปกป้องของรัฐบาลสหรัฐอเมริกา หมายถึง คอมพิวเตอร์ของรัฐบาล รวมทั้งคอมพิวเตอร์ซึ่งได้ถูกระบุไว้โดยรัฐบาลว่าเป็น คอมพิวเตอร์ที่เกี่ยวข้องกับการพาณิชย์ระหว่างมลรัฐ จะต้องเป็นกรณีที่เกิดความเสียหายที่เกินกว่าจำนวนเงิน \$5,000 หรือก่อให้เกิดผลร้ายต่อความปลอดภัยของมหาชนและความมั่นคงของชาติ อีกทั้งกฎหมายนี้จะครอบคลุมการดำเนินคดีกับบุคคลซึ่งจงใจปล่อยไวรัสหรือหนอน (Worms) เข้าไปในคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเพื่อก่อให้เกิด ความเสียหาย Title 18, USC 1030 Penalties (บทลงโทษ)

3. Title 18, USC 1362 กฎหมายของสหรัฐอเมริกา Title 18, USC 1362, Communications Lines, Stations, or Systems. ว่าด้วยสายเคเบิล, สถานี หรือ ระบบในการสื่อสาร ใช้ในการดำเนินคดีกับบุคคลซึ่ง จงใจสร้างผลร้าย หรือทำลายระบบ การสื่อสาร คมนาคม อีกทั้งกฎหมายนี้อาจใช้ในการดำเนินคดีกับบุคคลซึ่ง วางแผนที่จะดำเนินการ ละเมิดกฎหมายดังกล่าวนี้ Title 18, USC 1362 Penalties (บทลงโทษ) บุคคลซึ่งถูกตัดสินว่าได้ละเมิดกฎหมายตามมาตรา 1362 อาจ ถูกลงโทษจำคุก 10 ปี การทำความผิดครั้งแรก

4. Title 18, USC 2511 กฎหมายของสหรัฐอเมริกา Title 18 USC 2511, Interception and Disclosure of Wire, Oral, or Electronic Communications ว่าด้วยการดักเอาและเปิดเผย การสื่อสารโดย ทางสาย ไม่ว่าจะเป็นการสื่อสารทางเสียง หรือข้อความ แบบอิเล็กทรอนิกส์ กฎหมายนี้ใช้ในการดำเนินคดีกับบุคคลซึ่งจงใจดักจับการสื่อสารโดยทางสาย ทั้ง ที่เป็นการสื่อสารแบบเสียง และแบบอิเล็กทรอนิกส์และสามารถใช้ดำเนินคดีกับบุคคลซึ่งใช้เครื่องมือใด ๆ เพื่อดักเอาการสื่อสาร Title 18, USC 2511 Penalties (บทลงโทษ) สามารถลงโทษบุคคลซึ่งถูกตัดสินว่าได้ละเมิดกฎหมาย มาตราที่ 2511 อาจถูกลงโทษจำคุก 5 ปี สำหรับ การกระทำความผิดครั้งแรก

5. Title 18, USC 2701 กฎหมายของสหรัฐอเมริกา Title 18, USC 2701, Unlawful Access to Stored Communication. ว่าด้วยการเข้าถึงโดยไม่ถูกต้องตามกฎหมาย เพื่อลักลอบเอาการสื่อสารที่ได้ถูกเก็บไว้ กฎหมายนี้ใช้ในการดำเนินคดีกับบุคคลซึ่งจงใจเข้าไปในที่ใดซึ่งเป็นศูนย์ให้บริการและเก็บการสื่อสารโดยไม่ได้รับอนุญาต Title 18, USC 2701 Penalties (บทลงโทษ) บุคคลซึ่งถูกตัดสินว่าได้ละเมิดกฎหมาย มาตราที่ 2701 อาจถูกลงโทษ คุก 2 ปี สำหรับการกระทำความผิดครั้งแรก

6. Title 18, USC 2702 กฎหมายของสหรัฐอเมริกา Title 18, USC 2702, Disclosure of Contents ว่าด้วยการเปิดเผยเนื้อหา กฎหมายนี้ใช้ในการดำเนินคดีกับบุคคลซึ่งจงใจ เปิดเผยหรือ แฉการสื่อสาร หรือข้อมูลแบบอิเล็กทรอนิกส์ซึ่งได้มีการเก็บไว้ ณ ที่ใด กฎหมายนี้เป็นการให้อำนาจ

ในการดำเนินคดีแก่บุคคลซึ่งมอบข้อมูลให้แก่ผู้รับคนใดที่ไม่ได้รับอนุญาตให้มีข้อมูลนั้นไว้ในครอบครอง⁴³

Patriot Act รัฐบัญญัติว่า ด้วยความรักชาติ โดยรัฐบัญญัตินี้ได้ผ่านออกมา โดยนัยหนึ่งเป็นการตอบโต้การโจมตีโดย ผู้ก่อการร้ายถล่มอาคารเวิลด์เทรด ในกรุงนิวยอร์กและอาคารเพนตากอน ในกรุงวอชิงตัน เมื่อวันที่ 11 กันยายน 2001 Patriot Act ว่าด้วยความรักชาติเป็นการเสริมกฎหมายที่มีอยู่ในขณะนั้น โดยการขยายและเพิ่มโทษสำหรับอาชญากรรมซึ่งกระทำโดยการใช้อุปกรณ์เป็นเครื่องมือ และฉบับนี้มีบทเฉพาะซึ่งว่าด้วยการก่อการร้ายโดยทางไซเบอร์ จะต้องขยายขีดความสามารถทางด้านการพิสูจน์ หลักฐานคดีแบบไซเบอร์ ต่อมาเมื่อปี ค.ศ.2002 United States Patriot Act of โดยกฎหมายนี้ให้อำนาจในการที่จะดักฟังการสื่อสารในรูปแบบเสียงทางอินเทอร์เน็ต รวมถึงขยายคำจำกัดความของคำว่า คอมพิวเตอร์ที่อยู่ในความคุ้มครอง “Protected Computer” ให้ รวมถึงคอมพิวเตอร์ในต่างประเทศด้วยเพื่อชี้ให้เห็นถึงการขึ้นต่อกันและกัน ในบรรดาคอมพิวเตอร์ ทั้งหมดที่อยู่ในระบบเครือข่ายอินเทอร์เน็ต⁴⁴

การค้นและยึดคอมพิวเตอร์และการได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์ในการสอบสวนคดีอาญาแผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา สำนักงานคดีอาญากระทรวงยุติธรรมแห่งสหรัฐอเมริกา

ประเทศสหรัฐอเมริกา ได้มีการเรียนรู้จากประสบการณ์เกี่ยวกับอาชญากรรมทางไซเบอร์มาอย่างต่อเนื่อง ดังนั้น มาตรการทางกฎหมายในการป้องกัน ปราบปราม อาชญากรรมและการก่อการร้ายโดยทางไซเบอร์ สหรัฐอเมริกา จึงให้อำนาจและเครื่องมือแก่พนักงานสืบสวนสอบสวน เพื่อให้สามารถเข้าถึงพยานหลักฐานได้อย่างรวดเร็วทันต่อการทำลายพยานหลักฐานของอาชญากรรม

สรุปแล้วว่า การค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ที่อยู่ในความครอบครองของบุคคลใดในสหรัฐอเมริกา ก็ต้องมีหมายค้น และมีเหตุอันควรหรือมีความสมเหตุสมผลที่จะขอให้ศาลออกหมายค้น เพื่อตรวจสอบการใช้อำนาจของเจ้าพนักงานของรัฐ เพื่อไม่ให้เจ้าหน้าที่ตำรวจค้นและยึดพยานหลักฐานโดยผิดกฎหมายหรือขัดกับรัฐธรรมนูญ นอกจากการค้นตามบทบัญญัติรัฐธรรมนูญของประเทศสหรัฐอเมริกา ฉบับแก้ไข ครั้งที่ 4 ยังมีข้อยกเว้นที่ไม่ต้องขอหมายค้นอีกด้วย เช่น

1. ความยินยอม ซึ่งความยินยอมเกิดขึ้นได้หลายกรณี รวมถึงแถบข้อความแจ้งเตือนเมื่อเข้าสู่ระบบ (A Log In Banners) ข้อตกลงการเข้าใช้ (Terms-of-Use Agreement) หรือนโยบายบริษัท และสิ่งที่ต้องพิจารณาด้วย คือ เครื่องคอมพิวเตอร์เครื่องหนึ่งสามารถใช้ User ได้หลาย User และความยินยอมของ User คนหนึ่งก็เพียงพอแล้วสำหรับความยินยอม สำหรับการตรวจค้นในพื้นที่ส่วนบุคคล (Private Area) ของเครื่องคอมพิวเตอร์นั้น ๆ ก็ถือว่าความยินยอมดังกล่าวเพียงพอที่จะตรวจค้นพื้นที่ทั่วไป อย่างไรก็ตามความยินยอมอาจมีข้อจำกัดได้ ภายใต้เงื่อนไขของประเภทระยะเวลา และตัวแปรอื่น ๆ ความยินยอมอาจยกเลิกเพิกถอนเมื่อใดก็ได้

⁴³ Edward M. Wise, Computer Crime and Other Crimes Against Information Technology in the United States, In **International Review of Criminal Law** 64. (Toulouse, France: Association Internationale De Droit Penal, 1992), pp. 647-669.

⁴⁴ *Ibid.*

2. กรณีมีเหตุฉุกเฉิน เพื่อป้องกันการทำลายพยานหลักฐาน หน่วยงานบังคับใช้กฎหมายสามารถยึดอุปกรณ์เก็บข้อมูลอิเล็กทรอนิกส์ และในบางกรณีที่มียันตรายฉุกเฉินที่อาจทำให้สูญเสียข้อมูลหน่วยงานบังคับใช้กฎหมายสามารถที่จะตรวจค้นแบบมีข้อจำกัด ณ ขณะนั้นเพื่อรักษาข้อมูลนั้นไว้ได้

3.1.1.1 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์

การค้นข้อมูลอิเล็กทรอนิกส์เป็นการค้นที่แตกต่างจากการค้นที่อยู่เดิม ซึ่งเมื่อพนักงานสอบสวนเห็นสมควร จะค้นจะต้องมีหมายค้น โดยต้องบรรยายสถานที่ที่จะทำการค้นในหมายค้นนั้นด้วย สำหรับการค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์จะต้องทำการค้นหาฮาร์ดแวร์ หรือฮาร์ดดิสก์ ในการปฏิบัติหน้าที่ของพนักงานสอบสวนของสหรัฐอเมริกา จะต้องเป็นการค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์โดยไม่ขัดต่อหลักการไม่รบกวนพยานหลักฐาน ซึ่งได้มาโดยการค้นที่มีขอบ (Exclusionary Rule) ตามรัฐธรรมนูญสหรัฐอเมริกาแก้ไขเพิ่มเติมฉบับที่ 4 (The Fourth Amendment) บัญญัติว่า

สิทธิของบุคคลที่จะมีความปลอดภัยมั่นคงในร่างกาย เคหสถาน เอกสารและวัตถุสิ่งของต่อการค้น การยึด และการจับที่ไม่มีเหตุอันสมควร จะล่วงละเมิดมิได้ และห้ามมิให้มีการออกหมาย เว้นแต่จะโดยมีเหตุอันควร ซึ่งได้มาโดยการสอบสวนหรือพยานตนและหมายนั้นจะต้องระบุเฉพาะเจาะจงถึงสถานที่ที่จะถูกค้น ตัวบุคคลที่จะถูกจับ และสิ่งสิ่งของที่ถูกลัก

กฎหมายว่าด้วยวิธีพิจารณาความอาญาของสหรัฐอเมริกาได้รับรองหลักของรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่นี้ไว้ในมาตรา 41 (a) ซึ่งบัญญัติว่า

เจ้าพนักงานผู้มีอำนาจหรือพนักงานอัยการต้องขอหมายค้น

(1) หมายค้นต้องออกโดยศาล Magistrate ของมลรัฐ หรือศาลของสหรัฐ สำหรับการค้นสิ่งของหรือค้นหาบุคคลในเขตอำนาจศาล

(2) หมายค้นออกโดยศาล Magistrate สำหรับกรณีการสิ่งของหรือค้นหาบุคคลในเขตอำนาจศาลหรือค้นสิ่งของที่ถูกโยกย้ายหรือบุคคลหลบหนีออกนอกเขตก่อนจะถูกดำเนินการตามกฎหมาย

จากกฎหมายดังกล่าวจะเห็นได้ว่าเจ้าหน้าที่ของรัฐจะทำการค้นได้ก็ต่อเมื่อมีหมายค้น และหมายค้นดังกล่าวจะต้องออกโดยผู้พิพากษา แม้ในกรณีของการค้นข้อมูลอิเล็กทรอนิกส์ซึ่งเป็นพยานหลักฐานที่มีลักษณะพิเศษที่อาจถูกแก้ไขเปลี่ยนแปลงได้ง่าย เจ้าพนักงานของรัฐก็จะต้องทำการค้นโดยมีหมายเพราะต้องการจะให้กระบวนการในการออกหมายเป็นมาตรการในการตรวจสอบการใช้ดุลพินิจของเจ้าหน้าที่ (Warrant Process) เพื่อให้เจ้าหน้าที่ปฏิบัติหน้าที่โดยไม่ขัดกับรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 4 ในกรณีที่เจ้าหน้าที่ไม่จำเป็นที่จะต้องเข้าไปค้นในเคหสถานหรือสำนักงานของผู้อื่น แต่สามารถทำการค้นโดยใช้เครื่องคอมพิวเตอร์หรือเครื่องมืออื่นใด

เชื่อมต่อเข้ากับระบบ LAN หรือ WAN ของเคสสถานหรือสำนักงานตลอดจนเครือข่ายอินเทอร์เน็ต โดยไม่มีการบุกรุกเข้าไปทางกายภาพหากพิจารณาถึงสิทธิที่ได้รับการรับรองคุ้มครองตามรัฐธรรมนูญ แก้ไขเพิ่มเติมฉบับที่ 4 ซึ่งรวมไปถึงสิทธิส่วนบุคคลด้วย การค้นข้อมูลอิเล็กทรอนิกส์ในลักษณะนี้ ก็ถือเป็นการบุกรุก⁴⁵

3.1.1.2 การรับฟังเป็นพยานหลักฐานในศาล

ภายหลังที่กฎหมายอาชญากรรมทางคอมพิวเตอร์ในสหรัฐอเมริกาใช้บังคับแล้ว ยังมีปัญหาที่ตามมาอีกหลายประการ เช่น ปัญหาในการให้คำนิยามคำว่า “อาชญากรรมคอมพิวเตอร์” (Computer Crime) การจำกัดการให้ความคุ้มครองที่จำกัดเฉพาะงานของรัฐไม่รวมภาคเอกชน การขาดความชัดเจนในเรื่องของเขตอำนาจศาล และปัญหาเกี่ยวกับกับวิธีพิจารณาความ เช่น การแสวงหาพยานหลักฐาน และการการรับฟังเป็นพยานหลักฐาน ในศาล ทำให้ไม่สามารถนำผู้กระทำความผิดมาลงโทษได้

ศาลของสหรัฐอเมริกาจะไม่รับฟังพยานหลักฐานที่เกิดจากการค้นโดยมิชอบ ดังนั้น ในการค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ก็จะต้องเป็นการค้นที่ไม่ขัดต่อหลักการห้ามรับฟังพยานหลักฐานซึ่งได้มาโดยมิชอบ (Exclusionary Rule) ดังนั้น หากเจ้าหน้าที่แสวงหาพยานหลักฐานจากกล้องวงจรปิด จากข้อมูลอิเล็กทรอนิกส์โดยวิธีการที่ชอบด้วยกฎหมายเป็นการล่วงล้ำสิทธิส่วนบุคคล พยานหลักฐานดังกล่าวก็จะถูกตัดออกจากกระบวนการพิจารณาของศาลทันที โดยศาลจะไม่รับฟังทำให้ไม่สามารถนำตัวผู้กระทำความผิดมาลงโทษได้

สรุปว่ามาตรการทางกฎหมายของประเทศสหรัฐอเมริกา การค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ที่อยู่ในความครอบครองของบุคคลใดในทิวทัศน์ ก็ต้องมีหมายค้น และมีเหตุอันควรหรือมีความสมเหตุสมผลที่จะขอให้ศาลออกหมายค้น เพื่อตรวจสอบการใช้อำนาจของเจ้าพนักงานของรัฐ เพื่อไม่ให้เจ้าหน้าที่ตำรวจค้นและยึดพยานหลักฐานโดยผิดกฎหมายหรือขัดกับรัฐธรรมนูญ นอกจากการค้นตามบทบัญญัติรัฐธรรมนูญของประเทศสหรัฐอเมริกา ฉบับแก้ไข ครั้งที่ 4 แต่มีข้อยกเว้นกรณีที่ไม่ต้องขอหมายค้นอีก เช่น

- 1) ความยินยอม ซึ่งความยินยอมเกิดขึ้นได้หลายกรณี รวมถึงแถบข้อความแจ้งเตือนเมื่อเข้าสู่ระบบ (A Log in Banners) ข้อตกลงการเข้าใช้ (Terms-of-Use Agreement) หรือนโยบายบริษัท และสิ่งที่ต้องพิจารณาด้วย คือ เครื่องคอมพิวเตอร์เครื่องหนึ่งสามารถใช้ User ได้หลาย User และความยินยอมของ User คนหนึ่งก็เพียงพอแล้วสำหรับความยินยอม สำหรับการตรวจค้นในพื้นที่ส่วนบุคคล (Private Area) ของเครื่องคอมพิวเตอร์นั้น ๆ ก็ถือว่าความยินยอมดังกล่าวเพียงพอที่จะตรวจค้นพื้นที่ทั่วไป อย่างไรก็ตาม ความยินยอมอาจมีข้อจำกัดได้ภายใต้เงื่อนไขของประเภทเรื่อง ระยะเวลา และตัวแปรอื่น ๆ ความยินยอมอาจยกเลิกเพิกถอนเมื่อใดก็ได้

⁴⁵ Ibid.

2) กรณีมีเหตุฉุกเฉิน เพื่อป้องกันการทำลายพยานหลักฐาน หน่วยงานบังคับใช้กฎหมายสามารถยึดอุปกรณ์เก็บข้อมูลอิเล็กทรอนิกส์ และในบางคดีที่มีภัยอันตรายฉุกเฉินที่อาจจะทำให้สูญเสียชีวิตของหน่วยงานบังคับใช้กฎหมายสามารถที่จะตรวจค้นแบบมีข้อจำกัด ณ ขณะนั้น เพื่อรักษาข้อมูลนั้นไว้ได้ นอกจากนี้ ศาลสูงสุดของสหรัฐอเมริกาได้กำหนดมาตรฐานของความสมเหตุสมผลในกรณีที่เจ้าหน้าที่ผู้บังคับใช้กฎหมายเป็นผู้ดำเนินการค้น และยึดด้วยตนเองโดยไม่ผ่านการตรวจสอบเอาไว้ การออกหมายค้นจึงต้องมีการตรวจสอบโดยผู้พิพากษา ซึ่งเป็นนโยบายของศาลสูงสุดที่ต้องการให้กระบวนการออกหมาย (Warrant Process) เป็นมาตรการในการตรวจสอบดุลพินิจของเจ้าหน้าที่ผู้บังคับใช้กฎหมายในการค้นและยึด เพื่อเป็นหลักประกันว่าเจ้าหน้าที่ของฝ่ายบริหารจะไม่ทำการค้นและยึดพยานหลักฐานโดยผิดกฎหมายหรือขัดต่อรัฐธรรมนูญ พยานหลักฐานอิเล็กทรอนิกส์ที่ได้มาอาจถูกตัดโดยบทตัดพยาน ห้ามไม่ให้ศาลรับฟัง

กฎหมายลักษณะพยานของประเทศสหรัฐอเมริกา มีความชัดเจนถือเป็นตัวอย่างที่ดีในเรื่องบทบัญญัติพยานหลักฐานอิเล็กทรอนิกส์ โดยได้บัญญัติว่า ให้รับฟังได้โดยวางหลักไว้ใน Federal Rules of Evidence (แก้ไขข้อ 1002 ประกอบกับข้อ 1001 (3)) แสดงว่า Printouts จากการประมวลผลของเครื่องคอมพิวเตอร์ หรือความถูกต้องของเอกสารที่พิมพ์ผ่านเครื่องคอมพิวเตอร์ ถือเป็นเอกสารต้นฉบับ ทำให้หลัก Best Evidence Rule ไม่เป็นอุปสรรคในการรับฟังพยานหลักฐานทางคอมพิวเตอร์ที่เป็นสื่ออิเล็กทรอนิกส์⁴⁶

ประเทศสหรัฐอเมริกา ยังได้จัดทำคู่มือไว้สำหรับเป็นแนวทางที่ FBI จะได้ใช้ประโยชน์ในการแสวงหาและรวบรวมพยานหลักฐานอย่างชัดเจน เพื่อไม่ให้เจ้าหน้าที่ของฝ่ายบริหารจะไม่ทำการค้นและยึดพยานหลักฐานโดยผิดกฎหมายหรือขัดต่อรัฐธรรมนูญ

3.1.2 ประเทศอังกฤษ

ในประเทศอังกฤษก่อนที่จะมีกฎหมายอาญาว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือการรักษาความปลอดภัยของข้อมูลในคอมพิวเตอร์นั้น การเข้าถึงข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์โดยปราศจากอำนาจไม่ถือเป็นความผิดอาญา โดยพิจารณาเปรียบเทียบกับความผิดฐานบุกรุก (Trespass) ความผิดที่เกี่ยวกับทรัพย์สิน (Theft) ที่ผู้กระทำความผิดรับผิดชอบแต่เพียงในทางแพ่ง⁴⁷ โดยอังกฤษได้ออกกฎหมายเพื่อที่จะรับฟังเอกสารคอมพิวเตอร์โดยถือว่าเป็นข้อยกเว้นของพยานบอกเล่า คือ พระราชบัญญัติพยานทางแพ่ง ค.ศ.1968 (Civil Evidence 1986) พระราชบัญญัติพยานทางอาญา ค.ศ.1965 (Criminal Evidence Act 1965) และในปี ค.ศ.1984 อังกฤษได้บัญญัติกฎหมายใหม่คือ พระราชบัญญัติตำรวจและพยานทางอาญา ค.ศ.1984 เพื่อสร้างเงื่อนไขในการรับฟังเอกสารจากคอมพิวเตอร์ให้รัดกุมขึ้นกว่ากฎหมายเดิม

⁴⁶ พรทิพย์ ต้นทวนันท์, *เรื่องเดิม*, หน้า 68.

⁴⁷ เฉลิมพล ช่อโพธิ์ทอง, *ความผิดฐานลักทรัพย์และฉ้อโกง: ศึกษาเปรียบเทียบกฎหมายอังกฤษ เยอรมัน และไทย* (วิทยานิพนธ์ปริญญาโทบริหารนิติ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2535), หน้า 73.

ต่อมาเมื่อการกระทำความผิดอาญาโดยใช้คอมพิวเตอร์เข้ามามีส่วนเกี่ยวข้องมูลค่าความเสียหายที่เกิดขึ้นมีจำนวนมาก ประเทศอังกฤษจึงได้บัญญัติกฎหมายขึ้นมาควบคุมอาชญากรรมคอมพิวเตอร์ขึ้นมาบังคับใช้เมื่อ 29 สิงหาคม ค.ศ.1990 โดยมีเหตุผลในการประกาศใช้ว่า “พระราชบัญญัติฉบับนี้เป็นบทบัญญัติเพื่อคุ้มครองสำหรับการรักษาความปลอดภัยของคอมพิวเตอร์และอุปกรณ์ในการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการแก้ไขเปลี่ยนแปลงที่เกี่ยวข้องกับผลประโยชน์ที่มีขอบ”

3.1.2.1 กฎหมายในการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ ประเทศอังกฤษจะให้ความเคารพต่อสิทธิส่วนบุคคล โดยมีคดีตัวอย่างเกี่ยวกับนายจ้างและลูกจ้างที่ศาลตัดสินว่านายจ้าง ไม่ว่าข้อมูลนั้นจะเก็บไว้ในระบบธรรมดาหรือจัดเก็บไว้ในคอมพิวเตอร์ก็ตาม⁴⁸ ต่อมารัฐบาลอังกฤษได้พิจารณาถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ควรได้รับการคุ้มครอง จึงได้ออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เพราะจำเป็นต้องดำเนินการให้กฎหมายภายในของอังกฤษสอดคล้องกับอนุสัญญาแห่งสภายุโรปว่าด้วยการให้ความคุ้มครองข้อมูล (The Council of Europe’s Data Protection) รัฐสภาของประเทศไทยได้ออก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (The Data Protection Act 1984 แก้ไขเพิ่มเติม ค.ศ.1998) เพราะในการแสวงหาพยานหลักฐานของเจ้าพนักงานของรัฐ โดยล่วงล้ำเข้าไปรับรู้ถึงข้อมูลที่เกี่ยวข้องกับการดำเนินชีวิตของผู้ต้องสงสัยสารสนเทศที่อยู่ในความครอบครองของผู้ใช้ และการแสดงความคิดเห็นส่วนตัวเท่ากับการเป็นการล่วงล้ำข้อมูลส่วนบุคคลที่กฎหมายอังกฤษประสงค์จะให้ปกปิด ดังเช่น คดีระหว่างนายจ้างและลูกจ้างข้างต้น การรวบรวมพยานหลักฐานด้วยวิธีการ ดังกล่าว อาจถูกหาว่าเป็นพยานหลักฐานที่ได้มาโดยมิชอบได้

นอกจากนั้น ก็มีพระราชบัญญัติคุ้มครองสำหรับการรักษาความปลอดภัยของคอมพิวเตอร์ และอุปกรณ์ในการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการแก้ไขเปลี่ยนแปลงที่เกี่ยวข้องกับผลประโยชน์ที่มีขอบมีเนื้อหาสาระที่สำคัญของกฎหมาย ดังนี้

มาตรา 1 ความรับผิดชอบฐานเข้าถึงคอมพิวเตอร์และส่วนประกอบของคอมพิวเตอร์โดยไม่ได้รับอนุญาต

(1) บุคคลใดก็ตามย่อมมีความผิดถ้า

ก. บุคคลนั้นได้ทำการให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใด ๆ โดยเจตนาที่จะเข้าถึงสิ่งที่ปกป้องคุ้มครองไม่ให้เข้าสู่ระบบหรือได้ผ่านสิ่งปกป้องเช่นนั้นเข้าไปโปรแกรมใด ๆ หรือข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ใด ๆ หรือ

ข. บุคคลนั้นเจตนาที่จะเข้าถึงสิ่งที่ปกป้องคุ้มครองระบบโดยปราศจากอำนาจ และ

⁴⁸ Edward Wilding, *Computer Evidence: A Forensic Investigations Handbook* (London: Sweet & Maxwell, 1997), p. 93.

ค. บุคคลนั้นได้รู้อยู่ในขณะนั้นว่าตนเป็นต้นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานอันปราศจากอำนาจนั้น

(2) เจตนาของบุคคลที่ได้กระทำความผิดภายใต้มาตรานี้ ไม่จำเป็นต้องเป็นการกระทำต่อ

ก. โปรแกรมพิเศษหรือข้อมูลพิเศษเฉพาะเจาะจงใด ๆ

ข. โปรแกรมหรือข้อมูลเฉพาะชนิดใดชนิดหนึ่ง หรือ

ค. โปรแกรมหรือข้อมูลที่ถูกเก็บไว้เฉพาะในคอมพิวเตอร์ใด ๆ

(3) บุคคลใดกระทำความผิดตามมาตรานี้ต้องระวางโทษ. . .

มาตรา 2 การเข้าถึงโดยไม่ได้รับอนุญาต หมายถึง มีเจตนาที่จะกระทำการหรือให้ความสะดวกหรือส่งเสริมในการกระทำผิด ดังนี้

(1) บุคคลจะมีความผิดภายใต้บทบัญญัตินี้ถ้าหากว่าตนได้กระทำความผิดตามมาตรา 1 ด้วยเจตนา (มาตรา 1 บัญญัติว่าการเข้าถึงโดยไม่มีอำนาจเป็นความผิด)

ก. ได้กระทำความผิดในสิ่งที่มาตรานี้บังคับใช้ หรือ

ข. ให้ความสะดวกในการกระทำความผิด (ไม่ว่าโดยเจตนา หรือโดยบุคคลใด ๆ) และความผิดที่ตนจงใจกระทำความผิดหรือให้ความสะดวกดังกล่าวต่อไปในมาตรานี้ถือว่าเป็นผู้กระทำความผิด เช่นเดียวกันกับผู้กระทำความผิด

มาตรานี้บังคับใช้กับความผิดของบุคคลซึ่งมีอายุตั้งแต่ 21 ปี เพื่อวัตถุประสงค์ของมาตรานี้ไม่ว่าการกระทำความผิดของผู้กระทำความผิดที่อยู่ระยะไกลจะได้กระทำลงในโอกาสที่มีอำนาจในการเข้าถึงระบบนั้นหรือไม่ หรือโดยอาศัยโอกาสอื่นใดก็ได้บุคคลอาจมีความผิดตามมาตรา 1 นี้แม้ว่าข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำความผิดที่อยู่ระยะไกลไม่ได้กระทำลงก็ตาม ผู้กระทำความผิดตามมาตรา 1 นี้ต้องระวางโทษ

มาตรา 3 ความผิดฐานแก้ไขเปลี่ยนแปลง คอมพิวเตอร์และส่วนประกอบโดยไม่ได้รับอนุญาต บุคคลใดก็ตามย่อมมีความผิดถ้าผู้นั้นได้กระทำการใด ๆ อันเป็นการก่อให้เกิดการแก้ไขเปลี่ยนแปลงสิ่งซึ่งบรรจุอยู่ในคอมพิวเตอร์ใด ๆ และจะต้องกระทำการโดยเจตนาและจำเป็นต้องได้รู้ถึงการกระทำนั้นความมุ่งหมาย

(1) โดยเจตนาตามอนุ 1 ข้างต้นหมายถึง เจตนาที่จะก่อให้เกิดการเปลี่ยนแปลงสิ่งซึ่งบรรจุอยู่ในคอมพิวเตอร์ใด ๆ และกระทำโดย

ก. ทำให้เสียไปซึ่งระบบปฏิบัติการของคอมพิวเตอร์ใด ๆ

ข. ป้องกันหรือขัดขวางการเข้าถึงเพื่อที่จะยึดข้อมูลหรือโปรแกรมคอมพิวเตอร์ใด ๆ ในเครื่องคอมพิวเตอร์

ค. ทำให้เสียหายไปซึ่งระบบปฏิบัติการของโปรแกรมคอมพิวเตอร์นั้น หรือความน่าเชื่อถือของข้อมูลนั้น ๆ

(2) โดยเจตนาไม่จำเป็นที่จะต้องตรงกับ

ก. คอมพิวเตอร์ใด ๆ โดยเฉพาะ

ข. ข้อมูลหรือโปรแกรมเฉพาะหรือข้อมูล หรือโปรแกรมชนิดใดชนิดหนึ่งโดยเฉพาะ

ค. การแก้ไขเปลี่ยนแปลงใด ๆ โดยเฉพาะหรือการแก้ไขเปลี่ยนแปลงชนิดใดชนิดหนึ่งโดยเฉพาะ

(3) ความมุ่งหมายของอนุ (1) จำเป็นต้องรู้ถึงการกระทำนั้น หมายถึง การได้รู้ว่าการแก้ไขเปลี่ยนแปลงใด ๆ ผู้หนึ่งได้เจตนาก่อให้เกิดขึ้นโดยที่ไม่ได้รับอนุญาต

(4) ความมุ่งหมายของส่วนประกอบคอมพิวเตอร์ตามมาตรานี้ ไม่ว่าจะเป็นการแก้ไขโดยไม่ได้รับอนุญาตหรือเจตนากระทำต่อคอมพิวเตอร์ และส่วนประกอบตาม อนุ(2) หรือเป็นเจตนาที่กระทำอย่างถาวรหรือเพียงชั่วคราวก็ตาม

(5) การแก้ไขเปลี่ยนแปลงสิ่งซึ่งบรรจุอยู่ในคอมพิวเตอร์ จะได้รับการคุ้มครองตามความมุ่งหมายของกฎหมายของกฎหมายชดเชยความเสียหายจากอาชญากรรม ค.ศ.1971 ถ้าการแก้ไขเปลี่ยนแปลงนั้นมีผลกระทบโดยตรงต่อคอมพิวเตอร์ สื่อบันทึกของคอมพิวเตอร์และทำให้เสียไปตามลักษณะเงื่อนไขทางกายภาพหรือทางวัตถุ

(6) บุคคลใดกระทำความผิดตามมาตรานี้ต้องระวางโทษ

จากกฎหมาย Computer Misuse Act 1990 ของประเทศอังกฤษ มาตรา 1 เป็นการบัญญัติพื้นฐานที่ใช้กับความผิดเข้าถึงโดยไม่ได้รับอนุญาต มีสาระสำคัญในส่วนของการกระทำคือ ผู้กระทำความผิดจะต้องกระทำการอันเป็นเหตุให้คอมพิวเตอร์แสดงผลการทำงานใด ๆ โดยผู้กระทำจะต้องรับผิดชอบไม่ว่าผู้กระทำจะประสบผลสำเร็จในการเข้าสู่ระบบประมวลผลเข้าสู่โปรแกรมหรือข้อมูลหรือไม่ถือว่าเป็นความผิดสำเร็จแล้ว ส่วนความผิดในมาตรา 2 บังคับใช้กับกรณีกระทำการหรือให้ความสะดวกหรือส่งเสริมในการกระทำความผิด มาตรา 1 ซึ่งเป็นการควบคุมเครื่องจากระยะไกล เช่น การลักลอบเข้าระบบโดยใช้เครื่องระยะไกลและใช้บังคับกับที่มีอายุตั้งแต่ 21 ปีขึ้นไป โทษตามมาตรา 2 จะมีโทษสูงกว่ามาตรา 1 มาตรา 3 เป็นบทบัญญัติความผิดฐานแก้ไขเปลี่ยนแปลงคอมพิวเตอร์และส่วนประกอบอันเป็นฐานความผิดชนิดบังคับใช้กับความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ เจตนาในการกระทำความผิด

ในการกำหนดโทษสำหรับความผิดทางอาญาโดยทั่วไปจะต้องมีการแสดงออกถึงเจตนาในการกระทำความผิดทางอาญาด้วย ซึ่งนับว่าเป็นองค์ประกอบภายในของความรับผิดชอบทางอาญาในเรื่องนั้น ๆ เจตนาที่จะกระทำความผิด ได้มีการบัญญัติไว้ในตัวบทกฎหมายอาญาของประเทศทั่วโลก สำหรับการกระทำความผิดอาญาเกี่ยวกับคอมพิวเตอร์นั้นก็มีความผิดทางอาญาที่

ต้องการเจตนาตั้งเช่นความผิดอาญาอื่น ๆ โดยทั่วไปอันเป็นเจตนาธรรมดา ที่จะกระทำการอันเป็นความผิดนั้น ๆ และในขณะเดียวกันความผิดทางอาญาที่เกี่ยวกับคอมพิวเตอร์ในบางกรณีก็อาจต้องการ “เจตนาพิเศษ” ในการกระทำผิดนั้น ๆ มลรัฐแคลิฟอร์เนีย สหรัฐอเมริกา บัญญัติว่า “จำเลยจะต้องเข้าถึงระบบคอมพิวเตอร์” เพื่อจุดประสงค์ของการวางแผนหรือกลอุบายใด ๆ เพื่อที่จะข่มขู่หรือหลอกลวง หรือประโยชน์จากการบริการ “โดยเจตนาทุจริตและหลอกลวง” ซึ่งถ้าผู้กระทำความผิดขาดเจตนาตั้งกล่าวก็ไม่อาจมีการลงโทษทางอาญาเกิดขึ้นได้ แม้ว่าผู้กระทำความผิดยังอาจถูกดำเนินคดีทางแพ่งในข้อหาฐานละเมิดได้ก็ตาม

เหตุจูงใจ (Motives) ในการประกอบอาชญากรรมคอมพิวเตอร์ บรรดาอาชญากรทั้งหลายมักจะมีเหตุจูงใจในทำนองเดียวกัน คือ การประกอบอาชญากรรมเป็นการท้าทายและเป็นการเล่นเกม (Challenge and Game Playing) อาชญากรบางคนคิดว่าการประกอบอาชญากรรมคอมพิวเตอร์ไม่ได้เป็นการกระทำผิด แต่เป็นเรื่องที่คนทั่วไปมักจะกระทำกันซึ่งเป็นการกระทำแบบที่เรียกว่า Vending Machine Syndrom คือ ถ้าเราไปพบเงิน 2-3 เหรียญ ใน Vending Machine หรือในโทรศัพท์สาธารณะก็จะเก็บเงินนั้นไว้โดยไม่พยายามสืบหาเจ้าของ ดร.สแตนเลย์ วินเกอร์ (Dr. Stanley Winkler) จากบริษัท IBM ได้ทดลองเรื่องนี้ในประเทศต่าง ๆ

กรณีที่เครื่องคอมพิวเตอร์เป็นผู้บันทึกข้อมูลในระบบกฎหมายคอมพิวเตอร์ ถือว่าการบันทึกลักษณะอย่างข้อมูลอิเล็กทรอนิกส์ที่เป็นการนำสืบความจริงเป็นพยานเอกสารประเภทหนึ่ง เพราะมีมนุษย์เข้าไปมีส่วนเกี่ยวข้องกับการประมวลผลของเครื่องคอมพิวเตอร์ ดังนั้น การรับฟังพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์ประเภทนี้ต้องใช้หลักเกณฑ์เช่นเดียวกับการรับฟังพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์ประเภทนี้จึงต้องใช้หลักเกณฑ์เช่นเดียวกับการรับฟังพยานเอกสาร

ในการนำสืบสวนเป็นหน้าที่ของเจ้าหน้าที่ตำรวจ ในการแสวงหาข้อเท็จจริงและรวบรวมพยานหลักฐานเกี่ยวกับการกระทำความผิดอาญาที่เกิดขึ้น ซึ่งเจ้าพนักงานตำรวจมีสิทธิที่จะสอบถามปากคำบุคคลใดบุคคลหนึ่งไม่ว่าจะเป็นผู้ต้องสงสัยว่าได้กระทำความผิดนั้นหรือไม่ แต่ต้องอยู่ภายในกรอบซึ่งพระราชบัญญัติตำรวจและพยานหลักฐานในคดีอาญา ค.ศ.1984 (The Police and Criminal Evidence Act 1984: PACE)⁴⁹

สรุปได้ว่าประเทศอังกฤษมีการออกพระราชบัญญัติวางแนวทางในการปฏิบัติหน้าที่ของเจ้าพนักงานที่มีความชัดเจนทำให้บังคับใช้กฎหมายมีหลักเกณฑ์แน่นอน ทั้งนี้เพื่อให้การปฏิบัติหน้าที่ของพนักงานเป็นไปในมาตรฐานเดียวกัน

3.1.2.2 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงพยานอิเล็กทรอนิกส์ กฎหมายที่เป็นหลักเกณฑ์ในการค้นหาพยานหลักฐานของอังกฤษ คือ The Police and Criminal Evidence Act 1984 (PACE) มาตรา 1 บัญญัติว่า “การค้นเคหสถานต้องมีเหตุอันควรสงสัยตามสมควร โดยถือมาตรฐานของบุคคลในฐานะ และพฤติกรรมเกี่ยวกับผู้ค้นเป็นเกณฑ์” และค้นจะต้องมีการออกค้น จากศาล (Justice of the Peace) โดยศาลจะออกหมายค้นก็ต่อเมื่อเป็นเหตุอันควร

⁴⁹ ณรงค์ ใจหาญ และคณะ, รายงานศึกษาวิจัยฉบับสมบูรณ์ เรื่องสิทธิผู้ต้องหาจำเลยและผู้ต้องโทษในคดีอาญา (รายงานการวิจัย เสนอต่อคณะกรรมการกฤษฎีกา, 2540), หน้า 23.

เชื่อว่าเป็น ความผิดอาญาร้ายแรง (Serious Arrest able Offence) ดังนั้น จึงต้องพิจารณาว่า อาชญากรรมคอมพิวเตอร์จะถือเป็นความผิดอาญาร้ายแรงที่ศาลสมควรจะออกหมายค้นหรือไม่

การค้นและยึดพยานหลักฐานต่าง ๆ ตามกฎหมายวิธีพิจารณาความอาญาของ ประเทศอังกฤษต้องคำนึงถึงแนวความคิดในเรื่องการคุ้มครองสิทธิมนุษยชนในทางอาญา ซึ่งได้ บัญญัติรับรองไว้ในกฎบัตรแมกนาคาร์ตา (Magna Carta, 1215) กฎหมายของประเทศอังกฤษ ได้ วางมาตรการควบคุม และตรวจการทำงานของเจ้าพนักงานตำรวจโดยองค์กรภายนอกเอาไว้ ขณะเดียวกันก็ไม่ทำให้ประสิทธิภาพในการดำเนินงานของเจ้าหน้าที่ลดลง โดยให้เจ้าหน้าที่ของรัฐ ได้แก่ ตำรวจ อัยการ และผู้พิพากษา สามารถใช้ดุลพินิจ ในการบังคับใช้กฎหมายได้มากขึ้น และใน ขณะเดียวกันก็มีข้อบังคับที่ตราขึ้นเพื่อควบคุมการปฏิบัติงานเอาไว้โดยละเอียด

1) การค้นเครื่องคอมพิวเตอร์พีซีในที่รโหฐาน ตาม PACE วางหลักไว้ใน มาตรา 1 ว่า การค้นในเคสสถานต้องมีเหตุอันสมควรสงสัยตามสมควร โดยถือเอามาตรฐานของ บุคคลในฐานะ และพฤติการณ์เดียวกับผู้ค้นเป็นเกณฑ์และจะต้องขอหมายค้นจากศาลตั้งนั้น ในการ ค้นข้อมูลอิเล็กทรอนิกส์ไม่ว่าจะอยู่ที่ใดทั้งที่อยู่ในเคสสถานหรือที่รโหฐานอื่นเจ้าพนักงานตำรวจ จะต้องมีความสงสัยตามสมควรว่าจะมีพยานหลักฐานอยู่ที่นั่นและจะต้องมีศาลเป็นผู้ทำหน้าที่ ตรวจสอบการดำเนินงานอีกชั้นหนึ่งในการออกหมายค้นศาลจะออก

2) การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN ระบบ WAN และระบบ อินเทอร์เน็ต ตำรวจอังกฤษจะใช้วิธีนำเครื่องคอมพิวเตอร์หรือเครื่องมืออื่นเชื่อมต่อเข้าไปในระบบเฉพาะ ของสำนักงาน และระบบเครือข่ายอินเทอร์เน็ตเพื่อเข้าไปตรวจค้นข้อมูลในนั้น จะขอหมายจาก Justice of the Peace ไม่ได้ แต่จะต้องขอจาก Circuit Judge และศาลจะออกหมายให้ต่อเมื่อได้ สอนได้ความว่า“มีเหตุอันควรเชื่อ ว่าพยานหลักฐานที่เกี่ยวกับการสอบสวนในคดีความผิดเป็น ความผิดอาญาร้ายแรง(Serious Arrest able Offence) ซึ่งเกิดขึ้นในบ้านนี้ และถ้าไม่ค้นบ้านนี้ก็จะ ไม่ได้มาซึ่งพยานหลักฐานดังกล่าว และในการค้นนั้นจะได้มาซึ่งพยานหลักฐานอันเป็นประโยชน์ต่อ สาธารณชน”⁵⁰

3.1.2.3 การยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์ ในการยึดและรักษา พยานหลักฐานอิเล็กทรอนิกส์มีบัญญัติอยู่ใน PACE มาตรา 18, 19 ดังนี้

มาตรา 18 บัญญัติว่า “เมื่อค้นแล้วตำรวจต้องทำบันทึกการค้นและบันทึกรายการ สิ่งของที่ค้นและยึด รายการเหล่านั้นผู้ค้นต้องมอบให้แก่เจ้าของบ้านเมื่อผู้นั้นร้องขอ” และ

มาตรา 19 บัญญัติว่า “กรณีที่ตำรวจยึดวัตถุที่มีเหตุเชื่อได้ว่าเป็นพยานหลักฐานที่ เกี่ยวข้องกับการสอบสวน หรือความผิดอื่น หรือมีความผิดอื่นรวมอยู่ด้วย หรือมีความจำเป็นต้องยึด เพื่อป้องกันการการเคลื่อนย้าย ซ่อนเร้น หรือทำลายหลักฐาน”

จากบทบัญญัติดังกล่าวข้างต้นจะเห็นได้ว่า เครื่องคอมพิวเตอร์ที่ยึดได้นั้นเป็นวัตถุที่ ใช้เป็นพยานหลักฐานในการสอบสวนที่เจ้าหน้าที่ตำรวจยึดได้รวมทั้งข้อมูลที่อยู่ภายในเครื่องด้วย เว้นแต่กรณีที่ข้อมูลที่เป็นความลับ ที่จะต้องพิจารณาตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ประกอบ

⁵⁰ เรื่องเดียวกัน, หน้า 51.

3.1.2.4 การรับฟังเป็นพยานหลักฐานในศาล การรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ของศาลอังกฤษ โดยหลัก จะรับฟังแต่พยานหลักฐานโดยตรง พยานบอกเล่า (Hearsay) ถือว่ามีน้ำหนักน้อยหรือไม่รับฟังเลย แต่ The Police and Criminal Evidence Act 1984 เป็นกฎหมายพยานหลักฐานในคดีอาญา ที่บัญญัติเกี่ยวกับการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เป็นข้อยกเว้นของพยานบอกเล่า (Hearsay) โดยให้รับฟังพยานเอกสารที่เป็นผลจากการประมวลผลหรือคำนวณของเครื่องคอมพิวเตอร์ได้ การค้น และยึดพยานหลักฐานกระทำโดยเจ้าพนักงานตำรวจ

ประเทศอังกฤษแบ่งพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ออกเป็น 3 ประเภท เช่นเดียวกับประเทศอื่น ๆ ที่ใช้ระบบกฎหมายคอมมอนลอว์ (Common Law) กล่าวคือ พยานบุคคล พยานเอกสาร และพยานวัตถุ ส่วนพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ที่เครื่องคอมพิวเตอร์เป็นผู้บันทึกข้อมูล ศาลอังกฤษใช้ระบบกฎหมายคอมมอนลอว์ ก็ถือว่าการบันทึกลักษณะอย่างข้อมูลอิเล็กทรอนิกส์ที่เป็นการนำสืบความจริงเป็นพยานเอกสารประเภทหนึ่ง เพราะมีมนุษย์เข้าไปมีส่วนเกี่ยวข้องกับการประมวลผลของเครื่องคอมพิวเตอร์ ดังนั้น การรับฟังพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์ประเภทนี้ต้องใช้หลักเกณฑ์เช่นเดียวกับการรับฟังพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์ประเภทนี้จึงต้องใช้หลักเกณฑ์เช่นเดียวกับการรับฟังพยานเอกสาร แต่ต้องไม่มีความผิดพลาดในกระบวนการคอมพิวเตอร์ พยานนั้นถูกต้องแท้จริง ไม่ถูกแก้ไขเปลี่ยนแปลง

กรณีที่ประสบปัญหาการกระทำความผิดทางอินเทอร์เน็ต ที่การกระทำอาจเกิดขึ้นในต่างประเทศ อำนาจในการสอบสวนจะสามารถกระทำได้เพียงใด เช่น การกระทำความผิด เกิดขึ้นในประเทศเยอรมนี และผู้กระทำความผิดอยู่ที่ประเทศนั้นแต่เครือข่ายที่ใช้ข้อมูลหรือข้อมูลที่ใช้นั้นผ่านประเทศอังกฤษ จะต้องคำนึงถึงข้อตกลงระหว่างประเทศโดยเฉพาะข้อตกลงระหว่างประชาคมยุโรป ด้วยแม้ว่าจะต้องคำนึงถึงเรื่องดังกล่าว การดำเนินคดีตามกฎหมายอังกฤษจะถือหลักว่าถ้าเข้าหลักเกณฑ์ 2 ประการดังต่อไปนี้ประเทศอังกฤษก็อาจจะไม่นำมาดำเนินคดี คือ ถ้าผู้กระทำความผิดหรือผู้ร่วมกระทำความผิดไม่ใช่พลเมืองของประเทศอังกฤษ หรือความผิดที่เกิดขึ้นไม่ได้บัญญัติไว้ใน The Computer Misuse Act 1990

ศาลที่มีอำนาจพิจารณาคดี สามารถแบ่งได้ตามฐานความผิด ดังนี้

1) ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access) เป็นการกระทำความผิดที่ไม่ซับซ้อน ศาลที่มีอำนาจในการพิจารณาคดี คือ ศาลแขวง (Magistrate Court) จึงมีกฎหมายที่เกี่ยวข้องอีกฉบับ คือ The Magistrate's Court Act 1980 เป็นเรื่องเกี่ยวกับการกำหนดฐานความผิดแก่ผู้ที่ให้ความช่วยเหลือในการกระทำความผิดในมาตรา 44 (1) ซึ่งบัญญัติว่า “สามารถลงโทษบุคคลที่ความช่วยเหลือผู้ที่กระทำการเข้าถึงโดยปราศจากอำนาจ โดยการให้ความรู้ทางด้านข้อมูลการให้รหัสผ่านหรือให้วิธีการเข้าสู่ระบบเพื่อผ่านไปยังโปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์”

2) ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง และความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจขึ้นอยู่กับความร้ายแรงของการกระทำความผิด หากมีความร้ายแรงมากก็จะอยู่ในอำนาจพิจารณาของศาลสูงคดีอาญา (Crown Court) แต่ถ้าไม่ร้ายแรงมากก็จะอยู่ในอำนาจพิจารณาของ

ศาลแขวง (Magistrate Court) โดยลักษณะของข้อมูลอิเล็กทรอนิกส์ที่ไม่สามารถพิสูจน์ได้ในทางกายภาพจึงไม่สามารถนำมาพิสูจน์ในกระบวนการพิจารณาคดีอาญาได้ ดังนั้นรายงานที่ประมวลผลจากคอมพิวเตอร์ (Printout) จะเป็นพยานบอกเล่า (Earsay) เนื่องจากเกิดจากการกระทำของมนุษย์ ต้องห้ามรับฟัง ตามกฎหมาย Criminal Justice Act 1988 มาตรา 24 แต่จากความสามารถในการทำงานของคอมพิวเตอร์เองที่สามารถใช้เป็นเครื่องกล หรือเครื่องมือในการคำนวณจึงไม่น่าจะเป็นพยานหลักฐานในรูปพยานบอกเล่าเสมอไป ถ้าอ้างเป็นพยานหลักฐานโดยยืนยันการใช้ที่เป็นธุรกิจปกติและข้อมูลที่ได้ก็เกิดจากการประมวลผลโดยคอมพิวเตอร์อันเป็นปกติเช่นกัน⁵¹

สรุปมาตรการทางกฎหมายของประเทศอังกฤษ ได้ว่า ระบบกฎหมายของประเทศอังกฤษ Common Law รัฐธรรมนูญไม่ได้บัญญัติเป็นลายลักษณ์อักษร กฎหมายรัฐธรรมนูญของประเทศอังกฤษจึงกระจายอยู่ในรูปแบบต่าง ๆ ทั้งในรูปพระราชบัญญัติ หรือในรูปแบบของข้อตกลงและขนบธรรมเนียม ดังนั้นการปฏิบัติหน้าที่ของเจ้าพนักงานตำรวจ⁵²

ในการแสวงหาข้อเท็จจริงและรวบรวมพยานหลักฐานที่เกี่ยวกับการกระทำความผิดอาญา เจ้าหน้าที่ตำรวจมีสิทธิที่จะสอบถามปากคำบุคคลใดบุคคลหนึ่งไม่ว่าจะเป็นผู้ต้องสงสัยว่าได้กระทำความผิดนั้นหรือไม่ การปฏิบัติหน้าที่ของตำรวจไม่ได้อยู่ในบังคับแห่งบทบัญญัติกฎหมายใด แต่ต้องปฏิบัติตามข้อกำหนดที่เรียกว่า “ข้อบังคับของผู้พิพากษา”⁵³ นอกจากนั้นการแสวงหาพยานหลักฐานในคดีอาญาให้ตำรวจปฏิบัติตามพระราชบัญญัติตำรวจและพยานหลักฐานในคดีอาญา ค.ศ.1984 (The Police and Criminal Evidence Act 1984: PACE) ซึ่งประกอบไปด้วยเรื่องอำนาจในการจับกุม การค้นและยึด รวบรวมพยานหลักฐาน ตลอดจนการปฏิบัติหน้าที่ของเจ้าหน้าที่ตำรวจ แต่ในขณะเดียวกันก็ไม่ได้ทำให้ประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมของเจ้าหน้าที่ลดลง

การค้นพยานหลักฐานอิเล็กทรอนิกส์ในเคสสถาน หรือในที่อื่นใดนอกเหนือจากนี้ ตำรวจจะต้องมีเหตุอันควรสงสัยตามสมควรว่า จะมีพยานหลักฐานนี้อยู่ภายในนั้น การค้นจะต้องขอหมายค้นจากศาล และศาลจะออกหมายค้นให้เมื่อมีเหตุอันควรเชื่อว่าความผิดอาญาเกิดขึ้น และมีพยานหลักฐานชุกช่อนอยู่ในเคสสถานนั้น

⁵¹ Richard May, **Criminal Evidence** (London: Sweet & Maxwell, 1999), pp. 11-361.

⁵² มหาวิทยาลัยสุโขทัยธรรมาธิราช, สาขาวิชานิติศาสตร์, เอกสารการสอนชุดวิชาระบบกฎหมายไทยและต่างประเทศ (นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2528), หน้า 49.

⁵³ *เรื่องเดียวกัน*, หน้า 814.

3.2 หลักกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในต่างประเทศที่ใช้ระบบกฎหมาย Civil Law

ประเทศสหพันธ์สาธารณรัฐเยอรมนี

ประเทศสหพันธ์สาธารณรัฐเยอรมนีนับเป็นประเทศต้น ๆ ที่พยายามจะแก้ไขกฎหมาย หรือเพิ่มเติมกฎหมายเพื่ออุดช่องว่างของการกระทำความผิดทางคอมพิวเตอร์ รวมทั้งเป็นประเทศที่ร่วมลงนามในอนุสัญญาความร่วมมือที่เกี่ยวกับอาชญากรรมอินเทอร์เน็ต (Convention on Cybercrime) ซึ่งออกโดยคณะมนตรียุโรป (Europarat) ด้วย แนวคิดของประเทศเยอรมันไม่มีบทบัญญัติพิเศษโดยเฉพาะที่จะลงโทษพวกออาชญากรรมทางอิเล็กทรอนิกส์ แต่หากมีบทลงโทษทางอาญา German Criminal Code 1974 แก้ไขเพิ่มเติม (StGB: Strafgesetzbuch)⁵⁴

ประเทศสหพันธ์สาธารณรัฐเยอรมนีเป็นประเทศที่ใช้ประมวลกฎหมาย หรือประเทศ Civil Law ส่วนใหญ่ประเทศเยอรมนี จะเน้นปราบปรามกลุ่มอาชญากรรมกลุ่มที่ 2 คือ กลุ่มที่กระทำความผิดโดยอาศัยคอมพิวเตอร์เป็นเครื่องมือเช่น การเผยแพร่ข้อมูลต่าง ๆ ที่เนื้อหาที่เป็นความผิดตามกฎหมาย การหมิ่นประมาททางอินเทอร์เน็ต การเผยแพร่งานอันละเมิดทรัพย์สินทางปัญญา หรือการฟอกเงินทางอินเทอร์เน็ต

รัฐธรรมนูญของประเทศสหพันธ์สาธารณรัฐเยอรมนีเน้นการคุ้มครองสิทธิส่วนบุคคลเป็นอย่างมาก หลักการไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบในกฎหมายเยอรมันมีรากฐานมาจากรัฐธรรมนูญว่าด้วยการคุ้มครองสิทธิเสรีภาพของประชาชน การจำกัดสิทธิดังกล่าวจะกระทำได้อีกแต่อาศัยอำนาจแห่งกฎหมาย การค้นเคหสถานจะกระทำได้อีกแต่โดยคำสั่งของผู้พิพากษา และการค้นจะต้องกระทำในลักษณะที่กฎหมายบัญญัติไว้เท่านั้น⁵⁵

การปฏิบัติหน้าที่ของเจ้าพนักงานหรือเจ้าหน้าที่ตำรวจ จึงเป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญา “The Code of Criminal Procedure” ศาลมีอำนาจอย่างกว้างขวางในการที่จะใช้ดุลพินิจในการรับฟังพยานหลักฐานที่เสนอโดนคู่ความ และดุลพินิจนี้จะถูกโต้แย้งไม่ได้⁵⁶

สำหรับกรณีกฎหมายวิธีสบัญญัติ ว่าด้วยการจับกุม ตรวจค้น รวบรวมพยานหลักฐานในประเทศสหพันธ์สาธารณรัฐเยอรมนีวิธีการและหลักเกณฑ์เป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศเยอรมัน เพียงแต่อาชญากรรมทางอิเล็กทรอนิกส์เป็นการกระทำความผิดที่ต้องใช้ข้อมูลอิเล็กทรอนิกส์มาเป็นพยานหลักฐานพิสูจน์ความผิดของจำเลย ในประเทศเยอรมัน จึงมี

⁵⁴ ฉัตรมงคล รุ่งรัตน์มณีวงศ์, **มาตรการแสวงหา รวบรวมและการเสนอพยานหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์** (วิทยานิพนธ์ปริญญาโทบริหารคดี คณะนิติศาสตร์มหาวิทยาลัยรามคำแหง, 2547), หน้า 89

⁵⁵ Walter R. Clemens, “The Exclusionary Rule Under Foreign Law,” *The Journal of Criminal Law Criminology and Police Science* 52, 3 (September-October 1961).

⁵⁶ ฉัตรมงคล รุ่งรัตน์มณีวงศ์, *เรื่องเดิม*, หน้า 90-93.

ปัญหาว่า ยากมากสำหรับการดำเนินกระบวนการพิจารณาให้สมบูรณ์ได้ ยากต่อการที่ตำรวจจะตรวจพบ และรับรายงานการกระทำความผิด นอกจากนี้ มีปัญหาเรื่องเขตอำนาจสอบสวนเพราะการกระทำความผิด ไร้ขอบเขต จึงต้องคำนึงถึงข้อตกลงระหว่างรัฐไม่ให้เกิดปัญหาล่วงล้ำอธิปไตยของรัฐอื่น

1. การค้นเครื่องคอมพิวเตอร์พีซี (PC) ในที่รโหฐาน ข้อมูลอิเล็กทรอนิกส์ที่อยู่ในความครอบครองของมนุษย์ในที่รโหฐาน เช่น ในเครื่องคอมพิวเตอร์พีซี (PC) ในที่รโหฐานต้องปฏิบัติตามหลักประมวลกฎหมายวิธีพิจารณาความอาญา (StGB: Strafgesetzbuch) ซึ่งจำต้องเข้าใจกระบวนการทางวิธีพิจารณาความอาญา กล่าวคือ ในสหพันธ์สาธารณรัฐเยอรมนี การสอบสวนและการรวบรวมพยานหลักฐาน เพื่อทราบข้อเท็จจริงในเนื้อหา นอกจากพนักงานอัยการแล้วยังมีองค์กรอื่น ๆ ที่ช่วยในการสอบสวน คือ สำนักงานอาชญาวิทยาแห่งสหพันธ์รัฐ Bundeskriminalamt หรือเรียกชื่อย่อว่า BKA มีตำรวจ 2 ประเภท คือ ข้าราชการตำรวจซึ่งเป็นผู้ช่วยของพนักงานอัยการ และข้าราชการตำรวจอื่น ๆ ส่วนผู้พิพากษาสอบสวนนั้น จะเป็นผู้อนุญาตใช้มาตรการบางอย่างในการสอบสวนของพนักงานอัยการ โดยเป็นผู้ตรวจสอบว่ามาตรการที่ใช้นั้น ชอบด้วยกฎหมายหรือไม่

การได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ จึงอาศัยอำนาจการค้น การยึด จากองค์กรผู้มีหน้าที่ตามกฎหมาย ซึ่งอาจมีปัญหาและอุปสรรคว่า การดำเนินการตามกฎหมายของสหพันธ์สาธารณรัฐเยอรมนีจะเกิดปัญหาในการค้น และยึดพยานหลักฐานที่ไม่มีรูปร่างอย่างไร องค์กรผู้มีหน้าที่รวบรวมพยานหลักฐานข้างต้นจะดำเนินการค้นในที่รโหฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา ได้แก่

กรณีการออกหมายค้นมาตรา 105 วรรคแรกที่ว่า “หมายค้นออกโดยศาล คือ ผู้พิพากษาสอบสวน เว้นแต่กรณีเร่งด่วนการสั่งให้ค้นในเคหสถาน อาจทำได้โดยพนักงานอัยการ หรือพนักงานตำรวจผู้ช่วยอัยการ” การค้นตามกฎหมายของสหพันธ์สาธารณรัฐเยอรมนีจะต้องระบุรายละเอียดดังนี้ มาตรา 107 “รายละเอียดในหมายค้นจะต้องระบุมูลเหตุแห่งการค้น บุคคล และสิ่งของที่ต้องการค้นด้วย” “ห้ามมิให้ค้นเคหสถานในระหว่างกลางคืน เว้นแต่เป็นการค้นสถานที่ทางธุรกิจที่เปิดบริการสาธารณะในเวลากลางวัน หรือความผิดซึ่งหน้า หรือกรณีฉุกเฉินหรือการค้นนักโทษที่หลบหนีที่คุมขัง”

2. การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN, ระบบ WAN และระบบอินเทอร์เน็ต เป็นการแน่นอนว่าการเข้าตรวจค้นของตำรวจ หรือพนักงานอัยการผู้มีอำนาจ หากใช้วิธีการเชื่อมต่อเข้าไปในระบบ ระบบ LAN ระบบ WAN และในระบบเครือข่ายอินเทอร์เน็ตแม้ว่า จะไม่ได้บุกรุกทางกายภาพ แต่เป็นการล่วงล้ำสิทธิส่วนบุคคลเป็น “การค้น” ต้องมีหมายค้น ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 99 ได้ให้อำนาจค้น ยึดสิ่งของที่เป็นจดหมาย ไปรษณีย์ โทรเลข โดยเจ้าหน้าที่ดังกล่าวจะต้องขอคำสั่งจากศาลให้ยึดได้ มาตรา 100 วรรคแรกมิใช่กระทำได้โดยพลการ ซึ่งบทบัญญัตินี้กฎหมายมีเจตนารมณ์จะให้อำนาจเจ้าหน้าที่ไว้เป็นพิเศษ เพื่อประโยชน์ในการสอบสวน ซึ่งตำรวจเยอรมัน สามารถใช้กฎหมายข้อนี้ และขอความร่วมมือจาก ISP

3. การยึดและรักษาพยานหลักฐานทางอิเล็กทรอนิกส์ ความน่าเชื่อถือของการค้น ยึดพยานหลักฐาน กล่าวคือ ตามกฎหมายสหพันธ์สาธารณรัฐเยอรมนีอาจอยู่ที่วิธีการค้นที่เคร่งครัดตาม มาตรา 106 วรรคแรก บัญญัติว่า “การค้นต้องกระทำต่อหน้าเจ้าของสถานที่ หากไม่อยู่จะต้องกระทำต่อหน้าผู้แทนญาติ หรือเพื่อนบ้าน” การปฏิบัติตามกฎหมายดังกล่าว อย่างน้อยก็สร้างความน่าเชื่อถือ

ต่อศาลได้ว่าเจ้าหน้าที่โปรงใส พยานข้อมูลอิเล็กทรอนิกส์ที่ได้มาน่าจะตรงกับความจริงขณะที่ค้น นอกจากนี้ การยึดพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เกี่ยวข้องกับมาตรา 94 ที่วางหลักว่า สิ่งของที่อาจยึดได้

1) สิ่งของที่อาจเป็นพยานหลักฐานสำคัญในการสอบสวน หรือสิ่งของที่รีบไว้จะต้องจัดให้อยู่ในอารักขา หรือทำให้ปลอดภัยทางใดทางหนึ่ง

2) การยึดสิ่งของ ที่อยู่ในความครอบครองของบุคคล หรือไม่ยอมส่งให้ด้วยความสมัครใจให้ขอคำสั่งศาล

4. การรับฟังเป็นพยานหลักฐานในศาล พยานหลักฐานอิเล็กทรอนิกส์ ถ้านำส่งในฐานะพยานเอกสาร เกี่ยวข้องกับประมวลกฎหมายวิธีพิจารณาความอาญาสหพันธ์สาธารณรัฐเยอรมนี คือ มาตรา 244, 245, 249 และ 261 ถ้านำส่งในฐานะพยานวัตถุจะไม่ค่อยมีปัญหา เพราะพยานวัตถุสำหรับกฎหมายเยอรมันใช้พิสูจน์ต่อศาลโดยให้ศาลตรวจดูได้ การนำเสนอพยานอิเล็กทรอนิกส์ ในฐานะพยานเอกสาร เช่น การนำส่ง Printouts เพื่อพิสูจน์ข้อความในเอกสาร ต้องอยู่บนเงื่อนไขของความถูกต้องแท้จริง กล่าวคือ พยานเอกสารที่เสนอต่อศาลใช้ “ต้นฉบับ” เท่านั้น (มาตรา 244 วรรคสาม) ถ้าหาต้นฉบับไม่ได้ และต้องเป็นพยานที่มีความสำคัญในคดี (มาตรา 244 วรรคสอง)

สรุปได้ว่ากฎหมายประเทศสหพันธ์สาธารณรัฐเยอรมนี ในปัจจุบันการรวบรวมพยานหลักฐานคล้ายกับกฎหมายประเทศไทย พนักงานตำรวจกระทำภายใต้บทบัญญัติของกฎหมายที่ให้อำนาจไว้เท่านั้น การรวบรวมพยานหลักฐานในคดีเกี่ยวกับคอมพิวเตอร์ ไม่มีกฎหมายเฉพาะมารองรับแต่พัฒนาจากกฎหมายเดิมที่มีอยู่เพื่อให้ทันต่อความก้าวหน้าของเทคโนโลยี และ ศาลมีอำนาจอย่างกว้างขวางในการที่จะใช้ดุลพินิจในการรับฟังพยานหลักฐานที่เสนอโดยคู่ความ และดุลพินิจนี้จะถูกโต้แย้งไม่ได้ การรวบรวมพยานหลักฐานเพื่อที่จะทราบข้อเท็จจริงในเนื้อหา นอกจากพนักงานอัยการแล้ว ยังมีองค์กรอื่น ๆ ที่ช่วยในการสอบสวน คือ ตำรวจ และผู้พิพากษาสอบสวน องค์กรตำรวจที่มีหน้าที่ในการสอบสวนคือ สำนักงานอาชญาวิทยาแห่งสหพันธ์รัฐ

3.3 หลักกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทย

การพิจารณาถึงอำนาจหน้าที่ของเจ้าพนักงานและพนักงานสอบสวนก็เป็นสิ่งสำคัญ เพื่อให้เกิดความสมดุลในการใช้อำนาจและปกป้องคุ้มครองประชาชนในประเทศ ให้ปลอดภัยจากอาชญากรรมทางอิเล็กทรอนิกส์ หน่วยงานภาครัฐจึงมีบทบาทสำคัญในการควบคุมอาชญากรรมประเภทนี้อย่างจริงจัง เนื่องจากการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ มีความยุ่งยากในการตรวจพบ การเก็บ รวมถึงยากต่อการพิสูจน์ความผิดอาชญากรรมอิเล็กทรอนิกส์กระทำได้อย่างรวดเร็ว

ปัจจุบันประเทศไทยจะมีการพัฒนากฎหมายเพื่อให้ทันต่ออาชญากรรมทางเทคโนโลยี โดยมีการออกกฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาควบคุมอาชญากรรมทางอิเล็กทรอนิกส์โดยให้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ไว้ใน มาตรา 18 เพื่อให้ง่ายต่อการรวบรวมพยานหลักฐานและทันการกับลักษณะการกระทำความผิด แต่ในขณะที่จุดเริ่มต้นของการสืบสวนสอบสวนอยู่ที่พนักงานตำรวจและพนักงานสอบสวน ก็ยังคงปฏิบัติตาม

ประมวลกฎหมายวิธีพิจารณาความอาญาอยู่เช่นเดิม ดังนั้นจึงเห็นควรกำหนดมาตรการทางกฎหมาย เพื่อป้องกันและปราบปรามการกระทำความผิดทางอิเล็กทรอนิกส์ให้สัมฤทธิ์ผลในทางปฏิบัติต่อไป กฎหมายที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานในประเทศไทย ได้แก่

3.3.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550

ปรากฏอยู่ใน ส่วนที่ 3 สิทธิและเสรีภาพส่วนบุคคล มาตรา 33

บุคคลย่อมมีเสรีภาพในเคหสถานบุคคลย่อมได้รับความคุ้มครองในการที่จะอยู่อาศัยและครอบครองเคหสถานโดยปกติสุข การเข้าไปในเคหสถานโดยปราศจากความยินยอมของผู้ครอบครอง หรือการตรวจค้นเคหสถานหรือในที่รโหฐาน จะกระทำได้ เว้นแต่มีคำสั่งหรือหมายของศาล หรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ

3.3.1.1 ปัญหาการค้นและการยึด กฎหมายวิธีพิจารณาความอาญาของไทยบัญญัติถึงหลักการออกหมายค้นว่าจะต้องสามารถระบุได้ว่าจะค้นสิ่งใด ซึ่งอยู่ที่ใด แต่ข้อมูลคอมพิวเตอร์บางกรณีไม่อาจจะระบุได้ว่าอยู่ใน รูปแบบใด เก็บไว้ที่ใด ประกอบด้วยสิ่งใดบ้าง ตลอดจนหากในการค้นตามหมายค้น พบการกระทำความผิดอื่น ซึ่งไม่เกี่ยวกับความผิดที่มีการออกหมายค้น จะสามารถดำเนินการกับสิ่งที่ พบในขณะนั้นได้หรือไม่ การค้นข้อมูลในระบบเครือข่ายมีขอบเขตเพียงใด กล่าวคือสามารถค้น เข้าไปในข้อมูลที่อยู่ต่างประเทศได้หรือไม่ จะสามารถทำสำเนาข้อมูลได้หรือไม่ การยึด พยานหลักฐานที่เป็นข้อมูลในคอมพิวเตอร์ ซึ่งเป็นสิ่งไม่มีรูปร่าง จะทำได้โดยวิธีใด หากข้อมูลที่จะยึดมาจากระบบเครือข่ายคอมพิวเตอร์ของผู้อื่น และมีอยู่มากมายหลายแห่ง จะสามารถยึด ทั้งระบบได้หรือไม่ จึงน่าจะคิดว่าควรมีกฎหมายให้อำนาจพิเศษแก่เจ้าพนักงานในการตรวจค้น ยึดหลักฐานพยานหรือไม่

3.3.1.2 ปัญหาอำนาจ และความสามารถของเจ้าพนักงานที่บังคับใช้กฎหมาย เทคโนโลยีคอมพิวเตอร์เป็นเรื่องใหม่ เจ้าพนักงานบังคับใช้กฎหมายยังขาดความรู้ ความเข้าใจ บุคลากรที่มีความรู้ความสามารถยังมีอยู่จำกัด ทำให้การป้องกันอาชญากรรม คอมพิวเตอร์ยังขาดประสิทธิภาพ จึงน่าจะคิดว่าควรมีการจัดตั้งหน่วยงานเฉพาะกิจเกี่ยวกับ อาชญากรรมคอมพิวเตอร์ เพื่อให้มีเจ้าหน้าที่ที่มี ความรู้ความชำนาญเฉพาะในการดำเนินคดี อาชญากรรมประเภทนี้ นอกจากนี้ จึงควรปรับปรุงกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในเรื่องการให้อำนาจ พนักงานเจ้าหน้าที่ให้เหมาะสม เพื่อประสิทธิภาพในการบังคับใช้กฎหมาย ปัญหาพยานหลักฐานนี้น่าวิเคราะห์ว่าในชั้นสอบสวน พนักงานสอบสวนได้รวบรวมพยานหลักฐานได้แล้ว พนักงานอัยการจะใช้ดุลยพินิจอย่างไรในการพิจารณาส่งฟ้อง เพราะถ้า หากพนักงานสอบสวนได้มาด้วยความยากลำบาก แต่พนักงานอัยการสั่งไม่ฟ้อง ก็จะทำให้เกิด ความสิ้นเปลืองทางเศรษฐกิจ บุคลากร และเวลาในการปฏิบัติหน้าที่อย่างน่าเสียดาย แต่เมื่อถึง ชั้นศาลแล้ว ข้อมูลคอมพิวเตอร์เป็นพยานอิเล็กทรอนิกส์ จะจัดเป็นพยานเอกสารหรือพยาน วัตถุตามกฎหมาย เรื่องพยานหลักฐาน และศาลจะรับฟังพยานอิเล็กทรอนิกส์ได้หรือไม่ หากทำสำเนาข้อมูลคอมพิวเตอร์

เพื่อเป็นพยานหลักฐานจะเกิดปัญหาว่าศาลจะรับฟังสำเนา พยานหลักฐานหรือไม่ กฎหมายของไทยควรกำหนดให้มีพยานผู้เชี่ยวชาญในเรื่องนี้⁵⁷

3.3.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ในที่นี้จะวิเคราะห์ในเรื่องอำนาจหน้าที่ในหมวด 2 ตามมาตรา 18-21 ว่าด้วย พนักงานเจ้าหน้าที่ที่มีอำนาจหน้าที่ในการรวบรวมพยานหลักฐานกำหนดให้พนักงานเจ้าหน้าที่ที่มีอำนาจในการเข้าตรวจข้อมูลคอมพิวเตอร์ ในกรณีมีเหตุอันควรสงสัยว่าน่าจะมีการกระทำความผิดตามพระราชบัญญัติโดยมีอำนาจ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ เพื่อให้การดำเนินคดีตามพระราชบัญญัตินี้มีประสิทธิภาพจึงได้มีหลักการพิเศษเพิ่มขึ้น 2 ประการคือ การเพิ่มวิธีการพิเศษในการสืบสวนและสอบสวน และการเพิ่มให้มี “พนักงานเจ้าหน้าที่” เข้ามามีอำนาจในการสืบสวนและความผิดตามพระราชบัญญัตินี้ด้วยนอกเหนือจากพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญา โดยกล่าวถึงอำนาจของพนักงานเจ้าหน้าที่ดังนี้ การสืบสวนพิเศษตาม การรวบรวมพยานหลักฐานในคดีความผิดเกี่ยวกับคอมพิวเตอร์ ถือเป็นการรวบรวมพยานหลักฐานในทางคดีที่เกี่ยวกับความผิดอาญาในส่วนของความผิดเกี่ยวกับคอมพิวเตอร์นั้นค่อนข้างยุ่งยากและซับซ้อนเพราะผู้รวบรวมพยานหลักฐานนอกจากจะต้องมีความรู้ความเชี่ยวชาญเกี่ยวกับกฎหมายแล้วยังต้องมีความรู้เชี่ยวชาญในส่วนของการคอมพิวเตอร์ด้วยซึ่งบุคคลประเภทนี้มีน้อย ดังนั้น เมื่อใช้หลักกฎหมายวิธีพิจารณาความอาญาเพียงอย่างเดียวอาจก่อให้เกิดความบกพร่องในการรวบรวมพยานหลักฐาน

ดังนั้น จึงได้มีการบัญญัติกฎหมายขึ้นมาเพื่อให้สอดคล้องกับสภาพธรรมชาติของความผิดอันเกี่ยวกับคอมพิวเตอร์ (By Nature) แต่อย่างไรก็ตามหลักการเกี่ยวกับการสืบสวนสอบสวนการจับกุมค้น ขัง ย่อมไปตามประมวลกฎหมายพิจารณาความอาญาและกฎหมายอื่นที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยวิธีพิจารณาคดีในศาลแขวง กฎหมายว่าด้วยวิธีพิจารณาคดีเยาวชนและครอบครัว (ในส่วนที่เกี่ยวกับความผิดทางอาญา) เป็นต้น ซึ่งการผนวกรวมอำนาจการสืบสวนสอบสวนในประมวลกฎหมายวิธีพิจารณาความอาญาเข้ากับพระราชบัญญัตินี้ปรากฏอยู่ในมาตรา 29

3.3.2.1 อำนาจสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ มาตรา 29 ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญา มีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้ ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติ และรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง เพื่อให้การดำเนินคดีตามพระราชบัญญัตินี้มีประสิทธิภาพจึงได้มีหลักการพิเศษเพิ่มขึ้น คือ การเพิ่มวิธีการพิเศษในการสืบสวนและสอบสวน และการเพิ่มให้มี

⁵⁷ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550

“พนักงานเจ้าหน้าที่” เข้ามามีอำนาจในการสืบสวนและความผิดตามพระราชบัญญัติฉบับนี้ด้วย นอกเหนือจากพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญา

3.3.2.2 การสืบสวนพิเศษตามมาตรา 18 บัญญัติให้พนักงานเจ้าหน้าที่มีอำนาจพิเศษในการสืบสวนสอบสวนรวม 8 ประการ นอกเหนือจากอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญาทั่วไป คือ

1) มีอำนาจในการมีหนังสือสอบถามหรือเรียกบุคคลที่ข้องเกี่ยวกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูลหรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

2) มีอำนาจในการเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลที่เกี่ยวข้อง

3) มีอำนาจในการสั่งให้ผู้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่⁵⁸

4) มีอำนาจในการทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่คอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่ (พนักงานเจ้าหน้าที่ต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาต)

5) มีอำนาจในการสั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวให้แก่เจ้าพนักงานเจ้าหน้าที่ (พนักงานเจ้าหน้าที่ต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาต)

6) มีอำนาจในการตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิด และสั่งให้บุคคลนั้น ส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้ (พนักงานเจ้าหน้าที่ต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาต)

7) มีอำนาจในการถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว (พนักงานเจ้าหน้าที่ต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาต)

8) มีอำนาจในการยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้ (พนักงานเจ้าหน้าที่ต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาต)

⁵⁸ สุนติ คงเทพ, *เรื่องเดิม*, หน้า 183.

3.3.2.3 บทบัญญัติที่ให้อำนาจพนักงานเจ้าหน้าที่เป็นพิเศษคือมาตรา 18 ปรากฏตามวรรคหนึ่งของมาตราดังกล่าว ดังนี้ มาตรา 18 ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่าการกระทำความผิดตามพระราชบัญญัตินี้ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด

1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ ทิวเอกสาร ข้อมูล หรือหลักฐานอื่นใด ที่อยู่ในรูปแบบที่สามารถเข้าใจได้

2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากหนังสือผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง⁵⁹

3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครอง หรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าการกระทำความผิดตามพระราชบัญญัตินี้ ในระบบคอมพิวเตอร์นั้นยังมีได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลระบบคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งข้อมูลคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรือใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ทำการถอดรหัสลับหรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

3.3.2.4 หลักการใช้อำนาจของพนักงานเจ้าหน้าที่

ประการแรก การใช้อำนาจต้องอยู่ภายใต้บังคับมาตรา 19 ด้วย

ประการที่สอง พนักงานเจ้าหน้าที่จะใช้อำนาจได้ต่อเมื่อเป็นกรณีที่มีเหตุอันควรเชื่อได้ว่าการกระทำความผิดตามพระราชบัญญัตินี้ หากเชื่อว่าการกระทำความผิดกฎหมายอื่นย่อมไม่เข้าเงื่อนไขตามมาตรา

⁵⁹ เรื่องเดียวกัน, หน้า 184.

ประการที่สาม การใช้อำนาจของพนักงานเจ้าหน้าที่ต้องใช้เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้หลักฐาน เกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิดมาลงโทษ คำว่าใช้เฉพาะที่จำเป็นหมายความว่าถ้าไม่ใช้อำนาจนั้น ๆ ก็ไม่ได้มาซึ่งพยานหลักฐานนั้น ดังนั้นจำเป็นต้องใช้อำนาจ

ประการที่สี่ การใช้อำนาจของพนักงานเจ้าหน้าที่ใน 5 อนุมาตราต่อไปนี้ต้องอนุญาตศาล และศาลมีคำสั่งอนุญาตตามคำร้องก่อนแล้ว พนักงานเจ้าหน้าที่จึงจะสามารถดำเนินการได้ (ภายใต้บังคับมาตรา 19) คือ เหตุที่เป็นเช่นนี้เนื่องจากเห็นว่าการใช้อำนาจของพนักงานเจ้าหน้าที่อาจมีการกระทบกระเทือนต่อสิทธิเสรีภาพของบุคคลมากกว่าที่จะให้พนักงานเจ้าหน้าที่⁶⁰ใช้อำนาจเพียงลำพัง กล่าวคือ การให้ศาลตรวจสอบการใช้อำนาจของฝ่ายบริหารนั่นเอง หรือการกระทบกระเทือนต่อข้อมูลที่เกี่ยวข้องกับความลับทางการค้าหรืออาจกระทบต่อสิทธิประโยชน์ในทรัพย์สินทางปัญญาได้

1. การทำสำเนาข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์(กรณีในระบบคอมพิวเตอร์นั้นยังมีได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่)
2. การสั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้กับข้อมูลทางคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่
3. การตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลและสั่งให้บุคคลส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้
4. การถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคล หรือสั่งให้บุคคลทำการถอดรหัสลับหรือให้ความร่วมมือกับเจ้าพนักงานเจ้าหน้าที่ในการถอดรหัสลับ
5. การยึดหรืออายัดระบบคอมพิวเตอร์

ประการที่ห้า การใช้อำนาจของพนักงานเจ้าหน้าที่ 3 ประการ ดังต่อไปนี้ ไม่ต้องขออนุญาตศาลอันเป็นการใช้อำนาจตามบทบัญญัติมาตรา 18 (1) (2) หรือ (3) คือ พนักงานเจ้าหน้าที่ที่มีอำนาจมีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูลหรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าถึงได้ หมายความว่า “บุคคลที่ยึดถือหรือครอบครองเอกสาร ข้อมูล หรือหลักฐานใด ๆ ก็ตามต้องมีหน้าที่ชี้แจงหรือส่งข้อมูลหรือหลักฐานที่สามารถเข้าใจได้ย่อมหมายความว่า การส่งข้อมูลนั้น ๆ จะต้องส่งโปรแกรมหรือชุดคำสั่งในการอ่านการแปลข้อมูลนั้นมาด้วย มิฉะนั้นก็มิอาจเข้าใจได้เพราะหากคำสั่งหรือโปรแกรมหรือรหัสเป็นเรื่องเฉพาะบุคคลอื่นก็มิอาจรู้ได้ แต่หากโปรแกรมหรือคำสั่งทั่วไปก็ไม่จำเป็นต้องส่งมาก็ได้เช่นข้อมูล WORD, EXEL เหล่านี้เป็นเรื่องทั่ว ๆ ไป นอกเหนือจากส่งข้อมูลหรือเอกสารแล้วพนักงานเจ้าหน้าที่ยังมีอำนาจเรียกเรียกบุคคลมาให้ถ้อยคำหรือให้บุคคลชี้แจงเป็นหนังสือ หรือให้ส่งเอกสารหรือ วัตถุอื่นใดได้อีกด้วย⁶¹ การไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่

⁶⁰ เรื่องเดียวกัน, หน้า 184.

⁶¹ เรื่องเดียวกัน, หน้า 184.

ที่ตามมาตรา 18 (1) เป็นความผิดตามมาตรา (27) ต้องระวางโทษปรับไม่เกินสองแสนบาทและปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง⁶²

3.3.2.5 สาระสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้แก่ 17 ฐานความผิด ในการพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในส่วนของฐานความผิดนั้น อันครอบคลุมถึงการกระทำความผิดที่สำหรับการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์ในลักษณะต่าง ๆ ที่กระทบต่อความลับ (Confidentiality) ความครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบคอมพิวเตอร์และ ข้อมูลคอมพิวเตอร์ เช่น การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) การล่วงรู้มาตรการป้องกันการใช้ระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 6) การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) การดักจับข้อมูลคอมพิวเตอร์ (มาตรา 8) การรบกวนระบบคอมพิวเตอร์หรือ ข้อมูลคอมพิวเตอร์ (มาตรา 9 และมาตรา 10) การรบกวนระบบคอมพิวเตอร์ของบุคคลอื่นโดย ปกติสุข (มาตรา 11) การรบกวนระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่กระทบต่อความมั่นคงของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ และการบริการสาธารณะ (มาตรา 12) การเผยแพร่ชุดคำสั่งชั่วร้ายที่ใช้ในการกระทำความผิดตามมาตรา 5 ก่อนหน้านี้ (มาตรา 13) การเผยแพร่เนื้อหาอันไม่เหมาะสมหรือเป็นเท็จ เช่น ปลอมแปลง ข้อมูลคอมพิวเตอร์หรือ ทำข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือก่อให้เกิดความเสียหายหรือ ก่อให้เกิดความตื่นตระหนกกับประชาชน หรือเนื้อหาข้อมูลที่กระทบต่อสถาบันหรือการก่อการร้าย รวมทั้งข้อมูลคอมพิวเตอร์อันลามกทั้งหลาย และการ Forward หรือส่งต่อข้อมูลคอมพิวเตอร์ ข้างต้น (มาตรา 14) ผู้ให้บริการ ผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ต้องรับโทษด้วย (มาตรา 15) กำหนดฐานความผิดในเรื่องการติดต่อภาพของบุคคลอื่น อัน อาจให้เกิดความอับอายหรือเสียหาย ยกเว้นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำ ไม่มีความผิด (มาตรา 16) และรวมถึงการกระทำความผิดและกำหนดบทลงโทษในกรณีความผิดเกิดนอกราชอาณาจักร (มาตรา 17)

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นั้นได้กำหนดเกี่ยวกับบุคคลซึ่งเกี่ยวข้องในหลายส่วน เช่น ผู้ให้บริการซึ่งอาจหมายถึง ผู้ประกอบกิจการทางด้านโทรคมนาคม ผู้ให้บริการอินเทอร์เน็ต และผู้ให้บริการอื่น ๆ เช่น Web Hosting หรือหน่วยงานต่าง ๆ ที่ต้องกำหนดให้เจ้าหน้าที่หรือพนักงานผู้ดูแลระบบของตน เป็นต้น ทำหน้าที่ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ซึ่งเป็นข้อมูลสำคัญที่ใช้ใน การสืบสวนหรือสอบสวนเป็นระยะเวลา 90 วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่คอมพิวเตอร์ แต่ในกรณี จำเป็นเจ้าหน้าที่จะสั่งให้ผู้ให้บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ได้เกิน 90 วัน แต่ไม่เกิน 1 ปี เป็นกรณีพิเศษเฉพาะราย จากเดิมที่กำหนดให้เก็บ Traffic Data ไว้เพียง 30 วัน ไม่เกิน 90 วัน เท่านั้น อันเป็นระยะที่เหมาะสม และสอดคล้องกับความจำเป็นในการนำไปใช้ เพื่อประโยชน์ในการสืบสวนและสอบสวนทางปฏิบัติมากกว่า แต่เพื่อไม่ให้เป็นการกระทบกับผู้ให้บริการมากเกินไปในกฎหมายจึงได้

⁶² มาตรา 27 ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ตามมาตรา 18 หรือ มาตรา 20 หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา 21 ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

กำหนดให้รัฐมนตรี กระทรวงเทคโนโลยีสารสนเทศ และการสื่อสาร จัดทำประกาศว่า ใครบ้าง คือ "ผู้ให้บริการ" อันจะก่อให้เกิดภาระกับบุคคลหรือ หน่วยงานดังกล่าวเมื่อมีการประกาศหลังกฎหมาย บังคับใช้ต่อไป

โดยในเบื้องต้นการกำหนดว่า ใครบ้าง คือ ผู้ให้บริการนั้น ในเบื้องต้นไม่น่าจะ หมายถึงผู้ให้บริการทุกประเภท แต่น่าจะกำหนดให้หมายถึงแต่เพียงผู้ให้บริการกลุ่มใหญ่ ๆ เท่านั้น เช่น ผู้ประกอบกิจการทางด้านโทรคมนาคม หรือผู้ให้บริการอินเทอร์เน็ต เป็นต้น

นอกจากนั้น เพื่อให้รับกับประกาศเกี่ยวกับ “ผู้ให้บริการ” ในกฎหมายจึงได้ กำหนดให้รัฐมนตรี กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จัดทำประกาศเกี่ยวกับ “Traffic Data” ว่า หมายถึงอะไรบ้าง เพื่อผู้ให้บริการจะได้ไม่ต้องเก็บ Traffic Data ที่ไม่จำเป็น อันเป็นภาระ โดยใช้เหตุแต่อย่างใด อย่างไรก็ตาม ในการปฏิบัติหน้าที่ของ “พนักงานเจ้าหน้าที่” ซึ่งมีอำนาจหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นั้น จำเป็นต้องมีความรู้ความเข้าใจในลักษณะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรืออาชญากรรมทางคอมพิวเตอร์เป็นอย่างดี ในกฎหมายจึงได้กำหนดให้ “พนักงานเจ้าหน้าที่” ต้องมีคุณสมบัติซึ่งต้อง ผ่านการอบรมหลักสูตรที่กำหนดขึ้นเป็นพิเศษเพื่อให้สามารถทำหน้าที่ ตามกฎหมายฉบับนี้ได้ อย่างแท้จริง

3.3.3 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 เป็นกฎหมายรองรับในลักษณะ ที่เป็นเอกรูป และสอดคล้องกับมาตรฐานที่นานาประเทศยอมรับจึงจำเป็นต้องตราพระราชบัญญัตินี้ หมวด 4 ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ มาตรา 35 คำขอ การอนุญาต การจดทะเบียน คำสั่งทาง ปกครอง การชำระเงิน การ ประกาศ หรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือ โดยหน่วยงานของรัฐ ถ้าได้ กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนด โดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผล โดยชอบด้วยกฎหมาย เช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด

ในการออกพระราชกฤษฎีกาตามวรรคหนึ่ง พระราชกฤษฎีกาดังกล่าวอาจกำหนดให้ผู้ ประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้อง ได้รับใบอนุญาต แล้วแต่กรณีก่อนประกอบกิจการก็ได้ ในกรณีนี้ให้นำบทบัญญัติในหมวด ๓ และบท กำหนดโทษที่เกี่ยวข้องมาใช้บังคับโดยอนุโลมการรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ ให้เสมือนด้วยกระดาษเพื่อให้การดำเนินการใด ๆ ตามที่กฎหมายบัญญัติสามารถทำในรูปของข้อมูล อิเล็กทรอนิกส์ได้และมีผลผูกพันตามกฎหมาย

หมวด 1 ธุรกรรมทางอิเล็กทรอนิกส์ สาระสำคัญ ดังนี้

1. การรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ หลักการที่รับรองสถานะของ ข้อมูลอิเล็กทรอนิกส์นี้นับเป็นหลักการที่สำคัญที่สุดของพระราชบัญญัตินี้ก็ได้ โดยบัญญัติไว้ใน มาตรา 7 ว่า “ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใด เพียง เพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์” จะเห็นได้ว่าบทบัญญัตินี้เป็นหลักการ

พื้นฐานที่มีให้มีการเลือกปฏิบัติระหว่างสิ่งที่จัดทำขึ้นในรูปของหนังสือ หลักฐานเป็นหนังสือ หรือ ต้นฉบับ (Original) กับสิ่งที่จัดทำขึ้นในรูปของข้อมูลอิเล็กทรอนิกส์

2. การรับฟังพยานหลักฐาน และชี้แจงน้ำหนักพยานหลักฐาน ปรากฏอยู่ในมาตรา 11 บทบัญญัติในมาตรานี้เป็นการห้ามปฏิเสธการรับฟังพยานหลักฐานในกระบวนการพิจารณาด้วยเหตุที่ ข้อมูลนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ แต่ทั้งนี้ในเรื่องของการรับฟังพยานหลักฐานเป็นดุลยพินิจ ของศาลที่จะรับฟังหรือไม่ก็ได้ กฎหมายจึงต้องกำหนดหลักเกณฑ์ในการชี้แจงน้ำหนักพยานหลักฐานไว้ โดยให้พิจารณาถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง การเก็บรักษาหรือการสื่อสาร ข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการในการระบุตัวผู้ส่ง รวมถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง

3. สภาพปัญหาระหว่างประเทศ แต่ละประเทศมีภูมิหลังทางประวัติศาสตร์ศิลปธรรมจารีต ประเพณีต่างกัน ทำให้ส่งผล ถึงกฎหมายบางเรื่องแตกต่างกัน ซึ่งทำให้กฎหมายอาญาแต่ละประเทศ แตกต่างกันได้ อันทำให้เป็นอุปสรรคอยู่แล้ว ในกรณี ที่ว่าการกระทำอย่างหนึ่งอันเกิดในประเทศที่ บางเรื่องไม่ถือว่าเป็นความผิดแต่อีกประเทศหนึ่งถือว่าเป็นความผิด แม้แต่กฎหมายของแต่ละ ประเทศจะบัญญัติ การกระทำใดบนเครือข่ายอินเทอร์เน็ตว่าเป็นความผิดเหมือนกัน ก็ยังคงมีปัญหาที่ พบอีกคือปัญหาเขตอำนาจศาล

ปัญหาเรื่องเขตอำนาจศาลนี้เกิดเพราะอาชญากรรมคอมพิวเตอร์มีลักษณะ ไร้พรมแดน เกี่ยวพันกันได้หลายประเภท ผู้กระทำความผิด ผู้เสียหาย สถานที่เกิดการกระทำความผิด และ สถานที่เกิดผลแห่งการกระทำ ไม่จำเป็นต้องอยู่ในประเทศเดียวกัน ทำให้เกิดปัญหาว่า ความผิดที่ เกิดขึ้นในประเทศใด และจะสรุปได้อย่างไรว่าประเทศใดมีอำนาจสอบสวน จะ สอบสวนในมลรัฐหรือ สถานีดำรงไว้

ปัญหาความร่วมมือระหว่างประเทศในการดำเนินการคดี สืบเนื่องมาจากปัญหาเขตอำนาจ ศาล หากต้องสืบสวน สอบสวน และดำเนินคดีในประเทศหนึ่ง จะขอความร่วมมือกับประเทศที่ เกี่ยวข้องได้หรือไม่ และอยู่ในขอบเขตมากน้อยเพียงใด⁶³

นอกจากนี้ ประเทศไทยยังให้ความสำคัญกับอาชญากรรมไซเบอร์ (Cyber Crime) ภัยคุกคามของเศรษฐกิจรูปแบบใหม่ที่เป็นอาชญากรรมในรูปแบบใหม่ที่เข้าไปเกี่ยวข้องกับทุกพื้นที่ มนุษย์ใช้ชีวิต ในอนาคตต้องพัฒนากฎหมายให้ทันต่อการปราบปรามอาชญากรรมพวกนี้ เพราะ เป็นอันตรายมากต่อบุคคล และทำลายสังคมร้ายแรง จึงเป็นเรื่องที่ทุกหน่วยต้องให้ความร่วมมือกันพัฒนา กฎหมายเพื่อควบคุมการโจมตีทางไซเบอร์จึงมีการยกงานนโยบายความมั่นคงแห่งชาติ พ.ศ.2558-2562 เพื่อยกร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ⁶⁴

เหตุผล จากความก้าวหน้าทางเทคโนโลยีสารสนเทศซึ่งถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการสื่อสาร จึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและก่ออาชญากรรม

⁶³ ชัยวัฒน์ วงศ์วัฒนศานต์, ทวีศักดิ์ กอนันต์กุล และสุรางคณา แก้วจำนง, คำอธิบาย พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 (กรุงเทพฯ: สำนักเลขาธิการ คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, 2545).

⁶⁴ สภาความมั่นคงแห่งชาติ, มติคณะกรรมการรื้อยกร่างของสภาความมั่นคงแห่งชาติ, ครั้งที่ 2/2557, 29 สิงหาคม 2557.

ทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างอย่างรวดเร็วและปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายทั้งในระดับบุคคลและระดับประเทศ การป้องกันหรือรับมือกับภัยคุกคามหรือ ความเสี่ยงบนไซเบอร์จึงต้องอาศัยการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ดังนั้น เพื่อให้ประเทศไทยสามารถปกป้อง ป้องกันหรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมซึ่งกระทบต่อความ มั่นคงของชาติในมิติต่าง ๆ อันครอบคลุมถึงความมั่นคงทางการทหารความสงบเรียบร้อย ภายในประเทศ และความมั่นคงทางเศรษฐกิจได้อย่างเหมาะสม มีการดำเนินการที่รวดเร็วและมี ความเป็นเอกภาพ สมควรกำหนดให้มีคณะกรรมการขึ้นเพื่อกำหนดมาตรการด้านความมั่นคง ปลอดภัยไซเบอร์ของประเทศ ให้เป็นไปอย่างมีประสิทธิภาพ และให้เกิดผลสัมฤทธิ์⁶⁵

สรุปได้ว่าปัญหาในการรวบรวมและรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ตามประมวล กฎหมายวิธีพิจารณาความอาญาของพนักงานสอบสวนในประเทศไทยมีดังนี้ ปัญหาการค้นหรือการ เข้าถึงข้อมูลข้อมูลอิเล็กทรอนิกส์ จะทำอย่างไรพนักงานสอบสวนจะเข้าถึงพยานหลักฐานได้เร็วที่สุด เท่าที่จะทำได้ เพราะหลักฐานประเภทนี้มีธรรมชาติหรือลักษณะพิเศษ คือ ไม่มีรูปร่าง มองไม่เห็นและ สัมผัสด้วยตาเปล่าไม่ได้ อีกทั้งยังถูกลบ กำจัด ทำลาย แก้ไขหรือเปลี่ยนแปลงง่ายในเวลาอันสั้น ทำให้ ยากต่อการค้น รวบรวมเพื่อนำเสนอต่อศาล ปัญหาการยึดและการเก็บรักษาพยานหลักฐานว่าจะทำ อย่างไรให้ข้อมูลอยู่ในสภาพที่เป็นจริงมากที่สุด ไม่ถูกแก้ไขเปลี่ยนแปลง เพื่อนำเสนอต่อศาลให้มี ความน่าเชื่อถือ ปัญหาการนำเสนอพยานหลักฐานว่าจะนำเสนอในสถานะหรือฐานะเป็นพยานวัตถุ หรือพยานเอกสาร และทำอย่างไรจึงจะมีน้ำหนักพอที่ศาลจะรับฟังได้โดยปราศจากความเคลือบแคลง สงสัย

จากการที่ได้ศึกษาข้อมูลเกี่ยวกับมาตรการทางกฎหมายที่ให้อำนาจพนักงานสอบสวน ในการ รวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ของประเทศไทยนั้น พบว่าประเทศไทยยังต้องพัฒนา บุคลากรในสายนี้โดยการฝึกอบรมให้เกิดความรู้อย่างแท้จริงในการปฏิบัติงาน ตลอดจนควรจัดสัมมนา หรือเผยแพร่ข้อมูลให้ประชาชนเกิดความเข้าใจถึงวัตถุประสงค์ที่แท้จริงของ พระราชบัญญัติธุรกรรม อิเล็กทรอนิกส์และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เพื่อให้ บรรลุวัตถุประสงค์ในเรื่องความมั่นคงของชาติ และเพื่อให้เกิดเสถียรภาพของระบบสารสนเทศใน หน่วยงานทั้งภาครัฐ และเอกชนทั่วไป ไม่ให้เกิดความล่าช้าเมื่อเปรียบเทียบกับประเทศเพื่อนบ้าน ยกตัวอย่าง เช่น ประเทศเวียดนาม ที่กำลังพัฒนาด้านสารสนเทศแข่งกับประเทศไทยของเราอย่างน่า กลัว เราจึงควรหันมาจริงจังกับเรื่องความปลอดภัยข้อมูลให้มากกว่านี้ ไม่เช่นนั้นประเทศไทย จะเกิด คดีอาชญากรรมทาง คอมพิวเตอร์ มีความถี่มากขึ้น รูปแบบการกระทำความผิดก็มีความหลากหลายมากขึ้น และนับวันจะเป็นปัญหามากยิ่งขึ้นด้วย กรณีตัวอย่าง อาชญากรรมทางคอมพิวเตอร์ ในประเทศไทยที่ จะกล่าวต่อไปนี้เป็นเพียงการยกตัวอย่างรูปแบบในการกระทำความผิด หรือแผนประทุษกรรม ของคนร้าย ที่ใช้ในการกระทำความผิดในแต่ละรูปแบบ ซึ่งไม่ได้หมายความว่าแต่ละรูปแบบจะเกิดขึ้นเพียง 1 ราย โดย

⁶⁵ ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. , คำนวณที่ 12 ธันวาคม 2558 จาก <http://thainetizen.org/2015>

แต่ละรูปแบบอาจเกิดขึ้นหลายครั้ง ทั้งจากผู้กระทำผิดคนเดียวหรือหลายคน โดยจะขอยกตัวอย่างดังต่อไปนี้⁶⁶

จะเห็นได้ว่าการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ จะต้องมีการปรับใช้กฎหมายให้ตรงประเด็นข้อเท็จจริงและข้อกฎหมายมากที่สุด และศาลไทยสามารถรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ และลงโทษผู้กระทำผิดได้ แต่การรวบรวมพยานหลักฐานเพื่อดำเนินคดีกับอาชญากรรมทางอิเล็กทรอนิกส์หรืออาชญากรรมอินเทอร์เน็ต หรือไซเบอร์คราим (Cyber Crime) ค่อนข้างมีความยุ่งยากซับซ้อนกว่าพยานหลักฐานในคดีอาญาทั่วไป และเป็นที่ทราบกันดีว่าการติดต่อสัมพันธ์กันในเครือข่ายอินเทอร์เน็ตเชื่อมโยงจากแหล่งที่หนึ่งไปยังที่หนึ่ง ที่มีระยะทางไกลด้วยความรวดเร็วโดยไม่จำเป็นจะต้องพบเห็นหน้ากันแต่อย่างใด ดังนั้น ผู้กระทำความผิดเกี่ยวกับอาชญากรรมทางไซเบอร์สามารถเข้าไปติดต่อ สนทนา หลอกลวงผู้อื่น ในระบบอินเทอร์เน็ตมีหน้าตารูปร่างเช่นใด หรือเป็นบุคคลคนเดียวกันกับที่เห็นหรือไม่ ดังนั้นการสอบสวน จับกุม ผู้กระทำความผิด มาดำเนินคดีความผิดเกี่ยวกับอาชญากรรมทางอิเล็กทรอนิกส์ จึงมีความสำคัญอย่างยิ่งที่จะศึกษามาตรการทางกฎหมายที่หลากหลาย รวมถึงกฎหมายต่างประเทศดังที่กล่าวมาแล้วข้างต้น มาปรับปรุงแก้ไขกฎหมายของในต่อไป

⁶⁶ ญาณพล ยั่งยืน, อาชญากรรมทางคอมพิวเตอร์ (กรุงเทพฯ: ศูนย์ข้อมูลข้อสนเทศสำนักงานตำรวจแห่งชาติ, ม.ป.ป.).

บทที่ 4

วิเคราะห์มาตรการทางกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐาน อิเล็กทรอนิกส์ในประเทศไทย

ความเจริญก้าวหน้าทางเทคโนโลยีและการสื่อสารโดยเฉพาะการสื่อสารผ่านระบบอินเทอร์เน็ต ได้ถูกนำมาใช้เพื่อประโยชน์ทางด้านการสื่อสารในรูปแบบสื่อผสม (Multimedia) ไม่ว่าจะเป็นการส่งข้อความธรรมดา การส่งภาพและเสียง ส่งอีเมลล์ ส่งโทรสาร แฟกซ์ ข้อมูลอิเล็กทรอนิกส์ เช่น โปรแกรมคอมพิวเตอร์⁶⁷ ล้วนก่อให้เกิดพยานหลักฐานอิเล็กทรอนิกส์ได้ทั้งสิ้น เมื่อมีประโยชน์กับคนทั่วไป ก็มีกลุ่มบุคคลอีกกลุ่มหาประโยชน์โดยมิชอบจากเครือข่ายอินเทอร์เน็ต สิ่งที่มีคุณประโยชน์อย่างมากก็นำมาซึ่งปัญหามากมายตามมาเช่นเดียวกัน ปัญหาไม่ได้เกิดเฉพาะกับประเทศไทยเท่านั้น แต่ทุกประเทศต่างก็ประสบปัญหาการก่ออาชญากรรมผ่านเครือข่ายอินเทอร์เน็ต ต่างก็หามาตรการทางกฎหมายเพื่อป้องกันปราบปรามการกระทำความผิดรวมถึงแสวงหาพยานหลักฐานเพื่อดำเนินคดีกับผู้กระทำความผิด การดำเนินคดีกับอาชญากรรมทางเทคโนโลยีและการสื่อสาร หรืออาชญากรรมทางอิเล็กทรอนิกส์ มีปัญหาอยู่หลายประการ โดยเฉพาะอย่างยิ่งในการรวบรวมพยานหลักฐานในคดีที่เกี่ยวข้องกับอาชญากรรมทางอิเล็กทรอนิกส์ ความยุ่งยากของการรวบรวมพยานหลักฐานมีมากกว่าคดีอาญาทั่ว ๆ ไป เนื่องจากพยานหลักฐานอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์อันเป็นวัตถุไม่มีรูปร่างซึ่งง่ายต่อการทำลาย ยักยอก ถิ่นเท อีกทั้งอาชญากรส่วนใหญ่มีความชำนาญในการใช้เทคโนโลยี และในปัจจุบันจะเป็นการก่ออาชญากรรมข้ามชาติจึงเกิดปัญหาในเรื่องความร่วมมือ

ด้วยสภาพปัญหาดังที่กล่าวมาแล้วประกอบกับโครงสร้างทางกฎหมายของประเทศไทยกฎหมายที่ให้อำนาจหน้าที่แก่พนักงานสอบสวน ที่จะสามารถรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ยังไม่มีระเบียบปฏิบัติเอาไว้อย่างชัดเจน เพียงอาศัยการเทียบเคียงความผิดอื่นโดยใช้อำนาจไปตามประมวลกฎหมายวิธีพิจารณาความอาญานั้น ในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์จึงยังไม่ครอบคลุมถึงประเด็นการเข้าถึงข้อมูลทางอิเล็กทรอนิกส์ได้ จึงเกิดความขัดข้องในการรวบรวมพยานหลักฐาน เกิดความล่าช้าไม่ทันต่อการรวบรวมพยานหลักฐาน ในขณะที่อาชญากรส่วนใหญ่เป็นผู้เชี่ยวชาญด้านเทคโนโลยีสามารถทำลายพยานหลักฐานได้อย่างรวดเร็ว ด้วยสภาพปัญหาดังกล่าวมาแล้วข้างต้น ผู้เขียนซึ่งเป็นพนักงานสอบสวนจึงทำการวิเคราะห์สภาพปัญหาดังกล่าวเพื่อให้การรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ของประเทศไทยมีประสิทธิภาพยิ่งขึ้น

⁶⁷ พินัย ณ นคร, “กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์,”
บทบัญญัติ 56, 2 (มิถุนายน 2543): 1.

หากเปรียบเทียบกับต่างประเทศโดยเฉพาะสหรัฐอเมริกาและประเทศอังกฤษ พนักงานสอบสวนและเจ้าหน้าที่ตำรวจจะมีความรู้ความสามารถเชี่ยวชาญในด้านเทคโนโลยี ซึ่งในต่างประเทศเจ้าหน้าที่จะได้รับการอบรมทางเทคนิค เช่น โปรแกรมเมอร์ เพื่อการค้นพบข้อมูลที่จะใช้เป็นพยานหลักฐานได้ครบถ้วน ดังนั้น จึงได้ศึกษากฎหมายของต่างประเทศเพื่อหาแนวทางแก้ไขกฎหมายวิธีพิจารณาความอาญาของประเทศไทยเพื่อรับรองการปฏิบัติพนักงานสอบสวนทั่วไปต่อไป

4.1 วิเคราะห์กฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของประเทศไทย

4.1.1 ปัญหาการออกหมายค้นโดยศาล

หมายค้นของศาลถือเป็นหลักประกันการคุ้มครองสิทธิและเสรีภาพของประชาชนที่ดีที่สุด เพราะกระบวนการยุติธรรมมุ่งเน้นตรวจสอบการใช้อำนาจของเจ้าพนักงานมิให้กระทำเกินกว่าอำนาจและความจำเป็น โดยคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ตามบทบัญญัติแห่งรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550 มาตรา 4 โดยบัญญัติว่า ศักดิ์ศรีความเป็นมนุษย์ สิทธิเสรีภาพของบุคคลย่อมได้รับการคุ้มครอง⁶⁸ การค้นตัวบุคคลหรือกระทำได้อันกระทบต่อสิทธิและเสรีภาพตามวรรคหนึ่ง จะกระทำมิได้เว้นแต่มีเหตุตามที่กฎหมายบัญญัติ มาตรา 32⁶⁹ วรรคสี่ รวมถึงการเข้าไปในเคหสถานโดยปราศจากความยินยอมของผู้ครอบครองหรือการตรวจค้นเคหสถานหรือที่รโหฐาน จะกระทำมิได้ เว้นแต่มีคำสั่งหมายของศาล หรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ โดยกำหนดให้เฉพาะศาลเท่านั้นที่มีอำนาจออกหมายค้น มาตรา 33⁷⁰ ในทางปฏิบัติทำให้พนักงานสอบสวนเข้าถึงพยานหลักฐานได้ล่าช้าทำให้พยานหลักฐานถูกทำลายก่อนที่จะทำการค้น จึงสรุปได้ว่าพนักงานสอบสวนมีข้อจำกัดในเรื่องการค้น ดังนี้

4.1.1.1 เนื่องจากการค้นในที่รโหฐานต้องขอหมายค้นการขอหมายค้นก็ต้องมีเหตุอันควรเชื่อว่ามีพยานหลักฐานในสถานที่ที่จะค้นนั้น ในขณะที่สำนักงานเกี่ยวกับกระบวนการยุติธรรมต่าง ๆ ของไทยมีเขตที่ตั้งอยู่อย่างกระจัดกระจายมิได้อยู่ภายในเขตเดียวกันเหมือนต่างประเทศ การขอหมายศาลจึงต้องใช้เวลาเดินทาง ในขณะที่เดินทางอาชญากรก็อาจมีการแก้ไขเปลี่ยนแปลงหรือทำลายพยานหลักฐานไปแล้ว การที่หมายค้นให้ระบุสถานที่ค้นแต่อาชญากรประเภทนี้สามารถเข้าสู่ข้อมูลได้จากหลายสถานที่ในโลกเพื่อเข้ารระบบข้อมูลอิเล็กทรอนิกส์ที่เป็นพยานหลักฐานในคดีเพื่อทำลายหลักฐานโดยเฉพาะคนร้ายสมคบกันหลายคนยิ่งง่ายต่อการสื่อสารถึงกันให้ทำลายหลักฐานได้ง่าย

4.1.1.2 ลักษณะของพยานหลักฐานเนื่องจากคดีเกี่ยวกับอาชญากรรมทางเทคโนโลยีมีความละเอียดอ่อนจำเป็นต้องใช้ความรวดเร็ว การดำเนินการขอหมายค้นจึงเกิดความล่าช้า การที่รัฐประสงค์จะให้ความคุ้มครองสิทธิส่วนบุคคล จึงสร้างหลักประกันสิทธิของประชาชนด้วยการกำหนดมาตรการตรวจสอบการใช้ดุลพินิจของเจ้าพนักงานโดยองค์กรศาล และในส่วนอำนาจ

⁶⁸ มาตรา 4 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550

⁶⁹ มาตรา 32 วรรคสี่ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550

⁷⁰ มาตรา 33 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550

ในการออกหมายค้นกำหนดให้ศาลมีอำนาจแต่ผู้เดียว แม้แต่การค้นข้อมูลอิเล็กทรอนิกส์ที่ใช้อุปกรณ์เชื่อมต่อคอมพิวเตอร์เข้าไปค้นหาหลักฐานข้อมูลในเครื่องคอมพิวเตอร์ผู้ต้องสงสัยโดยไม่มีการรื้อลำเข้าไปในที่รื้อฐานก็ใช้หมายค้นเช่นเดียวกันเพราะถือว่าการรื้อลำเข้าไปในพื้นที่อันสงวนไว้เป็นสิทธิส่วนตัว

การดำเนินการขอหมายค้นจนถึงการอนุมัติหมายค้นโดยศาล ถือว่าเป็นขั้นตอนที่ล่าช้าขาดความคล่องตัวเมื่อเทียบกับความรวดเร็วของอาชญากรรมที่มุ่งจะทำลายพยานหลักฐานทางอิเล็กทรอนิกส์ เพียงปลายนิ้วสัมผัสเป็นพินัยพยานหลักฐานก็อาจถูกยักย้าย ถ่ายเท หรือถูกทำลายไปเรียบร้อยแล้ว

พนักงานสอบสวนใช้อำนาจได้ตามบทบัญญัติกฎหมายที่พอจะตีความเทียบเคียง แต่ไม่อาจใช้ได้โดยตรงคือประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 ประกอบมาตรา 105 ทำให้เกิดความล่าช้า แม้ว่าประเทศไทยจะมีหน่วยงานที่ตั้งขึ้นมาเพื่อดำเนินคดีกับอาชญากรรมทางเทคโนโลยีโดยตรงคือ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) กองบัญชาการตำรวจสอบสวนกลาง สำนักงานตำรวจแห่งชาติ แต่ก็ไม่สามารถแก้ปัญหาในการป้องกันปราบปรามและดำเนินคดีกับอาชญากรรมทางเทคโนโลยีได้เท่าที่ควร ยังคงเป็นความรับผิดชอบพนักงานสอบสวนทั่วไปที่จะต้องรับคำร้องทุกข์จากผู้เสียหายและประสานขอความร่วมมือจากพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ เท่านั้น

4.1.2 ปัญหาเกี่ยวกับการระบุรายละเอียดในหมายค้น

หมายค้น ถือเป็นหลักประกันการปฏิบัติหน้าที่ของเจ้าพนักงานมิให้กระทำการล่วงอำนาจตามอำเภอใจหรือลุแก่อำนาจ แต่การออกหมายค้นนั้นหากพนักงานสอบสวนใช้อำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญาก็จะมีข้อจำกัดมาก เช่น มาตรา 69 การขอหมายค้นศาลต้องระบุชัดเจนว่า สิ่งที่จะค้นนั้นใช้กระทำความผิด และจะค้นอะไร ส่วนไหนบ้าง ซึ่งระบุให้ชัดเจนได้ยากในส่วนของการคอมพิวเตอร์ แต่ครั้งจะใช้ มาตรา 92 ที่สามารถทำการค้นโดยไม่ต้องมีหมายศาลก็มีปัญหาอีกว่า ข้อมูลคอมพิวเตอร์มันเป็น “สิ่งของ” ตามนิยามกฎหมายหรือไม่ ปัญหาในการขอหมายค้นคือผู้จะทำการค้นหรือเจ้าพนักงานที่จะค้นต้องมีเหตุอันควรเชื่อ ว่าสิ่งของที่จะใช้เป็นพยานหลักฐานจะอยู่ในสถานที่ที่จะเข้าไปทำการค้น เหตุอันควรเชื่อเช่นนั้นต้องปรากฏให้เห็นในหมายค้นนั้นด้วย ซึ่งในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 60 (3) และ (4) (ค) คือ การให้ระบุสถานที่ที่จะค้น และลักษณะสิ่งของที่ต้องการค้นนั้นการขอหมายค้นจึงมีปัญหา 2 ประการ

4.1.2.1 การระบุสิ่งของที่จะค้นการยึด พยานหลักฐานที่เป็นข้อมูลในคอมพิวเตอร์และสื่ออิเล็กทรอนิกส์ เป็นสิ่งไม่มีรูปร่าง จะทำได้โดยวิธีใด หากข้อมูล ที่จะยึดมาจากกระบวนเครือข่ายคอมพิวเตอร์ของผู้อื่น และมีอยู่มากมายหลายแห่ง จะสามารถยึด ทั้งระบบได้หรือไม่ จึงน่าจะคิดว่าควรมีกฎหมายให้อำนาจพิเศษแก่เจ้าพนักงานในการตรวจค้น ยึด หลักฐานพยานหรือไม่

4.1.2.2 การระบุสถานที่ที่จะค้นในคำร้องขอหมายค้นจากศาล ตามมาตรา 69 การขอหมายค้นศาลต้องระบุชัดเจนว่า สิ่งที่จะค้นนั้นใช้กระทำความผิด และจะค้นอะไร ส่วนไหนบ้าง ซึ่งระบุให้ชัดเจนได้ยากในส่วนของการคอมพิวเตอร์⁷¹

4.1.3 ปัญหาการรับฟังพยานหลักฐานอิเล็กทรอนิกส์

การกระทำความผิดที่เกิดขึ้นจากอาชญากรรมทางอิเล็กทรอนิกส์ ก่อให้เกิดปัญหากับระบบกฎหมายภายในของประเทศต่าง ๆ ทั่วโลก เนื่องจาก การแสวงหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ถือเป็นมาตรการสำคัญ เพราะลักษณะของข้อมูลอิเล็กทรอนิกส์มีลักษณะที่ แตกต่างจากพยานหลักฐานทั่ว ๆ ไป ก่อให้เกิดปัญหาในการค้น การยึด สถานะในทาง พยานหลักฐานและการรับฟังเป็นพยานหลักฐานในศาล อาศัยเพียงกฎหมายวิธีพิจารณาความอาญา ซึ่งหมายถึงกฎหมายที่ว่าด้วยหลักเกณฑ์และวิธีการค้นหาความจริง อันเกี่ยวกับการกระทำความผิด และนำตัวผู้กระทำความผิดต่อกฎหมายอาญามาดำเนินการพิจารณา และลงโทษตามบทบัญญัติของกฎหมาย⁷² แม้การกระทำความผิดอาญาจะเป็นการกระทำที่กระทบต่อสังคมโดยรวม แต่การดำเนินคดีอาญาก็อ้อมมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลโดยหลีกเลี่ยงไม่ได้ จึงต้องคำนึงถึงกฎหมายวิธีพิจารณาความอาญาที่ให้ความคุ้มครองสิทธิและเสรีภาพของบุคคลในฐานะที่เขาเป็นส่วนหนึ่งของสังคมด้วย⁷³

ในคดีอาญาพยานหลักฐานทุกชนิดรับฟังได้ยกเว้นพยานหลักฐานที่ได้มาโดยมิชอบ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 สำหรับข้อมูลอิเล็กทรอนิกส์ที่ได้มาจากการค้นที่มีหมายพยานหลักฐานดังกล่าวยอมรับฟังได้ แต่ถ้าหากเป็นการค้นที่ไม่มีหมายค้นพยานหลักฐานที่ได้ก็ไม่สามารถรับฟังได้ เพราะความน่าเชื่อถือของพยานหลักฐานมีเพียงใดนั้น ก็ขึ้นอยู่กับวิธีการซึ่งนำพยานหลักฐาน โดยกฎหมายได้วางหลักการซึ่งนำหน้ามาตรา 227 คือ หลักพิสูจน์จนสิ้นสงสัย (In Dubio Pro Reo) และได้บัญญัติรับรองไว้ในรัฐธรรมนูญ มาตรา 33 วรรคหนึ่ง มีความผิด⁷⁴ โดยความสงสัยนั้นจะต้องเป็นความสงสัยในข้อเท็จจริง ไม่ใช่ในข้อกฎหมาย

ประเทศไทยมีหลักประกันโดยบัญญัติรับรองไว้ในรัฐธรรมนูญในการ ให้ความคุ้มครองสิทธิและเสรีภาพเป็นหลัก รัฐจะใช้อำนาจล่วงละเมิดสิทธิเสรีภาพของประชาชน ได้เป็นข้อยกเว้นในกรณีที่มิกฎหมายอำนาจ และเจ้าหน้าที่ของรัฐโดยชัดแจ้งจะต้องมี กระบวนการควบคุมที่แน่ชัดสามารถตรวจสอบได้ ดังนั้นแม้อาชญากรรมที่เกิดขึ้นมีความร้ายแรง จำเป็นจะต้องหาวิธีการในการแสวงหาพยานหลักฐานรูปแบบใหม่ ซึ่งเป็นการใช้อำนาจในการปราบปรามอาชญากรรมของเจ้าหน้าที่ของรัฐก็ยังคงต้องคำนึงถึงหลักเกณฑ์และรัฐธรรมนูญในการให้ความคุ้มครองสิทธิและเสรีภาพเป็นหลักรัฐจะ

⁷¹ อนินุพิไล เงินวิจิตร, ปัญหาในการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์ (วิทยานิพนธ์ปริญญาโทบริหารคดี คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2544), หน้า 69.

⁷² ณรงค์ ใจหาญ, หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1, พิมพ์ครั้งที่ 5 (กรุงเทพฯ: นิติธรรม, 2543), หน้า 22.

⁷³ สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, “แถลงการณ์เรื่องการดักฟังทางโทรศัพท์,” รพีสสาร 14, 4 (มกราคม-มีนาคม 2539): 34.

⁷⁴ คณิต ญ นคร, เรื่องเดิม, หน้า 56.

ใช้อำนาจล่วงละเมิดสิทธิเสรีภาพประชาชนไม่ได้ ยกเว้นในการกรณีที่มีกฎหมายบัญญัติอำนาจของเจ้าหน้าที่ของรัฐไว้โดยชัดแจ้ง จะต้องมีการควบคุมที่แน่นอน ดังนั้นแม้อาชญากรรมที่เกิดขึ้นในปัจจุบันจะมีความร้ายแรงมากและจะต้องมีวิธีการในการแสวงหาพยานหลักฐานรูปแบบใหม่ ๆ ซึ่งอำนาจในการปราบปรามอาชญากรรมของเจ้าหน้าที่ของรัฐ ก็ยังคงต้องคำนึงถึงหลักเกณฑ์และวิธีการที่กระทบสิทธิความเป็นบุคคลให้น้อยที่สุด

ข้อมูลทางอิเล็กทรอนิกส์ไม่อาจจะระบุได้ทุกกรณีว่าข้อมูลจะอยู่ในรูปแบบใด ประกอบด้วยสิ่งใดบ้างเพราะข้อมูลดังกล่าวมีลักษณะเป็นเพียงคลื่นกระแสไฟฟ้า และรหัสโปรแกรมที่ไม่สามารถจับต้องได้ทางกายภาพและอีกทั้งยังไม่สามารถระบุได้ว่าเก็บไว้ที่ใด ระบบอินเทอร์เน็ตอาจอยู่ในต่างประเทศ หรือมีการบันทึกข้อมูลต้นทางที่ต่างประเทศ แต่สถานที่ที่ดาวน์โหลดอาจอยู่ในประเทศไทยก็ได้ ดูเหมือนว่าการค้นหาพยานหลักฐานทางอิเล็กทรอนิกส์เพื่อระบุตัวผู้กระทำความผิดในโลกออนไลน์จะไม่ใช่ว่าเรื่องง่ายเพราะในทางเทคนิคอาจมีวิธีการหลบเลี่ยงได้หลายรูปแบบ แต่หากพนักงานสอบสวนมีความรู้ความสามารถและมีกฎหมายที่ให้อำนาจในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ได้อย่างรวดเร็ว ก็มีโอกาที่จะจับกุมผู้กระทำความผิดมาลงโทษตามกฎหมายได้

4.1.4 ปัญหาเกี่ยวกับเงื่อนไขเวลาที่จะทำการค้น

ปัญหาทางกฎหมายที่ว่า การค้นในที่รโหฐานต้องกระทำในเวลากลางวันเท่านั้น แต่เนื่องจากข้อมูลอิเล็กทรอนิกส์ ถูกลบ กำจัด ทำลาย แก้ไข เปลี่ยนแปลงได้โดยง่ายและรวดเร็วกว่าพยานหลักฐานอื่นหลายเท่า การค้นตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 96 บัญญัติว่า “การค้นในที่รโหฐานต้องกระทำระหว่างพระอาทิตย์ขึ้นและตก” หรืออีกนัยหนึ่งคือการค้นกระทำได้เฉพาะเวลากลางวันเท่านั้น ได้โดยไม่ต้องมีหมายค้น⁷⁵ ในส่วนที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์ ใช้อनुมาตรา (2) (4) และ (5) คือ เมื่อปรากฏความผิดซึ่งหน้ากำลังกระทำลงในที่รโหฐาน⁷⁶ การที่เข้าพนักงานสอบสวนทางไซเบอร์โดยบังเอิญขณะใช้บริการอินเทอร์เน็ตอยู่นั้น ถือเป็นความผิดซึ่งหน้าที่จะกระทำการค้นในที่ใดหรือไม่ เช่น การเข้าไปในห้องสนทนา (Chat Room) แล้วพบข้อความเชิญชวนในลักษณะเสนอขายบริการทางเพศอย่างโจ่งแจ้ง ดังนั้นถือว่าไม่ถือว่าเป็นความผิดซึ่งหน้า เพราะเจ้าพนักงานไม่ได้พบในขณะที่กระทำความผิด แต่เป็นการพบเมื่อกระทำความผิดได้เกิดขึ้นแล้ว ซึ่งกรณีเช่นนี้ถือว่าในทางกฎหมายต้องดำเนินการตามปกติคือการค้นต้องขอหมายค้นจากศาลก่อน ซึ่งเป็นไปได้ว่ากว่าจะได้หมายค้นข้อความในห้องสนทนานั้นอาจถูกลบทิ้งไปเรียบร้อยแล้ว กรณีเมื่อมีความสงสัยตามสมควรว่าสิ่งของที่ได้มาโดยการกระทำความผิดได้ซ่อนหรืออยู่ในนั้นประกอบทั้งต้องมีเหตุอันควรเชื่อว่าการกระทำนั้นหากเน้นเข้าไปอาจทำให้มีการย้ายสิ่งของออกจากที่รโหฐานนั้น

ข้อยกเว้นการเข้าค้นตามอนุมาตรานี้จะต้องปรากฏความจริงทั้งสองประการ คือ

1. มีความสงสัยว่าสิ่งของได้ซ่อนหรืออยู่ในนั้น และ
2. มีเหตุอันควรเชื่อว่าการที่จะดำเนินการในการออกหมายค้นจะเกิดความชักช้าอัน

⁷⁵ อนัญพิไล เงินวิจิตร, *เรื่องเดิม*, หน้า 69.

⁷⁶ มาตรา 69 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

อาจทำให้การโยกย้ายสิ่งของจากที่รโหฐานนั้นเสียก่อนได้ ข้อยกเว้นตามมาตรา 92 (2) นี้จำกัดเฉพาะกรณี “สิ่งของที่ได้มาโดยการกระทำผิด” เท่านั้น หมายถึงทรัพย์สินที่ได้มาจากการกระทำความผิดอาญาทั่วไป เช่น ทรัพย์สินที่ถูกปล้นหรือลักมา แต่อาชญากรรมทางไซเบอร์อาจเป็นข้อมูลความลับทางการค้าหรือข้อมูลส่วนบุคคลอื่นที่ลักลอบดัดแปลงมาเก็บไว้ใช้ประโยชน์โดยมิชอบ⁷⁷

4.1.5 ปัญหาในการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ของศาล

พยานหลักฐานที่ดี จะต้องสามารถทำให้ศาลสืบข้อสงสัยว่าจำเลยได้กระทำความผิดจริง และ “พยานหลักฐานที่ศาลจะรับฟังได้ต้องเป็นพยานหลักฐานที่ได้มาโดยชอบด้วยกฎหมาย และสามารถพิสูจน์ความผิดหรือความบริสุทธิ์ของจำเลยได้”⁷⁸

ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 บัญญัติไว้ว่า “พยานวัตถุ พยานเอกสารหรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิด หรือบริสุทธิ์ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานที่มีได้เกิดขึ้นการจูงใจมี คำนั่นสัญญา ชูเชิญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน” ส่วนสิ่งของที่มีไว้เป็นความผิด และสิ่งของที่ได้ใช้ในการกระทำความผิด เช่น เครื่องคอมพิวเตอร์ที่ใช้ในการนัดหมายเพื่อประกอบอาชญากรรม หรือใช้คอมพิวเตอร์ในการเข้าถึงข้อมูลของบุคคลโดยมิชอบแม้จะเป็นสิ่งของที่ต้องยึดเพื่อประกอบไว้ในสำนวน แต่ไม่ทำให้เจ้าพนักงานสามารถเข้าค้นได้โดยไม่มีหมายค้นแต่อาจเป็นเหตุให้ออกหมายค้นได้ตามมาตรา 69 (2) ได้เท่านั้น

มาตรา 69 (2) “เพื่อพบและยึดสิ่งของซึ่งมีไว้เป็นความผิด หรือได้มาโดยผิดกฎหมายหรือมีเหตุอันควรสงสัยว่าได้ใช้หรือตั้งใจจะใช้ในการกระทำความผิด” ทรัพย์สินของบุคคลที่อยู่ในความครอบครอง และเพื่อป้องกันการกล่าวอ้างกรณีเสียหายหรือสูญหาย ข้อยกเว้นนี้ยังไม่มี การต่อสู้หรือพิสูจน์ในศาล ดังนั้น จึงเป็นเรื่องที่ยังไม่ชัดเจนว่า เจ้าหน้าที่จะเข้าถึงพยานหลักฐานทางอิเล็กทรอนิกส์โดยปราศจากหมายค้นหรือไม่

จากการที่ได้วิเคราะห์มาแล้วข้างต้น จะเห็นได้ว่ากฎหมายวิธีพิจารณาความอาญาได้กำหนดให้เจ้าพนักงานทำการค้นได้เฉพาะเวลากลางวัน แต่บริการบนอินเทอร์เน็ตเปิดให้บริการตลอด 24 ชั่วโมง ดังนั้น การกระทำความผิดจึงอาจเกิดได้ตลอด 24 ชั่วโมง เช่นเดียวกัน ในขณะที่เจ้าหน้าที่ต้องรองานว่าพระอาทิตย์ขึ้นจึงจะทำการค้นได้ และข้อกฎหมายที่กำหนดให้ผู้มีอำนาจค้นต้องเป็นเจ้าพนักงานฝ่ายปกครองหรือตำรวจเท่านั้น โดยไม่เปิดช่องให้ผู้อื่นสามารถเข้ามาช่วยเจ้าพนักงานหรือตำรวจทำการตรวจค้นได้เลย นอกจากจะทำให้การค้นหาพยานหลักฐานทางอิเล็กทรอนิกส์ล่าช้า อีก

⁷⁷ 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

⁷⁸ การค้นและยึดคอมพิวเตอร์และการได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์ในการสอบสวนคดีอาญา แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา

ทั้งพยานหลักฐานทางอิเล็กทรอนิกส์ยังมีความซับซ้อน เพราะปัญหาจากเจ้าหน้าที่ยังขาดความรู้ความชำนาญ ในเรื่องคอมพิวเตอร์แล้ว พนักงานผู้ค้นเองที่อาจกลายเป็นผู้ทำลายพยานหลักฐานโดยรู้เท่าไม่ถึงการณ์⁷⁹

เมื่อพบข้อมูลที่จะใช้เป็นพยานหลักฐานแล้ว กฎหมายกำหนดวิธีการในการยึดและรักษาพยานหลักฐานไว้ว่า ต้องคงสภาพให้ตรงตามความเป็นจริงมากที่สุด ไม่ให้มีการแก้ไขเปลี่ยนแปลงใดๆ เพราะหากในทางปฏิบัติของเจ้าหน้าที่ขัดกับหลักการที่กฎหมายบัญญัติไว้ ก็จะทำให้การได้มาซึ่งพยานหลักฐานเป็นการมิชอบด้วยกฎหมาย และศาลสามารถไม่รับฟังได้

ดังนั้น สิ่งที่ต้องพิจารณาคือ ทำอย่างไรจะทำให้พยานหลักฐานอยู่ในสภาพที่เป็นจริงที่สุด เพื่อให้พยานมีน้ำหนัก น่าเชื่อถือ เนื่องจากข้อมูลสามารถลบ แก้ไขได้ง่ายโดยใช้เวลาเพียงสั้น ๆ และมักไม่เหลือร่องรอย จะทราบได้อย่างไรว่าข้อมูลดังกล่าวไม่ได้ถูกแก้ไขแต่งเติมมาก่อนเพื่อสร้างความเชื่อถือให้ศาลมั่นใจว่าสิ่งที่นำเสนอต่อศาลมีความถูกต้องเป็นสิ่งเดียวกับที่ยึดมาได้จากที่เกิดเหตุ กฎหมายได้ให้อำนาจพนักงานสอบสวนยึดไว้ซึ่งสิ่งของที่ค้นพบหรือบุคคลส่งมาให้ไว้ได้ เพื่อประโยชน์แก่การรวบรวมพยานหลักฐาน ได้แก่ สิ่งของที่ค้นพบว่ามีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิดหรือได้ใช้หรือสงสยว่าได้ใช้ในการกระทำความผิดแต่การยึดพยานหลักฐานที่เป็นข้อมูลในคอมพิวเตอร์ซึ่งเป็นสิ่งที่ไม่มีการปรุงแต่งด้วยวิธีการใด

ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 101 บัญญัติว่า “สิ่งของที่ยึดได้ในการค้นให้ห่อหรือบรรจุหีบห่อตราไว้ หรือทำเครื่องหมายไว้เป็นสำคัญ”⁸⁰ เพื่อป้องกันการสับเปลี่ยนพยานหลักฐาน แต่ข้อมูลคอมพิวเตอร์ไม่มีรูปร่าง ไม่สามารถบรรจุหีบห่อได้ ดังนั้น อาจใช้วิธียึดเครื่องคอมพิวเตอร์ที่มีข้อมูลนั้นอยู่ไว้แทน หรืออาจนำฮาร์ดดิสก์ที่มีข้อมูลนั้นเสนอต่อศาลก็ได้ อย่างไรก็ตาม การจะรู้ว่าฮาร์ดดิสก์นั้นมีข้อมูลอันเกี่ยวกับการกระทำความผิดหรือไม่ลำพังพนักงานสอบสวนเองอาจไม่สามารถเข้าใจ อาจทำให้ได้ข้อมูลไม่ครบถ้วน ถ้าไม่อาศัยผู้เชี่ยวชาญ นอกจากนี้ หากเป็นการพบข้อมูลที่ยึดในระบบเครือข่ายคอมพิวเตอร์ของผู้อื่นและมีอยู่มากมายหลายแห่ง ก็เกิดปัญหาในการปฏิบัติงานว่าจะสามารถยึดทั้งระบบได้หรือไม่

ประมวลกฎหมายวิธีพิจารณาความอาญา บัญญัติให้พนักงานสอบสวนมีอำนาจยึดไว้ซึ่งสิ่งของที่พบ หลักกฎหมายดังกล่าวมีประเด็นที่ต้องวิเคราะห์ว่า เมื่อพนักงานสอบสวนพบเครื่องคอมพิวเตอร์ส่วนบุคคลตามหมายค้น สิ่งที่พนักงานสอบสวนต้องการคือ ข้อมูลภายในเครื่องคอมพิวเตอร์นั้น ซึ่งเมื่อพนักงานสอบสวนสามารถเข้าถึงข้อมูลที่ต้องสงสยได้แล้ว จะต้องปฏิบัติตามด้วยความระมัดระวังโดยคำนึงถึงกรรมวิธีที่ถูกต้อง เพื่อกักหรือล็อกข้อมูลนั้นไว้ ให้อยู่และยึดพยานหลักฐานที่เกี่ยวข้องอย่างอื่นให้อยู่ในสภาพที่เป็นจริงที่สุด เพื่อให้สิ่งทั้งหลายที่ยึดถือนั้นมีน้ำหนักน่าเชื่อถือ ประมวลกฎหมายวิธีพิจารณาความอาญาได้กำหนดวิธีเก็บรักษาสิ่งของที่จะเป็นพยานหลักฐานในคดีอาญา

⁷⁹ กระมล ทองธรรมชาติ, *เรื่องน่ารู้เกี่ยวกับการปกครองและรัฐธรรมนูญของสหรัฐอเมริกา* (กรุงเทพฯ: โรงพิมพ์สังคมศาสตร์, 2513), หน้า 98.

⁸⁰ อนิยุพิไล เงินวิจิตร, *เรื่องเดิม*, หน้า 69.

กรณีอาชญากรรมไซเบอร์ สภาพที่แท้จริงของสิ่งที่ใช้เป็นพยานหลักฐานคือคลื่นแม่เหล็กไฟฟ้าที่เคลื่อนไหวอยู่ในภายในเครื่องคอมพิวเตอร์ ซึ่งไม่สามารถมองเห็นได้แต่มีความละเอียดอ่อนและไม่เสถียรภาพดังกล่าว นอกจากนี้การรวบรวมพยานหลักฐานทางคอมพิวเตอร์จำเป็นต้องมีการเปลี่ยนแปลงรูปลักษณะของข้อมูล เช่น การถ่ายโอนข้อมูลมาเก็บไว้ในแผ่นดิสก์ การพิมพ์ออกมาบนกระดาษโดยใช้เครื่องพิมพ์ ปัญหาในขั้นตอนการยึด ทำอย่างไรจึงจะสร้างความเชื่อถือได้ว่า

1. สิ่งที่เจ้าพนักงานนำเสนอขึ้นนั้นถูกต้องแท้จริงและเป็นสิ่งเดียวกันกับที่ยึดมาได้ ณ สถานที่เกิดเหตุ

2. สิ่งที่เจ้าพนักงานนำเสนอขึ้นมีความครบถ้วนบริบูรณ์เช่นเดียวกับวันที่ทำการยึด⁸¹

จากปัญหาในการยึดข้อมูลซึ่งบรรจุอยู่ในเครื่องอิเล็กทรอนิกส์ต่าง ๆ โดยเฉพาะคอมพิวเตอร์ การยึดพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ปัญหาสำคัญในการยึดรวบรวมพยานหลักฐาน ก็คือ ข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ ซึ่งเป็นข้อมูลที่ถูกจัดเก็บไว้ในสื่อบันทึกโดยอาศัยการจัดระเบียบของกระแสแม่เหล็กไฟฟ้า ซึ่งพนักงานสอบสวนทั่วไปมีอำนาจในการตรวจยึดได้มากนักอยู่แล้ว ความสำคัญของข้อมูลอิเล็กทรอนิกส์ จะเป็นสิ่งยืนยันได้ว่าการใช้เครื่องมือที่เก็บข้อมูลอิเล็กทรอนิกส์จึงเป็นพยานหลักฐานในการบ่งชี้ว่าผู้กระทำความผิด หรือผู้ต้องหาได้กระทำความผิดจริงหรือไม่ แต่ข้อมูลที่จัดเก็บในสื่ออิเล็กทรอนิกส์นั้น จะเป็นสิ่งที่ไม่มีรูปร่าง ทำให้เกิดปัญหาที่เจ้าหน้าที่ของรัฐอาศัยอำนาจทางกฎหมายอย่างไรในการยึดข้อมูลเหล่านั้น

ในปัจจุบันเป็นยุคของเทคโนโลยีข่าวสาร ถ้าใช้เทคโนโลยีให้เกิดประโยชน์ก็จะก่อให้เกิดประโยชน์ได้อย่างมากมายอีกทั้งยังนำเทคโนโลยีไปส่งเสริมให้มีการพัฒนาสังคมได้ในทุกด้าน การนำเทคโนโลยีมาใช้ยังทำให้ต้นทุนการผลิตน้อยลงทำให้บุคคลทั่วไปสามารถมีเครื่องคอมพิวเตอร์ที่มีสมรรถนะสูงมาใช้ในราคาที่ไม่แพง ดังนั้นจึงทำให้ผู้ประกอบการหรือองค์กรต่าง ๆ ซึ่งรวมถึงบรรดาอาชญากรทั้งหลายที่มุ่งสู่เครือข่ายทางอินเทอร์เน็ตเพื่อใช้ในการกระทำความผิดอาชญากรรมทางอิเล็กทรอนิกส์เพิ่มขึ้นอย่างรวดเร็วเป็นคู่ขนานกับการพัฒนาเครือข่ายทางเทคโนโลยีสารสนเทศ อีกทั้งอาชญากรรมที่กระทำบนอินเทอร์เน็ตมีองค์ประกอบความผิดทางอาญาที่ไม่ชัดเจน เป็นอาชญากรรมรูปแบบใหม่

ดังนั้น การสืบสวนติดตามผู้กระทำความผิดตามอย่างละเอียดและต่อเนื่องการพิสูจน์ทราบตัวบุคคลผู้ส่งและผู้รับข้อมูลที่แน่นอนเป็นเรื่องที่ยาก และส่วนใหญ่แล้วการกระทำความผิดเกิดขึ้นในสถานที่ปกปิดมิดชิดเจ้าหน้าที่ตำรวจจึงจำเป็นต้องมีหมายค้นเข้าไปตรวจสอบการกระทำความผิด ขั้นตอนและการรวบรวมพยานหลักฐานในการขอหมายค้นจากศาลก็มีความจำเป็นต้องมีระยะเวลาพอสมควร ซึ่งระยะเวลาที่พนักงานสอบสวนใช้มากเท่าใดในการขอหมายศาลก็จะเป็นระยะเวลาที่จะเปิดโอกาสให้อาชญากรรมทำลายพยานหลักฐานได้

⁸¹ การค้นและยึดคอมพิวเตอร์และการได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์ในการสอบสวนคดีอาญา แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา

4.2 วิเคราะห์กฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในต่างประเทศ

4.2.1 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาเป็นประเทศในกลุ่มที่ใช้ระบบกฎหมายคอมมอนลอว์ เป็นประเทศที่มีความเป็นประชาธิปไตยสูงและคำนึงถึงสิทธิเสรีภาพของพลเมืองเป็นสำคัญ ก็ประสบปัญหาไม่ต่างกับประเทศไทยในการขอพยานหลักฐานจากผู้ที่ครอบครองอยู่ ซึ่งทำให้รัฐต้องหามาตรการทางกฎหมายที่จะใช้บังคับ แต่ในขณะเดียวกันก็ต้องอยู่ภายใต้บังคับของกฎหมาย

เช่นกรณีตัวอย่าง บริษัทแอปเปิล ปฏิเสธคำร้องขอของ FBI ที่จะให้ทำการปลดล็อคโทรศัพท์ยี่ห้อ iPhone ของผู้ก่อการร้าย บริษัทแอปเปิล เชื่อว่าถ้าหากทำตามอาจก่อให้เกิดปัญหาในอนาคต เกี่ยวกับกรณีพิพาทนี้ทำให้ทาง FBI ได้ยื่นคำร้องต่อศาลแคลิฟอร์เนียให้ บริษัทแอปเปิล อนุญาตให้ทาง FBI สามารถเข้าถึงข้อมูลบน iPhone ได้ หลังจากเกิดคดีสะเทือนขวัญ ยิงกราดที่ San Bernardino เมื่อปี ค.ศ.2013 จนทำให้มีผู้เสียชีวิตถึง 14 ราย และ iPhone ของ Syed Rizwan Farook ซึ่งเป็นฆาตกร ได้ถูกล็อครหัสผ่านเอาไว้ ทำให้ทาง FBI ต้องการให้ บริษัทแอปเปิล สร้างโปรแกรมพิเศษขึ้นมาเพื่อให้ทาง FBI สามารถเข้าถึงข้อมูลดังกล่าวได้ แต่ทางบริษัทแอปเปิล ได้ปฏิเสธคำร้องขอของทาง FBI จนเป็นเหตุให้มีข้อพิพาทกัน FBI ได้ยื่นคำร้องต่อศาลแคลิฟอร์เนียในที่สุด แต่ก็ยังไม่ได้รับความร่วมมือ FBI จึงได้ผู้เชี่ยวชาญมาดำเนินการด้วยตนเองจนสามารถดึงข้อมูลได้ ซึ่งสำหรับบริษัทแอปเปิลแล้วหมายความว่าความปลอดภัยของข้อมูลในการเลือกใช้ iPhone ของลูกค้า นั้นหายไปทันที จนกลายเป็นบริษัทแอปเปิล ที่ต้องเร่งตรวจสอบหาวิธีการที่ทาง FBI ใช้จนสามารถเจาะเข้าไปดึงข้อมูล ได้เพื่อทำการปิดกั้นให้ได้โดยหลังจาก FBI สามารถดึงข้อมูลจาก iPhone ของผู้ก่อการร้ายในคดีที่ San Bernadino ได้นั้น FBI ก็ถูกฝ่ายตำรวจขอความช่วยเหลือเพราะตำรวจเองก็ต้องการที่จะให้ FBI ช่วยในการปลดล็อค iPhone ของผู้ร้ายในอีกหลาย ๆ คดีที่เกิดขึ้น เพื่อดูข้อมูลภายในบริษัทแอปเปิล จึงต้องรีบหาช่องโหว่ที่ทาง FBI นั้นเจาะเข้าไปดูข้อมูลให้เร็วที่สุด และทำการปิดช่องโหว่นั้นผ่าน Software Update จนปัจจุบัน Apple อาจจะขอคู่มือวิธีการดึงข้อมูลของ FBI ในคดีพ้อค้ายากับคำร้องขอให้ปลดล็อค iPhone 5s ได้

สิ่งเหล่านี้เป็นปัญหาในการรวบรวมพยานหลักฐานทั้งสิ้น จึงเป็นที่มาให้ประเทศสหรัฐอเมริกา กำหนดมาตรฐานขั้นต่ำให้เจ้าหน้าที่ที่บังคับใช้กฎหมายไว้อย่างชัดเจนไม่ว่าจะเป็นพนักงานตำรวจ พนักงานอัยการ การดำเนินคดีอาญาและการใช้อำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา ต้องผ่านการตรวจสอบจากศาล การค้น การยึดถือว่ามีผลกระทบต่อสิทธิเสรีภาพของผู้ถูกค้นหรือเจ้าของสถานที่ ดังนั้นการค้น การยึด ที่กระทำโดยไม่มีเหตุผลจะกระทำมิได้เว้นแต่มีเหตุอันสมควร

ในประเทศสหรัฐอเมริกาได้มีการพัฒนากฎหมายเกี่ยวกับอาชญากรรมทางอินเทอร์เน็ตอย่างต่อเนื่อง เพราะผลจากการลักลอบขโมยข้อมูล เช่น พวก (Hacker หรือ Cracker) การลักลอบโจรกรรมโดเมนเนม (Domain Name) ของผู้อื่นที่มีมูลค่ามหาศาล หรือพวกที่ปล่อยไวรัสโจมตีฐานข้อมูล (Data Base) ในหน่วยงานราชการ หรือเอกชน การกำหนดขอบเขตของการแสวงหาพยานหลักฐานของเจ้าหน้าที่ตำรวจจึงได้มีการกำหนดบทบัญญัติเกี่ยวข้องโดยตรงกับการปฏิบัติหน้าที่ของเจ้าพนักงาน ในการค้นและยึดในขณะที่ยานหลักฐานที่เป็นข้อมูลทางอิเล็กทรอนิกส์นั้นหากเข้าจนเกินไป ก็จะส่งผลร้ายมากกว่า ในเรื่องการค้นพยานหลักฐานทางอิเล็กทรอนิกส์ในช่วงแรก

สหรัฐอเมริกา มีกฎหมายคุ้มครองสิทธิส่วนบุคคลในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ (The Electronic Communication Privacy Act) แต่กฎหมายดังกล่าวกลับเอื้อประโยชน์ให้กับผู้กระทำผิดกฎหมาย และไม่สามารถสืบสวนหาตัวผู้กระทำผิดได้ อีกทั้งสหรัฐอเมริกายังเป็นประเทศแรก ๆ ที่รับรู้ถึงมหันตภัยร้ายของอาชญากรรมทางไซเบอร์ การก่อการร้ายที่รุนแรงยากต่อการสืบสวนติดตาม ผู้กระทำความผิดมาลงโทษ ในปี ค.ศ.1968 สภาองเกรสจึงอนุมัติให้ออกมาตรการในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ ในกรณีพยานหลักฐานอิเล็กทรอนิกส์ ที่มีลักษณะเฉพาะที่ถูกจำกัดลบ ทำลาย แก้ไข เปลี่ยนแปลงได้ในเวลาอันรวดเร็ว กว่าพยานหลักฐานทั่วไปน่าจะเป็นสภาวะการณ์ฉุกเฉินอย่างยิ่งเพื่อให้เจ้าพนักงานสามารถเข้าค้นและยึดพยานหลักฐานได้ในทันทีที่แน่ใจว่าเกี่ยวข้องกับการกระทำความผิดโดยอ้อมยักเว้นที่ไม่ต้องมีหมายค้น หรือสามารถค้นได้ก่อนค่อยขอหมายค้นภายหลัง ส่วนในเรื่องรายละเอียดของหมายค้นก็จะระบุภาพรวมกว้าง ๆ ไม่ต้องระบุรายละเอียดมากนัก หรือไม่จำเป็นว่าจะค้นอะไรบ้างในเครื่องคอมพิวเตอร์เป็นต้น

สำหรับประเทศสหรัฐอเมริกาได้มีการพัฒนากฎหมายที่ใช้สำหรับการค้นคอมพิวเตอร์และการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์มาอย่างต่อเนื่อง เพราะโครงสร้างกฎหมายของประเทศสหรัฐอเมริกาส่วนใหญ่มีหลักแตกต่างกันระหว่างเทคโนโลยีการสื่อสารใช้เสียง เช่น โทรศัพท์ กับการสื่อสารที่ไม่ใช้เสียง เช่น Fax หรือ E-mail จึงมีหลักการในการควบคุมและคุ้มครองสิทธิส่วนบุคคล (Privacy Right) แตกต่างกัน แต่ปัจจุบันปรากฏว่าข้อมูลและเสียงอาจปรากฏว่าร่วมกันในกาสื่อสารหนึ่งในระบบการปรับเปลี่ยนต่อไปเช่นที่ได้มีการแก้ไขเปลี่ยนแปลงใน The USA Patriot Act of 2001 เพื่อให้อำนาจพนักงาน มีอำนาจในการดักฟังการสื่อสารในเทคโนโลยีรูปแบบใหม่นั้นเอง

ประเทศสหรัฐอเมริกา ยังมีข้อยกเว้นที่ไม่ต้องขอหมายค้นอีกด้วย เช่น

1. ความยินยอม ซึ่งความยินยอมเกิดขึ้นได้หลายกรณี รวมถึงแถบข้อความแจ้งเตือนเมื่อเข้าสู่ระบบ (A log In Banners) ข้อตกลงการเข้าใช้ (Terms-of-Use Agreement) หรือนโยบายบริษัท และสิ่งที่ต้องพิจารณาด้วยคือ เครื่องคอมพิวเตอร์เครื่องหนึ่งสามารถใช้ User ได้หลาย User และความยินยอมของ User คนหนึ่งก็เพียงพอแล้วสำหรับความยินยอม สำหรับการตรวจค้นในพื้นที่ส่วนบุคคล (Private Area) ของเครื่องคอมพิวเตอร์นั้น ๆ ก็ถือว่าความยินยอมดังกล่าวเพียงพอที่จะตรวจค้นพื้นที่ทั่วไป อย่างไรก็ตามความยินยอมอาจมีข้อจำกัดได้ ภายใต้เงื่อนไขของประเภทระยะเวลา และตัวแปรอื่น ๆ ความยินยอมอาจยกเลิกเพิกถอนเมื่อใดก็ได้⁸²

2. กรณีมีเหตุฉุกเฉิน เพื่อป้องกันการทำลายพยานหลักฐาน หน่วยงานบังคับใช้กฎหมายสามารถยึดอุปกรณ์เก็บข้อมูลอิเล็กทรอนิกส์ และในบางคดีที่มีภัยอันตรายฉุกเฉินที่อาจจะทำให้สูญเสียชีวิต หน่วยงานบังคับใช้กฎหมายสามารถที่จะตรวจค้นแบบมีข้อจำกัด ณ ขณะนั้น เพื่อรักษาข้อมูลนั้นไว้ได้

⁸² การค้นและยึดคอมพิวเตอร์และการได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์ในการสอบสวนคดีอาญา แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา

3. กรณีมีการตรวจค้นเพื่อจับกุม โดยมีความจำเป็นเพื่อคุ้มครองความปลอดภัยให้กับเจ้าหน้าที่บังคับใช้กฎหมาย หรือเพื่อการเก็บรักษาพยานหลักฐาน ซึ่งการตรวจค้นเพื่อจับกุมนี้รวมถึงการตรวจค้นอุปกรณ์เก็บข้อมูลอิเล็กทรอนิกส์ เช่น โทรศัพท์เคลื่อนที่ ที่ถือครองโดยเป้าหมาย

4. กรณีตรวจค้นทรัพย์สิน ช้อยกเว้นในการตรวจค้นทรัพย์สินมีขึ้นเพื่อป้องกัน

ในประเทศสหรัฐอเมริกา การบังคับใช้กฎหมาย การยึดพยานหลักฐานทางอิเล็กทรอนิกส์นั้น อาจกล่าวได้ว่ามีแนวโน้มที่จะผ่อนคลายจากหลัก The Exclusionary Rule ซึ่งเป็นหลักฐานเกณฑ์ที่ศาลสูงไว้วางไว้เพื่อให้ The Fourth Amendment มีประสิทธิภาพในการเป็นหลักประกันสิทธิส่วนบุคคลของประชาชนชาวสหรัฐอเมริกาให้พ้นจากการรังละเมิดจากการปฏิบัติหน้าที่ของเจ้าพนักงาน โดยไม่มีเหตุผลและไม่จำเป็น โดยการที่ศาลจะไม่ยอมรับพยานหลักฐานที่ได้มาจากการยึดอันมิชอบด้วยกฎหมายรวมทั้งพยานหลักฐานโดยอ้อมอันสืบเนื่องมาจากพยานหลักฐานที่มิชอบนั้น

The Fourth Amendment เป็นบทบัญญัติที่ว่าด้วยสิทธิส่วนบุคคลของเอกชน อันได้แก่ สิทธิที่จะปลอดภัยจากการรุกรานเสรีภาพความมั่นคงและทรัพย์สินโดยไม่มีเหตุผลและไม่จำเป็นซึ่งถือเป็นเรื่องที่สำคัญมากสำหรับประชาชนชาวสหรัฐอเมริกา “กระบวนการการออกหมาย” จึงถือเป็นหลักประกันการคุ้มครองสิทธิส่วนบุคคลที่ดีได้ส่วนหนึ่งเพราะจะต้องผ่านการตรวจสอบจากผู้พิพากษามาจิตรตร ในเรื่อง “มีเหตุอันควรเชื่อ” (Probable Cause) ภายใต้คำสาบานของเจ้าพนักงานผู้ที่จะทำการยึดในประเทศสหรัฐอเมริกา การยึดมีวัตถุประสงค์เพื่อที่จะรวบรวมพยานหลักฐาน ซึ่งบทบัญญัติใน Title 18 แห่ง Federal Rules of Criminal Procedure Rule 41 ได้บัญญัติเกี่ยวกับเหตุในการยึดสิ่งของไว้ 4 กรณี ดังนี้

1. ทรัพย์สินซึ่งเป็นพยานหลักฐานในการกระทำความผิด
2. สิ่งของผิดกฎหมาย สิ่งของที่ได้มาจากการกระทำความผิด หรือสิ่งของอื่นใดที่ครอบครองไว้เป็นความผิด
3. ทรัพย์สินที่ทำขึ้นเพื่อใช้ หรือเจตนาที่จะใช้ หรือได้ใช้เป็นเครื่องมือในการกระทำความผิด

4. บุคคลซึ่งจะต้องถูกจับกุมตามหมายจับหรือบุคคลซึ่งถูกควบคุมโดยมิชอบด้วยกฎหมาย⁸³

จากบทบัญญัติในรัฐธรรมนูญดังกล่าวเห็นได้ว่า “probable cause” เป็นเงื่อนไขในการยึดหากปราศจาก Probable cause แล้ว ย่อมมีผลให้การออกหมายไม่ถูกต้องเมื่อไม่มีการออกหมายแล้ว การยึดที่จะกระทำไปโดยปราศจากหมายย่อมเป็นการดำเนินการที่ไม่ต้องต้องเช่นกัน สำหรับความหมายของคำว่า probable cause มีความหมายว่าอย่างไรนั้น Black’s Law Dictionary ได้ให้นิยามคำว่า probable cause ไว้เป็นสองนัยด้วยกันได้แก่

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

⁸³ อณัญพิไล เงินวิจิตร, *เรื่องเดิม*, หน้า 73.

นัยที่สองพิจารณาตามเจตนารมณ์ของรัฐธรรมนูญแก้ไขเพิ่มเติมครั้งที่ 4 หมายความว่า ข้อสรุปที่มากกว่าความสงสัยลอย ๆ แต่น้อยกว่าพยานหลักฐานที่ใช้พิสูจน์การกระทำความผิด (Which amounts to more than a bare suspicion but less than evidence that would justify a conviction)⁸⁴

จากคำอธิบายดังกล่าวก็ยังไม่ได้ข้อสรุปถึงความหมายของคำว่า Probable Cause เป็นที่ยุติ แต่อย่างใด ดังนั้นการหาความหมายของถ้อยคำดังกล่าวจึงอาจพิจารณาได้จากคำตัดสินของศาลฎีกา สหรัฐอเมริกา ในคดี Carroll v. United States (267 U.S.132 (1925)) ซึ่งศาลได้วินิจฉัยไว้ว่า probable cause เกิดขึ้นเมื่อข้อเท็จจริงและพฤติการณ์แวดล้อมต่าง ๆ ของตัวเจ้าหน้าที่ตำรวจที่ทราบเองและโดยที่เจ้าหน้าที่ตำรวจมีข้อมูลข่าวสารที่เพียงพอออกมายึดสิ่งของที่เชื่อว่าอยู่ในสถานที่นั้นหรืออยู่ที่บุคคลนั้นโดยความเชื่อที่ชอบด้วยเหตุผล ต่อมาในคดี Brinegar v. United States (338 U.S. 160 (1949)) ได้วินิจฉัยไว้ว่า Probable Cause ปรากฏเมื่อข้อเท็จจริงและพฤติการณ์แวดล้อมจากการสืบทราบของเจ้าหน้าที่ตำรวจและเจ้าหน้าที่ตำรวจที่มีข้อมูลข่าวสารที่หน้าเชื่อถือ โดยมีเหตุผลเพียงพอที่จะออกมายึด โดยที่วิญญูชนเชื่อว่ามีความผิดอาญาเกิดขึ้นหรือก่อกำเนิดตามความหมายที่ศาลฎีกาของสหรัฐอเมริกา ได้วินิจฉัยไว้ในคดีดังกล่าวเป็นที่เห็นได้ว่า Probable cause ความหมายทางภาวะวิสัย (objective) และไม่ได้เกิดขึ้นเองแต่ขึ้นอยู่กับพิจารณาของเจ้าหน้าที่ผู้ทำการยึดสิ่งของหรือผู้พิพากษาผู้มีอำนาจ⁸⁵

ในส่วนของการให้ความหมายของคำว่า Probabl Cause ซึ่งเป็นถ้อยคำในบทบัญญัติรัฐธรรมนูญแก้ไขเพิ่มเติมครั้งที่ 4 อันเป็นเงื่อนไขในการยึดสิ่งของ เมื่อนำมาเทียบเคียงกับหลักการที่กำหนดไว้ในประมวลวิธีพิจารณาความอาญาแล้วน่าจะมีความหมายเทียบเคียงได้กับบทบัญญัติตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 59/1 ที่ว่า “ก่อนออกหมายจะต้องปรากฏพยานหลักฐานตามสมควรที่ทำให้ศาลเชื่อได้ว่ามีเหตุที่จะออกหมาย เพราะ ในการพิจารณาการยึดสิ่งของ ย่อมมาจากข้อเท็จจริงและพฤติการณ์แวดล้อมต่าง ๆ ที่น่าเชื่อถือและมีเหตุผลเพียงพอที่จะยึดได้หรือไม่ ซึ่งเมื่อพิจารณาตามบทบัญญัติในมาตรา 59/1 แล้ว หมายความว่าบทบัญญัติดังกล่าวกำหนดให้มีการเสนอพยานหลักฐานที่เพียงพอที่ทำให้หน้าเชื่อว่ามีวัตถุสิ่งของที่ต้องการยึด

4.2.2 ประเทศอังกฤษ

ประเทศอังกฤษนั้น ในการตรวจค้นเรื่องคอมพิวเตอร์พีซีในทีรโหลฐานก็ดี การตรวจค้นข้อมูลอันเป็นความลับในระบบเครือข่ายดังกล่าวแล้วก็ดี เมื่อทำการตรวจค้นมาได้แล้วตำรวจอังกฤษจะยึดเครื่องคอมพิวเตอร์เป็นพยานหลักฐานได้หรือไม่ ต้องพิจารณาตาม PACE มาตรา 18 และมาตรา 19 ที่ว่า

PACE มาตรา 18 “เมื่อค้นแล้วตำรวจต้องทำบันทึกการค้น และบันทึกรายการสิ่งของที่ค้นละยึด รายการเหล่านั้นผู้ค้นต้องมอบให้แก่เจ้าของบ้าน เมื่อผู้นั้นร้องขอ”

⁸⁴ Black’s Law Dictionary, 7th ed. (St.Paul, Minn: West Group, 1999), p. 1219.

⁸⁵ Charles H. Whitebread and Christopher Slobogin, Procedure: An Analysis of Cases and Concepts, 4th ed. (New York: Foundation Press, 2000), p. 141.

PACE มาตรา 19 “ตำรวจยึดวัตถุที่มีเหตุผลเชื่อว่าพยานหลักฐานที่เกี่ยวกับการสอบสวนหรือความผิดอื่น หรือมีความผิดอื่นรวมอยู่ด้วย หรือมีความจำเป็นต้องยึดเพื่อป้องกันการเคลื่อนย้ายซ่อนเร้น หรือทำลายหลักฐาน”

ดังนั้น เครื่องคอมพิวเตอร์ที่ยึดได้เป็นวัตถุที่ใช้เป็นพยานหลักฐานเกี่ยวกับการสอบสวนที่ตำรวจอังกฤษมีอำนาจยึด นอกจากนี้ข้อมูลที่เก็บไว้ฮาร์ดดิสก์ภายในเครื่องก็เป็นวัตถุที่สามารถยึดได้เช่นกัน เว้นแต่ว่าข้อมูลที่เป็นความลับ ซึ่งจะต้องพิจารณาเรื่องกฎหมายคุ้มครองข้อมูลส่วนบุคคลประกอบ อีกทั้งผู้เขียนยังเห็นว่าปกติข้อมูลคอมพิวเตอร์ในกฎหมายลักษณะพยานของอังกฤษไม่สามารถพิสูจน์ด้วยตัวมันเองในกระบวนการพิจารณาคดีอาญาได้ เนื่องจากโดยทั่วไปแล้ว รายงานที่ประมวลผลจากคอมพิวเตอร์ (Printouts) จะเป็นพยานบอกเล่า (Hearsay) เพราะเป็นสิ่งที่ทำด้วยมือมนุษย์ ซึ่งห้ามรับฟังตามกฎหมายอังกฤษ Criminal Justice Act 1988 มาตรา 24 แต่ในทางกลับกันคอมพิวเตอร์อาจใช้เป็นเครื่องกล หรือเครื่องมือในการคำนวณ Printouts จึงไม่น่าจะเป็น Hearsay เสมอไป ถ้าผู้ยื่นพยานหลักฐาน ดังกล่าวได้แสดงให้เห็นว่า คอมพิวเตอร์ได้ถูกใช้ในในธุรกิจอันเป็นปกติ และข้อมูลดังกล่าวได้รับการประมวลผลโดยคอมพิวเตอร์อย่างเป็นปกติ

ในคดีอาญาพยานหลักฐานทางคอมพิวเตอร์จะพิจารณาจากกฎหมาย The Police and Criminal Evidence Act 1984 มาตรา 69 ในฐานะที่ยื่นพยานประเภทนี้แบบพยานเอกสาร

มาตรา 60 วางหลักไว้ว่า ในการดำเนินกระบวนการพิจารณาตามกฎหมาย พยานหลักฐานที่ประมวลผลโดยคอมพิวเตอร์ เอกสารที่ประมวลผลโดยคอมพิวเตอร์จะไม่ยอมให้นำเข้าพิสูจน์ข้อเท็จจริงเว้นแต่

1. ไม่มีเหตุผลที่จะเชื่อได้ว่าพยานเอกสารนั้นมีข้อผิดพลาดจากการใช้คอมพิวเตอร์นั้นประมวลผล
2. ในขณะเวลาที่คอมพิวเตอร์ประมวลผล กระบวนการในการพิมพ์เอกสารไม่เกิดความผิดพลาด และมีความถูกต้องแท้จริงในเนื้อหา

ในคดีอาญานี้ยอมรับฟังพยานหลักฐานจากการประมวลผลของคอมพิวเตอร์ ถ้าไม่มีความผิดพลาดในกระบวนการทำงานของคอมพิวเตอร์ และพยานนั้นมีความถูกต้องแท้จริงไม่ถูกแก้ไขเปลี่ยนแปลงในเนื้อหาที่รับฟังได้ สำหรับประเทศอังกฤษแล้วหลักนี้ในคดีอาญากลับเป็นบรรทัดฐานในคดีแพ่ง เมื่อวิเคราะห์หลักการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ในกฎหมายอังกฤษ ดังกล่าวแล้วจะเห็นว่าจำเป็นต้องมีการรับรองความถูกต้องแท้จริงของพยานหลักฐานที่เป็นเอกสารหรือพยานวัตถุซึ่งเป็นหลักเก่าแก่ของกฎหมายคอมมอนลอว์อยู่แล้ว การรับรองความถูกต้องแท้จริงนี้ต้องมีลายมือชื่อบุคคลที่รับผิดชอบในกระบวนการทำงานของคอมพิวเตอร์นั้น

โดยสรุป การค้นและยึดพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในประเทศอังกฤษ ตำรวจอังกฤษมีอำนาจกระทำได้โดยใช้อำนาจตามกฎหมาย The Police and Criminal Evidence Act 1984 ดังที่กล่าวมาแล้ว ซึ่งทั้งบทบัญญัติเกี่ยวกับการตรวจค้นในเคสสถาน และการตรวจค้นข้อมูลที่เป็นความลับ สำหรับส่วนที่เป็นความลับหรือข้อมูลส่วนบุคคลต้องพิจารณาประกอบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (The Data Protection Law 1998) ด้วย สำหรับกฎหมายลักษณะพยานนั้นอังกฤษมีบทบัญญัติในเรื่องการรับฟังพยานจากคอมพิวเตอร์ไว้ชัดเจนดังที่กล่าวมาแล้ว

4.2.3 ประเทศสหพันธ์สาธารณรัฐเยอรมนี

ประเทศสหพันธ์รัฐเยอรมนี เป็นกลุ่มประเทศที่ใช้ระบบกฎหมายซีวิลลอว์ ก็มีปัญหาในเรื่องการค้นเช่นเดียวกัน การค้นข้อมูลอิเล็กทรอนิกส์ ในระบบ LAN, ระบบ WAN และระบบอินเทอร์เน็ต ตำรวจ หรือพนักงานอัยการ ก็ต้องมีหมายค้น โดยหมายค้นต้องระบุรายละเอียดไว้ดังนี้

มาตรา 107 “รายละเอียดในหมายค้นจะต้องระบุมูลเหตุแห่งการค้น บุคคล และสิ่งของที่จะต้องค้นด้วย” ซึ่งถือว่าประสบปัญหาเช่นเดียวกันกับประเทศอื่น ประเทศเยอรมัน จึงใช้มาตรการทางกฎหมายคล้ายกับประเทศอื่นคืออ้างเหตุเร่งด่วนในกรณีที่เป็นพยานหลักฐานทางอิเล็กทรอนิกส์ นอกจากนี้ยังจัดตั้งองค์กรทำหน้าที่รวบรวมพยานหลักฐาน เช่นกรณีเร่งด่วนการส่งให้ค้นอาจทำได้โดยพนักงานอัยการ หรือพนักงานตำรวจผู้ช่วยอัยการ รวมถึงประเทศเยอรมันมีกฎหมายวิธีพิจารณาความอาญา มาตรา 99 ได้ให้อำนาจค้น ยึดสิ่งของที่เป็นจดหมาย ไปรษณีย์ โทรเลข และล่วงรู้ความลับของผู้ต้องหา เพื่อประโยชน์ในการสอบสวน สรุปคือ การได้มาโดยวิธีใดไม่สำคัญไปกว่าประโยชน์ของการสอบสวน ซึ่งตำรวจเยอรมันสามารถใช้กฎหมายข้อนี้และขอความร่วมมือจาก ISP การดำเนินการค้นในที่สาธารณะตามประมวลกฎหมายวิธีพิจารณาความอาญา ได้แก่ กรณีการออกหมายค้น มาตรา 105 วรรคแรกที่ว่า “หมายค้นออกโดยศาล คือผู้พิพากษาสอบสวน เว้นแต่กรณีเร่งด่วนการส่งให้ค้นในเคสสถาน อาจทำได้โดยพนักงานอัยการ หรือพนักงานตำรวจผู้ช่วยอัยการ”

การค้นตามกฎหมายของประเทศเยอรมันจะต้องระบุรายละเอียด ตามมาตรา 107 รายละเอียดในหมายค้นจะต้องระบุมูลเหตุแห่งการค้น บุคคล และสิ่งของที่ต้องการค้นด้วย”

“ห้ามมิให้ค้นเคสสถานในระหว่างกลางคืน เว้นแต่เป็นการค้นสถานที่ทางธุรกิจที่เปิดบริการสาธารณะในเวลากลางคืน หรือความผิดซึ่งหน้า หรือกรณีฉุกเฉินหรือการค้นนักโทษที่หลบหนีที่คุมขัง” นอกจากนี้ใน มาตรา 99 ได้ให้อำนาจตำรวจในการค้น ยึดสิ่งของที่เป็นจดหมาย ไปรษณีย์ โทรเลข โดยเจ้าหน้าที่ดังกล่าวจะต้องขอคำสั่งจากศาลให้ยึดได้ มาตรา 100 วรรคแรก มิใช่กระทำได้โดยพลการ ซึ่งบทบัญญัตินี้กฎหมายมีเจตนารมณ์จะให้อำนาจเจ้าหน้าที่ไว้เป็นพิเศษ เพื่อประโยชน์ในการสอบสวน ซึ่งตำรวจเยอรมัน สามารถใช้กฎหมายข้อนี้ และขอความร่วมมือจาก ISP

ความน่าเชื่อถือของการค้น ยึด พยานหลักฐาน กล่าวคือ ตามกฎหมายเยอรมันอาจอยู่ที่วิธีการค้นที่เคร่งครัดตามมาตรา 106 วรรคแรก

มาตรา 106 วรรคแรก “การค้นต้องกระทำต่อหน้าเจ้าของสถานที่ หากไม่อยู่จะต้องกระทำต่อหน้าผู้แทนญาติ หรือเพื่อนบ้าน”

สำหรับในประเทศเยอรมันการปฏิบัติตามกฎหมายดังกล่าวของเจ้าหน้าที่ตำรวจตามบทบัญญัติของกฎหมายดังกล่าวมาแล้วอย่างน้อยก็สร้างความน่าเชื่อถือต่อศาลได้ว่าเจ้าหน้าที่โปร่งใส พยานข้อมูลอิเล็กทรอนิกส์ที่ได้มาน่าจะตรงกับความจริงขณะที่ค้น

นอกจากนี้ การยึดพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เกี่ยวข้องกับมาตรา 94 ที่วางหลักว่า “สิ่งของที่น่าจะเป็นพยานหลักฐานสำคัญในการสอบสวน หรือสิ่งของที่รีบไว้จะต้องจัดให้อยู่ในอารักขา หรือทำให้ปลอดภัยทางใดทางหนึ่งการยึดสิ่งของ ที่อยู่ในความครอบครองของบุคคล หรือไม่ยอมส่งให้ด้วยความสมัครใจให้ขอคำสั่งศาล” ในขณะที่ประเทศเยอรมัน นั้นไม่มีบทบัญญัติพิเศษโดยเฉพาะที่จะลงโทษพวกอาชญากรรมทางอิเล็กทรอนิกส์เหมือนในประเทศสหรัฐอเมริกา แต่หากมีบทลงโทษทางอาญา German Criminal Code 1974 แก้ไขเพิ่มเติม (StGB:Strafgesetzbuch) ใน

การตรวจค้นข้อมูลอิเล็กทรอนิกส์ที่อยู่ในความครอบครองของมนุษย์ในที่รโหฐาน เช่น ในเครื่องคอมพิวเตอร์พีซี (PC) ในที่รโหฐานต้องปฏิบัติตามหลักประมวลกฎหมายวิธีพิจารณาความอาญา (StGB:Strafgesetzbuch) ซึ่งจำต้องเข้าใจกระบวนการทางวิธีพิจารณาความอาญา กล่าวคือ ในประเทศเยอรมัน การสอบสวนและการรวบรวมพยานหลักฐาน เพื่อทราบข้อเท็จจริงในเนื้อหา นอกจากพนักงานอัยการแล้วยังมีองค์กรอื่น ๆ ที่ช่วยในการสอบสวน คือ สำนักงานอาชญาวิทยาแห่งสหพันธ์รัฐ Bundekriminalamt หรือเรียกชื่อย่อว่า BKA มีตำรวจ 2 ประเภท คือ ข้าราชการตำรวจ ซึ่งเป็นผู้ช่วยของพนักงานอัยการ และข้าราชการตำรวจอื่น ๆ ส่วนผู้พิพากษาสอบสวนนั้น จะเป็นผู้อนุญาตให้มาตรการบางอย่างในการสอบสวนของพนักงานอัยการ โดยเป็นผู้ตรวจสอบว่ามาตรการที่ใช้ นั้น ชอบด้วยกฎหมายหรือไม่

สรุปกฎหมายเยอรมันในปัจจุบันการรวบรวมพยานหลักฐานคล้ายกับกฎหมายประเทศไทย พนักงานตำรวจกระทำภายใต้บทบัญญัติของกฎหมายที่ให้อำนาจไว้เท่านั้น การรวบรวมพยานหลักฐานในคดีเกี่ยวกับคอมพิวเตอร์ พัฒนากฎหมายที่มีอยู่ให้สามารถรองรับแต่พัฒนาจากกฎหมายเดิมที่มีอยู่เพื่อให้ทันต่อความก้าวหน้าของเทคโนโลยี และ ศาลมีอำนาจอย่างกว้างขวางในการที่จะใช้ดุลพินิจในการรับฟังพยานหลักฐานที่เสนอโดยคู่ความ และดุลพินิจนี้จะถูกโต้แย้งไม่ได้

4.3 ปัญหาความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้อง

ปัญหาของประเทศไทยพบว่าภาครัฐขาดแคลนบุคลากรที่มีความชำนาญเฉพาะด้านการสืบสวนสอบสวนและดำเนินคดีกับอาชญากรรมทางอิเล็กทรอนิกส์เป็นที่ทราบกันโดยทั่วไปว่าความเจริญก้าวหน้าทางเทคโนโลยีและการสื่อสารนำมาซึ่งอาชญากรรมทางไซเบอร์และไม่ว่าจะเป็นอาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมทั่วไปก็ล้วนเกี่ยวข้องกับพยานหลักฐานอิเล็กทรอนิกส์อย่างหลีกเลี่ยงไม่ได้ในชีวิตประจำวันของประชาชนส่วนใหญ่ การใช้โทรศัพท์ การส่งแฟกซ์ ส่งอีเมลล์ เกี่ยวข้องกับสื่ออิเล็กทรอนิกส์ทั้งสิ้น ดังนั้น การก่ออาชญากรรมทางอิเล็กทรอนิกส์ จึงกระทำได้ทุกที่ทุกเวลาที่มีเครือข่ายอินเทอร์เน็ต จึงจะพบเห็นประชาชนจำนวนมากประสบกับปัญหาถูกล่อลวงฉ้อโกง ผ่านเครื่องมืออิเล็กทรอนิกส์ รัฐขาดหน่วยงานที่รับผิดชอบโดยตรงเกี่ยวกับการสืบสวนสอบสวนปราบปรามการกระทำความผิดทางเทคโนโลยี รวมถึงพนักงานสอบสวนที่มีบทบาทสำคัญในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์นั้น ไม่มีบทบัญญัติกฎหมายให้อำนาจพนักงานสอบสวนทั่วไปเข้าถึงข้อมูลทางอิเล็กทรอนิกส์ได้ ต้องประสานหน่วยงานอื่น ๆ ในการขอข้อมูลซึ่งในทางปฏิบัติทำให้เกิดความล่าช้าในการประสานงานด้วยหนังสือราชการ

ปัจจุบันการกระทำความผิดอาญาส่วนใหญ่จะมีพยานหลักฐานที่เกี่ยวข้องกับพยานอิเล็กทรอนิกส์อย่างหลีกเลี่ยงไม่ได้ โดยเฉพาะโทรศัพท์มือถือสามารถเข้าสู่ระบบอินเทอร์เน็ตได้ 24 ชั่วโมง จึงเกิดคดีขึ้นมากมาย เช่น การล่อลวงให้โอนเงินซึ่งการโอนเงินกระทำได้ง่ายไม่ต้องเดินทางไปธนาคารเหมือนเช่นในอดีต การโอนเงินผ่านอินเทอร์เน็ตผ่านโทรศัพท์ มากขึ้นจึงง่ายต่อการก่ออาชญากรรม เมื่อศึกษาถึงอำนาจของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญากลับไม่พบว่าได้มีการบัญญัติอำนาจพิเศษในการเข้าถึงพยานหลักฐานอิเล็กทรอนิกส์แก่พนักงานสอบสวน

การรวบรวมพยานหลักฐานส่วนใหญ่จะเป็นลักษณะขอความร่วมมือหรือการออกหมายเรียก ซึ่งจากการปฏิบัติจริงไม่ได้รับความร่วมมือเท่าที่ควร เช่น ธนาкарเจ้าของข้อมูลที่จะใช้เป็นพยานหลักฐานไม่ให้ความร่วมมือในการจัดส่งเอกสารข้อมูลของผู้กระทำความผิด บริษัทผู้บริการโทรศัพท์เคลื่อนที่ค่ายต่าง ๆ เพราะส่วนใหญ่จะอ้างว่าเป็นความลับของลูกค้า หรือถึงแม้จะให้ใช้เวลานานซึ่งส่วนมากต้องติดตามด้วยตัวเองทำให้พนักงานสอบสวนต้องมีภาระในการติดตามพยานหลักฐาน คดีเกิดความล่าช้า ควรแก้ไขเพิ่มเติมกฎหมายวิธีพิจารณาความอาญาในส่วนที่เกี่ยวข้องกับอำนาจหน้าที่ในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ให้ชัดเจนเพื่อป้องกันให้กฎหมายมีช่องว่างทำให้ผู้ประกอบการไม่ให้ความร่วมมือ ภาคเอกชนขาดจิตสำนึกในเรื่องธรรมาภิบาลและความรับผิดชอบต่อสังคมขององค์กร สมควรให้หน่วยงานที่กำกับดูแลองค์กรภาคเอกชนที่มีบทบาทสำคัญในการควบคุมธุรกรรมที่ผิดกฎหมาย ร่วมกับหน่วยงานของรัฐมากยิ่งขึ้น

มาตรการปราบปรามอาชญากรรมของหน่วยงานรัฐ เป็นไปในลักษณะต่างคนต่างทำ ขาดความร่วมมืออย่างจริงจัง มีข้าราชการและนักการเมืองให้ความร่วมมือ กับขบวนการอาชญากรรม และมาตรการทางกฎหมายและความร่วมมือระหว่างประเทศของหลายประเทศ ยังไม่ก้าวหน้ามาก การกระทำความผิดมีลักษณะเป็นอาชญากรข้ามชาติมากขึ้นโดยผ่านเครือข่ายอินเทอร์เน็ตกระทบทั้งด้านความมั่นคง เศรษฐกิจและความสงบสุขในสังคม และเป็นปัญหาความมั่นคงนอกรูปแบบที่ทำนายอำนาจรัฐ โดยองค์กรอาชญากรรมขนาดใหญ่ได้ขยายธุรกิจมายังภูมิภาคต่าง ๆ มากขึ้น ซึ่งภูมิภาคเอเชียตะวันออกเฉียง และอาเซียนกำลังเป็นเป้าหมายที่สำคัญขององค์กรอาชญากรรมข้ามชาติ อาชญากรรมที่เป็นปัญหาสำคัญในอาเซียน ได้แก่ ยาเสพติด การค้ามนุษย์ การค้าพืชพันธุ์และสัตว์ป่า การฟอกเงิน อาชญากรรมทางเศรษฐกิจ และโจรสลัด โดยอาชญากรข้ามชาติจำนวนมากเข้ามาทำธุรกิจข้ามแดนในอาเซียน เช่น ขบวนการยาสูบ รัฐควรแสวงหามาตรการความร่วมมือระหว่างประเทศต่อไป

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

เนื่องจากการก่ออาชญากรรมทางอิเล็กทรอนิกส์ นั้นมีความยากต่อการตรวจพบ พยานหลักฐาน และยากต่อการพิสูจน์ความรับผิดชอบ นอกจากนั้นการกระทำความผิดสามารถทำได้อย่างรวดเร็ว ซึ่งนั่นหมายถึงอาจส่งผลเสียหายในวงกว้าง มาตรการด้านกฎหมายเป็นนโยบายของรัฐบาลไทยประการหนึ่งที่น่าสนใจในการต่อต้านอาชญากรรมทางเทคโนโลยี โดยได้มีการบัญญัติกฎหมายเพื่อกำหนดว่าการกระทำใดบ้างที่มีโทษทางอาญาและปัจจุบันประเทศไทยยังมีกฎหมายเฉพาะที่เกี่ยวข้องกับพยานหลักฐานทางอิเล็กทรอนิกส์ คือพระราชบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 แต่กลับไม่ได้ส่งผลให้การปราบปรามอาชญากรรมทางอิเล็กทรอนิกส์ให้มีประสิทธิภาพได้เท่าที่ควรจะเป็น อันเนื่องมาจากอาชญากรรมประเภทนี้ได้มีการพัฒนาไปอย่างรวดเร็วจนถึงการกระทำความผิดอาจเกิดขึ้นในต่างประเทศแต่ส่งผลร้ายกับประเทศไทย ซึ่งเป็นเรื่องที่ยากต่อการที่จะสืบสวนหาตัวผู้กระทำความผิดและอาชญากรรมทางอิเล็กทรอนิกส์หรืออาชญากรรมไซเบอร์ยังใหม่ต่อกระบวนการยุติธรรมในประเทศไทย

แม้ว่าประเทศไทยกฎหมายอาชญากรรมคอมพิวเตอร์จะมีผลบังคับใช้แล้ว แต่หน่วยงานฝ่ายกระบวนการยุติธรรมก็ยังไม่สามารถนำกฎหมายมาจัดการกับเหล่าอาชญากรไซเบอร์เหล่านี้ได้ การพิจารณาคดีอาชญากรรมทางอิเล็กทรอนิกส์นั้น จำเป็นอย่างยิ่งที่ผู้เกี่ยวข้องกับการรวบรวมพยานหลักฐานจะต้องมีความรู้ทางด้าน Information Security และเจาะลึกในการพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือ นิติคอมพิวเตอร์ (Computer Forensics) ซึ่งหมายถึง การแสวงหา การเก็บรักษา วิเคราะห์ และการนำเสนอพยานหลักฐานที่เกี่ยวข้องกับอิเล็กทรอนิกส์ ซึ่งได้แก่ คอมพิวเตอร์ โทรศัพท์ แฟกซ์ อีเมล อินเทอร์เน็ต กล่าวอีกนัยหนึ่งก็คือ การใช้กระบวนการที่จะระบุ บ่งชี้ เก็บรักษา และ กู้คืน บรรดาข้อมูลอิเล็กทรอนิกส์ที่เป็นพยานหลักฐานและมีความสำคัญต่อการสืบสวนปัญหา ก็คือ ผู้ที่เกี่ยวข้องไม่ว่าจะเป็นพนักงานสอบสวนของสำนักงานตำรวจแห่งชาติ, เจ้าหน้าที่กรมสอบสวนคดีพิเศษ (DSI) ของกระทรวงยุติธรรม, เจ้าหน้าที่ของสถาบันนิติวิทยาศาสตร์, ผู้พิพากษา และ อัยการ ตลอดจน ทนายความ มีความจำเป็นที่จะต้องเรียนรู้เรื่อง Computer Forensics เพื่อที่จะสามารถดำเนินการไต่สวนคดีอาชญากรรมคอมพิวเตอร์ได้อย่างถูกต้องและมีประสิทธิภาพ

จากการวิจัยพบว่าการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ เพื่อดำเนินคดีกับผู้กระทำความผิดกับอาชญากรรมทางเทคโนโลยีและการสื่อสาร หรืออาชญากรรมทางอิเล็กทรอนิกส์ มีปัญหาอยู่หลายประการสรุปได้ ดังนี้

1. การค้น เนื่องจากการค้นในทรีโหลฐานจำเป็นต้องขอมายค้น การขอมายค้นก็ต้องมีเหตุอันควรเชื่อว่ามียานหลักฐานในสถานที่ที่จะค้นนั้น ในขณะที่สำนักงานเกี่ยวกับกระบวนการยุติธรรมต่าง ๆ ของไทยมีเขตที่ตั้งอยู่อย่างกระจัดกระจายมิได้อยู่ภายในเขตเดียวกันเหมือนต่างประเทศ การขอมายศาลจึงต้องใช้เวลาเดินทาง ในขณะที่เดินทางไปขอมายค้น อาชญากรก็อาจมีการแก้ไขเปลี่ยนแปลงหรือทำลายพยานหลักฐานไปแล้ว มายค้นยังต้องระบุสถานที่ค้นอย่างชัดเจน แต่อาชญากรรมประเภทนี้ไม่มีขอบเขต สามารถเข้าสู่ข้อมูลได้จากหลายสถานที่ในโลกเพื่อเข้าระบบข้อมูลอิเล็กทรอนิกส์ที่เป็นพยานหลักฐานในคดี เพื่อทำลายพยานหลักฐานโดยเฉพาะคนร้ายสมคบกันหลายคนยิ่งง่ายต่อการสื่อสารถึงกันผ่านเครือข่ายอินเทอร์เน็ต การทำลายหลักฐานจึงเป็นเรื่องง่ายสำหรับอาชญากร

ด้วยลักษณะของพยานหลักฐานอิเล็กทรอนิกส์ มีความละเอียดอ่อน ซับซ้อนจำเป็นต้องใช้ความเร็วในการเข้าถึง การดำเนินการขอมายค้นจึงเกิดความล่าช้า การที่รัฐประสงค์จะให้ความคุ้มครองสิทธิส่วนบุคคล จึงสร้างหลักประกันสิทธิของประชาชนด้วยการกำหนดมาตรการตรวจสอบการใช้ดุลพินิจของเจ้าพนักงานโดยองค์กรศาล และในส่วนอำนาจในการออกมายค้นกำหนดให้ศาลมีอำนาจแต่ผู้เดียว แม้แต่การค้นข้อมูลอิเล็กทรอนิกส์ที่ใช้อุปกรณ์เชื่อมต่อคอมพิวเตอร์เข้าไปค้นหาหลักฐานข้อมูลในเครื่องคอมพิวเตอร์ผู้ต้องสงสัยโดยไม่มีการรูล้ำเข้าไปในทรีโหลฐานก็ใช้มายค้นเช่นเดียวกันเพราะถือว่าการล่งล้ำเข้าไปในพื้นที่อันสงวนไว้เป็นสิทธิส่วนตัว การค้นจนจึงต้องมีมายค้น

2. การยึด พยานหลักฐานที่เป็นข้อมูลในคอมพิวเตอร์และสื่ออิเล็กทรอนิกส์ เป็นสิ่งไม่มีรูปร่าง จะทำได้โดยวิธีใด หากข้อมูล ที่จะยึดมาจากระบบเครือข่ายคอมพิวเตอร์ของผู้อื่น และมีอยู่มากมายหลายแห่ง จะสามารถยึด ทั้งระบบได้หรือไม่ อย่างไรจึงเป็นปัญหาของพนักงานสอบสวน

ผู้วิจัยได้ศึกษาถึงอำนาจของพนักงานสอบสวนคดีพิเศษของประเทศไทย ก็ได้มีการบัญญัติในเรื่องอำนาจของพนักงานสอบสวนคดีพิเศษไว้ในการตรวจค้น ยึด หลักฐานพยานมาตรา 24 ให้พนักงานสอบสวนคดีพิเศษมีอำนาจเข้าไปในเคหสถาน หรือสถานที่ใด ๆ เพื่อตรวจค้น เมื่อมีเหตุสงสัยตามสมควรว่ามีบุคคลที่มีเหตุสงสัยว่ากระทำความผิดที่เป็นคดีพิเศษหลบซ่อนอยู่ หรือมีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้ ประกอบกับมีเหตุอันควรเชื่อว่าเนื่องจากการเน้นข่าวว่าจะเอามายค้นมาได้บุคคลนั้นจะหลบหนีไป หรือทรัพย์สินนั้นจะถูกโยกย้าย ซุกซ่อนทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิม มีอำนาจค้นบุคคล หรือยานพาหนะที่มีเหตุสงสัยตามสมควรว่ามีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้ มีอำนาจสอบถามเป็นหนังสือหรือเรียกให้สถาบันการเงิน ส่วนราชการ องค์กร หรือหน่วยงานของรัฐ หรือรัฐวิสาหกิจ ส่งเจ้าหน้าที่ที่เกี่ยวข้องมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา มีอำนาจทำหนังสือสอบถาม หรือเรียกบุคคลใด ๆ มาเพื่อให้ถ้อยคำใด ๆ ส่งคำชี้แจงเป็นหนังสือหรือส่งบัญชีเอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา มีอำนาจยึด หรืออายัดทรัพย์สินที่ค้นพบ หรือที่ส่งมาดังกล่าวไว้ใน (1)

(2) (3) และ (4) การใช้อำนาจตามวรรคหนึ่งให้พนักงานสอบสวนคดีพิเศษปฏิบัติปฏิบัติตามข้อบังคับที่ กพค.กำหนดเฉพาะ

มาตรา 25 ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสาร หรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการ

5.2 ข้อเสนอแนะ

สภาพปัญหาที่ผู้วิจัยได้ทำการศึกษาวิเคราะห์ถึงปัญหามาแล้วใน บทที่ 4 และบทสรุปผู้วิจัยพบว่าประเทศไทยจำเป็นจะมีการบัญญัติกฎหมายให้อำนาจพนักงานสอบสวนทั่วไปตามประมวลกฎหมายวิธีพิจารณาความอาญาสามารถเข้าถึงพยานหลักฐานซึ่งเป็นข้อมูลอิเล็กทรอนิกส์ได้ตามสมควร กรณีเร่งด่วนและกรณีที่เป็นการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ ซึ่งง่ายต่อการทำลายให้อำนาจพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาให้อำนาจเช่นเดียวกับพนักงานสอบสวนคดีพิเศษ

ควรจะมีการนำมาบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาเฉพาะกรณีที่เป็นการรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ รวมถึงควรให้อำนาจเหมือนกับพนักงานเจ้าหน้าที่ มาตรา 18-21 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มีอำนาจในการรวบรวมพยานหลักฐาน มีอำนาจในการเข้าตรวจข้อมูลคอมพิวเตอร์ ในกรณีมีเหตุอันควรสงสัยว่าน่าจะมีการกระทำความผิดตามพระราชบัญญัติโดยมีอำนาจ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ เพื่อให้การดำเนินคดีตามพระราชบัญญัตินี้มีประสิทธิภาพจึงได้มีหลักการพิเศษเพิ่มขึ้น 2 ประการคือ การเพิ่มวิธีการพิเศษในการสืบสวนและสอบสวน และการเพิ่มให้มี “พนักงานเจ้าหน้าที่” เข้ามามีอำนาจในการสืบสวนและความผิดตามพระราชบัญญัติฉบับนี้ด้วยนอกเหนือจากพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญา โดยกล่าวถึงอำนาจของพนักงานเจ้าหน้าที่ดังนี้ การสืบสวนพิเศษตามการรวบรวมพยานหลักฐานในคดีความผิดเกี่ยวกับคอมพิวเตอร์ ถือเป็นการรวบรวมพยานหลักฐานในทางคดีที่เกี่ยวกับความผิดอาญาในส่วนของความผิดเกี่ยวกับคอมพิวเตอร์ นั้นค่อนข้างยุ่งยากและซับซ้อนเพราะผู้รวบรวมพยานหลักฐานนอกจากจะต้องมีความรู้ความเชี่ยวชาญเกี่ยวกับกฎหมายแล้วยังต้องมีความรู้เชี่ยวชาญในส่วนของการคอมพิวเตอร์ด้วยซึ่งบุคคลประเภทนี้มีน้อย ดังนั้นเมื่อใช้หลักกฎหมายวิธีพิจารณาความอาญาเพียงอย่างเดียวอาจก่อให้เกิดความบกพร่องในการรวบรวมพยานหลักฐาน

5.2.1 อำนาจในการค้น

จากปัญหาในการระบุขอบเขตอำนาจของพนักงานเจ้าหน้าที่ในการค้นนั้นมีข้อจำกัดในการค้นอยู่มากเนื่องจากกฎหมายไม่ได้เปิดช่องให้พนักงานสอบสวนทั่วไปไม่มีอำนาจพิเศษในการค้น การค้นจึงกระทำได้และถูกจำกัดภายใต้บทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 96 โดยอาศัยเหตุที่จะออกหมายค้นได้ต้องปรากฏตามมาตรา 69 การค้นจึงต้องมีหมายค้นและการค้นในที่รโหฐานจะต้องกระทำในเวลากลางวันตามมาตรา 92 และ มาตรา 96 ซึ่งผู้วิจัยเห็นเห็นว่า

พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์มีลักษณะเฉพาะคือสามารถถูกเปลี่ยนแปลงแก้ไขได้ง่าย ควรให้มีการปรับแก้ไขกฎหมายมาตราดังกล่าวข้างต้นให้พนักงานสอบสวนสามารถระบุขอบเขตสถานที่ที่จะทำการค้นไ้ได้อย่างกว้าง ๆ และสามารถระบุได้หลายแห่งในหมายค้นและหากเป็นการค้นข้อมูลอิเล็กทรอนิกส์ ควรอาศัยเหตุที่จะเข้าข้อยกเว้นตามมาตรา 96 (2) กรณีฉุกเฉินอย่างยิ่งพนักงานสอบสวนจึงจะสามารถเข้าค้นได้ทั้งกลางวันกลางคืน

พยานหลักฐานที่เกี่ยวกับการกระทำความผิดของอาชญากรรมทางอิเล็กทรอนิกส์เป็นสิ่งที่สามารถที่จะถูกลบ ทำลาย ยักยอก แก้ไข เปลี่ยนแปลงได้ง่าย และสามารถกระทำได้อย่างรวดเร็วควรให้อำนาจพนักงานสอบสวนเข้าตรวจค้นของเจ้าหน้าที่ตำรวจได้ตลอด 24 ชั่วโมง กรณีมีเหตุอันควรเชื่อว่ามีสิ่งผิดกฎหมายชุกซ่อนอยู่หากเวลาเนิ่นช้าจะมีการยักยอกทำลาย หรือทำลายไป และควรให้อำนาจดำเนินการค้นได้โดยใช้ตีความตามมาตรา 98 (2) แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ว่าหากการกระทำความผิดเกี่ยวกับเทคโนโลยีและพยานหลักฐานเป็นข้อมูลอิเล็กทรอนิกส์ในการค้นและพบควรให้เป็นความผิดซึ่งหน้าพนักงานสอบสวนจึงจะมีอำนาจในการค้นสิ่งของอื่นในสถานที่ที่จะค้นนั้นได้ด้วย ในที่นี้ต้องอยู่ภายใต้กรอบการปฏิบัติหน้าที่ที่ชัดเจนเพื่อไม่ให้เกิดการกระทำของเจ้าพนักงานเป็นการปฏิบัติหน้าที่โดยมิชอบด้วย

นอกจากนั้นผู้วิจัยเห็นว่าควรมีกฎหมายรองรับการปฏิบัติหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์สามารถที่จะทำการกู้หรือทำให้ข้อมูลที่ถูกลบกลับคืนมาอย่างเดิมได้ด้วย โดยให้บัญญัติกฎหมายเพิ่มเติมในส่วนที่เป็นอำนาจหน้าที่ของพนักงานสอบสวนตามมาตรา 132 แห่งประมวลกฎหมายวิธีพิจารณาความอาญาว่ากรณีการรวบรวมพยานหลักฐานเฉพาะที่เกี่ยวข้องกับพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ที่มีความซับซ้อนจึงจำเป็นต้องมีการสืบสวนสอบสวนหาพยานหลักฐานเป็นกรณีพิเศษ พนักงานสอบสวนควรมีอำนาจเช่นเดียวกันกับพนักงานสอบสวนกรมสอบสวนคดีพิเศษ ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 มาตรา 21 มาตรา 24 และมาตรา 25 ด้วย

5.2.2 การแสวงหาและการรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ของพนักงานสอบสวน

การสืบสวนสอบสวนในคดีอาชญากรรมทางอิเล็กทรอนิกส์ไม่ใช่เรื่องง่ายที่เจ้าหน้าที่คนใดคนหนึ่งจะกระทำได้เหมือนคดีอาชญากรรมธรรมดาทั่วไป แต่ต้องเป็นเจ้าหน้าที่ที่มีความรู้ความเข้าใจในระบบต่าง ๆ ของเครื่องมืออิเล็กทรอนิกส์ นั้น ๆ รวมถึงมีเครื่องมือ และอุปกรณ์ในการตรวจสอบสถานที่เกิดเหตุจึงมีความสำคัญและพยานหลักฐานประเภทนี้มีความแตกต่างจากคดีอาชญากรรมธรรมดาทั่วไป การเก็บรวบรวมและตรวจพิสูจน์พยานหลักฐานนั้นปัญหาที่พบไม่ใช่ “การใช้เครื่องมือ” แต่อยู่ที่ “กระบวนการ” ดังนั้นการเก็บรวบรวมพยานหลักฐานคนทำคดีและคนตรวจพิสูจน์จึงมีความสำคัญเพื่อไม่ให้พยานหลักฐานเปลี่ยนแปลงโดยไม่ได้ตั้งใจ

ความร่วมมือระหว่างหน่วยงานจึงเป็นสิ่งสำคัญโดยเฉพาะพยานหลักฐานทางอิเล็กทรอนิกส์เป็นข้อมูลอิเล็กทรอนิกส์ (Electronic Data) มีลักษณะเฉพาะคือสามารถเปลี่ยนแปลงแก้ไขได้ง่าย ซึ่งพนักงานเจ้าหน้าที่ต้องตามให้ทันความพยายามกลบเกลื่อนร่องรอยของคนร้าย สำหรับความก้าวหน้าของเครื่องมือ เช่น ฮาร์ดดิสก์ที่ขนาดความจุเพิ่มมากขึ้นทุกวัน ทำให้ต้องใช้เวลาในการตรวจพิสูจน์ที่

นานขึ้นในขณะที่ทำงานแข่งกับเวลาควรมีการประสานงานกันระหว่างหน่วยงานของไทยมากขึ้น ควรมีการฝึกอบรมความรู้ขั้นสูงทางด้าน Information Security ซึ่งเป็นเรื่องจำเป็นสำหรับพนักงานสอบสวนตลอดจนผู้ที่เกี่ยวข้องในกระบวนการยุติธรรมจนถึงชั้นศาล หน่วยงานภาครัฐควรให้ความสำคัญเรื่องการฝึกอบรมบุคลากรดังกล่าวในเรื่องการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์และพัฒนาให้พร้อมรับกับกฎหมายอาชญากรรมทางอิเล็กทรอนิกส์ในประเทศไทยเพื่อปราบเหล่าอาชญากรทางเทคโนโลยีที่นับวันจะเพิ่มมากขึ้น และมีรูปแบบคดีที่ทวีความซับซ้อนมากขึ้น เพื่อให้ผู้ที่เกี่ยวข้องในกระบวนการยุติธรรมสามารถนำกฎหมายมาบังคับใช้ได้อย่างมีประสิทธิภาพในที่สุด

หมายเหตุ จากปัญหาที่กล่าวมาแล้วข้างต้นยังพบว่าหน่วยงานที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานแยกกันทำจึงไม่สามารถจะกระทำได้อย่างรวดเร็วการประสานขอความร่วมมือไม่ใช่จุดเดียวจบเกิดความยุ่งยาก ลำช้า ผู้วิจัยเสนอให้มีการจัดตั้งหน่วยงานพิเศษ ที่รับผิดชอบเกี่ยวกับการกระทำความผิดทางเทคโนโลยีสารสนเทศดำเนินคดีกับอาชญากรรมทางอิเล็กทรอนิกส์ ไม่ใช่จำกัดอยู่แค่การกระทำความผิดทางคอมพิวเตอร์ ประกอบด้วยบุคลากรที่มีความเชี่ยวชาญ มีความรู้ความชำนาญทางด้านคอมพิวเตอร์และอิเล็กทรอนิกส์นอกเหนือจากนักกฎหมาย การขอหมายค้นสามารถขอผ่านอินเทอร์เน็ตได้ใช้เมลล์และศาลอนุมัติส่งกลับมายังอีเมลผู้มีหน้าที่ยื่นคำขอ เชื่อว่าจะเกิดประสิทธิภาพอย่างสูงต่อการดำเนินคดีกับอาชญากรรมอิเล็กทรอนิกส์ แต่เนื่องจากผู้วิจัยมีระยะเวลาจะจัดจึงขอเสนอแนวทางไว้พอสังเขปเท่านั้น เพื่อรองรับการเทคโนโลยีในอนาคตต่อไป

บรรณานุกรม

กรมสอบสวนคดีพิเศษ. DSI กรมสอบสวนคดีพิเศษ (Department of Special Investigation).

ค้นวันที่ 12 ธันวาคม 2558 จาก <http://www.dsi.go.th>

กรมล ทอธรรมาชาติ. เรืองนำรู้เกี่ยวกับการปกครองและรัฐธรรมนูญของสหรัฐอเมริกา.

กรุงเทพฯ: โรงพิมพ์สังคมศาสตร์, 2513.

กุลพล พลวัน. พัฒนาการแห่งสิทธิมนุษยชน. พิมพ์ครั้งที่ 3. กรุงเทพฯ: วิญญูชน, 2538.

คณิต ณ นคร. กฎหมายวิธีพิจารณาความอาญา. กรุงเทพฯ: วิญญูชน, 2549.

คณิต ณ นคร. กฎหมายวิธีพิจารณาความอาญา. พิมพ์ครั้งที่ 8 แก้ไขเพิ่มเติม. กรุงเทพฯ:

นิติบรรณาการ, 2555.

คณิง ภาไชย. กฎหมายวิธีพิจารณาความอาญา เล่ม 1. พิมพ์ครั้งที่ 6. กรุงเทพฯ: ม.ป.พ, 2540.

คำวินิจฉัยของคณะกรรมการกฤษฎีกา ตามหนังสือ สำนักงานคณะกรรมการกฤษฎีกา ที่

นร.0601/618 (2542). วารสารอัยการนิเทศ. 61, 1: 183-194.

จรงค์ จุฑานนท์. การคุ้มครองสิทธิของประชาชนต่อการถูกจับและตรวจค้นโดยไม่ชอบธรรม.

2525.

นัตรมกล รุ่งรัตน์ณวิงษ์. มาตราการแสวงหา รวบรวมและการเสนอพยานหลักฐานในคดี

อาชญากรรมทางคอมพิวเตอร์. วิทยานิพนธ์ปริญญาามหาบัณฑิต คณะนิติศาสตร์

มหาวิทยาลัยรามคำแหง, 2547.

เฉลิมพล ช่อโพธิ์ทอง. ความผิดฐานลักทรัพย์และฉ้อโกง: ศึกษาเปรียบเทียบกฎหมายอังกฤษ

เยอรมัน และไทย. วิทยานิพนธ์ปริญญาามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัย

ธรรมศาสตร์, 2535.

ชัยวัฒน์ วงศ์วัฒนศานต์, ทวีศักดิ์ กอนันต์กุล และสุรางคณา แก้วจำนง. คำอธิบายพระราชบัญญัติ

ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544. กรุงเทพฯ: สำนักเลขานุการ

คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, 2545.

ญาณพล ยิ่งยืน. อาชญากรรมทางคอมพิวเตอร์. กรุงเทพฯ: ศูนย์ข้อมูลข้อสนเทศ สำนักงานตำรวจ

แห่งชาติ, ม.ป.ป.

ณรงค์ ใจหาญ. หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1. พิมพ์ครั้งที่ 5. กรุงเทพฯ: นิติธรรม,

2543.

ณรงค์ ใจหาญ และคณะ. รายงานศึกษาวิจัยฉบับสมบูรณ์ เรื่องสิทธิผู้ต้องหาจำเลยและผู้ต้องโทษ

ในคดีอาญา. รายงานการวิจัย เสนอต่อคณะกรรมการกฤษฎีกา, 2540.

เดชชาติ วงศ์โกมลเชษฐ์. รัฐธรรมนูญนานาชาติ. กรุงเทพฯ: สภาวิจัยแห่งชาติ, 2516.

นารี กิตติสมบูรณ์สุข. การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนจากข้อมูลอิเล็กทรอนิกส์ใน

อาชญากรรมคอมพิวเตอร์. วิทยานิพนธ์ปริญญาามหาบัณฑิต คณะนิติศาสตร์ปริติ พนม

ยงค์ มหาวิทยาลัยธุรกิจบัณฑิต, 2549.

บรรเจิด สิงคะเนติ. **หลักพื้นฐานของสิทธิเสรีภาพ และศักดิ์ศรีความเป็นมนุษย์ตาม**

รัฐธรรมนูญ พ.ศ.2540. พิมพ์ครั้งที่ 2. กรุงเทพฯ: วิญญูชน, 2547.

ประมวลกฎหมายวิธีพิจารณาความอาญา. ค้นวันที่ 12 ธันวาคม 2558 จาก <http://www.supreme court.or.th/file/elc/internet/Law%20courts/Code%20of%20Criminal%20Procedure/Code%20of%20Criminal%20Procedure.pdf>

ประยุทธ์ พึ่งเคหา. **ปัญหาเกี่ยวกับอำนาจพนักงานสอบสวนในการรวบรวมพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา.** วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2554.

พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความอาญา (ฉบับที่ 22) พ.ศ.2547.

ราชกิจจานุเบกษา. 121, ตอนพิเศษ 79ก (23 ธันวาคม 2547).

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550. **ราชกิจจานุเบกษา** 124, 27ก (18 มิถุนายน 2550).

พรทิพย์ ตันทวนันท์. **อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์.** วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548.

พรเพชร วิชิตชลชัย. การรับฟังข้อมูลจากสื่ออิเล็กทรอนิกส์เป็นพยานหลักฐาน ปัญหาและเสนอแนะ. **ตุลพาท.** 42, 4 (ตุลาคม-ธันวาคม 2538): 85-103.

พินัย ณ นคร. กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์. **บทบัญญัติ.** 56, 2 (มิถุนายน 2543): 1.

ไพบูลย์ อมรวิญญูเกียรติ. **คำอธิบาย พ.ร.บ.คอมพิวเตอร์ พ.ศ.2550.** กรุงเทพฯ: โปรวิชั่น, 2553.

มหาวิทยาลัยสุโขทัยธรรมมาธิราช, สาขาวิชานิติศาสตร์. **เอกสารการสอนชุดวิชากฎหมายวิธี**

บัญญัติ 3. พิมพ์ครั้งที่ 12. นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมมาธิราช, 2539.

มหาวิทยาลัยสุโขทัยธรรมมาธิราช, สาขาวิชานิติศาสตร์. **เอกสารการสอนชุดวิชาระบบกฎหมายไทยและต่างประเทศ.** นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมมาธิราช, 2528.

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550. **ราชกิจจานุเบกษา.** 124, 47ก (24 สิงหาคม 2550).

ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ค้นวันที่ 12 ธันวาคม 2558 จาก <http://thainetizen.org/2015>

วัชรภรณ์ สุริยาภักดิ์. **คอมพิวเตอร์เบื้องต้นและเทคนิคการเขียนโปรแกรม.** กรุงเทพฯ: ไทยเจริญการพิมพ์, 2543.

วัลลิกา เนติบัณฑิตฤทธิ์. ปัญหาการรวบรวมและพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีอาญา. **วารสารศาลยุติธรรมปริทัศน์** (กันยายน 2550): 14-19.

วิศรุต อนุศาสนนันท์ . **อำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ศึกษาเปรียบเทียบระหว่างประเทศไทยกับสหรัฐอเมริกา.**

สารนิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ, 2550.

ศุภฤกษ์ ศุกรเสพย์. **การค้นในทรีโพรฐานของเจ้าพนักงานป้องกันและปราบปรามยาเสพติด.**

วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิต, 2545.

- สภาความมั่นคงแห่งชาติ. **มติคณะกรรมการร้อยกรองของสภาความมั่นคงแห่งชาติ**. ครั้งที่ 2/2557. 29 สิงหาคม 2557.
- สราวุธ เบญจกุล. “E-Crime” อาชญากรรมทางอิเล็กทรอนิกส์ มหันตภัยในโลกยุคใหม่. ค้นวันที่ 12 ธันวาคม 2558 จาก <http://www.manager.co.th/Daily/ViewNews.aspx?NewsID=9500000078831>
- สำนักงานคณะกรรมการกฤษฎีกา. **พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2544**. ค้นวันที่ 12 ธันวาคม 2558 จาก <http://oic.mof.go.th/home/wp-content/uploads/2015/06/41...2544.pdf>
- สำนักงานคณะกรรมการกฤษฎีกา. **พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547**. ค้นวันที่ 12 ธันวาคม 2558 จาก <http://www.law.moi.go.th/pdf...2547.pdf>
- สุนตี คงเทพ. **คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์**. กรุงเทพฯ: ม.ป.พ., 2558.
- สุปรียา อภิวัฒนาการ. **อาชญากรรมทางคอมพิวเตอร์: ศึกษากรณีการหลอกลวงทางอินเทอร์เน็ต**. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2545.
- สุรพันธ์ มั่นคงดี. **พยานหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์**. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2541.
- สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. แดงการณเรื่องการดักฟังทางโทรศัพท์. **รพีสาร**. 14, 4 (มกราคม-มีนาคม 2539): 34-36.
- โสภณ รัตนาร. **กฎหมายลักษณะพยาน**. กรุงเทพฯ: 21 เซนจูรี, 2536.
- อนิรุพีไล เงินวิจิตร. **ปัญหาในการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์**. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2544.
- อภิสิทธิ์ สารภี. **ปัญหากฎหมายในการแสวงหาพยานหลักฐานในคดีอาญาทางโทรคมนาคมชั้นสืบสวนสอบสวน**. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2550.
- อัมรัตน์ วัฒสมบัติ. **ปัญหาเกี่ยวกับอำนาจพนักงานสอบสวนในการรวบรวมพยานหลักฐานคดีอาชญากรรมทางคอมพิวเตอร์**. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2550.
- อาชญากรรมทางคอมพิวเตอร์**. ค้นวันที่ 12 ธันวาคม 2558 จาก www.polsci.chula.ac.th/sumonthip/buss-cricomp.doc
- Adams, Jo-Ann M. Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet. **Santa Clara High Technology Law Journal**. 12, 2 (January 1996). Retrieved March 10, 2016 from <http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1206&context=chtlj>
- Clemens, Walter R. The Exclusionary Rule under Foreign Law. **The Journal of Criminal Law Criminology and Police Science**. 52, 3 (September-October 1961).
- May, Richard. **Criminal Evidence**. London: Sweet & Maxwell, 1999.

Nelson, Harold L. and Teeter, Dwight L. **Law of Mass Communication: Freedom and Control of Print and Broadcast Media.** 5th ed. Mineola, NJ.: The Foundation Press, 1986.

Orion Investigation. **Orionforensics.com.** Retrieved July 31, 2015 from <http://www.orionforensics.com>

Whitebread, Charles H. and Stobogin, Christopher. **Procedure: An Analysis of Cases and Concepts.** 4th ed. New York: Foundation Press, 2000.

Wilding, Edward. **Computer Evidence: A Forensic Investigations Handbook.** London: Sweet & Maxwell, 1997.

Wise, Edward M. Computer Crime and Other Crimes Against Information Technology in the United States. In **International Review of Criminal Law 64.** Toulouse, France: Association Internationale De Droit Penal, 1992. Pp. 647-669.

ภาคผนวก

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

หน้า ๔
เล่ม ๑๒๔ ตอนที่ ๒๓ ก ราชกิจจานุเบกษา ๑๘ มิถุนายน ๒๕๕๐



พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๕๐

เป็นปีที่ ๖๒ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของ
สภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศ
ในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงาน
เข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์
หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

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

“ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการ ไม่ว่าต้องเสียค่าใช้จ่ายหรือไม่ก็ตาม

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑

ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำความผิดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำความผิดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดช้าลง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำความผิดต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

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

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

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

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

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

ถ้าการกระทำความผิดหนึ่ง เป็นการนำเข้าสู่ข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ

จะต้องรับโทษภายในราชอาณาจักร

หมวด ๒

พนักงานเจ้าหน้าที่

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๘ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจากรางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจากรางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมีได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจากรางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจากรางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ขีดหรืออาชั้ระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความคิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๕ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๔ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทีกเหตุอันควรเชื่อที่ทำได้ต้องใช้อำนาจตามมาตรา ๑๔ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทีกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่ทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๔ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทีกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๔ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การขีดหรืออาชั้ตามมาตรา ๑๔ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการขีดหรืออาชั้มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้วพนักงานเจ้าหน้าที่จะสั่งขีดหรืออาชั้ไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องขีดหรืออาชั้ไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลาขีดหรืออาชั้ได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะขีดหรืออาชั้หรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ขีดหรือถอนการอาชั้โดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา ๒๐ ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสอง ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้อง พร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีการสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา ๒๑ ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีการสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำความผิดคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกิน หกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้ตามมาตรา ๑๘ ต้องระวางโทษจำคุก ไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้ตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้อื่นผู้ใด ต้องระวางโทษ จำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ ได้ตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมาย วิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มีได้เกิดขึ้นจากการจงใจ มีคำมั่นสัญญา ชูเชิญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่มีข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการ ผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะราย และเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ให้บริการ นับตั้งแต่เริ่มให้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การให้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรี ประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้ และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๒๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงาน ฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์ หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ถิ่น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ

พลเอก สุรยุทธ์ จุลานนท์

นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำความผิดประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้อิทธิพล หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำความผิดดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

ประวัติผู้เขียน

ชื่อ ชื่อสกุล

ร้อยตำรวจเอกหญิงปิ่นพันธุ์ ชันเขต

ประวัติการศึกษา

นิติศาสตรบัณฑิต
มหาวิทยาลัยเกษมบัณฑิต
ปีที่สำเร็จการศึกษา พ.ศ.2548

ประสบการณ์ทำงาน

พ.ศ.2555-2557
พนักงานสอบสวน
สถานีตำรวจนครบาลสามเสน

พ.ศ.2557-ปัจจุบัน
รองสารวัตร (สอบสวน)
สถานีตำรวจนครบาลมีนบุรี