การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจาก
ข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์

นารี กิตติสมบูรณ์สุข

DPU

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

สาขาวิชานิติศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์

พ.ศ. 2549

ISBN 974-671-367-1

A search for evidence which is a personal information from the electronic data in Computer crime

Naree Kittisomboonsuk

DPU

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Laws

Department of Law

Graduate School, Dhurakij Pundit University

2006

ISBN 974-671-367-1

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้โดยความอนุเคราะห์เป็นอย่างดียิ่งอันผู้เขียนต้องขอกราบขอบพระคุณต่อท่าน รองศาสตราจารย์ ดร. อุดม รัฐอมฤต อาจารย์ที่ปรึกษา ซึ่งท่านได้ให้คำแนะนำและข้อคิดต่างๆ รวมทั้งตรวจแก้วิทยานิพนธ์จนสำเร็จ และต้องขอกราบพระคุณท่านอาจารย์ ดร. อุทัย อาทิเวช อาจารย์ที่ปรึกษาร่วม ที่ได้ให้คำแนะนำและข้อคิดต่างๆ

ผู้เขียนใคร่ขอขอบคุณท่าน ศาสตราจารย์ ดร. คณิต ณ นคร ประธานกรรมการสอบวิทยานิพนธ์ ท่านรองศาสตราจารย์ ดร. สุรศักดิ์ ลิขสิทธิ์วัฒนกุล และท่านอาจารย์ชาญเชาว์ ไชยานุกิจ ที่กรุณาสละเวลาอันมีค่าของท่านให้คำแนะนำ และเป็นกรรมการสอบวิทยานิพนธ์ฉบับนี้

นอกจากนี้ผู้เขียนใคร่ขอขอบคุณเพื่อนที่คอยให้กำลังใจ และให้ความช่วยเหลือข้าพเจ้าตลอดมา ตลอดจนครอบครัวของผู้เขียนอันได้แก่ คุณพ่อวรพจน์ กิตติสมบูรณ์สุข คุณแม่ฮุยใหม่ กิตติสมบูรณ์สุข พี่สาวคนโตนางสาวอนุสรณ์ กิตติสมบูรณ์สุข พี่ชายคนโตนายจรัส กิตติสมบูรณ์สุข พี่ชายคนรองนายเจริญกิตติสมบูรณ์สุข พี่ชายคนที่สามนายดำรงค์ กิตติสมบูรณ์สุข พี่ชายคนที่สี่นายเติมทรัพย์ กิตติสมบูรณ์สุข พี่ชายคนที่ห้านายอุดมศักดิ์ กิตติสมบูรณ์สุข พี่สาวคนสุดท้ายนางสาวอารีรัตน์ กิตติสมบูรณ์สุข พี่สะใภ้ทั้ง 5 คน และเหล่าหลานๆที่น่ารักทั้ง 8 คนที่คอยให้กำลังใจ และสนับสนุนผู้เขียนตลอดมา

ผู้เขียนสำนึกในความเมตตากรุณาของบุคคลต่างๆ ที่ได้กล่าวนามไว้ข้างต้นและปิติยินดีอย่างยิ่งที่ได้มีโอกาสเผยแพร่ประกาศเกียรติคุณของท่านให้ปรากฏไว้เป็นลายลักษณ์อักษรควบคู่กับวิทยานิพนธ์นี้ตลอดไป

คุณค่าของวิทยานิพนธ์ฉบับนี้ที่ขอมอบเป็นเครื่องบูชาพระคุณบิดา มารดา ครูบาอาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ให้แก่ข้าเจ้า ญาติพี่น้อง เพื่อนฝูง ผู้มีพระคุณทุกท่าน และขออาราธนาอำนาจคุณพระศรีรัตนตรัยและสิ่งศักดิ์สิทธิ์ในสากลโลกนี้ ให้ดลบันดาลให้ท่านเหล่านี้ มีความสุขสมปรารถนาทุกประการ

นารี กิตติสมบูรณ์สุข

สารบัญ

หน้า

บทคัดย่อภาษาไทย……. ฆ

บทคัดย่อภาษาอังกฤษ…… จ

กิตติกรรมประกาศ…….. ช

บทที่

1. บทนำ…… 1

1.1 ความเป็นมาและความสำคัญของปัญหา……. 1

1.2 สมมติฐานของวิทยานิพนธ์……... 2

1.3 วัตถุประสงค์ของการศึกษา…..…….. 3

1.4 วิธีการศึกษา…… 4

1.5 ขอบเขตของการศึกษา…… 4

1.6 ประโยชน์ที่คาดว่าจะได้รับ…… 4

2. การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์…….. 5

2.1 ความหมาย ความสำคัญ และประเภท ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล…….. 5

2.2 หลักเกณฑ์การคุ้มครองสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล..…… 14

2.3 การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในคดีอาญา……. 27

3. การเข้าถึงข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในกฎหมายต่างประเทศ……... 31

3.1 ประเทศสหรัฐอเมริกา…… 31

3.2 ประเทศอังกฤษ……. 38

3.3 ประเทศญี่ปุ่น……. 47

4. วิเคราะห์มาตรการทางกฎหมายในการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในประเทศไทย……. 55

4.1 มาตรการทางกฎหมายของไทยที่เกี่ยวกับคอมพิวเตอร์ที่มีในปัจจุบัน…..……... 55

4.2 วิเคราะห์ปัญหาที่ไม่อาจคุ้มครองสิทธิในข้อมูลข่าวสารส่วนบุคคลได้อย่างชัดเจน…… 63

DPU

สารบัญ (ต่อ)

หน้า

5. สรุปและเสนอแนะ…… 65

5.1 บทสรุป…….. 65

5.2 ข้อเสนอแนะ…….. 66

บรรณานุกรม…….. 69

DPU

หัวข้อวิทยานิพนธ์	การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์
ชื่อผู้เขียน	นารี กิตติสมบูรณ์สุข
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ดร. อุดม รัฐอมฤต
อาจารย์ที่ปรึกษาร่วม	ดร. อุทัย อาทิเวช
สาขาวิชา	นิติศาสตร์
ปีการศึกษา	2548

บทคัดย่อ

อาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมที่ร้ายแรงเป็นภัยต่อสังคมรูปแบบหนึ่ง ที่ก่อให้เกิดความเสียหายแก่ระบบเศรษฐกิจเป็นอย่างมาก แทบทุกประเทศต่างก็เล็งเห็นถึงอันตรายจากอาชญากรรมประเภทนี้ และผลกระทบที่เกิดกับกฎหมายอาญาของประเทศต่างๆ ทั่วโลก เนื่องจากกฎหมายอาญาที่ใช้อยู่ไม่เพียงพอที่จะดำเนินคดีกับอาชญากรได้ จึงพยายามหามาตรการทางกฎหมายใหม่ๆ เพื่อค้นหาวิธีการป้องกันและปราบปราม สำหรับประเทศไทยเป็นประเทศหนึ่งที่เห็นความสำคัญของปัญหาดังกล่าวจึงมีการร่างกฎหมายอาชญากรรมคอมพิวเตอร์ขึ้นเป็นกฎหมายเฉพาะ อย่างไรก็ตามสิ่งที่ควรคำนึงถึงควบคู่ไปกันไปคือการมีกฎหมายบังคับใช้ กล่าวคือต้องมีการปรับปรุงกฎหมายวิธีสบัญญัติให้มีประสิทธิภาพด้วย โดยเฉพาะปัญหาการรวบรวมพยานหลักฐานและการรับฟังพยานหลักฐานคอมพิวเตอร์ที่เป็นข้อมูลส่วนบุคคล

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 29 ได้บัญญัติรับรองสิทธิและเสรีภาพของประชาชนไว้เป็นหลักพื้นฐาน ซึ่งในทางปฏิบัติรัฐสามารถบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ในบางกรณี ดังนั้นจึงมีบทบัญญัติที่ให้อำนาจรัฐตรากฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ภายในขอบเขตที่รัฐธรรมนูญกำหนด เช่น ในมาตรา 37 บัญญัติรับรองคุ้มครองสิทธิความเป็นอยู่ส่วนตัวของบุคคล ซึ่งเป็นสิทธิส่วนบุคคล และรัฐธรรมนูญก็มีบทบัญญัติให้อำนาจรัฐกระทำการใดๆ ก็ได้หากเป็นกรณีที่กระทำไปเพื่อประโยชน์สาธารณะ ดังนั้นรัฐอาจอาศัยข้อยกเว้นดังกล่าวบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคลเกินความจำเป็น หรือตามอำเภอใจ โดยอ้าง “ประโยชน์สาธารณะ” เช่น รัฐอาจบัญญัติกฎหมายอนุญาตให้เจ้าหน้าที่ของรัฐเข้าตรวจสอบข้อมูลส่วนบุคคลของบุคคลใดบุคคลหนึ่งได้ตลอดเวลา ตามแต่จะเป็นสมควรโดยเฉพาะข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บอยู่

ในเครื่องคอมพิวเตอร์ เป็นต้น การกระทำดังกล่าวถือเป็นการกระทำที่กระทบกระเทือนต่อสาระสำคัญแห่งสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล ซึ่งจะมีผลตามบทบัญญัติในมาตรา 6 ที่ถือว่าบทบัญญัติดังกล่าวขัดหรือแย้งกับรัฐธรรมนูญซึ่งถือเป็นกฎหมายสูงสุดของประเทศ ทำให้บทบัญญัติดังกล่าวไม่สามารถใช้บังคับได้ ทั้งๆที่ การเข้าสู่ข้อมูลส่วนบุคคลนี้ เป็นมาตรการใหม่ที่รัฐสามารถนำมาใช้แสวงหาพยานหลักฐานเพื่อมาดำเนินคดีกับอาชญากรที่ก่ออาชญากรรมที่การแสวงหาพยานหลักฐานรูปแบบดั้งเดิมไม่สามารถแก้ปัญหาได้ เช่น อาชญากรรมคอมพิวเตอร์ ดังนั้น จึงควรมีการบัญญัติกฎหมายขึ้นมาให้อำนาจ และควบคุมการใช้อำนาจของเจ้าหน้าที่ของรัฐในการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลได้ ภายในขอบเขตที่ไม่เป็นการกระทบกระเทือนต่อสาระสำคัญแห่งสิทธิในข้อมูลข่าวสารส่วนบุคคล

พยานหลักฐานที่เป็นข้อมูลส่วนบุคคลโดยทั่วไปนอกจากจะได้รับความคุ้มครองตามประมวลกฎหมายอาญาแล้วยังได้รับความคุ้มครองตามรัฐธรรมนูญในส่วนของสิทธิส่วนบุคคล และสำหรับพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งมีลักษณะแตกต่างไปจากพยานหลักฐานทั่วๆ ไป กล่าวคือพยานหลักฐานประเภทนี้เป็นสิ่งที่ไม่มีรูปร่าง มองไม่เห็นด้วยตาเปล่า และอยู่ในรูปของคลื่นแม่เหล็กไฟฟ้า อาจถูกแก้ไขเปลี่ยนแปลง ลบ ทำลายได้ง่าย เจ้าหน้าที่ในกระบวนการยุติธรรมทั้งหลายจึงต้องประสบปัญหาในการดำเนินคดีกับผู้กระทำความผิด โดยเฉพาะพนักงานสอบสวนที่มีหน้าที่ในการรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดของจำเลยและนำเสนอต่อศาล ผู้วิจัยได้ทำการศึกษาวิจัยปัญหาการรวบรวมพยานหลักฐานและพิสูจน์พยานหลักฐานที่เป็นอิเล็กทรอนิกส์และเป็นข้อมูลส่วนบุคคล ภายในกรอบของ 3 หัวข้อใหญ่ ได้แก่ ลักษณะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ สิทธิส่วนบุคคล กระบวนการค้น และกระบวนการนำเสนอพยานหลักฐานต่อศาล ภายใต้สมมติฐานว่าการรวบรวมพยานหลักฐานที่เป็นการละเมิดสิทธิส่วนบุคคลที่ได้รับการคุ้มครองตามรัฐธรรมนูญและกฎหมายอาญาเจ้าหน้าที่ของรัฐสามารถกระทำได้เพียงใด ปัจจุบันมีกฎหมายฉบับใดให้อำนาจกระทำได้หรือไม่อย่างไร และควรจะกระทำอย่างไรเพื่อที่จะนำตัวผู้กระทำความผิดมาลงโทษให้ได้

ผลจากการศึกษาและวิเคราะห์ปัญหาทั้งในประเทศไทยและต่างประเทศ ตลอดจนศึกษาแนวทางแก้ไขปัญหาของต่างประเทศ โดยเฉพาะของประเทศสหรัฐอเมริกา อังกฤษ และญี่ปุ่น พบว่าการที่จะให้เจ้าหน้าที่ของรัฐเข้าถึงหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ได้เร็ว และไม่เป็นการละเมิดสิทธิในข้อมูลข่าวสารส่วนบุคคลจะต้องมีกฎหมายให้อำนาจในการปฏิบัติงานได้ ควรต้องมีองค์กรที่เป็นกลางเป็นผู้ให้อำนาจในการตรวจสอบการใช้อำนาจ และควรมีหลักกฎหมายลักษณะพยานหลักฐานเกี่ยวกับพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ที่ชัดเจนกว่านี้

Thesis Title Pursuing of electronic materials and personal data in Computer crime
Author Naree Kittisomboonsuk
Thesis Advisor Vice Prof. Dr. Udom Rathaarmarit
Co-Thesis Advisor Dr. Uthai Arthiveth
Department Law
Academic Year 2005

ABSTRACT

One of the most damage in Social is computerized criminal that destroying economics. In every country of the world realized this typical hazardous criminal and its effected. Due to insufficient criminal laws to indict them. Therefore the search of new suppressive and protective statues have been made with much effect. Thailand country also realized this crucial problem. Then proposing bill of computerized criminal however there must be concerned the usage of proper laws. Also developing criminal procedure effectiveness especially pursuing of personal data evidences and notified them.

The Kingdom of Thailand constitution B.E. 2540 code 29 provide basically for personal right and freedom which limited by state practice able to legislate laws in some case. Dealing with the constitution such as code 37 provide personal right protection. As same as the constitution provide state authority apply to public interests case. When state inhabited an exemption to legislate laws that too limited personal right and freedom informations. By claimable of public interests for instance, state made laws allowing officers to persue personal informations any of time. Especially those appropriate personal data from computers. The performance hold effected to right and freedom of person which have results according to the legislation code 6. Mean that the constitution, highest laws of country, was protected. It unable to extort even access to personal data became a new criterion of state in pursuing evidence to persecute criminals. The former procedure unable solving computerized criminal problems. So that could legislation laws for controlling authority performance of state officers uneffected in area of personal information right.

Generally said personal data evidence must protected by criminal procedure code and constitution in the differentiation of electronic data. The typical evidence have no shape, invisible and dwell in electromagnetic site which easily destroying or erasing. Especially when ascertain officers gathered all of them accusing to court. My studied in this research has 3 points of personal electronic data. Such as electronic evidence descriptions, personal right, persuing procedure and adducing evidence under hypothesis that violated personal right. Beneat the constitution and criminal procedure whether officers could do. Nowadays, whether laws provide authority and how the penalty of wrongdoers.

Problems analysis and results of this study received from Thailand and other countries' solution. Especially United States, England and Japan found that state officers could persuing electronic evidences rapidly. They also didn't violate personal right as dealing with laws and authority performance. There could have neutral organization checking the use of power. And should have electronic evidence description more obviously.

DPU

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเครื่องคอมพิวเตอร์เป็นเครื่องมือที่ให้คุณประโยชน์แก่มนุษย์มากมาย ไม่ว่าจะเป็นการใช้ในการติดต่อสื่อสาร วิทยาศาสตร์ การแพทย์ การศึกษา การปกครอง การทหาร การพาณิชย์ฯลฯ ในขณะที่เครื่องคอมพิวเตอร์ได้ก่อคุณประโยชน์นานัปการให้แก่มนุษย์ ก็ได้ก่อให้เกิดความเสียหายแก่มนุษย์ที่ไม่สามารถประเมินได้ หากจะได้นำไปใช้เป็นเครื่องมือในการกระทำความผิด เช่น อาชญากรรมที่เป็นการขโมยข้อมูล การปลอมแปลง การเผยแพร่ข้อมูลที่ไม่เหมาะสม การฟอกเงิน การแทรกแซงทางการค้า การค้าขายสิ่งผิดกฎหมาย เช่น การค้ายาเสพติด การขายบริการทางเพศ ฯลฯ

อาชญากรรมคอมพิวเตอร์ เป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่งที่เกี่ยวกับการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายหลักทรัพย์ และการฉ้อโกงประชาชน โดยเป็นการกระทำที่ดำเนินการและใช้คอมพิวเตอร์ในการกระทำความผิด ทำให้เหยื่อได้รับความเสียหายและผู้กระทำได้รับผลประโยชน์จากการกระทำนั้น ความเสียหายที่เกิดขึ้นก็มิได้เป็นความเสียหายแต่เฉพาะผู้เสียหายเพียงคนเดียวเท่านั้น แต่ยังก่อให้เกิดความเสียหายกับระบบเศรษฐกิจ สังคม ความสงบเรียบร้อย และความมั่นคงทั้งภายในและระหว่างประเทศ เป็นอาชญากรรมที่ยากแก่การสืบสวนติดตามและจับกุม เนื่องจากระยะเวลาในการกระทำความผิดก็เป็นไปอย่างรวดเร็ว ไม่มีขอบเขตจำกัด และไร้พรมแดน แตกต่างจากอาชญากรรมที่มีมาแต่เดิม[1]

ในขณะที่กฎหมายที่มีผลใช้บังคับยังคงเป็นกฎหมายเดิมๆ แต่การกระทำความผิดของอาชญากรพัฒนาไปตามการเจริญเติบโตของเทคโนโลยี ทำให้มาตรการทางกฎหมายที่มีมาแต่เดิมไม่สามารถนำมาบังคับใช้กับการกระทำความผิดที่เกิดขึ้นได้อย่างมีประสิทธิภาพ เนื่องจากการใช้กฎหมายอาญาจะต้องยึดถือหลัก “ไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย” (nullum crimen nulla poena sine lege)

---

[1] วีระพงษ์ บุญโญภาส. (2544). **อาชญากรรมทางเศรษฐกิจ** (พิมพ์ครั้งที่ 3). หน้า 109–110.

ปัญหาอาชญากรรมคอมพิวเตอร์จึงเป็นปัญหาที่นานาอารยประเทศต่างให้ความสนใจ และได้พยายามวางมาตรการขึ้นเพื่อแก้ไขปัญหาที่เกิดขึ้น ประเทศไทยเองก็มีความจำเป็นเร่งด่วนในการหาทางแก้ไขโดยการวางมาตรการที่สามารถแก้ไขปัญหาได้อย่างแท้จริง

อย่างไรก็ตาม การออกกฎหมายมาใช้จะต้องคำนึงถึงทางปฏิบัติ เพื่อให้เกิดผลบังคับได้อย่างแท้จริง โดยเฉพาะในเรื่องของการรวบรวบพยานหลักฐาน ซึ่งเป็นหัวใจสำคัญของการดำเนินคดีอาญา โดยที่พยานหลักฐานในความผิดอาชญากรรมคอมพิวเตอร์เป็นข้อมูลอิเล็กทรอนิกส์ที่กฎหมายจะต้องให้อำนาจเจ้าหน้าที่ของรัฐในการแสวงหา โดยจะต้องไม่เป็นการล่วงละเมิดต่อสิทธิเสรีภาพในข้อมูลข่าวสารส่วนบุคคลที่ได้รับความคุ้มครองตามรัฐธรรมนูญอย่างไม่เป็นธรรม และตัวเจ้าพนักงานของรัฐเองก็จะต้องเป็นผู้ที่มีความรู้ความสามารถทางด้านนี้อย่างแท้จริง

1.2 สมมติฐานของวิทยานิพนธ์

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 29 ได้บัญญัติรับรองสิทธิและเสรีภาพของประชาชนไว้เป็นหลักพื้นฐาน ซึ่งในทางปฏิบัติรัฐสามารถบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ในบางกรณี ดังนั้นจึงมีบทบัญญัติที่ให้อำนาจรัฐตรากฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ภายในขอบเขตที่รัฐธรรมนูญกำหนด เช่น ในมาตรา 37 บัญญัติรับรองคุ้มครองสิทธิความเป็นอยู่ส่วนตัวของบุคคล ซึ่งเป็นสิทธิส่วนบุคคล และรัฐธรรมนูญก็มีบทบัญญัติให้อำนาจรัฐกระทำการใดๆ ก็ได้หากเป็นกรณีที่กระทำไปเพื่อประโยชน์สาธารณะ ดังนั้นรัฐอาจอาศัยข้อยกเว้นดังกล่าวบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคลเกินความจำเป็น หรือตามอำเภอใจ โดยอ้าง “ประโยชน์สาธารณะ” เช่น รัฐอาจบัญญัติกฎหมายอนุญาตให้เจ้าหน้าที่ของรัฐเข้าตรวจสอบข้อมูลส่วนบุคคลของบุคคลใดบุคคลหนึ่งได้ตลอดเวลา ตามแต่จะเป็นสมควรโดยเฉพาะข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ เป็นต้น การกระทำดังกล่าวถือเป็นการกระทำที่กระทบกระเทือนต่อสาระสำคัญแห่งสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล ซึ่งจะมีผลตามบทบัญญัติในมาตรา 6 ที่ถือว่าบทบัญญัติดังกล่าวขัดหรือแย้งกับรัฐธรรมนูญซึ่งถือเป็นกฎหมายสูงสุดของประเทศ ทำให้บทบัญญัติดังกล่าวไม่สามารถใช้บังคับได้ ทั้งๆที่ การเข้าสู่ข้อมูลส่วนบุคคลนี้ เป็นมาตรการใหม่ที่รัฐสามารถนำมาใช้แสวงหาพยานหลักฐานเพื่อมาดำเนินคดีกับอาชญากรที่ก่ออาชญากรรมที่การแสวงหาพยานหลักฐานรูปแบบดั้งเดิมไม่สามารถแก้ปัญหาได้ เช่น อาชญากรรมคอมพิวเตอร์ ดังนั้น จึงควรมีการบัญญัติกฎหมายขึ้นมาให้อำนาจ และควบคุมการใช้อำนาจของเจ้าหน้าาที่ของรัฐในการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลได้ ภายในขอบเขตที่ไม่เป็นการกระทบกระเทือนต่อสาระสำคัญแห่งสิทธิในข้อมูลข่าวสารส่วนบุคคล

1.3 วัตถุประสงค์ของการศึกษา

1.3.1 ศึกษามาตรการทางกฎหมายของประเทศไทย และกฎหมายต่างประเทศเกี่ยวกับวิธีการและขั้นตอนในการรวบรวมพยานหลักฐานที่เป็นข้อมูลข่าวสารส่วนบุคคลที่อยู่ในเครื่องคอมพิวเตอร์ ได้แก่ กฎหมายที่คุ้มครองสิทธิในข้อมูลข่าวสารส่วนบุคคล กฎหมายที่ให้อำนาจเจ้าพนักงานของรัฐเข้าสู่ข้อมูลข่าวสารส่วนบุคคล และการรับฟังเป็นพยานหลักฐานในคดีได้

1.3.2 วิเคราะห์ปัญหาความขัดแย้งระหว่างบทบัญญัติของกฎหมาย และการใช้อำนาจของเจ้าพนักงานของรัฐในการรวบรวมพยานหลักฐานที่เป็นข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์

1.3.3 ศึกษาแนวทางการแก้ปัญหาการรวบรวมพยานหลักฐานที่เป็นข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ในต่างประเทศ และวิเคราะห์กรณีที่นำมาใช้ในประเทศไทย

1.4 วิธีการศึกษา

ศึกษาจากเอกสารที่เป็นตัวบทกฎหมาย คำพิพากษา ตำรา บทความภาษาไทย และภาษาต่างประเทศ เพื่อนำมาเป็นข้อมูลในการวิเคราะห์และเปรียบเทียบเพื่อให้เกิดองค์ความรู้และเป็นแนวทางในการแก้ไขปัญหาที่เหมาะสม

1.5 ขอบเขตของการศึกษา

ทำการศึกษาถึงข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคล และวิเคราะห์หลักกฎหมายวิธีพิจารณาความอาญาที่มีอยู่ว่าจะนำมาใช้กับการเข้าถึงข้อมูลส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ได้เพียงใด โดยจะทำการศึกษาเปรียบเทียบกับกฎหมายต่างประเทศที่เกี่ยวข้องกับการแสวงหาข้อมูลอิเล็กทรอนิกส์ไปเป็นพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ได้ทราบแนวทางสำหรับการกำหนดมาตรการใช้อำนาจของรัฐในการแสวงหาพยานหลักฐานจากข้อมูลอเล็กทรอนิกส์ที่สามารถแก้ปัญหาอาชญากรรมคอมพิวเตอร์ให้ได้อย่างมีประสิทธิภาพ และเหมาะสม คำนึงถึงการคุ้มครองข้อมูลข่าวสารส่วนบุคคล

1.6.2 สามารถนำไปใช้ในการบัญญัติกฎหมาย การแก้ไขปรับปรุงกฎหมาย และการปฏิบัติตามกฎหมายที่เกี่ยวข้องเพื่อให้ตรงตามเจตนารมณ์ของรัฐธรรมนูญ

DPU

บทที่ 2
การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์

ขั้นตอนที่สำคัญขั้นตอนหนึ่งในการดำเนินกระบวนการยุติธรรมทางอาญา นั่นคือการดำเนินคดีอาญาชั้นก่อนฟ้อง (Vorverfahren) คือ การดำเนินการทั้งปวงของเจ้าพนักงานก่อนการยื่นฟ้อง ได้แก่ การสอบสวนของพนักงานสอบสวนและการดำเนินการของพนักงานอัยการก่อนการยื่นฟ้อง [1] และในการดำเนินการสอบสวนก็ครอบคลุมเนื้อหา 2 ประการ ได้แก่ การรวบรวมพยานหลักฐานและการใช้มาตรการบังคับ [2] ดังนั้นการแสวงหาและรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดจึงเป็นขั้นตอนก่อนการฟ้อง เมื่อมีการกระทำความผิดอาญาเกิดขึ้นการที่จะลงโทษผู้กระทำความผิดได้จะต้องมีการรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิด ถ้าไม่มีพยานหลักฐานก็ไม่สามารถที่จะดำเนินกระบวนการยุติธรรมทางอาญาขั้นตอนอื่นๆ ต่อไปได้ เมื่อพยานหลักฐานที่จะนำมาพิสูจน์การกระทำความผิดเป็นส่วนสำคัญของกระบวนการยุติธรรมทางอาญา ผู้กระทำความผิดก็ย่อมที่จะปกปิด ซ่อนเร้น พยานหลักฐานดังกล่าวอยู่ในคอมพิวเตอร์หรือสื่ออิเล็กทรอนิกส์ต่างๆ ซึ่งข้อมูลจากสื่อเหล่านี้อาจใช้เป็นพยานหลักฐานในคดีอาญาได้

ด้วยเหตุนี้กฎหมายวิธีพิจารณาความอาญาจึงต้องมีเครื่องมือในการแสวงหาพยานหลักฐาน ในที่นี้ได้แก่การค้น ซึ่งเป็นมาตรการบังคับในการดำเนินคดีอาญาประการหนึ่ง ซึ่งในที่นี้เป็นการค้นหาพยานหลักฐานจากเครื่องคอมพิวเตอร์หรือสื่ออิเล็กทรอนิกส์ต่างๆ เฉพาะที่เป็นข้อมูลส่วนบุคคล และเป็นมาตรการบังคับที่รุนแรงมาก เพราะเป็นมาตรการบังคับที่กระทบถึงสิทธิและเสรีภาพของบุคคล ดังนั้นจึงจำเป็นที่จะต้องเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ เพื่อประโยชน์ในการแสวงหาพยานหลักฐานที่มีลักษณะดังกล่าวต่อไป

---

[1] คณิต ณ นคร. (2546). **กฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 6, แก้ไขเพิ่มเติม ปรับปรุงใหม่). หน้า 308.

[2] คณิต ณ นคร. เล่มเดิม. หน้า 313.

2.1 ความหมาย ความสำคัญ และประเภท ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

2.1.1 ความหมายของข้อมูลอิเล็กทรอนิกส์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 ให้ความหมายคำว่า "ข้อมูลอิเล็กทรอนิกส์" หมายถึง ข้อความที่ได้ส่ง รับ เก็บรักษาหรือประมวลผลด้วยวิธีการอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์หรือโทรสาร

มาตรา 4 ยังได้ให้คำนิยามคำว่า อิเล็กทรอนิกส์ ข้อความ ระบบข้อมูล การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ ผู้ส่งข้อมูล ผู้รับข้อมูล และบุคคลที่เป็นสื่อกลาง ไว้ดังนี้

"อิเล็กทรอนิกส์" หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่างๆ เช่นว่านั้น

"ข้อความ" หมายความว่า เรื่องราวหรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ

"ระบบข้อมูล" หมายความว่า กระบวนการประมวลผลด้วยเครื่องมืออิเล็กทรอนิกส์สำหรับ สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลข้อมูลอิเล็กทรอนิกส์

"การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์" หมายความว่า การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

"ผู้ส่งข้อมูล" หมายความ บุคคลซึ่งผู้ส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีที่ผู้นั้นกำหนด โดยบุคคลนั้นอาจจะส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

"ผู้รับข้อมูล" หมายความว่า บุคคลซึ่งผู้ส่งข้อมูลประสงค์จะส่งข้อมูลอิเล็กทรอนิกส์ให้และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

"บุคคลที่เป็นสื่อกลาง" หมายความว่า บุคคลซึ่งกระทำการในนามผู้อื่นในการส่ง รับ หรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์อันใดอันหนึ่งโดยเฉพาะ รวมถึงให้บริการอื่นที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น

DPU

นอกจากนี้ยังมีร่างกฎหมายเกี่ยวกับกิจการอินเตอร์เน็ต โดยคณะกรรมการกฎหมายได้เสนอร่างพระราชบัญญัติส่งเสริมกิจการอินเตอร์เน็ต ร่าง 1 ให้นิยามคำว่า คอมพิวเตอร์ อินเตอร์เน็ต ข้อมูลและข้อมูลข่าวสาร[3] ดังนี้

"คอมพิวเตอร์" หมายความว่า อุปกรณ์ที่ใช้ประมวล วิเคราะห์ข้อมูล ซึ่งทำงานด้วยอิเล็กทรอนิกส์แม่เหล็กไฟฟ้าใยแก้ว อิเล็กทรอนิกส์หรืออุปกรณ์ที่เชื่อมต่อ หรือเกี่ยวข้องกับอุปกรณ์ดังกล่าว ซึ่งใช้งานด้วยเหตุผลทางวิทยาศาสตร์ คณิตศาสตร์ เก็บบันทึกและแสดงข้อมูลและหมายรวมถึงการเก็บบันทึกข้อมูลหรือการสื่อสารที่ต่อเชื่อมโดยตรง หรือใช้งานร่วมกับอุปกรณ์นั้นๆ หรืออุปกรณ์ที่เชื่อมต่อระหว่างอุปกรณ์ดังกล่าว แต่ไม่รวมตลอดถึงเครื่องพิมพ์อักษรอัตโนมัติ หรือเครื่องติดตั้งตัวอักษร หรือคำนวณตัวเลขแบบพกพา หรืออุปกรณ์ร่วมทั้งการเผยแพร่ Program ด้วยวิธีใดๆ

"อินเตอร์เน็ต" หมายความว่า ระบบเครือข่ายที่มีเครื่องคอมพิวเตอร์เชื่อมโยงกันทั่วโลก โดยอาศัยการสื่อสารด้วยระเบียบวิธีในการสื่อสารกันระหว่างเครื่องคอมพิวเตอร์ เชื่อมต่อกันในระบบปฏิบัติการแบบมีผู้ใช้หลายคน

"ข้อมูล" หมายความว่า สิ่งที่เป็นข้อเท็จจริง เช่น ข้อความ จำนวนเลข เสียงและภาพ ซึ่งแสดงในรูปแบบที่คอมพิวเตอร์สามารถประมวลผลได้

"ข้อมูลข่าวสาร" หมายความว่า สิ่งที่สื่อความหมาย

และร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ได้ให้ความหมายของคำว่า ระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ ไว้ดังนี้

"ระบบคอมพิวเตอร์" ในพระราชบัญญัตินี้ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดชุดคำสั่งและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ หรือชุดคำสั่ง บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้

เมื่อพิจารณาจากความหมายของคำว่า "ระบบคอมพิวเตอร์" จากร่างพระราชบัญญัติส่งเสริมกิจการอินเตอร์เน็ต ร่าง 1 และร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ข้างต้น "ระบบคอมพิวเตอร์" จึงได้แก่ฮาร์ดแวร์และซอฟต์แวร์ที่พัฒนาขึ้นเพื่อประมวลผลข้อมูลดิจิทัล (digital data) อันประกอบด้วยเครื่องคอมพิวเตอร์ และอุปกรณ์รอบข้าง

---

[3] คณะกรรมการบริหารสมาคมอินเตอร์เน็ตนานาชาติ ประเทศไทย, "ร่างพระราชบัญญัติส่งเสริมกิจการอินเตอร์เน็ต พ.ศ. …….. (ร่าง 1)," <http://www.acm.th.org/law/internetlaw1b.html>

(peripheral) ต่างๆ ในการรับเข้าหรือป้อนข้อมูล (input) นำออกหรือแสดงผลข้อมูล (output) และบันทึกหรือเก็บข้อมูล (store and record) ดังนั้น ระบบคอมพิวเตอร์จึงอาจเป็นอุปกรณ์เพียงเครื่องเดียว หรือหลายเครื่องอันมีลักษณะเป็นชุดเชื่อมต่อกันโดยอาจผ่านระบบเครือข่าย และมีลักษณะการทำงานโดยอัตโนมัติตามโปรแกรมที่กำหนดไว้ และไม่มีการแทรกแซงโดยตรงจากมนุษย์ ส่วนโปรแกรมคอมพิวเตอร์จะหมายถึงชุดคำสั่งที่ทำหน้าที่สั่งการให้คอมพิวเตอร์ทำงาน

ดังนั้นข้อมูลคอมพิวเตอร์ จึงไม่ใช่เฉพาะตัวอักขระ หรือข้อความที่สื่อความหมาย อ่านเข้าใจได้ที่หน้าจอภาพ (monitor) เท่านั้น แต่เป็นข้อมูลดิจิทัลที่อยู่ในระบบคอมพิวเตอร์ และอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้

ตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 มาตรา 4 ให้ความหมายคำว่า “ข้อมูลข่าวสาร” “ข้อมูลข่าวสารส่วนบุคคล” ดังนี้

คำว่า “ข้อมูลข่าวสาร” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

คำว่า “ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

ตามร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. … มาตรา 4 ได้ให้ความหมายคำว่า “ข้อมูลส่วนบุคคล” “บันทึกข้อมูลส่วนบุคคล” ดังนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อเท็จจริงเกี่ยวกับตัวบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม

“บันทึกข้อมูลส่วนบุคคล” หมายความว่า เอกสาร ฐานข้อมูล หรือรูปภาพหรือสิ่งซึ่งแสดงภาพของบุคคลในรูปแบบอื่น ทั้งนี้ไม่รวมถึงสิ่งพิมพ์ซึ่งเผยแพร่ทั่วไปหรือเอกสารที่เก็บไว้ในห้องสมุด หอศิลปะ หรือพิพิธภัณฑ์ เพื่อประโยชน์ในการใช้อ้างอิง การศึกษา การจัดนิทรรศการ หรือเอกสารที่เป็นอนุสรณ์ หรือจดหมายหรือสิ่งอื่นใดที่มีการส่งในทางปกติธุระของการไปรษณีย์ เว้นแต่ข้อความจะกำหนดไว้เป็นอย่างอื่น

เมื่อพิจารณาตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 และร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...ความหมายของคำว่าข้อมูลส่วนบุคคล ควรหมายถึง ข้อมูลข่าวสารที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคล และเป็นข้อมูลที่ได้รับความคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ไม่เปิดเผยต่อผู้ที่ไม่มีสิทธิรับรู้ แม้หลักพื้นฐานของที่สำคัญ 2 ประการของของข้อมูลข่าวสารของราชการนั้น ได้แก่ หลักที่ว่าบุคคลไม่จำต้องเป็นผู้มีส่วนได้เสียกับข้อมูลข่าวสารส่วนที่ขอ และเปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น[4] แต่ในเรื่องข้อมูลข่าวสารส่วนบุคคลนี้ กฎหมายต้องการคุ้มครองความเป็นอยู่ส่วนบุคคลตามที่รัฐธรรมนูญได้บัญญัติไว้ในมาตรา 34 ดังนั้น จึงได้กำหนดหลักการสำคัญแตกต่างไปจากข้อมูลข่าวสารของทางราชการ โดยกำหนดไว้เป็นหลักการว่า "ข้อมูลข่าวสารส่วนบุคคลจะเปิดเผยต่อบุคคลอื่นโดยปราศจากความยินยอมมิได้ เว้นแต่จะเข้าข้อยกเว้น" โดยกฎหมายฉบับนี้ได้บัญญัติเป็นข้อยกเว้นไว้ในมาตรา 24

ข้อมูลข่าวสารส่วนบุคคลนั้นอาจเป็นข้อมูลของบุคคลที่ยังมีชีวิตอยู่ หรือแม้กระทั่งผู้ที่ถึงแก่กรรมไปแล้ว เพราะหากข้อมูลของบุคคลเหล่านั้นถูกเปิดเผยออกไปก็อาจเป็นผลร้ายแก่ชื่อเสียงของผู้ตาย ญาติพี่น้อง หรือวงศ์ตระกูลได้[5]

2.1.2 การประมวลผลข้อมูล (Data Processing) เมื่อมีข้อมูลเกิดขึ้น หรือมีการรวบรวมข้อมูลต่างๆ ขึ้น วิธีการจัดการข้อมูล ไม่ว่าการคำนวณ การเรียงลำดับ หรือการจัดกลุ่ม ต่างก็เป็นการประมวลผล (Processing) ทั้งสิ้น การประมวลผล จึงหมายถึง วิธีการจัดการกับข้อมูล โดยมีจุดมุ่งหมายเพื่อให้ได้ผลลัพธ์อย่างใดอย่างหนึ่ง ข้อสรุปที่ได้ เรียกว่าข้อสนเทศ (Information) ซึ่งสามารถนำไปใช้ในการตัดสินใจต่างๆ ที่เกี่ยวข้อง ขึ้นอยู่กับการนำไปใช้ประโยชน์ของแต่ละคน

ก. ขั้นตอนของการประมวลผลข้อมูล[6] แบ่งเป็น 3 ขั้นตอน ได้แก่

(1) การเตรียมข้อมูล (Input) การเตรียมข้อมูล (Input) คือการเก็บรวบรวมข้อมูลเพื่อรอประมวลผล ซึ่งหมายรวมถึงการเปลี่ยนสภาพข้อมูลให้อยู่ในรูปแบบที่เหมาะสมและพร้อมที่จะประมวลผลต่อไป การเปลี่ยนสภาพข้อมูลประกอบด้วย

- การลงรหัส (Coding) หมายถึงการให้รหัสแทนข้อมูลจริง ทำให้ข้อมูลอยู่ในรูปแบบที่กะทัดรัดสะดวกแก่การประมวลผล ซึ่งรหัสที่ใช้อาจเป็นตัวเลขหรือตัวอักษรก็ได้ เช่น ข้อมูลเพศชาย ใช้แทนด้วยตัว ช. ส่วนเพศหญิงใช้ตัว ญ. เป็นต้น

---

[4] หฤทัย หงส์สิริ และ มานิต จุมปา. (2542). **คำอธิบายข้อมูลข่าวสารของทางราชการ**. หน้า 86.

[5] หฤทัย หงส์สิริ และ มานิต จุมปา. เล่มเดิม. หน้า 19.

[6] วัชราภรณ์ สุริยาภิวัฒน์. (2543). **คอมพิวเตอร์เบื้องต้นและเทคนิคการเขียนโปรแกรม**. หน้า 26-27.

- การบรรณาธิกรณ์ (Editing) หมายถึงการตรวจสอบความถูกต้องและความเป็นไปได้ของข้อมูลและปรับปรุงแก้ไขเท่าที่จะทำได้ เช่น ผู้ให้ข้อมูลเป็นเพศหญิง แต่ตอบว่าเคยเกณฑ์ทหาร ก็ต้องทำการตรวจสอบโดยพิจารณาจากคำตอบที่ได้จากคำถามข้ออื่น หรือไปสอบถามใหม่ แล้วแก้ไข

- การแยกประเภท (Classifying) หมายถึงการจัดประเภทข้อมูลให้เป็นกลุ่มตามลักษณะต่างๆ ของข้อมูล เพื่อสะดวกต่อการประมวลผลต่อไป

- การบันทึกข้อมูลในสื่อ (Media) ที่เหมาะสม หมายถึงการจัดเตรียมข้อมูลให้อยู่ในสื่อหรืออุปกรณ์ที่ใช้ได้กับเครื่องมือการประมวลผลที่มีอยู่ เช่นบันทึกข้อมูลลงแผ่นดิสก์ หรือเทปแม่เหล็กเพื่อนำไปประมวลผลด้วยเครื่องคอมพิวเตอร์ต่อไป

(2) การประมวลผล (Processing) หมายถึงวิธีการจัดการกับข้อมูล ซึ่งอาจเป็นการคำนวณการรวมข้อมูลมากกว่าหนึ่งชุดเข้าด้วยกัน (Merge) การดึงข้อมูลมาใช้ (Retrieve) หรือการเรียงลำดับ (Sort)

(3) การนำเสนอผลลัพธ์ (Output) หมายถึงการนำผลลัพธ์ที่ได้จากการประมวลผลมาแสดงให้ทราบ เช่น แสดงผลสรุปในรูปของตาราง หรือกราฟ

ข. ประเภทของการประมวลผลข้อมูล[7] เมื่อพิจารณาจากอุปกรณ์ที่ใช้เป็นหลัก สามารถแบ่งการประมวลผลข้อมูลได้ 3 ประเภท

(1) การประมวลผลข้อมูลด้วยมือ (Manual Data Processing) เป็นวิธีการประมวลผลข้อมูลที่มีมาแต่เดิม อุปกรณ์ที่ใช้ได้แก่ กระดาษทด เครื่องคิดเลข ลูกคิด ใช้กับข้อมูลที่มีจำนวนน้อยและการคำนวณไม่ยุ่งยาก และเป็นงานที่ไม่รีบเร่ง

(2) การประมวลผลข้อมูลด้วยเครื่องจักรกล (Mechanical Data Processing) เป็นการใช้แรงงานคนร่วมกับเครื่องจักร ที่ใช้กันมากได้แก่ เครื่องจักรทำบัญชี ซึ่งเป็นเครื่องประมวลผลประเภทกึ่งอิเล็กทรอนิกส์ที่เรียกว่า “เครื่อง Unit Record” เช่น เครื่องเจาะบัตร (Card Punch) เครื่องรวมบัตร (Collator) เครื่องเรียงบัตร (Card Sorter) เครื่องแปลบัตร (Interpreter) ฯลฯ เป็นการประมวลผลที่เหมาะกับงานระดับกลางที่มีข้อมูลไม่มากนักและต้องการความรวดเร็วในการทำงานปานกลาง

(3) การประมวลผลข้อมูลด้วยเครื่องคอมพิวเตอร์ (Electronic Data Processing - EDP.) หมายถึงการประมวลผลข้อมูลด้วยเครื่องอิเล็กทรอนิกส์ และเครื่องอิเล็กทรอนิกส์ที่ใช้ก็คือคอมพิวเตอร์นั่นเอง เหมาะกับงานที่มีปริมาณมาก และมีขั้นตอนการทำงานซ้ำๆกัน ต้องการ

---

[7] วัชราภรณ์ สุริยาภิวัฒน์. เล่มเดิม. หน้า 28-29.

ประสิทธิภาพในการทำงาน ให้ผลลัพธ์ที่ถูกต้อง เป็นการคำนวณที่มีสูตรยุ่งยากซับซ้อน และเป็นงานที่ต้องการภาพพจน์ที่ทันสมัย ฯลฯ

2.1.3 ระบบและประโยชน์ของเครือข่ายคอมพิวเตอร์

ก. ระบบเครือข่ายคอมพิวเตอร์ เป็นระบบการสื่อสารที่ประกอบด้วยเครื่องคอมพิวเตอร์หลายเครื่องเชื่อมต่อถึงกันเพื่อให้ผู้ใช้คอมพิวเตอร์สามารถสื่อสารถึงกัน ใช้ข้อมูลร่วมกัน หรือเพื่อแลกเปลี่ยนข้อมูลระหว่างกัน การเชื่อมโยงของระบบเครือข่ายจะผ่านช่องทางการสื่อสารต่างๆ กัน เช่น สายโทรศัพท์ สายไฟฟ้า หรือผ่านสื่อกลาง เช่น ไมโครเวฟ [8] เป็นต้น การแบ่งประเภทระบบเครือข่ายสามารถแบ่งได้จากลักษณะการติดตั้งทางภูมิศาสตร์ แบ่งได้ 3 แบบ ได้แก่

(1) เครือข่ายท้องถิ่น (Local Area Network หรือ LAN) เป็นเครือข่ายระยะใกล้ เช่น ภายในอาคารสำนักงาน เป็นต้น ระบบเครือข่ายชนิดนี้จะช่วยให้สะดวกในการติดต่อ ช่วยลดต้นทุน

(2) เครือข่ายระดับเมือง (Metropolitan Area Network หรือ MAN) เป็นเครือข่ายขนาดกลาง ใช้ภายในเมืองหรือจังหวัด เช่น เคเบิลทีวี

(3) เครือข่ายระดับประเทศ (Wide Area Network หรือ WAN) เป็นเครือข่ายที่มีขนาดใหญ่ ติดตั้งใช้งานในบริเวณกว้าง มีสถานีจุดเชื่อมมากมาย ต้องใช้สื่อกลางหลายชนิด เช่น ระบบคลื่นวิทยุ ไมโครเวฟ หรือดาวเทียม เป็นต้น

(4) ระบบเครือข่ายระหว่างประเทศ (International Network หรือ Inter-Net) เป็นระบบที่ติดต่อข้ามประเทศโดยใช้สายเคเบิล หรือดาวเทียม

จะเห็นได้ว่าระบบเครือข่ายช่วยให้เกิดความรวดเร็วในการติดต่อสื่อสาร ทำให้การส่งข้อมูลข่าวสารในยุคโลกาภิวัฒน์สามารถทำได้สะดวกสบายมากขึ้น ไม่ว่าจะอยู่ในส่วนใดของโลกก็สามารถส่งผ่านข้อมูลข่าวสารถึงกันได้ และแต่ละเครือข่ายก็สามารถเชื่อมกับเครือข่ายอื่นๆ ได้ โดยผ่านคอมพิวเตอร์ขนาดใหญ่ที่มีระบบปฏิบัติงานข่ายงาน (Network Operating System) เป็นซอฟท์แวร์ควบคุมข่ายงาน และมีแผ่นวงจรข่ายงาน (Network Interface Card) คอยควบคุมให้คอมพิวเตอร์ในเครือข่ายเดียวกันทำงานประสานกัน และมีฮาร์ดแวร์ ที่เรียกว่า “เกตเวย์ (Gateway)” คอมพิวเตอร์ในแต่ละจุดจะทำหน้าที่เสมือนเป็นตัวเชื่อมและควบคุม เรียกว่า “สะพาน (Bridge)” มีการเชื่อมคอมพิวเตอร์ให้ถูกต้องตามลักษณะที่เหมาะสม โดยจัดให้มีคอมพิวเตอร์ที่มีความสามารถสูงเครื่องหนึ่ง เป็นเครื่องกลางที่ทำหน้าที่ควบคุมเครือข่ายงานและแฟ้มข้อมูล ลักษณะเหมือนเป็น

---

[8] ระบบไมโครเวฟ เป็นระบบการสื่อสารแบบไม่มีสาย ชนิดที่เป็นคลื่นวิทยุที่มีความถี่ระหว่าง 300 Mhs และ 30 Ghs และเดินทางเป็นเส้นตรง อุปกรณ์ที่ใช้ในการรับส่ง คือ จานสัญญาณไมโครเวฟ ซึ่งมักติดตั้งในที่สูง ข้อดี คือสามารถส่งสัญญาณด้วยความถี่กว้าง และแทบจะไม่มีการรบกวนจากภายนอก ข้อเสียคือถ้าทิศทางการส่งมีสิ่งกีดขวางจะทำให้การส่งสัญญาณทำได้ไม่ดี

DPU

แม่ข่าย หรือตัวบริการแฟ้มข้อมูล (File Server) ให้คอมพิวเตอร์เครื่องอื่นๆ เชื่อมโยงเข้ามาหาคอมพิวเตอร์ที่เป็นแม่ข่ายตัวนี้ ลักษณะการเชื่อมโยงนี้ เรียกว่า "โทโพโลยี (Topology)

ข. ประโยชน์ของเครือข่ายคอมพิวเตอร์ การนำคอมพิวเตอร์เข้ามาประยุกต์ในการดำเนินงานต่างๆ โดยการเชื่อมโยงคอมพิวเตอร์หลายๆ เครื่องเข้าด้วยกัน จัดทำเป็นระบบเครือข่าย ทำให้เกิดความสะดวกสบายและรวดเร็วในการการสื่อสารข้อมูลระหว่างบุคคล เพราะปัจจุบันมีเครือข่ายคอมพิวเตอร์เชื่อมโยงไปทั่วโลก โดยเฉพาะเครือข่ายที่เรียกว่า "อินเตอร์เน็ต (Internet)" ซึ่งมีเครือข่ายเชื่อมโยงคอมพิวเตอร์ครอบคลุมไปทั่วโลกภายใต้มาตรฐานเดียวกัน มาตรฐานดังกล่าวทำให้คอมพิวเตอร์ในเครือข่ายพูดภาษาเดียวกัน ทำให้คนสามารถติดต่อและรับรู้ข่าวสารกันได้รวดเร็ว เป็นประโยชน์อย่างมากในทุกๆ ด้าน เช่น

(1) ด้านธุรกิจ เครือข่ายที่มีประโยชน์ทางธุรกิจ เช่น ธนาคาร มีระบบออนไลน์บนเครือข่ายช่วยให้สามารถสอบถามยอดเงิน หรือโอนเงินได้รวดเร็ว การติดต่อระหว่างสำนักงานใหญ่และสาขาก็สามารถทำได้อย่างสะดวกรวดเร็ว

(2) ด้านการศึกษา มีการศึกษาทางไกล (Tele Education) เป็นการค้นคว้าทางวิชาการ การแบ่งปันหรือถ่ายทอดความรู้ระหว่างบุคคลที่อยู่ห่างไกลกัน

(3) ด้านการแพทย์ มีการแพทย์ทางไกล (Tele Medicine) โดยนำระบบเครือข่ายมาใช้ในการเก็บทะเบียนประวัติคนไข้ โดยใช้ฐานข้อมูลร่วมกัน มีการปรึกษาวินิจฉัยโรค และรักษาผ่านเครือข่ายคอมพิวเตอร์

(4) ด้านความมั่นคงปลอดภัยระหว่างประเทศ เช่น การเก็บประวัติอาชญากรด้วยฐานข้อมูลเดียวกัน โดยทุกสถานีตำรวจมีเครือข่ายคอมพิวเตอร์ที่สามารถเรียกและตรวจสอบข้อมูลได้ ทำให้การปราบปรามอาชญากรรมสามารถทำได้รวดเร็วทันต่อเหตุการณ์

(5) ด้านการสื่อสาร โดยการส่งจดหมายอิเล็กทรอนิกส์ ที่เรียกว่า "E-Mail (Electronic Mail) ซึ่งช่วยให้การสื่อสารทางไกลสะดวกและรวดเร็ว เพราะสามารถสื่อสารกันได้ทั้งจดหมาย ภาพ หรือเสียง นอกจากนี้ยังมีบริการอื่นๆ อีกหลายชนิดบนเครือข่ายอินเตอร์เน็ต เช่น จดหมายข่าว หรือจดหมายเวียน (Mail) การใช้คอมพิวเตอร์บนเครื่องอื่น (Telnet) และการขนถ่ายแฟ้ม (FTP – File Transfer) เป็นต้น

(6) การประชุมทางไกล (Tele Conference) เป็นการประชุมของบุคคลที่อยู่คนละสถานที่และห่างไกลกัน อาจเป็นคนละห้อง คนละตึก คนละจังหวัด คนละประเทศ หรือคนละทวีป โดยอาศัยอุปกรณ์โทรคมนาคมสื่อสารถึงกัน ข่าวสารที่รับส่งถึงได้ทั้งตัวอักษร เสียง และภาพพร้อมๆ กัน โดยทั่วไปการประชุมทางไกลจะแบ่งเป็น 2 ประเภท ได้แก่

- การประชุมทางไกลเฉพาะเสียง (Audio Conference) เป็นการประชุมที่อาศัยระบบโทรศัพท์ หรือวงจรเช่าจากองค์การโทรศัพท์ หรือการสื่อสารแห่งประเทศ เมื่อผู้เข้าประชุมพร้อมจึงเริ่มประชุม โดยผู้เข้าร่วมประชุมทุกคนจะได้ยินเสียงพูดพร้อมๆ กันเสมือนนั่งประชุมอยู่ในที่เดียวกัน และผู้ดำเนินการประชุมเป็นผู้จัดระเบียบการพูด

- การประชุมทางไกลทั้งเสียงและภาพ (Video Conference) เป็นการประชุมที่ใช้สายโทรศัพท์ หรือวงจรพิเศษเป็นสื่อนำภาพ เสียง และข้อมูล ไปยังผู้เข้าร่วมประชุม การใช้บริการสื่อสารรวมระบบดิจิตอล (ISDN – Integrated Service Digital Network) นั้น ช่วยรวมบริการด้านเสียง ภาพ และข้อมูลไว้ในเครือข่ายเดียวกัน โดยใช้เคเบิลใยแก้วนำแสงต่อเข้ากับคู่สายเพียงคู่เดียวก็ทำงานได้ทั้งเสียงและภาพ

2.1.4 การเข้าถึง (Access) ข้อมูล

ก. ความหมายของคำว่า “การเข้าถึง (Access) ข้อมูล”

การเข้าถึง (Access) ข้อมูลเป็นคำที่ไม่ได้มีความหมายเป็นพิเศษสำหรับนักคอมพิวเตอร์โดยทั่วๆไป แต่มีความสำคัญสำหรับการศึกษาถึงการลักลอบเข้าถึงข้อมูลโดยปราศจากอำนาจในทางกฎหมาย ซึ่งถือเป็นการกระทำความผิดทางอาญา

ตามร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... มาตรา 5 ได้กล่าวถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กรณีที่มีการเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหนึ่งเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ

การเข้าถึงตามร่างมาตรา 5 หากเป็นการเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน เป็นความผิดตามร่างมาตรา 7 ในบางกรณีการกระทำความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 7 นี้อาจไม่จำต้องกระทำผิดฐานเข้าถึงระบบคอมพิวเตอร์ตามมาตรา 5 ก่อนก็ได้ เช่น การเอาแผ่นบันทึกข้อมูลของผู้อื่นที่มีการตั้งรหัสผ่านไว้ไปเปิดอ่านในระบบคอมพิวเตอร์ของตนเอง

และถ้าผู้ที่ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ นำมาตรการดังกล่าวไปเปิดเผยโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น เป็นความผิดตามร่างมาตรา 6

เกี่ยวกับความผิดตามร่างมาตรา 5 และมาตรา 7 นี้ มีความเห็นในอีกแง่มุมหนึ่งว่า หากมาตรการป้องกันการเข้าถึงนั้นเป็นมาตรการที่ไม่แน่นหนา ประหนึ่งบ้านที่ใช้กลอนประตูคุณภาพต่ำ การบุกรุกหรือการเข้าถึงกระทำได้ง่ายและอาจไม่ได้เกิดจากความตั้งใจ และเป็นไปได้ที่บุคคลในครอบครัวเดียวกันนั้นเองที่ต้องการใช้เครื่องคอมพิวเตอร์นั้น โดยไม่มีเจตนาร้าย ด้วยเหตุนี้

กฎหมายจึงได้บัญญัติไว้ให้เป็นความผิดอันยอมความได้ และกำหนดโทษไว้ไม่สูงนักและในการประชุมของคณะกรรมการกฤษฎีกา นักวิชาการ-ผู้เชี่ยวชาญทางคอมพิวเตอร์ท่านหนึ่งได้เปรียบเทียบความผิดข้างต้นไว้น่าฟังว่า หากเปรียบระบบคอมพิวเตอร์เป็นบ้านหลังหนึ่ง การเข้าถึงระบบคอมพิวเตอร์อันเป็นความผิดตามร่างมาตรา 5 นั้น ก็เสมือนกับการบุกรุกเข้าไปในบ้านของผู้อื่น การเข้าถึงข้อมูลคอมพิวเตอร์อันเป็นความผิดตามร่างมาตรา 7 ก็เสมือนว่าผู้บุกรุกนั้นนอกจากจะเข้าไปในบ้านหลังนั้นได้แล้ว ยังได้เข้าไปรื้อค้นเอกสารในตู้เก็บเอกสารในนั้นด้วย ส่วนความผิดตามร่างมาตรา ๖ นั้น เสมือนเป็นการนำกุญแจผีที่ไขเข้าไปในบ้านได้ แจกจ่ายให้กับบุคคลอื่นนั่นเอง[9]

กฎหมายของประเทศสหรัฐอเมริกา ได้ให้คำนิยาม คำว่า “การเข้าถึง (Access) ข้อมูล” ไว้ ดังนี้

การเข้าถึง (Access) หมายถึง การเข้าไปสู่ (Approach) สั่ง (Instruct) สื่อสารกับ (Communicate with) ใส่ข้อมูลเข้าไปเก็บไว้ (Store data in) ล้วงข้อมูลมา (Retrieve data from) หรือเอาประโยชน์จาก (Make use of any resources of) เครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์มาใช้

จากคำนิยามดังกล่าวสามารถแยกพิจารณาในส่วนที่สำคัญ ดังนี้

เข้าไปสู่ (Approach) หมายถึง การกระทำที่เป็นการเข้าไปหาสิ่งที่ต้องการ ซึ่งอยู่ภายในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

การสั่ง (Instruct) หมายถึง การกระทำที่เป็นการสั่งให้เครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ทำงานตามที่ต้องการ

การสื่อสาร (Communicate with) หมายถึง การกระทำที่เป็นการติดต่อกับเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ ด้วยวิธีการสื่อสาร เช่น การติดต่อผ่านสายโทรศัพท์ ฯลฯ เพื่อให้ได้ประโยชน์ตามที่ต้องการ

การใส่ข้อมูลเข้าไปเก็บไว้ (Store data in) หมายถึง การกระทำที่เป็นการใส่ข้อมูลเข้าไปเก็บไว้ในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เพื่อประโยชน์ที่จะได้จากการทำงานของเครื่องคอมพิวเตอร์ในภายหลัง

การล้วงข้อมูลมาจาก (Retrieve data from) หมายถึง การกระทำที่เป็นการเอาข้อมูลออกมาจากเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เพื่อประโยชน์ของตน

---

[9] แนวความคิดและหลักการของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ . นายสุนทร เปลี่ยนสี, นิติกร ๕ ฝ่ายกฎหมายกระบวนการยุติธรรมทางอาญา สำนักงานคณะกรรมการกฤษฎีกา

การเอาประโยชน์จาก (Make use of any resources of) หมายถึง การกระทำใดๆ ต่อเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เพื่อประโยชน์ของตน

ดังนั้น การเข้าถึงนี้ อาจเป็นการเข้าถึงโดยผู้กระทำผิดรู้หรือได้รหัสผ่านของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์มาโดยมิชอบ แล้วทำการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น หรืออาจเป็นการเข้าถึงผ่านระบบเครือข่าย ผู้กระทำผิดอาจเป็นผู้มีความรู้ด้านคอมพิวเตอร์ดีพอที่จะเจาะมาตรการป้องกันการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้นได้ สังเกตว่า ร่างกฎหมายฉบับนี้เอาผิดกับผู้ที่พยายามเจาะ (hacking or cracking) เข้าไปในระบบของผู้อื่นเลยทีเดียว ไม่คำนึงว่าเข้าไปโดยประสงค์อย่างไร เพียงแต่เข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงไว้ ก็เป็นความผิดสำเร็จทันที

ข. วิธีการเข้าถึง (Access) ข้อมูล ความเจริญก้าวหน้าด้านเทคโนโลยีในปัจจุบันทำให้ไม่จำเป็นที่จะต้องเข้าไปถึงคอมพิวเตอร์ที่บันทึกข้อมูลหลัก เพียงแต่มีคอมพิวเตอร์ส่วนบุคคล (Personal Computer : PC.) ที่ติดตั้งซอฟต์แวร์ในการติดต่อกับเครือข่ายและโมเด็มที่พ่วงคู่กับสายโทรศัพท์ ที่เรียกว่า “การต่อเชื่อมคอมพิวเตอร์เข้าสู่สายอินเตอร์เน็ต” ก็จะสามารถติดต่อสื่อสารกับคอมพิวเตอร์เครื่องที่ประสงค์จะเข้าถึง และใช้ข้อมูลภายในนั้นได้

ค. มาตรการรักษาความปลอดภัยของข้อมูลในคอมพิวเตอร์ เป้าหมายสำคัญของการรักษาความปลอดภัยที่แท้จริง คือ การปกป้องให้ข้อมูลนั้นเป็นความลับ มีความสมบูรณ์ถูกต้อง และคงอยู่ตลอดเวลาที่เก็บอยู่ในเครื่องคอมพิวเตอร์[10] ระบบการรักษาความปลอดภัยของข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์นั้น โดยทั่วไป อุปกรณ์ต่างๆ ของเครื่องคอมพิวเตอร์จะจำกัดการเข้าถึงโดยผู้ใช้ ซึ่งจะต้องระบุตัวผู้ใช้ (User Identification : User-ID) เอาไว้ โดยใช้รหัสผ่าน (Password) เพื่อใช้เป็นกุญแจในการเข้าสู่ระบบ

2.2 หลักเกณฑ์การคุ้มครองสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล

การให้ความคุ้มครองสิทธิของประชาชนจากการละเมิดสิทธิเสรีภาพของเจ้าพนักงานของรัฐ ไม่ว่าจะเป็นการดำเนินการจับกุม หรือการตรวจค้น ก่อนศตวรรษที่ 18 เป็นเหตุให้เจ้าพนักงานของรัฐมีอำนาจมากในการปฏิบัติหน้าที่โดยไม่มีหลักเกณฑ์ใดมาจำกัดอำนาจของเจ้าพนักงานเหล่านั้นได้ เช่น เจ้าพนักงานของรัฐในประเทศฝรั่งเศสสามารถจับบุคคลไปขังไว้โดยไม่

---

[10] เจนศักดิ์ ตั้งพันธุ์สุริยะ. (2543). **แรกเริ่มเรียนรู้ เรื่องรักษาความปลอดภัยให้ระบบคอมพิวเตอร์.** เรียบเรียงจาก Computer Security for Dummies ของ Peter T. Davis และ Barry D. Lewis. หน้า 27.

แจ้งข้อกล่าวหา และสามารถขังไว้ได้โดยไม่มีกำหนดเวลา[11] ในศตวรรษที่ 8 นักปราชญ์หลายท่าน เช่น มองเตสกิเออ ฯลฯ จึงได้สร้างแนวคิดเกี่ยวกับสิทธิมนุษยชนขึ้น เป็นการนำไปสู่แนวความคิดในการให้ความคุ้มครองสิทธิมนุษยชนมากขึ้นเห็นได้จากการจัดทำเอกสารที่เกี่ยวกับการให้ความคุ้มครองสิทธิของบุคคล เช่น ในประเทศสหรัฐอเมริกามีการจัดทำ The Declaration of Independence[12] และประเทศอังกฤษได้จัดทำ Magna Carta [13]

2.2.1 ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 เดิมการให้ความคุ้มครองสิทธิและเสรีภาพของบุคคลจะเป็นการให้ความคุ้มครองกันภายในรัฐใดรัฐหนึ่งเท่านั้น จนกระทั่งวันที่ 10 ธันวาคม ค.ศ. 1948 องค์การสหประชาชาติได้มีการประชุมและประกาศ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 เป็นการให้ความร่วมมือกันระหว่างประเทศเพื่อให้ความคุ้มครองสิทธิและเสรีภาพของบุคคล และพัฒนาไปในทิศทางเดียว กัน[14]

ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ได้กำหนดหลักเกณฑ์ที่สำคัญเกี่ยวกับการคุ้มครองสิทธิในความเป็นอยู่ทั่วไปของประชาชน ดังนี้ “บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นอยู่ส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือการถูกลบหลู่ในเกียรติยศ และชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับการคุ้มครองจากกฎหมายต่อการแทรกแซงหรือการลบหลู่ดังกล่าวนั้น” จากบทบัญญัติดังกล่าวเป็นการให้ความคุ้มครองความเป็นอยู่ทั่วไปในชีวิตส่วนตัวของบุคคลทั้งที่เป็นการดำเนินชีวิตประจำวัน การติดต่อสื่อสาร เป็นหลัก และยกเว้นในกรณีที่เพื่อประโยชน์สาธารณะ และมีกฎหมายอนุญาตให้ทำได้ แต่ก็ต้องมีการควบคุมมิให้มีการใช้อำนาจที่กระทบกระเทือนต่อสิทธิของประชาชนมากเกินไป สมัชชาสหประชาชาติจึงได้สร้างหลักการควบคุมการใช้อำนาจของรัฐขึ้นมา โดยประกาศใช้ “ประมวลจรรยาบรรณสำหรับเจ้าหน้าที่ผู้มีหน้าที่โดยกฎหมาย” (Code of Conduct for Law Enforcement) ซึ่งข้อที่ 1 บัญญัติให้เจ้าพนักงานผู้มีหน้าที่รักษากฎหมายต้องปฏิบัติตามกฎหมาย โดยมุ่งที่จะให้บริการแก่ประชาชน และคุ้มครองให้ประชาชนปลอดภัยจากการกระทำที่ผิดกฎหมาย และข้อ 2 บัญญัติ ให้เจ้าพนักงานผู้มีหน้าที่รักษา

---

[11] จงรักษ์ จุฑานนท์. (2525). **การคุ้มครองสิทธิของประชาชนต่อการถูกจับและตรวจค้นโดยไม่ชอบธรรม**. หน้า 1.

[12] กุลพล พลวัน. (2538). **พัฒนาการสิทธิมนุษยชน** (พิมพ์ครั้งที่ 3). หน้า 31

[13] กุลพล พลวัน. เล่มเดิม. หน้า 74

[14] กุลพล พลวัน. เล่มเดิม. หน้า 36.

กฎหมาย เมื่อมีการปฏิบัติตามกฎหมายที่เป็นการกระทบกระเทือนถึงสิทธิสิทธิดังกล่าว การกระทำนั้นต้องเคารพ และคุ้มครองศักดิ์ศรีความเป็นมนุษย์ และจะต้องไม่ทำลายล้างหลักสิทธิมนุษยชน[15]

2.2.2 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 นับแต่ประเทศไทยมีการเปลี่ยนแปลงการปกครองจากระบอบสมบูรณาญาสิทธิราชย์ (Absolute Monarchy) มาเป็นระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข (Liberal Democracy with the King as Head of the State) ในปี พ.ศ. 2475 ตั้งแต่นั้นการจัดทำรัฐธรรมนูญแห่งราชอาณาจักรไทยฉบับต่างๆ ก็เหมือนกับรัฐเสรีประชาธิปไตยอื่นๆ คือได้รับแรงบันดาลใจมาจาก "ลัทธิปัจเจกชน" (Individualism)[16] เช่นเดียวกับการจัดทำรัฐธรรมนูญของรัฐเสรีประชาธิปไตย (Liberal and Democratic State) อื่นๆ ซึ่งแนวความคิดของลัทธินี้สอนว่า "มนุษย์ทุกคนเกิดมามีศักดิ์ศรี" นั่นคือ ศักดิ์ศรีความเป็นมนุษย์ (Human Dignity) รัฐธรรมนูญของรัฐเสรีประชาธิปไตยทุกรัฐจึงได้บัญญัติรับรองและให้ความคุ้มครองศักดิ์ศรีความเป็นมนุษย์ของปัจเจกชนไว้อย่างชัดเจนเป็น "สิทธิและเสรีภาพขั้นพื้นฐาน" (Fundamental Rights and Liberties) ซึ่งรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 4 บัญญัติว่า "ศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของบุคคลย่อมได้รับความคุ้มครอง" มาตรา 26 บัญญัติว่า "การใช้อำนาจโดยองค์กรของรัฐทุกองค์กร ต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพตามรัฐธรรมนูญนี้" และมาตรา 27 บัญญัติว่า "สิทธิและเสรีภาพที่รัฐธรรมนูญนี้รับรองไว้โดยชัดแจ้ง โดยปริยาย หรือโดยคำวินิจฉัยของศาลรัฐธรรมนูญ ย่อมได้รับความคุ้มครองและผูกพันรัฐสภา คณะรัฐมนตรี ศาล และองค์กรอื่นของรัฐโดยตรงในการตรากฎหมาย การใช้บังคับกฎหมายและการตีความกฎหมายทั้งปวง" แสดงให้เห็นว่า ไม่ว่าสิทธิหรือเสรีภาพของบุคคลจะต้องอยู่ภายใต้ "ประโยชน์ส่วนรวม" (General Interest) หรือ "ประโยชน์สาธารณะ" (Public Interest) หรือ "ความมั่นคงแห่งชาติ" (National Security)

"สิทธิตามรัฐธรรมนูญ" นั้น ถือว่าเป็น "สิทธิตามกฎหมายมหาชน" (das subjektive oeffentliche Recht) หมายถึงอำนาจตามรัฐธรรมนูญหรือกฎหมายสูงสุดได้บัญญัติให้การรับรองคุ้มครองแก่ปัจเจกบุคคลในอันที่จะกระทำการใด หรือไม่กระทำการใด การให้อำนาจแก่ปัจเจกบุคคลดังกล่าวได้ก่อให้เกิดสิทธิเรียกร้องที่จะไม่ให้บุคคลใดแทรกแซงในสิทธิตามรัฐธรรมนูญของตน โดยเฉพาะอย่างยิ่งเรียกร้องต่อองค์กรของรัฐมิให้แทรกแซงในขอบเขตสิทธิของตน ในบางกรณีการรับรองดังกล่าวได้ก่อให้เกิดสิทธิเรียกร้องให้รัฐดำเนินการอย่างใดอย่างหนึ่ง

---

[15] ศุภฤกษ์ ศุกรเสพย์. (2545). **การค้นในที่รโหฐานของเจ้าพนักงานป้องกันและปราบปรามยาเสพติด**. หน้า 10.

[16] Pierre WIGNY. **Droit constitutionnel : Principle et droit prositif.** Tome premier, Bruxelles, Bruylant, 1952, pp. 257-258.

สิทธิตามรัฐธรรมนูญจึงเป็นความสัมพันธ์ระหว่างปัจเจกบุคคลต่อรัฐ และสิทธิตามรัฐธรรมนูญเป็นสิ่งที่ผูกพันองค์กรผู้ใช้อำนาจรัฐทั้งหลายที่จะต้องให้ความเคารพ ปกป้อง และคุ้มครองสิทธิตามรัฐธรรมนูญดังกล่าว เพื่อให้สิทธิตามรัฐธรรมนูญดังกล่าวมีผลในทางปฏิบัติ[17]

"เสรีภาพตามรัฐธรรมนูญ" หมายถึง อำนาจของบุคคลในอันที่จะกำหนดตนเอง (Self – determination) โดยอำนาจนี้บุคคลย่อมเลือกวิถีชีวิตของตนได้ด้วยตนเองตามใจปรารถนา เสรีภาพจึงเป็นอำนาจที่บุคคลมีอยู่เหนือตนเอง[18]

จะเห็นได้ว่ารัฐธรรมนูญฉบับปัจจุบันมีเจตนารมณ์ที่จะให้ความคุ้มครองสิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์ของประชาชนเป็นสำคัญ ดังจะเห็นได้จากบทบัญญัติในมาตรา 26 บัญญัติว่า "การใช้อำนาจโดยองค์กรของรัฐทุกองค์กร ต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพตามบทบัญญัติแห่งรัฐธรรมนูญนี้"

มาตรา 29 วรรคแรก บัญญัติว่า "การจำกัดสิทธิและเสรีภาพของบุคคลที่รัฐธรรมนูญรับรองไว้จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อการที่รัฐธรรมนูญนี้กำหนดไว้และเท่าที่จำเป็นเท่านั้น และจะกระทบกระเทือนต่อสาระสำคัญแห่งสิทธิและเสรีภาพนั้นมิได้"

และมาตรา 37 วรรคแรก บัญญัติว่า "บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบด้วยกฎหมาย

จากบทบัญญัติดังกล่าวที่กำหนดขึ้นเพื่อปกป้องสิทธิและเสรีภาพของประชาชนมิให้ถูกล่วงละเมิด แม้กฎหมายจะให้การรับรองเสรีภาพอย่างใดอย่างหนึ่งให้แก่บุคคลใดบุคคลหนึ่ง ย่อมมีผลก่อให้เกิดหน้าที่แก่ผู้อื่นด้วยเช่นกัน แต่หน้าที่ที่เกิดขึ้นกับผู้อื่นอันเนื่องมาจากการที่กฎหมายบัญญัติรับรองเสรีภาพให้แก่บุคคลหนึ่งนี้ เป็นแต่เพียงหน้าที่ที่จะต้องเคารพเสรีภาพของผู้ทรงเสรีภาพ และผู้ทรงเสรีภาพเองก็คงมีอำนาจตามกฎหมายแต่เพียงที่จะเรียกร้องให้ผู้อื่นละเว้นจากการรบกวนขัดขวางการใช้เสรีภาพของตนเท่านั้น หาได้มีอำนาจที่จะเรียกร้องให้ผู้อื่นกระทำการอย่างใดอย่างหนึ่งซึ่งมีลักษณะเป็นการส่งเสริมหรือช่วยเหลือการใช้เสรีภาพของตนด้วย

สิทธิและเสรีภาพตามรัฐธรรมนูญนั้นมีผลผูกพันโดยตรงต่ออำนาจนิติบัญญัติ อำนาจบริหารและอำนาจตุลาการ[19] เพราะอำนาจนิติบัญญัติ อำนาจบริหาร และอำนาจตุลาการ ต่างก็เป็น

---

[17] บรรเจิด สิงคะเนติ. (2543). **หลักพื้นฐานของสิทธิเสรีภาพ และศักดิ์ศรีความเป็นมนุษย์ตามรัฐธรรมนูญ พ.ศ. 2540**. หน้า 47.

[18] วรพจน์ วิศรุตพิชญ์. (2543). **สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540**. หน้า 22.

[19] บรรเจิด สิงคะเนติ. เล่มเดิม. หน้า 52.

อำนาจที่มาจากอำนาจอธิปไตย ซึ่งเป็นส่วนหนึ่งที่แสดงออกถึงความเป็นรัฐ นอกจากอาณาเขต และพลเมือง

ปัจจุบันพระราชบัญญัติ การสอบสวนคดีพิเศษ พ.ศ. 2547 มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคลซึ่งมาตรา ๒๙ ประกอบกับมาตรา ๓๑ มาตรา ๓๔ มาตรา ๓๕ มาตรา ๓๖ มาตรา ๓๗ มาตรา ๔๘ มาตรา ๕๘ มาตรา ๒๓๗ และมาตรา ๒๓๘ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย ได้แก่บทบัญญัติต่อไปนี้

มาตรา ๒๔ บัญญัติว่า "เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานสอบสวนคดีพิเศษมีอำนาจดังต่อไปนี้ด้วย

(๑) เข้าไปในเคหสถาน หรือสถานที่ใดๆ เพื่อตรวจค้น เมื่อมีเหตุสงสัยตามสมควรว่ามีบุคคลที่มีเหตุสงสัยว่ากระทำความผิดที่เป็นคดีพิเศษหลบซ่อนอยู่ หรือมีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้ ประกอบกับมีเหตุอันควรเชื่อว่าเนื่องจากการเนิ่นช้ากว่าจะเอาหมายค้นมาได้บุคคลนั้นจะหลบหนีไป หรือทรัพย์สินนั้นจะถูกโยกย้าย ซุกซ่อน ทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิม

(๒) ค้นบุคคล หรือยานพาหนะที่มีเหตุสงสัยตามสมควรว่ามีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้

(๓) มีหนังสือสอบถามหรือเรียกให้สถาบันการเงิน ส่วนราชการ องค์การ หรือหน่วยงานของรัฐ หรือรัฐวิสาหกิจ ส่งเจ้าหน้าที่ที่เกี่ยวข้องมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชีเอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(๔) มีหนังสือสอบถาม หรือเรียกบุคคลใดๆ มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชีเอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(๕) ยึด หรืออายัดทรัพย์สินที่ค้นพบ หรือที่ส่งมาดังกล่าวไว้ใน (๑) (๒) (๓) และ (๔) การใช้อำนาจตามวรรคหนึ่ง ให้พนักงานสอบสวนคดีพิเศษปฏิบัติตามข้อบังคับที่ กคพ. กำหนด เฉพาะการใช้อำนาจตามวรรคหนึ่ง (๑) นอกจากพนักงานสอบสวนคดีพิเศษต้องดำเนินการเกี่ยวกับวิธีการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาแล้ว ให้พนักงานสอบสวนคดีพิเศษแสดงความบริสุทธิ์ก่อนการเข้าค้น รายงานเหตุผลและผลการตรวจค้นเป็นหนังสือต่อผู้บังคับบัญชาเหนือขึ้นไป และบันทึกเหตุสงสัยตามสมควรและเหตุอันควรเชื่อที่ทำให้สามารถเข้าค้นได้เป็นหนังสือให้ไว้แก่ผู้ครอบครองเคหสถานหรือสถานที่ค้น แต่ถ้าไม่มีผู้ครอบครองอยู่ ณ ที่นั้น ให้พนักงาน

สอบสวนคดีพิเศษส่งมอบสำเนาหนังสือนั้นให้แก่ผู้ครอบครองดังกล่าวในทันทีที่กระทำได้ และหากเป็นการเข้าค้นในเวลากลางคืนภายหลังพระอาทิตย์ตก พนักงานสอบสวนคดีพิเศษผู้เป็นหัวหน้าในการเข้าค้นต้องเป็นข้าราชการพลเรือนตำแหน่งตั้งแต่ระดับ ๗ ขึ้นไปด้วย

ให้พนักงานสอบสวนคดีพิเศษผู้เป็นหัวหน้าในการเข้าค้นส่งสำเนาบันทึกเหตุสงสัยตามสมควรและเหตุอันควรเชื่อตามวรรคสาม และสำเนาบันทึกการตรวจค้นและบัญชีทรัพย์ที่ยึดหรืออายัดต่อศาลจังหวัดที่มีอำนาจเหนือท้องที่ที่ทำการค้น หรือศาลอาญาในเขตกรุงเทพมหานครภายในสี่สิบแปดชั่วโมงหลังจากสิ้นสุดการตรวจค้น เพื่อเป็นหลักฐาน

พนักงานสอบสวนคดีพิเศษระดับใดจะมีอำนาจหน้าที่ตามที่ได้กำหนดไว้ตามวรรคหนึ่งทั้งหมดหรือแต่บางส่วน หรือจะต้องได้รับอนุมัติจากบุคคลใดก่อนดำเนินการให้เป็นไปตามที่อธิบดีกำหนดโดยทำเอกสารให้ไว้ประจำตัวพนักงานสอบสวนคดีพิเศษผู้ได้รับอนุมัตินั้นและพนักงานสอบสวนคดีพิเศษผู้นั้นต้องแสดงเอกสารดังกล่าวต่อบุคคลที่เกี่ยวข้องทุกครั้ง

มาตรา 25 ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษพนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

(๑) มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ

(๒) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

(๓) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวันโดยกำหนดเงื่อนไขใดๆ ก็ได้ และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อพนักงานสอบสวนคดีพิเศษได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

บรรดาข้อมูลข่าวสารที่ได้มาตามวรรคหนึ่ง ให้เก็บรักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษซึ่งได้รับอนุญาตตามวรรคหนึ่ง และให้ใช้ประโยชน์ในการสืบสวนหรือใช้เป็นพยานหลักฐานเฉพาะในการดำเนินคดีพิเศษดังกล่าวเท่านั้น ส่วนข้อมูลข่าวสารอื่นให้ทำลายเสียทั้งสิ้น ทั้งนี้ ตามข้อบังคับที่ กคพ. กำหนด

มาตรา 26 ห้ามมิให้บุคคลใดเปิดเผยข้อมูลข่าวสารที่ได้มาเนื่องจากการดำเนินการตามมาตรา 25 เว้นแต่เป็นข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษซึ่งได้รับอนุญาตตามมาตรา 25 และเป็นการปฏิบัติตามอำนาจหน้าที่หรือตามกฎหมายหรือตามคำสั่งศาล

จะเห็นได้ว่าอำนาจที่กฎหมายมอบให้กับพนักงานสอบสวนคดีพิเศษตามบทบัญญัติข้างต้นเป็นการกระทำที่กระทบต่อสิทธิเสรีภาพของประชาชน และจะทำให้เกิดการใช้อำนาจที่ไร้ขอบเขต และประเทศไทยเองก็ยังไม่มีบทบัญญัติของกฎหมายที่ให้การคุ้มครองสิทธิในชีวิตส่วนตัวของบุคคลโดยตรง แต่หากพิจารณาบทกฎหมายที่มีในปัจจุบันแล้วจะพบว่า กฎหมายที่ให้ความคุ้มครองสิทธิส่วนบุคคลมีมากมายพอสมควร ไม่เฉพาะที่ปรากฏอยู่ในประมวลกฎหมายอาญาในความผิดฐานหมิ่นประมาท ความผิดฐานดูหมิ่น ความผิดฐานบุกรุก และความผิดฐานก่อความเดือดร้อนรำคาญเท่านั้น ในประมวลกฎหมายแพ่งและพาณิชย์ ก็มีอยู่ในมาตรา 420 ซึ่งบัญญัติว่า "ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น"

คำว่า "สิทธิอย่างหนึ่งอย่างใด" นี้ก็น่าจะมีความหมายถึง สิทธิในชีวิตส่วนตัวด้วย ซึ่งจะต้องพิจารณากันเป็นกรณีๆ ไป

จะเห็นได้ว่ากฎหมายไทยถือว่าการละเมิดสิทธิในชีวิตส่วนตัวนั้น ถือเป็นความผิดฐานละเมิดตามปกติธรรมดาไม่ได้แยกเป็นพิเศษเหมือนสหรัฐอเมริกา โดยจะต้องพิจารณาถึงเจตนาว่าเป็นการกระทำโดยจงใจหรือประมาทเลินเล่อที่กระทำต่อบุคคลอื่นโดยมิชอบด้วยกฎหมาย แต่การล่วงละเมิดสิทธิในชีวิตส่วนตัวของบุคคลในสหรัฐอเมริกานั้นจะพิจารณาจากผลของการกระทำเป็นสำคัญ และประเทศไทยยังไม่ปรากฏว่ามีคดีเกี่ยวกับการละเมิดสิทธิในชีวิตส่วนตัวขึ้นสู่ศาลดังเช่นที่เกิดขึ้นในประเทศสหรัฐอเมริกา

แม้ว่ารัฐธรรมนูญของประเทศสหรัฐอเมริกาจะไม่มีการกล่าวถึงสิทธิในชีวิตส่วนตัวไว้โดยตรง แต่ศาลสูงของสหรัฐอเมริกาก็ได้วินิจฉัยรับรองว่าสิทธิในชีวิตส่วนตัวเสมือนเป็นสิทธิประการหนึ่งในรัฐธรรมนูญ โดยเฉพาะในคดี Griswold V. Connecticut 381 U.S. 479 (1965) ศาล

สูงสหรัฐได้วินิจฉัยไว้อย่างชัดเจนว่า เจตนารมณ์ของรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 1 เป็นเสมือนศูนย์รวมความรู้ที่ทุกคนไขว่คว้าได้ สิทธิเสรีภาพในการพูด และการพิมพ์โฆษณา ไม่เพียงแต่จะหมายถึงการพูดและการพิมพ์เท่านั้น แต่รวมไปถึงสิทธิในการจำหน่ายจ่ายแจก

ขณะเดียวกันบทบัญญัติรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 3 และ 4 ก็บัญญัติห้ามมิให้บุกรุกเข้าไปในเคหสถานของบุคคลอื่นโดยปราศจากความยินยอม และสิทธิของบุคคลที่จะมีความปลอดภัยในร่างกาย เคหสถาน เอกสาร และทรัพย์สิ่งของจากการตรวจค้น จับกุม ยึดโดยไม่มีเหตุอันสมควร และในบทบัญญัติรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 9 ก็บัญญัติคุ้มครองสิทธิของบุคคลที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองในคดีอาญาและรับรองว่าบรรดาสิทธิต่างๆ ในรัฐธรรมนูญจะตีความให้เป็นการปฏิเสธหรือลิดรอนสิทธิของผู้อื่นไม่ได้

สรุปแล้วบทบัญญัติรัฐธรรมนูญของสหรัฐอเมริกาล้วนแฝงไว้ด้วยสิทธิในชีวิตส่วนบุคคลแทบทั้งสิ้น จึงไม่อาจปฏิเสธได้ว่าสิทธิส่วนบุคคลเป็นสิทธิประการหนึ่ง ซึ่งย่อมได้รับการรับรองโดยกฎหมายโดยชอบ หากผู้ใดละเมิดก็จะมีความผิด โดยยึดถือแนวความคิดคล้ายๆกับการหมิ่นประมาทในตัวของมันเอง (Libel perse)

2.2.3 กฎหมายวิธีพิจารณาความอาญา บทบัญญัติสำคัญของกฎหมายวิธีพิจารณาความอาญาจะอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งเดิมบทบัญญัติที่มีก็เป็นไปเพื่อความสะดวกในการใช้อำนาจของรัฐ การคำนึงถึงสิทธิเสรีภาพส่วนบุคคลมีเพียงส่วนน้อย แต่ได้ให้ความสำคัญมากขึ้นในรัฐธรรมนูญฉบับปัจจุบัน[20]

2.2.3.1 สถานะของผู้ถูกกล่าวหา บทบัญญัติที่ให้ความสำคัญต่อสิทธิเสรีภาพส่วนบุคคลของผู้ถูกกล่าวหา ได้แก่ มาตรา 165 วรรคสาม บัญญัติว่า “ก่อนที่ศาลประทับฟ้องมิให้ถือว่าจำเลยอยู่ในฐานะเช่นนั้น” นั่นคือ ก่อนที่ผู้ที่ถูกผู้เสียหายฟ้องถูกศาลประทับฟ้องยังไม่ถือเป็น “จำเลย” ผู้ถูกกล่าวหาในปัจจุบันจึงไม่ถือเป็นวัตถุแห่งการซักฟอกหรือเป็น “กรรมในคดี” (Prozess-objekt) อีกต่อ แต่เป็น “ประธานในคดี” (Prozess-subjekt) [21] ซึ่งสอดคล้องกับบทบัญญัติในรัฐธรรมนูญมาตรา 241 วรรคหนึ่ง บัญญัติว่า “ในคดีอาญา ผู้ต้องหาหรือจำเลยย่อมมีสิทธิได้รับการสอบสวนหรือการพิจารณาคดีด้วยความเร็ว ต่อเนื่อง และเป็นธรรม”

2.2.3.2 สิทธิของผู้ถูกกล่าวหา สิทธิของผู้ต้องหาที่จะไม่ให้การ เป็นสิทธิของผู้ถูกกล่าวหาในทางอยู่เฉย ซึ่งเป็นสิทธิที่จะตัดสินใจในคดีด้วยตนเอง ในมาตรา 134 บัญญัติว่า “เมื่อผู้ต้องหาเต็มใจให้การอย่างใด ก็ให้จดคำให้การไว้ ถ้าผู้ต้องหาไม่เต็มใจให้การเลยก็ให้บันทึกไว้”

---

[20] คณิต ณ นคร. เล่มเดิม. หน้า 31.

[21] คณิต ณ นคร. เล่มเดิม. หน้า 102.

และในชั้นศาล มาตรา 174 บัญญัติว่า "ถ้าจำเลยไม่ยอมให้การ ก็ให้ศาลจดรายงานไว้และพิจารณาต่อไป" และเพื่อประกันสิทธิในการให้การหรือไม่ให้การของจำเลย มาตรา 135 บัญญัติว่า "ห้ามมิให้พนักงานสอบสวนทำหรือจัดให้ทำการใดๆ ซึ่งเป็นการล่อลวง หรือขู่เข็ญ หรือให้สัญญากับผู้ต้องหาเพื่อจูงใจให้เขาให้การอย่างใดๆ ในเรื่องที่ต้องหานั้น"

การล่อลวง หรือขู่เข็ญ หรือให้สัญญา ซึ่งเป็นการกระทำที่มิชอบด้วยกฎหมายตามที่บัญญัติไว้ในมาตรา 135 นั้น เป็นเพียงการกระทำต้องห้ามที่กฎหมายบัญญัติเป็นตัวอย่างไว้เท่านั้น แต่ความหมายที่บทบัญญัติในมาตรานี้ต้องการแสดงให้ปรากฏก็คือ "การกระทำที่เป็นการละเมิดเสรีภาพในการตัดสินใจของผู้ต้องหา" ทุกสถาน[22]

บทบัญญัติที่ถือว่าขัดแย้งกับบทบัญญัติที่ให้ความคุ้มครองสิทธิของผู้ถูกกล่าวหาในทางอยู่เฉย ได้แก่ มาตรา 132 บัญญัติว่า "เพื่อประโยชน์แห่งการรวบรวมพยานหลักฐาน พนักงานสอบสวนมีอำนาจตรวจค้นผู้ต้องหา จำเลยหรือพิมพ์ลายนิ้วมือ ลายมือหรือลายเท้า" เป็นบทบัญญัติที่แสดงให้เห็นถึงอำนาจของรัฐในการแสวงหาพยานหลักฐานจากผู้ต้องหา หรือจำเลยเพื่อประโยชน์ในการรวบรวมพยานหลักฐาน โดยไม่จำเป็นจะต้องได้รับความยินยอมจากผู้ต้องหาหรือจำเลยดังกล่าว เพียงแต่การตรวจค้นนั้น มาตรา 85 วรรคหนึ่ง บัญญัติว่า "เจ้าพนักงานผู้จับหรือรับตัวผู้ถูกจับไว้ มีอำนาจค้นตัวผู้ต้องหา" และวรรคสอง บัญญัติว่า "การค้นนั้นจักต้องทำโดยสุภาพ ถ้าค้นตัวหญิงต้องให้หญิงอื่นเป็นผู้ค้น" ซึ่งแสดงถึงความเคารพสถานะความเป็นประธานในคดีของผู้ต้องหา

2.2.3.3 สถานะของผู้ต้องหา มาตรา 2 (2) นิยามคำว่า "ผู้ต้องหา" ว่าหมายความถึงบุคคลผู้ถูกหาว่าได้กระทำผิด แต่ยังมิได้ถูกฟ้องต่อศาล จากคำนิยาม บุคคลที่จะมีสถานะเป็นผู้ต้องหาตามกฎหมายจึงต้องเป็นบุคคลที่มีผู้กล่าวหาบุคคลนั้นว่าได้กระทำความผิดอาญาต่อเจ้าพนักงาน หรือเจ้าพนักงานกล่าวหาเอง

ในการกล่าวหาต่อเจ้าพนักงาน มาตรา 2 (7) อาจทำในรูปของคำร้องทุกข์ของผู้เสียหาย หรือตามมาตรา 2 (8) คำกล่าวโทษโดยบุคคลอื่น

2.2.3.4 สถานะของจำเลย มาตรา 2 (3) นิยามคำว่า "จำเลย" ว่าหมายถึงบุคคลซึ่งถูกฟ้องยังศาลแล้วโดยข้อหาว่าได้กระทำความผิด

ดังนั้นจะถือว่าบุคคลซึ่งถูกฟ้องยังศาลแล้วเป็นจำเลยในทันทีที่ยื่นฟ้องจะต้องพิจารณาจากผู้ฟ้องเป็นหลัก หากพนักงานอัยการเป็นผู้ฟ้อง ผู้ถูกฟ้องจะตกเป็นจำเลยทันทีโดยไม่ต้องมีการไต่สวนมูลฟ้องก่อนหรือไม่ แต่ในกรณีที่ผู้เสียหายเป็นผู้ฟ้อง มาตรา 165 วรรคสามตอนท้าย บัญญัติ

---

[22] คณิต ณ นคร. เล่มเดิม. หน้า 105..

ว่า “ก่อนที่ศาลจะประทับฟ้องมิให้ถือว่าจำเลยอยู่ในฐานะเช่นนั้น” ดังนั้นก่อนศาลประทับฟ้องผู้ถูกฟ้องจึงยังไม่ตกเป็นจำเลย

2.2.3.5 การแสวงหาพยานหลักฐาน พยานหลักฐานเป็นเครื่องมือประการหนึ่งในการดำเนินคดีอาญาที่มีความสำคัญมาก ซึ่งในคดีอาญาพยานหลักฐานทุกชนิดรับฟังได้ ดังจะเห็นได้จากมาตรา 226 บัญญัติว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ให้อ้างเป็นพยานหลักฐานได้แต่ต้องเป็นพยานหลักฐานชนิดที่มิได้เกิดจากแรงจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบด้วยประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน”

กระบวนการสำคัญชั้นต้นในการดำเนินคดีอาญา ได้แก่ การสืบสวนและการสอบสวน ซึ่งบทบัญญัติดังกล่าวถือเป็นหลักเบื้องต้นทั่วไปเกี่ยวกับพยานหลักฐานที่แสดงสถานะและความเป็นอิสระในการแสวงหาพยานหลักฐาน แต่สำหรับปัญหาอาชญากรรมที่มีอยู่ในปัจจุบัน เพื่อให้การบังคับใช้กฎหมายป้องกันและปราบปรามอาชญากรรมสำคัญๆ ให้มีประสิทธิภาพมากขึ้นจึงมีการบัญญัติ พระราชบัญญัติ การสอบสวนคดีพิเศษ พ.ศ. 2547 ขึ้น

โดยกฎหมายฉบับนี้ได้กำหนดลักษณะของอาชญากรรมที่เป็นคดีพิเศษแตกต่างไปจากอาชญากรรมธรรมดา เนื่องจากเป็นอาชญากรรมที่มีลักษณะพิเศษ เช่น อาชญากรรมทางเศรษฐกิจหรืออาชญากรรมทางธุรกิจ มีผลกระทบที่รุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของสังคม ประโยชน์ส่วนรวมของประชาชน หรือความมั่นคงของประเทศความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของประเทศ หรือคดีอาญาที่มีผู้มีอิทธิพลเป็นผู้ร่วมกระทำความผิด รวมทั้งอาชญากรรมที่เป็นองค์กรอาชญากรรม และอาชญากรรมข้ามชาติด้วย เป็นอาชญากรรมที่ให้ผลตอบแทนแก่ผู้ประกอบอาชญากรรมเป็นอย่างมาก ทั้งนี้ วิธีการและลักษณะการกระทำความผิดมีความซับซ้อนเป็นการยากที่เจ้าหน้าที่ของรัฐบาลจะเข้าถึงผู้เป็นตัวการที่อยู่เบื้องหลัง เพื่อนำมาดำเนินคดีและลงโทษตามกฎหมายได้ เนื่องจากขาดความรู้ความเชี่ยวชาญและเทคนิคเฉพาะด้านในการสืบสวนสอบสวนเพื่อรวบรวมพยานหลักฐานสำหรับการดำเนินคดี

ดังนั้นจึงมีการกำหนดมาตรการและวิธีการต่างๆ ที่เพิ่มประสิทธิภาพในการปฏิบัติหน้าที่ของพนักงานสอบสวนคดีพิเศษ เช่น การกำหนดให้มีคุณสมบัติเบื้องต้นและคุณสมบัติพิเศษ การผ่านการอบรมตามหลักสูตรที่กำหนด และการผ่านการประเมินความรู้ความสามารถ เป็นต้น นอกจากการเพิ่มประสิทธิภาพให้กับเจ้าหน้าที่สืบสวนสอบสวนโดยเฉพาะแล้ว กฎหมายยังให้อำนาจลักษณะพิเศษไว้ด้วย เพื่อแก้ไขปัญหาความบกพร่องของกระบวนการยุติธรรมให้มีประสิทธิภาพมากขึ้น เนื่องจากระบบการสอบสวนในปัจจุบันยังไม่สามารถแก้ไขปัญหาความบกพร่องของพยานหลักฐานในคดีบางประเภทได้ รวมทั้งระบบการสอบสวนที่มีอยู่แต่เดิม จะเห็น

ได้จากอาชญากรรมที่มีความเชี่ยวชาญในการใช้เทคโนโลยีระดับสูงในการประกอบอาชญากรรม ในขณะเดียวกันก็ใช้ความรู้ความเชี่ยวชาญในการปกปิดซ่อนเร้นทำลายพยานหลักฐาน

เพื่อการแสวงหาพยานหลักฐาน และนำตัวผู้กระทำความผิดมาลงโทษให้ได้ โดยอำนาจหน้าที่หลักของพนักงานสอบสวน ตามมาตรา 2 (6) นิยามว่า "พนักงานสอบสวน หมายความถึงเจ้าพนักงานซึ่งกฎหมายให้อำนาจและหน้าที่ทำการสอบสวน" และมาตรา 121 วรรคหนึ่ง บัญญัติว่า "พนักงานสอบสวนมีอำนาจสอบสวนคดีอาญาทั้งปวง" ซึ่งเป็นบทบัญญัติถึงอำนาจในการสอบสวนของพนักงานสอบสวน

การสอบสวนโดยทั่วไปจะเริ่มเมื่อรู้เรื่องความสงสัยว่ามีการกระทำความผิดอาญาเกิดขึ้น แต่การรู้นั้นสามารถรู้ได้ 2 ทาง ได้แก่ เมื่อมีการร้องทุกข์หรือการกล่าวโทษ และรู้เองซึ่งพิจารณาจากฐานความผิดอาญาประกอบ นั่นคือหากเป็นการกระทำความผิดที่เกี่ยวข้องกับประโยชน์ได้เสียของประชาชนส่วนรวม พนักงานสอบสวนก็ต้องทำการสอบสวนโดยไม่ชักช้า

โดยหลักจุดประสงค์ในการรวบรวมพยานหลักฐานก็เพื่อความน่าเชื่อถือของพยานหลักฐานเหล่านั้น แต่ปัญหาในทางปฏิบัติหรือปัญหาทางเทคนิคของคดีพิเศษคือปัญหาในการแสวงหาพยานหลักฐาน ซึ่งไม่มีประจักษ์พยานเพราะผู้กระทำความผิดจะไม่มีส่วนเกี่ยวข้องกับพยานหลักฐานโดยตรง หรือสามารถทำลายพยานหลักฐานได้โดยง่าย ดังนั้นพนักงานสอบสวนจึงต้องมีความรู้ความเชี่ยวชาญสำหรับวิธีและมาตรการพิเศษที่จะใช้ในการแสวงหาพยานหลักฐานเพื่อนำมาดำเนินคดีกับผู้กระทำความผิดให้ได้

สำหรับ พระราชบัญญัติ การสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 21 (1) บัญญัติว่า

"(๑) คดีความผิดทางอาญาตามกฎหมายที่กำหนดไว้ในบัญชีท้ายพระราชบัญญัตินี้ และที่กำหนดในกฎกระทรวงโดยการเสนอแนะของ กคพ. โดยคดีความผิดทางอาญาตามกฎหมายดังกล่าว จะต้องมีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้

(ก) คดีความผิดทางอาญาที่มีความซับซ้อน จำเป็นต้องใช้วิธีการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเป็นพิเศษ

(ข) คดีความผิดทางอาญาที่มีหรืออาจมีผลกระทบอย่างรุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน ความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของประเทศ

(ค) คดีความผิดทางอาญาที่มีลักษณะเป็นการกระทำความผิดข้ามชาติที่สำคัญ หรือเป็นการกระทำขององค์กรอาชญากรรม หรือ

(ง) คดีความผิดทางอาญาที่มีผู้ทรงอิทธิพลที่สำคัญเป็นตัวการ ผู้ใช้หรือผู้สนับสนุน

ทั้งนี้ ตามรายละเอียดของลักษณะของการกระทำความผิดที่ กคพ. กำหนด

DPU

(๒) คดีความผิดทางอาญาอื่นนอกจาก (๑) ตามที่ กคพ. มีมติด้วยคะแนนเสียงไม่น้อยกว่าสองในสามของกรรมการทั้งหมดเท่าที่มีอยู่

ในคดีที่มีการกระทำอันเป็นกรรมเดียวผิดต่อกฎหมายหลายบท และบทใดบทหนึ่งจะต้องดำเนินการโดยพนักงานสอบสวนคดีพิเศษตามพระราชบัญญัตินี้ หรือคดีที่มีการกระทำความผิดหลายเรื่องต่อเนื่องหรือเกี่ยวพันกัน และความผิดเรื่องใดเรื่องหนึ่งจะต้องดำเนินการโดยพนักงานสอบสวนคดีพิเศษตามพระราชบัญญัตินี้ ให้พนักงานสอบสวนคดีพิเศษมีอำนาจสืบสวนสอบสวนสำหรับความผิดบทอื่นหรือเรื่องอื่นด้วย และให้ถือว่าคดีดังกล่าวเป็นคดีพิเศษ

บรรดาคดีใดที่ได้ทำการสอบสวนเสร็จแล้วโดยพนักงานสอบสวนคดีพิเศษ ให้ถือว่าการสอบสวนนั้นเป็นการสอบสวนในคดีพิเศษตามพระราชบัญญัตินี้แล้ว...”

ดังนั้นคดีพิเศษที่เจ้าพนักงานสอบสวนคดีพิเศษจะทำการสอบสวนได้จะต้องมีลักษณะตามที่กฎหมายบัญญัติเอาไว้ข้างต้น

โดยลักษณะพิเศษของคดีพิเศษทำให้การรวบรวมพยานหลักฐานเป็นไปอย่างยากลำบาก ทำให้การสอบสวนขาดประสิทธิภาพ พยานหลักฐานขาดความน่าเชื่อถือ ตามปกติกฎหมายจึงกำหนดให้พนักงานสอบสวนคดีพิเศษมีอำนาจพิเศษในการแสวงหาพยานหลักฐานดังกล่าวโดยการขออนุญาตต่อศาล เช่นการดักฟังวิทยุหรือโทรศัพท์ การเข้าสู่ข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์

เมื่อกฎหมายให้สิทธิแก่บุคคลหนึ่งก็ย่อมก่อให้เกิดหน้าที่แก่บุคคลอื่นในอันที่จะไม่ก้าวล่วงต่อสิทธิส่วนบุคคลนี้ และหากมีการก้าวล่วงต่อสิทธิส่วนบุคคล เจ้าของสิทธิชอบที่จะได้รับการแก้ไขเยียวยา คือ การเรียกร้องให้ชดใช้ค่าเสียหายหรือกระทำการใดๆ เพื่อทดแทนความเสียหายหรือกำหนดโทษทางอาญาแก่ผู้ที่กระทำความผิดตามบทบัญญัติของกฎหมาย

การที่เจ้าหน้าที่ของรัฐผู้มีอำนาจมีหน้าที่ในการแสวงหา สืบสวน และสอบสวนเพื่อนำตัวผู้ที่กระทำความผิดมาลงโทษ ดังนั้นการปฏิบัติหน้าที่ของเจ้าหน้าที่อาจจะเข้าไปก้าวล่วงในสิทธิส่วนบุคคลของแต่ละคนได้โดยง่าย ดังนั้น การศึกษาในส่วนที่เกี่ยวกับสิทธิส่วนบุคคลจึงเป็นเรื่องที่ไม่อาจมองข้ามไปได้ เพราะเจ้าหน้าที่ของรัฐก็ไม่ใช่บุคคลที่ได้รับการยกเว้นใดๆ จากความรับผิดในการก้าวล่วงต่อสิทธิส่วนบุคคลของผู้อื่น แม้กฎหมายจะให้อำนาจเจ้าหน้าที่ของรัฐในการใช้ดุลพินิจเพื่อเป็นมาตรการเสริมที่จะช่วยในการบังคับใช้กฎหมายให้มีประสิทธิภาพมากยิ่งขึ้น แต่การใช้ดุลพินิจของเจ้าหน้าที่ของรัฐก็เป็นอันตรายต่อสิทธิส่วนบุคคลเช่นกัน การใช้ดุลพินิจของเจ้าหน้าที่ของรัฐจึงต้องอยู่ภายใต้กฎหมาย โดยเฉพาะในเรื่องที่เกี่ยวกับชีวิตส่วนตัวของบุคคลเจ้าหน้าที่ของรัฐอาจมีความผิดฐานละเมิด ดังนั้นเจ้าหน้าที่ของรัฐจึงต้องปฏิบัติหน้าที่ด้วยความระมัดระวังมิให้ผู้อื่นได้รับความเดือดร้อนจากการละเมิดสิทธิส่วนบุคคล

กฎหมายว่าด้วยสิทธิในชีวิตส่วนตัว (Law of Privacy) ของต่างประเทศได้บัญญัติถึงการกระทำบางอย่างซึ่งถึงแม้ว่าจะไม่เป็นถึงกับเป็นการโฆษณาหมิ่นประมาท หรือทำให้บุคคลอื่นเสื่อมเสียเกียรติยศ ชื่อเสียงโดยตรง แต่ก็อาจมีลักษณะที่เป็นการล่วงละเมิดต่อสิทธิเสรีภาพในความเป็นอยู่ส่วนตัวของบุคคลอย่างเห็นได้ชัด เช่น คอยติดตามบุคคลอื่นตลอดเวลาจนก่อให้เกิดความรำคาญ หรือการเข้าตรวจสอบข้อมูลส่วนบุคคลที่บันทึกไว้ในเครื่องคอมพิวเตอร์ ซึ่งเป็นการกระทำความผิดฐานละเมิดตามหลักกฎหมายแพ่งก็ไม่ชัดเจน เพราะผู้กระทำหาได้ทำให้เกิดความเสียหายแก่ร่างกาย เกียรติยศ ชื่อเสียงของบุคคลนั้นโดยมิชอบด้วยกฎหมายไม่ แต่การกระทำดังกล่าวเป็นที่แน่นอนว่าย่อมทำให้บุคลนั้นต้องสูญเสียความเป็นอิสระส่วนตัวไป เพราะการถูกสอดแทรกหรือเกี่ยวข้องจากการกระทำของเจ้าหน้าที่ของรัฐ ซึ่งย่อมต้องขัดกับความต้องการส่วนบุคคลแน่นอน

การพิจารณาเรื่องสิทธิส่วนบุคคลในเบื้องต้น ผู้พิจารณาจะต้องคำนึงถึงอยู่เสมอว่ากฎหมายว่าด้วยสิทธิในชีวิตส่วนตัวไม่มีรูปแบบมาตรฐาน (Uniform) เช่นเดียวกับกฎหมายลักษณะอื่นๆ เพราะลักษณะที่จะถือเป็นการละเมิดสิทธิส่วนบุคคลมีความเห็นหลากหลายแตกต่างกันไปตามสภาพเศรษฐกิจ สังคม และวัฒนธรรมของแต่ละประเทศ เพราะการละเมิดสิทธิส่วนบุคคลเป็นเรื่องเกี่ยวกับความรู้สึกของแต่ละคนอันมีลักษณะทำให้เกิดความเสียหายต่อความเป็นส่วนตัวของเขา ขณะเดียวกันก็ต้องระลึกอยู่เสมอว่าคำพิพากษาหรือกฎหมายที่เกี่ยวกับสิทธิส่วนบุคคลที่มีนั้นเป็นสิ่งที่แสดงออกถึงความพยายามที่จะจุดดุลยภาพระหว่างผลประโยชน์สาธารณะกับสิทธิส่วนบุคคลให้เกิดความพอดี

สิทธิส่วนบุคคล (Right of Privacy) ในความหมายที่แคบที่สุดอาจกล่าวได้ว่า หมายถึงสิทธิที่จะอยู่โดยลำพังปราศจากการรบกวน (The right to be let alone) และเป็นสิทธิที่ได้รับการกล่าวถึงมากที่สุดในช่วงปี ค.ศ. 1980 เพราะเป็นช่วงเวลาที่ประเทศสหรัฐอเมริกาได้รับการขนานนามว่าเป็นสังคมแห่งข่าวสาร กล่าวคือ อิสระของข่าวสารที่ประชาชนหรือสื่อมวลชนจะสามารถเข้าล่วงรู้และนำออกเผยแพร่สู่สาธารณชนได้รับการยอมรับเป็นอย่างมาก ขณะเดียวกันก็เป็นเรื่องยากที่จะเก็บข้อมูลข่าวสารของแต่ละคนไว้โดยปราศจากการแทรกแซงจากเจ้าหน้าที่ของรัฐ หรือเอกชนที่ต่างมุ่งแสวงหาผลประโยชน์ในเชิงธุรกิจของตนเป็นสำคัญ[23]

แต่เนื่องจากลักษณะของการสอบสวนคดีพิเศษต่างๆ จำเป็นที่จะต้องมีระบบการตรวจสอบการใช้อำนาจหน้าที่ของเจ้าพนักงานสอบสวนคดีพิเศษและเจ้าหน้าที่ที่เกี่ยวข้อง รวมทั้งมีการประเมินผลการปฏิบัติหน้าที่เป็นระยะๆ นอกเหนือจากการมีระบบคัดสรรบุคลากรที่เข้มงวด

---

[23] Haroldd L. Nelson & Dwight L. Teeter. (1986). **Law of Mass Communication : Freedom and Control of Print and Broadcast Media** (Fifth Edition). p. 200.

และโปร่งใส เพื่อให้งานสอบสวนคดีพิเศษมีประสิทธิภาพและเป็นอีกส่วนหนึ่งของกระบวนการยุติธรรมในปัจจุบัน

2.3 การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในคดีอาญา

2.3.1 การค้นหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ การค้นเป็นมาตรการบังคับ (Zwangsmassnahme หรือ compulsory measures) ซึ่งเป็นเครื่องมือในการดำเนินคดีอาญาที่สำคัญและจำเป็นต้องมี หากขาดไปการดำเนินคดีอาญาก็ย่อมไม่อาจกระทำได้[24] โดยกำหนดให้เจ้าพนักงานของรัฐ 2 ประเภท เป็นผู้ดำเนินการค้น ได้แก่ พนักงานฝ่ายปกครอง และเจ้าพนักงานตำรวจหรือพนักงานสอบสวน ประชาชนทั่วไปไม่สามารถทำการค้นได้ไม่ว่าจะเป็นกรณีใดก็ตาม[25] และมีเหตุในการออกหมายค้นได้ตามมาตรา 69 (1) – (5)

การค้นจึงเป็นการดำเนินการของเจ้าพนักงานของรัฐที่กฎหมายอนุญาตให้เข้าไปแสวงหาพยานหลักฐานได้ตามสถานที่ต่างๆ หรือจากตัวบุคคลก็ย่อมกระทำได้ เมื่อการค้นเป็นการแสวงหาพยานหลักฐานจากสถานที่ต่างๆ หรือจากตัวบุคคล การค้นของเจ้าพนักงานย่อมเป็นการกระทำที่กระทบกระเทือนต่อสิทธิส่วนบุคคล[26] เสรีภาพในเคหสถาน[27] และสิทธิเสรีภาพในชีวิตและ ร่างกาย[28] และในกรณีที่พยานหลักฐานที่เจ้าพนักงานของรัฐแสวงหามิใช่พยานวัตถุ พยานเอกสาร หรือพยานบุคคล เช่น ข้อมูลอิเล็กทรอนิกส์ ซึ่งกฎหมายไทยมิได้มีการจัดเอาไว้ว่าเป็นพยานหลักฐานประเภทใด และยังมีข้อโต้แย้งกันอยู่ว่าจะเป็นพยานเอกสารหรือพยานวัตถุ

แต่เมื่อพิจารณาจากการแสวงหาพยานหลักฐานดังกล่าวแล้ว อาจทำได้ 2 วิธีได้แก่

(1) เป็นข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ส่วนบุคคลของบุคคลใดบุคคลหนึ่ง ไม่ว่าจะอยู่ที่ใดที่พนักงานของรัฐไม่สามารถใช้เครื่องมือใดๆ เชื่อมเข้าไปในเครื่องคอมพิวเตอร์เพื่อเรียกดูข้อมูลที่ถูกจัดเก็บไว้ในฮาร์ดดิสได้ นอกจากเข้าไปค้นในที่ที่เครื่องคอมพิวเตอร์นั้นอยู่ ซึ่งก็เป็นการบุกรุกเข้าไปในเคหสถานของผู้เป็นเจ้าของ จึงจะได้ข้อมูลที่เป็นพยานหลักฐานมา และ

(2) เป็นการจัดเก็บข้อมูลในรูปของเครือข่าย เช่นเครือข่ายในระบบ LAN (Local Area Network) เป็นระบบเครือข่ายท้องถิ่นภายในอาคารเดียวกัน หรือ ระบบ WAN (Wide Area Network) เป็นระบบเครือข่ายระยะไกลจำกัดเฉพาะกลุ่ม เช่นระบบธนาคาร ใช้เฉพาะกลุ่มธนาคาร

---

[24] คณิต ณ นคร. เล่มเดิม. หน้า 190.

[25] คนึง ฤาไชย. (2540). **กฎหมายวิธีพิจารณาความอาญา เล่ม 1** (พิมพ์ครั้งที่ 6). หน้า 252.

[26] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 34

[27] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 35

[28] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 31

และรวมถึงระบบอินเตอร์เน็ต ซึ่งเจ้าพนักงานของรัฐไม่จำต้องเข้าไปในที่รโหฐานเพื่อค้นหาพยานหลักฐาน แต่อาจใช้เครื่องมือหรือเครื่องคอมพิวเตอร์อีกเครื่องเชื่อมไปที่แม่ข่าย หรือเซิร์ฟเวอร์ (Server) เพื่อเรียกข้อมูลมาตรวจดูก็ได้

2.3.1.1 การค้นพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์ที่อยู่ในที่รโหฐาน ตามคำนิยามของคำว่า "รโหฐาน" ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 2 (13) หมายถึงสถานที่ใดๆ ซึ่งประชาชนไม่มีความชอบธรรมที่จะเข้าไปได้ หรือเป็น "ที่ส่วนตัว" (Private Place) ที่แสดงถึงเจตนาหวงกันของเจ้าของหรือผู้ครอบครอง[29] การคุ้มครองเสรีภาพในเคหสถานของบุคคลตามรัฐธรรมนูญ มาตรา 35 การที่เจ้าพนักงานของรัฐเข้าไปค้นหาข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งอยู่ในที่รโหฐานได้จะต้องเป็นกรณีที่มีกฎหมายบัญญัติไว้ และจะต้องมีหมายค้น ดังที่บัญญัติไว้ตามรัฐธรรมนูญ มาตรา 238[30] ซึ่งจะต้องมีเหตุในการออกหมายค้นตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 69 เว้นแต่เป็นกรณีที่กฎหมายบัญญัติให้มีการค้นได้โดยไม่ต้องมีหมายตามมาตรา 92[31] หากเจ้าพนักงานของรัฐทำการตรวจค้นโดยไม่มีหมาย และไม่เข้ากรณียกเว้น การค้นดังกล่าวก็เป็นการค้นที่มิชอบ เป็นเหตุให้ศาลไม่สามารถรับฟังเป็นพยานหลักฐานได้

ดังนั้นการเข้าตรวจค้นที่รโหฐานเพื่อค้นหาในเครื่องคอมพิวเตอร์ส่วนบุคคล หรือเครื่องคอมพิวเตอร์ที่เชื่อมโยงเครือข่ายในเคหสถานเดียวกันของผู้ต้องสงสัยซึ่งเป็น "สิ่งของที่ใช้ในการกระทำความผิด" เพื่อค้นหาข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นพยานหลักฐานแสดงการกระทำความผิดของผู้ต้องสงสัย เจ้าพนักงานของรัฐจำเป็นจะต้องมีหมายค้นจากศาล ในการรวบรวมพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132[32]

หากพิจารณาจากลักษณะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งสามารถทำลายแก้ไขได้ง่ายโดยใช้เวลาเพียงสั้นๆ แต่การออกหมายค้นจากศาลต้องใช้เวลาพอสมควร หากผู้ต้องสงสัยทราบว่าจะถูกค้น ก็สามารถทำลายหรือแก้ไขได้โดยง่าย ถึงแม้มีความจำเป็นเร่งด่วน จะถือเป็นเข้าเหตุยกเว้นตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92 และใช้อำนาจตามมาตรา 92 วรรคสอง ซึ่งไม่น่าจะยกเป็นเหตุยกเว้นได้ เพราะโดยหลักการค้นจะต้องมีหมาย สำหรับ

---

[29] คณิต ณ นคร. เล่มเดิม. หน้า 220.

[30] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 238

[31] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92

[32] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132

การค้นตามมาตรา 92 เป็นการค้นในกรณีพิเศษ จึงต้องมีกฎหมายบัญญัติเอาไว้อย่างชัดแจ้ง ประกอบกับคำวินิจฉัยของคณะกรรมการกฤษฎีกาที่ นร. 0601/618[33] ให้ความเห็นว่า

บทบัญญัติมาตรา 92 วรรคสอง แห่งประมวลกฎหมายวิธีพิจารณาความอาญาในส่วนที่บัญญัติให้พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ค้นด้วยตนเองโดยไม่ต้องมีหมายค้น ในกรณีที่อาจออกหมายค้นได้ ขัดต่อมาตรา 238 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยเป็นอันใช้บังคับมิได้...

ดังนั้น การค้นข้อมูลอิเล็กทรอนิกส์ในกฎหมายไทยปัจจุบันจึงต้องมีหมายค้น เจ้าพนักงานของรัฐจึงจะทำการค้นได้ หากเป็นการค้นโดยไม่มีหมาย ก็ถือว่าพยานหลักฐานที่ได้เป็นพยานหลักฐานที่ได้มาโดยมิชอบ ศาลไม่สามารถนำมาใช้ประกอบการพิจารณาได้

2.3.1.2 การค้นพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์โดยการเชื่อมเข้าระบบ กรณีที่เจ้าพนักงานของรัฐเข้าค้นข้อมูลอิเล็กทรอนิกส์ได้โดยไม่ต้องเข้าไปในที่รโหฐาน แต่ใช้เครื่องคอมพิวเตอร์เชื่อมจากภายนอก ไม่ว่าจะเป็นระบบ LAN, WAN หรือ อินเตอร์เน็ต ลักษณะไม่เป็นการบุกรุกตามประมวลกฎหมายอาญา เพราะไม่ได้เข้าไปยังเคหสถานของผู้อื่น แต่เป็นการละเมิดสิทธิส่วนบุคคลตามรัฐธรรมนูญ มาตรา 34 โดยถือว่าเป็นการค้นเช่นกัน การใช้อำนาจของเจ้าพนักงานของรัฐ ย่อมจะต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของประชาชนตามดังที่บัญญัติไว้ในรัฐธรรมนูญมาตรา 26

ดังนั้น การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN, WAN หรือ อินเตอร์เน็ต แม้ในกฎหมายไทยปัจจุบันยังไม่มีกฎหมายบัญญัติไว้โดยเฉพาะ แต่เมื่อพิจารณาถึงสิ่งที่กฎหมายประสงค์จะให้ความคุ้มครอง นั่นคือสิทธิส่วนบุคคล การค้นจึงต้องมีหมายค้นเช่นเดียวกับการค้นโดยทั่วไป หากเป็นการค้นโดยไม่มีหมาย ก็ถือว่าพยานหลักฐานที่ได้เป็นพยานหลักฐานที่ได้มาโดยมิชอบเช่นกัน และศาลก็ไม่สามารถนำมาใช้ประกอบการพิจารณาได้

2.3.2 การยึดและเก็บรักษาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานที่ไม่มีรูปร่าง ซึ่งจะทำการยึดอย่างเช่นพยานหลักฐานทั่วไป ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 101[34] ไม่ได้ โดยลักษณะของข้อมูลอิเล็กทรอนิกส์ การยึดสามารถกระทำได้โดยการยึดเครื่องคอมพิวเตอร์หรือเครื่องอิเล็กทรอนิกส์ที่มีข้อมูลนั้น หรือการนำฮาร์ดดิสก์ที่มีข้อมูลนั้นเสนอต่อศาล

---

[33] คำวินิจฉัยของคณะกรรมการกฤษฎีกา ตามหนังสือ สำนักงานคณะกรรมการกฤษฎีกาที่ นร. 0601/618 (2542). **วารสารอัยการนิเทศ**, 61, 1. หน้า .183-194.

[34] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 101

กรณีที่เป็นข้อมูลอิเล็กทรอนิกส์ในระบบเครือข่ายอินเตอร์เน็ต ซึ่งต้องมีการเจาะเข้าไปใน E-mail ที่มีข้อมูลส่วนตัว การจะยึดข้อมูลส่วนบุคคลดังกล่าว เจ้าพนักงานของรัฐไม่สามารถทำได้ เพราะเป็นการละเมิดสิทธิส่วนบุคคล สามารถทำได้เพียงการยึดข้อมูลที่มีการเผยแพร่ต่อสาธารณชนเพื่อนำเสนอต่อศาลเท่านั้น

ในการตรวจสอบพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ว่าเกี่ยวข้องกับการกระทำความผิดหรือไม่นั้น ลำพังเจ้าพนักงานของรัฐเองอาจไม่สามารถทำได้ ทำให้ได้ข้อมูลไม่ครบถ้วน จึงจำเป็นต้องมีผู้เชี่ยวชาญ เช่น โปรแกรมเมอร์ที่เป็นผู้เชี่ยวชาญพิเศษโดยเฉพาะเป็นผู้ช่วยเหลือเจ้าพนักงานของรัฐในการปฏิบัติหน้าที่ โดยจะทำหน้าที่เข้าสู่ข้อมูล ตรวจสอบ เก็บข้อมูลหรือพยานหลักฐานให้ครบถ้วน ตลอดจนเก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นให้อยู่ในสภาพที่สามารถใช้ประโยชน์ได้ เพราะวัสดุที่ใช้ในการเก็บรักษาข้อมูล เช่นฮาร์ดดิสก์ เป็นวัสดุที่อาจถูกทำลายได้โดยสภาพแวดล้อมทางธรรมชาติ เช่น ความชื้น ความเย็นจัด ร้อนจัด หรือสนามแม่เหล็ก ทั้งจะต้องทำหน้าที่ยืนยันต่อศาลว่าข้อมูลอิเล็กทรอนิกส์ที่นำเสนอต่อศาลเป็นข้อมูลที่ได้ทำการยึดมา ลักษณะจึงเหมือนกับเป็นพยานผู้เชี่ยวชาญ ผู้ที่จะทำหน้าที่ตรวจสอบพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์อย่างเป็นกลาง และทำหน้าที่เก็บรักษา แต่ขณะนี้ยังไม่มีผู้ที่จะทำหน้าที่ดังกล่าวได้ เพราะไม่มีกฎหมายกำหนดให้มี จึงยังเป็นหน้าที่ของเจ้าพนักงานของรัฐโดยทั่วๆไป ซึ่งไม่ใช่ผู้ที่มีความรู้ความสามารถโดยเฉพาะ

โดยสรุปการตรวจค้น และการยึดข้อมูลอิเล็กทรอนิกส์ เพื่อนำมาเป็นพยานหลักฐานในอาชญากรรมคอมพิวเตอร์นั้น ไม่อาจกระทำได้หากไม่มีหมายค้น บางกรณีก็ไม่สามารถทำได้อย่างทันท่วงที เป็นปัญหาในเรื่องของอำนาจของเจ้าพนักงานของรัฐที่ยังไม่มีกฎหมายให้อำนาจเอาไว้โดยเฉพาะ ตลอดจนการตรวจสอบและการเก็บรักษา ก็ยังต้องใช้วิธีการตามที่บัญญัติเอาไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาเท่านั้น ซึ่งไม่เพียงพอแล้วกับสังคมในปัจจุบัน

บทที่ 3
การเข้าถึงข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในกฎหมายต่างประเทศ

ในบทที่แล้วได้กล่าวถึงความหมาย ลักษณะ และสภาพปัญหาของการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมทางคอมพิวเตอร์รูปแบบต่างๆดังที่ได้กล่าวมาแล้ว ซึ่งปัญหาอาชญากรรมคอมพิวเตอร์นี้ก็มิใช่ว่าจะเกิดแต่เฉพาะในประเทศไทยเท่านั้น แต่ยังส่งผลกระทบต่อกฎหมายอาญาของประเทศอื่นๆ ด้วย ดังนั้นในบทนี้จะกล่าวถึงแนวความคิดในการบัญญัติกฎหมายเพื่อรักษาความปลอดภัยของข้อมูล สภาพปัญหาเกี่ยวกับการปราบปรามอาชญากรรมคอมพิวเตอร์ และมาตรการทางกฎหมายและปัญหาเกี่ยวกับการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์ของประเทศต่างๆ ได้แก่ ประเทศสหรัฐอเมริกา อังกฤษ และญี่ปุ่น โดยการศึกษาถึงแนวความคิด เหตุผล ขั้นตอน วิธีการ และระยะเวลาในการค้น และการรับฟังเป็นพยานหลักฐานในศาลของประเทศต่างๆ เพื่อเป็นแนวทางในการแก้ปัญหาที่เกิดขึ้นในกฎหมายไทยต่อไป

3.1 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาเป็นประเทศหนึ่งที่มีความเจริญก้าวหน้าทางเทคโนโลยีในหลายๆด้าน และมีกฎหมายที่จะใช้ดำเนินคดีกับอาชญากรรมคอมพิวเตอร์มากกว่า 40 ฉบับ เช่น National Stolen Property Act , Copyright Act ฯลฯ จึงต้องพิจารณาว่ากฎหมายที่มีอยู่ทั้ง 40 ฉบับนั้น สามารถนำมาใช้บังคับและครอบคลุมความผิดอาญาเกี่ยวกับคอมพิวเตอร์ได้มากน้อยเพียงใด สำหรับความผิดเกี่ยวกับคอมพิวเตอร์สหรัฐเองก็มีการบัญญัติกฎหมายตั้งแต่ปี ค.ศ. 1984 คือ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA) ซึ่งแบ่งความผิดเกี่ยวกับคอมพิวเตอร์เป็น 3 ลักษณะ ได้แก่

ก. Subsection 1030 (a) (1) ความผิดที่ก่อความเสียหายแก่ความมั่นคงของรัฐโดยตรง

ข. Subsection 1030 (a) (2) ความผิดที่ก่อให้เกิดความเสียหายต่อระบบความเชื่อถือส่วนบุคคลที่มีในสถาบันการเงิน หรือหน่วยงานที่ทำหน้าที่ดูแลประวัติ และผู้บริโภค

ค. Su bsection 1030 (a) (3) ความผิดที่กระทำต่อข้อมูลข่าวสารของเครื่องคอมพิวเตอร์อันก่อให้เกิดความเสียหายต่อรัฐบาลสหรัฐ[1]

และมีการแก้ไขเพิ่มเติมในปี 1988 และ 1990 ตามลำดับเพื่อให้ครอบคลุมความผิดที่เกิดขึ้น สภาคองเกรสได้มีมติให้ออกกฎหมาย The National Information Infrastructure Protection Act of 1996 (NIIPA) [2] และเพิ่มเติมการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ใน U.S. Code title 18 มาตรา 1030 (18 U.S.C.A. section 1030)[3] สำหรับกฎหมายของมลรัฐต่างๆ เริ่มมีใน ค.ศ. 1987 โดยเริ่มมีที่มลรัฐอริโซน่า และมลรัฐฟลอริดา และหลังจากถูกกลุ่มผู้ก่อการร้ายโจมตีตึกเพนทากอนและอาคารเวิลด์เทรดเซ็นเตอร์ เมื่อวันที่ 11 กันยายน ค.ศ. 2001 จึงให้ความสำคัญกับการรักษาความปลอดภัยและความเป็นส่วนตัวกันมากขึ้น และได้จัดสรรเงินเพื่อแก้ปัญหาอาชญากรรม โดยเฉพาะในส่วนที่เกี่ยวกับความปลอดภัยในเครือข่ายคอมพิวเตอร์ (Cyber-security) และการวิจัยเกี่ยวกับการก่อการร้ายในเครือข่ายคอมพิวเตอร์ (Cyber-terrorism) [4]

3.1.1 มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา ประเทศสหรัฐอเมริกาเป็นประเทศแรกที่ประกาศใช้กฎหมายจำกัดการใช้อินเตอร์เน็ตเพื่อความบันเทิงทางเพศ คือกฎหมายควบคุมสื่อลามกและข้อความที่ไม่สมควรทางเพศบนอินเตอร์เน็ต (Communications Decency Act 1996 : CDA.) ซึ่งมีเนื้อหากำกับสิ่งที่ให้บริการทางอินเตอร์เน็ตโดยเฉพาะ โดยกำหนดให้บุคคลที่ส่งภาพหรือข้อความลามกอนาจารหรือไม่เหมาะสมขัดต่อศีลธรรมอันดี แก่ผู้เยาว์อายุต่ำกว่า 18 ปี มีความผิดต้องรับโทษปรับหรือจำคุกไม่เกิน 2 ปี [5] และถ้าผู้ใดอนุญาตให้ผู้เยาว์อายุต่ำกว่า 18 ปี ใช้อินเตอร์เน็ตหรือสถานที่เพื่อการดังกล่าวย่อมมีความผิดด้วย[6] จะเห็นได้ว่ากฎหมายฉบับนี้จำกัดสิทธิเสรีภาพและความเป็นส่วนตัวของบุคคล เมื่อกฎหมายฉบับนี้ใช้บังคับในวันที่ 8 กุมภาพันธ์ 1996 สมาคมสิทธิทางแพ่งของสหรัฐอเมริกัน (ACLU) และ

---

[1] นิติ ผดุงชัย. (2532,มิถุนายน). “กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับ Computer.” **วารสารอัยการ**. หน้า 86-88.

[2] Michael Hatcher , Jay Mc Danell , and Stacy Ostfeld. (1999). “Computer Crimes.” **American Criminal Law Review**. 36 : p.402.

[3] Ibid.p.401.

[4] “The Governance Challenge : Creating a smart and Secure Cyberspace,” Madanmohan Rao report from the ‘New Directions in Internet Policy’ conference in Atlanta, <http://www.indiainfoline.com/nevi/inwi/mm66.html.>,2002.

[5] CDA, Section 223.

[6] CDA, Section 223 (a) (2).

สมาคมห้องสมุด (ALA) ได้ยื่นฟ้องต่อศาลขอประกาศว่ากฎหมายฉบับนี้ขัดต่อรัฐธรรมนูญว่าด้วยการคุ้มครองเสรีภาพในการแสดงออก และสิทธิความเป็นส่วนตัว ตามบทแก้ไขเพิ่มเติมฉบับที่ 1 (First Amendment) และรัฐบาลสหรัฐอเมริกาก็ได้โต้แย้งว่ากฎหมายฉบับนี้บังคับใช้แต่เฉพาะบุคคลที่ไม่สุจริตและรู้ว่าผู้เยาว์ใช้บริการในสถานที่ของตน และยกเว้นบุคคลที่ไม่รู้ว่าข้อความที่ผ่านคอมพิวเตอร์ของตนนั้นเป็นข้อความหรือภาพลามก การจำกัดเสรีภาพจะกระทำต่อเด็กและเยาวชนเท่านั้น ไม่รวมถึงบุคคลทั่วไป แต่ในที่สุดศาลก็ตัดสินให้ระงับใช้กฎหมายฉบับนี้เพราะอาจจะขัดต่อรัฐธรรมนูญ [7]

3.1.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ ในปี ค.ศ. 1986 สภาคองเกรสของสหรัฐอเมริกาได้ออก The Computer Fraud and Abuse Act of 1986 ซึ่งกฎหมายฉบับนี้มีบทบัญญัติที่เปลี่ยนแปลงไปจากกฎหมายที่มีอยู่เดิม ได้แก่

3.1.2.1 ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access)

3.1.2.2 ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration)

3.1.2.3 ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction)

3.1.2.1 ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access) ความผิดฐานเข้าถึงโดยปราศจากอำนาจเป็นความผิดฐานหนึ่ง ที่เป็นการฉ้อโกงหรือกระทำการใดๆ ต่อเครื่องคอมพิวเตอร์โดยเจตนา เป็นการกระทำโดยปราศจากอำนาจ หรือกระทำเกินกว่าอำนาจที่มีอยู่ ได้แก่

(1) เข้าสู่ระบบคอมพิวเตอร์โดยรู้ว่าไม่มีอำนาจ และได้ไปซึ่งข้อมูลนั้น โดยมีเหตุเชื่อได้ว่าข้อมูลนั้นอาจถูกใช้ไปเพื่อการอันเป็นภัยต่อความมั่นคงของประเทศ หรือเพื่อประโยชน์ของชาติอื่น ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 20 ปี

(2) เข้าสู่ระบบคอมพิวเตอร์โดยรู้ว่าไม่มีอำนาจ และได้ไปซึ่งข้อมูลทางการเงินหรือข้อมูลของสถาบันการเงิน ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(3) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ และปลอมแปลงหรือแสร้งว่าเป็นเจ้าหน้าที่ของรัฐเพื่อเปิดระบบประมวลผล ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

---

[7] เลอสรร ธนสุกาญจน์และคณะ. (2541). **กฎหมายสำหรับบริการอินเตอร์เน็ตในประเทศไทย กรอบ ข้อเสนอแนะ และการควบคุมดูแล การให้บริการ**. หน้า 154.

(4) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ เพื่อผลประโยชน์ใดๆ ด้วยเจตนาฉ้อโกงหรือได้ไปซึ่งสิ่งมีค่าใดๆ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(5) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ และได้แก้ไขเปลี่ยนแปลงหรือทำลายข้อมูลที่ได้เข้าถึงนั้นเพื่อผลประโยชน์ใดๆ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(6) รู้และใช้รหัสผ่านโดยปราศจากอำนาจเพื่อเข้าถึงข้อมูลในคอมพิวเตอร์ของรัฐบาลเพื่อการค้าระหว่างรัฐหรือการค้าระหว่างประเทศ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

นอกจากความผิดข้างต้นแล้ว การเข้าถึงข้อมูลในคอมพิวเตอร์โดยปราศจากอำนาจสหรัฐอเมริกาถือเป็นการกระทำที่มิชอบเกี่ยวข้องกับกฎหมายอื่นๆอีก ดังนี้

(1) ประมวลกฎหมายอาญาสหรัฐอเมริกา เนื่องจากการเข้าถึงข้อมูลในคอมพิวเตอร์ถือเป็นการลักขโมยบริการ (Theft of Service) เพราะเป็นการใช้บริการโดยไม่มีอำนาจ แม้ในบางครั้งจะไม่ก่อให้เกิดความเสียหายก็ตาม แต่กฎหมายก็ถือว่ามีความผิด โดยถือว่าเป็นความเสี่ยงต่อการก่อให้เกิดความเสียหายต่อสารสนเทศได้และผู้กระทำย่อมรู้ตัวดี และความเสียหายจะเกิดขึ้นในอนาคต[8] เพราะว่าในการเข้าถึงโดยปราศจากอำนาจ อาจทำให้เจ้าของที่แท้จริงไม่สามารถเข้าสู่ระบบได้ จึงมีการบัญญัติกฎหมายนี้ขึ้นเพื่อคุ้มครองผู้เช่าหรือผู้มีอำนาจใช้สายสื่อสารที่ต่อเชื่อมกับระบบคอมพิวเตอร์ และกรณีของพนักงานของบริษัทที่ใช้คอมพิวเตอร์ทำงานส่วนตัวหรือคัดลอกทำสำเนาข้อมูลโดยไม่ได้รับความยินยอมจากนายจ้าง ที่เรียกว่า “การทำงานกลางคืน” (Moonlight) ก็เป็นการกระทำที่ปราศจากอำนาจ ถือเป็นการลักสิ่งที่มีค่าใดๆ (Thing of Value) อันเป็นความผิดฐานลักทรัพย์ และการกระทำดังกล่าวยังเข้าลักษณะความผิดฐานปลอมแปลงเอกสารและความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญาด้วย ซึ่งจะเห็นได้ว่ามีกฎหมายมากกว่า40 มาตราในบรรพที่ 8 ประมวลกฎหมายอาญาสหรัฐอเมริกาที่บัญญัติถึงการใช้เครื่องคอมพิวเตอร์ในการกระทำความผิดไม่ว่าโดยตรงหรือโดยอ้อม

(2) กฎหมายการสื่อสารทางอิเล็กทรอนิกส์ส่วนบุคคล (The Electronic Communication Privacy Act of 1986) กฎหมายฉบับนี้เป็นกฎหมายที่รับประกันการสื่อสารระหว่างบุคคลที่ผ่านทางโทรศัพท์ในระบบต่างๆ คลื่นวิทยุ การสื่อสารผ่านดาวเทียม และการสื่อสารผ่านทางเครือข่าย

---

[8] สุเนติ คงเทพ . (2541). **เอกสารประกอบการสัมมนาแนวทางในการแก้ปัญหากฎหมายอาชญากรรมยุคไอที เรื่องการไม่มีอำนาจเข้าสู่ระบบประมวลผล**. หน้า 16.

คอมพิวเตอร์ ไปรษณีย์อิเล็กทรอนิกส์ สาระสำคัญของกฎหมายฉบับนี้ คือ คำนิยามและข้อยกเว้นการจำกัดการสื่อสารของภาคเอกชน การเก็บรักษาและการใช้ข้อมูลจากการสื่อสาร การรับจดทะเบียน ฯลฯ

(3) กฎหมายการฉ้อโกงบัตรเครดิต (The Credit Card Fraud Act of 1984) เป็นกฎหมายที่ออกมาเพื่อควบคุมการฉ้อโกงบัตรเครดิตและการปลอมบัตรเครดิต แต่คำนิยามของคำว่า "บัตรเครดิต" ในกฎหมายฉบับนี้ได้ครอบคลุมไปถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ด้วย เช่น การกระทำความผิดที่เข้าถึงสื่อทางคอมพิวเตอร์ หมายความรวมถึงบัตรต่างๆ แผ่นพลาสติก รหัส หมายเลขบัญชี หรือสิ่งอื่นๆของบัญชี และการเข้าถึงให้หมายความถึงการเข้าถึงทางด้านบัญชีและการเข้าถึงสื่อทางคอมพิวเตอร์ อันถือเป็นการกระทำที่ได้ไปซึ่งผลประโยชน์ในด้านต่างๆ ส่วนที่กล่าวถึงการกระทำความผิดเกี่ยวกับเครื่องคอมพิวเตอร์นั้น เป็นการกระทำความผิดฐานฉ้อโกงการทำ ใช้ จำหน่าย ปลอมสื่อทางคอมพิวเตอร์ หรือการเข้าถึงโดยปราศจากอำนาจ ลักษณะของการกระทำความผิดตามกฎหมายฉบับนี้ที่เกิดขึ้นในปัจจุบัน ได้แก่ การลักลอบเข้าสู่ระบบคอมพิวเตอร์เพื่อค้นหา ทดสอบ หรือการแก้ไขเปลี่ยนแปลงข้อมูลต่างๆ เช่น หมายเลขโทรศัพท์ หมายเลขบัญชีธนาคาร หรือรหัสผ่าน

(4) กฎหมายลิขสิทธิ์ (The Copyright Act of 1976) กรณีที่มีการเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์โดยปราศจากอำนาจในลักษณะที่เป็นการลักขโมยโปรแกรมหรือข้อมูลในคอมพิวเตอร์นั้น ถือเป็นการละเมิดลิขสิทธิ์ที่มีโทษทางอาญา ตามรายงานของคณะกรรมาธิการรัฐสภาเกี่ยวกับกฎหมายลิขสิทธิ์ ค.ศ. 1976 หน้า 54 ระบุว่า "งานวรรณกรรม" (Literary Works) ให้รวมถึงฐานข้อมูลทางคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ รวมถึงงานประพันธ์ที่เป็นการแสดงออกถึงความคิดดั้งเดิมของนักเขียนโปรแกรม จึงเป็นสิทธิของผู้เขียนโปรแกรมที่จะปกป้องเอกสารและลายเส้นของรหัสคอมพิวเตอร์จากการคัดลอกหรือทำสำเนา แต่การคุ้มครองดังกล่าวก็มิได้ครอบคลุมถึง "ขั้นตอนวิธี" (Algorithms) ของผู้เขียนโปรแกรมด้วย การกระทำความผิดตามกฎหมายฉบับนี้มีโทษทั้งทางแพ่งและในทางอาญา

(5) กฎหมายการฉ้อโกงทางสายโทรศัพท์ (The Wire Fraud Act) เดิมประมวลกฎหมายสหรัฐอเมริกา มีการยกเว้นการกระทำความผิดทางสายสื่อสารสาธารณะ แต่เมื่อมีการใช้คอมพิวเตอร์จากเครือข่ายทางไกลกระทำการฉ้อโกงทางคอมพิวเตอร์ขึ้นเป็นจำนวนมาก ทั้งเป็นการกระทำความผิดของบุคคลเพียงคนเดียวและหลายคนร่วมมือกัน และผู้ที่กระทำความผิดก็ได้ผลประโยชน์ไปเป็นจำนวนมาก รัฐจึงมีมาตรการออกมาเพื่อปกป้องคุ้มครองการส่งข้อมูลผ่านทางสายสื่อสารสาธารณะดังกล่าว

(6) กฎหมายเกี่ยวกับระเบียบสถาบันทางการเงินและการควบคุมอัตราดอกเบี้ย (The Financial Institutions Regulatory and Interest rate Control Act of 1978 : FIRA) ในส่วนที่เป็นเรื่องการโอนเงินทางอิเล็กทรอนิกส์ (The Electronic Fund Transfer Act) ซึ่งมีการกำหนดคำนิยามและสิทธิส่วนบุคคลของผู้บริโภคที่ได้รับผลกระทบจากการโอนเงินทางอิเล็กทรอนิกส์ โดยกฎหมายฉบับนี้ได้กำหนดให้รัฐบาลกลางออกระเบียบการโอนเงินทางอิเล็กทรอนิกส์ขึ้น

(7) กฎหมายคุ้มครองส่วนบุคคล (The Privacy Act of 1974) กรณีที่เป็นการเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจที่จะกระทำได้ โดยกระทำผ่านฐานข้อมูลในเครื่องคอมพิวเตอร์ เป็นการให้ความคุ้มครองความเป็นส่วนตัวของบุคคล ดังนั้นการเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์โดยปราศจากอำนาจจึงอาจมีความผิดตามกฎหมายฉบับนี้ด้วย

3.1.2.2 ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration) ความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูลตาม The Computer Fraud and Abuse Act 1986 ครอบคลุมถึงการแก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ และข้อมูลที่ถูกจัดเก็บอยู่ในคอมพิวเตอร์ เหตุที่นำความผิดดังกล่าวมาบัญญัติเอาไว้ต่างหาก เนื่องมาจากการกระทำความผิดดังกล่าวมีลักษณะคล้ายกับความผิดฐานปลอมแปลงเอกสาร แต่เมื่อมีการกระทำความผิดเกิดขึ้นกลับไม่สามารถนำบทบัญญัติของกฎหมายในความผิดฐานปลอมแปลงเอกสารมาใช้บังคับได้ เพราะประสบปัญหาการตีความ โดยเฉพาะเรื่องขององค์ประกอบของความผิด ฝ่ายนิติบัญญัติของรัฐบาลกลางและมลรัฐต่างๆ จึงจำเป็นที่จะต้องบัญญัติกฎหมายขึ้นมาใช้บังคับกับความผิดดังกล่าวโดยเฉพาะ

การกระทำที่เป็นการแก้ไขเปลี่ยนแปลงโปรแกรมคอมพิวเตอร์หรือการแก้ไขเปลี่ยนแปลงข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์ ในส่วนที่เกี่ยวกับความผิดฐานปลอมเอกสารนั้นตีความจากคำว่า “เอกสาร” ที่หมายความรวมถึงโปรแกรมคอมพิวเตอร์และข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์

3.1.2.3 ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction) ความผิดฐานทำให้เสียหายหรือทำลายทางคอมพิวเตอร์ตาม The Computer Fraud and Abuse Act 1986 นั้น เป็นการกระทำที่ทำให้เกิดความเสียหายหรือทำลายโปรแกรมคอมพิวเตอร์หรือข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์และการกระทำให้เกิดความเสียหายโดยตรงต่อเครื่องคอมพิวเตอร์รวมทั้งอุปกรณ์ต่างๆของเครื่องคอมพิวเตอร์ที่เรียกว่าฮาร์ดแวร์ (Hardware) ด้วย โดยบัญญัติแยกต่างหากจากความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญา เนื่องจากเห็นว่าเป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายที่ร้ายแรง และก่อให้เกิดความเสียหายต่อเทคโนโลยี

3.1.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ การค้นข้อมูลอิเล็กทรอนิกส์เป็นการค้นที่แตกต่างจากการค้นที่มีอยู่แต่เดิม ซึ่งเมื่อพนักงานสอบสวนเห็นสมควรจะค้นจะต้องมีหมายค้น โดยจะต้องบรรยายสถานที่ที่จะทำการค้นในหมายนั้นด้วย แต่สำหรับการค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์จะต้องทำการค้นหาจากฮาร์ดแวร์หรือฮาร์ดดิสก์

ในการปฏิบัติหน้าที่ของพนักงานสอบสวนของสหรัฐอเมริกาจะต้องเป็นการค้นหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์โดยไม่ขัดต่อหลักการไม่รับฟังพยานหลักฐาน ซึ่งได้มาโดยการค้นที่มิชอบ (Exclusionary Rule) ตามรัฐธรรมนูญสหรัฐอเมริกาแก้ไขเพิ่มเติมฉบับที่ 4 (The Fourth Amendment) บัญญัติว่า "สิทธิของบุคคลที่จะมีความปลอดภัยมั่นคงในร่างกาย เคหสถาน เอกสารและวัตถุสิ่งของ ต่อการค้น การยึด และการจับที่ไม่มีเหตุอันสมควร จะถูกล่วงละเมิดมิได้ และห้ามมิให้มีการออกหมาย เว้นแต่จะโดยมีเหตุอันควร ซึ่งได้มาโดยการสาบาน หรือปฏิญาณตน และหมายนั้นจะต้องระบุเฉพาะเจาะจงถึงสถานที่ที่จะถูกค้น ตัวบุคคลที่จะถูกจับ และสิ่งของที่ถูกยึด"

นอกจากนี้กฎว่าด้วยวิธีพิจารณาความอาญาของสหรัฐได้รับรองหลักของรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่นี้ไว้ในมาตรา 41 (a) ซึ่งบัญญัติว่า "เจ้าพนักงานผู้มีอำนาจหรือพนักงานอัยการต้องขอหมายค้น…

(1) หมายค้นต้องออกโดยศาล Magistrate ของมลรัฐ หรือศาลของสหรัฐ สำหรับการค้นสิ่งของหรือค้นหาบุคคลในเขตอำนาจศาล

(2) หมายค้นออกโดยศาล Magistrate สำหรับกรณีการค้นสิ่งของหรือค้นหาบุคคลในเขตอำนาจศาลหรือค้นสิ่งของที่ถูกโยกย้ายหรือบุคคลหลบหนีออกนอกเขตก่อนจะถูกดำเนินการตามกฎหมาย"

จากกฎหมายดังกล่าวจะเห็นได้ว่าเจ้าหน้าที่ของรัฐจะทำการค้นได้ก็ต่อเมื่อมีหมายค้น และหมายค้นดังกล่าวจะต้องออกโดยผู้พิพากษา แม้ในกรณีของการค้นข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นพยานหลักฐานที่มีลักษณะพิเศษ ที่อาจถูกแก้ไขเปลี่ยนแปลงได้ง่าย เจ้าพนักงานของรัฐก็จะต้องทำการค้นโดยมีหมาย เพราะต้องการจะให้กระบวนการในการออกหมายเป็นมาตรการในการตรวจสอบการใช้ดุลพินิจของเจ้าหน้าที่ (Warrant Process) เพื่อให้เจ้าหน้าที่ปฏิบัติหน้าที่โดยไม่ขัดกับรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 4

ในกรณีที่เจ้าหน้าที่ไม่จำเป็นที่จะต้องเข้าไปค้นในเคหสถานหรือสำนักงานของผู้อื่น แต่สามารถทำการค้นโดยการใช้เครื่องคอมพิวเตอร์หรือเครื่องมืออื่นใดเชื่อมต่อเข้ากับระบบ LAN หรือ WAN ของเคหสถาน หรือสำนักงาน ตลอดจนเครือข่ายอินเตอร์เน็ต โดยไม่มีการบุกรุกเข้าไปทางกายภาพ หากพิจารณาถึงสิทธิที่ได้รับการรับรองคุ้มครองตามรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่

DPU

4 ซึ่งรวมไปถึงสิทธิส่วนบุคคลด้วย การค้นข้อมูลอิเล็กทรอนิกส์ในลักษณะนี้ ก็ถือเป็นการบุกรุกเช่นกัน

3.1.4 การรับฟังเป็นพยานหลักฐานในศาล ภายหลังที่กฎหมายอาชญากรรมคอมพิวเตอร์ในสหรัฐอเมริกาใช้บังคับแล้วยังมีปัญหาที่ตามมาอีกหลายประการ เช่น ปัญหาในการให้คำนิยามคำว่า "อาชญากรรมคอมพิวเตอร์" (Computer crime) การจำกัดการให้ความคุ้มครองที่จำกัดเฉพาะงานของรัฐไม่รวมภาคเอกชน การขาดความชัดเจนในเรื่องของเขตอำนาจศาล และปัญหาเกี่ยวกับวิธีพิจารณาความ เช่น การแสวงหาพยานหลักฐาน และการรับฟังเป็นพยานหลักฐานในศาล ทำให้ไม่สามารถนำผู้กระทำผิดมาลงโทษได้

ศาลของสหรัฐอเมริกาจะไม่รับฟังพยานหลักฐานที่เกิดจากการค้นโดยมิชอบ ดังนั้นในการค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ก็จะต้องเป็นการค้นที่ไม่ขัดต่อหลักการห้ามรับฟังพยานหลักฐานซึ่งได้มาโดยมิชอบ (Exclusionary Rule) ดังนั้นหากเจ้าหน้าที่แสวงหาพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์โดยวิธีการที่มิชอบด้วยกฎหมาย เป็นการล่วงล้ำสิทธิส่วนบุคคล พยานหลักฐานดังกล่าวก็จะถูกตัดออกจากกระบวนการพิจารณาของศาลทันที โดยศาลจะไม่รับฟัง ทำให้ไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้

3.2 ประเทศอังกฤษ

ก่อนที่จะมีกฎหมายอาญาว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือการรักษาความปลอดภัยของข้อมูลในคอมพิวเตอร์นั้น การเข้าถึงข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ในประเทศอังกฤษโดยปราศจากอำนาจไม่ถือเป็นความผิดอาญา โดยพิจารณาเปรียบเทียบจากความผิดฐานบุกรุก (Trespass) ความผิดเกี่ยวกับทรัพย์ (Theft) ที่ผู้กระทำผิดรับผิดแต่เพียงในทางแพ่ง [9] ต่อมาจึงได้บัญญัติ The Computer Misuse Act 1990 เป็นกฎหมายอาญาว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ขึ้นเป็นฉบับแรก ทั้งได้วางมาตรการในการรักษาความปลอดภัยของข้อมูลเอาไว้ด้วย

3.2.1 มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศอังกฤษ วัฒนธรรมของประเทศอังกฤษนั้นให้ความเคารพต่อสิทธิส่วนบุคคล โดยมีคดีตัวอย่างเกี่ยวกับนายจ้างและลูกจ้างที่ศาลตัดสินว่านายจ้างไม่อาจเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง ไม่ว่าข้อมูลนั้นจะเก็บไว้

---

[9] เฉลิมพล ช่อโพธิ์ทอง. (2535). **ความผิดฐานลักทรัพย์และฉ้อโกง : ศึกษาเปรียบเทียบกฎหมายอังกฤษ เยอรมัน และไทย**. หน้า 73.

ในระบบธรรมดาหรือเก็บไว้ในคอมพิวเตอร์ก็ตาม[10] ต่อมารัฐบาลอังกฤษได้พิจารณาถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ว่าควรจะมีกฎหมายคุ้มครอง เพราะจำเป็นต้องดำเนินการให้กฎหมายภายในของอังกฤษสอดคล้องกับอนุสัญญาแห่งสภายุโรปว่าด้วยการให้ความคุ้มครองข้อมูล (The Council of Europe's Data Protection) รัฐสภาของประเทศอังกฤษได้ออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (The Data Protection Act 1984 แก้ไขเพิ่มเติม ค.ศ. 1998) เพราะในการแสวงหาพยานหลักฐานของเจ้าพนักงานของรัฐ โดยล่วงล้ำเข้าไปรับรู้ถึงข้อมูลที่เกี่ยวกับการดำเนินชีวิตของผู้ต้องสงสัยหรือสารสนเทศที่อยู่ในความครอบครองของผู้ใช้ และการแสดงความคิดเห็นส่วนตัว เท่ากับเป็นการล่วงล้ำข้อมูลส่วนบุคคลที่กฎหมายอังกฤษประสงค์จะให้ปกปิด ดังเช่นคดีระหว่างนายจ้างและลูกจ้างข้างต้น การรวบรวมพยานหลักฐานด้วยวิธีการดังกล่าวอาจถูกหาว่าเป็นพยานหลักฐานที่ได้มาโดยมิชอบได้

3.2.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของอังกฤษ คือ The Data Protection Act 1998 และมีมาตรการควบคุม และตรวจสอบการทำงานของเจ้าหน้าที่โดยองค์กรภายนอกไว้อย่างรัดกุม และไม่ทำให้ประสิทธิภาพในการปราบปรามอาชญากรรมของเจ้าหน้าที่ลดลง โดยการให้ดุลพินิจในการปฏิบัติหน้าที่ของเจ้าหน้าที่ ภายใต้กฎเกณฑ์ที่กฎหมายบัญญัติไว้ใน The Police and Criminal Evidence Act 1984

กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ของอังกฤษ คือ The Computer Misuse Act 1990 ที่กำหนดความผิดไว้ 3 รูปแบบ ได้แก่

3.2.2.1 ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access)

3.2.2.2 ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง (Ulterial Hacking Offence หรือ Unauthorized Access with Intent to Commit or Facilitate Commission of Further Offences) และ

3.2.2.3 ความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ (Modification of Computer Material หรือ Unauthorized Modification)

---

[10] Edward Wilding. (1997). **Computer Evidence : A Forensic Investigations Handbook**. London : Sweet & Maxwell Ltd. p.93.

3.2.2.1 ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access) ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 1 บัญญัติว่า

(1) บุคคลจะมีความผิดเมื่อ

(a) บุคคลได้กระทำการให้คอมพิวเตอร์แสดงผล หรือแสดงการทำงานใดๆ ด้วยเจตนาที่จะผ่านสิ่งป้องกันที่มีไว้เพื่อกันการเข้าถึงระบบ และได้ทำการผ่านสิ่งป้องกันเช่นว่านั้นเข้าถึงโปรแกรมคอมพิวเตอร์ใดๆ หรือสารสนเทศที่เก็บไว้ในคอมพิวเตอร์ใดๆ

(b) การผ่านสิ่งป้องกันเข้าไปยังระบบนั้น เป็นการกระทำโดยปราศจากอำนาจ

(c) บุคคลนั้นได้รู้ขณะที่กระทำอยู่แล้วว่า การกระทำอันเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการกระทำนั้นปราศจากอำนาจ

(2) เจตนาของบุคคลที่ได้กระทำความผิดภายใต้มาตรานี้ ไม่จำเป็นต้องเป็นการกระทำที่เป็น

(a) โปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล

(b) โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือ

(c) โปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ

(3) บุคคลที่มีความผิดภายใต้บทบัญญัตินี้ จะต้องถูกพิจารณาคดีแบบรวดรัดและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

จากบทบัญญัติข้างต้นเป็นบทบัญญัติที่ไม่มีความซับซ้อน แสดงถึงการเข้าถึงข้อมูลโดยปราศจากอำนาจ แต่จะเป็นการกระทำที่มีความผิดตามมาตรานี้จะต้องเป็นการทำให้เครื่องคอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ รวมทั้งการสั่งให้เครื่องคอมพิวเตอร์แสดงการทำงานโดยระยะทางไกล (Remote) โดยไม่คำนึงถึงผลของการกระทำ ซึ่งรวมถึงการพยายามกระทำความผิดด้วย แต่ไม่รวมถึงการทำงานทางกายภาพที่กระทำต่อเครื่องหรืออุปกรณ์คอมพิวเตอร์

หากพิจารณาความรับผิดทางอาญาในระบบคอมมอนลอว์ สำหรับความผิดฐานเข้าถึงโดยปราศจากอำนาจ สามารถแยกพิจารณาได้เป็น 2 ส่วน ได้แก่

ก. ส่วนของการกระทำ (Actus Reus) คือการที่ผู้ใดกระทำการอย่างหนึ่งอย่างใดเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ และผู้กระทำต้องรับผิดแม้จะไม่สำเร็จ ทั้งนี้ไม่รวมถึงการกระทำที่เพียงแต่สัมผัสทางกายกับอุปกรณ์หรือเครื่องคอมพิวเตอร์โดยไม่มีการกระทำใดๆต่อเครื่องคอมพิวเตอร์ และการดูข้อมูลที่ปรากฏบนจอภาพ การดักข้อมูล หรือการดักฟังข้อมูล

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) แยกพิจารณาได้ดังนี้

(1) เจตนาที่จะผ่านสิ่งป้องกันที่มีเพื่อเข้าสู่ระบบ เพื่อเข้าสู่ข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ใดๆก็เป็นความผิดแล้ว ไม่จำเป็นจะต้องเป็นเจตนาโดยตรงต่อโปรแกรมหรือข้อมูลใดๆ ตามที่บัญญัติใน (2) แสดงให้เห็นว่าเจตนาของผู้กระทำไม่จำเป็นจะต้องเป็นเจตนาโดยตรงต่อโปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือโปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ ดังนั้น การกระทำโดยประมาทก็อาจมีความผิดตามมาตรานี้ได้

(2) เจตนาภายใน คือผู้กระทำต้องรู้ในขณะที่กระทำว่าตนไม่มีอำนาจที่จะกระทำได้ เป็นการทำให้เครื่องคอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ โดยปราศจากอำนาจ

ดังนั้นในการฟ้องร้องผู้กระทำความผิด โจทก์จะต้องพิสูจน์ให้ศาลเห็นว่าจำเลยมีเจตนาเข้าสู่ระบบและจำเลยรู้ว่าการกระทำของตนเป็นการทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ และเป็นการกระทำโดยปราศจากอำนาจ การพิสูจน์องค์ประกอบภายในทั้ง 2 ประการข้างต้นนี้ถือเป็นหลักในการพิสูจน์ความผิดของผู้กระทำความผิดตามหลักพื้นฐานของคอมมอนลอว์

3.2.2.2 ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง (Ulterial Hacking Offence หรือ Unauthorized Access with Intent to Commit or Facilitate Commission of Further Offences) ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 2 บัญญัติว่า

(1) บุคคลจะมีความผิดภายใต้บทบัญญัตินี้ ถ้าหากว่าเขาได้กระทำความผิดตามมาตรา 1 ข้างต้นโดยมีเจตนา

(a) กระทำความผิดในสิ่งที่มาตรานี้ใช้บังคับ หรือ

(b) ให้ความสะดวกในการกระทำความผิดไม่ว่าจะเป็นการกระทำความผิดของตนเองหรือของผู้อื่น และความผิดที่เขาเจตนากระทำหรือให้ความสะดวกดังจะกล่าวต่อไปในมาตรานี้ให้ถือว่าเป็นผู้กระทำความผิดเช่นเดียวกับผู้ที่กระทำความผิดที่ตนช่วยเหลือ

(2) มาตรานี้ใช้กับความผิด

(a) ความผิดที่บัญญัติไว้ในกฎหมายหรือ

(b) ใช้กับบุคคลที่มีอายุตั้งแต่ 21 ปีขึ้นไป

(3) ภายใต้บทบัญญัติของมาตรานี้ ไม่ว่าการกระทำความผิดของผู้กระทำที่อยู่ระยะไกล (Remote) จะได้กระทำไปในโอกาสที่ปราศจากอำนาจเข้าสู่ระบบหรือไม่ หรือโดยอาศัยโอกาสอื่นใดก็ตาม

(4) บุคคลอาจจะมีความผิดตามมาตรานี้ แม้จะปรากฏข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำที่อยู่ระยะไกลจะไม่ได้กระทำลงก็ตาม

(5) บุคคลผู้กระทำความผิดตามมาตรานี้จะต้อง

(a) ถูกพิจารณาอย่างรวดเร็วและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

จากบทบัญญัติดังกล่าวข้างต้นจะเห็นได้ว่าความผิดฐานนี้เป็นความผิดที่มีความซับซ้อนกว่าและร้ายแรงกว่าความผิดฐานเข้าถึงโดยปราศจากอำนาจ จึงไม่นำมาบัญญัติเอาไว้ต่างหาก เพราะการกระทำความผิดในมาตรานี้จะต้องเป็นการกระทำโดยเจตนาที่จะกระทำความผิดและปราศจากอำนาจที่จะกระทำ หรือเป็นการกระทำเพื่อให้ความสะดวกแก่ผู้กระทำความผิดเพื่อที่จะกระทำความผิดที่ร้ายแรง ข้อแตกต่างระหว่างมาตรา 1 กับมาตรา 2 นี้จึงอยู่ที่การพิสูจน์เจตนาในอนาคต นั่นคือการกระทำความผิดตามมาตรา 1 เป็นการกระทำที่ไม่อาจพิสูจน์เจตนาในอนาคตได้ ซึ่งจะมีโทษเบากว่า โดยถือว่าเป็นความผิดที่เรียกว่า “ความผิดที่ไกลออกไป” (Further Offence) หมายถึงความผิดที่ไม่จำเป็นต้องพิสูจน์ถึงเจตนาของผู้กระทำความผิดว่าได้เกิดขึ้นหรือไม่ แต่ถ้าเป็นกรณีที่สามารถพิสูจน์เจตนาในอนาคตได้ก็จะเป็นการกระทำความผิดตามมาตรา 2 ที่จะมีบทลงโทษผู้กระทำความผิดที่คิดจะกระทำความผิดในอนาคต และถ้าหากไม่สามารถลงโทษผู้กระผิดตามมาตรา 2 นี้ได้ก็สามารถลงโทษได้ตามมาตรา 1 ความผิดที่เกิดขึ้นในลักษณะนี้ ได้แก่ ความผิดฐานฉ้อโกง ความผิดฐานลักทรัพย์ และความผิดฐานยักยอกทรัพย์

การพิจารณาความรับผิดทางอาญาในทางคอมมอนลอว์ สำหรับความผิดฐานนี้สามารถแยกพิจารณาได้ ดังนี้

ก. การกระทำ (Actus Reus) โจทก์ต้องพิสูจน์ให้ได้ว่าจำเลยได้เข้าถึงสาระสำคัญ ได้แก่ โปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์ และ

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) ผู้กระทำมีเจตนาที่จะกระทำความผิดอื่นโดยไม่คำนึงถึงเวลาของการกระทำความผิดอื่นว่าจะกระทำในเวลาใด ไม่ว่าจะเป็นขณะที่เกือบจะเป็นเวลาเดียวกับที่เข้าถึงโดยปราศจากอำนาจ หรือในโอกาสต่อมา นั่นคือหากผู้กระทำความผิดเพียงแต่ได้ข้อเท็จจริงมาโดยตั้งใจที่จะกระทำการเข้าถึงโดยปราศจากอำนาจ แต่ยังไม่ลงมือกระทำก็ถือว่ามีความผิดตาม (4) แล้ว

3.2.2.3 ความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ (Modification of Computer Material หรือ Unauthorized Modification) ความผิดเกี่ยวกับการ

ทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 3 บัญญัติว่า

(1) บุคคลจะมีความผิดถ้า

(a) ผู้นั้นได้กระทำการใดๆ ซึ่งก่อให้เกิดการแก้ไขเปลี่ยนแปลงในเนื้อหาสาระของคอมพิวเตอร์ใดๆ และ

(b) ผู้ที่กระทำการเช่นว่านั้น จะต้องมีเจตนาหรือจะต้องรู้ถึงการกระทำของตนในขณะที่กระทำการนั้น

(2) ภายใต้บทบัญญัติของอนุมาตรา (1) (b) เจตนานั้นจะต้องเป็นเจตนาที่ต้องการแก้ไขเปลี่ยนแปลงเนื้อหาสาระของคอมพิวเตอร์ใดๆ โดยการกระทำ เช่น

(a) ทำให้เกิดความเสียหายต่อการทำงานของเครื่องคอมพิวเตอร์

(b) ขัดขวางหรือทำการกีดกันการเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลในคอมพิวเตอร์หรือ

(c) ทำให้เกิดความเสียหายต่อการทำงานของโปรแกรมคอมพิวเตอร์ หรือทำลายความเชื่อถือของข้อมูล

(3) เจตนาของการกระทำดังกล่าว ไม่จำต้องเป็นเจตนาโดยตรงต่อ

(a) คอมพิวเตอร์เฉพาะเจาะจงใดๆ

(b) โปรแกรมหรือข้อมูลพิเศษเฉพาะเจาะจงใดๆ หรือโปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่งโดยเฉพาะ หรือ

(c) การแก้ไขเปลี่ยนแปลงพิเศษเฉพาะเจาะจงใดๆ หรือการแก้ไขเปลี่ยนแปลงชนิดใดชนิดหนึ่งโดยเฉพาะ

(4) ภายใต้บทบัญญัติของอนุมาตรา (1) (b) ผู้กระทำต้องรู้ว่าการแก้ไขเปลี่ยนแปลงดังกล่าว กระทำไปโดยปราศจากอำนาจ และผู้กระทำมีเจตนาเช่นนั้น

(5) มาตรานี้ไม่ถือวัตถุประสงค์เป็นสิ่งสำคัญ โดยไม่คำนึงถึงการแก้ไขเปลี่ยนแปลงโดยปราศจากอำนาจ หรือผลจากเจตนาที่จะก่อขึ้นตาม (2) ไม่ว่าจะเป็นเจตนาที่จะก่อให้เกิดขึ้นเป็นการถาวรหรือชั่วคราว

(6) การแก้ไขเปลี่ยนแปลงในเนื้อหาสาระของคอมพิวเตอร์ตามกฎหมายฉบับนี้ จะไม่ถือว่าเป็นการก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ใดๆ ตามกฎหมายอาญาเกี่ยวกับการก่อให้เกิดความเสียหายเว้นแต่การกระทำนั้นมีผลทางกายภาพเท่านั้น

(7) บุคคลที่กระทำความผิดตามมาตรานี้จะต้อง

DPU

(a) ถูกพิจารณาอย่างรวดเร็วและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

การพิจารณาความรับผิดทางอาญาในทางคอมมอนลอว์ สำหรับความผิดฐานนี้สามารถแยกพิจารณาได้ ดังนี้

ก. การกระทำ (Actus Reus) มีการกำหนดขอบเขตของการกระทำความผิดไว้ค่อนข้างจำกัด โดยเน้นแต่เฉพาะที่เป็นการแก้ไขเปลี่ยนแปลง (Modification) ในเนื้อหาสาระ (Content) ของคอมพิวเตอร์เท่านั้น และแม้ว่าการกระทำดังกล่าวจะมีความสัมพันธ์กับการก่อให้เกิดความเสียหายทางอาญา แต่ก็ไม่ถือว่าเป็นความผิดตามกฎหมายอาญา เว้นแต่จะเป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายทางกายภาพ

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) ผู้กระทำจะต้องมีเจตนาและรู้อยู่ในขณะที่กระทำการแก้ไขเปลี่ยนแปลง ส่วนผลของการกระทำนั้นจะก่อให้เกิดความเสียหายกับทำให้เกิดความเสียหายต่อการทำงานของเครื่องคอมพิวเตอร์ ขัดขวางหรือทำการกีดกันการเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลในคอมพิวเตอร์ ทำให้เกิดความเสียหายต่อการทำงานของโปรแกรมคอมพิวเตอร์ หรือทำลายความเชื่อถือของข้อมูลเครื่องคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือข้อมูลในเครื่องคอมพิวเตอร์อย่างไรไม่จำต้องนำมาพิจารณา

3.2.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ กฎหมายที่เป็นหลักเกณฑ์ในการค้นหาพยานหลักฐานของอังกฤษ คือ The Police and Criminal Evidence Act 1984 (PACE) มาตรา 1 บัญญัติว่า “การค้นเคหสถานต้องมีเหตุอันควรสงสัยตามสมควร โดยถือมาตรฐานของบุคคลในฐานะและพฤติการณ์เดียวกับผู้ค้นเป็นเกณฑ์” และการค้นจะต้องมีการออกหมายค้นจากศาล (Justice of the peace) โดยศาลจะออกหมายค้นก็ต่อเมื่อเป็นเหตุอันควรเชื่อว่าเป็นความผิดอาญาร้ายแรง (Serious arrestable offence) ดังนั้น จึงต้องพิจารณาว่าอาชญากรรมคอมพิวเตอร์จะถือเป็นความผิดอาญาร้ายแรงที่ศาลสมควรจะออกหมายค้นหรือไม่

การค้นและยึดพยานหลักฐานต่างๆ ตามกฎหมายวิธีพิจารณาความอาญาของประเทศอังกฤษต้องคำนึงถึงแนวความคิดในเรื่องการคุ้มครองสิทธิมนุษยชนในทางอาญา ซึ่งได้บัญญัติรับรองไว้ในกฎบัตรแมคนาคาร์ตา (Magna Carta, 1215) กฎหมายของประเทศอังกฤษได้วางมาตรการควบคุม และตรวจสอบการทำงานของเจ้าพนักงานตำรวจโดยองค์กรภายนอกเอาไว้ ขณะเดียวกันก็ไม่ทำให้ประสิทธิภาพในการดำเนินงานของเจ้าหน้าที่ลดลง โดยให้เจ้าหน้าที่ของรัฐ

ได้แก่ ตำรวจ อัยการ และผู้พิพากษา สามารถใช้ดุลพินิจในการบังคับใช้กฎหมายได้มากขึ้น และในขณะเดียวกันก็มีข้อบังคับที่ตราขึ้นเพื่อควบคุมการปฏิบัติงานเอาไว้โดยละเอียด[11]

การค้นตาม The Police and Criminal Evidence Act 1984 (PACE) สามารถแยกพิจารณาได้ ดังนี้

3.2.3.1 การค้นเครื่องคอมพิวเตอร์พีซีในที่รโหฐาน

3.2.3.2 การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN ระบบ WAN และระบบอินเตอร์เน็ต

3.2.3.3 การยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์

3.2.3.1 การค้นเครื่องคอมพิวเตอร์พีซีในที่รโหฐาน ตาม PACEวางหลักไว้ในมาตรา 1 ว่า การค้นในเคหสถานต้องมีเหตุอันควรสงสัยตามสมควร โดยถือเอามาตรฐานของบุคคลในฐานะและพฤติการณ์เดียวกับผู้ค้นเป็นเกณฑ์ และจะต้องขอหมายค้นจากศาล[12] ดังนั้นในการค้นข้อมูลอิเล็กทรอนิกส์ ไม่ว่าจะอยู่ที่ใดทั้งที่อยู่ในเคหสถาน หรือที่รโหฐานอื่น เจ้าพนักงานตำรวจจะต้องมีเหตุอันควรสงสัยตามสมควรว่าจะมีพยานหลักฐานอยู่ที่นั้น และจะต้องมีศาลเป็นผู้ทำหน้าที่ตรวจสอบการดำเนินงานอีกชั้นหนึ่ง ในการออกหมายค้นนั้นศาลจะออกให้ก็ต่อเมื่อมีเหตุอันควรเชื่อว่ามีความผิดอาญาร้ายแรง (Serious Arrestable Offence) เกิดขึ้นและพยานหลักฐานที่จะพิสูจน์ความผิดได้ถูกเก็บอยู่ในนั้น จึงต้องพิจารณาว่าอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นเป็นความผิดอาญาร้ายแรงที่ศาลจะออกหมายค้นหรือไม่ ถ้าอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นเป็นความผิดอาญาร้ายแรง ศาลก็จะออกหมายค้นให้ และในการเข้าตรวจค้นตามหลักใน PACE มาตรา 16 จะต้องกระทำภายในหนึ่งเดือนนับแต่วันออกหมายค้น โดยจะต้องแจ้งเหตุแห่งการค้น และต้องค้นในเวลาที่เหมาะสม กรณีที่เจ้าของบ้านอยู่ด้วยในเวลาที่ค้น ตำรวจต้องแสดงหมายและมอบสำเนาหมายค้นให้ไว้ แต่ถ้าเจ้าของบ้านไม่อยู่ต้องปิดหมายค้นไว้ในที่ที่เหมาะสม แต่พยานหลักฐานนั้นต้องไม่เป็นพยานหลักฐานที่เป็นความลับตาม PACE มาตรา 15 ,16

กรณีการค้นโดยไม่มีหมายวางหลักไว้ใน PACE มาตรา 17 กำหนดให้ผู้ค้นจะต้องเป็นเจ้าพนักงานตำรวจที่อยู่ในเครื่องแบบ และต้องเป็นการค้นเพื่อช่วยชีวิตบุคคลในเคหสถานนั้น และเพื่อป้องกันการทำลายทรัพย์อย่างร้ายแรง

3.2.3.2 การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN ระบบ WAN และระบบอินเตอร์เน็ต

---

[11]ณรงค์ ใจหาญและคณะ. (2540). **รายงานศึกษาวิจัยฉบับสมบูรณ์ เรื่อง สิทธิผู้ต้องหา จำเลย และผู้ต้องโทษในคดีอาญา (รายงานการศึกษาวิจัยเสนอต่อคณะกรรมการกฤษฎีกา)**. หน้า 23.

[12] ณรงค์ ใจหาญและคณะ. เล่มเดิม. หน้า 51.

ตำรวจอังกฤษจะใช้วิธีนำเครื่องคอมพิวเตอร์หรือเครื่องมืออื่นเชื่อมเข้าไปในระบบเฉพาะของสำนักงาน และระบบเครือข่ายอินเตอร์เน็ต เพื่อเข้าไปตรวจค้นข้อมูลในนั้น จะขอหมายจาก Justice of the Peace ไม่ได้ แต่จะต้องขอจาก Circuit Judge และศาลจะออกหมายให้ต่อเมื่อไต่สวนได้ความว่า "มีเหตุอันควรเชื่อว่าพยานหลักฐานที่เกี่ยวกับการสอบสวนในคดีความผิดเป็น ความผิดอาญาร้ายแรง (Serious Arrestable Offence) ซึ่งเกิดขึ้นในบ้านนี้ และถ้าไม่ค้นบ้านนี้ก็จะไม่ได้มาซึ่งพยานหลักฐานดังกล่าว และในการค้นนั้นจะได้มาซึ่งพยานหลักฐานอันเป็นประโยชน์ต่อสาธารณชน"[13]

3.2.3.3 การยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์ ในการยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์มีบัญญัติอยู่ใน PACE มาตรา 18,19 ดังนี้

มาตรา 18 บัญญัติว่า "เมื่อค้นแล้วตำรวจต้องทำบันทึกการค้นและบันทึกรายการสิ่งของที่ค้นและยึด รายการเหล่านั้นผู้ค้นต้องมอบให้แก่เจ้าของบ้านเมื่อผู้นั้นร้องขอ" และ

มาตรา 19 บัญญัติว่า "กรณีที่ตำรวจยึดวัตถุที่มีเหตุเชื่อได้ว่าเป็นพยานหลักฐานที่เกี่ยวข้องกับการสอบสวน หรือความผิดอื่น หรือมีความผิดอื่นรวมอยู่ด้วย หรือมีความจำเป็นต้องยึดเพื่อป้องกันการเคลื่อนย้าย ซ่อนเร้น หรือทำลายหลักฐาน"

จากบทบัญญัติข้างต้นจะเห็นได้ว่าเครื่องคอมพิวเตอร์ที่ยึดได้นั้นเป็นวัตถุที่ใช้เป็นพยานหลักฐานในการสอบสวนที่เจ้าหน้าที่ตำรวจยึดได้ รวมทั้งข้อมูลที่อยู่ภายในเครื่องด้วย เว้นแต่กรณีที่เป็นข้อมูลที่เป็นความลับ ที่จะต้องพิจารณาตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลประกอบ

3.2.4 การรับฟังเป็นพยานหลักฐานในศาล การรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ของศาลอังกฤษ โดยหลักจะรับฟังแต่พยานหลักฐานโดยตรง พยานบอกเล่า (Hearsay) ถือว่ามีน้ำหนักน้อยหรือไม่รับฟังเลย แต่ The Police and Criminal Evidence Act 1984 เป็นกฎหมายพยานหลักฐานในคดีอาญา ที่มีบทบัญญัติเกี่ยวกับการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์อยู่ เป็นข้อยกเว้นของพยานบอกเล่า (Hearsay) โดยให้รับฟังพยานเอกสารที่เป็นผลจากการประมวลผลหรือคำนวณของเครื่องคอมพิวเตอร์ได้ การค้นและยึดพยานหลักฐานกระทำโดยเจ้าพนักงานตำรวจ กรณีที่ประสบปัญหาการกระทำความผิดทางอินเตอร์เน็ตที่การกระทำอาจเกิดขึ้นในต่างประเทศ อำนาจในการสอบสวนจะสามารถกระทำได้เพียงใด เช่น การกระทำความผิดเกิดขึ้นในประเทศเยอรมนี และผู้กระทำความผิดอยู่ที่ประเทศนั้น แต่เครือข่ายที่ใช้ข้อมูลหรือข้อมูลที่ใช้ผ่านประเทศอังกฤษจะต้องคำนึงถึงข้อตกลงระหว่างประเทศ โดยเฉพาะข้อตกลงระหว่าง

---

[13] ณรงค์ ใจหาญและคณะ. เล่มเดิม. หน้า 52.

ประชาคมยุโรปด้วย แม้ว่าจะต้องคำนึงถึงเรื่องดังกล่าวการดำเนินคดีตามกฎหมายอังกฤษจะถือหลักว่า ถ้าเข้าหลักเกณฑ์ 2 ประการดังต่อไปนี้ประเทศอังกฤษก็อาจจะไม่นำมาดำเนินคดี คือ

ก. ถ้าผู้กระทำความผิดหรือผู้ร่วมกระทำความผิดไม่ใช่พลเมืองของประเทศอังกฤษ หรือ

ข. ความผิดที่เกิดขึ้นไม่ได้บัญญัติไว้ใน The Computer Misuse Act 1990

ศาลที่มีอำนาจในการพิจารณาคดี สามารถแบ่งได้ตามฐานความผิด ดังนี้

(1) ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access) เป็นการกระทำความผิดที่ไม่ซับซ้อน ศาลที่มีอำนาจในการพิจารณาคดีคือศาลแขวง(Magistrate Court) จึงมีกฎหมายที่เกี่ยวข้องอีกฉบับคือ The Magistrate's Court Act 1980 เป็นเรื่องเกี่ยวกับการกำหนดฐานความผิดแก่ผู้ที่ให้ความช่วยเหลือในการกระทำความผิดใน มาตรา 44 (1) ซึ่งบัญญัติว่า "สามารถลงโทษบุคคลที่ให้ความช่วยเหลือผู้ที่กระทำการเข้าถึงโดยปราศจากอำนาจ โดยการให้ความรู้ทางด้านข้อมูล การให้รหัสผ่าน หรือให้วิธีการเข้าสู่ระบบเพื่อผ่านไปยังโปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์"

(2) ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง และความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ ขึ้นอยู่กับความร้ายแรงของการกระทำความผิด หากมีความร้ายแรงมากก็จะอยู่ในอำนาจพิจารณาของศาลสูงคดีอาญา (Crown Court) แต่ถ้าไม่ร้ายแรงมากก็จะอยู่ในอำนาจพิจารณาของศาลแขวง (Magistrate Court)

โดยลักษณะของข้อมูลอิเล็กทรอนิกส์ที่ไม่สามารถพิสูจน์ได้ในทางกายภาพ จึงไม่สามารถนำมาพิสูจน์ในกระบวนพิจารณาคดีอาญาได้ ดังนั้นรายงานที่ประมวลผลจากคอมพิวเตอร์ (Printout) จะเป็นพยานบอกเล่า (Hearsay) เนื่องจากเกิดจากการกระทำของมนุษย์ ต้องห้ามรับฟังตามกฎหมาย Criminal Justice Act 1988 มาตรา 24 แต่จากความสามารถในการทำงานของคอมพิวเตอร์เองที่สามารถใช้เป็นเครื่องกล หรือเครื่องมือในการคำนวณ จึงไม่น่าจะเป็นพยานหลักฐานในรูปพยานบอกเล่าเสมอไป ถ้าอ้างเป็นพยานหลักฐานโดยยืนยันการใช้ที่เป็นธุรกิจปกติ และข้อมูลที่ได้ก็เกิดจากการประมวลผลโดยคอมพิวเตอร์อันเป็นปกติเช่นกัน[14]

3.3 ประเทศญี่ปุ่น

---

[14] Richard May. (1999). **Criminal Evidence. London**. p. 11-36.

รัฐธรรมนูญของประเทศญี่ปุ่นไม่ได้วางหลักคุ้มครองความเป็นอยู่ส่วนตัวไว้โดยชัดแจ้งแต่เป็นหลักที่อาจสังเคราะห์ขึ้นจากหลักเสรีภาพทั่วไปที่บัญญัติไว้ในมาตรา 13[15] ประกอบกับหลักเสรีภาพในการติดต่อสื่อสารกันโดยอิสระในมาตรา 21[16] และหลักเสรีภาพในเคหสถาน ในเอกสาร และทรัพย์สินส่วนตัว ในมาตรา 35[17] ดังนั้นการเข้าไปในเคหสถาน การค้นและการยึดทรัพย์สินจะกระทำมิได้ ยกเว้นมีหมายที่ออกโดยข้าราชการฝ่ายตุลาการ โดยในหมายนั้นจะต้องระบุเหตุผลที่สมควรและกำหนดสถานที่ตรวจค้นและทรัพย์ที่ต้องการยึดไว้โดยชัดแจ้ง

3.3.1 มาตรการเพื่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศญี่ปุ่น การค้นตามกฎหมายวิธีพิจารณาความอาญาของญี่ปุ่นนั้น ให้อำนาจพนักงานอัยการ หรือเจ้าพนักงานตำรวจดำเนินการค้นได้ ภายใต้รัฐธรรมนูญ มาตรา 35 วรรคหนึ่ง ดังนั้นทำการค้นได้ตามกฎหมายญี่ปุ่นต้องมีหมายค้น การค้นข้อมูลอิเล็กทรอนิกส์ก็เช่นกัน ยกเว้นกรณีที่เป็นการกระทำความผิดซึ่งหน้าตามมาตรา 33 ที่ไม่ต้องมีหมายค้น เนื่องจากเป็นการกระทำความผิดหรือถูกจับเนื่องจากการกระทำความผิดซึ่งหน้า รัฐธรรมนูญได้วางหลักเกณฑ์ให้เจ้าพนักงานสามารถค้น และยึดได้ก็ต่อเมื่อมีหมายค้นหรือหมายยึด หรือเป็นกรณีที่เป็นการค้นหรือการยึดที่สืบเนื่องจากการจับกุมตัวผู้กระทำความผิด

สำหรับการค้นเพื่อทำการยึดจดหมายหรือโทรสาร เนื่องจากรัฐธรรมนูญได้ให้ความคุ้มครองสิทธิเสรีภาพในการสื่อสารของบุคคลไว้ใน มาตรา 35 วรรคหนึ่ง ดังนั้นการยึดจดหมายหรือโทรสารที่บุคคลใช้ติดต่อสื่อสารกันย่อมเป็นการกระทำที่ขัดต่อสิทธิเสรีภาพในการสื่อสารที่รัฐธรรมนูญได้บัญญัติรับรองไว้ แต่ถ้าเป็นกรณีที่เจ้าพนักงานกระทำไปเพื่อการแสวงหาพยานหลักฐานในการพิสูจน์ความผิด หรือเพื่อป้องกันอาชญากรรมก็สามารถดำเนินการค้นและยึดได้ [18]

---

[15] มาตรา 13 บัญญัติว่า "ประชาชนทุกคนย่อมได้รับการเคารพในฐานะปัจเจกบุคคล สิทธิของประชาชนในชีวิต เสรีภาพ และการแสวงหาความผาสุกภายในขอบเขตที่ไม่ขัดต่อประโยชน์สุขอันร่วมกันของสาธารณะ ต้องได้รับความเคารพสูงสุดในการออกกฎหมายหรือในการอื่นใดที่เกี่ยวกับการปกครองประเทศ"

[16] มาตรา 21 บัญญัติว่า "เสรีภาพในการชุมนุม การรวมกลุ่ม รวมทั้งการพูด การพิมพ์ และสิ่งใดทั้งปวงที่เป็นการแสดงออกเป็นสิ่งที่ได้รับการคุ้มครอง

[17] มาตรา 35 บัญญัติว่า "บุคคลใดก็ตาม หากไม่มีหมายซึ่งออกโดยเหตุผลอันชอบธรรมและระบุชัดถึงสถานที่ที่จะตรวจค้นและสิ่งของที่จะอายัด สิทธิที่จะไม่ให้เข้าไปในเคหสถาน ไม่ให้ถูกตรวจค้นและอายัดเอกสารและสิ่งของในครอบครอง ย่อมจะไม่ถูกละเมิด เว้นแต่กรณีตามมาตรา 33

การตรวจค้นและอายัดจะดำเนินการโดยหมายแต่ละประเภท ซึ่งออกโดยเจ้าพนักงานกระบวนการยุติธรรมที่มีอำนาจ"

[18] Shigemitsu Dando. (1965). **Japanese Criminal Procedure**. p. 270

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในการประมวลผลด้วยเครื่องคอมพิวเตอร์ของหน่วยงานฝ่ายปกครอง ค.ศ. 1988 รัฐสภาญี่ปุ่นบัญญัติขึ้นโดยอาศัยแนวทางของ Organization for Economic Co-operation and Development (OECD) ที่เสนอให้กำหนดหน้าที่ของหน่วยงานในการรักษาความปลอดภัย วางหลักเกณฑ์ในการเข้าถึงข้อมูล และการแก้ไขข้อมูลให้ถูกต้อง โดยกฎหมายฉบับนี้ได้กำหนดให้หน่วยงานของรัฐจำกัดบทบาทในการรวบรวมข้อมูลข่าวสารส่วนบุคคลและโฆษณาให้สาธารณชนทราบการจัดระบบข้อมูลข่าวสารส่วนบุคคลของหน่วยงาน และห้ามมิให้หน่วยงานของรัฐใช้ข้อมูลของรัฐโดยผิดวัตถุประสงค์ คือห้ามมิให้นำข้อมูลข่าวสารส่วนบุคคลซึ่งจัดเก็บโดยมีวัตถุประสงค์อย่างหนึ่งไปใช้ในวัตถุประสงค์อย่างอื่น

3.3.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ การดักฟังการติดต่อสื่อสารถือเป็นการละเมิดเสรีภาพในการติดต่อสื่อสารซึ่งได้รับความคุ้มครองตามรัฐธรรมนูญ มาตรา 21 วรรคสองตอนท้าย บัญญัติว่า “ความลับในการสื่อสารจะละเมิดมิได้” ดังนั้นโดยหลักแล้วการดักฟังย่อมกระทำมิได้ อย่างไรก็ดีรัฐสภาญี่ปุ่นได้ตรากฎหมายว่าด้วยการดักฟังการสื่อสารทางโทรคมนาคม (Communications Interception Law) ขึ้นใช้บังคับในเดือนสิงหาคม ค.ศ. 1999 ซึ่งให้อำนาจเจ้าพนักงานอัยการหรือตำรวจชั้นผู้ใหญ่ในการดักฟังทางโทรศัพท์หรือการดักจับสัญญาณโทรสารและติดตามเฝ้าดูกฎหมายอิเล็กทรอนิกส์ในการสอบสวนคดียาเสพติด การฆาตกรรม หรือคดีอาญาที่มีการใช้อาวุธ หรือการลักลอบหนีภาษีของชาวต่างชาติ โดยจะต้องได้รับอนุญาตจากศาล และให้มีระยะเวลาดักฟังยาวนานที่สุดไม่เกิน 10 วัน โดยจะขอขยายได้ไม่เกิน 30 วัน

นอกจากนี้ในการดักฟังจะต้องมีบุคคลอื่นที่เป็นบุคคลภายนอก เช่น เจ้าหน้าที่ของบริษัทโทรเลขโทรศัพท์แห่งชาติของญี่ปุ่นร่วมฟังด้วยและภายหลังจากการดักฟังสิ้นสุดลงเจ้าพนักงานตำรวจหรือพนักงานอัยการซึ่งทำหน้าที่ดักฟังจะต้องแจ้งให้ผู้ถูกดักฟังทราบถึงการดักฟังนั้นภายใน 30 วัน

สำหรับสิ่งที่กฎหมายญี่ปุ่นบัญญัติไม่ให้ดำเนินการค้นหรือยึด[19] ได้แก่

ก. เอกสารที่เป็นความลับทางราชการ ซึ่งเจ้าพนักงานจะทำการค้นหรือยึดได้ก็ต่อเมื่อมีคำร้องไปยังหัวหน้าหน่วยงานที่มีเอกสารดังกล่าว และต้องได้รับความยินยอมให้ทำการตรวจค้นหรือยึดเอกสารดังกล่าวจากหัวหน้าหน่วยงานนั้นๆด้วย หากหัวหน้าหน่วยงานดังกล่าวไม่ยินยอมให้ค้นหรือยึดเอกสารนั้น เนื่องจากความมั่นคงของประเทศก็สามารถทำได้

---

[19] Ibid. p.300.

ข. เอกสารหรือสิ่งของที่เป็นความลับของลูกค้าในทางการแพทย์ หรือลูกความ เจ้าพนักงานไม่สามารถเข้าไปค้นหรือยึดได้ เว้นแต่จะได้รับความยินยอมจากบุคคลผู้ครอบครอง หากผู้ครอบครองไม่ยินยอมให้เจ้าพนักงานทำการค้นหรือยึดก็ต้องแจ้งเหตุผลที่ไม่ยินยอมให้เจ้าพนักงานทราบด้วย

3.3.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ รัฐธรรมนูญของประเทศญี่ปุ่นบัญญัติไว้ว่าการค้นจะกระทำได้ก็ต่อเมื่อมีหมายที่ออกโดยศาล และจะต้องเป็นการค้นเพื่อการสืบสวนการกระทำความผิดอาญา เป็นการแสวงหาพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดอาญา ซึ่งการแสวงหาพยานหลักฐานดังกล่าวจะกระทำได้ทั้งก่อน และระหว่างการพิจารณา

3.3.3.1 เหตุแห่งค้น ตามกฎหมายประเทศญี่ปุ่น แบ่งออกเป็น 2 ประเภท ได้แก่

ก. กรณีปกติ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 218 กฎหมายบัญญัติให้อำนาจเจ้าพนักงานของรัฐ ได้แก่ พนักงานอัยการ อัยการผู้ช่วย หรือตำรวจสามารถดำเนินการค้นและยึดได้ แต่ถ้าเป็นการค้นหรือยึดในที่รโหฐานก็ต้องดำเนินการตามหมายค้นหรือยึดที่ออกโดยศาล โดยกำหนดว่าการค้นหรือยึดสิ่งของต่างๆนั้นต้องเป็นไปเพื่อการสืบสวนการกระทำความผิดอาญา การสอบสวนเป็นกระบวนการที่กฎหมายอนุญาตให้เจ้าพนักงานดังกล่าวข้างต้นมีอำนาจในการแสวงหาพยานหลักฐานเพื่อพิสูจน์การกระทำความผิด โดยการแสวงหาพยานหลักฐานนั้นจะต้องกระทำก่อนหรือในระหว่างการพิจารณาคดี[20] เหตุที่เจ้าพนักงานจะขอหมายค้นหรือหมายยึดภายในที่รโหฐานได้ ต้องเป็นกรณีที่มีการแสวงหาพยานหลักฐานที่พิสูจน์การกระทำความผิดกรณีที่พยานหลักฐานดังกล่าวเป็นวัตถุสิ่งของ หากเป็นการค้นหาตัวบุคคลนั้นรัฐธรรมนูญ มาตรา 33 ได้กำหนดว่าเป็นการค้นเพื่อจับกุมผู้กระทำความผิดตามหมายจับ หรือค้นเพื่อหาตัวบุคคลที่ได้กระทำความผิดซึ่งหน้า เจ้าพนักงานสามารถดำเนินการค้นภายในที่รโหฐานได้โดยไม่จำเป็นต้องขอหมายศาล

ข. กรณีพิเศษ เป็นการค้นที่รโหฐานกรณีที่ไม่ต้องมีหมายค้น หรือหมายยึด แต่ก็ต้องเป็นกรณีที่สืบเนื่องมาจากการจับกุม ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 199 บัญญัติหลักเกณฑ์ที่สามารถทำได้ 3 กรณี ได้แก่

(1) การค้นและยึดที่สืบเนื่องจากการจับกุมภายใต้หมายจับที่ออกโดยศาล ตามมาตรา 199 ประกอบมาตรา 220 โดยมาตรา 220 อนุญาตให้เจ้าพนักงานสามารถทำการค้นและยึดสิ่งของกรณีที่เจ้าพนักงานทำการจับกุมผู้ต้องหาที่ศาลออกหมายจับได้ โดยกฎหมายกำหนดให้เจ้าพนักงาน

---

[20] Ibid. p.303.

เหล่านั้นแจ้งต่อศาลว่ามีการกระทำความผิดเกิดขึ้น และเชื่อว่าบุคคลที่จะต้องถูกจับมีความผิดอาญาดังกล่าว

หากเจ้าพนักงานเห็นว่าสิ่งใดสามารถใช้ในการพิสูจน์ความผิดได้ ก็สามารถนำเหตุผลดังกล่าวไปขออนุญาตต่อศาล เพื่อขอหมายค้นเข้าไปค้นหาสิ่งของดังกล่าวมาประกอบการพิจารณาได้ แต่ถ้าเป็นความผิดที่มีอัตราโทษน้อย เช่น โทษปรับไม่เกิน 100 เยน เป็นต้น ไม่จำต้องขอหมายจับจากศาล

3.3.3.2 วิธีการค้น ตามกฎหมายประเทศญี่ปุ่น แบ่งออกเป็น 2 ประเภท ได้แก่

ก.การค้นที่สืบเนื่องจากการจับกุมตามหมายจับ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 201 เมื่อเจ้าพนักงานได้รับหมายจับจากศาลแล้วสามารถไปดำเนินการตามหมายจับดังกล่าวได้เลย หากบุคคลดังกล่าวอยู่ภายในเคหสถาน หรือสถานที่ใดก็ตาม เจ้าพนักงานสามารถเข้าไปได้โดยไม่ต้องมีหมายค้นจากศาล แต่เมื่อพบบุคคลดังกล่าวแล้วก็ต้องแสดงหมายจับให้ดู

ข. การค้นที่สืบเนื่องจากการจับกุมที่ผู้กระทำความผิดได้กระทำความผิดซึ่งหน้า ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 213 บัญญัติให้อำนาจเจ้าพนักงานได้แก่ เจ้าพนักงานอัยการ อัยการผู้ช่วย หรือตำรวจ สามารถทำการจับกุมผู้ที่กระทำความผิดซึ่งหน้าตนได้โดยไม่ต้องมีหมายจับ ถ้าการจับกุมดังกล่าวเกิดขึ้นในที่รโหฐาน เจ้าพนักงานสามารถค้นและยึดสิ่งของภายในสถานที่ดังกล่าวได้โดยไม่ต้องมีหมาย แต่จะต้องเป็นกรณีที่สามารถออกหมายค้นหรือยึดได้ด้วย และเมื่อพบสิ่งที่ต้องการยึดแล้วจะต้องรีบคืนสิ่งของดังกล่าวให้เจ้าของที่แท้จริงโดยด่วน

สำหรับการกระทำความผิดซึ่งหน้านั้น ตามกฎหมายญี่ปุ่น ได้แก่การกระทำความผิดที่บุคคลได้ลงมือกระทำความผิดในขณะนั้น หรือเพิ่งลงมือกระทำความผิด มีลักษณะการกระทำความผิด 4 ประเภท [21] ได้แก่

(1) เมื่อพบเห็นการกระทำความผิดและติดตามจับกุมแบบกระชั้นชิด

(2) เมื่อพบผู้กระทำความผิดครอบครองทรัพย์สิน อาวุธ หรือสิ่งของที่เกี่ยวข้องกับการกระทำความผิด

(3) เมื่อพบว่าร่างกาย หรือเสื้อผ้าของบุคคลดังกล่าวมีร่องรอยการต่อสู้ บาดแผล หรือมีสิ่งที่บ่งบอกว่าได้กระทำความผิดมา

(4) เมื่อเจ้าพนักงานเรียกให้หยุดแต่กลับวิ่งหนี

---

[21] Ibid. p.310.

หากพบเห็นลักษณะของการกระทำประเภทใดประเภทหนึ่งข้างต้นแล้ว ผู้กระทำความผิดได้ถูกจับกุมในเคหสถาน หรือที่รโหฐาน เจ้าพนักงานที่มีอำนาจสามารถทำการตรวจค้นและยึดสิ่งของภายในสถานที่ดังกล่าวได้โดยไม่ต้องมีหมายค้น หรือยึด

ค. การค้นในกรณีฉุกเฉิน เป็นการค้นหรือการยึดในที่รโหฐานที่สืบเนื่องมาจากการจับกุมผู้ต้องหาในกรณีฉุกเฉินตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 210 กรณีที่มีเหตุเพียงพอที่จะเชื่อว่ามีการกระทำความผิดที่มีอัตราโทษจำคุกมากกว่า 3 ปีขึ้นไป โดยเจ้าพนักงานอัยการ อัยการผู้ช่วย หรือตำรวจ แต่ไม่สามารถขอหมายศาลได้ในขณะนั้น เป็นเหตุให้จับกุมโดยไม่มีหมาย เมื่อทำการจับกุมผู้ต้องหาได้แล้วต้องรีบดำเนินการขอหมายศาลทันที เมื่อเจ้าพนักงานทำการจับกุมผู้ต้องหาได้แล้ว เจ้าพนักงานก็สามารถทำการตรวจค้นหรือยึดได้โดยไม่ต้องมีหมายค้น แต่ถ้าศาลไม่ออกหมายจับให้ เจ้าพนักงานผู้ดำเนินการจับกุมก็ต้องปล่อยตัวบุคคลดังกล่าวทันที พร้อมทั้งคืนสิ่งที่ค้นหรือยึดมาด้วย หากศาลออกหมาย[22]

ง.การค้นโดยประชาชนทั่วไป กรณีที่เป็นการกระทำความผิดซึ่งหน้า ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 213 ให้อำนาจประชาชนทั่วไปสามารถจับกุมผู้ที่กระทำความผิดดังกล่าวได้ด้วย แต่กฎหมายไม่อนุญาตให้บุคคลดังกล่าวตรวจค้น หรือยึดสิ่งของ

3.3.3.3 ระยะเวลาในการค้น การที่กฎหมายให้อำนาจเจ้าพนักงานทำการค้นได้ถือเป็นการกระทำที่ละเมิดต่อสิทธิของบุคคลผู้เป็นเจ้าของ เพราะสิ่งที่กฎหมายประสงค์จะคุ้มครอง คือ สิทธิในการครอบครองและการพักอาศัยของบุคคลในเคหสถาน แต่ด้วยเหตุจำเป็นจึงอนุญาตให้ทำได้ อย่างไรก็ตามกฎหมายก็ได้กำหนดระยะเวลาในการค้นเอาไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 116 เนื่องจากเป็นการกระทำที่รบกวนสิทธิของผู้เป็นเจ้าของสถานที่กฎหมายจึงบัญญัติให้ทำการค้นและยึดได้แต่ในเวลากลางวันเท่านั้น ซึ่งเป็นเวลาตั้งแต่พระอาทิตย์ขึ้นจนถึงพระอาทิตย์ตก เพราะในเวลากลางคืนเป็นเวลาพักผ่อนของผู้ครอบครอง

กรณีที่เจ้าพนักงานทำการตรวจค้นในเวลากลางวันแล้วไม่เสร็จในช่วงเวลานั้น ก็สามารถทำการตรวจค้นต่อเนื่องไปในเวลากลางคืนได้ และกฎหมายก็ให้อำนาจทำการค้นในเวลากลางคืนได้ ตามมาตรา 117 กรณีที่ศาลเห็นว่าจำเป็นที่จะต้องทำการค้นในเวลากลางคืน โดยระบุลงไปในหมายไว้ด้วย สถานที่ที่ศาลอนุญาตให้ทำการตรวจค้นในเวลากลางคืนได้ เช่น สถานบันเทิงเริงรมย์ บ่อนการพนัน โรงแรม หรือร้านอาหาร ฯลฯ

---

[22] Ibid. p.316.

3.3.4 การรับฟังเป็นพยานหลักฐานในศาล ศาลสูงสุดของประเทศญี่ปุ่นได้วางมาตรการในการรับฟังพยานหลักฐานสำหรับการค้นเอาไว้เช่นเดียวกับประเทศอื่นๆ คือ ห้ามมิให้รับฟังพยานหลักฐานที่ได้มาจากการค้น โดยไม่มีหมายค้น โดยมาตรการดังกล่าวเป็นเพียงวิธีการในการป้องกันมิให้เจ้าหน้าที่ใช้อำนาจในทางมิชอบเท่านั้น มิใช่ไม่รับฟังพยานหลักฐานดังกล่าวเลย เพราะในทางปฏิบัติของศาลญี่ปุ่นการรับฟังพยานหลักฐานจะพิจารณาถึงความรุนแรงของการกระทำความผิด ประกอบกับความมุ่งหมายของการสอบสวน

จากการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกานั้นไม่ได้มีกฎหมายที่เป็นกลางซึ่งจะวางหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ กฎหมายที่มีผลใช้บังคับอยู่ในปัจจุบันเป็นแต่เพียงกฎหมายที่ให้ความคุ้มครองเฉพาะเรื่อง เช่น การเงิน คอมพิวเตอร์ ฯลฯ ทั้งยังขาดหน่ายงานอิสระที่เป็นองค์กรกลางคอยทำหน้าที่ควบคุม ตรวจตรา และบังคับการให้เป็นไปตามกฎหมาย สำหรับหน่วยงานที่มีอยู่ในปัจจุบันก็ขาดความเป็นอิสระและไม่มีอำนาจเด็ดขาด เนื่องจากเป็นหน่วยงานของฝ่ายบริหาร

สำหรับประเทศอังกฤษซึ่งให้ความเคารพต่อสิทธิส่วนบุคคล และความจำเป็นที่จะต้องดำเนินการให้กฎหมายภายในของตนสอดคล้องกับอนุสัญญาแห่งสภายุโรปว่าด้วยการให้ความคุ้มครองข้อมูล (The Council of Europe's Data Protection) รัฐสภาของประเทศอังกฤษจึงต้องออกกฎหมายเพื่อแสวงหาพยานหลักฐานของเจ้าพนักงานของรัฐ สามารถล่วงล้ำเข้าไปรับรู้ถึงข้อมูลที่เกี่ยวกับการดำเนินชีวิตของผู้ต้องสงสัยหรือสารสนเทศที่อยู่ในความครอบครองของผู้ใช้ และการแสดงความคิดเห็นส่วนตัว เท่ากับเป็นการล่วงล้ำข้อมูลส่วนบุคคลที่กฎหมายอังกฤษประสงค์จะให้ปกปิด ดังเช่นคดีระหว่างนายจ้างและลูกจ้างข้างต้น การรวบรวมพยานหลักฐานด้วยวิธีการดังกล่าวอาจถูกหาว่าเป็นพยานหลักฐานที่ได้มาโดยมิชอบได้ ทั้งกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของอังกฤษ ที่มีมาตรการควบคุม และตรวจสอบการทำงานของเจ้าหน้าที่โดยองค์กรภายนอกไว้อย่างรัดกุม และไม่ทำให้ประสิทธิภาพในการปราบปรามอาชญากรรมของเจ้าหน้าที่ลดลง โดยการให้ดุลพินิจในการปฏิบัติหน้าที่ของเจ้าหน้าที่ ภายใต้กฎเกณฑ์ที่กฎหมายบัญญัติไว้ จึงดูมีความน่าเชื่อถือที่สุด

ประเทศญี่ปุ่นเองก็มีความพยายามที่จะตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลไว้เป็นกฎหมายทั่วไป แต่ก็ไม่ได้วางมาตรการที่ให้ความคุ้มครองที่เคร่งครัดเกินไป เพราะในขณะเดียวกันก็ให้ตรากฎหมายให้อำนาจเจ้าพนักงานของรัฐเข้าสู่ข้อมูลบางประเภทได้ แต่การแสวงหาพยานหลักฐานจากข้อมูลส่วนบุคคลในประเทศญี่ปุ่นเมื่อเทียบกับอีกสองประเทศข้างต้น ก็ยังเป็นเรื่องใหม่ที่ยังต้องรอให้มีการวางมาตรการ บัญญัติกฎหมายลำดับรอง เพื่อบังคับใช้ตามกฎหมายที่มีอยู่ให้มีประสิทธิภาพมากขึ้น เนื่องจากกฎหมายที่มีนั้นยังไม่สามารถนำมาใช้บังคับได้อย่างเต็มที่

อย่างไรก็ดีประสบการณ์ของทั้งสามประเทศต่างก็มีประโยชน์ต่อการนำมาศึกษาเปรียบเทียบกับกฎหมายของไทยที่มีอยู่

DPU

บทที่ 4
วิเคราะห์มาตรการทางกฎหมายในการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในประเทศไทย

ระบบอินเตอร์เน็ตได้รับการพัฒนาขึ้นมาเพื่อประโยชน์ทางด้านการสื่อสารระหว่างมนุษย์ในรูปของสื่อผสม (Multimedia) ซึ่งบุคคลสามารถติดต่อถึงกันได้โดยอาศัยสื่อหลายประเภทผสมกัน ไม่ว่าจะเป็นการรับส่งข้อความธรรมดา การรับส่งภาพ หรือเสียง ตลอดจนข้อมูลอิเล็กทรอนิกส์ เช่น โปรแกรมคอมพิวเตอร์ [1] มีการส่งเสริมให้มีการใช้คอมพิวเตอร์ในประเทศต่างๆ แม้เครื่องมืออิเล็กทรอนิกส์ โดยเฉพาะคอมพิวเตอร์และเครือข่ายอินเตอร์เน็ตนั้นก็มีทั้งคุณและโทษ แต่ก็น่าจะเป็นคุณมากกว่า ประเทศต่างๆจึงให้ความสำคัญ และพยายามที่จะหามาตรการมาแก้ปัญหาที่เกิดขึ้นบนเครือข่ายคอมพิวเตอร์ ประเทศต่างๆ ทั้งในยุโรป อเมริกา ออสเตรเลีย และประเทศในแถบเอเชีย เช่น ญี่ปุ่น ต่างก็พยายามหามาตรการป้องกันและปราบปรามการกระทำความผิดที่เกิดขึ้น แต่การบังคับใช้กฎหมายที่มีอยู่ในปัจจุบันมักไม่มีประสิทธิภาพ และสำหรับอาชญากรรมคอมพิวเตอร์ที่มีการกระทำความผิดที่มิใช่เกิดขึ้นแต่เพียงประเทศใดประเทศหนึ่ง แต่มีลักษณะเป็นอาชญากรรมข้ามชาติ จึงเกิดปัญหาความร่วมมือระหว่างประเทศ มาตรการในการแก้ไขปัญหาระหว่างประเทศในปัจจุบันอยู่ในรูปของความร่วมมือระหว่างประเทศ เพื่อลดช่องว่างที่มีอยู่ให้ลดน้อยลง หรือจัดให้มีความร่วมมือในลักษณะขององค์กรต่อองค์กร หรือประเทศต่อประเทศเพื่อช่วยเหลือซึ่งกันและกันในด้านการสืบสวนสอบสวน

4.1 มาตรการทางกฎหมายในการรับฟังเป็นพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในปัจจุบัน

เมื่อมีการกระทำความผิดเกี่ยวกับข้อมูลส่วนบุคคลที่เก็บอยู่ในเครื่องคอมพิวเตอร์เกิดขึ้น การกระทำดังกล่าวนอกจากจะเป็นอาชญากรรมคอมพิวเตอร์แล้ว การเข้าถึงข้อมูลในคอมพิวเตอร์โดยปราศจากอำนาจตามกฎหมายไทยถือเป็นการกระทำที่มิชอบก่อให้เกิดประเด็น

---

[1] พินัย ณ นคร. (2543, มิถุนายน). “กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์.” **บทบัณฑิตย์, 56, 2**. หน้า 1.

ปัญหา ดังนี้

4.1.1 การรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

4.1.1.1 ประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายวิธีพิจารณาความอาญา หมายถึง กฎหมายที่ว่าด้วยหลักเกณฑ์และวิธีการค้นหาความจริง อันเกี่ยวกับการกระทำความผิด และนำตัวผู้กระทำความผิดต่อกฎหมายอาญามาดำเนินการพิจารณา และลงโทษตามบทบัญญัติของกฎหมาย[2] แม้การกระทำความผิดอาญาจะเป็นการกระทำที่กระทบกระเทือนต่อสังคมโดยรวมก็ตาม แต่การดำเนินคดีอาญาก็ย่อมมีผลกระทบต่อสิทธิและเสรีภาพส่วนบุคคลโดยง่ายด้วย จึงต้องคำนึงถึงกฎหมายวิธีพิจารณาความอาญาที่ให้ความคุ้มครองสิทธิและเสรีภาพส่วนบุคคลในฐานะที่เขาเป็นส่วนหนึ่งของสังคม[3]

ในคดีอาญาพยานหลักฐานทุกชนิดรับฟังได้ ยกเว้นพยานหลักฐานที่ได้มาโดยมิชอบตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 สำหรับข้อมูลอิเล็กทรอนิกส์ ที่ได้มาจากการค้นที่มีหมายพยานหลักฐานดังกล่าวย่อมรับฟังได้ แต่ถ้าหากเป็นการค้นที่ไม่มีหมายพยานหลักฐานที่ได้ก็ไม่สามารถรับฟังได้ เพราะการจะเชื่อถือพยานหลักฐานนั้นเพียงใด ก็ขึ้นอยู่กับการชั่งน้ำหนักพยานหลักฐาน โดยกฎหมายได้วางหลักการชั่งน้ำหนักพยานหลักฐานเอาไว้ในมาตรา 227 คือ หลักพิสูจน์จนสิ้นสงสัย (in dubio pro reo) และได้บัญญัติรับรองไว้ในรัฐธรรมนูญ มาตรา 33 วรรคหนึ่ง ให้สันนิษฐานไว้ก่อนว่าผู้ต้องหาหรือจำเลยไม่มีความผิด โดยความสงสัยนั้นจะต้องเป็นความสงสัยในข้อเท็จจริง ไม่ใช่ความสงสัยในข้อกฎหมาย[4]

สำหรับประเทศไทยมีการให้หลักประกัน โดยบัญญัติรับรองไว้ในรัฐธรรมนูญ ในการให้ความคุ้มครองสิทธิและเสรีภาพเป็นหลัก รัฐจะใช้อำนาจล่วงละเมิดสิทธิเสรีภาพของประชาชนได้เป็นข้อยกเว้นในกรณีที่มีกฎหมายให้อำนาจ และมีเจ้าหน้าที่ของรัฐโดยชัดแจ้ง จะต้องมีกระบวนการควบคุมที่แน่ชัดสามารถตรวจสอบได้ ดังนั้นแม้อาชญากรรมที่เกิดขึ้นในปัจจุบันจะมีความร้ายแรงมาก จำเป็นจะต้องมีวิธีการในการแสวงหาพยานหลักฐานรูปแบบใหม่ๆ ซึ่งเป็นการใช้อำนาจในการปราบปรามอาชญากรรมของเจ้าหน้าที่ของรัฐ ก็ยังคงต้องคำนึงถึงหลักเกณฑ์นี้

การตรวจสอบเพื่อค้นหาข้อมูลในระบบอินเตอร์เน็ตหรือข้อมูลคอมพิวเตอร์นั้นก็เป็นกรณีที่มีความจำเป็นต้องมีหลักเกณฑ์ทางกฎหมายที่เพิ่มจากประมวลกฎหมายวิธีพิจารณาความ

---

[2] ณรงค์ ใจหาญ. (2543). **หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1** (พิมพ์ครั้งที่ 5). หน้า 22.

[3] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. (2539, มกราคม-มีนาคม). "แถลงการณ์เรื่อง การดักฟังทางโทรศัพท์." **รพีสาร, 14, 4**. หน้า 34.

[4] คณิต ณ นคร. เล่มเดิม. หน้า 56.

อาญากำหนดไว้ ซึ่งปัจจุบันยังไม่มีบัญญัติไว้ว่าควรดำเนินการอย่างไร นอกจากมีกำหนดไว้ในกฎหมายพิเศษบางฉบับ เช่นพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542

4.1.1.2 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 การฟอกเงิน (Money Laundering) คือการนำเงินหรือทรัพย์สินที่ได้มาจากการกระทำความผิดหรือได้มาโดยไม่ชอบด้วยกฎหมายมาเปลี่ยนสภาพเป็นเงินหรือทรัพย์สินที่ได้มาอย่างถูกต้อง เป็นการทำเงินสกปรกให้เป็นเงินสะอาด[5] เช่น เอาเงินที่ผิดกฎหมายไปลงทุนทำธุรกิจที่ถูกกฎหมาย โอนเงินออกนอกประเทศ เปิดบัญชีโดยใช้ชื่อปลอม ฯลฯ ไม่ว่าจะเป็นรูปแบบใดการกระทำดังกล่าวก็เพื่อที่จะปกปิดแหล่งที่มา และซุกซ่อนทรัพย์สิน รวมทั้งปกปิดผู้เป็นเจ้าของที่แท้จริง เพื่อทำให้ดูเสมือนว่าเป็นเงินหรือทรัพย์สินที่ถูกต้องตามกฎหมาย

ขั้นตอนของการฟอกเงินไม่ว่าจะเป็นการกระทำรูปแบบใดย่อมเหมือนกัน นั่นคือ ต้องมีการยักย้ายเงินหรือทรัพย์สิน ทำการปกปิดร่องรอยของเงินหรือทรัพย์สินดังกล่าวและนำเงินหรือทรัพย์สินนั้นกลับมาให้เสมือนเป็นเงินหรือทรัพย์สินที่ถูกต้องตามกฎหมาย

เนื่องจากปัจจุบันอาชญากรซึ่งกระทำความผิดกฎหมายบางประเภทได้นำเงินหรือทรัพย์สินที่เกี่ยวกับการกระทำความผิดนั้นมากระทำการในรูปแบบต่างๆ อันเป็นการฟอกเงิน เพื่อนำเงินหรือทรัพย์สินนั้นไปใช้ในการกระทำความผิดต่อไปอีก ทำให้ยากต่อการปราบปรามการกระทำความผิดกฎหมายเหล่านั้น และกฎหมายที่มีอยู่ก็ไม่สามารถปราบปรามการฟอกเงินหรือดำเนินการกับเงินหรือทรัพย์สินนั้นได้เท่าที่ควร ดังนั้นเพื่อเป็นการป้องกันและปราบปรามอาชญากรรม สมควรกำหนดมาตรการต่างๆ ให้สามารถดำเนินการป้องกันและปราบปรามการฟอกเงินให้ได้อย่างมีประสิทธิภาพ

หลักสากลที่นานาประเทศต่างถือเป็นหลักเกี่ยวกับกฎหมายฟอกเงิน ได้แก่ ให้ถือว่ากฎหมายฟอกเงินเป็นความผิดอาญา ที่มีการลงโทษทางอาญาและในขณะเดียวกันก็ให้มีโทษริบทรัพย์ในทางแพ่งด้วย มีวิธีการสืบสวนพิเศษโดยให้สถาบันการเงินจัดให้ลูกค้าแสดงตน ตรวจสอบกิจการของลูกค้า เก็บบันทึกข้อมูล และให้รายงานกิจการที่น่าสงสัยว่าจะเป็นการฟอกเงิน[6] นั่นคือ ธนาคารหรือสถาบันการเงินต้องจัดตั้งระบบการตรวจค้นหาข้อมูลของลูกค้าที่มีเหตุอันควรสงสัย และให้รายงานเหตุอันควรสงสัยนั้นให้เจ้าพนักงานผู้มีอำนาจหน้าที่ทราบ โดยไม่มีความผิดเรื่องเปิดเผยความลับของลูกค้าซึ่งจะเห็นได้ว่าเป็นมาตรการที่สำคัญมากในประเทศสหรัฐอเมริกา[7]

---

[5] สหัส สิงหวิริยะ. (2547). **คำอธิบายพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542** (พิมพ์ครั้งที่ 2). หน้า 3.

[6] สหัส สิงหวิริยะ. เล่มเดิม. หน้า 4.

[7] วาทิน คำทรงศรี. (2539). **การฟอกเงิน**. หน้า 102.

สำหรับกฎหมายไทยตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงินฯ มาตรา 46 ในกรณีที่มีเหตุอันควรเชื่อได้ว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อใช้ประโยชน์ในการกระทำความผิดฐานฟอกเงิน พนักงงานเจ้าหน้าที่ซึ่งเลขาธิการมอบหมายเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลแพ่งเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชี ข้อมูลทางการสื่อสาร เช่น การดักฟังโทรศัพท์ หรือข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็ได้ [8] นั่นคือต้องมีคำสั่งอนุญาตจากศาลแพ่งเสียก่อน จึงจะกระทำการตามมาตรา 46 นี้ได้

ในกรณีตามวรรคหนึ่ง ศาลจะสั่งอนุญาตให้พนักงานเจ้าหน้าที่ผู้ยื่นคำขอดำเนินการโดยใช้เครื่องมือหรืออุปกรณ์ใดๆ ตามที่เห็นสมควรก็ได้ แต่อนุญาตได้ไม่เกิดคราวละ 90 วัน [9]

เมื่อพิจารณาการกระทำความผิดมูลฐานตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542มาตรา 3 (1) ความผิดเกี่ยวกับยาเสพติด[10] ประกอบกับ พระราชบัญญัติมาตรการในการปราบปรามผู้กระทำผิดเกี่ยวกับยาเสพติด พ.ศ. 2534 คำว่า "มีเหตุอันควรสงสัย" ตามกฎหมายดังกล่าวมีขอเขตที่กว้างมาก โดยเริ่มต้นจากมีสิ่งบอกเหตุอย่างใดก็ได้ ไม่ว่าจะเป็นปรากฏการณ์หรือพฤติกรรมใดๆ ก็ได้ จนถึงเหตุที่มีพยานหลักฐานเพียงพอที่จะนำตัวจับกุมไปดำเนินคดี ส่งฟ้องและขอให้ศาลลงโทษ[11] จะเห็นได้ว่าข้อสันนิษฐานดังกล่าวเป็นข้อสันนิษฐานที่เอื้ออำนวยต่อการปฏิบัติหน้าที่ของเจ้าพนักงาน ดังนั้น เหตุอันควรสงสัยจึงไม่ควรเป็นปรากฏการณ์หรือพฤติกรรมใดๆ ก็ได้ แต่ควรจะเป็นปรากฏการณ์หรือพฤติกรรมที่อยู่ในวิสัยของปุถุชนที่สามารถคิดพิจารณาตามสามัญสำนึกว่าการจะเป็นเช่นนั้นได้ เพียงแต่ไม่มีข้อมูลบ่งชี้ จึงยังเป็นที่สงสัย

4.1.2 ปัญหาการรับฟังเป็นพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในศาลไทย

4.1.2.1 สถานะของข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในศาลไทย สภาพปัญหาที่เกิดขึ้นในปัจจุบัน คือ การจะนำเสนอข้อมูลอิเล็กทรอนิกส์เสนอต่อศาล จะนำเสนอในรูปของพยานหลักฐานชนิดใด หากพิจารณาจากลักษณะของพยานหลักฐานต่างๆแล้ว ข้อมูลอิเล็กทรอนิกส์น่าจะมีลักษณะที่สอดคล้องกับพยานหลักฐาน 2 ประเภทได้แก่ พยานเอกสาร หรือพยานวัตถุ ซึ่ง

---

[8] ดู พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, มาตรา 46 วรรคแรก.

[9] ดู พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, มาตรา 46 วรรคสอง.

[10] ดู พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, มาตรา 3 (1).

[11] วาทิน คำทรงศรี . เล่มเดิม. หน้า 73.

จำเป็นที่จะต้องกำหนดลักษณะของข้อมูลอิเล็กทรอนิกส์ให้ชัดเจนว่าเป็นพยานหลักฐานชนิดใด เนื่องจากการนำสืบ และวัตถุประสงค์ในการเสนอพยานหลักฐานทั้ง 2 ชนิดนั้นแตกต่างกัน

(1) เป็นพยานเอกสาร หมายถึง ข้อความในเอกสารที่มีการอ้างความหมายของข้อความเป็นพยาน[12]

พยานเอกสาร หมายถึง สิ่งซึ่งมีการบันทึกตัวอักษร ตัวเลข รูปรอยหรือเครื่องหมายซึ่งสามารถแสดงข้อความหรือความหมายอย่างใดอย่างหนึ่งให้ศาลตรวจดูได้ สิ่งนั้นจะเป็นอะไรก็ได้ และจะบันทึกไว้โดยวิธีเขียนด้วยมือ พิมพ์ พิมพ์ดีด แกะสลัก ถักร้อยหรือวิธีอื่นใดก็ได้[13]

ประมวลกฎหมายวิธีพิจารณาความอาญาและประมวลกฎหมายวิธีพิจารณาความแพ่ง ไม่ได้บัญญัติความหมายของคำว่า "เอกสาร" หรือ "พยานเอกสาร" เอาไว้ แม้จะมีการกล่าวถึงพยานเอกสารเอาไว้หลายชนิดในประมวลกฎหมายทั้ง 2 ฉบับ เช่น เอกสารมหาชน เอกสารราชการ หรือเอกสารเอกชน ความหมายของคำว่า "เอกสาร" นั้น ปรากฏอยู่ในประมวลกฎหมายอาญามาตรา 1 (7) หมายความว่า "กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น"

จะเห็นได้ว่าพยานเอกสารนั้น ประกอบด้วยตัววัตถุที่รองรับข้อความ และข้อความซึ่งเกิดขึ้นจากตัวอักษร ตัวเลข ผัง หรือแผนแบบต่างๆ ไม่ว่าจะโดยการพิมพ์ ถ่ายภาพ หรือวิธีอื่น ลงบนตัววัตถุที่รองรับ

ปกติแล้วพยานเอกสารจึงเป็นการบันทึกข้อความไว้บนกระดาษ โดยสิ่งที่ถูกบันทึกนั้นจะต้องสามารถสื่อความหมาย หรือแสดงข้อเท็จจริงบางอย่างได้ แต่ในบางครั้งก็อาจจะบันทึกลงบนวัสดุอื่นที่ไม่ใช่กระดาษก็ได้ เช่น ผ้า กระดาน แผ่นไม้ แผ่นหิน โลหะ ฯลฯ เพราะสิ่งที่จะพิสูจน์ข้อเท็จจริงคือสิ่งที่บันทึกอยู่บนนั้นเท่านั้น

ดังนั้น ข้อมูลอิเล็กทรอนิกส์ ที่มีลักษณะเป็นพยานเอกสารเมื่ออยู่ในรูปของการพิมพ์ออกมา (Print out)เป็นข้อความที่สื่อได้ด้วยตัวอักษร ตัวเลข หรือแผนแบบต่างๆ บนกระดาษ

ปัญหาที่ต้องพิจารณาต่อมาคือ จะนำเสนอข้อมูลอิเล็กทรอนิกส์ในฐานะ "ต้นฉบับ" หรือ "สำเนา" เพราะสำหรับระบบกฎหมายของประเทศคอมมอนลอว์ ก็จะรับฟังแต่เฉพาะต้นฉบับ โดยถือว่าเป็นพยานหลักฐานที่ถูกต้อง แท้จริงและน่าเชื่อถือที่สุด และหากเป็นสำเนาก็จะถือเป็น

---

[12] เข็มชัย ชุติวงศ์. (2543). **คำอธิบายกฎหมายลักษณะพยาน** (พิมพ์ครั้งที่ 7). หน้า 8.

[13] โสภณ รัตนากร. (2547). **คำอธิบายพยาน** (พิมพ์ครั้งที่ 7). หน้า 22.

พยานบอกเล่า (Hearsay) และสำหรับประเทศไทย แม้ปัญหาดังกล่าวจะไม่มี แต่ก็มีปัญหาในกรณีของคดีแพ่งที่กฎหมายบัญญัติให้ต้องใช้ต้นฉบับในการพิสูจน์ข้อเท็จจริงเท่านั้น

ตามบทบัญญัติของกฎหมายในเรื่องของการทำนิติกรรมสัญญา กฎหมายบัญญัติให้ต้องทำเป็นหนังสือ หรือมีหลักฐานเป็นหนังสือลงลายมือชื่อของผู้ทำนิติกรรมนั้น มิฉะนั้นจะไม่มีผลบังคับกันในทางกฎหมาย แต่ความเจริญก้าวหน้าของเทคโนโลยีในปัจจุบันมีการนำสื่ออิเล็กทรอนิกส์มาใช้ในการทำนิติกรรมสัญญา ได้แก่ โทรเลข เทเล็กซ์ โทรสาร และอินเตอร์เน็ต เรียกว่า "ธุรกรรมทางอิเล็กทรอนิกส์" เป็นการทำนิติกรรมสัญญาในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ไม่ได้ทำลงบนกระดาษเช่นในสมัยก่อน จึงมีการบัญญัติ พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ขึ้นมาใช้บังคับในกรณีนี้โดยเฉพาะ แต่ก็ยังมิได้มีการแก้ปัญหาการรับรองพยานหลักฐานในรูปของข้อมูลอิเล็กทรอนิกส์ในคดีอาญา ว่าเป็นพยานเอกสารหรือไม่แต่อย่างใด

(2) เป็นพยานวัตถุ หมายถึง วัตถุสิ่งของที่คู่ความอ้างเป็นพยาน การอ้างสถานที่ให้ศาลตรวจก็อยู่ในความหมายของพยานวัตถุ[14]

พยานวัตถุ ได้แก่ วัตถุหรือสิ่งใดที่อาจพิสูจน์ความจริงต่อศาลได้ โดยการตรวจดู มิใช่โดยการอ่านหรือการพิจารณาข้อความที่บันทึกไว้[15]

เมื่อพิจารณาเปรียบเทียบกับลักษณะของพยานเอกสารแล้ว จะเห็นว่า เอกสารฉบับหนึ่งอาจเป็นพยานเอกสารหรือพยานวัตถุก็ได้ ขึ้นอยู่กับวัตถุประสงค์ในการอ้าง นั่นคือหากต้องการให้ศาลพิจารณาข้อความในเอกสารนั้นก็เป็นพยานเอกสาร แต่ถ้าเป็นการอ้างเพื่อให้ศาลพิจารณารูปลักษณะของพยานหลักฐานชิ้นนั้นก็เป็นพยานวัตถุ โดยทั่วไปแล้วพยานวัตถุจะมีความสำคัญในคดีอาญามากกว่าในคดีแพ่ง เพราะเป็นพยานที่ดีที่สุดในการพิสูจน์ข้อเท็จจริงบางประการที่เกิดขึ้น ได้แก่ ของกลางต่างๆ

ในความเป็นจริงสื่ออิเล็กทรอนิกส์ไม่จำกัดอยู่แต่เฉพาะคอมพิวเตอร์ แต่มีทั้งกล้องถ่ายภาพ กล้องถ่ายภาพยนตร์ เครื่องบันทึกเสียง ซึ่งต่างก็มีลักษณะเป็นพยานวัตถุ ข้อมูลอิเล็กทรอนิกส์เป็นข้อมูลที่เกิดจากการประมวลผลโดยเครื่องคอมพิวเตอร์ เป็นพยานหลักฐานประเภทหนึ่งเช่นกัน

ดังนั้นการจะพิจารณาว่าสื่ออิเล็กทรอนิกส์เป็นพยานเอกสารหรือพยานวัตถุ จำเป็นที่จะต้องคำนึงถึงวัตถุประสงค์ของการนำสืบพยานหลักฐานชิ้นนั้นว่าจะเป็นการนำสืบตัววัตถุหรือนำ

---

[14] เข็มชัย ชุติวงศ์. เล่มเดิม. หน้า 8.

[15] โสภณ รัตนากร. เล่มเดิม. หน้า 22.

DPU

สืบข้อความ เช่น ต้องการนำสืบข้อเท็จจริงจากข้อความในเอกสารที่ได้พิมพ์ออกมาจากเครื่องคอมพิวเตอร์ ก็เป็นการนำสืบพยานหลักฐานที่เป็นเอกสาร หรือการนำสืบแถบบันทึกเสียงเป็นพยานวัตถุ[16] ศาลฎีกาเคยมีคำพิพากษา แสดงให้เห็นว่าแถบบันทึกเสียงสามารถตรวจสอบได้ด้วยการฟัง เพราะการนำสืบพยานวัตถุเป็นการรับรู้ด้วยประสาทสัมผัส รูป รส กลิ่น เสียง[17]

4.1.2.2 การจำกัดสถานะของพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ปัญหาสถานะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ว่าจะเป็นพยานเอกสารหรือพยานวัตถุนั้น มิได้มีบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา ในขณะที่กฎหมายได้บัญญัติถึงรูปแบบบังคับของการนำพยานหลักฐานเข้าสู่การพิจารณา โดยเรียกว่าเป็น “การจำกัดพยานหลักฐาน” โดยจำกัดสถานะของพยานหลักฐาน และการกำหนดหลักเกณฑ์การรับฟังและการสืบการจำกัดสถานะของพยานหลักฐาน เป็นการกำหนดชนิดของพยานหลักฐานตามที่กฎหมายบัญญัติเอาไว้ ที่จะใช้รับฟังได้ในคดีอาญา สำหรับปัญหาสถานะของพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์นั้น ก็ยังคงเป็นปัญหาที่สรุปไม่ได้ระหว่างพยานเอกสาร กรณีที่ Printout ออกมาเป็นเอกสาร หรือเป็นพยานวัตถุ กรณีที่อยู่ในรูปของฮาร์ดดิสก์

แต่ไม่ว่าจะเป็นพยานเอกสารหรือพยานวัตถุ ต่างก็เป็นพยานหลักฐานที่กฎหมายบัญญัติให้รับฟังได้ในคดีอาญา จึงเห็นว่าไม่น่าจะมีปัญหาในข้อนี้

4.1.2.3 ปัญหาการรับฟังพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในชั้นศาล ดังได้กล่าวมาแล้วขั้นตอนในการค้น และยึดพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ นั้นต้องกระทำไปภายในขอบเขตที่มีกฎหมายให้อำนาจกระทำได้ เพราะในการดำเนินกระบวนการทางอาญาย่อมต้องก้าวล่วงสิทธิของบุคคลโดยไม่สามารถหลีกเลี่ยงได้ หากในขั้นตอนของการค้น และยึดพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ได้กระทำไปโดยมิชอบแล้วการรับฟังพยานหลักฐานดังกล่าวในศาลไทยก็อาจเกิดปัญหา โดยพิจารณาตามหลักกฎหมายต่อไปนี้

(1) หลักสันนิษฐานไว้ก่อนว่าเป็นผู้บริสุทธิ์ ในคดีอาญาให้สันนิษฐานไว้ก่อนว่าจำเลยหรือผู้ต้องหาไม่มีความผิด [18] โดยมีกฎหมายวิธีพิจารณาความอาญา มาตรา 227 วรรคสอง และรัฐธรรมนูญ มาตรา 33 วรรคหนึ่งที่บัญญัติรับรองหลักนี้ นั่นคือศาลจะต้องรับฟังพยานหลักฐานจนปราศจากความสงสัยอันควรว่าจำเลยได้กระทำผิดจริงจึงจะลงโทษจำเลย มิใช่จะยอมรับบังคับตาม

---

[16] คำพิพากษาฎีกาที่ 7155/2539 (ส่งเสริม) เล่ม 12. หน้า 176.

[17] โสภณ รัตนากร. เล่มเดิม. หน้า 449.

[18] คณิต ณ นคร. เล่มเดิม. หน้า 56.

พยานหลักฐานที่มีเหตุผลมากกว่าอย่างคดีแพ่งเท่านั้น ดังนั้นจึงเกิดหลักดังกล่าว และในกรณีสงสัยก็จะต้องยกประโยชน์แห่งความสงสัย (in dubio pro reo) ให้แก่จำเลย แต่ความสงสัยในที่นี้จำกัดเฉพาะความสงสัยในข้อเท็จจริงเท่านั้น จะไม่ใช้หลักนี้กับความสงสัยในข้อกฎหมาย

(2) หลักการไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ ในการรับฟังพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ไม่ว่าจะเป็นการรับฟังในรูปของพยานเอกสารหรือพยานวัตถุก็ตามรับฟังได้ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 และมีบทบัญญัติรับรองเอาไว้ในรัฐธรรมนูญ และต่างก็มีบทบัญญัติที่เหมือนกันคือยกเว้นไม่รับฟังกรณีที่เป็นพยานหลักฐานที่ได้มาโดยมิชอบ ซึ่งถือเป็นบทตัดพยานในกฎหมายไทย หมายความว่าพยานหลักฐานทุกชนิดที่จะรับฟังได้ จะต้องเป็นพยานหลักฐานที่ได้มาโดยชอบ

ดังนั้น พยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ที่จะใช้รับฟังได้ในศาล จึงต้องเป็นพยานหลักฐานที่ได้มาโดยชอบ ตามนัยของกฎหมาย นั่นคือ กรณีเป็นพยานหลักฐานที่ได้จากการค้นจะต้องมีหมายค้นโดยชอบเสียก่อน เจ้าพนักงานของรัฐจึงจะสามารถเข้าไปค้นข้อมูลอิเล็กทรอนิกส์นั้นๆมาใช้อ้างอิงเป็นพยานหลักฐานได้

(3) การกำหนดหลักเกณฑ์การรับฟังและการนำสืบ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 โดยหลักคือรับฟังพยานหลักฐานที่ได้มาโดยชอบ และยกเว้นไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ และกำหนดขอบเขตในการค้นหาความจริงในคดีอาญา ไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 231 ซึ่งเป็นการห้ามสืบพยานหลักฐานอันจะเป็นการเปิดเผยความลับ มาตรา 234 การให้การเป็นปฏิปักษ์ต่อตนเอง (Self incrimination) และมาตรา 132 การตรวจตัวผู้ต้องหาได้เมื่อเขายินยอม[19]

(4) หลักการพิสูจน์จนสิ้นสงสัย หลักประกันสิทธิของบุคคลตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ข้อ 11 (1) และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง ข้อ 14 (2) และรัฐธรรมนูญ มาตรา 33 การบัญญัติรับรองสถานะของบุคคลที่ยังไม่มีคำพิพากษาของศาลว่ามีความผิด ว่าจะต้องได้รับการปฏิบัติอย่างบุคคลธรรมดาทั่วไป จะปฏิบัติต่อเขาเสมือนกับเป็นผู้ที่กระทำความผิดแล้วมิได้ การจะเข้าค้นข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคล จึงต้องมีเหตุให้ทำการค้นได้ตามที่กฎหมายบัญญัติเอาไว้อย่างชัดเจน สำหรับประเทศไทยก็คือประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 69 เท่านั้น และผลจากหลักสันนิษฐานว่าเป็นผู้บริสุทธิ์จนกว่าศาลจะมีคำพิพากษา ทำให้ต้องมีการพิสูจน์การกระทำความผิดของผู้ถูกกล่าวหาจนสิ้นสงสัยตามมาตรา 227

---

[19] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 231 ,243 วรรคหนึ่ง และ 132

เนื่องจากการค้นข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคล เป็นการกระทำที่ละเมิดต่อสิทธิส่วนบุคคลอย่างร้ายแรง ทำให้ต้องมีเหตุที่กฎหมายบัญญัติเอาไว้อย่างชัดเจน ตามหลักการสันนิษฐานว่าเป็นผู้บริสุทธิ์จนกว่าศาลจะมีคำพิพากษาเสร็จเด็ดขาดว่ามีความผิด โดยจะต้องพิสูจน์จนสิ้นสงสัยโดยการชั่งน้ำหนักพยานหลักฐาน

ที่กล่าวมาล้วนเป็นหลักเกณฑ์การรับฟังและการสืบพยานหลักฐานโดยทั่วๆไปในคดีอาญา ซึ่งผู้เขียนเห็นว่าจะต้องนำมาเป็นหลักเกณฑ์ในการรับฟังและการสืบพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เช่นกัน

4.2 วิเคราะห์ปัญหาที่ไม่อาจคุ้มครองสิทธิในข้อมูลข่าวสารส่วนบุคคลได้อย่างชัดเจน

4.2.1 มาตรการทางกฎหมายในการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ แม้รัฐจะมีองค์กรหลายองค์กรในกระบวนการยุติธรรมที่มีหน้าที่ปราบปรามอาชญากรรม ซึ่งในบางประเทศให้ความสำคัญกับประสิทธิภาพของกระบวนการยุติธรรมที่มุ่งปราบปรามอาชญากรรมมากเกินไป จนทำให้หลักประกันสิทธิส่วนบุคคลน้อยลง แต่บางประเทศก็คำนึงถึงหลักประกันสิทธิส่วนบุคคลมากกว่าประสิทธิภาพของกระบวนการยุติธรรม โดยยอมสละความมีประสิทธิภาพของการปราบปรามอาชญากรรมบางประการไป เพื่อธำรงไว้ซึ่งสิทธิเสรีภาพส่วนบุคคล[20]

กฎหมายวิธีพิจารณาความอาญา หมายถึง กฎหมายที่ว่าด้วยหลักเกณฑ์และวิธีการค้นหาความจริง อันเกี่ยวกับการกระทำความผิดและนำตัวผู้กระทำความผิดต่อกฎหมายอาญามาดำเนินการพิจารณา และลงโทษตามบทบัญญัติของกฎหมาย[21] แม้การกระทำความผิดอาญาจะเป็นการกระทำที่กระทบกระเทือนต่อสังคมโดยรวมก็ตาม แต่การดำเนินคดีอาญาก็ย่อมมีผลกระทบต่อสิทธิและเสรีภาพส่วนบุคคลโดยง่ายด้วย จึงต้องคำนึงถึงกฎหมายวิธีพิจารณาความอาญาที่ให้ความคุ้มครองสิทธิและเสรีภาพส่วนบุคคลในฐานะที่เขาเป็นส่วนหนึ่งของสังคม[22]

สำหรับประเทศไทยมีการให้หลักประกัน โดยบัญญัติรับรองไว้ในรัฐธรรมนูญ ในการให้ความคุ้มครองสิทธิและเสรีภาพเป็นหลัก รัฐจะใช้อำนาจล่วงละเมิดสิทธิเสรีภาพของประชาชนได้เป็นข้อยกเว้นในกรณีที่มีกฎหมายให้อำนาจ และมีเจ้าหน้าที่ของรัฐโดยชัดแจ้ง จะต้องมีกระบวนการควบคุมที่แน่ชัดสามารถตรวจสอบได้ ดังนั้นแม้อาชญากรรมที่เกิดขึ้นในปัจจุบันจะมี

---

[20] ประธาน วัฒนวาณิชย์. (2520, พฤศจิกายน). "ระบบความยุติธรรมทางอาญา : แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม." **วารสารนิติศาสตร์ 9, 2**. หน้า 143.

[21] ณรงค์ ใจหาญ. เล่มเดิม. หน้า 22.

[22] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. แหล่งเดิม. หน้า 34.

ความร้ายแรงมาก จำเป็นจะต้องมีวิธีการในการแสวงหาพยานหลักฐานรูปแบบใหม่ๆ ซึ่งเป็นการใช้อำนาจในการปราบปรามอาชญากรรมของเจ้าหน้าที่ของรัฐ ก็ยังคงต้องคำนึงถึงหลักเกณฑ์นี้

4.2.2 ความจำเป็นในการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ปัจจุบันประเทศไทยยังไม่มีการวางหลักไว้ในกฎหมายส่วนสารบัญญัติสำหรับอาชญากรรมรูปแบบใหม่ๆ จึงต้องมีการแก้ไขปรับปรุงต่อไป เนื่องจากอาชญากรรมที่เกิดขึ้นในขณะนี้มีลักษณะที่แตกต่างไปจากอาชญากรรมพื้นฐาน หรืออาชญากรรมแบบดั้งเดิม เมื่อมีการกระทำความความผิดเกิดขึ้นแต่ยังไม่มีการบัญญัติกฎหมายเกี่ยวกับการกระทำความผิดดังกล่าวไว้โดยเฉพาะ เช่น อาชญากรรมเศรษฐกิจ ก็จำต้องใช้กฎหมายที่มีอยู่ลงโทษผู้กระทำความผิด ตามประมวลกฎหมายอาญาผู้กระทำความผิดก็อาจรับผิดแต่เพียงในฐานละเมิดต่อผู้เสียหายเท่านั้น แต่ความเสียหายที่เกิดอาจก่อให้เกิดความเสียหายต่อระบบเศรษฐกิจของประเทศ หรือในกรณีอาชญากรรมคอมพิวเตอร์ที่ผู้กระทำความผิดใช้เครื่องคอมพิวเตอร์ในการกระทำความผิด ก็เป็นเพียงการใช้คอมพิวเตอร์ในการกระทำความผิดเท่านั้น แต่การกระทำความเสียหายต่อข้อมูล ระบบโปรแกรม หรือชุดคำสั่ง ทำให้ผู้อื่นเสียหายก็ไม่สามารถนำมาปรับใช้ได้ เพราะอาจขัดกับหลัก “ไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย” อันเป็นหัวใจสำคัญของกฎหมายอาญา

ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานรูปแบบใหม่ที่กระการยุติธรรมจำเป็นต้องให้ความสนใจ เนื่องจากอาชญากรรมรูปแบบใหม่ๆ เช่น อาชญากรรมทางเศรษฐกิจ อาชญากรรมทางคอมพิวเตอร์ และอาชญากรรมบนเครือข่ายอินเตอร์เน็ต ฯลฯ ซึ่งอาชญากรรมเหล่านี้ถือเป็นอาชญากรรมที่มีลักษณะพิเศษ แตกต่างไปจากอาชญากรรมที่มีอยู่แต่เดิม จึงต้องให้ความสำคัญเพราะกฎหมายมักตามไม่เทคโนโลยีที่มีอยู่ ความล้ำหน้าของเทคโนโลยีแม้มีประโยชน์แต่ก็ก่อให้เกิดการกระทำความผิดที่ร้ายแรง เช่น อาชญากรรมทางเศรษฐกิจ ที่มีการแสดงออกไม่รุนแรงแต่กลับก่อให้เกิดความเสียหายในระดับประเทศ

พยานหลักฐานในคดีอาญามีความสำคัญมาก เพราะคดีอาญาต้องตัดสินด้วยพยานหลักฐานเสมอ[23] การแสวงหาพยานหลักฐานจึงมีความจำเป็น แต่พยานหลักฐานบางชนิด เช่น พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เป็นพยานหลักฐานที่ยากต่อการเข้าถึง และรวบรวม บางครั้งผลจากการแสวงหาพยานหลักฐานเหล่านี้อาจกระทบถึงสิทธิเสรีภาพของผู้อื่น ในคดีอาญาพยานหลักฐานทุกชนิดรับฟังได้ แต่ต้องเป็นไปตามหลักเกณฑ์ว่าด้วยการสืบและการรับฟัง[24] ดังนั้น

---

[23] คณิต ณ นคร. เล่มเดิม. หน้า 138.

[24] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา, มาตรา 226.

เจ้าพนักงานของรัฐจึงต้องตระหนักและระมัดระวังทุกขั้นตอนในการแสวงหาพยานหลักฐานว่าจะต้องเป็นไปตามหลักเกณฑ์ว่าด้วยการสืบ เพื่อที่จะรับฟังได้เป็นพยานหลักฐาน

DPU

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

จุดประสงค์ในการแสวงหาพยานหลักฐานในคดีอาญานั้นก็เพื่อจะพิสูจน์ให้ได้ความว่าจำเลยเป็นผู้กระทำความผิดตามที่ถูกฟ้องหรือไม่ มีการกระทำอย่างไร ในเวลาใด สถานที่ใด และมีใครเป็นผู้เกี่ยวข้องบ้าง ซึ่งเป็นหลักเกณฑ์เกี่ยวกับพยานหลักฐานในคดีอาญาที่มีมาแต่เดิม สำหรับอาชญากรรมคอมพิวเตอร์ซึ่งเป็นการกระทำความผิดที่เกิดขึ้นจากความเจริญก้าวหน้าของเทคโนโลยี ไม่ว่าจะเป็นการกระทำความผิดต่อข้อมูลในคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ ซึ่งเป็นสิ่งที่ไม่มีรูปร่าง แตกต่างจากการก่ออาชญากรรมรูปแบบดั้งเดิมที่เป็นการกระทำต่อสิ่งที่มีรูปร่าง การให้ความหมายของคำว่า “อาชญากรรมคอมพิวเตอร์” จึงเป็นการให้ความหมายที่สอดคล้องกับสิ่งที่ผู้ให้ความหมายศึกษาและประสงค์จะให้ความคุ้มครอง ทำให้ไม่มีความหมายที่เป็นสากล แต่ก็มีความเห็นตรงกันประการหนึ่งก็คืออาชญากรรมคอมพิวเตอร์ เป็นการกระทำความผิดที่เกี่ยวเนื่องกับคอมพิวเตอร์ไม่ว่าจะในทางใดก็ตาม

การกระทำความผิดที่เกิดจากอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้น ก่อให้เกิดปัญหากับระบบกฎหมายภายในของประเทศต่างๆทั่วโลก เนื่องจาก การแสวงหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ถือเป็นมาตรการสำคัญ เพราะลักษณะของข้อมูลอิเล็กทรอนิกส์มีลักษณะที่แตกต่างจากพยานหลักฐานทั่วๆไป ก่อให้เกิดปัญหาในการค้น การยึด สถานะในทางพยานหลักฐานและการรับฟังเป็นพยานหลักฐานในศาล ไม่มีกฎหมายใช้บังคับ และไม่มีกฎหมายให้อำนาจเจ้าหน้าที่ของรัฐในการแสวงหาพยานหลักฐานดังกล่าว

ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 34 ได้ให้การรับรองคุ้มครองสิทธิของบุคคลในความเป็นอยู่ส่วนตัว (Right to privacy) ซึ่งไม่ใช่สิทธิในการใช้ชีวิตส่วนตัวเท่านั้น แต่ยังรวมไปถึงสิทธิในข้อมูลข่าวสารส่วนบุคคลด้วย ไม่ว่าข้อมูลนั้นจะจัดเก็บไว้ที่ใด การจะเข้าสู่ข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ โดยหลักแล้วจึงไม่สามารถทำได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เพื่อรักษาความมั่นคงของรัฐ ความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน และการจะจำกัดสิทธิของบุคคลจะต้องทำไปเท่าที่จำเป็น ตามเงื่อนไขที่รัฐธรรมนูญ กำหนดไว้ในมาตรา 29 ด้วย

ในปัจจุบันกฎหมายได้ให้อำนาจเจ้าหน้าที่ของรัฐสามารถเข้าสู่ข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46 และพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม พ.ศ. 2544 มาตรา 14 จัตวา ที่มีบทบัญญัติไปในทำนองเดียวกัน โดยกฎหมายทั้งสองฉบับดังกล่าวได้จำกัดฐานความผิดไว้เฉพาะความผิดฐานฟอกเงิน และความผิดเกี่ยวกับยาเสพติดเท่านั้น ไม่ครอบคลุมไปถึงการกระทำความผิดประเภทอื่นด้วย ดังนั้นการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลโดยประการอื่นนอกจากที่กล่าวมาแล้ว จึงเป็นการกระทำที่มิชอบด้วยกฎหมาย พยานหลักฐานที่ได้มาก็ถือเป็นพยานหลักฐานที่ได้มาโดยมิชอบ และไม่สามารถรับฟังได้ในศาล แต่รูปแบบการประกอบอาชญากรรมในปัจจุบันมีการพัฒนาไปมาก ไม่จำกัดอยู่แต่เฉพาะความผิดฐานฟอกเงิน หรือความผิดเกี่ยวกับยาเสพติด เช่น อาชญากรรมคอมพิวเตอร์ อาชญากรรมทางการเมือง หรือองค์กรอาชญากรรม ฯลฯ ซึ่งการกระทำความผิดดังกล่าวนั้นยากที่จะแสวงหาพยานหลักฐานมาเอาผิดกับผู้กระทำผิดได้ การเข้าสู่ข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ถือเป็นมาตรการพิเศษที่รัฐสามารถจะนำมาใช้แก้ปัญหาในการแสวงหาพยานหลักฐานได้เป็นอย่างดี แต่ก็จะต้องกระทำไปภายในขอบเขตที่รัฐธรรมนูญบัญญัติรับรองให้กระทำได้

เพื่อแก้ปัญหาการแสวงหาพยานหลักฐาน และการให้ความคุ้มครองข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคลในอาชญากรรมคอมพิวเตอร์ ในประเทศต่างๆ เช่น สหรัฐอเมริกา อังกฤษ และญี่ปุ่น ฯลฯ ได้มีการบัญญัติกฎหมายขึ้นมาใหม่ หรือแก้ไขปรับปรุงกฎหมายที่ใช้บังคับอยู่เพื่อแก้ปัญหาดังกล่าว

สำหรับประเทศไทยปัจจุบันยังไม่มีบทบัญญัติในประมวลกฎหมายอาญาให้ดำเนินคดีกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในรูปแบบต่างๆได้ และมาตรการในการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาก็ยังไม่มีบทบัญญัติเอาไว้ มีแต่เพียงกฎหมายพิเศษบางฉบับที่บัญญัติเอาไว้ แต่ก็จำกัดเฉพาะความผิดบางฐานเท่านั้น ไม่ครอบคลุมถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฐานอื่นๆ ด้วย ซึ่งจำเป็นที่จะต้องแก้ปัญหาทั้งการแสวงหาพยานหลักฐาน และการให้ความคุ้มครองข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคลในอาชญากรรมคอมพิวเตอร์ ไม่ว่าจะเป็นการบัญญัติกฎหมายขึ้นใหม่หรือแก้ไขปรับปรุงกฎหมายที่ใช้บังคับอยู่เพื่อแก้ปัญหาดังกล่าวดังเช่นในต่างประเทศ

5.2 ข้อเสนอแนะ

เนื่องจากการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ เป็นการกระทำที่ละเมิดสิทธิและเสรีภาพส่วนบุคคลอย่างร้ายแรง จึงจำเป็นที่จะต้องมีมาตรการที่ชัดเจน

โดยกฎหมายจะต้องบัญญัติประเภทของความผิด ที่จำเป็นจะต้องใช้วิธีการนี้ในการแสวงหาพยานหลักฐาน โดยเฉพาะอาชญากรรมคอมพิวเตอร์ เป็นการให้อำนาจเจ้าหน้าที่ในการรวบรวมพยานหลักฐาน และอำนาจที่ให้แก่เจ้าพนักงานสอบสวน เช่น อำนาจในการเชื่อมต่อเข้าไปในเครือข่ายอินเตอร์เน็ตไม่ว่าในกรณีใด เพื่อตรวจสอบเครื่องมือ อุปกรณ์ หรือเครื่องคอมพิวเตอร์ ซึ่งมีเหตุอันควรสงสัยว่าเกี่ยวข้องกับการกระทำความผิดอาชญากรรมคอมพิวเตอร์ ทั้งยังมีอำนาจมอบหมายให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์เหล่านั้น เพื่อช่วยเหลือได้ตามสมควร นั่นคือเจ้าหน้าที่ของรัฐจำเป็นที่จะต้องมีความรู้ในเรื่องคอมพิวเตอร์ดีพอที่จะดำเนินงานได้ และควรจะมีองค์กรกลางที่เป็นอิสระจากพนักงานสอบสวนเป็นผู้ทำหน้าที่ในการรวบรวมพยานหลักฐานประเภทนี้ เพื่อป้องกันการใช้อำนาจในทางมิชอบ

จากลักษณะของข้อมูลอิเล็กทรอนิกส์ ที่แตกต่างจากพยานหลักฐานชนิดอื่นๆ และสามารถเทียบเคียงได้กับพยานเอกสาร และพยานวัตถุ ซึ่งก่อให้เกิดปัญหาการจำแนกสถานะของพยานหลักฐานชนิดนี้ จนนำไปสู่ปัญหาในการนำเสนอต่อศาล จึงควรวางหลักกฎหมายกำหนดสถานะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ให้ชัดเจนว่าเป็นพยานหลักฐานชนิดใด และจะนำเสนอต่อศาลด้วยวิธีการใด โดยการกำหนดสถานะที่ชัดเจนของข้อมูลอิเล็กทรอนิกส์ให้ชัดเจนก็จะทำให้เข้าใจได้ว่าข้อมูลอิเล็กทรอนิกส์ เป็นวัตถุใดที่พนักงานสอบสวนจะทำการค้นได้ เพราะในการออกหมายอาญาไม่ว่าจะเป็นหมายค้น หรือยึดก็ตาม จำเป็นจะต้องมีการระบุสถานที่ค้น และวัตถุที่ค้นเอาไว้

สำหรับหมายอาญาก็จะต้องระบุเหตุในการค้น และยึด ควรวางหลักกฎหมายให้ชัดเจนโดยจะต้องไม่คลุมเครือ เช่นหมายค้นฮาร์ดแวร์ ซอฟท์แวร์ หรือข้อมูล โดยจะต้องระบุวิธีการ และระยะเวลาในการค้นให้ชัดเจนไม่มากไม่น้อยจนเกินไป รวมทั้งให้อำนาจเจ้าพนักงานสอบสวนทำการกักข้อมูลที่ค้นได้เพื่อใช้ประโยชน์ในการสอบสวนต่อไป ไม่ว่ากรณีใดการค้นข้อมูลอิเล็กทรอนิกส์ก็จะต้องมีหมายค้น แต่เพราะลักษณะของข้อมูลอิเล็กทรอนิกส์ เป็นพยานหลักฐานที่แก้ไขเปลี่ยนแปลงได้ง่าย ดังนั้นจึงควรมีมาตรการทางกฎหมายให้อำนาจเจ้าพนักงาน หรือมีอำนาจมอบหมายให้ผู้เชี่ยวชาญทำการเก็บกู้พยานหลักฐานที่ถูกทำลาย แก้ไขหรือเปลี่ยนแปลงไปให้กลับคืนมา โดยจะต้องวางหลักเกณฑ์ในการกู้ข้อมูลดังกล่าวให้ชัดเจน

ประเทศต่างๆต้องตระหนักถึงปัญหาอาชญากรรมคอมพิวเตอร์ว่าไม่ใช่ปัญหาของประเทศใดประเทศหนึ่ง แต่เป็นปัญหาระหว่างประเทศจึงควรให้ความร่วมมือกับประเทศต่างๆ หรือองค์การระหว่างประเทศในการหามาตรการแก้ไขปัญหา การวางหลักกฎหมายและการรวบรวมพยานหลักฐาน บัญญัติเป็นแนวทางไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา หรือบัญญัติกฎหมายพิเศษขึ้นมาใช้บังคับเป็นการเฉพาะ

ที่สำคัญต้องให้ความรู้แก่ประชาชนถึงปัญหาอาชญากรรมคอมพิวเตอร์ เพื่อให้เกิดความเข้าใจ และใช้คอมพิวเตอร์ได้อย่างถูกต้องและระมัดระวัง ทั้งคอยเป็นหูเป็นตาให้กับทางราชการในการค้นหาผู้กระทำความผิด

DPU

บรรณานุกรม

DPU

บรรณานุกรม

ภาษาไทย

หนังสือ

กุลพล พลวัน. (2538). **พัฒนาการสิทธิมนุษยชน** (พิมพ์ครั้งที่ 6). กรุงเทพฯ : วิญญูชน.

เกียรติขจร วัจนะสวัสดิ์. (2542). **คำอธิบายกฎหมายอาญา ภาค 1** . กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

เกียรติขจร วัจนะสวัสดิ์. (2547). **คำอธิบายหลักกฎหมายวิธีพิจารณาความอาญาว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณาพร้อมด้วยตัวบทและคำอธิบายมาตราที่แก้ไขเพิ่มเติมใหม่** (พิมพ์ครั้งที่ 3 แก้ไขใหม่). กรุงเทพฯ : หจก.จิรรัชการพิมพ์.

เข็มชัย ชุติวงศ์. (2543). **คำอธิบายกฎหมายลักษณะพยาน** (พิมพ์ครั้งที่ 7 ปรับปรุงใหม่). กรุงเทพฯ : นิติบรรณาการ.

คณิต ณ นคร. (2543). **กฎหมายอาญาภาคความผิด** (พิมพ์ครั้งที่ 7). กรุงเทพฯ : มหาวิทยาลัยธรรมศาสตร์.

คณิต ณ นคร. (2546). **กฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม-ปรับปรุงใหม่). กรุงเทพฯ : วิญญูชน.

คนึง ฤาไชย. (2530). **กฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 5). กรุงเทพฯ : มหาวิทยาลัยธรรมศาสตร์.

จีรนิติ หะวานนท์. (2544). **สิทธิทางวิธีพิจารณาความอาญาตามรัฐธรรมนูญ** (พิมพ์ครั้งที่ 2 ปรับปรุงใหม่). กรุงเทพฯ : วิญญูชน.

จิตติ ติงศภัทิย์. (2525). **กฎหมายอาญา ภาค 1**. กรุงเทพฯ : สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตสภา.

ณรงค์ ใจหาญ. (2547). **หลักกฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 7 ปรับปรุงใหม่). กรุงเทพฯ : วิญญูชน.

ทวีเกียรติ มีนะกนิษฐ์. (2543). **กฎหมายอาญา : หลักและปัญหา** (พิมพ์ครั้งที่ 2). กรุงเทพฯ : นิติธรรม.

บรรเจิด สิงคะเนติ. (2543). **หลักพื้นฐานของสิทธิเสรีภาพ และศักดิ์ศรีความเป็นมนุษย์ตามรัฐธรรมนูญ พ.ศ.2540**. กรุงเทพฯ : วิญญูชน.

ปีเตอร์ ที. เดวิส และแบรี่ ดี. เลวิส. (2543). **แรกเริ่มเรียนรู้ เรื่องรักษาความปลอดภัยให้ระบบคอมพิวเตอร์**. แปลจาก Computer Security Dummies โดย เจนศักดิ์ ตั้งพันธ์สุริยะ. กรุงเทพฯ : บริษัท ซีเอ็ดยูเคชั่น จำกัด.

วัชราภรณ์ สุริยาภิวัฒน์. (2543). **คอมพิวเตอร์เบื้องต้นและเทคนิคการเขียนโปรแกรม**. กรุงเทพฯ : ห้างหุ้นส่วนจำกัด ไทยเจริญการพิมพ์.

วาทิน คำทรงศรี. (2539). **การฟอกเงิน**. กรุงเทพฯ : วิญญูชน.

วรพจน์ วิศรุตพิชญ์. (2538). **สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540**. กรุงเทพฯ : วิญญูชน.

วีระ โลจายะ. (2524). **กฎหมายสิทธิมนุษยชน**. กรุงเทพฯ : มหาวิทยาลัยรามคำแหง.

สหัส สิงหวิริยะ. (2547). **คำอธิบายพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542** (พิมพ์ครั้งที่ 2). กรุงเทพฯ : นิติธรรม.

แสวง บุญเฉลิมวิภาส. (2542). **หลักกฎหมายอาญา** (พิพม์ครั้งที่ 2). กรุงเทพฯ : โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลักธรรมศาสตร์.

หยุด แสงอุทัย. (2523). **กฎหมายอาญาภาค 1** (พิพม์ครั้งที่ 14). กรุงเทพฯ : สำนักพิมพ์หาวิทยาลัยธรรมศาสตร์.

หฤทัย หงส์สิริ และมานิตย์ จุมปา. (2542). **คำอธิบายข้อมูลข่าวสารของทางราชการ**. กรุงเทพฯ : นิติธรรม.

อุดม รัฐอมฤต นพนิธิ สุริยะ และบรรเจิด สิงคะเนติ. (2544). **การอ้างศักดิ์ศรีความเป็นมนุษย์หรือใช้สิทธิและเสรีภาพของบุคคลดังกล่าวตามมาตรา 28 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2540**. กรุงเทพฯ : สำนักงานศาลรัฐธรรมนูญ.

บทความ

"การสัมนนาทางวิชาการเรื่อง ศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของบุคคลตามรัฐธรรมนูญ." **วารสารศาลรัฐธรรมนูญ, 1,3.** (2542, กันยายน-ธันวาคม). หน้า 37-48.

กุลพล พลวัน. (2540, มิถุนายน). "กลไกตามรัฐธรรมนูญในการคุ้มครองสิทธิและเสรีภาพของประชาชน." **บทบัณฑิตย์, 52, 2.** หน้า 36-52.

จิรนิติ หะวานนท์. (2527, พฤษภาคม-มิถุนายน). "หลักการไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ : เปรียบเทียบระหว่างกฎหมาย อเมริกา และกฎหมายเยอรมัน." **ดุลพาห, 31, 3.** หน้า 34-52.

นิติ ผดุงชัย. (2532,มิถุนายน). “กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับ Computer.” **วารสารอัยการ**, หน้า 86-88.

ณรงค์ ใจหาญ. (2540, มิถุนายน). “หลักประกันสิทธิของประชาชนในคดีอาญาใหม่ : ปัจจุบันและทศวรรษหน้า 2540-2550.” **บทบัณฑิตย์, 53, 2.** หน้า 64-86.

ประธาน วัฒนวาณิชย์. (2520, พฤศจิกายน). “ระบบความยุติธรรมทางอาญา : แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม.” **วารสารนิติศาสตร์, 9,2**. หน้า 143-156.

สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. (2539, มกราคม-มีนาคม). ”แถลงการณ์เรื่อง การดักฟังทางโทรศัพท์.” **รพีสาร, 14, 4.** หน้า 34- 54.

วิทยานิพนธ์

กิตติพันธุ์ เกียรติสุนทร. (2538). **มาตรการทางอาญาในการคุ้มครองข้อมูลส่วนบุคคล**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

กิตติมา ประคุณคดี. (2533). **การดักฟังทางโทรศัพท์โดยเจ้าพนักงาน**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

กงจักร โพธิ์พร้อม. (2529). **ปัญหากฎหมายมหาชนบางประการเกี่ยวด้วยการควบคุมการใช้ข่าวสารโดยเครื่องคอมพิวเตอร์**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

จงรัก จุทานนท์. (2524). **การคุ้มครองสิทธิของประชาชนต่อการถูกจับและตรวจค้นที่ไม่ชอบธรรม**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

ศุภฤกษ์ ศุกรเสพย์. (2545). **การค้นในที่รโหฐานของเจ้าพนักงานป้องกันและปราบปรามยาเสพติด**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

สุชาติ ตระกูลเกษมสุข. (2543). **การคุ้มครองสิทธิส่วนบุคคลจากการดักฟังทางโทรศัพท์**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

DPU

ภาษาต่างประเทศ

BOOKS

Dando, Shigemitsu. (1965). **Japanese Criminal Procedure**. South Hackensack,NJ: Fred Rothman & Co.

May, Richard. (1999). **Criminal Evidence**. London : Sweet & Maxwell Ltd.

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

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

DPU

การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจาก
ข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์

นารี กิตติสมบูรณ์สุข

DPU

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

สาขาวิชานิติศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์

พ.ศ. 2549

ISBN 974-671-367-1

Pursuing of electronic materials and personal data in computer crime

Naree Kittisomboonsuk

DPU

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Laws

Department of Law

Graduate School, Dhurakij Pundit University

2006

ISBN 974-671-367-1

หัวข้อวิทยานิพนธ์	การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์
ชื่อผู้เขียน	นารี กิตติสมบูรณ์สุข
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ดร. อุดม รัฐอมฤต
อาจารย์ที่ปรึกษาร่วม	ดร. อุทัย อาทิเวช
สาขาวิชา	นิติศาสตร์
ปีการศึกษา	2548

บทคัดย่อ

อาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมที่ร้ายแรงเป็นภัยต่อสังคมรูปแบบหนึ่ง ที่ก่อให้เกิดความเสียหายแก่ระบบเศรษฐกิจเป็นอย่างมาก แทบทุกประเทศต่างก็เล็งเห็นถึงอันตรายจากอาชญากรรมประเภทนี้ และผลกระทบที่เกิดกับกฎหมายอาญาของประเทศต่างๆ ทั่วโลก เนื่องจากกฎหมายอาญาที่ใช้อยู่ไม่เพียงพอที่จะดำเนินคดีกับอาชญากรได้ จึงพยายามหามาตรการทางกฎหมายใหม่ๆ เพื่อค้นหาวิธีการป้องกันและปราบปราม สำหรับประเทศไทยเป็นประเทศหนึ่งที่เห็นความสำคัญของปัญหาดังกล่าวจึงมีการร่างกฎหมายอาชญากรรมคอมพิวเตอร์ขึ้นเป็นกฎหมายเฉพาะ อย่างไรก็ตามสิ่งที่ควรคำนึงถึงควบคู่ไปกันไปคือการมีกฎหมายบังคับใช้ กล่าวคือต้องมีการปรับปรุงกฎหมายวิธีสบัญญัติให้มีประสิทธิภาพด้วย โดยเฉพาะปัญหาการรวบรวมพยานหลักฐานและการรับฟังพยานหลักฐานคอมพิวเตอร์ที่เป็นข้อมูลส่วนบุคคล

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 29 ได้บัญญัติรับรองสิทธิและเสรีภาพของประชาชนไว้เป็นหลักพื้นฐาน ซึ่งในทางปฏิบัติรัฐสามารถบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ในบางกรณี ดังนั้นจึงมีบทบัญญัติที่ให้อำนาจรัฐตรากฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ภายในขอบเขตที่รัฐธรรมนูญกำหนด เช่น ในมาตรา 37 บัญญัติรับรองคุ้มครองสิทธิความเป็นอยู่ส่วนตัวของบุคคล ซึ่งเป็นสิทธิส่วนบุคคล และรัฐธรรมนูญก็มีบทบัญญัติให้อำนาจรัฐกระทำการใดๆ ก็ได้หากเป็นกรณีที่กระทำไปเพื่อประโยชน์สาธารณะ ดังนั้นรัฐอาจอาศัยข้อยกเว้นดังกล่าวบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคลเกินความจำเป็น หรือตามอำเภอใจ โดยอ้าง “ประโยชน์สาธารณะ” เช่น รัฐอาจบัญญัติกฎหมายอนุญาตให้เจ้าหน้าที่ของรัฐเข้าตรวจสอบข้อมูลส่วนบุคคลของบุคคลใดบุคคลหนึ่งได้ตลอดเวลา ตามแต่จะเป็นสมควรโดยเฉพาะข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บอยู่

ในเครื่องคอมพิวเตอร์ เป็นต้น การกระทำดังกล่าวถือเป็นการกระทำที่กระทบกระเทือนต่อสาระสำคัญแห่งสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล ซึ่งจะมีผลตามบทบัญญัติในมาตรา 6 ที่ถือว่าบทบัญญัติดังกล่าวขัดหรือแย้งกับรัฐธรรมนูญซึ่งถือเป็นกฎหมายสูงสุดของประเทศ ทำให้บทบัญญัติดังกล่าวไม่สามารถใช้บังคับได้ ทั้งๆที่ การเข้าสู่ข้อมูลส่วนบุคคลนี้ เป็นมาตรการใหม่ที่รัฐสามารถนำมาใช้แสวงหาพยานหลักฐานเพื่อมาดำเนินคดีกับอาชญากรที่ก่ออาชญากรรมที่การแสวงหาพยานหลักฐานรูปแบบดั้งเดิมไม่สามารถแก้ปัญหาได้ เช่น อาชญากรรมคอมพิวเตอร์ ดังนั้น จึงควรมีการบัญญัติกฎหมายขึ้นมาให้อำนาจ และควบคุมการใช้อำนาจของเจ้าหน้าที่ของรัฐในการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลได้ ภายในขอบเขตที่ไม่เป็นการกระทบกระเทือนต่อสาระสำคัญแห่งสิทธิในข้อมูลข่าวสารส่วนบุคคล

พยานหลักฐานที่เป็นข้อมูลส่วนบุคคลโดยทั่วไปนอกจากจะได้รับความคุ้มครองตามประมวลกฎหมายอาญาแล้วยังได้รับความคุ้มครองตามรัฐธรรมนูญในส่วนของสิทธิส่วนบุคคล และสำหรับพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งมีลักษณะแตกต่างไปจากพยานหลักฐานทั่วๆ ไป กล่าวคือพยานหลักฐานประเภทนี้เป็นสิ่งที่ไม่มีรูปร่าง มองไม่เห็นด้วยตาเปล่า และอยู่ในรูปของคลื่นแม่เหล็กไฟฟ้า อาจถูกแก้ไขเปลี่ยนแปลง ลบ ทำลายได้ง่าย เจ้าหน้าที่ในกระบวนการยุติธรรมทั้งหลายจึงต้องประสบปัญหาในการดำเนินคดีกับผู้กระทำความผิด โดยเฉพาะพนักงานสอบสวนที่มีหน้าที่ในการรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดของจำเลยและนำเสนอต่อศาล ผู้วิจัยได้ทำการศึกษาวิจัยปัญหาการรวบรวมพยานหลักฐานและพิสูจน์พยานหลักฐานที่เป็นอิเล็กทรอนิกส์และเป็นข้อมูลส่วนบุคคล ภายในกรอบของ 3 หัวข้อใหญ่ ได้แก่ ลักษณะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ สิทธิส่วนบุคคล กระบวนการค้น และกระบวนการนำเสนอพยานหลักฐานต่อศาล ภายใต้สมมติฐานว่าการรวบรวมพยานหลักฐานที่เป็นการละเมิดสิทธิส่วนบุคคลที่ได้รับการคุ้มครองตามรัฐธรรมนูญและกฎหมายอาญาเจ้าหน้าที่ของรัฐสามารถกระทำได้เพียงใด ปัจจุบันมีกฎหมายฉบับใดให้อำนาจกระทำได้หรือไม่อย่างไร และควรจะกระทำอย่างไรเพื่อที่จะนำตัวผู้กระทำความผิดมาลงโทษให้ได้

ผลจากการศึกษาและวิเคราะห์ปัญหาทั้งในประเทศไทยและต่างประเทศ ตลอดจนศึกษาแนวทางแก้ไขปัญหาของต่างประเทศ โดยเฉพาะของประเทศสหรัฐอเมริกา อังกฤษ และญี่ปุ่น พบว่าการที่จะให้เจ้าหน้าที่ของรัฐเข้าถึงหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ได้เร็ว และไม่เป็นการละเมิดสิทธิในข้อมูลข่าวสารส่วนบุคคลจะต้องมีกฎหมายให้อำนาจในการปฏิบัติงานได้ ควรต้องมีองค์กรที่เป็นกลางเป็นผู้ให้อำนาจในการตรวจสอบการใช้อำนาจ และควรมีหลักกฎหมายลักษณะพยานหลักฐานเกี่ยวกับพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ที่ชัดเจนกว่านี้

Thesis Title Pursuing of electronic materials and personal data in Computer crime
Author Naree Kittisomboonsuk
Thesis Advisor Vice Prof. Dr. Udom Rathaarmarit
Co-Thesis Advisor Dr. Uthai Arthiveth
Department Law
Academic Year 2005

ABSTRACT

One of the most damage in Social is computerized criminal that destroying economics. In every country of the world realized this typical hazardous criminal and its effected. Due to insufficient criminal laws to indict them. Therefore the search of new suppressive and protective statues have been made with much effect. Thailand country also realized this crucial problem. Then proposing bill of computerized criminal however there must be concerned the usage of proper laws. Also developing criminal procedure effectiveness especially pursuing of personal data evidences and notified them.

The Kingdom of Thailand constitution B.E. 2540 code 29 provide basically for personal right and freedom which limited by state practice able to legislate laws in some case. Dealing with the constitution such as code 37 provide personal right protection. As same as the constitution provide state authority apply to public interests case. When state inhabited an exemption to legislate laws that too limited personal right and freedom informations. By claimable of public interests for instance, state made laws allowing officers to persue personal informations any of time. Especially those appropriate personal data from computers. The performance hold effected to right and freedom of person which have results according to the legislation code 6. Mean that the constitution, highest laws of country, was protected. It unable to extort even access to personal data became a new criterion of state in pursuing evidence to persecute criminals. The former procedure unable solving computerized criminal problems. So that could legislation laws for controlling authority performance of state officers uneffected in area of personal information right.

Generally said personal data evidence must protected by criminal procedure code and constitution in the differentiation of electronic data. The typical evidence have no shape, invisible and dwell in electromagnetic site which easily destroying or erasing. Especially when ascertain officers gathered all of them accusing to court. My studied in this research has 3 points of personal electronic data. Such as electronic evidence descriptions, personal right, persuing procedure and adducing evidence under hypothesis that violated personal right. Beneat the constitution and criminal procedure whether officers could do. Nowadays, whether laws provide authority and how the penalty of wrongdoers.

Problems analysis and results of this study received from Thailand and other countries' solution. Especially United States, England and Japan found that state officers could persuing electronic evidences rapidly. They also didn't violate personal right as dealing with laws and authority performance. There could have neutral organization checking the use of power. And should have electronic evidence description more obviously.

DPU

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้โดยความอนุเคราะห์เป็นอย่างดียิ่งอันผู้เขียนต้องขอกราบขอบพระคุณต่อท่าน รองศาสตราจารย์ ดร. อุดม รัฐอมฤต อาจารย์ที่ปรึกษา ซึ่งท่านได้ให้คำแนะนำและข้อคิดต่างๆ รวมทั้งตรวจแก้วิทยานิพนธ์จนสำเร็จ และต้องขอกราบพระคุณท่านอาจารย์ ดร. อุทัย อาทิเวช อาจารย์ที่ปรึกษาร่วม ที่ได้ให้คำแนะนำและข้อคิดต่างๆ

ผู้เขียนใคร่ขอขอบคุณท่าน ศาสตราจารย์ ดร. คณิต ณ นคร ประธานกรรมการสอบวิทยานิพนธ์ ท่านรองศาสตราจารย์ ดร. สุรศักดิ์ ลิขสิทธิ์วัฒนกุล และท่านอาจารย์ชาญเชาว์ ไชยานุกิจ ที่กรุณาสละเวลาอันมีค่าของท่านให้คำแนะนำ และเป็นกรรมการสอบวิทยานิพนธ์ฉบับนี้

นอกจากนี้ผู้เขียนใคร่ขอขอบคุณเพื่อนที่คอยให้กำลังใจ และให้ความช่วยเหลือข้าพเจ้าตลอดมา ตลอดจนครอบครัวของผู้เขียนอันได้แก่ คุณพ่อวรพจน์ กิตติสมบูรณ์สุข คุณแม่ฮุยใหม่ กิตติสมบูรณ์สุข พี่สาวคนโตนางสาวอนุสรณ์ กิตติสมบูรณ์สุข พี่ชายคนโตนายจรัส กิตติสมบูรณ์สุข พี่ชายคนรองนายเจริญกิตติสมบูรณ์สุข พี่ชายคนที่สามนายดำรงค์ กิตติสมบูรณ์สุข พี่ชายคนที่สี่นายเติมทรัพย์ กิตติสมบูรณ์สุข พี่ชายคนที่ห้านายอุดมศักดิ์ กิตติสมบูรณ์สุข พี่สาวคนสุดท้ายนางสาวอารีรัตน์ กิตติสมบูรณ์สุข พี่สะใภ้ทั้ง 5 คน และเหล่าหลานๆที่น่ารักทั้ง 8 คนที่คอยให้กำลังใจ และสนับสนุนผู้เขียนตลอดมา

ผู้เขียนสำนึกในความเมตตากรุณาของบุคคลต่างๆ ที่ได้กล่าวนามไว้ข้างต้นและปิติยินดีอย่างยิ่งที่ได้มีโอกาสเผยแพร่ประกาศเกียรติคุณของท่านให้ปรากฏไว้เป็นลายลักษณ์อักษรควบคู่กับวิทยานิพนธ์นี้ตลอดไป

คุณค่าของวิทยานิพนธ์ฉบับนี้ที่ขอมอบเป็นเครื่องบูชาพระคุณบิดา มารดา ครูบาอาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ให้แก่ข้าเจ้า ญาติพี่น้อง เพื่อนฝูง ผู้มีพระคุณทุกท่าน และขออาราธนาอำนาจคุณพระศรีรัตนตรัยและสิ่งศักดิ์สิทธิ์ในสากลโลกนี้ ให้ดลบันดาลให้ท่านเหล่านี้ มีความสุขสมปรารถนาทุกประการ

นารี กิตติสมบูรณ์สุข

สารบัญ

หน้า

บทคัดย่อภาษาไทย……. ฆ

บทคัดย่อภาษาอังกฤษ…… จ

กิตติกรรมประกาศ…….. ช

บทที่

1. บทนำ…… 1

1.1 ความเป็นมาและความสำคัญของปัญหา……. 1

1.2 สมมติฐานของวิทยานิพนธ์……... 2

1.3 วัตถุประสงค์ของการศึกษา…..…….. 3

1.4 วิธีการศึกษา…… 4

1.5 ขอบเขตของการศึกษา…… 4

1.6 ประโยชน์ที่คาดว่าจะได้รับ…… 4

2. การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์…….. 5

2.1 ความหมาย ความสำคัญ และประเภท ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล…….. 5

2.2 หลักเกณฑ์การคุ้มครองสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล..…… 14

2.3 การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในคดีอาญา……. 27

3. การเข้าถึงข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในกฎหมายต่างประเทศ……... 31

3.1 ประเทศสหรัฐอเมริกา…… 31

3.2 ประเทศอังกฤษ……. 38

3.3 ประเทศญี่ปุ่น……. 47

4. วิเคราะห์มาตรการทางกฎหมายในการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในประเทศไทย……. 55

4.1 มาตรการทางกฎหมายของไทยที่เกี่ยวกับคอมพิวเตอร์ที่มีในปัจจุบัน…..……... 55

4.2 วิเคราะห์ปัญหาที่ไม่อาจคุ้มครองสิทธิในข้อมูลข่าวสารส่วนบุคคลได้อย่างชัดเจน…… 63

DPU

สารบัญ (ต่อ)

หน้า

5. สรุปและเสนอแนะ…… 65

5.1 บทสรุป…….. 65

5.2 ข้อเสนอแนะ…….. 66

บรรณานุกรม…….. 69

DPU

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเครื่องคอมพิวเตอร์เป็นเครื่องมือที่ให้คุณประโยชน์แก่มนุษย์มากมาย ไม่ว่าจะเป็นการใช้ในการติดต่อสื่อสาร วิทยาศาสตร์ การแพทย์ การศึกษา การปกครอง การทหาร การพาณิชย์ฯลฯ ในขณะที่เครื่องคอมพิวเตอร์ได้ก่อคุณประโยชน์นานัปการให้แก่มนุษย์ ก็ได้ก่อให้เกิดความเสียหายแก่มนุษย์ที่ไม่สามารถประเมินได้ หากจะได้นำไปใช้เป็นเครื่องมือในการกระทำความผิด เช่น อาชญากรรมที่เป็นการขโมยข้อมูล การปลอมแปลง การเผยแพร่ข้อมูลที่ไม่เหมาะสม การฟอกเงิน การแทรกแซงทางการค้า การค้าขายสิ่งผิดกฎหมาย เช่น การค้ายาเสพติด การขายบริการทางเพศ ฯลฯ

อาชญากรรมคอมพิวเตอร์ เป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่งที่เกี่ยวกับการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายหลักทรัพย์ และการฉ้อโกงประชาชน โดยเป็นการกระทำที่ดำเนินการและใช้คอมพิวเตอร์ในการกระทำความผิด ทำให้เหยื่อได้รับความเสียหายและผู้กระทำได้รับผลประโยชน์จากการกระทำนั้น ความเสียหายที่เกิดขึ้นก็มิได้เป็นความเสียหายแต่เฉพาะผู้เสียหายเพียงคนเดียวเท่านั้น แต่ยังก่อให้เกิดความเสียหายกับระบบเศรษฐกิจ สังคม ความสงบเรียบร้อย และความมั่นคงทั้งภายในและระหว่างประเทศ เป็นอาชญากรรมที่ยากแก่การสืบสวนติดตามและจับกุม เนื่องจากระยะเวลาในการกระทำความผิดก็เป็นไปอย่างรวดเร็ว ไม่มีขอบเขตจำกัด และไร้พรมแดน แตกต่างจากอาชญากรรมที่มีมาแต่เดิม[1]

ในขณะที่กฎหมายที่มีผลใช้บังคับยังคงเป็นกฎหมายเดิมๆ แต่การกระทำความผิดของอาชญากรพัฒนาไปตามการเจริญเติบโตของเทคโนโลยี ทำให้มาตรการทางกฎหมายที่มีมาแต่เดิมไม่สามารถนำมาบังคับใช้กับการกระทำความผิดที่เกิดขึ้นได้อย่างมีประสิทธิภาพ เนื่องจากการใช้กฎหมายอาญาจะต้องยึดถือหลัก “ไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย” (nullum crimen nulla poena sine lege)

---

[1] วีระพงษ์ บุญโญภาส. (2544). **อาชญากรรมทางเศรษฐกิจ** (พิมพ์ครั้งที่ 3). หน้า 109–110.

ปัญหาอาชญากรรมคอมพิวเตอร์จึงเป็นปัญหาที่นานาอารยประเทศต่างให้ความสนใจ และได้พยายามวางมาตรการขึ้นเพื่อแก้ไขปัญหาที่เกิดขึ้น ประเทศไทยเองก็มีความจำเป็นเร่งด่วนในการหาทางแก้ไขโดยการวางมาตรการที่สามารถแก้ไขปัญหาได้อย่างแท้จริง

อย่างไรก็ตาม การออกกฎหมายมาใช้จะต้องคำนึงถึงทางปฏิบัติ เพื่อให้เกิดผลบังคับได้อย่างแท้จริง โดยเฉพาะในเรื่องของการรวบรวบพยานหลักฐาน ซึ่งเป็นหัวใจสำคัญของการดำเนินคดีอาญา โดยที่พยานหลักฐานในความผิดอาชญากรรมคอมพิวเตอร์เป็นข้อมูลอิเล็กทรอนิกส์ที่กฎหมายจะต้องให้อำนาจเจ้าหน้าที่ของรัฐในการแสวงหา โดยจะต้องไม่เป็นการล่วงละเมิดต่อสิทธิเสรีภาพในข้อมูลข่าวสารส่วนบุคคลที่ได้รับความคุ้มครองตามรัฐธรรมนูญอย่างไม่เป็นธรรม และตัวเจ้าพนักงานของรัฐเองก็จะต้องเป็นผู้ที่มีความรู้ความสามารถทางด้านนี้อย่างแท้จริง

1.2 สมมติฐานของวิทยานิพนธ์

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 29 ได้บัญญัติรับรองสิทธิและเสรีภาพของประชาชนไว้เป็นหลักพื้นฐาน ซึ่งในทางปฏิบัติรัฐสามารถบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ในบางกรณี ดังนั้นจึงมีบทบัญญัติที่ให้อำนาจรัฐตรากฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ภายในขอบเขตที่รัฐธรรมนูญกำหนด เช่น ในมาตรา 37 บัญญัติรับรองคุ้มครองสิทธิความเป็นอยู่ส่วนตัวของบุคคล ซึ่งเป็นสิทธิส่วนบุคคล และรัฐธรรมนูญก็มีบทบัญญัติให้อำนาจรัฐกระทำการใดๆ ก็ได้หากเป็นกรณีที่กระทำไปเพื่อประโยชน์สาธารณะ ดังนั้นรัฐอาจอาศัยข้อยกเว้นดังกล่าวบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคลเกินความจำเป็น หรือตามอำเภอใจ โดยอ้าง “ประโยชน์สาธารณะ” เช่น รัฐอาจบัญญัติกฎหมายอนุญาตให้เจ้าหน้าที่ของรัฐเข้าตรวจสอบข้อมูลส่วนบุคคลของบุคคลใดบุคคลหนึ่งได้ตลอดเวลา ตามแต่จะเป็นสมควรโดยเฉพาะข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ เป็นต้น การกระทำดังกล่าวถือเป็นการกระทำที่กระทบกระเทือนต่อสาระสำคัญแห่งสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล ซึ่งจะมีผลตามบทบัญญัติในมาตรา 6 ที่ถือว่าบทบัญญัติดังกล่าวขัดหรือแย้งกับรัฐธรรมนูญซึ่งถือเป็นกฎหมายสูงสุดของประเทศ ทำให้บทบัญญัติดังกล่าวไม่สามารถใช้บังคับได้ ทั้งๆที่ การเข้าสู่ข้อมูลส่วนบุคคลนี้ เป็นมาตรการใหม่ที่รัฐสามารถนำมาใช้แสวงหาพยานหลักฐานเพื่อมาดำเนินคดีกับอาชญากรที่ก่ออาชญากรรมที่การแสวงหาพยานหลักฐานรูปแบบดั้งเดิมไม่สามารถแก้ปัญหาได้ เช่น อาชญากรรมคอมพิวเตอร์ ดังนั้น จึงควรมีการบัญญัติกฎหมายขึ้นมาให้อำนาจ และควบคุมการใช้อำนาจของเจ้าหน้าาที่ของรัฐในการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลได้ ภายในขอบเขตที่ไม่เป็นการกระทบกระเทือนต่อสาระสำคัญแห่งสิทธิในข้อมูลข่าวสารส่วนบุคคล

1.3 วัตถุประสงค์ของการศึกษา

1.3.1 ศึกษามาตรการทางกฎหมายของประเทศไทย และกฎหมายต่างประเทศเกี่ยวกับวิธีการและขั้นตอนในการรวบรวมพยานหลักฐานที่เป็นข้อมูลข่าวสารส่วนบุคคลที่อยู่ในเครื่องคอมพิวเตอร์ ได้แก่ กฎหมายที่คุ้มครองสิทธิในข้อมูลข่าวสารส่วนบุคคล กฎหมายที่ให้อำนาจเจ้าพนักงานของรัฐเข้าสู่ข้อมูลข่าวสารส่วนบุคคล และการรับฟังเป็นพยานหลักฐานในคดีได้

1.3.2 วิเคราะห์ปัญหาความขัดแย้งระหว่างบทบัญญัติของกฎหมาย และการใช้อำนาจของเจ้าพนักงานของรัฐในการรวบรวมพยานหลักฐานที่เป็นข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์

1.3.3 ศึกษาแนวทางการแก้ปัญหาการรวบรวมพยานหลักฐานที่เป็นข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ในต่างประเทศ และวิเคราะห์กรณีที่นำมาใช้ในประเทศไทย

1.4 วิธีการศึกษา

ศึกษาจากเอกสารที่เป็นตัวบทกฎหมาย คำพิพากษา ตำรา บทความภาษาไทย และภาษาต่างประเทศ เพื่อนำมาเป็นข้อมูลในการวิเคราะห์และเปรียบเทียบเพื่อให้เกิดองค์ความรู้และเป็นแนวทางในการแก้ไขปัญหาที่เหมาะสม

1.5 ขอบเขตของการศึกษา

ทำการศึกษาถึงข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคล และวิเคราะห์หลักกฎหมายวิธีพิจารณาความอาญาที่มีอยู่ว่าจะนำมาใช้กับการเข้าถึงข้อมูลส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ได้เพียงใด โดยจะทำการศึกษาเปรียบเทียบกับกฎหมายต่างประเทศที่เกี่ยวข้องกับการแสวงหาข้อมูลอิเล็กทรอนิกส์ไปเป็นพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ได้ทราบแนวทางสำหรับการกำหนดมาตรการใช้อำนาจของรัฐในการแสวงหาพยานหลักฐานจากข้อมูลอเล็กทรอนิกส์ที่สามารถแก้ปัญหาอาชญากรรมคอมพิวเตอร์ให้ได้อย่างมีประสิทธิภาพ และเหมาะสม คำนึงถึงการคุ้มครองข้อมูลข่าวสารส่วนบุคคล

1.6.2 สามารถนำไปใช้ในการบัญญัติกฎหมาย การแก้ไขปรับปรุงกฎหมาย และการปฏิบัติตามกฎหมายที่เกี่ยวข้องเพื่อให้ตรงตามเจตนารมณ์ของรัฐธรรมนูญ

DPU

บทที่ 2
การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์

ขั้นตอนที่สำคัญขั้นตอนหนึ่งในการดำเนินกระบวนการยุติธรรมทางอาญา นั่นคือการดำเนินคดีอาญาชั้นก่อนฟ้อง (Vorverfahren) คือ การดำเนินการทั้งปวงของเจ้าพนักงานก่อนการยื่นฟ้อง ได้แก่ การสอบสวนของพนักงานสอบสวนและการดำเนินการของพนักงานอัยการก่อนการยื่นฟ้อง [1] และในการดำเนินการสอบสวนก็ครอบคลุมเนื้อหา 2 ประการ ได้แก่ การรวบรวมพยานหลักฐานและการใช้มาตรการบังคับ [2] ดังนั้นการแสวงหาและรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดจึงเป็นขั้นตอนก่อนการฟ้อง เมื่อมีการกระทำความผิดอาญาเกิดขึ้นการที่จะลงโทษผู้กระทำความผิดได้จะต้องมีการรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิด ถ้าไม่มีพยานหลักฐานก็ไม่สามารถที่จะดำเนินกระบวนการยุติธรรมทางอาญาขั้นตอนอื่นๆ ต่อไปได้ เมื่อพยานหลักฐานที่จะนำมาพิสูจน์การกระทำความผิดเป็นส่วนสำคัญของกระบวนการยุติธรรมทางอาญา ผู้กระทำความผิดก็ย่อมที่จะปกปิด ซ่อนเร้น พยานหลักฐานดังกล่าวอยู่ในคอมพิวเตอร์หรือสื่ออิเล็กทรอนิกส์ต่างๆ ซึ่งข้อมูลจากสื่อเหล่านี้อาจใช้เป็นพยานหลักฐานในคดีอาญาได้

ด้วยเหตุนี้กฎหมายวิธีพิจารณาความอาญาจึงต้องมีเครื่องมือในการแสวงหาพยานหลักฐาน ในที่นี้ได้แก่การค้น ซึ่งเป็นมาตรการบังคับในการดำเนินคดีอาญาประการหนึ่ง ซึ่งในที่นี้เป็นการค้นหาพยานหลักฐานจากเครื่องคอมพิวเตอร์หรือสื่ออิเล็กทรอนิกส์ต่างๆ เฉพาะที่เป็นข้อมูลส่วนบุคคล และเป็นมาตรการบังคับที่รุนแรงมาก เพราะเป็นมาตรการบังคับที่กระทบถึงสิทธิและเสรีภาพของบุคคล ดังนั้นจึงจำเป็นที่จะต้องเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ เพื่อประโยชน์ในการแสวงหาพยานหลักฐานที่มีลักษณะดังกล่าวต่อไป

---

[1] คณิต ณ นคร. (2546). **กฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 6, แก้ไขเพิ่มเติม ปรับปรุงใหม่). หน้า 308.

[2] คณิต ณ นคร. เล่มเดิม. หน้า 313.

2.1 ความหมาย ความสำคัญ และประเภท ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

2.1.1 ความหมายของข้อมูลอิเล็กทรอนิกส์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 ให้ความหมายคำว่า "ข้อมูลอิเล็กทรอนิกส์" หมายถึง ข้อความที่ได้ส่ง รับ เก็บรักษาหรือประมวลผลด้วยวิธีการอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์หรือโทรสาร

มาตรา 4 ยังได้ให้คำนิยามคำว่า อิเล็กทรอนิกส์ ข้อความ ระบบข้อมูล การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ ผู้ส่งข้อมูล ผู้รับข้อมูล และบุคคลที่เป็นสื่อกลาง ไว้ดังนี้

"อิเล็กทรอนิกส์" หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่างๆ เช่นว่านั้น

"ข้อความ" หมายความว่า เรื่องราวหรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ

"ระบบข้อมูล" หมายความว่า กระบวนการประมวลผลด้วยเครื่องมืออิเล็กทรอนิกส์สำหรับ สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลข้อมูลอิเล็กทรอนิกส์

"การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์" หมายความว่า การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

"ผู้ส่งข้อมูล" หมายความ บุคคลซึ่งผู้ส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีที่ผู้นั้นกำหนด โดยบุคคลนั้นอาจจะส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

"ผู้รับข้อมูล" หมายความว่า บุคคลซึ่งผู้ส่งข้อมูลประสงค์จะส่งข้อมูลอิเล็กทรอนิกส์ให้และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

"บุคคลที่เป็นสื่อกลาง" หมายความว่า บุคคลซึ่งกระทำการในนามผู้อื่นในการส่ง รับ หรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์อันใดอันหนึ่งโดยเฉพาะ รวมถึงให้บริการอื่นที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น

DPU

นอกจากนี้ยังมีร่างกฎหมายเกี่ยวกับกิจการอินเตอร์เน็ต โดยคณะกรรมการกฎหมายได้เสนอร่างพระราชบัญญัติส่งเสริมกิจการอินเตอร์เน็ต ร่าง 1 ให้นิยามคำว่า คอมพิวเตอร์ อินเตอร์เน็ต ข้อมูลและข้อมูลข่าวสาร[3] ดังนี้

"คอมพิวเตอร์" หมายความว่า อุปกรณ์ที่ใช้ประมวล วิเคราะห์ข้อมูล ซึ่งทำงานด้วยอิเล็กทรอนิกส์แม่เหล็กไฟฟ้าใยแก้ว อิเล็กทรอนิกส์หรืออุปกรณ์ที่เชื่อมต่อ หรือเกี่ยวข้องกับอุปกรณ์ดังกล่าว ซึ่งใช้งานด้วยเหตุผลทางวิทยาศาสตร์ คณิตศาสตร์ เก็บบันทึกและแสดงข้อมูลและหมายรวมถึงการเก็บบันทึกข้อมูลหรือการสื่อสารที่ต่อเชื่อมโดยตรง หรือใช้งานร่วมกับอุปกรณ์นั้นๆ หรืออุปกรณ์ที่เชื่อมต่อระหว่างอุปกรณ์ดังกล่าว แต่ไม่รวมตลอดถึงเครื่องพิมพ์อักษรอัตโนมัติ หรือเครื่องติดตั้งตัวอักษร หรือคำนวณตัวเลขแบบพกพา หรืออุปกรณ์ร่วมทั้งการเผยแพร่ Program ด้วยวิธีใดๆ

"อินเตอร์เน็ต" หมายความว่า ระบบเครือข่ายที่มีเครื่องคอมพิวเตอร์เชื่อมโยงกันทั่วโลก โดยอาศัยการสื่อสารด้วยระเบียบวิธีในการสื่อสารกันระหว่างเครื่องคอมพิวเตอร์ เชื่อมต่อกันในระบบปฏิบัติการแบบมีผู้ใช้หลายคน

"ข้อมูล" หมายความว่า สิ่งที่เป็นข้อเท็จจริง เช่น ข้อความ จำนวนเลข เสียงและภาพ ซึ่งแสดงในรูปแบบที่คอมพิวเตอร์สามารถประมวลผลได้

"ข้อมูลข่าวสาร" หมายความว่า สิ่งที่สื่อความหมาย

และร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ได้ให้ความหมายของคำว่า ระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ ไว้ดังนี้

"ระบบคอมพิวเตอร์" ในพระราชบัญญัตินี้ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดชุดคำสั่งและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ หรือชุดคำสั่ง บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้

เมื่อพิจารณาจากความหมายของคำว่า "ระบบคอมพิวเตอร์" จากร่างพระราชบัญญัติส่งเสริมกิจการอินเตอร์เน็ต ร่าง 1 และร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ข้างต้น "ระบบคอมพิวเตอร์" จึงได้แก่ฮาร์ดแวร์และซอฟต์แวร์ที่พัฒนาขึ้นเพื่อประมวลผลข้อมูลดิจิทัล (digital data) อันประกอบด้วยเครื่องคอมพิวเตอร์ และอุปกรณ์รอบข้าง

---

[3] คณะกรรมการบริหารสมาคมอินเตอร์เน็ตนานาชาติ ประเทศไทย, "ร่างพระราชบัญญัติส่งเสริมกิจการอินเตอร์เน็ต พ.ศ. …….. (ร่าง 1)," <http://www.acm.th.org/law/internetlaw1b.html>

(peripheral) ต่างๆ ในการรับเข้าหรือป้อนข้อมูล (input) นำออกหรือแสดงผลข้อมูล (output) และบันทึกหรือเก็บข้อมูล (store and record) ดังนั้น ระบบคอมพิวเตอร์จึงอาจเป็นอุปกรณ์เพียงเครื่องเดียว หรือหลายเครื่องอันมีลักษณะเป็นชุดเชื่อมต่อกันโดยอาจผ่านระบบเครือข่าย และมีลักษณะการทำงานโดยอัตโนมัติตามโปรแกรมที่กำหนดไว้ และไม่มีการแทรกแซงโดยตรงจากมนุษย์ ส่วนโปรแกรมคอมพิวเตอร์จะหมายถึงชุดคำสั่งที่ทำหน้าที่สั่งการให้คอมพิวเตอร์ทำงาน

ดังนั้นข้อมูลคอมพิวเตอร์ จึงไม่ใช่เฉพาะตัวอักขระ หรือข้อความที่สื่อความหมาย อ่านเข้าใจได้ที่หน้าจอภาพ (monitor) เท่านั้น แต่เป็นข้อมูลดิจิทัลที่อยู่ในระบบคอมพิวเตอร์ และอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้

ตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 มาตรา 4 ให้ความหมายคำว่า “ข้อมูลข่าวสาร” “ข้อมูลข่าวสารส่วนบุคคล” ดังนี้

คำว่า “ข้อมูลข่าวสาร” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

คำว่า “ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

ตามร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. … มาตรา 4 ได้ให้ความหมายคำว่า “ข้อมูลส่วนบุคคล” “บันทึกข้อมูลส่วนบุคคล” ดังนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อเท็จจริงเกี่ยวกับตัวบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม

“บันทึกข้อมูลส่วนบุคคล” หมายความว่า เอกสาร ฐานข้อมูล หรือรูปภาพหรือสิ่งซึ่งแสดงภาพของบุคคลในรูปแบบอื่น ทั้งนี้ไม่รวมถึงสิ่งพิมพ์ซึ่งเผยแพร่ทั่วไปหรือเอกสารที่เก็บไว้ในห้องสมุด หอศิลปะ หรือพิพิธภัณฑ์ เพื่อประโยชน์ในการใช้อ้างอิง การศึกษา การจัดนิทรรศการ หรือเอกสารที่เป็นอนุสรณ์ หรือจดหมายหรือสิ่งอื่นใดที่มีการส่งในทางปกติธุระของการไปรษณีย์ เว้นแต่ข้อความจะกำหนดไว้เป็นอย่างอื่น

เมื่อพิจารณาตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 และร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...ความหมายของคำว่าข้อมูลส่วนบุคคล ควรหมายถึง ข้อมูลข่าวสารที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคล และเป็นข้อมูลที่ได้รับความคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ไม่เปิดเผยต่อผู้ที่ไม่มีสิทธิรับรู้ แม้หลักพื้นฐานของที่สำคัญ 2 ประการของของข้อมูลข่าวสารของราชการนั้น ได้แก่ หลักที่ว่าบุคคลไม่จำต้องเป็นผู้มีส่วนได้เสียกับข้อมูลข่าวสารส่วนที่ขอ และเปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น[4] แต่ในเรื่องข้อมูลข่าวสารส่วนบุคคลนี้ กฎหมายต้องการคุ้มครองความเป็นอยู่ส่วนบุคคลตามที่รัฐธรรมนูญได้บัญญัติไว้ในมาตรา 34 ดังนั้น จึงได้กำหนดหลักการสำคัญแตกต่างไปจากข้อมูลข่าวสารของทางราชการ โดยกำหนดไว้เป็นหลักการว่า "ข้อมูลข่าวสารส่วนบุคคลจะเปิดเผยต่อบุคคลอื่นโดยปราศจากความยินยอมมิได้ เว้นแต่จะเข้าข้อยกเว้น" โดยกฎหมายฉบับนี้ได้บัญญัติเป็นข้อยกเว้นไว้ในมาตรา 24

ข้อมูลข่าวสารส่วนบุคคลนั้นอาจเป็นข้อมูลของบุคคลที่ยังมีชีวิตอยู่ หรือแม้กระทั่งผู้ที่ถึงแก่กรรมไปแล้ว เพราะหากข้อมูลของบุคคลเหล่านั้นถูกเปิดเผยออกไปก็อาจเป็นผลร้ายแก่ชื่อเสียงของผู้ตาย ญาติพี่น้อง หรือวงศ์ตระกูลได้[5]

2.1.2 การประมวลผลข้อมูล (Data Processing) เมื่อมีข้อมูลเกิดขึ้น หรือมีการรวบรวมข้อมูลต่างๆ ขึ้น วิธีการจัดการข้อมูล ไม่ว่าการคำนวณ การเรียงลำดับ หรือการจัดกลุ่ม ต่างก็เป็นการประมวลผล (Processing) ทั้งสิ้น การประมวลผล จึงหมายถึง วิธีการจัดการกับข้อมูล โดยมีจุดมุ่งหมายเพื่อให้ได้ผลลัพธ์อย่างใดอย่างหนึ่ง ข้อสรุปที่ได้ เรียกว่าข้อสนเทศ (Information) ซึ่งสามารถนำไปใช้ในการตัดสินใจต่างๆ ที่เกี่ยวข้อง ขึ้นอยู่กับการนำไปใช้ประโยชน์ของแต่ละคน

ก. ขั้นตอนของการประมวลผลข้อมูล[6] แบ่งเป็น 3 ขั้นตอน ได้แก่

(1) การเตรียมข้อมูล (Input) การเตรียมข้อมูล (Input) คือการเก็บรวบรวมข้อมูลเพื่อรอประมวลผล ซึ่งหมายรวมถึงการเปลี่ยนสภาพข้อมูลให้อยู่ในรูปแบบที่เหมาะสมและพร้อมที่จะประมวลผลต่อไป การเปลี่ยนสภาพข้อมูลประกอบด้วย

- การลงรหัส (Coding) หมายถึงการให้รหัสแทนข้อมูลจริง ทำให้ข้อมูลอยู่ในรูปแบบที่กะทัดรัดสะดวกแก่การประมวลผล ซึ่งรหัสที่ใช้อาจเป็นตัวเลขหรือตัวอักษรก็ได้ เช่น ข้อมูลเพศชาย ใช้แทนด้วยตัว ช. ส่วนเพศหญิงใช้ตัว ญ. เป็นต้น

---

[4] หฤทัย หงส์สิริ และ มานิต จุมปา. (2542). **คำอธิบายข้อมูลข่าวสารของทางราชการ**. หน้า 86.

[5] หฤทัย หงส์สิริ และ มานิต จุมปา. เล่มเดิม. หน้า 19.

[6] วัชราภรณ์ สุริยาภิวัฒน์. (2543). **คอมพิวเตอร์เบื้องต้นและเทคนิคการเขียนโปรแกรม**. หน้า 26-27.

- การบรรณาธิกรณ์ (Editing) หมายถึงการตรวจสอบความถูกต้องและความเป็นไปได้ของข้อมูลและปรับปรุงแก้ไขเท่าที่จะทำได้ เช่น ผู้ให้ข้อมูลเป็นเพศหญิง แต่ตอบว่าเคยเกณฑ์ทหาร ก็ต้องทำการตรวจสอบโดยพิจารณาจากคำตอบที่ได้จากคำถามข้ออื่น หรือไปสอบถามใหม่ แล้วแก้ไข

- การแยกประเภท (Classifying) หมายถึงการจัดประเภทข้อมูลให้เป็นกลุ่มตามลักษณะต่างๆ ของข้อมูล เพื่อสะดวกต่อการประมวลผลต่อไป

- การบันทึกข้อมูลในสื่อ (Media) ที่เหมาะสม หมายถึงการจัดเตรียมข้อมูลให้อยู่ในสื่อหรืออุปกรณ์ที่ใช้ได้กับเครื่องมือการประมวลผลที่มีอยู่ เช่นบันทึกข้อมูลลงแผ่นดิสก์ หรือเทปแม่เหล็กเพื่อนำไปประมวลผลด้วยเครื่องคอมพิวเตอร์ต่อไป

(2) การประมวลผล (Processing) หมายถึงวิธีการจัดการกับข้อมูล ซึ่งอาจเป็นการคำนวณการรวมข้อมูลมากกว่าหนึ่งชุดเข้าด้วยกัน (Merge) การดึงข้อมูลมาใช้ (Retrieve) หรือการเรียงลำดับ (Sort)

(3) การนำเสนอผลลัพธ์ (Output) หมายถึงการนำผลลัพธ์ที่ได้จากการประมวลผลมาแสดงให้ทราบ เช่น แสดงผลสรุปในรูปของตาราง หรือกราฟ

ข. ประเภทของการประมวลผลข้อมูล[7] เมื่อพิจารณาจากอุปกรณ์ที่ใช้เป็นหลัก สามารถแบ่งการประมวลผลข้อมูลได้ 3 ประเภท

(1) การประมวลผลข้อมูลด้วยมือ (Manual Data Processing) เป็นวิธีการประมวลผลข้อมูลที่มีมาแต่เดิม อุปกรณ์ที่ใช้ได้แก่ กระดาษทด เครื่องคิดเลข ลูกคิด ใช้กับข้อมูลที่มีจำนวนน้อยและการคำนวณไม่ยุ่งยาก และเป็นงานที่ไม่รีบเร่ง

(2) การประมวลผลข้อมูลด้วยเครื่องจักรกล (Mechanical Data Processing) เป็นการใช้แรงงานคนร่วมกับเครื่องจักร ที่ใช้กันมากได้แก่ เครื่องจักรทำบัญชี ซึ่งเป็นเครื่องประมวลผลประเภทกึ่งอิเล็กทรอนิกส์ที่เรียกว่า “เครื่อง Unit Record” เช่น เครื่องเจาะบัตร (Card Punch) เครื่องรวมบัตร (Collator) เครื่องเรียงบัตร (Card Sorter) เครื่องแปลบัตร (Interpreter) ฯลฯ เป็นการประมวลผลที่เหมาะกับงานระดับกลางที่มีข้อมูลไม่มากนักและต้องการความรวดเร็วในการทำงานปานกลาง

(3) การประมวลผลข้อมูลด้วยเครื่องคอมพิวเตอร์ (Electronic Data Processing - EDP.) หมายถึงการประมวลผลข้อมูลด้วยเครื่องอิเล็กทรอนิกส์ และเครื่องอิเล็กทรอนิกส์ที่ใช้ก็คือคอมพิวเตอร์นั่นเอง เหมาะกับงานที่มีปริมาณมาก และมีขั้นตอนการทำงานซ้ำๆกัน ต้องการ

---

[7] วัชราภรณ์ สุริยาภิวัฒน์. เล่มเดิม. หน้า 28-29.

ประสิทธิภาพในการทำงาน ให้ผลลัพธ์ที่ถูกต้อง เป็นการคำนวณที่มีสูตรยุ่งยากซับซ้อน และเป็นงานที่ต้องการภาพพจน์ที่ทันสมัย ฯลฯ

2.1.3 ระบบและประโยชน์ของเครือข่ายคอมพิวเตอร์

ก. ระบบเครือข่ายคอมพิวเตอร์ เป็นระบบการสื่อสารที่ประกอบด้วยเครื่องคอมพิวเตอร์หลายเครื่องเชื่อมต่อถึงกันเพื่อให้ผู้ใช้คอมพิวเตอร์สามารถสื่อสารถึงกัน ใช้ข้อมูลร่วมกัน หรือเพื่อแลกเปลี่ยนข้อมูลระหว่างกัน การเชื่อมโยงของระบบเครือข่ายจะผ่านช่องทางการสื่อสารต่างๆ กัน เช่น สายโทรศัพท์ สายไฟฟ้า หรือผ่านสื่อกลาง เช่น ไมโครเวฟ [8] เป็นต้น การแบ่งประเภทระบบเครือข่ายสามารถแบ่งได้จากลักษณะการติดตั้งทางภูมิศาสตร์ แบ่งได้ 3 แบบ ได้แก่

(1) เครือข่ายท้องถิ่น (Local Area Network หรือ LAN) เป็นเครือข่ายระยะใกล้ เช่น ภายในอาคารสำนักงาน เป็นต้น ระบบเครือข่ายชนิดนี้จะช่วยให้สะดวกในการติดต่อ ช่วยลดต้นทุน

(2) เครือข่ายระดับเมือง (Metropolitan Area Network หรือ MAN) เป็นเครือข่ายขนาดกลาง ใช้ภายในเมืองหรือจังหวัด เช่น เคเบิลทีวี

(3) เครือข่ายระดับประเทศ (Wide Area Network หรือ WAN) เป็นเครือข่ายที่มีขนาดใหญ่ ติดตั้งใช้งานในบริเวณกว้าง มีสถานีจุดเชื่อมมากมาย ต้องใช้สื่อกลางหลายชนิด เช่น ระบบคลื่นวิทยุ ไมโครเวฟ หรือดาวเทียม เป็นต้น

(4) ระบบเครือข่ายระหว่างประเทศ (International Network หรือ Inter-Net) เป็นระบบที่ติดต่อข้ามประเทศโดยใช้สายเคเบิล หรือดาวเทียม

จะเห็นได้ว่าระบบเครือข่ายช่วยให้เกิดความรวดเร็วในการติดต่อสื่อสาร ทำให้การส่งข้อมูลข่าวสารในยุคโลกาภิวัฒน์สามารถทำได้สะดวกสบายมากขึ้น ไม่ว่าจะอยู่ในส่วนใดของโลกก็สามารถส่งผ่านข้อมูลข่าวสารถึงกันได้ และแต่ละเครือข่ายก็สามารถเชื่อมกับเครือข่ายอื่นๆ ได้ โดยผ่านคอมพิวเตอร์ขนาดใหญ่ที่มีระบบปฏิบัติงานข่ายงาน (Network Operating System) เป็นซอฟท์แวร์ควบคุมข่ายงาน และมีแผ่นวงจรข่ายงาน (Network Interface Card) คอยควบคุมให้คอมพิวเตอร์ในเครือข่ายเดียวกันทำงานประสานกัน และมีฮาร์ดแวร์ ที่เรียกว่า “เกตเวย์ (Gateway)” คอมพิวเตอร์ในแต่ละจุดจะทำหน้าที่เสมือนเป็นตัวเชื่อมและควบคุม เรียกว่า “สะพาน (Bridge)” มีการเชื่อมคอมพิวเตอร์ให้ถูกต้องตามลักษณะที่เหมาะสม โดยจัดให้มีคอมพิวเตอร์ที่มีความสามารถสูงเครื่องหนึ่ง เป็นเครื่องกลางที่ทำหน้าที่ควบคุมเครือข่ายงานและแฟ้มข้อมูล ลักษณะเหมือนเป็น

---

[8] ระบบไมโครเวฟ เป็นระบบการสื่อสารแบบไม่มีสาย ชนิดที่เป็นคลื่นวิทยุที่มีความถี่ระหว่าง 300 Mhs และ 30 Ghs และเดินทางเป็นเส้นตรง อุปกรณ์ที่ใช้ในการรับส่ง คือ จานสัญญาณไมโครเวฟ ซึ่งมักติดตั้งในที่สูง ข้อดี คือสามารถส่งสัญญาณด้วยความถี่กว้าง และแทบจะไม่มีการรบกวนจากภายนอก ข้อเสียคือถ้าทิศทางการส่งมีสิ่งกีดขวางจะทำให้การส่งสัญญาณทำได้ไม่ดี

DPU

แม่ข่าย หรือตัวบริการแฟ้มข้อมูล (File Server) ให้คอมพิวเตอร์เครื่องอื่นๆ เชื่อมโยงเข้ามาหาคอมพิวเตอร์ที่เป็นแม่ข่ายตัวนี้ ลักษณะการเชื่อมโยงนี้ เรียกว่า "โทโพโลยี (Topology)

ข. ประโยชน์ของเครือข่ายคอมพิวเตอร์ การนำคอมพิวเตอร์เข้ามาประยุกต์ในการดำเนินงานต่างๆ โดยการเชื่อมโยงคอมพิวเตอร์หลายๆ เครื่องเข้าด้วยกัน จัดทำเป็นระบบเครือข่าย ทำให้เกิดความสะดวกสบายและรวดเร็วในการการสื่อสารข้อมูลระหว่างบุคคล เพราะปัจจุบันมีเครือข่ายคอมพิวเตอร์เชื่อมโยงไปทั่วโลก โดยเฉพาะเครือข่ายที่เรียกว่า "อินเตอร์เน็ต (Internet)" ซึ่งมีเครือข่ายเชื่อมโยงคอมพิวเตอร์ครอบคลุมไปทั่วโลกภายใต้มาตรฐานเดียวกัน มาตรฐานดังกล่าวทำให้คอมพิวเตอร์ในเครือข่ายพูดภาษาเดียวกัน ทำให้คนสามารถติดต่อและรับรู้ข่าวสารกันได้รวดเร็ว เป็นประโยชน์อย่างมากในทุกๆ ด้าน เช่น

(1) ด้านธุรกิจ เครือข่ายที่มีประโยชน์ทางธุรกิจ เช่น ธนาคาร มีระบบออนไลน์บนเครือข่ายช่วยให้สามารถสอบถามยอดเงิน หรือโอนเงินได้รวดเร็ว การติดต่อระหว่างสำนักงานใหญ่และสาขาก็สามารถทำได้อย่างสะดวกรวดเร็ว

(2) ด้านการศึกษา มีการศึกษาทางไกล (Tele Education) เป็นการค้นคว้าทางวิชาการ การแบ่งปันหรือถ่ายทอดความรู้ระหว่างบุคคลที่อยู่ห่างไกลกัน

(3) ด้านการแพทย์ มีการแพทย์ทางไกล (Tele Medicine) โดยนำระบบเครือข่ายมาใช้ในการเก็บทะเบียนประวัติคนไข้ โดยใช้ฐานข้อมูลร่วมกัน มีการปรึกษาวินิจฉัยโรค และรักษาผ่านเครือข่ายคอมพิวเตอร์

(4) ด้านความมั่นคงปลอดภัยระหว่างประเทศ เช่น การเก็บประวัติอาชญากรด้วยฐานข้อมูลเดียวกัน โดยทุกสถานีตำรวจมีเครือข่ายคอมพิวเตอร์ที่สามารถเรียกและตรวจสอบข้อมูลได้ ทำให้การปราบปรามอาชญากรรมสามารถทำได้รวดเร็วทันต่อเหตุการณ์

(5) ด้านการสื่อสาร โดยการส่งจดหมายอิเล็กทรอนิกส์ ที่เรียกว่า "E-Mail (Electronic Mail) ซึ่งช่วยให้การสื่อสารทางไกลสะดวกและรวดเร็ว เพราะสามารถสื่อสารกันได้ทั้งจดหมาย ภาพ หรือเสียง นอกจากนี้ยังมีบริการอื่นๆ อีกหลายชนิดบนเครือข่ายอินเตอร์เน็ต เช่น จดหมายข่าว หรือจดหมายเวียน (Mail) การใช้คอมพิวเตอร์บนเครื่องอื่น (Telnet) และการขนถ่ายแฟ้ม (FTP – File Transfer) เป็นต้น

(6) การประชุมทางไกล (Tele Conference) เป็นการประชุมของบุคคลที่อยู่คนละสถานที่และห่างไกลกัน อาจเป็นคนละห้อง คนละตึก คนละจังหวัด คนละประเทศ หรือคนละทวีป โดยอาศัยอุปกรณ์โทรคมนาคมสื่อสารถึงกัน ข่าวสารที่รับส่งถึงได้ทั้งตัวอักษร เสียง และภาพพร้อมๆ กัน โดยทั่วไปการประชุมทางไกลจะแบ่งเป็น 2 ประเภท ได้แก่

- การประชุมทางไกลเฉพาะเสียง (Audio Conference) เป็นการประชุมที่อาศัยระบบโทรศัพท์ หรือวงจรเช่าจากองค์การโทรศัพท์ หรือการสื่อสารแห่งประเทศ เมื่อผู้เข้าประชุมพร้อมจึงเริ่มประชุม โดยผู้เข้าร่วมประชุมทุกคนจะได้ยินเสียงพูดพร้อมๆ กันเสมือนนั่งประชุมอยู่ในที่เดียวกัน และผู้ดำเนินการประชุมเป็นผู้จัดระเบียบการพูด

- การประชุมทางไกลทั้งเสียงและภาพ (Video Conference) เป็นการประชุมที่ใช้สายโทรศัพท์ หรือวงจรพิเศษเป็นสื่อนำภาพ เสียง และข้อมูล ไปยังผู้เข้าร่วมประชุม การใช้บริการสื่อสารรวมระบบดิจิตอล (ISDN – Integrated Service Digital Network) นั้น ช่วยรวมบริการด้านเสียง ภาพ และข้อมูลไว้ในเครือข่ายเดียวกัน โดยใช้เคเบิลใยแก้วนำแสงต่อเข้ากับคู่สายเพียงคู่เดียวก็ทำงานได้ทั้งเสียงและภาพ

2.1.4 การเข้าถึง (Access) ข้อมูล

ก. ความหมายของคำว่า “การเข้าถึง (Access) ข้อมูล”

การเข้าถึง (Access) ข้อมูลเป็นคำที่ไม่ได้มีความหมายเป็นพิเศษสำหรับนักคอมพิวเตอร์โดยทั่วๆไป แต่มีความสำคัญสำหรับการศึกษาถึงการลักลอบเข้าถึงข้อมูลโดยปราศจากอำนาจในทางกฎหมาย ซึ่งถือเป็นการกระทำความผิดทางอาญา

ตามร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... มาตรา 5 ได้กล่าวถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กรณีที่มีการเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหนึ่งเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ

การเข้าถึงตามร่างมาตรา 5 หากเป็นการเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน เป็นความผิดตามร่างมาตรา 7 ในบางกรณีการกระทำความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 7 นี้อาจไม่จำต้องกระทำผิดฐานเข้าถึงระบบคอมพิวเตอร์ตามมาตรา 5 ก่อนก็ได้ เช่น การเอาแผ่นบันทึกข้อมูลของผู้อื่นที่มีการตั้งรหัสผ่านไว้ไปเปิดอ่านในระบบคอมพิวเตอร์ของตนเอง

และถ้าผู้ที่ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ นำมาตรการดังกล่าวไปเปิดเผยโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น เป็นความผิดตามร่างมาตรา 6

เกี่ยวกับความผิดตามร่างมาตรา 5 และมาตรา 7 นี้ มีความเห็นในอีกแง่มุมหนึ่งว่า หากมาตรการป้องกันการเข้าถึงนั้นเป็นมาตรการที่ไม่แน่นหนา ประหนึ่งบ้านที่ใช้กลอนประตูคุณภาพต่ำ การบุกรุกหรือการเข้าถึงกระทำได้ง่ายและอาจไม่ได้เกิดจากความตั้งใจ และเป็นไปได้ที่บุคคลในครอบครัวเดียวกันนั้นเองที่ต้องการใช้เครื่องคอมพิวเตอร์นั้น โดยไม่มีเจตนาร้าย ด้วยเหตุนี้

กฎหมายจึงได้บัญญัติไว้ให้เป็นความผิดอันยอมความได้ และกำหนดโทษไว้ไม่สูงนักและในการประชุมของคณะกรรมการกฤษฎีกา นักวิชาการ-ผู้เชี่ยวชาญทางคอมพิวเตอร์ท่านหนึ่งได้เปรียบเทียบความผิดข้างต้นไว้น่าฟังว่า หากเปรียบระบบคอมพิวเตอร์เป็นบ้านหลังหนึ่ง การเข้าถึงระบบคอมพิวเตอร์อันเป็นความผิดตามร่างมาตรา 5 นั้น ก็เสมือนกับการบุกรุกเข้าไปในบ้านของผู้อื่น การเข้าถึงข้อมูลคอมพิวเตอร์อันเป็นความผิดตามร่างมาตรา 7 ก็เสมือนว่าผู้บุกรุกนั้นนอกจากจะเข้าไปในบ้านหลังนั้นได้แล้ว ยังได้เข้าไปรื้อค้นเอกสารในตู้เก็บเอกสารในนั้นด้วย ส่วนความผิดตามร่างมาตรา ๖ นั้น เสมือนเป็นการนำกุญแจผีที่ไขเข้าไปในบ้านได้ แจกจ่ายให้กับบุคคลอื่นนั่นเอง[9]

กฎหมายของประเทศสหรัฐอเมริกา ได้ให้คำนิยาม คำว่า “การเข้าถึง (Access) ข้อมูล” ไว้ ดังนี้

การเข้าถึง (Access) หมายถึง การเข้าไปสู่ (Approach) สั่ง (Instruct) สื่อสารกับ (Communicate with) ใส่ข้อมูลเข้าไปเก็บไว้ (Store data in) ล้วงข้อมูลมา (Retrieve data from) หรือเอาประโยชน์จาก (Make use of any resources of) เครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์มาใช้

จากคำนิยามดังกล่าวสามารถแยกพิจารณาในส่วนที่สำคัญ ดังนี้

เข้าไปสู่ (Approach) หมายถึง การกระทำที่เป็นการเข้าไปหาสิ่งที่ต้องการ ซึ่งอยู่ภายในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

การสั่ง (Instruct) หมายถึง การกระทำที่เป็นการสั่งให้เครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ทำงานตามที่ต้องการ

การสื่อสาร (Communicate with) หมายถึง การกระทำที่เป็นการติดต่อกับเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ ด้วยวิธีการสื่อสาร เช่น การติดต่อผ่านสายโทรศัพท์ ฯลฯ เพื่อให้ได้ประโยชน์ตามที่ต้องการ

การใส่ข้อมูลเข้าไปเก็บไว้ (Store data in) หมายถึง การกระทำที่เป็นการใส่ข้อมูลเข้าไปเก็บไว้ในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เพื่อประโยชน์ที่จะได้จากการทำงานของเครื่องคอมพิวเตอร์ในภายหลัง

การล้วงข้อมูลมาจาก (Retrieve data from) หมายถึง การกระทำที่เป็นการเอาข้อมูลออกมาจากเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เพื่อประโยชน์ของตน

---

[9] แนวความคิดและหลักการของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ . นายสุนทร เปลี่ยนสี, นิติกร ๕ ฝ่ายกฎหมายกระบวนการยุติธรรมทางอาญา สำนักงานคณะกรรมการกฤษฎีกา

การเอาประโยชน์จาก (Make use of any resources of) หมายถึง การกระทำใดๆ ต่อเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เพื่อประโยชน์ของตน

ดังนั้น การเข้าถึงนี้ อาจเป็นการเข้าถึงโดยผู้กระทำผิดรู้หรือได้รหัสผ่านของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์มาโดยมิชอบ แล้วทำการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น หรืออาจเป็นการเข้าถึงผ่านระบบเครือข่าย ผู้กระทำผิดอาจเป็นผู้มีความรู้ด้านคอมพิวเตอร์ดีพอที่จะเจาะมาตรการป้องกันการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้นได้ สังเกตว่า ร่างกฎหมายฉบับนี้เอาผิดกับผู้ที่พยายามเจาะ (hacking or cracking) เข้าไปในระบบของผู้อื่นเลยทีเดียว ไม่คำนึงว่าเข้าไปโดยประสงค์อย่างไร เพียงแต่เข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงไว้ ก็เป็นความผิดสำเร็จทันที

ข. วิธีการเข้าถึง (Access) ข้อมูล ความเจริญก้าวหน้าด้านเทคโนโลยีในปัจจุบันทำให้ไม่จำเป็นที่จะต้องเข้าไปถึงคอมพิวเตอร์ที่บันทึกข้อมูลหลัก เพียงแต่มีคอมพิวเตอร์ส่วนบุคคล (Personal Computer : PC.) ที่ติดตั้งซอฟต์แวร์ในการติดต่อกับเครือข่ายและโมเด็มที่พ่วงคู่กับสายโทรศัพท์ ที่เรียกว่า “การต่อเชื่อมคอมพิวเตอร์เข้าสู่สายอินเตอร์เน็ต” ก็จะสามารถติดต่อสื่อสารกับคอมพิวเตอร์เครื่องที่ประสงค์จะเข้าถึง และใช้ข้อมูลภายในนั้นได้

ค. มาตรการรักษาความปลอดภัยของข้อมูลในคอมพิวเตอร์ เป้าหมายสำคัญของการรักษาความปลอดภัยที่แท้จริง คือ การปกป้องให้ข้อมูลนั้นเป็นความลับ มีความสมบูรณ์ถูกต้อง และคงอยู่ตลอดเวลาที่เก็บอยู่ในเครื่องคอมพิวเตอร์[10] ระบบการรักษาความปลอดภัยของข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์นั้น โดยทั่วไป อุปกรณ์ต่างๆ ของเครื่องคอมพิวเตอร์จะจำกัดการเข้าถึงโดยผู้ใช้ ซึ่งจะต้องระบุตัวผู้ใช้ (User Identification : User-ID) เอาไว้ โดยใช้รหัสผ่าน (Password) เพื่อใช้เป็นกุญแจในการเข้าสู่ระบบ

2.2 หลักเกณฑ์การคุ้มครองสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล

การให้ความคุ้มครองสิทธิของประชาชนจากการละเมิดสิทธิเสรีภาพของเจ้าพนักงานของรัฐ ไม่ว่าจะเป็นการดำเนินการจับกุม หรือการตรวจค้น ก่อนศตวรรษที่ 18 เป็นเหตุให้เจ้าพนักงานของรัฐมีอำนาจมากในการปฏิบัติหน้าที่โดยไม่มีหลักเกณฑ์ใดมาจำกัดอำนาจของเจ้าพนักงานเหล่านั้นได้ เช่น เจ้าพนักงานของรัฐในประเทศฝรั่งเศสสามารถจับบุคคลไปขังไว้โดยไม่

---

[10] เจนศักดิ์ ตั้งพันธุ์สุริยะ. (2543). **แรกเริ่มเรียนรู้ เรื่องรักษาความปลอดภัยให้ระบบคอมพิวเตอร์.** เรียบเรียงจาก Computer Security for Dummies ของ Peter T. Davis และ Barry D. Lewis. หน้า 27.

แจ้งข้อกล่าวหา และสามารถขังไว้ได้โดยไม่มีกำหนดเวลา[11] ในศตวรรษที่ 8 นักปราชญ์หลายท่าน เช่น มองเตสกิเออ ฯลฯ จึงได้สร้างแนวคิดเกี่ยวกับสิทธิมนุษยชนขึ้น เป็นการนำไปสู่แนวความคิดในการให้ความคุ้มครองสิทธิมนุษยชนมากขึ้นเห็นได้จากการจัดทำเอกสารที่เกี่ยวกับการให้ความคุ้มครองสิทธิของบุคคล เช่น ในประเทศสหรัฐอเมริกามีการจัดทำ The Declaration of Independence[12] และประเทศอังกฤษได้จัดทำ Magna Carta [13]

2.2.1 ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 เดิมการให้ความคุ้มครองสิทธิและเสรีภาพของบุคคลจะเป็นการให้ความคุ้มครองกันภายในรัฐใดรัฐหนึ่งเท่านั้น จนกระทั่งวันที่ 10 ธันวาคม ค.ศ. 1948 องค์การสหประชาชาติได้มีการประชุมและประกาศ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 เป็นการให้ความร่วมมือกันระหว่างประเทศเพื่อให้ความคุ้มครองสิทธิและเสรีภาพของบุคคล และพัฒนาไปในทิศทางเดียว กัน[14]

ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ได้กำหนดหลักเกณฑ์ที่สำคัญเกี่ยวกับการคุ้มครองสิทธิในความเป็นอยู่ทั่วไปของประชาชน ดังนี้ “บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นอยู่ส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือการถูกลบหลู่ในเกียรติยศ และชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับการคุ้มครองจากกฎหมายต่อการแทรกแซงหรือการลบหลู่ดังกล่าวนั้น” จากบทบัญญัติดังกล่าวเป็นการให้ความคุ้มครองความเป็นอยู่ทั่วไปในชีวิตส่วนตัวของบุคคลทั้งที่เป็นการดำเนินชีวิตประจำวัน การติดต่อสื่อสาร เป็นหลัก และยกเว้นในกรณีที่เพื่อประโยชน์สาธารณะ และมีกฎหมายอนุญาตให้ทำได้ แต่ก็ต้องมีการควบคุมมิให้มีการใช้อำนาจที่กระทบกระเทือนต่อสิทธิของประชาชนมากเกินไป สมัชชาสหประชาชาติจึงได้สร้างหลักการควบคุมการใช้อำนาจของรัฐขึ้นมา โดยประกาศใช้ “ประมวลจรรยาบรรณสำหรับเจ้าหน้าที่ผู้มีหน้าที่โดยกฎหมาย” (Code of Conduct for Law Enforcement) ซึ่งข้อที่ 1 บัญญัติให้เจ้าพนักงานผู้มีหน้าที่รักษากฎหมายต้องปฏิบัติตามกฎหมาย โดยมุ่งที่จะให้บริการแก่ประชาชน และคุ้มครองให้ประชาชนปลอดภัยจากการกระทำที่ผิดกฎหมาย และข้อ 2 บัญญัติ ให้เจ้าพนักงานผู้มีหน้าที่รักษา

---

[11] จงรักษ์ จุฑานนท์. (2525). **การคุ้มครองสิทธิของประชาชนต่อการถูกจับและตรวจค้นโดยไม่ชอบธรรม**. หน้า 1.

[12] กุลพล พลวัน. (2538). **พัฒนาการสิทธิมนุษยชน** (พิมพ์ครั้งที่ 3). หน้า 31

[13] กุลพล พลวัน. เล่มเดิม. หน้า 74

[14] กุลพล พลวัน. เล่มเดิม. หน้า 36.

กฎหมาย เมื่อมีการปฏิบัติตามกฎหมายที่เป็นการกระทบกระเทือนถึงสิทธิสิทธิดังกล่าว การกระทำนั้นต้องเคารพ และคุ้มครองศักดิ์ศรีความเป็นมนุษย์ และจะต้องไม่ทำลายล้างหลักสิทธิมนุษยชน[15]

2.2.2 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 นับแต่ประเทศไทยมีการเปลี่ยนแปลงการปกครองจากระบอบสมบูรณาญาสิทธิราชย์ (Absolute Monarchy) มาเป็นระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข (Liberal Democracy with the King as Head of the State) ในปี พ.ศ. 2475 ตั้งแต่นั้นการจัดทำรัฐธรรมนูญแห่งราชอาณาจักรไทยฉบับต่างๆ ก็เหมือนกับรัฐเสรีประชาธิปไตยอื่นๆ คือได้รับแรงบันดาลใจมาจาก "ลัทธิปัจเจกชน" (Individualism)[16] เช่นเดียวกับการจัดทำรัฐธรรมนูญของรัฐเสรีประชาธิปไตย (Liberal and Democratic State) อื่นๆ ซึ่งแนวความคิดของลัทธินี้สอนว่า "มนุษย์ทุกคนเกิดมามีศักดิ์ศรี" นั่นคือ ศักดิ์ศรีความเป็นมนุษย์ (Human Dignity) รัฐธรรมนูญของรัฐเสรีประชาธิปไตยทุกรัฐจึงได้บัญญัติรับรองและให้ความคุ้มครองศักดิ์ศรีความเป็นมนุษย์ของปัจเจกชนไว้อย่างชัดเจนเป็น "สิทธิและเสรีภาพขั้นพื้นฐาน" (Fundamental Rights and Liberties) ซึ่งรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 4 บัญญัติว่า "ศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของบุคคลย่อมได้รับความคุ้มครอง" มาตรา 26 บัญญัติว่า "การใช้อำนาจโดยองค์กรของรัฐทุกองค์กร ต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพตามรัฐธรรมนูญนี้" และมาตรา 27 บัญญัติว่า "สิทธิและเสรีภาพที่รัฐธรรมนูญนี้รับรองไว้โดยชัดแจ้ง โดยปริยาย หรือโดยคำวินิจฉัยของศาลรัฐธรรมนูญ ย่อมได้รับความคุ้มครองและผูกพันรัฐสภา คณะรัฐมนตรี ศาล และองค์กรอื่นของรัฐโดยตรงในการตรากฎหมาย การใช้บังคับกฎหมายและการตีความกฎหมายทั้งปวง" แสดงให้เห็นว่า ไม่ว่าสิทธิหรือเสรีภาพของบุคคลจะต้องอยู่ภายใต้ "ประโยชน์ส่วนรวม" (General Interest) หรือ "ประโยชน์สาธารณะ" (Public Interest) หรือ "ความมั่นคงแห่งชาติ" (National Security)

"สิทธิตามรัฐธรรมนูญ" นั้น ถือว่าเป็น "สิทธิตามกฎหมายมหาชน" (das subjektive oeffentliche Recht) หมายถึงอำนาจตามรัฐธรรมนูญหรือกฎหมายสูงสุดได้บัญญัติให้การรับรองคุ้มครองแก่ปัจเจกบุคคลในอันที่จะกระทำการใด หรือไม่กระทำการใด การให้อำนาจแก่ปัจเจกบุคคลดังกล่าวได้ก่อให้เกิดสิทธิเรียกร้องที่จะไม่ให้บุคคลใดแทรกแซงในสิทธิตามรัฐธรรมนูญของตน โดยเฉพาะอย่างยิ่งเรียกร้องต่อองค์กรของรัฐมิให้แทรกแซงในขอบเขตสิทธิของตน ในบางกรณีการรับรองดังกล่าวได้ก่อให้เกิดสิทธิเรียกร้องให้รัฐดำเนินการอย่างใดอย่างหนึ่ง

---

[15] ศุภฤกษ์ ศุกรเสพย์. (2545). **การค้นในที่รโหฐานของเจ้าพนักงานป้องกันและปราบปรามยาเสพติด**. หน้า 10.

[16] Pierre WIGNY. **Droit constitutionnel : Principle et droit prositif.** Tome premier, Bruxelles, Bruylant, 1952, pp. 257-258.

สิทธิตามรัฐธรรมนูญจึงเป็นความสัมพันธ์ระหว่างปัจเจกบุคคลต่อรัฐ และสิทธิตามรัฐธรรมนูญเป็นสิ่งที่ผูกพันองค์กรผู้ใช้อำนาจรัฐทั้งหลายที่จะต้องให้ความเคารพ ปกป้อง และคุ้มครองสิทธิตามรัฐธรรมนูญดังกล่าว เพื่อให้สิทธิตามรัฐธรรมนูญดังกล่าวมีผลในทางปฏิบัติ[17]

"เสรีภาพตามรัฐธรรมนูญ" หมายถึง อำนาจของบุคคลในอันที่จะกำหนดตนเอง (Self – determination) โดยอำนาจนี้บุคคลย่อมเลือกวิถีชีวิตของตนได้ด้วยตนเองตามใจปรารถนา เสรีภาพจึงเป็นอำนาจที่บุคคลมีอยู่เหนือตนเอง[18]

จะเห็นได้ว่ารัฐธรรมนูญฉบับปัจจุบันมีเจตนารมณ์ที่จะให้ความคุ้มครองสิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์ของประชาชนเป็นสำคัญ ดังจะเห็นได้จากบทบัญญัติในมาตรา 26 บัญญัติว่า "การใช้อำนาจโดยองค์กรของรัฐทุกองค์กร ต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพตามบทบัญญัติแห่งรัฐธรรมนูญนี้"

มาตรา 29 วรรคแรก บัญญัติว่า "การจำกัดสิทธิและเสรีภาพของบุคคลที่รัฐธรรมนูญรับรองไว้จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อการที่รัฐธรรมนูญนี้กำหนดไว้และเท่าที่จำเป็นเท่านั้น และจะกระทบกระเทือนต่อสาระสำคัญแห่งสิทธิและเสรีภาพนั้นมิได้"

และมาตรา 37 วรรคแรก บัญญัติว่า "บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบด้วยกฎหมาย

จากบทบัญญัติดังกล่าวที่กำหนดขึ้นเพื่อปกป้องสิทธิและเสรีภาพของประชาชนมิให้ถูกล่วงละเมิด แม้กฎหมายจะให้การรับรองเสรีภาพอย่างใดอย่างหนึ่งให้แก่บุคคลใดบุคคลหนึ่ง ย่อมมีผลก่อให้เกิดหน้าที่แก่ผู้อื่นด้วยเช่นกัน แต่หน้าที่ที่เกิดขึ้นกับผู้อื่นอันเนื่องมาจากการที่กฎหมายบัญญัติรับรองเสรีภาพให้แก่บุคคลหนึ่งนี้ เป็นแต่เพียงหน้าที่ที่จะต้องเคารพเสรีภาพของผู้ทรงเสรีภาพ และผู้ทรงเสรีภาพเองก็คงมีอำนาจตามกฎหมายแต่เพียงที่จะเรียกร้องให้ผู้อื่นละเว้นจากการรบกวนขัดขวางการใช้เสรีภาพของตนเท่านั้น หาได้มีอำนาจที่จะเรียกร้องให้ผู้อื่นกระทำการอย่างใดอย่างหนึ่งซึ่งมีลักษณะเป็นการส่งเสริมหรือช่วยเหลือการใช้เสรีภาพของตนด้วย

สิทธิและเสรีภาพตามรัฐธรรมนูญนั้นมีผลผูกพันโดยตรงต่ออำนาจนิติบัญญัติ อำนาจบริหารและอำนาจตุลาการ[19] เพราะอำนาจนิติบัญญัติ อำนาจบริหาร และอำนาจตุลาการ ต่างก็เป็น

---

[17] บรรเจิด สิงคะเนติ. (2543). **หลักพื้นฐานของสิทธิเสรีภาพ และศักดิ์ศรีความเป็นมนุษย์ตามรัฐธรรมนูญ พ.ศ. 2540**. หน้า 47.

[18] วรพจน์ วิศรุตพิชญ์. (2543). **สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540**. หน้า 22.

[19] บรรเจิด สิงคะเนติ. เล่มเดิม. หน้า 52.

อำนาจที่มาจากอำนาจอธิปไตย ซึ่งเป็นส่วนหนึ่งที่แสดงออกถึงความเป็นรัฐ นอกจากอาณาเขต และพลเมือง

ปัจจุบันพระราชบัญญัติ การสอบสวนคดีพิเศษ พ.ศ. 2547 มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคลซึ่งมาตรา ๒๙ ประกอบกับมาตรา ๓๑ มาตรา ๓๔ มาตรา ๓๕ มาตรา ๓๖ มาตรา ๓๗ มาตรา ๔๘ มาตรา ๕๘ มาตรา ๒๓๗ และมาตรา ๒๓๘ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย ได้แก่บทบัญญัติต่อไปนี้

มาตรา ๒๔ บัญญัติว่า "เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานสอบสวนคดีพิเศษมีอำนาจดังต่อไปนี้ด้วย

(๑) เข้าไปในเคหสถาน หรือสถานที่ใดๆ เพื่อตรวจค้น เมื่อมีเหตุสงสัยตามสมควรว่ามีบุคคลที่มีเหตุสงสัยว่ากระทำความผิดที่เป็นคดีพิเศษหลบซ่อนอยู่ หรือมีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้ ประกอบกับมีเหตุอันควรเชื่อว่าเนื่องจากการเนิ่นช้ากว่าจะเอาหมายค้นมาได้บุคคลนั้นจะหลบหนีไป หรือทรัพย์สินนั้นจะถูกโยกย้าย ซุกซ่อน ทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิม

(๒) ค้นบุคคล หรือยานพาหนะที่มีเหตุสงสัยตามสมควรว่ามีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้

(๓) มีหนังสือสอบถามหรือเรียกให้สถาบันการเงิน ส่วนราชการ องค์การ หรือหน่วยงานของรัฐ หรือรัฐวิสาหกิจ ส่งเจ้าหน้าที่ที่เกี่ยวข้องมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชีเอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(๔) มีหนังสือสอบถาม หรือเรียกบุคคลใดๆ มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชีเอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(๕) ยึด หรืออายัดทรัพย์สินที่ค้นพบ หรือที่ส่งมาดังกล่าวไว้ใน (๑) (๒) (๓) และ (๔) การใช้อำนาจตามวรรคหนึ่ง ให้พนักงานสอบสวนคดีพิเศษปฏิบัติตามข้อบังคับที่ กคพ. กำหนด เฉพาะการใช้อำนาจตามวรรคหนึ่ง (๑) นอกจากพนักงานสอบสวนคดีพิเศษต้องดำเนินการเกี่ยวกับวิธีการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาแล้ว ให้พนักงานสอบสวนคดีพิเศษแสดงความบริสุทธิ์ก่อนการเข้าค้น รายงานเหตุผลและผลการตรวจค้นเป็นหนังสือต่อผู้บังคับบัญชาเหนือขึ้นไป และบันทึกเหตุสงสัยตามสมควรและเหตุอันควรเชื่อที่ทำให้สามารถเข้าค้นได้เป็นหนังสือให้ไว้แก่ผู้ครอบครองเคหสถานหรือสถานที่ค้น แต่ถ้าไม่มีผู้ครอบครองอยู่ ณ ที่นั้น ให้พนักงาน

สอบสวนคดีพิเศษส่งมอบสำเนาหนังสือนั้นให้แก่ผู้ครอบครองดังกล่าวในทันทีที่กระทำได้ และหากเป็นการเข้าค้นในเวลากลางคืนภายหลังพระอาทิตย์ตก พนักงานสอบสวนคดีพิเศษผู้เป็นหัวหน้าในการเข้าค้นต้องเป็นข้าราชการพลเรือนตำแหน่งตั้งแต่ระดับ ๗ ขึ้นไปด้วย

ให้พนักงานสอบสวนคดีพิเศษผู้เป็นหัวหน้าในการเข้าค้นส่งสำเนาบันทึกเหตุสงสัยตามสมควรและเหตุอันควรเชื่อตามวรรคสาม และสำเนาบันทึกการตรวจค้นและบัญชีทรัพย์ที่ยึดหรืออายัดต่อศาลจังหวัดที่มีอำนาจเหนือท้องที่ที่ทำการค้น หรือศาลอาญาในเขตกรุงเทพมหานครภายในสี่สิบแปดชั่วโมงหลังจากสิ้นสุดการตรวจค้น เพื่อเป็นหลักฐาน

พนักงานสอบสวนคดีพิเศษระดับใดจะมีอำนาจหน้าที่ตามที่ได้กำหนดไว้ตามวรรคหนึ่งทั้งหมดหรือแต่บางส่วน หรือจะต้องได้รับอนุมัติจากบุคคลใดก่อนดำเนินการให้เป็นไปตามที่อธิบดีกำหนดโดยทำเอกสารให้ไว้ประจำตัวพนักงานสอบสวนคดีพิเศษผู้ได้รับอนุมัตินั้นและพนักงานสอบสวนคดีพิเศษผู้นั้นต้องแสดงเอกสารดังกล่าวต่อบุคคลที่เกี่ยวข้องทุกครั้ง

มาตรา 25 ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษพนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

(๑) มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ

(๒) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

(๓) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวันโดยกำหนดเงื่อนไขใดๆ ก็ได้ และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อพนักงานสอบสวนคดีพิเศษได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

บรรดาข้อมูลข่าวสารที่ได้มาตามวรรคหนึ่ง ให้เก็บรักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษซึ่งได้รับอนุญาตตามวรรคหนึ่ง และให้ใช้ประโยชน์ในการสืบสวนหรือใช้เป็นพยานหลักฐานเฉพาะในการดำเนินคดีพิเศษดังกล่าวเท่านั้น ส่วนข้อมูลข่าวสารอื่นให้ทำลายเสียทั้งสิ้น ทั้งนี้ ตามข้อบังคับที่ กคพ. กำหนด

มาตรา 26 ห้ามมิให้บุคคลใดเปิดเผยข้อมูลข่าวสารที่ได้มาเนื่องจากการดำเนินการตามมาตรา 25 เว้นแต่เป็นข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษซึ่งได้รับอนุญาตตามมาตรา 25 และเป็นการปฏิบัติตามอำนาจหน้าที่หรือตามกฎหมายหรือตามคำสั่งศาล

จะเห็นได้ว่าอำนาจที่กฎหมายมอบให้กับพนักงานสอบสวนคดีพิเศษตามบทบัญญัติข้างต้นเป็นการกระทำที่กระทบต่อสิทธิเสรีภาพของประชาชน และจะทำให้เกิดการใช้อำนาจที่ไร้ขอบเขต และประเทศไทยเองก็ยังไม่มีบทบัญญัติของกฎหมายที่ให้การคุ้มครองสิทธิในชีวิตส่วนตัวของบุคคลโดยตรง แต่หากพิจารณาบทกฎหมายที่มีในปัจจุบันแล้วจะพบว่า กฎหมายที่ให้ความคุ้มครองสิทธิส่วนบุคคลมีมากมายพอสมควร ไม่เฉพาะที่ปรากฏอยู่ในประมวลกฎหมายอาญาในความผิดฐานหมิ่นประมาท ความผิดฐานดูหมิ่น ความผิดฐานบุกรุก และความผิดฐานก่อความเดือดร้อนรำคาญเท่านั้น ในประมวลกฎหมายแพ่งและพาณิชย์ ก็มีอยู่ในมาตรา 420 ซึ่งบัญญัติว่า "ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น"

คำว่า "สิทธิอย่างหนึ่งอย่างใด" นี้ก็น่าจะมีความหมายถึง สิทธิในชีวิตส่วนตัวด้วย ซึ่งจะต้องพิจารณากันเป็นกรณีๆ ไป

จะเห็นได้ว่ากฎหมายไทยถือว่าการละเมิดสิทธิในชีวิตส่วนตัวนั้น ถือเป็นความผิดฐานละเมิดตามปกติธรรมดาไม่ได้แยกเป็นพิเศษเหมือนสหรัฐอเมริกา โดยจะต้องพิจารณาถึงเจตนาว่าเป็นการกระทำโดยจงใจหรือประมาทเลินเล่อที่กระทำต่อบุคคลอื่นโดยมิชอบด้วยกฎหมาย แต่การล่วงละเมิดสิทธิในชีวิตส่วนตัวของบุคคลในสหรัฐอเมริกานั้นจะพิจารณาจากผลของการกระทำเป็นสำคัญ และประเทศไทยยังไม่ปรากฏว่ามีคดีเกี่ยวกับการละเมิดสิทธิในชีวิตส่วนตัวขึ้นสู่ศาลดังเช่นที่เกิดขึ้นในประเทศสหรัฐอเมริกา

แม้ว่ารัฐธรรมนูญของประเทศสหรัฐอเมริกาจะไม่มีการกล่าวถึงสิทธิในชีวิตส่วนตัวไว้โดยตรง แต่ศาลสูงของสหรัฐอเมริกาก็ได้วินิจฉัยรับรองว่าสิทธิในชีวิตส่วนตัวเสมือนเป็นสิทธิประการหนึ่งในรัฐธรรมนูญ โดยเฉพาะในคดี Griswold V. Connecticut 381 U.S. 479 (1965) ศาล

สูงสหรัฐได้วินิจฉัยไว้อย่างชัดเจนว่า เจตนารมณ์ของรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 1 เป็นเสมือนศูนย์รวมความรู้ที่ทุกคนไขว่คว้าได้ สิทธิเสรีภาพในการพูด และการพิมพ์โฆษณา ไม่เพียงแต่จะหมายถึงการพูดและการพิมพ์เท่านั้น แต่รวมไปถึงสิทธิในการจำหน่ายจ่ายแจก

ขณะเดียวกันบทบัญญัติรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 3 และ 4 ก็บัญญัติห้ามมิให้บุกรุกเข้าไปในเคหสถานของบุคคลอื่นโดยปราศจากความยินยอม และสิทธิของบุคคลที่จะมีความปลอดภัยในร่างกาย เคหสถาน เอกสาร และทรัพย์สิ่งของจากการตรวจค้น จับกุม ยึดโดยไม่มีเหตุอันสมควร และในบทบัญญัติรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 9 ก็บัญญัติคุ้มครองสิทธิของบุคคลที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองในคดีอาญาและรับรองว่าบรรดาสิทธิต่างๆ ในรัฐธรรมนูญจะตีความให้เป็นการปฏิเสธหรือลิดรอนสิทธิของผู้อื่นไม่ได้

สรุปแล้วบทบัญญัติรัฐธรรมนูญของสหรัฐอเมริกาล้วนแฝงไว้ด้วยสิทธิในชีวิตส่วนบุคคลแทบทั้งสิ้น จึงไม่อาจปฏิเสธได้ว่าสิทธิส่วนบุคคลเป็นสิทธิประการหนึ่ง ซึ่งย่อมได้รับการรับรองโดยกฎหมายโดยชอบ หากผู้ใดละเมิดก็จะมีความผิด โดยยึดถือแนวความคิดคล้ายๆกับการหมิ่นประมาทในตัวของมันเอง (Libel perse)

2.2.3 กฎหมายวิธีพิจารณาความอาญา บทบัญญัติสำคัญของกฎหมายวิธีพิจารณาความอาญาจะอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งเดิมบทบัญญัติที่มีก็เป็นไปเพื่อความสะดวกในการใช้อำนาจของรัฐ การคำนึงถึงสิทธิเสรีภาพส่วนบุคคลมีเพียงส่วนน้อย แต่ได้ให้ความสำคัญมากขึ้นในรัฐธรรมนูญฉบับปัจจุบัน[20]

2.2.3.1 สถานะของผู้ถูกกล่าวหา บทบัญญัติที่ให้ความสำคัญต่อสิทธิเสรีภาพส่วนบุคคลของผู้ถูกกล่าวหา ได้แก่ มาตรา 165 วรรคสาม บัญญัติว่า “ก่อนที่ศาลประทับฟ้องมิให้ถือว่าจำเลยอยู่ในฐานะเช่นนั้น” นั่นคือ ก่อนที่ผู้ที่ถูกผู้เสียหายฟ้องถูกศาลประทับฟ้องยังไม่ถือเป็น “จำเลย” ผู้ถูกกล่าวหาในปัจจุบันจึงไม่ถือเป็นวัตถุแห่งการซักฟอกหรือเป็น “กรรมในคดี” (Prozess-objekt) อีกต่อ แต่เป็น “ประธานในคดี” (Prozess-subjekt) [21] ซึ่งสอดคล้องกับบทบัญญัติในรัฐธรรมนูญมาตรา 241 วรรคหนึ่ง บัญญัติว่า “ในคดีอาญา ผู้ต้องหาหรือจำเลยย่อมมีสิทธิได้รับการสอบสวนหรือการพิจารณาคดีด้วยความเร็ว ต่อเนื่อง และเป็นธรรม”

2.2.3.2 สิทธิของผู้ถูกกล่าวหา สิทธิของผู้ต้องหาที่จะไม่ให้การ เป็นสิทธิของผู้ถูกกล่าวหาในทางอยู่เฉย ซึ่งเป็นสิทธิที่จะตัดสินใจในคดีด้วยตนเอง ในมาตรา 134 บัญญัติว่า “เมื่อผู้ต้องหาเต็มใจให้การอย่างใด ก็ให้จดคำให้การไว้ ถ้าผู้ต้องหาไม่เต็มใจให้การเลยก็ให้บันทึกไว้”

---

[20] คณิต ณ นคร. เล่มเดิม. หน้า 31.

[21] คณิต ณ นคร. เล่มเดิม. หน้า 102.

และในชั้นศาล มาตรา 174 บัญญัติว่า "ถ้าจำเลยไม่ยอมให้การ ก็ให้ศาลจดรายงานไว้และพิจารณาต่อไป" และเพื่อประกันสิทธิในการให้การหรือไม่ให้การของจำเลย มาตรา 135 บัญญัติว่า "ห้ามมิให้พนักงานสอบสวนทำหรือจัดให้ทำการใดๆ ซึ่งเป็นการล่อลวง หรือขู่เข็ญ หรือให้สัญญากับผู้ต้องหาเพื่อจูงใจให้เขาให้การอย่างใดๆ ในเรื่องที่ต้องหานั้น"

การล่อลวง หรือขู่เข็ญ หรือให้สัญญา ซึ่งเป็นการกระทำที่มิชอบด้วยกฎหมายตามที่บัญญัติไว้ในมาตรา 135 นั้น เป็นเพียงการกระทำต้องห้ามที่กฎหมายบัญญัติเป็นตัวอย่างไว้เท่านั้น แต่ความหมายที่บทบัญญัติในมาตรานี้ต้องการแสดงให้ปรากฏก็คือ "การกระทำที่เป็นการละเมิดเสรีภาพในการตัดสินใจของผู้ต้องหา" ทุกสถาน[22]

บทบัญญัติที่ถือว่าขัดแย้งกับบทบัญญัติที่ให้ความคุ้มครองสิทธิของผู้ถูกกล่าวหาในทางอยู่เฉย ได้แก่ มาตรา 132 บัญญัติว่า "เพื่อประโยชน์แห่งการรวบรวมพยานหลักฐาน พนักงานสอบสวนมีอำนาจตรวจค้นผู้ต้องหา จำเลยหรือพิมพ์ลายนิ้วมือ ลายมือหรือลายเท้า" เป็นบทบัญญัติที่แสดงให้เห็นถึงอำนาจของรัฐในการแสวงหาพยานหลักฐานจากผู้ต้องหา หรือจำเลยเพื่อประโยชน์ในการรวบรวมพยานหลักฐาน โดยไม่จำเป็นจะต้องได้รับความยินยอมจากผู้ต้องหาหรือจำเลยดังกล่าว เพียงแต่การตรวจค้นนั้น มาตรา 85 วรรคหนึ่ง บัญญัติว่า "เจ้าพนักงานผู้จับหรือรับตัวผู้ถูกจับไว้ มีอำนาจค้นตัวผู้ต้องหา" และวรรคสอง บัญญัติว่า "การค้นนั้นจักต้องทำโดยสุภาพ ถ้าค้นตัวหญิงต้องให้หญิงอื่นเป็นผู้ค้น" ซึ่งแสดงถึงความเคารพสถานะความเป็นประธานในคดีของผู้ต้องหา

2.2.3.3 สถานะของผู้ต้องหา มาตรา 2 (2) นิยามคำว่า "ผู้ต้องหา" ว่าหมายความถึงบุคคลผู้ถูกหาว่าได้กระทำผิด แต่ยังมิได้ถูกฟ้องต่อศาล จากคำนิยาม บุคคลที่จะมีสถานะเป็นผู้ต้องหาตามกฎหมายจึงต้องเป็นบุคคลที่มีผู้กล่าวหาบุคคลนั้นว่าได้กระทำความผิดอาญาต่อเจ้าพนักงาน หรือเจ้าพนักงานกล่าวหาเอง

ในการกล่าวหาต่อเจ้าพนักงาน มาตรา 2 (7) อาจทำในรูปของคำร้องทุกข์ของผู้เสียหาย หรือตามมาตรา 2 (8) คำกล่าวโทษโดยบุคคลอื่น

2.2.3.4 สถานะของจำเลย มาตรา 2 (3) นิยามคำว่า "จำเลย" ว่าหมายถึงบุคคลซึ่งถูกฟ้องยังศาลแล้วโดยข้อหาว่าได้กระทำความผิด

ดังนั้นจะถือว่าบุคคลซึ่งถูกฟ้องยังศาลแล้วเป็นจำเลยในทันทีที่ยื่นฟ้องจะต้องพิจารณาจากผู้ฟ้องเป็นหลัก หากพนักงานอัยการเป็นผู้ฟ้อง ผู้ถูกฟ้องจะตกเป็นจำเลยทันทีโดยไม่ต้องมีการไต่สวนมูลฟ้องก่อนหรือไม่ แต่ในกรณีที่ผู้เสียหายเป็นผู้ฟ้อง มาตรา 165 วรรคสามตอนท้าย บัญญัติ

---

[22] คณิต ณ นคร. เล่มเดิม. หน้า 105..

ว่า “ก่อนที่ศาลจะประทับฟ้องมิให้ถือว่าจำเลยอยู่ในฐานะเช่นนั้น” ดังนั้นก่อนศาลประทับฟ้องผู้ถูกฟ้องจึงยังไม่ตกเป็นจำเลย

2.2.3.5 การแสวงหาพยานหลักฐาน พยานหลักฐานเป็นเครื่องมือประการหนึ่งในการดำเนินคดีอาญาที่มีความสำคัญมาก ซึ่งในคดีอาญาพยานหลักฐานทุกชนิดรับฟังได้ ดังจะเห็นได้จากมาตรา 226 บัญญัติว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ให้อ้างเป็นพยานหลักฐานได้แต่ต้องเป็นพยานหลักฐานชนิดที่มิได้เกิดจากแรงจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบด้วยประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน”

กระบวนการสำคัญชั้นต้นในการดำเนินคดีอาญา ได้แก่ การสืบสวนและการสอบสวน ซึ่งบทบัญญัติดังกล่าวถือเป็นหลักเบื้องต้นทั่วไปเกี่ยวกับพยานหลักฐานที่แสดงสถานะและความเป็นอิสระในการแสวงหาพยานหลักฐาน แต่สำหรับปัญหาอาชญากรรมที่มีอยู่ในปัจจุบัน เพื่อให้การบังคับใช้กฎหมายป้องกันและปราบปรามอาชญากรรมสำคัญๆ ให้มีประสิทธิภาพมากขึ้นจึงมีการบัญญัติ พระราชบัญญัติ การสอบสวนคดีพิเศษ พ.ศ. 2547 ขึ้น

โดยกฎหมายฉบับนี้ได้กำหนดลักษณะของอาชญากรรมที่เป็นคดีพิเศษแตกต่างไปจากอาชญากรรมธรรมดา เนื่องจากเป็นอาชญากรรมที่มีลักษณะพิเศษ เช่น อาชญากรรมทางเศรษฐกิจหรืออาชญากรรมทางธุรกิจ มีผลกระทบที่รุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของสังคม ประโยชน์ส่วนรวมของประชาชน หรือความมั่นคงของประเทศความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของประเทศ หรือคดีอาญาที่มีผู้มีอิทธิพลเป็นผู้ร่วมกระทำความผิด รวมทั้งอาชญากรรมที่เป็นองค์กรอาชญากรรม และอาชญากรรมข้ามชาติด้วย เป็นอาชญากรรมที่ให้ผลตอบแทนแก่ผู้ประกอบอาชญากรรมเป็นอย่างมาก ทั้งนี้ วิธีการและลักษณะการกระทำความผิดมีความซับซ้อนเป็นการยากที่เจ้าหน้าที่ของรัฐบาลจะเข้าถึงผู้เป็นตัวการที่อยู่เบื้องหลัง เพื่อนำมาดำเนินคดีและลงโทษตามกฎหมายได้ เนื่องจากขาดความรู้ความเชี่ยวชาญและเทคนิคเฉพาะด้านในการสืบสวนสอบสวนเพื่อรวบรวมพยานหลักฐานสำหรับการดำเนินคดี

ดังนั้นจึงมีการกำหนดมาตรการและวิธีการต่างๆ ที่เพิ่มประสิทธิภาพในการปฏิบัติหน้าที่ของพนักงานสอบสวนคดีพิเศษ เช่น การกำหนดให้มีคุณสมบัติเบื้องต้นและคุณสมบัติพิเศษ การผ่านการอบรมตามหลักสูตรที่กำหนด และการผ่านการประเมินความรู้ความสามารถ เป็นต้น นอกจากการเพิ่มประสิทธิภาพให้กับเจ้าหน้าที่สืบสวนสอบสวนโดยเฉพาะแล้ว กฎหมายยังให้อำนาจลักษณะพิเศษไว้ด้วย เพื่อแก้ไขปัญหาความบกพร่องของกระบวนการยุติธรรมให้มีประสิทธิภาพมากขึ้น เนื่องจากระบบการสอบสวนในปัจจุบันยังไม่สามารถแก้ไขปัญหาความบกพร่องของพยานหลักฐานในคดีบางประเภทได้ รวมทั้งระบบการสอบสวนที่มีอยู่แต่เดิม จะเห็น

ได้จากอาชญากรรมที่มีความเชี่ยวชาญในการใช้เทคโนโลยีระดับสูงในการประกอบอาชญากรรม ในขณะเดียวกันก็ใช้ความรู้ความเชี่ยวชาญในการปกปิดซ่อนเร้นทำลายพยานหลักฐาน

เพื่อการแสวงหาพยานหลักฐาน และนำตัวผู้กระทำความผิดมาลงโทษให้ได้ โดยอำนาจหน้าที่หลักของพนักงานสอบสวน ตามมาตรา 2 (6) นิยามว่า "พนักงานสอบสวน หมายความถึงเจ้าพนักงานซึ่งกฎหมายให้อำนาจและหน้าที่ทำการสอบสวน" และมาตรา 121 วรรคหนึ่ง บัญญัติว่า "พนักงานสอบสวนมีอำนาจสอบสวนคดีอาญาทั้งปวง" ซึ่งเป็นบทบัญญัติถึงอำนาจในการสอบสวนของพนักงานสอบสวน

การสอบสวนโดยทั่วไปจะเริ่มเมื่อรู้เรื่องความสงสัยว่ามีการกระทำความผิดอาญาเกิดขึ้น แต่การรู้นั้นสามารถรู้ได้ 2 ทาง ได้แก่ เมื่อมีการร้องทุกข์หรือการกล่าวโทษ และรู้เองซึ่งพิจารณาจากฐานความผิดอาญาประกอบ นั่นคือหากเป็นการกระทำความผิดที่เกี่ยวข้องกับประโยชน์ได้เสียของประชาชนส่วนรวม พนักงานสอบสวนก็ต้องทำการสอบสวนโดยไม่ชักช้า

โดยหลักจุดประสงค์ในการรวบรวมพยานหลักฐานก็เพื่อความน่าเชื่อถือของพยานหลักฐานเหล่านั้น แต่ปัญหาในทางปฏิบัติหรือปัญหาทางเทคนิคของคดีพิเศษคือปัญหาในการแสวงหาพยานหลักฐาน ซึ่งไม่มีประจักษ์พยานเพราะผู้กระทำความผิดจะไม่มีส่วนเกี่ยวข้องกับพยานหลักฐานโดยตรง หรือสามารถทำลายพยานหลักฐานได้โดยง่าย ดังนั้นพนักงานสอบสวนจึงต้องมีความรู้ความเชี่ยวชาญสำหรับวิธีและมาตรการพิเศษที่จะใช้ในการแสวงหาพยานหลักฐานเพื่อนำมาดำเนินคดีกับผู้กระทำความผิดให้ได้

สำหรับ พระราชบัญญัติ การสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 21 (1) บัญญัติว่า

"(๑) คดีความผิดทางอาญาตามกฎหมายที่กำหนดไว้ในบัญชีท้ายพระราชบัญญัตินี้ และที่กำหนดในกฎกระทรวงโดยการเสนอแนะของ กคพ. โดยคดีความผิดทางอาญาตามกฎหมายดังกล่าว จะต้องมีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้

(ก) คดีความผิดทางอาญาที่มีความซับซ้อน จำเป็นต้องใช้วิธีการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเป็นพิเศษ

(ข) คดีความผิดทางอาญาที่มีหรืออาจมีผลกระทบอย่างรุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน ความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของประเทศ

(ค) คดีความผิดทางอาญาที่มีลักษณะเป็นการกระทำความผิดข้ามชาติที่สำคัญ หรือเป็นการกระทำขององค์กรอาชญากรรม หรือ

(ง) คดีความผิดทางอาญาที่มีผู้ทรงอิทธิพลที่สำคัญเป็นตัวการ ผู้ใช้หรือผู้สนับสนุน

ทั้งนี้ ตามรายละเอียดของลักษณะของการกระทำความผิดที่ กคพ. กำหนด

DPU

(๒) คดีความผิดทางอาญาอื่นนอกจาก (๑) ตามที่ กคพ. มีมติด้วยคะแนนเสียงไม่น้อยกว่าสองในสามของกรรมการทั้งหมดเท่าที่มีอยู่

ในคดีที่มีการกระทำอันเป็นกรรมเดียวผิดต่อกฎหมายหลายบท และบทใดบทหนึ่งจะต้องดำเนินการโดยพนักงานสอบสวนคดีพิเศษตามพระราชบัญญัตินี้ หรือคดีที่มีการกระทำความผิดหลายเรื่องต่อเนื่องหรือเกี่ยวพันกัน และความผิดเรื่องใดเรื่องหนึ่งจะต้องดำเนินการโดยพนักงานสอบสวนคดีพิเศษตามพระราชบัญญัตินี้ ให้พนักงานสอบสวนคดีพิเศษมีอำนาจสืบสวนสอบสวนสำหรับความผิดบทอื่นหรือเรื่องอื่นด้วย และให้ถือว่าคดีดังกล่าวเป็นคดีพิเศษ

บรรดาคดีใดที่ได้ทำการสอบสวนเสร็จแล้วโดยพนักงานสอบสวนคดีพิเศษ ให้ถือว่าการสอบสวนนั้นเป็นการสอบสวนในคดีพิเศษตามพระราชบัญญัตินี้แล้ว...”

ดังนั้นคดีพิเศษที่เจ้าพนักงานสอบสวนคดีพิเศษจะทำการสอบสวนได้จะต้องมีลักษณะตามที่กฎหมายบัญญัติเอาไว้ข้างต้น

โดยลักษณะพิเศษของคดีพิเศษทำให้การรวบรวมพยานหลักฐานเป็นไปอย่างยากลำบาก ทำให้การสอบสวนขาดประสิทธิภาพ พยานหลักฐานขาดความน่าเชื่อถือ ตามปกติกฎหมายจึงกำหนดให้พนักงานสอบสวนคดีพิเศษมีอำนาจพิเศษในการแสวงหาพยานหลักฐานดังกล่าวโดยการขออนุญาตต่อศาล เช่นการดักฟังวิทยุหรือโทรศัพท์ การเข้าสู่ข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์

เมื่อกฎหมายให้สิทธิแก่บุคคลหนึ่งก็ย่อมก่อให้เกิดหน้าที่แก่บุคคลอื่นในอันที่จะไม่ก้าวล่วงต่อสิทธิส่วนบุคคลนี้ และหากมีการก้าวล่วงต่อสิทธิส่วนบุคคล เจ้าของสิทธิชอบที่จะได้รับการแก้ไขเยียวยา คือ การเรียกร้องให้ชดใช้ค่าเสียหายหรือกระทำการใดๆ เพื่อทดแทนความเสียหายหรือกำหนดโทษทางอาญาแก่ผู้ที่กระทำความผิดตามบทบัญญัติของกฎหมาย

การที่เจ้าหน้าที่ของรัฐผู้มีอำนาจมีหน้าที่ในการแสวงหา สืบสวน และสอบสวนเพื่อนำตัวผู้ที่กระทำความผิดมาลงโทษ ดังนั้นการปฏิบัติหน้าที่ของเจ้าหน้าที่อาจจะเข้าไปก้าวล่วงในสิทธิส่วนบุคคลของแต่ละคนได้โดยง่าย ดังนั้น การศึกษาในส่วนที่เกี่ยวกับสิทธิส่วนบุคคลจึงเป็นเรื่องที่ไม่อาจมองข้ามไปได้ เพราะเจ้าหน้าที่ของรัฐก็ไม่ใช่บุคคลที่ได้รับการยกเว้นใดๆ จากความรับผิดในการก้าวล่วงต่อสิทธิส่วนบุคคลของผู้อื่น แม้กฎหมายจะให้อำนาจเจ้าหน้าที่ของรัฐในการใช้ดุลพินิจเพื่อเป็นมาตรการเสริมที่จะช่วยในการบังคับใช้กฎหมายให้มีประสิทธิภาพมากยิ่งขึ้น แต่การใช้ดุลพินิจของเจ้าหน้าที่ของรัฐก็เป็นอันตรายต่อสิทธิส่วนบุคคลเช่นกัน การใช้ดุลพินิจของเจ้าหน้าที่ของรัฐจึงต้องอยู่ภายใต้กฎหมาย โดยเฉพาะในเรื่องที่เกี่ยวกับชีวิตส่วนตัวของบุคคลเจ้าหน้าที่ของรัฐอาจมีความผิดฐานละเมิด ดังนั้นเจ้าหน้าที่ของรัฐจึงต้องปฏิบัติหน้าที่ด้วยความระมัดระวังมิให้ผู้อื่นได้รับความเดือดร้อนจากการละเมิดสิทธิส่วนบุคคล

กฎหมายว่าด้วยสิทธิในชีวิตส่วนตัว (Law of Privacy) ของต่างประเทศได้บัญญัติถึงการกระทำบางอย่างซึ่งถึงแม้ว่าจะไม่เป็นถึงกับเป็นการโฆษณาหมิ่นประมาท หรือทำให้บุคคลอื่นเสื่อมเสียเกียรติยศ ชื่อเสียงโดยตรง แต่ก็อาจมีลักษณะที่เป็นการล่วงละเมิดต่อสิทธิเสรีภาพในความเป็นอยู่ส่วนตัวของบุคคลอย่างเห็นได้ชัด เช่น คอยติดตามบุคคลอื่นตลอดเวลาจนก่อให้เกิดความรำคาญ หรือการเข้าตรวจสอบข้อมูลส่วนบุคคลที่บันทึกไว้ในเครื่องคอมพิวเตอร์ ซึ่งเป็นการกระทำความผิดฐานละเมิดตามหลักกฎหมายแพ่งก็ไม่ชัดเจน เพราะผู้กระทำหาได้ทำให้เกิดความเสียหายแก่ร่างกาย เกียรติยศ ชื่อเสียงของบุคคลนั้นโดยมิชอบด้วยกฎหมายไม่ แต่การกระทำดังกล่าวเป็นที่แน่นอนว่าย่อมทำให้บุคลนั้นต้องสูญเสียความเป็นอิสระส่วนตัวไป เพราะการถูกสอดแทรกหรือเกี่ยวข้องจากการกระทำของเจ้าหน้าที่ของรัฐ ซึ่งย่อมต้องขัดกับความต้องการส่วนบุคคลแน่นอน

การพิจารณาเรื่องสิทธิส่วนบุคคลในเบื้องต้น ผู้พิจารณาจะต้องคำนึงถึงอยู่เสมอว่ากฎหมายว่าด้วยสิทธิในชีวิตส่วนตัวไม่มีรูปแบบมาตรฐาน (Uniform) เช่นเดียวกับกฎหมายลักษณะอื่นๆ เพราะลักษณะที่จะถือเป็นการละเมิดสิทธิส่วนบุคคลมีความเห็นหลากหลายแตกต่างกันไปตามสภาพเศรษฐกิจ สังคม และวัฒนธรรมของแต่ละประเทศ เพราะการละเมิดสิทธิส่วนบุคคลเป็นเรื่องเกี่ยวกับความรู้สึกของแต่ละคนอันมีลักษณะทำให้เกิดความเสียหายต่อความเป็นส่วนตัวของเขา ขณะเดียวกันก็ต้องระลึกอยู่เสมอว่าคำพิพากษาหรือกฎหมายที่เกี่ยวกับสิทธิส่วนบุคคลที่มีนั้นเป็นสิ่งที่แสดงออกถึงความพยายามที่จะจุดดุลยภาพระหว่างผลประโยชน์สาธารณะกับสิทธิส่วนบุคคลให้เกิดความพอดี

สิทธิส่วนบุคคล (Right of Privacy) ในความหมายที่แคบที่สุดอาจกล่าวได้ว่า หมายถึงสิทธิที่จะอยู่โดยลำพังปราศจากการรบกวน (The right to be let alone) และเป็นสิทธิที่ได้รับการกล่าวถึงมากที่สุดในช่วงปี ค.ศ. 1980 เพราะเป็นช่วงเวลาที่ประเทศสหรัฐอเมริกาได้รับการขนานนามว่าเป็นสังคมแห่งข่าวสาร กล่าวคือ อิสระของข่าวสารที่ประชาชนหรือสื่อมวลชนจะสามารถเข้าล่วงรู้และนำออกเผยแพร่สู่สาธารณชนได้รับการยอมรับเป็นอย่างมาก ขณะเดียวกันก็เป็นเรื่องยากที่จะเก็บข้อมูลข่าวสารของแต่ละคนไว้โดยปราศจากการแทรกแซงจากเจ้าหน้าที่ของรัฐ หรือเอกชนที่ต่างมุ่งแสวงหาผลประโยชน์ในเชิงธุรกิจของตนเป็นสำคัญ[23]

แต่เนื่องจากลักษณะของการสอบสวนคดีพิเศษต่างๆ จำเป็นที่จะต้องมีระบบการตรวจสอบการใช้อำนาจหน้าที่ของเจ้าพนักงานสอบสวนคดีพิเศษและเจ้าหน้าที่ที่เกี่ยวข้อง รวมทั้งมีการประเมินผลการปฏิบัติหน้าที่เป็นระยะๆ นอกเหนือจากการมีระบบคัดสรรบุคลากรที่เข้มงวด

---

[23] Haroldd L. Nelson & Dwight L. Teeter. (1986). **Law of Mass Communication : Freedom and Control of Print and Broadcast Media** (Fifth Edition). p. 200.

และโปร่งใส เพื่อให้งานสอบสวนคดีพิเศษมีประสิทธิภาพและเป็นอีกส่วนหนึ่งของกระบวนการยุติธรรมในปัจจุบัน

2.3 การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในคดีอาญา

2.3.1 การค้นหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ การค้นเป็นมาตรการบังคับ (Zwangsmassnahme หรือ compulsory measures) ซึ่งเป็นเครื่องมือในการดำเนินคดีอาญาที่สำคัญและจำเป็นต้องมี หากขาดไปการดำเนินคดีอาญาก็ย่อมไม่อาจกระทำได้[24] โดยกำหนดให้เจ้าพนักงานของรัฐ 2 ประเภท เป็นผู้ดำเนินการค้น ได้แก่ พนักงานฝ่ายปกครอง และเจ้าพนักงานตำรวจหรือพนักงานสอบสวน ประชาชนทั่วไปไม่สามารถทำการค้นได้ไม่ว่าจะเป็นกรณีใดก็ตาม[25] และมีเหตุในการออกหมายค้นได้ตามมาตรา 69 (1) – (5)

การค้นจึงเป็นการดำเนินการของเจ้าพนักงานของรัฐที่กฎหมายอนุญาตให้เข้าไปแสวงหาพยานหลักฐานได้ตามสถานที่ต่างๆ หรือจากตัวบุคคลก็ย่อมกระทำได้ เมื่อการค้นเป็นการแสวงหาพยานหลักฐานจากสถานที่ต่างๆ หรือจากตัวบุคคล การค้นของเจ้าพนักงานย่อมเป็นการกระทำที่กระทบกระเทือนต่อสิทธิส่วนบุคคล[26] เสรีภาพในเคหสถาน[27] และสิทธิเสรีภาพในชีวิตและ ร่างกาย[28] และในกรณีที่พยานหลักฐานที่เจ้าพนักงานของรัฐแสวงหามิใช่พยานวัตถุ พยานเอกสาร หรือพยานบุคคล เช่น ข้อมูลอิเล็กทรอนิกส์ ซึ่งกฎหมายไทยมิได้มีการจัดเอาไว้ว่าเป็นพยานหลักฐานประเภทใด และยังมีข้อโต้แย้งกันอยู่ว่าจะเป็นพยานเอกสารหรือพยานวัตถุ

แต่เมื่อพิจารณาจากการแสวงหาพยานหลักฐานดังกล่าวแล้ว อาจทำได้ 2 วิธีได้แก่

(1) เป็นข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ส่วนบุคคลของบุคคลใดบุคคลหนึ่ง ไม่ว่าจะอยู่ที่ใดที่พนักงานของรัฐไม่สามารถใช้เครื่องมือใดๆ เชื่อมเข้าไปในเครื่องคอมพิวเตอร์เพื่อเรียกดูข้อมูลที่ถูกจัดเก็บไว้ในฮาร์ดดิสได้ นอกจากเข้าไปค้นในที่ที่เครื่องคอมพิวเตอร์นั้นอยู่ ซึ่งก็เป็นการบุกรุกเข้าไปในเคหสถานของผู้เป็นเจ้าของ จึงจะได้ข้อมูลที่เป็นพยานหลักฐานมา และ

(2) เป็นการจัดเก็บข้อมูลในรูปของเครือข่าย เช่นเครือข่ายในระบบ LAN (Local Area Network) เป็นระบบเครือข่ายท้องถิ่นภายในอาคารเดียวกัน หรือ ระบบ WAN (Wide Area Network) เป็นระบบเครือข่ายระยะไกลจำกัดเฉพาะกลุ่ม เช่นระบบธนาคาร ใช้เฉพาะกลุ่มธนาคาร

---

[24] คณิต ณ นคร. เล่มเดิม. หน้า 190.

[25] คนึง ฤาไชย. (2540). **กฎหมายวิธีพิจารณาความอาญา เล่ม 1** (พิมพ์ครั้งที่ 6). หน้า 252.

[26] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 34

[27] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 35

[28] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 31

และรวมถึงระบบอินเตอร์เน็ต ซึ่งเจ้าพนักงานของรัฐไม่จำต้องเข้าไปในที่รโหฐานเพื่อค้นหาพยานหลักฐาน แต่อาจใช้เครื่องมือหรือเครื่องคอมพิวเตอร์อีกเครื่องเชื่อมไปที่แม่ข่าย หรือเซิร์ฟเวอร์ (Server) เพื่อเรียกข้อมูลมาตรวจดูก็ได้

2.3.1.1 การค้นพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์ที่อยู่ในที่รโหฐาน ตามคำนิยามของคำว่า "รโหฐาน" ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 2 (13) หมายถึงสถานที่ใดๆ ซึ่งประชาชนไม่มีความชอบธรรมที่จะเข้าไปได้ หรือเป็น "ที่ส่วนตัว" (Private Place) ที่แสดงถึงเจตนาหวงกันของเจ้าของหรือผู้ครอบครอง[29] การคุ้มครองเสรีภาพในเคหสถานของบุคคลตามรัฐธรรมนูญ มาตรา 35 การที่เจ้าพนักงานของรัฐเข้าไปค้นหาข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งอยู่ในที่รโหฐานได้จะต้องเป็นกรณีที่มีกฎหมายบัญญัติไว้ และจะต้องมีหมายค้น ดังที่บัญญัติไว้ตามรัฐธรรมนูญ มาตรา 238[30] ซึ่งจะต้องมีเหตุในการออกหมายค้นตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 69 เว้นแต่เป็นกรณีที่กฎหมายบัญญัติให้มีการค้นได้โดยไม่ต้องมีหมายตามมาตรา 92[31] หากเจ้าพนักงานของรัฐทำการตรวจค้นโดยไม่มีหมาย และไม่เข้ากรณียกเว้น การค้นดังกล่าวก็เป็นการค้นที่มิชอบ เป็นเหตุให้ศาลไม่สามารถรับฟังเป็นพยานหลักฐานได้

ดังนั้นการเข้าตรวจค้นที่รโหฐานเพื่อค้นหาในเครื่องคอมพิวเตอร์ส่วนบุคคล หรือเครื่องคอมพิวเตอร์ที่เชื่อมโยงเครือข่ายในเคหสถานเดียวกันของผู้ต้องสงสัยซึ่งเป็น "สิ่งของที่ใช้ในการกระทำความผิด" เพื่อค้นหาข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นพยานหลักฐานแสดงการกระทำความผิดของผู้ต้องสงสัย เจ้าพนักงานของรัฐจำเป็นจะต้องมีหมายค้นจากศาล ในการรวบรวมพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132[32]

หากพิจารณาจากลักษณะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งสามารถทำลายแก้ไขได้ง่ายโดยใช้เวลาเพียงสั้นๆ แต่การออกหมายค้นจากศาลต้องใช้เวลาพอสมควร หากผู้ต้องสงสัยทราบว่าจะถูกค้น ก็สามารถทำลายหรือแก้ไขได้โดยง่าย ถึงแม้มีความจำเป็นเร่งด่วน จะถือเป็นเข้าเหตุยกเว้นตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92 และใช้อำนาจตามมาตรา 92 วรรคสอง ซึ่งไม่น่าจะยกเป็นเหตุยกเว้นได้ เพราะโดยหลักการค้นจะต้องมีหมาย สำหรับ

---

[29] คณิต ณ นคร. เล่มเดิม. หน้า 220.

[30] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 238

[31] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92

[32] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132

การค้นตามมาตรา 92 เป็นการค้นในกรณีพิเศษ จึงต้องมีกฎหมายบัญญัติเอาไว้อย่างชัดแจ้ง ประกอบกับคำวินิจฉัยของคณะกรรมการกฤษฎีกาที่ นร. 0601/618[33] ให้ความเห็นว่า

บทบัญญัติมาตรา 92 วรรคสอง แห่งประมวลกฎหมายวิธีพิจารณาความอาญาในส่วนที่บัญญัติให้พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ค้นด้วยตนเองโดยไม่ต้องมีหมายค้น ในกรณีที่อาจออกหมายค้นได้ ขัดต่อมาตรา 238 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยเป็นอันใช้บังคับมิได้...

ดังนั้น การค้นข้อมูลอิเล็กทรอนิกส์ในกฎหมายไทยปัจจุบันจึงต้องมีหมายค้น เจ้าพนักงานของรัฐจึงจะทำการค้นได้ หากเป็นการค้นโดยไม่มีหมาย ก็ถือว่าพยานหลักฐานที่ได้เป็นพยานหลักฐานที่ได้มาโดยมิชอบ ศาลไม่สามารถนำมาใช้ประกอบการพิจารณาได้

2.3.1.2 การค้นพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์โดยการเชื่อมเข้าระบบ กรณีที่เจ้าพนักงานของรัฐเข้าค้นข้อมูลอิเล็กทรอนิกส์ได้โดยไม่ต้องเข้าไปในที่รโหฐาน แต่ใช้เครื่องคอมพิวเตอร์เชื่อมจากภายนอก ไม่ว่าจะเป็นระบบ LAN, WAN หรือ อินเตอร์เน็ต ลักษณะไม่เป็นการบุกรุกตามประมวลกฎหมายอาญา เพราะไม่ได้เข้าไปยังเคหสถานของผู้อื่น แต่เป็นการละเมิดสิทธิส่วนบุคคลตามรัฐธรรมนูญ มาตรา 34 โดยถือว่าเป็นการค้นเช่นกัน การใช้อำนาจของเจ้าพนักงานของรัฐ ย่อมจะต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของประชาชนตามดังที่บัญญัติไว้ในรัฐธรรมนูญมาตรา 26

ดังนั้น การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN, WAN หรือ อินเตอร์เน็ต แม้ในกฎหมายไทยปัจจุบันยังไม่มีกฎหมายบัญญัติไว้โดยเฉพาะ แต่เมื่อพิจารณาถึงสิ่งที่กฎหมายประสงค์จะให้ความคุ้มครอง นั่นคือสิทธิส่วนบุคคล การค้นจึงต้องมีหมายค้นเช่นเดียวกับการค้นโดยทั่วไป หากเป็นการค้นโดยไม่มีหมาย ก็ถือว่าพยานหลักฐานที่ได้เป็นพยานหลักฐานที่ได้มาโดยมิชอบเช่นกัน และศาลก็ไม่สามารถนำมาใช้ประกอบการพิจารณาได้

2.3.2 การยึดและเก็บรักษาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานที่ไม่มีรูปร่าง ซึ่งจะทำการยึดอย่างเช่นพยานหลักฐานทั่วไป ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 101[34] ไม่ได้ โดยลักษณะของข้อมูลอิเล็กทรอนิกส์ การยึดสามารถกระทำได้โดยการยึดเครื่องคอมพิวเตอร์หรือเครื่องอิเล็กทรอนิกส์ที่มีข้อมูลนั้น หรือการนำฮาร์ดดิสก์ที่มีข้อมูลนั้นเสนอต่อศาล

---

[33] คำวินิจฉัยของคณะกรรมการกฤษฎีกา ตามหนังสือ สำนักงานคณะกรรมการกฤษฎีกาที่ นร. 0601/618 (2542). **วารสารอัยการนิเทศ**, 61, 1. หน้า .183-194.

[34] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 101

กรณีที่เป็นข้อมูลอิเล็กทรอนิกส์ในระบบเครือข่ายอินเตอร์เน็ต ซึ่งต้องมีการเจาะเข้าไปใน E-mail ที่มีข้อมูลส่วนตัว การจะยึดข้อมูลส่วนบุคคลดังกล่าว เจ้าพนักงานของรัฐไม่สามารถทำได้ เพราะเป็นการละเมิดสิทธิส่วนบุคคล สามารถทำได้เพียงการยึดข้อมูลที่มีการเผยแพร่ต่อสาธารณชนเพื่อนำเสนอต่อศาลเท่านั้น

ในการตรวจสอบพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ว่าเกี่ยวข้องกับการกระทำความผิดหรือไม่นั้น ลำพังเจ้าพนักงานของรัฐเองอาจไม่สามารถทำได้ ทำให้ได้ข้อมูลไม่ครบถ้วน จึงจำเป็นต้องมีผู้เชี่ยวชาญ เช่น โปรแกรมเมอร์ที่เป็นผู้เชี่ยวชาญพิเศษโดยเฉพาะเป็นผู้ช่วยเหลือเจ้าพนักงานของรัฐในการปฏิบัติหน้าที่ โดยจะทำหน้าที่เข้าสู่ข้อมูล ตรวจสอบ เก็บข้อมูลหรือพยานหลักฐานให้ครบถ้วน ตลอดจนเก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นให้อยู่ในสภาพที่สามารถใช้ประโยชน์ได้ เพราะวัสดุที่ใช้ในการเก็บรักษาข้อมูล เช่นฮาร์ดดิสก์ เป็นวัสดุที่อาจถูกทำลายได้โดยสภาพแวดล้อมทางธรรมชาติ เช่น ความชื้น ความเย็นจัด ร้อนจัด หรือสนามแม่เหล็ก ทั้งจะต้องทำหน้าที่ยืนยันต่อศาลว่าข้อมูลอิเล็กทรอนิกส์ที่นำเสนอต่อศาลเป็นข้อมูลที่ได้ทำการยึดมา ลักษณะจึงเหมือนกับเป็นพยานผู้เชี่ยวชาญ ผู้ที่จะทำหน้าที่ตรวจสอบพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์อย่างเป็นกลาง และทำหน้าที่เก็บรักษา แต่ขณะนี้ยังไม่มีผู้ที่จะทำหน้าที่ดังกล่าวได้ เพราะไม่มีกฎหมายกำหนดให้มี จึงยังเป็นหน้าที่ของเจ้าพนักงานของรัฐโดยทั่วๆไป ซึ่งไม่ใช่ผู้ที่มีความรู้ความสามารถโดยเฉพาะ

โดยสรุปการตรวจค้น และการยึดข้อมูลอิเล็กทรอนิกส์ เพื่อนำมาเป็นพยานหลักฐานในอาชญากรรมคอมพิวเตอร์นั้น ไม่อาจกระทำได้หากไม่มีหมายค้น บางกรณีก็ไม่สามารถทำได้อย่างทันท่วงที เป็นปัญหาในเรื่องของอำนาจของเจ้าพนักงานของรัฐที่ยังไม่มีกฎหมายให้อำนาจเอาไว้โดยเฉพาะ ตลอดจนการตรวจสอบและการเก็บรักษา ก็ยังต้องใช้วิธีการตามที่บัญญัติเอาไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาเท่านั้น ซึ่งไม่เพียงพอแล้วกับสังคมในปัจจุบัน

บทที่ 3
การเข้าถึงข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในกฎหมายต่างประเทศ

ในบทที่แล้วได้กล่าวถึงความหมาย ลักษณะ และสภาพปัญหาของการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมทางคอมพิวเตอร์รูปแบบต่างๆดังที่ได้กล่าวมาแล้ว ซึ่งปัญหาอาชญากรรมคอมพิวเตอร์นี้ก็มิใช่ว่าจะเกิดแต่เฉพาะในประเทศไทยเท่านั้น แต่ยังส่งผลกระทบต่อกฎหมายอาญาของประเทศอื่นๆ ด้วย ดังนั้นในบทนี้จะกล่าวถึงแนวความคิดในการบัญญัติกฎหมายเพื่อรักษาความปลอดภัยของข้อมูล สภาพปัญหาเกี่ยวกับการปราบปรามอาชญากรรมคอมพิวเตอร์ และมาตรการทางกฎหมายและปัญหาเกี่ยวกับการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์ของประเทศต่างๆ ได้แก่ ประเทศสหรัฐอเมริกา อังกฤษ และญี่ปุ่น โดยการศึกษาถึงแนวความคิด เหตุผล ขั้นตอน วิธีการ และระยะเวลาในการค้น และการรับฟังเป็นพยานหลักฐานในศาลของประเทศต่างๆ เพื่อเป็นแนวทางในการแก้ปัญหาที่เกิดขึ้นในกฎหมายไทยต่อไป

3.1 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาเป็นประเทศหนึ่งที่มีความเจริญก้าวหน้าทางเทคโนโลยีในหลายๆด้าน และมีกฎหมายที่จะใช้ดำเนินคดีกับอาชญากรรมคอมพิวเตอร์มากกว่า 40 ฉบับ เช่น National Stolen Property Act , Copyright Act ฯลฯ จึงต้องพิจารณาว่ากฎหมายที่มีอยู่ทั้ง 40 ฉบับนั้น สามารถนำมาใช้บังคับและครอบคลุมความผิดอาญาเกี่ยวกับคอมพิวเตอร์ได้มากน้อยเพียงใด สำหรับความผิดเกี่ยวกับคอมพิวเตอร์สหรัฐเองก็มีการบัญญัติกฎหมายตั้งแต่ปี ค.ศ. 1984 คือ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA) ซึ่งแบ่งความผิดเกี่ยวกับคอมพิวเตอร์เป็น 3 ลักษณะ ได้แก่

ก. Subsection 1030 (a) (1) ความผิดที่ก่อความเสียหายแก่ความมั่นคงของรัฐโดยตรง

ข. Subsection 1030 (a) (2) ความผิดที่ก่อให้เกิดความเสียหายต่อระบบความเชื่อถือส่วนบุคคลที่มีในสถาบันการเงิน หรือหน่วยงานที่ทำหน้าที่ดูแลประวัติ และผู้บริโภค

ค. Su bsection 1030 (a) (3) ความผิดที่กระทำต่อข้อมูลข่าวสารของเครื่องคอมพิวเตอร์อันก่อให้เกิดความเสียหายต่อรัฐบาลสหรัฐ[1]

และมีการแก้ไขเพิ่มเติมในปี 1988 และ 1990 ตามลำดับเพื่อให้ครอบคลุมความผิดที่เกิดขึ้น สภาคองเกรสได้มีมติให้ออกกฎหมาย The National Information Infrastructure Protection Act of 1996 (NIIPA) [2] และเพิ่มเติมการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ใน U.S. Code title 18 มาตรา 1030 (18 U.S.C.A. section 1030)[3] สำหรับกฎหมายของมลรัฐต่างๆ เริ่มมีใน ค.ศ. 1987 โดยเริ่มมีที่มลรัฐอริโซน่า และมลรัฐฟลอริดา และหลังจากถูกกลุ่มผู้ก่อการร้ายโจมตีตึกเพนทากอนและอาคารเวิลด์เทรดเซ็นเตอร์ เมื่อวันที่ 11 กันยายน ค.ศ. 2001 จึงให้ความสำคัญกับการรักษาความปลอดภัยและความเป็นส่วนตัวกันมากขึ้น และได้จัดสรรเงินเพื่อแก้ปัญหาอาชญากรรม โดยเฉพาะในส่วนที่เกี่ยวกับความปลอดภัยในเครือข่ายคอมพิวเตอร์ (Cyber-security) และการวิจัยเกี่ยวกับการก่อการร้ายในเครือข่ายคอมพิวเตอร์ (Cyber-terrorism) [4]

3.1.1 มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา ประเทศสหรัฐอเมริกาเป็นประเทศแรกที่ประกาศใช้กฎหมายจำกัดการใช้อินเตอร์เน็ตเพื่อความบันเทิงทางเพศ คือกฎหมายควบคุมสื่อลามกและข้อความที่ไม่สมควรทางเพศบนอินเตอร์เน็ต (Communications Decency Act 1996 : CDA.) ซึ่งมีเนื้อหากำกับสิ่งที่ให้บริการทางอินเตอร์เน็ตโดยเฉพาะ โดยกำหนดให้บุคคลที่ส่งภาพหรือข้อความลามกอนาจารหรือไม่เหมาะสมขัดต่อศีลธรรมอันดี แก่ผู้เยาว์อายุต่ำกว่า 18 ปี มีความผิดต้องรับโทษปรับหรือจำคุกไม่เกิน 2 ปี [5] และถ้าผู้ใดอนุญาตให้ผู้เยาว์อายุต่ำกว่า 18 ปี ใช้อินเตอร์เน็ตหรือสถานที่เพื่อการดังกล่าวย่อมมีความผิดด้วย[6] จะเห็นได้ว่ากฎหมายฉบับนี้จำกัดสิทธิเสรีภาพและความเป็นส่วนตัวของบุคคล เมื่อกฎหมายฉบับนี้ใช้บังคับในวันที่ 8 กุมภาพันธ์ 1996 สมาคมสิทธิทางแพ่งของสหรัฐอเมริกัน (ACLU) และ

---

[1] นิติ ผดุงชัย. (2532,มิถุนายน). “กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับ Computer.” **วารสารอัยการ**. หน้า 86-88.

[2] Michael Hatcher , Jay Mc Danell , and Stacy Ostfeld. (1999). “Computer Crimes.” **American Criminal Law Review**. 36 : p.402.

[3] Ibid.p.401.

[4] “The Governance Challenge : Creating a smart and Secure Cyberspace,” Madanmohan Rao report from the ‘New Directions in Internet Policy’ conference in Atlanta, <http://www.indiainfoline.com/nevi/inwi/mm66.html.>,2002.

[5] CDA, Section 223.

[6] CDA, Section 223 (a) (2).

สมาคมห้องสมุด (ALA) ได้ยื่นฟ้องต่อศาลขอประกาศว่ากฎหมายฉบับนี้ขัดต่อรัฐธรรมนูญว่าด้วยการคุ้มครองเสรีภาพในการแสดงออก และสิทธิความเป็นส่วนตัว ตามบทแก้ไขเพิ่มเติมฉบับที่ 1 (First Amendment) และรัฐบาลสหรัฐอเมริกาก็ได้โต้แย้งว่ากฎหมายฉบับนี้บังคับใช้แต่เฉพาะบุคคลที่ไม่สุจริตและรู้ว่าผู้เยาว์ใช้บริการในสถานที่ของตน และยกเว้นบุคคลที่ไม่รู้ว่าข้อความที่ผ่านคอมพิวเตอร์ของตนนั้นเป็นข้อความหรือภาพลามก การจำกัดเสรีภาพจะกระทำต่อเด็กและเยาวชนเท่านั้น ไม่รวมถึงบุคคลทั่วไป แต่ในที่สุดศาลก็ตัดสินให้ระงับใช้กฎหมายฉบับนี้เพราะอาจจะขัดต่อรัฐธรรมนูญ [7]

3.1.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ ในปี ค.ศ. 1986 สภาคองเกรสของสหรัฐอเมริกาได้ออก The Computer Fraud and Abuse Act of 1986 ซึ่งกฎหมายฉบับนี้มีบทบัญญัติที่เปลี่ยนแปลงไปจากกฎหมายที่มีอยู่เดิม ได้แก่

3.1.2.1 ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access)

3.1.2.2 ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration)

3.1.2.3 ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction)

3.1.2.1 ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access) ความผิดฐานเข้าถึงโดยปราศจากอำนาจเป็นความผิดฐานหนึ่ง ที่เป็นการฉ้อโกงหรือกระทำการใดๆ ต่อเครื่องคอมพิวเตอร์โดยเจตนา เป็นการกระทำโดยปราศจากอำนาจ หรือกระทำเกินกว่าอำนาจที่มีอยู่ ได้แก่

(1) เข้าสู่ระบบคอมพิวเตอร์โดยรู้ว่าไม่มีอำนาจ และได้ไปซึ่งข้อมูลนั้น โดยมีเหตุเชื่อได้ว่าข้อมูลนั้นอาจถูกใช้ไปเพื่อการอันเป็นภัยต่อความมั่นคงของประเทศ หรือเพื่อประโยชน์ของชาติอื่น ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 20 ปี

(2) เข้าสู่ระบบคอมพิวเตอร์โดยรู้ว่าไม่มีอำนาจ และได้ไปซึ่งข้อมูลทางการเงินหรือข้อมูลของสถาบันการเงิน ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(3) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ และปลอมแปลงหรือแสร้งว่าเป็นเจ้าหน้าที่ของรัฐเพื่อเปิดระบบประมวลผล ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

---

[7] เลอสรร ธนสุกาญจน์และคณะ. (2541). **กฎหมายสำหรับบริการอินเตอร์เน็ตในประเทศไทย กรอบ ข้อเสนอแนะ และการควบคุมดูแล การให้บริการ**. หน้า 154.

(4) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ เพื่อผลประโยชน์ใดๆ ด้วยเจตนาฉ้อโกงหรือได้ไปซึ่งสิ่งมีค่าใดๆ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(5) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ และได้แก้ไขเปลี่ยนแปลงหรือทำลายข้อมูลที่ได้เข้าถึงนั้นเพื่อผลประโยชน์ใดๆ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(6) รู้และใช้รหัสผ่านโดยปราศจากอำนาจเพื่อเข้าถึงข้อมูลในคอมพิวเตอร์ของรัฐบาลเพื่อการค้าระหว่างรัฐหรือการค้าระหว่างประเทศ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

นอกจากความผิดข้างต้นแล้ว การเข้าถึงข้อมูลในคอมพิวเตอร์โดยปราศจากอำนาจสหรัฐอเมริกาถือเป็นการกระทำที่มิชอบเกี่ยวข้องกับกฎหมายอื่นๆอีก ดังนี้

(1) ประมวลกฎหมายอาญาสหรัฐอเมริกา เนื่องจากการเข้าถึงข้อมูลในคอมพิวเตอร์ถือเป็นการลักขโมยบริการ (Theft of Service) เพราะเป็นการใช้บริการโดยไม่มีอำนาจ แม้ในบางครั้งจะไม่ก่อให้เกิดความเสียหายก็ตาม แต่กฎหมายก็ถือว่ามีความผิด โดยถือว่าเป็นความเสี่ยงต่อการก่อให้เกิดความเสียหายต่อสารสนเทศได้และผู้กระทำย่อมรู้ตัวดี และความเสียหายจะเกิดขึ้นในอนาคต[8] เพราะว่าในการเข้าถึงโดยปราศจากอำนาจ อาจทำให้เจ้าของที่แท้จริงไม่สามารถเข้าสู่ระบบได้ จึงมีการบัญญัติกฎหมายนี้ขึ้นเพื่อคุ้มครองผู้เช่าหรือผู้มีอำนาจใช้สายสื่อสารที่ต่อเชื่อมกับระบบคอมพิวเตอร์ และกรณีของพนักงานของบริษัทที่ใช้คอมพิวเตอร์ทำงานส่วนตัวหรือคัดลอกทำสำเนาข้อมูลโดยไม่ได้รับความยินยอมจากนายจ้าง ที่เรียกว่า “การทำงานกลางคืน” (Moonlight) ก็เป็นการกระทำที่ปราศจากอำนาจ ถือเป็นการลักสิ่งที่มีค่าใดๆ (Thing of Value) อันเป็นความผิดฐานลักทรัพย์ และการกระทำดังกล่าวยังเข้าลักษณะความผิดฐานปลอมแปลงเอกสารและความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญาด้วย ซึ่งจะเห็นได้ว่ามีกฎหมายมากกว่า40 มาตราในบรรพที่ 8 ประมวลกฎหมายอาญาสหรัฐอเมริกาที่บัญญัติถึงการใช้เครื่องคอมพิวเตอร์ในการกระทำความผิดไม่ว่าโดยตรงหรือโดยอ้อม

(2) กฎหมายการสื่อสารทางอิเล็กทรอนิกส์ส่วนบุคคล (The Electronic Communication Privacy Act of 1986) กฎหมายฉบับนี้เป็นกฎหมายที่รับประกันการสื่อสารระหว่างบุคคลที่ผ่านทางโทรศัพท์ในระบบต่างๆ คลื่นวิทยุ การสื่อสารผ่านดาวเทียม และการสื่อสารผ่านทางเครือข่าย

---

[8] สุเนติ คงเทพ . (2541). **เอกสารประกอบการสัมมนาแนวทางในการแก้ปัญหากฎหมายอาชญากรรมยุคไอที เรื่องการไม่มีอำนาจเข้าสู่ระบบประมวลผล**. หน้า 16.

คอมพิวเตอร์ ไปรษณีย์อิเล็กทรอนิกส์ สาระสำคัญของกฎหมายฉบับนี้ คือ คำนิยามและข้อยกเว้นการจำกัดการสื่อสารของภาคเอกชน การเก็บรักษาและการใช้ข้อมูลจากการสื่อสาร การรับจดทะเบียน ฯลฯ

(3) กฎหมายการฉ้อโกงบัตรเครดิต (The Credit Card Fraud Act of 1984) เป็นกฎหมายที่ออกมาเพื่อควบคุมการฉ้อโกงบัตรเครดิตและการปลอมบัตรเครดิต แต่คำนิยามของคำว่า "บัตรเครดิต" ในกฎหมายฉบับนี้ได้ครอบคลุมไปถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ด้วย เช่น การกระทำความผิดที่เข้าถึงสื่อทางคอมพิวเตอร์ หมายความรวมถึงบัตรต่างๆ แผ่นพลาสติก รหัส หมายเลขบัญชี หรือสิ่งอื่นๆของบัญชี และการเข้าถึงให้หมายความถึงการเข้าถึงทางด้านบัญชีและการเข้าถึงสื่อทางคอมพิวเตอร์ อันถือเป็นการกระทำที่ได้ไปซึ่งผลประโยชน์ในด้านต่างๆ ส่วนที่กล่าวถึงการกระทำความผิดเกี่ยวกับเครื่องคอมพิวเตอร์นั้น เป็นการกระทำความผิดฐานฉ้อโกงการทำ ใช้ จำหน่าย ปลอมสื่อทางคอมพิวเตอร์ หรือการเข้าถึงโดยปราศจากอำนาจ ลักษณะของการกระทำความผิดตามกฎหมายฉบับนี้ที่เกิดขึ้นในปัจจุบัน ได้แก่ การลักลอบเข้าสู่ระบบคอมพิวเตอร์เพื่อค้นหา ทดสอบ หรือการแก้ไขเปลี่ยนแปลงข้อมูลต่างๆ เช่น หมายเลขโทรศัพท์ หมายเลขบัญชีธนาคาร หรือรหัสผ่าน

(4) กฎหมายลิขสิทธิ์ (The Copyright Act of 1976) กรณีที่มีการเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์โดยปราศจากอำนาจในลักษณะที่เป็นการลักขโมยโปรแกรมหรือข้อมูลในคอมพิวเตอร์นั้น ถือเป็นการละเมิดลิขสิทธิ์ที่มีโทษทางอาญา ตามรายงานของคณะกรรมาธิการรัฐสภาเกี่ยวกับกฎหมายลิขสิทธิ์ ค.ศ. 1976 หน้า 54 ระบุว่า "งานวรรณกรรม" (Literary Works) ให้รวมถึงฐานข้อมูลทางคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ รวมถึงงานประพันธ์ที่เป็นการแสดงออกถึงความคิดดั้งเดิมของนักเขียนโปรแกรม จึงเป็นสิทธิของผู้เขียนโปรแกรมที่จะปกป้องเอกสารและลายเส้นของรหัสคอมพิวเตอร์จากการคัดลอกหรือทำสำเนา แต่การคุ้มครองดังกล่าวก็มิได้ครอบคลุมถึง "ขั้นตอนวิธี" (Algorithms) ของผู้เขียนโปรแกรมด้วย การกระทำความผิดตามกฎหมายฉบับนี้มีโทษทั้งทางแพ่งและในทางอาญา

(5) กฎหมายการฉ้อโกงทางสายโทรศัพท์ (The Wire Fraud Act) เดิมประมวลกฎหมายสหรัฐอเมริกา มีการยกเว้นการกระทำความผิดทางสายสื่อสารสาธารณะ แต่เมื่อมีการใช้คอมพิวเตอร์จากเครือข่ายทางไกลกระทำการฉ้อโกงทางคอมพิวเตอร์ขึ้นเป็นจำนวนมาก ทั้งเป็นการกระทำความผิดของบุคคลเพียงคนเดียวและหลายคนร่วมมือกัน และผู้ที่กระทำความผิดก็ได้ผลประโยชน์ไปเป็นจำนวนมาก รัฐจึงมีมาตรการออกมาเพื่อปกป้องคุ้มครองการส่งข้อมูลผ่านทางสายสื่อสารสาธารณะดังกล่าว

(6) กฎหมายเกี่ยวกับระเบียบสถาบันทางการเงินและการควบคุมอัตราดอกเบี้ย (The Financial Institutions Regulatory and Interest rate Control Act of 1978 : FIRA) ในส่วนที่เป็นเรื่องการโอนเงินทางอิเล็กทรอนิกส์ (The Electronic Fund Transfer Act) ซึ่งมีการกำหนดคำนิยามและสิทธิส่วนบุคคลของผู้บริโภคที่ได้รับผลกระทบจากการโอนเงินทางอิเล็กทรอนิกส์ โดยกฎหมายฉบับนี้ได้กำหนดให้รัฐบาลกลางออกระเบียบการโอนเงินทางอิเล็กทรอนิกส์ขึ้น

(7) กฎหมายคุ้มครองส่วนบุคคล (The Privacy Act of 1974) กรณีที่เป็นการเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจที่จะกระทำได้ โดยกระทำผ่านฐานข้อมูลในเครื่องคอมพิวเตอร์ เป็นการให้ความคุ้มครองความเป็นส่วนตัวของบุคคล ดังนั้นการเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์โดยปราศจากอำนาจจึงอาจมีความผิดตามกฎหมายฉบับนี้ด้วย

3.1.2.2 ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration) ความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูลตาม The Computer Fraud and Abuse Act 1986 ครอบคลุมถึงการแก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ และข้อมูลที่ถูกจัดเก็บอยู่ในคอมพิวเตอร์ เหตุที่นำความผิดดังกล่าวมาบัญญัติเอาไว้ต่างหาก เนื่องมาจากการกระทำความผิดดังกล่าวมีลักษณะคล้ายกับความผิดฐานปลอมแปลงเอกสาร แต่เมื่อมีการกระทำความผิดเกิดขึ้นกลับไม่สามารถนำบทบัญญัติของกฎหมายในความผิดฐานปลอมแปลงเอกสารมาใช้บังคับได้ เพราะประสบปัญหาการตีความ โดยเฉพาะเรื่องขององค์ประกอบของความผิด ฝ่ายนิติบัญญัติของรัฐบาลกลางและมลรัฐต่างๆ จึงจำเป็นที่จะต้องบัญญัติกฎหมายขึ้นมาใช้บังคับกับความผิดดังกล่าวโดยเฉพาะ

การกระทำที่เป็นการแก้ไขเปลี่ยนแปลงโปรแกรมคอมพิวเตอร์หรือการแก้ไขเปลี่ยนแปลงข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์ ในส่วนที่เกี่ยวกับความผิดฐานปลอมเอกสารนั้นตีความจากคำว่า “เอกสาร” ที่หมายความรวมถึงโปรแกรมคอมพิวเตอร์และข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์

3.1.2.3 ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction) ความผิดฐานทำให้เสียหายหรือทำลายทางคอมพิวเตอร์ตาม The Computer Fraud and Abuse Act 1986 นั้น เป็นการกระทำที่ทำให้เกิดความเสียหายหรือทำลายโปรแกรมคอมพิวเตอร์หรือข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์และการกระทำให้เกิดความเสียหายโดยตรงต่อเครื่องคอมพิวเตอร์รวมทั้งอุปกรณ์ต่างๆของเครื่องคอมพิวเตอร์ที่เรียกว่าฮาร์ดแวร์ (Hardware) ด้วย โดยบัญญัติแยกต่างหากจากความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญา เนื่องจากเห็นว่าเป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายที่ร้ายแรง และก่อให้เกิดความเสียหายต่อเทคโนโลยี

3.1.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ การค้นข้อมูลอิเล็กทรอนิกส์เป็นการค้นที่แตกต่างจากการค้นที่มีอยู่แต่เดิม ซึ่งเมื่อพนักงานสอบสวนเห็นสมควรจะค้นจะต้องมีหมายค้น โดยจะต้องบรรยายสถานที่ที่จะทำการค้นในหมายนั้นด้วย แต่สำหรับการค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์จะต้องทำการค้นหาจากฮาร์ดแวร์หรือฮาร์ดดิสก์

ในการปฏิบัติหน้าที่ของพนักงานสอบสวนของสหรัฐอเมริกาจะต้องเป็นการค้นหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์โดยไม่ขัดต่อหลักการไม่รับฟังพยานหลักฐาน ซึ่งได้มาโดยการค้นที่มิชอบ (Exclusionary Rule) ตามรัฐธรรมนูญสหรัฐอเมริกาแก้ไขเพิ่มเติมฉบับที่ 4 (The Fourth Amendment) บัญญัติว่า "สิทธิของบุคคลที่จะมีความปลอดภัยมั่นคงในร่างกาย เคหสถาน เอกสารและวัตถุสิ่งของ ต่อการค้น การยึด และการจับที่ไม่มีเหตุอันสมควร จะถูกล่วงละเมิดมิได้ และห้ามมิให้มีการออกหมาย เว้นแต่จะโดยมีเหตุอันควร ซึ่งได้มาโดยการสาบาน หรือปฏิญาณตน และหมายนั้นจะต้องระบุเฉพาะเจาะจงถึงสถานที่ที่จะถูกค้น ตัวบุคคลที่จะถูกจับ และสิ่งของที่ถูกยึด"

นอกจากนี้กฎว่าด้วยวิธีพิจารณาความอาญาของสหรัฐได้รับรองหลักของรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่นี้ไว้ในมาตรา 41 (a) ซึ่งบัญญัติว่า "เจ้าพนักงานผู้มีอำนาจหรือพนักงานอัยการต้องขอหมายค้น…

(1) หมายค้นต้องออกโดยศาล Magistrate ของมลรัฐ หรือศาลของสหรัฐ สำหรับการค้นสิ่งของหรือค้นหาบุคคลในเขตอำนาจศาล

(2) หมายค้นออกโดยศาล Magistrate สำหรับกรณีการค้นสิ่งของหรือค้นหาบุคคลในเขตอำนาจศาลหรือค้นสิ่งของที่ถูกโยกย้ายหรือบุคคลหลบหนีออกนอกเขตก่อนจะถูกดำเนินการตามกฎหมาย"

จากกฎหมายดังกล่าวจะเห็นได้ว่าเจ้าหน้าที่ของรัฐจะทำการค้นได้ก็ต่อเมื่อมีหมายค้น และหมายค้นดังกล่าวจะต้องออกโดยผู้พิพากษา แม้ในกรณีของการค้นข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นพยานหลักฐานที่มีลักษณะพิเศษ ที่อาจถูกแก้ไขเปลี่ยนแปลงได้ง่าย เจ้าพนักงานของรัฐก็จะต้องทำการค้นโดยมีหมาย เพราะต้องการจะให้กระบวนการในการออกหมายเป็นมาตรการในการตรวจสอบการใช้ดุลพินิจของเจ้าหน้าที่ (Warrant Process) เพื่อให้เจ้าหน้าที่ปฏิบัติหน้าที่โดยไม่ขัดกับรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 4

ในกรณีที่เจ้าหน้าที่ไม่จำเป็นที่จะต้องเข้าไปค้นในเคหสถานหรือสำนักงานของผู้อื่น แต่สามารถทำการค้นโดยการใช้เครื่องคอมพิวเตอร์หรือเครื่องมืออื่นใดเชื่อมต่อเข้ากับระบบ LAN หรือ WAN ของเคหสถาน หรือสำนักงาน ตลอดจนเครือข่ายอินเตอร์เน็ต โดยไม่มีการบุกรุกเข้าไปทางกายภาพ หากพิจารณาถึงสิทธิที่ได้รับการรับรองคุ้มครองตามรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่

DPU

4 ซึ่งรวมไปถึงสิทธิส่วนบุคคลด้วย การค้นข้อมูลอิเล็กทรอนิกส์ในลักษณะนี้ ก็ถือเป็นการบุกรุกเช่นกัน

3.1.4 การรับฟังเป็นพยานหลักฐานในศาล ภายหลังที่กฎหมายอาชญากรรมคอมพิวเตอร์ในสหรัฐอเมริกาใช้บังคับแล้วยังมีปัญหาที่ตามมาอีกหลายประการ เช่น ปัญหาในการให้คำนิยามคำว่า "อาชญากรรมคอมพิวเตอร์" (Computer crime) การจำกัดการให้ความคุ้มครองที่จำกัดเฉพาะงานของรัฐไม่รวมภาคเอกชน การขาดความชัดเจนในเรื่องของเขตอำนาจศาล และปัญหาเกี่ยวกับวิธีพิจารณาความ เช่น การแสวงหาพยานหลักฐาน และการรับฟังเป็นพยานหลักฐานในศาล ทำให้ไม่สามารถนำผู้กระทำผิดมาลงโทษได้

ศาลของสหรัฐอเมริกาจะไม่รับฟังพยานหลักฐานที่เกิดจากการค้นโดยมิชอบ ดังนั้นในการค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ก็จะต้องเป็นการค้นที่ไม่ขัดต่อหลักการห้ามรับฟังพยานหลักฐานซึ่งได้มาโดยมิชอบ (Exclusionary Rule) ดังนั้นหากเจ้าหน้าที่แสวงหาพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์โดยวิธีการที่มิชอบด้วยกฎหมาย เป็นการล่วงล้ำสิทธิส่วนบุคคล พยานหลักฐานดังกล่าวก็จะถูกตัดออกจากกระบวนการพิจารณาของศาลทันที โดยศาลจะไม่รับฟัง ทำให้ไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้

3.2 ประเทศอังกฤษ

ก่อนที่จะมีกฎหมายอาญาว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือการรักษาความปลอดภัยของข้อมูลในคอมพิวเตอร์นั้น การเข้าถึงข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ในประเทศอังกฤษโดยปราศจากอำนาจไม่ถือเป็นความผิดอาญา โดยพิจารณาเปรียบเทียบจากความผิดฐานบุกรุก (Trespass) ความผิดเกี่ยวกับทรัพย์ (Theft) ที่ผู้กระทำผิดรับผิดแต่เพียงในทางแพ่ง [9] ต่อมาจึงได้บัญญัติ The Computer Misuse Act 1990 เป็นกฎหมายอาญาว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ขึ้นเป็นฉบับแรก ทั้งได้วางมาตรการในการรักษาความปลอดภัยของข้อมูลเอาไว้ด้วย

3.2.1 มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศอังกฤษ วัฒนธรรมของประเทศอังกฤษนั้นให้ความเคารพต่อสิทธิส่วนบุคคล โดยมีคดีตัวอย่างเกี่ยวกับนายจ้างและลูกจ้างที่ศาลตัดสินว่านายจ้างไม่อาจเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง ไม่ว่าข้อมูลนั้นจะเก็บไว้

---

[9] เฉลิมพล ช่อโพธิ์ทอง. (2535). **ความผิดฐานลักทรัพย์และฉ้อโกง : ศึกษาเปรียบเทียบกฎหมายอังกฤษ เยอรมัน และไทย**. หน้า 73.

ในระบบธรรมดาหรือเก็บไว้ในคอมพิวเตอร์ก็ตาม[10] ต่อมารัฐบาลอังกฤษได้พิจารณาถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ว่าควรจะมีกฎหมายคุ้มครอง เพราะจำเป็นต้องดำเนินการให้กฎหมายภายในของอังกฤษสอดคล้องกับอนุสัญญาแห่งสภายุโรปว่าด้วยการให้ความคุ้มครองข้อมูล (The Council of Europe's Data Protection) รัฐสภาของประเทศอังกฤษได้ออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (The Data Protection Act 1984 แก้ไขเพิ่มเติม ค.ศ. 1998) เพราะในการแสวงหาพยานหลักฐานของเจ้าพนักงานของรัฐ โดยล่วงล้ำเข้าไปรับรู้ถึงข้อมูลที่เกี่ยวกับการดำเนินชีวิตของผู้ต้องสงสัยหรือสารสนเทศที่อยู่ในความครอบครองของผู้ใช้ และการแสดงความคิดเห็นส่วนตัว เท่ากับเป็นการล่วงล้ำข้อมูลส่วนบุคคลที่กฎหมายอังกฤษประสงค์จะให้ปกปิด ดังเช่นคดีระหว่างนายจ้างและลูกจ้างข้างต้น การรวบรวมพยานหลักฐานด้วยวิธีการดังกล่าวอาจถูกหาว่าเป็นพยานหลักฐานที่ได้มาโดยมิชอบได้

3.2.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของอังกฤษ คือ The Data Protection Act 1998 และมีมาตรการควบคุม และตรวจสอบการทำงานของเจ้าหน้าที่โดยองค์กรภายนอกไว้อย่างรัดกุม และไม่ทำให้ประสิทธิภาพในการปราบปรามอาชญากรรมของเจ้าหน้าที่ลดลง โดยการให้ดุลพินิจในการปฏิบัติหน้าที่ของเจ้าหน้าที่ ภายใต้กฎเกณฑ์ที่กฎหมายบัญญัติไว้ใน The Police and Criminal Evidence Act 1984

กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ของอังกฤษ คือ The Computer Misuse Act 1990 ที่กำหนดความผิดไว้ 3 รูปแบบ ได้แก่

3.2.2.1 ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access)

3.2.2.2 ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง (Ulterial Hacking Offence หรือ Unauthorized Access with Intent to Commit or Facilitate Commission of Further Offences) และ

3.2.2.3 ความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ (Modification of Computer Material หรือ Unauthorized Modification)

---

[10] Edward Wilding. (1997). **Computer Evidence : A Forensic Investigations Handbook**. London : Sweet & Maxwell Ltd. p.93.

3.2.2.1 ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access) ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 1 บัญญัติว่า

(1) บุคคลจะมีความผิดเมื่อ

(a) บุคคลได้กระทำการให้คอมพิวเตอร์แสดงผล หรือแสดงการทำงานใดๆ ด้วยเจตนาที่จะผ่านสิ่งป้องกันที่มีไว้เพื่อกันการเข้าถึงระบบ และได้ทำการผ่านสิ่งป้องกันเช่นว่านั้นเข้าถึงโปรแกรมคอมพิวเตอร์ใดๆ หรือสารสนเทศที่เก็บไว้ในคอมพิวเตอร์ใดๆ

(b) การผ่านสิ่งป้องกันเข้าไปยังระบบนั้น เป็นการกระทำโดยปราศจากอำนาจ

(c) บุคคลนั้นได้รู้ขณะที่กระทำอยู่แล้วว่า การกระทำอันเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการกระทำนั้นปราศจากอำนาจ

(2) เจตนาของบุคคลที่ได้กระทำความผิดภายใต้มาตรานี้ ไม่จำเป็นต้องเป็นการกระทำที่เป็น

(a) โปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล

(b) โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือ

(c) โปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ

(3) บุคคลที่มีความผิดภายใต้บทบัญญัตินี้ จะต้องถูกพิจารณาคดีแบบรวดรัดและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

จากบทบัญญัติข้างต้นเป็นบทบัญญัติที่ไม่มีความซับซ้อน แสดงถึงการเข้าถึงข้อมูลโดยปราศจากอำนาจ แต่จะเป็นการกระทำที่มีความผิดตามมาตรานี้จะต้องเป็นการทำให้เครื่องคอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ รวมทั้งการสั่งให้เครื่องคอมพิวเตอร์แสดงการทำงานโดยระยะทางไกล (Remote) โดยไม่คำนึงถึงผลของการกระทำ ซึ่งรวมถึงการพยายามกระทำความผิดด้วย แต่ไม่รวมถึงการทำงานทางกายภาพที่กระทำต่อเครื่องหรืออุปกรณ์คอมพิวเตอร์

หากพิจารณาความรับผิดทางอาญาในระบบคอมมอนลอว์ สำหรับความผิดฐานเข้าถึงโดยปราศจากอำนาจ สามารถแยกพิจารณาได้เป็น 2 ส่วน ได้แก่

ก. ส่วนของการกระทำ (Actus Reus) คือการที่ผู้ใดกระทำการอย่างหนึ่งอย่างใดเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ และผู้กระทำต้องรับผิดแม้จะไม่สำเร็จ ทั้งนี้ไม่รวมถึงการกระทำที่เพียงแต่สัมผัสทางกายกับอุปกรณ์หรือเครื่องคอมพิวเตอร์โดยไม่มีการกระทำใดๆต่อเครื่องคอมพิวเตอร์ และการดูข้อมูลที่ปรากฏบนจอภาพ การดักข้อมูล หรือการดักฟังข้อมูล

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) แยกพิจารณาได้ดังนี้

(1) เจตนาที่จะผ่านสิ่งป้องกันที่มีเพื่อเข้าสู่ระบบ เพื่อเข้าสู่ข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ใดๆก็เป็นความผิดแล้ว ไม่จำเป็นจะต้องเป็นเจตนาโดยตรงต่อโปรแกรมหรือข้อมูลใดๆ ตามที่บัญญัติใน (2) แสดงให้เห็นว่าเจตนาของผู้กระทำไม่จำเป็นจะต้องเป็นเจตนาโดยตรงต่อโปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือโปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ ดังนั้น การกระทำโดยประมาทก็อาจมีความผิดตามมาตรานี้ได้

(2) เจตนาภายใน คือผู้กระทำต้องรู้ในขณะที่กระทำว่าตนไม่มีอำนาจที่จะกระทำได้ เป็นการทำให้เครื่องคอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ โดยปราศจากอำนาจ

ดังนั้นในการฟ้องร้องผู้กระทำความผิด โจทก์จะต้องพิสูจน์ให้ศาลเห็นว่าจำเลยมีเจตนาเข้าสู่ระบบและจำเลยรู้ว่าการกระทำของตนเป็นการทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ และเป็นการกระทำโดยปราศจากอำนาจ การพิสูจน์องค์ประกอบภายในทั้ง 2 ประการข้างต้นนี้ถือเป็นหลักในการพิสูจน์ความผิดของผู้กระทำความผิดตามหลักพื้นฐานของคอมมอนลอว์

3.2.2.2 ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง (Ulterial Hacking Offence หรือ Unauthorized Access with Intent to Commit or Facilitate Commission of Further Offences) ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 2 บัญญัติว่า

(1) บุคคลจะมีความผิดภายใต้บทบัญญัตินี้ ถ้าหากว่าเขาได้กระทำความผิดตามมาตรา 1 ข้างต้นโดยมีเจตนา

(a) กระทำความผิดในสิ่งที่มาตรานี้ใช้บังคับ หรือ

(b) ให้ความสะดวกในการกระทำความผิดไม่ว่าจะเป็นการกระทำความผิดของตนเองหรือของผู้อื่น และความผิดที่เขาเจตนากระทำหรือให้ความสะดวกดังจะกล่าวต่อไปในมาตรานี้ให้ถือว่าเป็นผู้กระทำความผิดเช่นเดียวกับผู้ที่กระทำความผิดที่ตนช่วยเหลือ

(2) มาตรานี้ใช้กับความผิด

(a) ความผิดที่บัญญัติไว้ในกฎหมายหรือ

(b) ใช้กับบุคคลที่มีอายุตั้งแต่ 21 ปีขึ้นไป

(3) ภายใต้บทบัญญัติของมาตรานี้ ไม่ว่าการกระทำความผิดของผู้กระทำที่อยู่ระยะไกล (Remote) จะได้กระทำไปในโอกาสที่ปราศจากอำนาจเข้าสู่ระบบหรือไม่ หรือโดยอาศัยโอกาสอื่นใดก็ตาม

(4) บุคคลอาจจะมีความผิดตามมาตรานี้ แม้จะปรากฏข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำที่อยู่ระยะไกลจะไม่ได้กระทำลงก็ตาม

(5) บุคคลผู้กระทำความผิดตามมาตรานี้จะต้อง

(a) ถูกพิจารณาอย่างรวดเร็วและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

จากบทบัญญัติดังกล่าวข้างต้นจะเห็นได้ว่าความผิดฐานนี้เป็นความผิดที่มีความซับซ้อนกว่าและร้ายแรงกว่าความผิดฐานเข้าถึงโดยปราศจากอำนาจ จึงไม่นำมาบัญญัติเอาไว้ต่างหาก เพราะการกระทำความผิดในมาตรานี้จะต้องเป็นการกระทำโดยเจตนาที่จะกระทำความผิดและปราศจากอำนาจที่จะกระทำ หรือเป็นการกระทำเพื่อให้ความสะดวกแก่ผู้กระทำความผิดเพื่อที่จะกระทำความผิดที่ร้ายแรง ข้อแตกต่างระหว่างมาตรา 1 กับมาตรา 2 นี้จึงอยู่ที่การพิสูจน์เจตนาในอนาคต นั่นคือการกระทำความผิดตามมาตรา 1 เป็นการกระทำที่ไม่อาจพิสูจน์เจตนาในอนาคตได้ ซึ่งจะมีโทษเบากว่า โดยถือว่าเป็นความผิดที่เรียกว่า “ความผิดที่ไกลออกไป” (Further Offence) หมายถึงความผิดที่ไม่จำเป็นต้องพิสูจน์ถึงเจตนาของผู้กระทำความผิดว่าได้เกิดขึ้นหรือไม่ แต่ถ้าเป็นกรณีที่สามารถพิสูจน์เจตนาในอนาคตได้ก็จะเป็นการกระทำความผิดตามมาตรา 2 ที่จะมีบทลงโทษผู้กระทำความผิดที่คิดจะกระทำความผิดในอนาคต และถ้าหากไม่สามารถลงโทษผู้กระผิดตามมาตรา 2 นี้ได้ก็สามารถลงโทษได้ตามมาตรา 1 ความผิดที่เกิดขึ้นในลักษณะนี้ ได้แก่ ความผิดฐานฉ้อโกง ความผิดฐานลักทรัพย์ และความผิดฐานยักยอกทรัพย์

การพิจารณาความรับผิดทางอาญาในทางคอมมอนลอว์ สำหรับความผิดฐานนี้สามารถแยกพิจารณาได้ ดังนี้

ก. การกระทำ (Actus Reus) โจทก์ต้องพิสูจน์ให้ได้ว่าจำเลยได้เข้าถึงสาระสำคัญ ได้แก่ โปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์ และ

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) ผู้กระทำมีเจตนาที่จะกระทำความผิดอื่นโดยไม่คำนึงถึงเวลาของการกระทำความผิดอื่นว่าจะกระทำในเวลาใด ไม่ว่าจะเป็นขณะที่เกือบจะเป็นเวลาเดียวกับที่เข้าถึงโดยปราศจากอำนาจ หรือในโอกาสต่อมา นั่นคือหากผู้กระทำความผิดเพียงแต่ได้ข้อเท็จจริงมาโดยตั้งใจที่จะกระทำการเข้าถึงโดยปราศจากอำนาจ แต่ยังไม่ลงมือกระทำก็ถือว่ามีความผิดตาม (4) แล้ว

3.2.2.3 ความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ (Modification of Computer Material หรือ Unauthorized Modification) ความผิดเกี่ยวกับการ

ทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 3 บัญญัติว่า

(1) บุคคลจะมีความผิดถ้า

(a) ผู้นั้นได้กระทำการใดๆ ซึ่งก่อให้เกิดการแก้ไขเปลี่ยนแปลงในเนื้อหาสาระของคอมพิวเตอร์ใดๆ และ

(b) ผู้ที่กระทำการเช่นว่านั้น จะต้องมีเจตนาหรือจะต้องรู้ถึงการกระทำของตนในขณะที่กระทำการนั้น

(2) ภายใต้บทบัญญัติของอนุมาตรา (1) (b) เจตนานั้นจะต้องเป็นเจตนาที่ต้องการแก้ไขเปลี่ยนแปลงเนื้อหาสาระของคอมพิวเตอร์ใดๆ โดยการกระทำ เช่น

(a) ทำให้เกิดความเสียหายต่อการทำงานของเครื่องคอมพิวเตอร์

(b) ขัดขวางหรือทำการกีดกันการเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลในคอมพิวเตอร์หรือ

(c) ทำให้เกิดความเสียหายต่อการทำงานของโปรแกรมคอมพิวเตอร์ หรือทำลายความเชื่อถือของข้อมูล

(3) เจตนาของการกระทำดังกล่าว ไม่จำต้องเป็นเจตนาโดยตรงต่อ

(a) คอมพิวเตอร์เฉพาะเจาะจงใดๆ

(b) โปรแกรมหรือข้อมูลพิเศษเฉพาะเจาะจงใดๆ หรือโปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่งโดยเฉพาะ หรือ

(c) การแก้ไขเปลี่ยนแปลงพิเศษเฉพาะเจาะจงใดๆ หรือการแก้ไขเปลี่ยนแปลงชนิดใดชนิดหนึ่งโดยเฉพาะ

(4) ภายใต้บทบัญญัติของอนุมาตรา (1) (b) ผู้กระทำต้องรู้ว่าการแก้ไขเปลี่ยนแปลงดังกล่าว กระทำไปโดยปราศจากอำนาจ และผู้กระทำมีเจตนาเช่นนั้น

(5) มาตรานี้ไม่ถือวัตถุประสงค์เป็นสิ่งสำคัญ โดยไม่คำนึงถึงการแก้ไขเปลี่ยนแปลงโดยปราศจากอำนาจ หรือผลจากเจตนาที่จะก่อขึ้นตาม (2) ไม่ว่าจะเป็นเจตนาที่จะก่อให้เกิดขึ้นเป็นการถาวรหรือชั่วคราว

(6) การแก้ไขเปลี่ยนแปลงในเนื้อหาสาระของคอมพิวเตอร์ตามกฎหมายฉบับนี้ จะไม่ถือว่าเป็นการก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ใดๆ ตามกฎหมายอาญาเกี่ยวกับการก่อให้เกิดความเสียหายเว้นแต่การกระทำนั้นมีผลทางกายภาพเท่านั้น

(7) บุคคลที่กระทำความผิดตามมาตรานี้จะต้อง

DPU

(a) ถูกพิจารณาอย่างรวดเร็วและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

การพิจารณาความรับผิดทางอาญาในทางคอมมอนลอว์ สำหรับความผิดฐานนี้สามารถแยกพิจารณาได้ ดังนี้

ก. การกระทำ (Actus Reus) มีการกำหนดขอบเขตของการกระทำความผิดไว้ค่อนข้างจำกัด โดยเน้นแต่เฉพาะที่เป็นการแก้ไขเปลี่ยนแปลง (Modification) ในเนื้อหาสาระ (Content) ของคอมพิวเตอร์เท่านั้น และแม้ว่าการกระทำดังกล่าวจะมีความสัมพันธ์กับการก่อให้เกิดความเสียหายทางอาญา แต่ก็ไม่ถือว่าเป็นความผิดตามกฎหมายอาญา เว้นแต่จะเป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายทางกายภาพ

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) ผู้กระทำจะต้องมีเจตนาและรู้อยู่ในขณะที่กระทำการแก้ไขเปลี่ยนแปลง ส่วนผลของการกระทำนั้นจะก่อให้เกิดความเสียหายกับทำให้เกิดความเสียหายต่อการทำงานของเครื่องคอมพิวเตอร์ ขัดขวางหรือทำการกีดกันการเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลในคอมพิวเตอร์ ทำให้เกิดความเสียหายต่อการทำงานของโปรแกรมคอมพิวเตอร์ หรือทำลายความเชื่อถือของข้อมูลเครื่องคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือข้อมูลในเครื่องคอมพิวเตอร์อย่างไรไม่จำต้องนำมาพิจารณา

3.2.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ กฎหมายที่เป็นหลักเกณฑ์ในการค้นหาพยานหลักฐานของอังกฤษ คือ The Police and Criminal Evidence Act 1984 (PACE) มาตรา 1 บัญญัติว่า “การค้นเคหสถานต้องมีเหตุอันควรสงสัยตามสมควร โดยถือมาตรฐานของบุคคลในฐานะและพฤติการณ์เดียวกับผู้ค้นเป็นเกณฑ์” และการค้นจะต้องมีการออกหมายค้นจากศาล (Justice of the peace) โดยศาลจะออกหมายค้นก็ต่อเมื่อเป็นเหตุอันควรเชื่อว่าเป็นความผิดอาญาร้ายแรง (Serious arrestable offence) ดังนั้น จึงต้องพิจารณาว่าอาชญากรรมคอมพิวเตอร์จะถือเป็นความผิดอาญาร้ายแรงที่ศาลสมควรจะออกหมายค้นหรือไม่

การค้นและยึดพยานหลักฐานต่างๆ ตามกฎหมายวิธีพิจารณาความอาญาของประเทศอังกฤษต้องคำนึงถึงแนวความคิดในเรื่องการคุ้มครองสิทธิมนุษยชนในทางอาญา ซึ่งได้บัญญัติรับรองไว้ในกฎบัตรแมคนาคาร์ตา (Magna Carta, 1215) กฎหมายของประเทศอังกฤษได้วางมาตรการควบคุม และตรวจสอบการทำงานของเจ้าพนักงานตำรวจโดยองค์กรภายนอกเอาไว้ ขณะเดียวกันก็ไม่ทำให้ประสิทธิภาพในการดำเนินงานของเจ้าหน้าที่ลดลง โดยให้เจ้าหน้าที่ของรัฐ

ได้แก่ ตำรวจ อัยการ และผู้พิพากษา สามารถใช้ดุลพินิจในการบังคับใช้กฎหมายได้มากขึ้น และในขณะเดียวกันก็มีข้อบังคับที่ตราขึ้นเพื่อควบคุมการปฏิบัติงานเอาไว้โดยละเอียด[11]

การค้นตาม The Police and Criminal Evidence Act 1984 (PACE) สามารถแยกพิจารณาได้ ดังนี้

3.2.3.1 การค้นเครื่องคอมพิวเตอร์พีซีในที่รโหฐาน

3.2.3.2 การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN ระบบ WAN และระบบอินเตอร์เน็ต

3.2.3.3 การยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์

3.2.3.1 การค้นเครื่องคอมพิวเตอร์พีซีในที่รโหฐาน ตาม PACEวางหลักไว้ในมาตรา 1 ว่า การค้นในเคหสถานต้องมีเหตุอันควรสงสัยตามสมควร โดยถือเอามาตรฐานของบุคคลในฐานะและพฤติการณ์เดียวกับผู้ค้นเป็นเกณฑ์ และจะต้องขอหมายค้นจากศาล[12] ดังนั้นในการค้นข้อมูลอิเล็กทรอนิกส์ ไม่ว่าจะอยู่ที่ใดทั้งที่อยู่ในเคหสถาน หรือที่รโหฐานอื่น เจ้าพนักงานตำรวจจะต้องมีเหตุอันควรสงสัยตามสมควรว่าจะมีพยานหลักฐานอยู่ที่นั้น และจะต้องมีศาลเป็นผู้ทำหน้าที่ตรวจสอบการดำเนินงานอีกชั้นหนึ่ง ในการออกหมายค้นนั้นศาลจะออกให้ก็ต่อเมื่อมีเหตุอันควรเชื่อว่ามีความผิดอาญาร้ายแรง (Serious Arrestable Offence) เกิดขึ้นและพยานหลักฐานที่จะพิสูจน์ความผิดได้ถูกเก็บอยู่ในนั้น จึงต้องพิจารณาว่าอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นเป็นความผิดอาญาร้ายแรงที่ศาลจะออกหมายค้นหรือไม่ ถ้าอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นเป็นความผิดอาญาร้ายแรง ศาลก็จะออกหมายค้นให้ และในการเข้าตรวจค้นตามหลักใน PACE มาตรา 16 จะต้องกระทำภายในหนึ่งเดือนนับแต่วันออกหมายค้น โดยจะต้องแจ้งเหตุแห่งการค้น และต้องค้นในเวลาที่เหมาะสม กรณีที่เจ้าของบ้านอยู่ด้วยในเวลาที่ค้น ตำรวจต้องแสดงหมายและมอบสำเนาหมายค้นให้ไว้ แต่ถ้าเจ้าของบ้านไม่อยู่ต้องปิดหมายค้นไว้ในที่ที่เหมาะสม แต่พยานหลักฐานนั้นต้องไม่เป็นพยานหลักฐานที่เป็นความลับตาม PACE มาตรา 15 ,16

กรณีการค้นโดยไม่มีหมายวางหลักไว้ใน PACE มาตรา 17 กำหนดให้ผู้ค้นจะต้องเป็นเจ้าพนักงานตำรวจที่อยู่ในเครื่องแบบ และต้องเป็นการค้นเพื่อช่วยชีวิตบุคคลในเคหสถานนั้น และเพื่อป้องกันการทำลายทรัพย์อย่างร้ายแรง

3.2.3.2 การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN ระบบ WAN และระบบอินเตอร์เน็ต

---

[11]ณรงค์ ใจหาญและคณะ. (2540). **รายงานศึกษาวิจัยฉบับสมบูรณ์ เรื่อง สิทธิผู้ต้องหา จำเลย และผู้ต้องโทษในคดีอาญา (รายงานการศึกษาวิจัยเสนอต่อคณะกรรมการกฤษฎีกา)**. หน้า 23.

[12] ณรงค์ ใจหาญและคณะ. เล่มเดิม. หน้า 51.

ตำรวจอังกฤษจะใช้วิธีนำเครื่องคอมพิวเตอร์หรือเครื่องมืออื่นเชื่อมเข้าไปในระบบเฉพาะของสำนักงาน และระบบเครือข่ายอินเตอร์เน็ต เพื่อเข้าไปตรวจค้นข้อมูลในนั้น จะขอหมายจาก Justice of the Peace ไม่ได้ แต่จะต้องขอจาก Circuit Judge และศาลจะออกหมายให้ต่อเมื่อไต่สวนได้ความว่า "มีเหตุอันควรเชื่อว่าพยานหลักฐานที่เกี่ยวกับการสอบสวนในคดีความผิดเป็น ความผิดอาญาร้ายแรง (Serious Arrestable Offence) ซึ่งเกิดขึ้นในบ้านนี้ และถ้าไม่ค้นบ้านนี้ก็จะไม่ได้มาซึ่งพยานหลักฐานดังกล่าว และในการค้นนั้นจะได้มาซึ่งพยานหลักฐานอันเป็นประโยชน์ต่อสาธารณชน"[13]

3.2.3.3 การยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์ ในการยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์มีบัญญัติอยู่ใน PACE มาตรา 18,19 ดังนี้

มาตรา 18 บัญญัติว่า "เมื่อค้นแล้วตำรวจต้องทำบันทึกการค้นและบันทึกรายการสิ่งของที่ค้นและยึด รายการเหล่านั้นผู้ค้นต้องมอบให้แก่เจ้าของบ้านเมื่อผู้นั้นร้องขอ" และ

มาตรา 19 บัญญัติว่า "กรณีที่ตำรวจยึดวัตถุที่มีเหตุเชื่อได้ว่าเป็นพยานหลักฐานที่เกี่ยวข้องกับการสอบสวน หรือความผิดอื่น หรือมีความผิดอื่นรวมอยู่ด้วย หรือมีความจำเป็นต้องยึดเพื่อป้องกันการเคลื่อนย้าย ซ่อนเร้น หรือทำลายหลักฐาน"

จากบทบัญญัติข้างต้นจะเห็นได้ว่าเครื่องคอมพิวเตอร์ที่ยึดได้นั้นเป็นวัตถุที่ใช้เป็นพยานหลักฐานในการสอบสวนที่เจ้าหน้าที่ตำรวจยึดได้ รวมทั้งข้อมูลที่อยู่ภายในเครื่องด้วย เว้นแต่กรณีที่เป็นข้อมูลที่เป็นความลับ ที่จะต้องพิจารณาตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลประกอบ

3.2.4 การรับฟังเป็นพยานหลักฐานในศาล การรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ของศาลอังกฤษ โดยหลักจะรับฟังแต่พยานหลักฐานโดยตรง พยานบอกเล่า (Hearsay) ถือว่ามีน้ำหนักน้อยหรือไม่รับฟังเลย แต่ The Police and Criminal Evidence Act 1984 เป็นกฎหมายพยานหลักฐานในคดีอาญา ที่มีบทบัญญัติเกี่ยวกับการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์อยู่ เป็นข้อยกเว้นของพยานบอกเล่า (Hearsay) โดยให้รับฟังพยานเอกสารที่เป็นผลจากการประมวลผลหรือคำนวณของเครื่องคอมพิวเตอร์ได้ การค้นและยึดพยานหลักฐานกระทำโดยเจ้าพนักงานตำรวจ กรณีที่ประสบปัญหาการกระทำความผิดทางอินเตอร์เน็ตที่การกระทำอาจเกิดขึ้นในต่างประเทศ อำนาจในการสอบสวนจะสามารถกระทำได้เพียงใด เช่น การกระทำความผิดเกิดขึ้นในประเทศเยอรมนี และผู้กระทำความผิดอยู่ที่ประเทศนั้น แต่เครือข่ายที่ใช้ข้อมูลหรือข้อมูลที่ใช้ผ่านประเทศอังกฤษจะต้องคำนึงถึงข้อตกลงระหว่างประเทศ โดยเฉพาะข้อตกลงระหว่าง

---

[13] ณรงค์ ใจหาญและคณะ. เล่มเดิม. หน้า 52.

ประชาคมยุโรปด้วย แม้ว่าจะต้องคำนึงถึงเรื่องดังกล่าวการดำเนินคดีตามกฎหมายอังกฤษจะถือหลักว่า ถ้าเข้าหลักเกณฑ์ 2 ประการดังต่อไปนี้ประเทศอังกฤษก็อาจจะไม่นำมาดำเนินคดี คือ

ก. ถ้าผู้กระทำความผิดหรือผู้ร่วมกระทำความผิดไม่ใช่พลเมืองของประเทศอังกฤษ หรือ

ข. ความผิดที่เกิดขึ้นไม่ได้บัญญัติไว้ใน The Computer Misuse Act 1990

ศาลที่มีอำนาจในการพิจารณาคดี สามารถแบ่งได้ตามฐานความผิด ดังนี้

(1) ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access) เป็นการกระทำความผิดที่ไม่ซับซ้อน ศาลที่มีอำนาจในการพิจารณาคดีคือศาลแขวง(Magistrate Court) จึงมีกฎหมายที่เกี่ยวข้องอีกฉบับคือ The Magistrate's Court Act 1980 เป็นเรื่องเกี่ยวกับการกำหนดฐานความผิดแก่ผู้ที่ให้ความช่วยเหลือในการกระทำความผิดใน มาตรา 44 (1) ซึ่งบัญญัติว่า "สามารถลงโทษบุคคลที่ให้ความช่วยเหลือผู้ที่กระทำการเข้าถึงโดยปราศจากอำนาจ โดยการให้ความรู้ทางด้านข้อมูล การให้รหัสผ่าน หรือให้วิธีการเข้าสู่ระบบเพื่อผ่านไปยังโปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์"

(2) ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง และความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ ขึ้นอยู่กับความร้ายแรงของการกระทำความผิด หากมีความร้ายแรงมากก็จะอยู่ในอำนาจพิจารณาของศาลสูงคดีอาญา (Crown Court) แต่ถ้าไม่ร้ายแรงมากก็จะอยู่ในอำนาจพิจารณาของศาลแขวง (Magistrate Court)

โดยลักษณะของข้อมูลอิเล็กทรอนิกส์ที่ไม่สามารถพิสูจน์ได้ในทางกายภาพ จึงไม่สามารถนำมาพิสูจน์ในกระบวนพิจารณาคดีอาญาได้ ดังนั้นรายงานที่ประมวลผลจากคอมพิวเตอร์ (Printout) จะเป็นพยานบอกเล่า (Hearsay) เนื่องจากเกิดจากการกระทำของมนุษย์ ต้องห้ามรับฟังตามกฎหมาย Criminal Justice Act 1988 มาตรา 24 แต่จากความสามารถในการทำงานของคอมพิวเตอร์เองที่สามารถใช้เป็นเครื่องกล หรือเครื่องมือในการคำนวณ จึงไม่น่าจะเป็นพยานหลักฐานในรูปพยานบอกเล่าเสมอไป ถ้าอ้างเป็นพยานหลักฐานโดยยืนยันการใช้ที่เป็นธุรกิจปกติ และข้อมูลที่ได้ก็เกิดจากการประมวลผลโดยคอมพิวเตอร์อันเป็นปกติเช่นกัน[14]

3.3 ประเทศญี่ปุ่น

---

[14] Richard May. (1999). **Criminal Evidence. London**. p. 11-36.

รัฐธรรมนูญของประเทศญี่ปุ่นไม่ได้วางหลักคุ้มครองความเป็นอยู่ส่วนตัวไว้โดยชัดแจ้งแต่เป็นหลักที่อาจสังเคราะห์ขึ้นจากหลักเสรีภาพทั่วไปที่บัญญัติไว้ในมาตรา 13[15] ประกอบกับหลักเสรีภาพในการติดต่อสื่อสารกันโดยอิสระในมาตรา 21[16] และหลักเสรีภาพในเคหสถาน ในเอกสาร และทรัพย์สินส่วนตัว ในมาตรา 35[17] ดังนั้นการเข้าไปในเคหสถาน การค้นและการยึดทรัพย์สินจะกระทำมิได้ ยกเว้นมีหมายที่ออกโดยข้าราชการฝ่ายตุลาการ โดยในหมายนั้นจะต้องระบุเหตุผลที่สมควรและกำหนดสถานที่ตรวจค้นและทรัพย์ที่ต้องการยึดไว้โดยชัดแจ้ง

3.3.1 มาตรการเพื่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศญี่ปุ่น การค้นตามกฎหมายวิธีพิจารณาความอาญาของญี่ปุ่นนั้น ให้อำนาจพนักงานอัยการ หรือเจ้าพนักงานตำรวจดำเนินการค้นได้ ภายใต้รัฐธรรมนูญ มาตรา 35 วรรคหนึ่ง ดังนั้นทำการค้นได้ตามกฎหมายญี่ปุ่นต้องมีหมายค้น การค้นข้อมูลอิเล็กทรอนิกส์ก็เช่นกัน ยกเว้นกรณีที่เป็นการกระทำความผิดซึ่งหน้าตามมาตรา 33 ที่ไม่ต้องมีหมายค้น เนื่องจากเป็นการกระทำความผิดหรือถูกจับเนื่องจากการกระทำความผิดซึ่งหน้า รัฐธรรมนูญได้วางหลักเกณฑ์ให้เจ้าพนักงานสามารถค้น และยึดได้ก็ต่อเมื่อมีหมายค้นหรือหมายยึด หรือเป็นกรณีที่เป็นการค้นหรือการยึดที่สืบเนื่องจากการจับกุมตัวผู้กระทำความผิด

สำหรับการค้นเพื่อทำการยึดจดหมายหรือโทรสาร เนื่องจากรัฐธรรมนูญได้ให้ความคุ้มครองสิทธิเสรีภาพในการสื่อสารของบุคคลไว้ใน มาตรา 35 วรรคหนึ่ง ดังนั้นการยึดจดหมายหรือโทรสารที่บุคคลใช้ติดต่อสื่อสารกันย่อมเป็นการกระทำที่ขัดต่อสิทธิเสรีภาพในการสื่อสารที่รัฐธรรมนูญได้บัญญัติรับรองไว้ แต่ถ้าเป็นกรณีที่เจ้าพนักงานกระทำไปเพื่อการแสวงหาพยานหลักฐานในการพิสูจน์ความผิด หรือเพื่อป้องกันอาชญากรรมก็สามารถดำเนินการค้นและยึดได้ [18]

---

[15] มาตรา 13 บัญญัติว่า "ประชาชนทุกคนย่อมได้รับการเคารพในฐานะปัจเจกบุคคล สิทธิของประชาชนในชีวิต เสรีภาพ และการแสวงหาความผาสุกภายในขอบเขตที่ไม่ขัดต่อประโยชน์สุขอันร่วมกันของสาธารณะ ต้องได้รับความเคารพสูงสุดในการออกกฎหมายหรือในการอื่นใดที่เกี่ยวกับการปกครองประเทศ"

[16] มาตรา 21 บัญญัติว่า "เสรีภาพในการชุมนุม การรวมกลุ่ม รวมทั้งการพูด การพิมพ์ และสิ่งใดทั้งปวงที่เป็นการแสดงออกเป็นสิ่งที่ได้รับการคุ้มครอง

[17] มาตรา 35 บัญญัติว่า "บุคคลใดก็ตาม หากไม่มีหมายซึ่งออกโดยเหตุผลอันชอบธรรมและระบุชัดถึงสถานที่ที่จะตรวจค้นและสิ่งของที่จะอายัด สิทธิที่จะไม่ให้เข้าไปในเคหสถาน ไม่ให้ถูกตรวจค้นและอายัดเอกสารและสิ่งของในครอบครอง ย่อมจะไม่ถูกละเมิด เว้นแต่กรณีตามมาตรา 33

การตรวจค้นและอายัดจะดำเนินการโดยหมายแต่ละประเภท ซึ่งออกโดยเจ้าพนักงานกระบวนการยุติธรรมที่มีอำนาจ"

[18] Shigemitsu Dando. (1965). **Japanese Criminal Procedure**. p. 270

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในการประมวลผลด้วยเครื่องคอมพิวเตอร์ของหน่วยงานฝ่ายปกครอง ค.ศ. 1988 รัฐสภาญี่ปุ่นบัญญัติขึ้นโดยอาศัยแนวทางของ Organization for Economic Co-operation and Development (OECD) ที่เสนอให้กำหนดหน้าที่ของหน่วยงานในการรักษาความปลอดภัย วางหลักเกณฑ์ในการเข้าถึงข้อมูล และการแก้ไขข้อมูลให้ถูกต้อง โดยกฎหมายฉบับนี้ได้กำหนดให้หน่วยงานของรัฐจำกัดบทบาทในการรวบรวมข้อมูลข่าวสารส่วนบุคคลและโฆษณาให้สาธารณชนทราบการจัดระบบข้อมูลข่าวสารส่วนบุคคลของหน่วยงาน และห้ามมิให้หน่วยงานของรัฐใช้ข้อมูลของรัฐโดยผิดวัตถุประสงค์ คือห้ามมิให้นำข้อมูลข่าวสารส่วนบุคคลซึ่งจัดเก็บโดยมีวัตถุประสงค์อย่างหนึ่งไปใช้ในวัตถุประสงค์อย่างอื่น

3.3.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ การดักฟังการติดต่อสื่อสารถือเป็นการละเมิดเสรีภาพในการติดต่อสื่อสารซึ่งได้รับความคุ้มครองตามรัฐธรรมนูญ มาตรา 21 วรรคสองตอนท้าย บัญญัติว่า “ความลับในการสื่อสารจะละเมิดมิได้” ดังนั้นโดยหลักแล้วการดักฟังย่อมกระทำมิได้ อย่างไรก็ดีรัฐสภาญี่ปุ่นได้ตรากฎหมายว่าด้วยการดักฟังการสื่อสารทางโทรคมนาคม (Communications Interception Law) ขึ้นใช้บังคับในเดือนสิงหาคม ค.ศ. 1999 ซึ่งให้อำนาจเจ้าพนักงานอัยการหรือตำรวจชั้นผู้ใหญ่ในการดักฟังทางโทรศัพท์หรือการดักจับสัญญาณโทรสารและติดตามเฝ้าดูกฎหมายอิเล็กทรอนิกส์ในการสอบสวนคดียาเสพติด การฆาตกรรม หรือคดีอาญาที่มีการใช้อาวุธ หรือการลักลอบหนีภาษีของชาวต่างชาติ โดยจะต้องได้รับอนุญาตจากศาล และให้มีระยะเวลาดักฟังยาวนานที่สุดไม่เกิน 10 วัน โดยจะขอขยายได้ไม่เกิน 30 วัน

นอกจากนี้ในการดักฟังจะต้องมีบุคคลอื่นที่เป็นบุคคลภายนอก เช่น เจ้าหน้าที่ของบริษัทโทรเลขโทรศัพท์แห่งชาติของญี่ปุ่นร่วมฟังด้วยและภายหลังจากการดักฟังสิ้นสุดลงเจ้าพนักงานตำรวจหรือพนักงานอัยการซึ่งทำหน้าที่ดักฟังจะต้องแจ้งให้ผู้ถูกดักฟังทราบถึงการดักฟังนั้นภายใน 30 วัน

สำหรับสิ่งที่กฎหมายญี่ปุ่นบัญญัติไม่ให้ดำเนินการค้นหรือยึด[19] ได้แก่

ก. เอกสารที่เป็นความลับทางราชการ ซึ่งเจ้าพนักงานจะทำการค้นหรือยึดได้ก็ต่อเมื่อมีคำร้องไปยังหัวหน้าหน่วยงานที่มีเอกสารดังกล่าว และต้องได้รับความยินยอมให้ทำการตรวจค้นหรือยึดเอกสารดังกล่าวจากหัวหน้าหน่วยงานนั้นๆด้วย หากหัวหน้าหน่วยงานดังกล่าวไม่ยินยอมให้ค้นหรือยึดเอกสารนั้น เนื่องจากความมั่นคงของประเทศก็สามารถทำได้

---

[19] Ibid. p.300.

ข. เอกสารหรือสิ่งของที่เป็นความลับของลูกค้าในทางการแพทย์ หรือลูกความ เจ้าพนักงานไม่สามารถเข้าไปค้นหรือยึดได้ เว้นแต่จะได้รับความยินยอมจากบุคคลผู้ครอบครอง หากผู้ครอบครองไม่ยินยอมให้เจ้าพนักงานทำการค้นหรือยึดก็ต้องแจ้งเหตุผลที่ไม่ยินยอมให้เจ้าพนักงานทราบด้วย

3.3.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ รัฐธรรมนูญของประเทศญี่ปุ่นบัญญัติไว้ว่าการค้นจะกระทำได้ก็ต่อเมื่อมีหมายที่ออกโดยศาล และจะต้องเป็นการค้นเพื่อการสืบสวนการกระทำความผิดอาญา เป็นการแสวงหาพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดอาญา ซึ่งการแสวงหาพยานหลักฐานดังกล่าวจะกระทำได้ทั้งก่อน และระหว่างการพิจารณา

3.3.3.1 เหตุแห่งค้น ตามกฎหมายประเทศญี่ปุ่น แบ่งออกเป็น 2 ประเภท ได้แก่

ก. กรณีปกติ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 218 กฎหมายบัญญัติให้อำนาจเจ้าพนักงานของรัฐ ได้แก่ พนักงานอัยการ อัยการผู้ช่วย หรือตำรวจสามารถดำเนินการค้นและยึดได้ แต่ถ้าเป็นการค้นหรือยึดในที่รโหฐานก็ต้องดำเนินการตามหมายค้นหรือยึดที่ออกโดยศาล โดยกำหนดว่าการค้นหรือยึดสิ่งของต่างๆนั้นต้องเป็นไปเพื่อการสืบสวนการกระทำความผิดอาญา การสอบสวนเป็นกระบวนการที่กฎหมายอนุญาตให้เจ้าพนักงานดังกล่าวข้างต้นมีอำนาจในการแสวงหาพยานหลักฐานเพื่อพิสูจน์การกระทำความผิด โดยการแสวงหาพยานหลักฐานนั้นจะต้องกระทำก่อนหรือในระหว่างการพิจารณาคดี[20] เหตุที่เจ้าพนักงานจะขอหมายค้นหรือหมายยึดภายในที่รโหฐานได้ ต้องเป็นกรณีที่มีการแสวงหาพยานหลักฐานที่พิสูจน์การกระทำความผิดกรณีที่พยานหลักฐานดังกล่าวเป็นวัตถุสิ่งของ หากเป็นการค้นหาตัวบุคคลนั้นรัฐธรรมนูญ มาตรา 33 ได้กำหนดว่าเป็นการค้นเพื่อจับกุมผู้กระทำความผิดตามหมายจับ หรือค้นเพื่อหาตัวบุคคลที่ได้กระทำความผิดซึ่งหน้า เจ้าพนักงานสามารถดำเนินการค้นภายในที่รโหฐานได้โดยไม่จำเป็นต้องขอหมายศาล

ข. กรณีพิเศษ เป็นการค้นที่รโหฐานกรณีที่ไม่ต้องมีหมายค้น หรือหมายยึด แต่ก็ต้องเป็นกรณีที่สืบเนื่องมาจากการจับกุม ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 199 บัญญัติหลักเกณฑ์ที่สามารถทำได้ 3 กรณี ได้แก่

(1) การค้นและยึดที่สืบเนื่องจากการจับกุมภายใต้หมายจับที่ออกโดยศาล ตามมาตรา 199 ประกอบมาตรา 220 โดยมาตรา 220 อนุญาตให้เจ้าพนักงานสามารถทำการค้นและยึดสิ่งของกรณีที่เจ้าพนักงานทำการจับกุมผู้ต้องหาที่ศาลออกหมายจับได้ โดยกฎหมายกำหนดให้เจ้าพนักงาน

---

[20] Ibid. p.303.

เหล่านั้นแจ้งต่อศาลว่ามีการกระทำความผิดเกิดขึ้น และเชื่อว่าบุคคลที่จะต้องถูกจับมีความผิดอาญาดังกล่าว

หากเจ้าพนักงานเห็นว่าสิ่งใดสามารถใช้ในการพิสูจน์ความผิดได้ ก็สามารถนำเหตุผลดังกล่าวไปขออนุญาตต่อศาล เพื่อขอหมายค้นเข้าไปค้นหาสิ่งของดังกล่าวมาประกอบการพิจารณาได้ แต่ถ้าเป็นความผิดที่มีอัตราโทษน้อย เช่น โทษปรับไม่เกิน 100 เยน เป็นต้น ไม่จำต้องขอหมายจับจากศาล

3.3.3.2 วิธีการค้น ตามกฎหมายประเทศญี่ปุ่น แบ่งออกเป็น 2 ประเภท ได้แก่

ก.การค้นที่สืบเนื่องจากการจับกุมตามหมายจับ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 201 เมื่อเจ้าพนักงานได้รับหมายจับจากศาลแล้วสามารถไปดำเนินการตามหมายจับดังกล่าวได้เลย หากบุคคลดังกล่าวอยู่ภายในเคหสถาน หรือสถานที่ใดก็ตาม เจ้าพนักงานสามารถเข้าไปได้โดยไม่ต้องมีหมายค้นจากศาล แต่เมื่อพบบุคคลดังกล่าวแล้วก็ต้องแสดงหมายจับให้ดู

ข. การค้นที่สืบเนื่องจากการจับกุมที่ผู้กระทำความผิดได้กระทำความผิดซึ่งหน้า ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 213 บัญญัติให้อำนาจเจ้าพนักงานได้แก่ เจ้าพนักงานอัยการ อัยการผู้ช่วย หรือตำรวจ สามารถทำการจับกุมผู้ที่กระทำความผิดซึ่งหน้าตนได้โดยไม่ต้องมีหมายจับ ถ้าการจับกุมดังกล่าวเกิดขึ้นในที่รโหฐาน เจ้าพนักงานสามารถค้นและยึดสิ่งของภายในสถานที่ดังกล่าวได้โดยไม่ต้องมีหมาย แต่จะต้องเป็นกรณีที่สามารถออกหมายค้นหรือยึดได้ด้วย และเมื่อพบสิ่งที่ต้องการยึดแล้วจะต้องรีบคืนสิ่งของดังกล่าวให้เจ้าของที่แท้จริงโดยด่วน

สำหรับการกระทำความผิดซึ่งหน้านั้น ตามกฎหมายญี่ปุ่น ได้แก่การกระทำความผิดที่บุคคลได้ลงมือกระทำความผิดในขณะนั้น หรือเพิ่งลงมือกระทำความผิด มีลักษณะการกระทำความผิด 4 ประเภท [21] ได้แก่

(1) เมื่อพบเห็นการกระทำความผิดและติดตามจับกุมแบบกระชั้นชิด

(2) เมื่อพบผู้กระทำความผิดครอบครองทรัพย์สิน อาวุธ หรือสิ่งของที่เกี่ยวข้องกับการกระทำความผิด

(3) เมื่อพบว่าร่างกาย หรือเสื้อผ้าของบุคคลดังกล่าวมีร่องรอยการต่อสู้ บาดแผล หรือมีสิ่งที่บ่งบอกว่าได้กระทำความผิดมา

(4) เมื่อเจ้าพนักงานเรียกให้หยุดแต่กลับวิ่งหนี

---

[21] Ibid. p.310.

หากพบเห็นลักษณะของการกระทำประเภทใดประเภทหนึ่งข้างต้นแล้ว ผู้กระทำความผิดได้ถูกจับกุมในเคหสถาน หรือที่รโหฐาน เจ้าพนักงานที่มีอำนาจสามารถทำการตรวจค้นและยึดสิ่งของภายในสถานที่ดังกล่าวได้โดยไม่ต้องมีหมายค้น หรือยึด

ค. การค้นในกรณีฉุกเฉิน เป็นการค้นหรือการยึดในที่รโหฐานที่สืบเนื่องมาจากการจับกุมผู้ต้องหาในกรณีฉุกเฉินตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 210 กรณีที่มีเหตุเพียงพอที่จะเชื่อว่ามีการกระทำความผิดที่มีอัตราโทษจำคุกมากกว่า 3 ปีขึ้นไป โดยเจ้าพนักงานอัยการ อัยการผู้ช่วย หรือตำรวจ แต่ไม่สามารถขอหมายศาลได้ในขณะนั้น เป็นเหตุให้จับกุมโดยไม่มีหมาย เมื่อทำการจับกุมผู้ต้องหาได้แล้วต้องรีบดำเนินการขอหมายศาลทันที เมื่อเจ้าพนักงานทำการจับกุมผู้ต้องหาได้แล้ว เจ้าพนักงานก็สามารถทำการตรวจค้นหรือยึดได้โดยไม่ต้องมีหมายค้น แต่ถ้าศาลไม่ออกหมายจับให้ เจ้าพนักงานผู้ดำเนินการจับกุมก็ต้องปล่อยตัวบุคคลดังกล่าวทันที พร้อมทั้งคืนสิ่งที่ค้นหรือยึดมาด้วย หากศาลออกหมาย[22]

ง.การค้นโดยประชาชนทั่วไป กรณีที่เป็นการกระทำความผิดซึ่งหน้า ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 213 ให้อำนาจประชาชนทั่วไปสามารถจับกุมผู้ที่กระทำความผิดดังกล่าวได้ด้วย แต่กฎหมายไม่อนุญาตให้บุคคลดังกล่าวตรวจค้น หรือยึดสิ่งของ

3.3.3.3 ระยะเวลาในการค้น การที่กฎหมายให้อำนาจเจ้าพนักงานทำการค้นได้ถือเป็นการกระทำที่ละเมิดต่อสิทธิของบุคคลผู้เป็นเจ้าของ เพราะสิ่งที่กฎหมายประสงค์จะคุ้มครอง คือ สิทธิในการครอบครองและการพักอาศัยของบุคคลในเคหสถาน แต่ด้วยเหตุจำเป็นจึงอนุญาตให้ทำได้ อย่างไรก็ตามกฎหมายก็ได้กำหนดระยะเวลาในการค้นเอาไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 116 เนื่องจากเป็นการกระทำที่รบกวนสิทธิของผู้เป็นเจ้าของสถานที่กฎหมายจึงบัญญัติให้ทำการค้นและยึดได้แต่ในเวลากลางวันเท่านั้น ซึ่งเป็นเวลาตั้งแต่พระอาทิตย์ขึ้นจนถึงพระอาทิตย์ตก เพราะในเวลากลางคืนเป็นเวลาพักผ่อนของผู้ครอบครอง

กรณีที่เจ้าพนักงานทำการตรวจค้นในเวลากลางวันแล้วไม่เสร็จในช่วงเวลานั้น ก็สามารถทำการตรวจค้นต่อเนื่องไปในเวลากลางคืนได้ และกฎหมายก็ให้อำนาจทำการค้นในเวลากลางคืนได้ ตามมาตรา 117 กรณีที่ศาลเห็นว่าจำเป็นที่จะต้องทำการค้นในเวลากลางคืน โดยระบุลงไปในหมายไว้ด้วย สถานที่ที่ศาลอนุญาตให้ทำการตรวจค้นในเวลากลางคืนได้ เช่น สถานบันเทิงเริงรมย์ บ่อนการพนัน โรงแรม หรือร้านอาหาร ฯลฯ

---

[22] Ibid. p.316.

3.3.4 การรับฟังเป็นพยานหลักฐานในศาล ศาลสูงสุดของประเทศญี่ปุ่นได้วางมาตรการในการรับฟังพยานหลักฐานสำหรับการค้นเอาไว้เช่นเดียวกับประเทศอื่นๆ คือ ห้ามมิให้รับฟังพยานหลักฐานที่ได้มาจากการค้น โดยไม่มีหมายค้น โดยมาตรการดังกล่าวเป็นเพียงวิธีการในการป้องกันมิให้เจ้าหน้าที่ใช้อำนาจในทางมิชอบเท่านั้น มิใช่ไม่รับฟังพยานหลักฐานดังกล่าวเลย เพราะในทางปฏิบัติของศาลญี่ปุ่นการรับฟังพยานหลักฐานจะพิจารณาถึงความรุนแรงของการกระทำความผิด ประกอบกับความมุ่งหมายของการสอบสวน

จากการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกานั้นไม่ได้มีกฎหมายที่เป็นกลางซึ่งจะวางหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ กฎหมายที่มีผลใช้บังคับอยู่ในปัจจุบันเป็นแต่เพียงกฎหมายที่ให้ความคุ้มครองเฉพาะเรื่อง เช่น การเงิน คอมพิวเตอร์ ฯลฯ ทั้งยังขาดหน่ายงานอิสระที่เป็นองค์กรกลางคอยทำหน้าที่ควบคุม ตรวจตรา และบังคับการให้เป็นไปตามกฎหมาย สำหรับหน่วยงานที่มีอยู่ในปัจจุบันก็ขาดความเป็นอิสระและไม่มีอำนาจเด็ดขาด เนื่องจากเป็นหน่วยงานของฝ่ายบริหาร

สำหรับประเทศอังกฤษซึ่งให้ความเคารพต่อสิทธิส่วนบุคคล และความจำเป็นที่จะต้องดำเนินการให้กฎหมายภายในของตนสอดคล้องกับอนุสัญญาแห่งสภายุโรปว่าด้วยการให้ความคุ้มครองข้อมูล (The Council of Europe's Data Protection) รัฐสภาของประเทศอังกฤษจึงต้องออกกฎหมายเพื่อแสวงหาพยานหลักฐานของเจ้าพนักงานของรัฐ สามารถล่วงล้ำเข้าไปรับรู้ถึงข้อมูลที่เกี่ยวกับการดำเนินชีวิตของผู้ต้องสงสัยหรือสารสนเทศที่อยู่ในความครอบครองของผู้ใช้ และการแสดงความคิดเห็นส่วนตัว เท่ากับเป็นการล่วงล้ำข้อมูลส่วนบุคคลที่กฎหมายอังกฤษประสงค์จะให้ปกปิด ดังเช่นคดีระหว่างนายจ้างและลูกจ้างข้างต้น การรวบรวมพยานหลักฐานด้วยวิธีการดังกล่าวอาจถูกหาว่าเป็นพยานหลักฐานที่ได้มาโดยมิชอบได้ ทั้งกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของอังกฤษ ที่มีมาตรการควบคุม และตรวจสอบการทำงานของเจ้าหน้าที่โดยองค์กรภายนอกไว้อย่างรัดกุม และไม่ทำให้ประสิทธิภาพในการปราบปรามอาชญากรรมของเจ้าหน้าที่ลดลง โดยการให้ดุลพินิจในการปฏิบัติหน้าที่ของเจ้าหน้าที่ ภายใต้กฎเกณฑ์ที่กฎหมายบัญญัติไว้ จึงดูมีความน่าเชื่อถือที่สุด

ประเทศญี่ปุ่นเองก็มีความพยายามที่จะตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลไว้เป็นกฎหมายทั่วไป แต่ก็ไม่ได้วางมาตรการที่ให้ความคุ้มครองที่เคร่งครัดเกินไป เพราะในขณะเดียวกันก็ให้ตรากฎหมายให้อำนาจเจ้าพนักงานของรัฐเข้าสู่ข้อมูลบางประเภทได้ แต่การแสวงหาพยานหลักฐานจากข้อมูลส่วนบุคคลในประเทศญี่ปุ่นเมื่อเทียบกับอีกสองประเทศข้างต้น ก็ยังเป็นเรื่องใหม่ที่ยังต้องรอให้มีการวางมาตรการ บัญญัติกฎหมายลำดับรอง เพื่อบังคับใช้ตามกฎหมายที่มีอยู่ให้มีประสิทธิภาพมากขึ้น เนื่องจากกฎหมายที่มีนั้นยังไม่สามารถนำมาใช้บังคับได้อย่างเต็มที่

อย่างไรก็ดีประสบการณ์ของทั้งสามประเทศต่างก็มีประโยชน์ต่อการนำมาศึกษาเปรียบเทียบกับกฎหมายของไทยที่มีอยู่

DPU

บทที่ 4
วิเคราะห์มาตรการทางกฎหมายในการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในประเทศไทย

ระบบอินเตอร์เน็ตได้รับการพัฒนาขึ้นมาเพื่อประโยชน์ทางด้านการสื่อสารระหว่างมนุษย์ในรูปของสื่อผสม (Multimedia) ซึ่งบุคคลสามารถติดต่อถึงกันได้โดยอาศัยสื่อหลายประเภทผสมกัน ไม่ว่าจะเป็นการรับส่งข้อความธรรมดา การรับส่งภาพ หรือเสียง ตลอดจนข้อมูลอิเล็กทรอนิกส์ เช่น โปรแกรมคอมพิวเตอร์ [1] มีการส่งเสริมให้มีการใช้คอมพิวเตอร์ในประเทศต่างๆ แม้เครื่องมืออิเล็กทรอนิกส์ โดยเฉพาะคอมพิวเตอร์และเครือข่ายอินเตอร์เน็ตนั้นก็มีทั้งคุณและโทษ แต่ก็น่าจะเป็นคุณมากกว่า ประเทศต่างๆจึงให้ความสำคัญ และพยายามที่จะหามาตรการมาแก้ปัญหาที่เกิดขึ้นบนเครือข่ายคอมพิวเตอร์ ประเทศต่างๆ ทั้งในยุโรป อเมริกา ออสเตรเลีย และประเทศในแถบเอเชีย เช่น ญี่ปุ่น ต่างก็พยายามหามาตรการป้องกันและปราบปรามการกระทำความผิดที่เกิดขึ้น แต่การบังคับใช้กฎหมายที่มีอยู่ในปัจจุบันมักไม่มีประสิทธิภาพ และสำหรับอาชญากรรมคอมพิวเตอร์ที่มีการกระทำความผิดที่มิใช่เกิดขึ้นแต่เพียงประเทศใดประเทศหนึ่ง แต่มีลักษณะเป็นอาชญากรรมข้ามชาติ จึงเกิดปัญหาความร่วมมือระหว่างประเทศ มาตรการในการแก้ไขปัญหาระหว่างประเทศในปัจจุบันอยู่ในรูปของความร่วมมือระหว่างประเทศ เพื่อลดช่องว่างที่มีอยู่ให้ลดน้อยลง หรือจัดให้มีความร่วมมือในลักษณะขององค์กรต่อองค์กร หรือประเทศต่อประเทศเพื่อช่วยเหลือซึ่งกันและกันในด้านการสืบสวนสอบสวน

4.1 มาตรการทางกฎหมายในการรับฟังเป็นพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในปัจจุบัน

เมื่อมีการกระทำความผิดเกี่ยวกับข้อมูลส่วนบุคคลที่เก็บอยู่ในเครื่องคอมพิวเตอร์เกิดขึ้น การกระทำดังกล่าวนอกจากจะเป็นอาชญากรรมคอมพิวเตอร์แล้ว การเข้าถึงข้อมูลในคอมพิวเตอร์โดยปราศจากอำนาจตามกฎหมายไทยถือเป็นการกระทำที่มิชอบก่อให้เกิดประเด็น

---

[1] พินัย ณ นคร. (2543, มิถุนายน). “กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์.” **บทบัณฑิตย์, 56, 2**. หน้า 1.

ปัญหา ดังนี้

4.1.1 การรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

4.1.1.1 ประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายวิธีพิจารณาความอาญา หมายถึง กฎหมายที่ว่าด้วยหลักเกณฑ์และวิธีการค้นหาความจริง อันเกี่ยวกับการกระทำความผิด และนำตัวผู้กระทำความผิดต่อกฎหมายอาญามาดำเนินการพิจารณา และลงโทษตามบทบัญญัติของกฎหมาย[2] แม้การกระทำความผิดอาญาจะเป็นการกระทำที่กระทบกระเทือนต่อสังคมโดยรวมก็ตาม แต่การดำเนินคดีอาญาก็ย่อมมีผลกระทบต่อสิทธิและเสรีภาพส่วนบุคคลโดยง่ายด้วย จึงต้องคำนึงถึงกฎหมายวิธีพิจารณาความอาญาที่ให้ความคุ้มครองสิทธิและเสรีภาพส่วนบุคคลในฐานะที่เขาเป็นส่วนหนึ่งของสังคม[3]

ในคดีอาญาพยานหลักฐานทุกชนิดรับฟังได้ ยกเว้นพยานหลักฐานที่ได้มาโดยมิชอบตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 สำหรับข้อมูลอิเล็กทรอนิกส์ ที่ได้มาจากการค้นที่มีหมายพยานหลักฐานดังกล่าวย่อมรับฟังได้ แต่ถ้าหากเป็นการค้นที่ไม่มีหมายพยานหลักฐานที่ได้ก็ไม่สามารถรับฟังได้ เพราะการจะเชื่อถือพยานหลักฐานนั้นเพียงใด ก็ขึ้นอยู่กับการชั่งน้ำหนักพยานหลักฐาน โดยกฎหมายได้วางหลักการชั่งน้ำหนักพยานหลักฐานเอาไว้ในมาตรา 227 คือ หลักพิสูจน์จนสิ้นสงสัย (in dubio pro reo) และได้บัญญัติรับรองไว้ในรัฐธรรมนูญ มาตรา 33 วรรคหนึ่ง ให้สันนิษฐานไว้ก่อนว่าผู้ต้องหาหรือจำเลยไม่มีความผิด โดยความสงสัยนั้นจะต้องเป็นความสงสัยในข้อเท็จจริง ไม่ใช่ความสงสัยในข้อกฎหมาย[4]

สำหรับประเทศไทยมีการให้หลักประกัน โดยบัญญัติรับรองไว้ในรัฐธรรมนูญ ในการให้ความคุ้มครองสิทธิและเสรีภาพเป็นหลัก รัฐจะใช้อำนาจล่วงละเมิดสิทธิเสรีภาพของประชาชนได้เป็นข้อยกเว้นในกรณีที่มีกฎหมายให้อำนาจ และมีเจ้าหน้าที่ของรัฐโดยชัดแจ้ง จะต้องมีกระบวนการควบคุมที่แน่ชัดสามารถตรวจสอบได้ ดังนั้นแม้อาชญากรรมที่เกิดขึ้นในปัจจุบันจะมีความร้ายแรงมาก จำเป็นจะต้องมีวิธีการในการแสวงหาพยานหลักฐานรูปแบบใหม่ๆ ซึ่งเป็นการใช้อำนาจในการปราบปรามอาชญากรรมของเจ้าหน้าที่ของรัฐ ก็ยังคงต้องคำนึงถึงหลักเกณฑ์นี้

การตรวจสอบเพื่อค้นหาข้อมูลในระบบอินเตอร์เน็ตหรือข้อมูลคอมพิวเตอร์นั้นก็เป็นกรณีที่มีความจำเป็นต้องมีหลักเกณฑ์ทางกฎหมายที่เพิ่มจากประมวลกฎหมายวิธีพิจารณาความ

---

[2] ณรงค์ ใจหาญ. (2543). **หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1** (พิมพ์ครั้งที่ 5). หน้า 22.

[3] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. (2539, มกราคม-มีนาคม). "แถลงการณ์เรื่อง การดักฟังทางโทรศัพท์." **รพีสาร, 14, 4**. หน้า 34.

[4] คณิต ณ นคร. เล่มเดิม. หน้า 56.

อาญากำหนดไว้ ซึ่งปัจจุบันยังไม่มีบัญญัติไว้ว่าควรดำเนินการอย่างไร นอกจากมีกำหนดไว้ในกฎหมายพิเศษบางฉบับ เช่นพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542

4.1.1.2 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 การฟอกเงิน (Money Laundering) คือการนำเงินหรือทรัพย์สินที่ได้มาจากการกระทำความผิดหรือได้มาโดยไม่ชอบด้วยกฎหมายมาเปลี่ยนสภาพเป็นเงินหรือทรัพย์สินที่ได้มาอย่างถูกต้อง เป็นการทำเงินสกปรกให้เป็นเงินสะอาด[5] เช่น เอาเงินที่ผิดกฎหมายไปลงทุนทำธุรกิจที่ถูกกฎหมาย โอนเงินออกนอกประเทศ เปิดบัญชีโดยใช้ชื่อปลอม ฯลฯ ไม่ว่าจะเป็นรูปแบบใดการกระทำดังกล่าวก็เพื่อที่จะปกปิดแหล่งที่มา และซุกซ่อนทรัพย์สิน รวมทั้งปกปิดผู้เป็นเจ้าของที่แท้จริง เพื่อทำให้ดูเสมือนว่าเป็นเงินหรือทรัพย์สินที่ถูกต้องตามกฎหมาย

ขั้นตอนของการฟอกเงินไม่ว่าจะเป็นการกระทำรูปแบบใดย่อมเหมือนกัน นั่นคือ ต้องมีการยักย้ายเงินหรือทรัพย์สิน ทำการปกปิดร่องรอยของเงินหรือทรัพย์สินดังกล่าวและนำเงินหรือทรัพย์สินนั้นกลับมาให้เสมือนเป็นเงินหรือทรัพย์สินที่ถูกต้องตามกฎหมาย

เนื่องจากปัจจุบันอาชญากรซึ่งกระทำความผิดกฎหมายบางประเภทได้นำเงินหรือทรัพย์สินที่เกี่ยวกับการกระทำความผิดนั้นมากระทำการในรูปแบบต่างๆ อันเป็นการฟอกเงิน เพื่อนำเงินหรือทรัพย์สินนั้นไปใช้ในการกระทำความผิดต่อไปอีก ทำให้ยากต่อการปราบปรามการกระทำความผิดกฎหมายเหล่านั้น และกฎหมายที่มีอยู่ก็ไม่สามารถปราบปรามการฟอกเงินหรือดำเนินการกับเงินหรือทรัพย์สินนั้นได้เท่าที่ควร ดังนั้นเพื่อเป็นการป้องกันและปราบปรามอาชญากรรม สมควรกำหนดมาตรการต่างๆ ให้สามารถดำเนินการป้องกันและปราบปรามการฟอกเงินให้ได้อย่างมีประสิทธิภาพ

หลักสากลที่นานาประเทศต่างถือเป็นหลักเกี่ยวกับกฎหมายฟอกเงิน ได้แก่ ให้ถือว่ากฎหมายฟอกเงินเป็นความผิดอาญา ที่มีการลงโทษทางอาญาและในขณะเดียวกันก็ให้มีโทษริบทรัพย์ในทางแพ่งด้วย มีวิธีการสืบสวนพิเศษโดยให้สถาบันการเงินจัดให้ลูกค้าแสดงตน ตรวจสอบกิจการของลูกค้า เก็บบันทึกข้อมูล และให้รายงานกิจการที่น่าสงสัยว่าจะเป็นการฟอกเงิน[6] นั่นคือ ธนาคารหรือสถาบันการเงินต้องจัดตั้งระบบการตรวจค้นหาข้อมูลของลูกค้าที่มีเหตุอันควรสงสัย และให้รายงานเหตุอันควรสงสัยนั้นให้เจ้าพนักงานผู้มีอำนาจหน้าที่ทราบ โดยไม่มีความผิดเรื่องเปิดเผยความลับของลูกค้าซึ่งจะเห็นได้ว่าเป็นมาตรการที่สำคัญมากในประเทศสหรัฐอเมริกา[7]

---

[5] สหัส สิงหวิริยะ. (2547). **คำอธิบายพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542** (พิมพ์ครั้งที่ 2). หน้า 3.

[6] สหัส สิงหวิริยะ. เล่มเดิม. หน้า 4.

[7] วาทิน คำทรงศรี. (2539). **การฟอกเงิน**. หน้า 102.

สำหรับกฎหมายไทยตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงินฯ มาตรา 46 ในกรณีที่มีเหตุอันควรเชื่อได้ว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อใช้ประโยชน์ในการกระทำความผิดฐานฟอกเงิน พนักงงานเจ้าหน้าที่ซึ่งเลขาธิการมอบหมายเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลแพ่งเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชี ข้อมูลทางการสื่อสาร เช่น การดักฟังโทรศัพท์ หรือข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็ได้ [8] นั่นคือต้องมีคำสั่งอนุญาตจากศาลแพ่งเสียก่อน จึงจะกระทำการตามมาตรา 46 นี้ได้

ในกรณีตามวรรคหนึ่ง ศาลจะสั่งอนุญาตให้พนักงานเจ้าหน้าที่ผู้ยื่นคำขอดำเนินการโดยใช้เครื่องมือหรืออุปกรณ์ใดๆ ตามที่เห็นสมควรก็ได้ แต่อนุญาตได้ไม่เกิดคราวละ 90 วัน [9]

เมื่อพิจารณาการกระทำความผิดมูลฐานตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542มาตรา 3 (1) ความผิดเกี่ยวกับยาเสพติด[10] ประกอบกับ พระราชบัญญัติมาตรการในการปราบปรามผู้กระทำผิดเกี่ยวกับยาเสพติด พ.ศ. 2534 คำว่า "มีเหตุอันควรสงสัย" ตามกฎหมายดังกล่าวมีขอเขตที่กว้างมาก โดยเริ่มต้นจากมีสิ่งบอกเหตุอย่างใดก็ได้ ไม่ว่าจะเป็นปรากฏการณ์หรือพฤติกรรมใดๆ ก็ได้ จนถึงเหตุที่มีพยานหลักฐานเพียงพอที่จะนำตัวจับกุมไปดำเนินคดี ส่งฟ้องและขอให้ศาลลงโทษ[11] จะเห็นได้ว่าข้อสันนิษฐานดังกล่าวเป็นข้อสันนิษฐานที่เอื้ออำนวยต่อการปฏิบัติหน้าที่ของเจ้าพนักงาน ดังนั้น เหตุอันควรสงสัยจึงไม่ควรเป็นปรากฏการณ์หรือพฤติกรรมใดๆ ก็ได้ แต่ควรจะเป็นปรากฏการณ์หรือพฤติกรรมที่อยู่ในวิสัยของปุถุชนที่สามารถคิดพิจารณาตามสามัญสำนึกว่าการจะเป็นเช่นนั้นได้ เพียงแต่ไม่มีข้อมูลบ่งชี้ จึงยังเป็นที่สงสัย

4.1.2 ปัญหาการรับฟังเป็นพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในศาลไทย

4.1.2.1 สถานะของข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในศาลไทย สภาพปัญหาที่เกิดขึ้นในปัจจุบัน คือ การจะนำเสนอข้อมูลอิเล็กทรอนิกส์เสนอต่อศาล จะนำเสนอในรูปของพยานหลักฐานชนิดใด หากพิจารณาจากลักษณะของพยานหลักฐานต่างๆแล้ว ข้อมูลอิเล็กทรอนิกส์น่าจะมีลักษณะที่สอดคล้องกับพยานหลักฐาน 2 ประเภทได้แก่ พยานเอกสาร หรือพยานวัตถุ ซึ่ง

---

[8] ดู พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, มาตรา 46 วรรคแรก.

[9] ดู พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, มาตรา 46 วรรคสอง.

[10] ดู พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, มาตรา 3 (1).

[11] วาทิน คำทรงศรี . เล่มเดิม. หน้า 73.

จำเป็นที่จะต้องกำหนดลักษณะของข้อมูลอิเล็กทรอนิกส์ให้ชัดเจนว่าเป็นพยานหลักฐานชนิดใด เนื่องจากการนำสืบ และวัตถุประสงค์ในการเสนอพยานหลักฐานทั้ง 2 ชนิดนั้นแตกต่างกัน

(1) เป็นพยานเอกสาร หมายถึง ข้อความในเอกสารที่มีการอ้างความหมายของข้อความเป็นพยาน[12]

พยานเอกสาร หมายถึง สิ่งซึ่งมีการบันทึกตัวอักษร ตัวเลข รูปรอยหรือเครื่องหมายซึ่งสามารถแสดงข้อความหรือความหมายอย่างใดอย่างหนึ่งให้ศาลตรวจดูได้ สิ่งนั้นจะเป็นอะไรก็ได้ และจะบันทึกไว้โดยวิธีเขียนด้วยมือ พิมพ์ พิมพ์ดีด แกะสลัก ถักร้อยหรือวิธีอื่นใดก็ได้[13]

ประมวลกฎหมายวิธีพิจารณาความอาญาและประมวลกฎหมายวิธีพิจารณาความแพ่ง ไม่ได้บัญญัติความหมายของคำว่า "เอกสาร" หรือ "พยานเอกสาร" เอาไว้ แม้จะมีการกล่าวถึงพยานเอกสารเอาไว้หลายชนิดในประมวลกฎหมายทั้ง 2 ฉบับ เช่น เอกสารมหาชน เอกสารราชการ หรือเอกสารเอกชน ความหมายของคำว่า "เอกสาร" นั้น ปรากฏอยู่ในประมวลกฎหมายอาญามาตรา 1 (7) หมายความว่า "กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น"

จะเห็นได้ว่าพยานเอกสารนั้น ประกอบด้วยตัววัตถุที่รองรับข้อความ และข้อความซึ่งเกิดขึ้นจากตัวอักษร ตัวเลข ผัง หรือแผนแบบต่างๆ ไม่ว่าจะโดยการพิมพ์ ถ่ายภาพ หรือวิธีอื่น ลงบนตัววัตถุที่รองรับ

ปกติแล้วพยานเอกสารจึงเป็นการบันทึกข้อความไว้บนกระดาษ โดยสิ่งที่ถูกบันทึกนั้นจะต้องสามารถสื่อความหมาย หรือแสดงข้อเท็จจริงบางอย่างได้ แต่ในบางครั้งก็อาจจะบันทึกลงบนวัสดุอื่นที่ไม่ใช่กระดาษก็ได้ เช่น ผ้า กระดาน แผ่นไม้ แผ่นหิน โลหะ ฯลฯ เพราะสิ่งที่จะพิสูจน์ข้อเท็จจริงคือสิ่งที่บันทึกอยู่บนนั้นเท่านั้น

ดังนั้น ข้อมูลอิเล็กทรอนิกส์ ที่มีลักษณะเป็นพยานเอกสารเมื่ออยู่ในรูปของการพิมพ์ออกมา (Print out)เป็นข้อความที่สื่อได้ด้วยตัวอักษร ตัวเลข หรือแผนแบบต่างๆ บนกระดาษ

ปัญหาที่ต้องพิจารณาต่อมาคือ จะนำเสนอข้อมูลอิเล็กทรอนิกส์ในฐานะ "ต้นฉบับ" หรือ "สำเนา" เพราะสำหรับระบบกฎหมายของประเทศคอมมอนลอว์ ก็จะรับฟังแต่เฉพาะต้นฉบับ โดยถือว่าเป็นพยานหลักฐานที่ถูกต้อง แท้จริงและน่าเชื่อถือที่สุด และหากเป็นสำเนาก็จะถือเป็น

---

[12] เข็มชัย ชุติวงศ์. (2543). **คำอธิบายกฎหมายลักษณะพยาน** (พิมพ์ครั้งที่ 7). หน้า 8.

[13] โสภณ รัตนากร. (2547). **คำอธิบายพยาน** (พิมพ์ครั้งที่ 7). หน้า 22.

พยานบอกเล่า (Hearsay) และสำหรับประเทศไทย แม้ปัญหาดังกล่าวจะไม่มี แต่ก็มีปัญหาในกรณีของคดีแพ่งที่กฎหมายบัญญัติให้ต้องใช้ต้นฉบับในการพิสูจน์ข้อเท็จจริงเท่านั้น

ตามบทบัญญัติของกฎหมายในเรื่องของการทำนิติกรรมสัญญา กฎหมายบัญญัติให้ต้องทำเป็นหนังสือ หรือมีหลักฐานเป็นหนังสือลงลายมือชื่อของผู้ทำนิติกรรมนั้น มิฉะนั้นจะไม่มีผลบังคับกันในทางกฎหมาย แต่ความเจริญก้าวหน้าของเทคโนโลยีในปัจจุบันมีการนำสื่ออิเล็กทรอนิกส์มาใช้ในการทำนิติกรรมสัญญา ได้แก่ โทรเลข เทเล็กซ์ โทรสาร และอินเตอร์เน็ต เรียกว่า "ธุรกรรมทางอิเล็กทรอนิกส์" เป็นการทำนิติกรรมสัญญาในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ไม่ได้ทำลงบนกระดาษเช่นในสมัยก่อน จึงมีการบัญญัติ พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ขึ้นมาใช้บังคับในกรณีนี้โดยเฉพาะ แต่ก็ยังมิได้มีการแก้ปัญหาการรับรองพยานหลักฐานในรูปของข้อมูลอิเล็กทรอนิกส์ในคดีอาญา ว่าเป็นพยานเอกสารหรือไม่แต่อย่างใด

(2) เป็นพยานวัตถุ หมายถึง วัตถุสิ่งของที่คู่ความอ้างเป็นพยาน การอ้างสถานที่ให้ศาลตรวจก็อยู่ในความหมายของพยานวัตถุ[14]

พยานวัตถุ ได้แก่ วัตถุหรือสิ่งใดที่อาจพิสูจน์ความจริงต่อศาลได้ โดยการตรวจดู มิใช่โดยการอ่านหรือการพิจารณาข้อความที่บันทึกไว้[15]

เมื่อพิจารณาเปรียบเทียบกับลักษณะของพยานเอกสารแล้ว จะเห็นว่า เอกสารฉบับหนึ่งอาจเป็นพยานเอกสารหรือพยานวัตถุก็ได้ ขึ้นอยู่กับวัตถุประสงค์ในการอ้าง นั่นคือหากต้องการให้ศาลพิจารณาข้อความในเอกสารนั้นก็เป็นพยานเอกสาร แต่ถ้าเป็นการอ้างเพื่อให้ศาลพิจารณารูปลักษณะของพยานหลักฐานชิ้นนั้นก็เป็นพยานวัตถุ โดยทั่วไปแล้วพยานวัตถุจะมีความสำคัญในคดีอาญามากกว่าในคดีแพ่ง เพราะเป็นพยานที่ดีที่สุดในการพิสูจน์ข้อเท็จจริงบางประการที่เกิดขึ้น ได้แก่ ของกลางต่างๆ

ในความเป็นจริงสื่ออิเล็กทรอนิกส์ไม่จำกัดอยู่แต่เฉพาะคอมพิวเตอร์ แต่มีทั้งกล้องถ่ายภาพ กล้องถ่ายภาพยนตร์ เครื่องบันทึกเสียง ซึ่งต่างก็มีลักษณะเป็นพยานวัตถุ ข้อมูลอิเล็กทรอนิกส์เป็นข้อมูลที่เกิดจากการประมวลผลโดยเครื่องคอมพิวเตอร์ เป็นพยานหลักฐานประเภทหนึ่งเช่นกัน

ดังนั้นการจะพิจารณาว่าสื่ออิเล็กทรอนิกส์เป็นพยานเอกสารหรือพยานวัตถุ จำเป็นที่จะต้องคำนึงถึงวัตถุประสงค์ของการนำสืบพยานหลักฐานชิ้นนั้นว่าจะเป็นการนำสืบตัววัตถุหรือนำ

---

[14] เข็มชัย ชุติวงศ์. เล่มเดิม. หน้า 8.

[15] โสภณ รัตนากร. เล่มเดิม. หน้า 22.

DPU

สืบข้อความ เช่น ต้องการนำสืบข้อเท็จจริงจากข้อความในเอกสารที่ได้พิมพ์ออกมาจากเครื่องคอมพิวเตอร์ ก็เป็นการนำสืบพยานหลักฐานที่เป็นเอกสาร หรือการนำสืบแถบบันทึกเสียงเป็นพยานวัตถุ[16] ศาลฎีกาเคยมีคำพิพากษา แสดงให้เห็นว่าแถบบันทึกเสียงสามารถตรวจสอบได้ด้วยการฟัง เพราะการนำสืบพยานวัตถุเป็นการรับรู้ด้วยประสาทสัมผัส รูป รส กลิ่น เสียง[17]

4.1.2.2 การจำกัดสถานะของพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ปัญหาสถานะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ว่าจะเป็นพยานเอกสารหรือพยานวัตถุนั้น มิได้มีบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา ในขณะที่กฎหมายได้บัญญัติถึงรูปแบบบังคับของการนำพยานหลักฐานเข้าสู่การพิจารณา โดยเรียกว่าเป็น “การจำกัดพยานหลักฐาน” โดยจำกัดสถานะของพยานหลักฐาน และการกำหนดหลักเกณฑ์การรับฟังและการสืบการจำกัดสถานะของพยานหลักฐาน เป็นการกำหนดชนิดของพยานหลักฐานตามที่กฎหมายบัญญัติเอาไว้ ที่จะใช้รับฟังได้ในคดีอาญา สำหรับปัญหาสถานะของพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์นั้น ก็ยังคงเป็นปัญหาที่สรุปไม่ได้ระหว่างพยานเอกสาร กรณีที่ Printout ออกมาเป็นเอกสาร หรือเป็นพยานวัตถุ กรณีที่อยู่ในรูปของฮาร์ดดิสก์

แต่ไม่ว่าจะเป็นพยานเอกสารหรือพยานวัตถุ ต่างก็เป็นพยานหลักฐานที่กฎหมายบัญญัติให้รับฟังได้ในคดีอาญา จึงเห็นว่าไม่น่าจะมีปัญหาในข้อนี้

4.1.2.3 ปัญหาการรับฟังพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในชั้นศาล ดังได้กล่าวมาแล้วขั้นตอนในการค้น และยึดพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ นั้นต้องกระทำไปภายในขอบเขตที่มีกฎหมายให้อำนาจกระทำได้ เพราะในการดำเนินกระบวนการทางอาญาย่อมต้องก้าวล่วงสิทธิของบุคคลโดยไม่สามารถหลีกเลี่ยงได้ หากในขั้นตอนของการค้น และยึดพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ได้กระทำไปโดยมิชอบแล้วการรับฟังพยานหลักฐานดังกล่าวในศาลไทยก็อาจเกิดปัญหา โดยพิจารณาตามหลักกฎหมายต่อไปนี้

(1) หลักสันนิษฐานไว้ก่อนว่าเป็นผู้บริสุทธิ์ ในคดีอาญาให้สันนิษฐานไว้ก่อนว่าจำเลยหรือผู้ต้องหาไม่มีความผิด [18] โดยมีกฎหมายวิธีพิจารณาความอาญา มาตรา 227 วรรคสอง และรัฐธรรมนูญ มาตรา 33 วรรคหนึ่งที่บัญญัติรับรองหลักนี้ นั่นคือศาลจะต้องรับฟังพยานหลักฐานจนปราศจากความสงสัยอันควรว่าจำเลยได้กระทำผิดจริงจึงจะลงโทษจำเลย มิใช่จะยอมรับบังคับตาม

---

[16] คำพิพากษาฎีกาที่ 7155/2539 (ส่งเสริม) เล่ม 12. หน้า 176.

[17] โสภณ รัตนากร. เล่มเดิม. หน้า 449.

[18] คณิต ณ นคร. เล่มเดิม. หน้า 56.

พยานหลักฐานที่มีเหตุผลมากกว่าอย่างคดีแพ่งเท่านั้น ดังนั้นจึงเกิดหลักดังกล่าว และในกรณีสงสัยก็จะต้องยกประโยชน์แห่งความสงสัย (in dubio pro reo) ให้แก่จำเลย แต่ความสงสัยในที่นี้จำกัดเฉพาะความสงสัยในข้อเท็จจริงเท่านั้น จะไม่ใช้หลักนี้กับความสงสัยในข้อกฎหมาย

(2) หลักการไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ ในการรับฟังพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ไม่ว่าจะเป็นการรับฟังในรูปของพยานเอกสารหรือพยานวัตถุก็ตามรับฟังได้ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 และมีบทบัญญัติรับรองเอาไว้ในรัฐธรรมนูญ และต่างก็มีบทบัญญัติที่เหมือนกันคือยกเว้นไม่รับฟังกรณีที่เป็นพยานหลักฐานที่ได้มาโดยมิชอบ ซึ่งถือเป็นบทตัดพยานในกฎหมายไทย หมายความว่าพยานหลักฐานทุกชนิดที่จะรับฟังได้ จะต้องเป็นพยานหลักฐานที่ได้มาโดยชอบ

ดังนั้น พยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ที่จะใช้รับฟังได้ในศาล จึงต้องเป็นพยานหลักฐานที่ได้มาโดยชอบ ตามนัยของกฎหมาย นั่นคือ กรณีเป็นพยานหลักฐานที่ได้จากการค้นจะต้องมีหมายค้นโดยชอบเสียก่อน เจ้าพนักงานของรัฐจึงจะสามารถเข้าไปค้นข้อมูลอิเล็กทรอนิกส์นั้นๆมาใช้อ้างอิงเป็นพยานหลักฐานได้

(3) การกำหนดหลักเกณฑ์การรับฟังและการนำสืบ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 โดยหลักคือรับฟังพยานหลักฐานที่ได้มาโดยชอบ และยกเว้นไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ และกำหนดขอบเขตในการค้นหาความจริงในคดีอาญา ไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 231 ซึ่งเป็นการห้ามสืบพยานหลักฐานอันจะเป็นการเปิดเผยความลับ มาตรา 234 การให้การเป็นปฏิปักษ์ต่อตนเอง (Self incrimination) และมาตรา 132 การตรวจตัวผู้ต้องหาได้เมื่อเขายินยอม[19]

(4) หลักการพิสูจน์จนสิ้นสงสัย หลักประกันสิทธิของบุคคลตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ข้อ 11 (1) และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง ข้อ 14 (2) และรัฐธรรมนูญ มาตรา 33 การบัญญัติรับรองสถานะของบุคคลที่ยังไม่มีคำพิพากษาของศาลว่ามีความผิด ว่าจะต้องได้รับการปฏิบัติอย่างบุคคลธรรมดาทั่วไป จะปฏิบัติต่อเขาเสมือนกับเป็นผู้ที่กระทำความผิดแล้วมิได้ การจะเข้าค้นข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคล จึงต้องมีเหตุให้ทำการค้นได้ตามที่กฎหมายบัญญัติเอาไว้อย่างชัดเจน สำหรับประเทศไทยก็คือประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 69 เท่านั้น และผลจากหลักสันนิษฐานว่าเป็นผู้บริสุทธิ์จนกว่าศาลจะมีคำพิพากษา ทำให้ต้องมีการพิสูจน์การกระทำความผิดของผู้ถูกกล่าวหาจนสิ้นสงสัยตามมาตรา 227

---

[19] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 231 ,243 วรรคหนึ่ง และ 132

เนื่องจากการค้นข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคล เป็นการกระทำที่ละเมิดต่อสิทธิส่วนบุคคลอย่างร้ายแรง ทำให้ต้องมีเหตุที่กฎหมายบัญญัติเอาไว้อย่างชัดเจน ตามหลักการสันนิษฐานว่าเป็นผู้บริสุทธิ์จนกว่าศาลจะมีคำพิพากษาเสร็จเด็ดขาดว่ามีความผิด โดยจะต้องพิสูจน์จนสิ้นสงสัยโดยการชั่งน้ำหนักพยานหลักฐาน

ที่กล่าวมาล้วนเป็นหลักเกณฑ์การรับฟังและการสืบพยานหลักฐานโดยทั่วๆไปในคดีอาญา ซึ่งผู้เขียนเห็นว่าจะต้องนำมาเป็นหลักเกณฑ์ในการรับฟังและการสืบพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เช่นกัน

4.2 วิเคราะห์ปัญหาที่ไม่อาจคุ้มครองสิทธิในข้อมูลข่าวสารส่วนบุคคลได้อย่างชัดเจน

4.2.1 มาตรการทางกฎหมายในการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ แม้รัฐจะมีองค์กรหลายองค์กรในกระบวนการยุติธรรมที่มีหน้าที่ปราบปรามอาชญากรรม ซึ่งในบางประเทศให้ความสำคัญกับประสิทธิภาพของกระบวนการยุติธรรมที่มุ่งปราบปรามอาชญากรรมมากเกินไป จนทำให้หลักประกันสิทธิส่วนบุคคลน้อยลง แต่บางประเทศก็คำนึงถึงหลักประกันสิทธิส่วนบุคคลมากกว่าประสิทธิภาพของกระบวนการยุติธรรม โดยยอมสละความมีประสิทธิภาพของการปราบปรามอาชญากรรมบางประการไป เพื่อธำรงไว้ซึ่งสิทธิเสรีภาพส่วนบุคคล[20]

กฎหมายวิธีพิจารณาความอาญา หมายถึง กฎหมายที่ว่าด้วยหลักเกณฑ์และวิธีการค้นหาความจริง อันเกี่ยวกับการกระทำความผิดและนำตัวผู้กระทำความผิดต่อกฎหมายอาญามาดำเนินการพิจารณา และลงโทษตามบทบัญญัติของกฎหมาย[21] แม้การกระทำความผิดอาญาจะเป็นการกระทำที่กระทบกระเทือนต่อสังคมโดยรวมก็ตาม แต่การดำเนินคดีอาญาก็ย่อมมีผลกระทบต่อสิทธิและเสรีภาพส่วนบุคคลโดยง่ายด้วย จึงต้องคำนึงถึงกฎหมายวิธีพิจารณาความอาญาที่ให้ความคุ้มครองสิทธิและเสรีภาพส่วนบุคคลในฐานะที่เขาเป็นส่วนหนึ่งของสังคม[22]

สำหรับประเทศไทยมีการให้หลักประกัน โดยบัญญัติรับรองไว้ในรัฐธรรมนูญ ในการให้ความคุ้มครองสิทธิและเสรีภาพเป็นหลัก รัฐจะใช้อำนาจล่วงละเมิดสิทธิเสรีภาพของประชาชนได้เป็นข้อยกเว้นในกรณีที่มีกฎหมายให้อำนาจ และมีเจ้าหน้าที่ของรัฐโดยชัดแจ้ง จะต้องมีกระบวนการควบคุมที่แน่ชัดสามารถตรวจสอบได้ ดังนั้นแม้อาชญากรรมที่เกิดขึ้นในปัจจุบันจะมี

---

[20] ประธาน วัฒนวาณิชย์. (2520, พฤศจิกายน). "ระบบความยุติธรรมทางอาญา : แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม." **วารสารนิติศาสตร์ 9, 2**. หน้า 143.

[21] ณรงค์ ใจหาญ. เล่มเดิม. หน้า 22.

[22] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. แหล่งเดิม. หน้า 34.

ความร้ายแรงมาก จำเป็นจะต้องมีวิธีการในการแสวงหาพยานหลักฐานรูปแบบใหม่ๆ ซึ่งเป็นการใช้อำนาจในการปราบปรามอาชญากรรมของเจ้าหน้าที่ของรัฐ ก็ยังคงต้องคำนึงถึงหลักเกณฑ์นี้

4.2.2 ความจำเป็นในการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ปัจจุบันประเทศไทยยังไม่มีการวางหลักไว้ในกฎหมายส่วนสารบัญญัติสำหรับอาชญากรรมรูปแบบใหม่ๆ จึงต้องมีการแก้ไขปรับปรุงต่อไป เนื่องจากอาชญากรรมที่เกิดขึ้นในขณะนี้มีลักษณะที่แตกต่างไปจากอาชญากรรมพื้นฐาน หรืออาชญากรรมแบบดั้งเดิม เมื่อมีการกระทำความความผิดเกิดขึ้นแต่ยังไม่มีการบัญญัติกฎหมายเกี่ยวกับการกระทำความผิดดังกล่าวไว้โดยเฉพาะ เช่น อาชญากรรมเศรษฐกิจ ก็จำต้องใช้กฎหมายที่มีอยู่ลงโทษผู้กระทำความผิด ตามประมวลกฎหมายอาญาผู้กระทำความผิดก็อาจรับผิดแต่เพียงในฐานละเมิดต่อผู้เสียหายเท่านั้น แต่ความเสียหายที่เกิดอาจก่อให้เกิดความเสียหายต่อระบบเศรษฐกิจของประเทศ หรือในกรณีอาชญากรรมคอมพิวเตอร์ที่ผู้กระทำความผิดใช้เครื่องคอมพิวเตอร์ในการกระทำความผิด ก็เป็นเพียงการใช้คอมพิวเตอร์ในการกระทำความผิดเท่านั้น แต่การกระทำความเสียหายต่อข้อมูล ระบบโปรแกรม หรือชุดคำสั่ง ทำให้ผู้อื่นเสียหายก็ไม่สามารถนำมาปรับใช้ได้ เพราะอาจขัดกับหลัก “ไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย” อันเป็นหัวใจสำคัญของกฎหมายอาญา

ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานรูปแบบใหม่ที่กระการยุติธรรมจำเป็นต้องให้ความสนใจ เนื่องจากอาชญากรรมรูปแบบใหม่ๆ เช่น อาชญากรรมทางเศรษฐกิจ อาชญากรรมทางคอมพิวเตอร์ และอาชญากรรมบนเครือข่ายอินเตอร์เน็ต ฯลฯ ซึ่งอาชญากรรมเหล่านี้ถือเป็นอาชญากรรมที่มีลักษณะพิเศษ แตกต่างไปจากอาชญากรรมที่มีอยู่แต่เดิม จึงต้องให้ความสำคัญเพราะกฎหมายมักตามไม่เทคโนโลยีที่มีอยู่ ความล้ำหน้าของเทคโนโลยีแม้มีประโยชน์แต่ก็ก่อให้เกิดการกระทำความผิดที่ร้ายแรง เช่น อาชญากรรมทางเศรษฐกิจ ที่มีการแสดงออกไม่รุนแรงแต่กลับก่อให้เกิดความเสียหายในระดับประเทศ

พยานหลักฐานในคดีอาญามีความสำคัญมาก เพราะคดีอาญาต้องตัดสินด้วยพยานหลักฐานเสมอ[23] การแสวงหาพยานหลักฐานจึงมีความจำเป็น แต่พยานหลักฐานบางชนิด เช่น พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เป็นพยานหลักฐานที่ยากต่อการเข้าถึง และรวบรวม บางครั้งผลจากการแสวงหาพยานหลักฐานเหล่านี้อาจกระทบถึงสิทธิเสรีภาพของผู้อื่น ในคดีอาญาพยานหลักฐานทุกชนิดรับฟังได้ แต่ต้องเป็นไปตามหลักเกณฑ์ว่าด้วยการสืบและการรับฟัง[24] ดังนั้น

---

[23] คณิต ณ นคร. เล่มเดิม. หน้า 138.

[24] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา, มาตรา 226.

เจ้าพนักงานของรัฐจึงต้องตระหนักและระมัดระวังทุกขั้นตอนในการแสวงหาพยานหลักฐานว่าจะต้องเป็นไปตามหลักเกณฑ์ว่าด้วยการสืบ เพื่อที่จะรับฟังได้เป็นพยานหลักฐาน

DPU

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

จุดประสงค์ในการแสวงหาพยานหลักฐานในคดีอาญานั้นก็เพื่อจะพิสูจน์ให้ได้ความว่าจำเลยเป็นผู้กระทำความผิดตามที่ถูกฟ้องหรือไม่ มีการกระทำอย่างไร ในเวลาใด สถานที่ใด และมีใครเป็นผู้เกี่ยวข้องบ้าง ซึ่งเป็นหลักเกณฑ์เกี่ยวกับพยานหลักฐานในคดีอาญาที่มีมาแต่เดิม สำหรับอาชญากรรมคอมพิวเตอร์ซึ่งเป็นการกระทำความผิดที่เกิดขึ้นจากความเจริญก้าวหน้าของเทคโนโลยี ไม่ว่าจะเป็นการกระทำความผิดต่อข้อมูลในคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ ซึ่งเป็นสิ่งที่ไม่มีรูปร่าง แตกต่างจากการก่ออาชญากรรมรูปแบบดั้งเดิมที่เป็นการกระทำต่อสิ่งที่มีรูปร่าง การให้ความหมายของคำว่า “อาชญากรรมคอมพิวเตอร์” จึงเป็นการให้ความหมายที่สอดคล้องกับสิ่งที่ผู้ให้ความหมายศึกษาและประสงค์จะให้ความคุ้มครอง ทำให้ไม่มีความหมายที่เป็นสากล แต่ก็มีความเห็นตรงกันประการหนึ่งก็คืออาชญากรรมคอมพิวเตอร์ เป็นการกระทำความผิดที่เกี่ยวเนื่องกับคอมพิวเตอร์ไม่ว่าจะในทางใดก็ตาม

การกระทำความผิดที่เกิดจากอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้น ก่อให้เกิดปัญหากับระบบกฎหมายภายในของประเทศต่างๆทั่วโลก เนื่องจาก การแสวงหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ถือเป็นมาตรการสำคัญ เพราะลักษณะของข้อมูลอิเล็กทรอนิกส์มีลักษณะที่แตกต่างจากพยานหลักฐานทั่วๆไป ก่อให้เกิดปัญหาในการค้น การยึด สถานะในทางพยานหลักฐานและการรับฟังเป็นพยานหลักฐานในศาล ไม่มีกฎหมายใช้บังคับ และไม่มีกฎหมายให้อำนาจเจ้าหน้าที่ของรัฐในการแสวงหาพยานหลักฐานดังกล่าว

ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 34 ได้ให้การรับรองคุ้มครองสิทธิของบุคคลในความเป็นอยู่ส่วนตัว (Right to privacy) ซึ่งไม่ใช่สิทธิในการใช้ชีวิตส่วนตัวเท่านั้น แต่ยังรวมไปถึงสิทธิในข้อมูลข่าวสารส่วนบุคคลด้วย ไม่ว่าข้อมูลนั้นจะจัดเก็บไว้ที่ใด การจะเข้าสู่ข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ โดยหลักแล้วจึงไม่สามารถทำได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เพื่อรักษาความมั่นคงของรัฐ ความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน และการจะจำกัดสิทธิของบุคคลจะต้องทำไปเท่าที่จำเป็น ตามเงื่อนไขที่รัฐธรรมนูญ กำหนดไว้ในมาตรา 29 ด้วย

ในปัจจุบันกฎหมายได้ให้อำนาจเจ้าหน้าที่ของรัฐสามารถเข้าสู่ข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46 และพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม พ.ศ. 2544 มาตรา 14 จัตวา ที่มีบทบัญญัติไปในทำนองเดียวกัน โดยกฎหมายทั้งสองฉบับดังกล่าวได้จำกัดฐานความผิดไว้เฉพาะความผิดฐานฟอกเงิน และความผิดเกี่ยวกับยาเสพติดเท่านั้น ไม่ครอบคลุมไปถึงการกระทำความผิดประเภทอื่นด้วย ดังนั้นการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลโดยประการอื่นนอกจากที่กล่าวมาแล้ว จึงเป็นการกระทำที่มิชอบด้วยกฎหมาย พยานหลักฐานที่ได้มาก็ถือเป็นพยานหลักฐานที่ได้มาโดยมิชอบ และไม่สามารถรับฟังได้ในศาล แต่รูปแบบการประกอบอาชญากรรมในปัจจุบันมีการพัฒนาไปมาก ไม่จำกัดอยู่แต่เฉพาะความผิดฐานฟอกเงิน หรือความผิดเกี่ยวกับยาเสพติด เช่น อาชญากรรมคอมพิวเตอร์ อาชญากรรมทางการเมือง หรือองค์กรอาชญากรรม ฯลฯ ซึ่งการกระทำความผิดดังกล่าวนั้นยากที่จะแสวงหาพยานหลักฐานมาเอาผิดกับผู้กระทำผิดได้ การเข้าสู่ข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ถือเป็นมาตรการพิเศษที่รัฐสามารถจะนำมาใช้แก้ปัญหาในการแสวงหาพยานหลักฐานได้เป็นอย่างดี แต่ก็จะต้องกระทำไปภายในขอบเขตที่รัฐธรรมนูญบัญญัติรับรองให้กระทำได้

เพื่อแก้ปัญหาการแสวงหาพยานหลักฐาน และการให้ความคุ้มครองข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคลในอาชญากรรมคอมพิวเตอร์ ในประเทศต่างๆ เช่น สหรัฐอเมริกา อังกฤษ และญี่ปุ่น ฯลฯ ได้มีการบัญญัติกฎหมายขึ้นมาใหม่ หรือแก้ไขปรับปรุงกฎหมายที่ใช้บังคับอยู่เพื่อแก้ปัญหาดังกล่าว

สำหรับประเทศไทยปัจจุบันยังไม่มีบทบัญญัติในประมวลกฎหมายอาญาให้ดำเนินคดีกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในรูปแบบต่างๆได้ และมาตรการในการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาก็ยังไม่มีบทบัญญัติเอาไว้ มีแต่เพียงกฎหมายพิเศษบางฉบับที่บัญญัติเอาไว้ แต่ก็จำกัดเฉพาะความผิดบางฐานเท่านั้น ไม่ครอบคลุมถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฐานอื่นๆ ด้วย ซึ่งจำเป็นที่จะต้องแก้ปัญหาทั้งการแสวงหาพยานหลักฐาน และการให้ความคุ้มครองข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคลในอาชญากรรมคอมพิวเตอร์ ไม่ว่าจะเป็นการบัญญัติกฎหมายขึ้นใหม่หรือแก้ไขปรับปรุงกฎหมายที่ใช้บังคับอยู่เพื่อแก้ปัญหาดังกล่าวดังเช่นในต่างประเทศ

5.2 ข้อเสนอแนะ

เนื่องจากการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ เป็นการกระทำที่ละเมิดสิทธิและเสรีภาพส่วนบุคคลอย่างร้ายแรง จึงจำเป็นที่จะต้องมีมาตรการที่ชัดเจน

โดยกฎหมายจะต้องบัญญัติประเภทของความผิด ที่จำเป็นจะต้องใช้วิธีการนี้ในการแสวงหาพยานหลักฐาน โดยเฉพาะอาชญากรรมคอมพิวเตอร์ เป็นการให้อำนาจเจ้าหน้าที่ในการรวบรวมพยานหลักฐาน และอำนาจที่ให้แก่เจ้าพนักงานสอบสวน เช่น อำนาจในการเชื่อมต่อเข้าไปในเครือข่ายอินเตอร์เน็ตไม่ว่าในกรณีใด เพื่อตรวจสอบเครื่องมือ อุปกรณ์ หรือเครื่องคอมพิวเตอร์ ซึ่งมีเหตุอันควรสงสัยว่าเกี่ยวข้องกับการกระทำความผิดอาชญากรรมคอมพิวเตอร์ ทั้งยังมีอำนาจมอบหมายให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์เหล่านั้น เพื่อช่วยเหลือได้ตามสมควร นั่นคือเจ้าหน้าที่ของรัฐจำเป็นที่จะต้องมีความรู้ในเรื่องคอมพิวเตอร์ดีพอที่จะดำเนินงานได้ และควรจะมีองค์กรกลางที่เป็นอิสระจากพนักงานสอบสวนเป็นผู้ทำหน้าที่ในการรวบรวมพยานหลักฐานประเภทนี้ เพื่อป้องกันการใช้อำนาจในทางมิชอบ

จากลักษณะของข้อมูลอิเล็กทรอนิกส์ ที่แตกต่างจากพยานหลักฐานชนิดอื่นๆ และสามารถเทียบเคียงได้กับพยานเอกสาร และพยานวัตถุ ซึ่งก่อให้เกิดปัญหาการจำแนกสถานะของพยานหลักฐานชนิดนี้ จนนำไปสู่ปัญหาในการนำเสนอต่อศาล จึงควรวางหลักกฎหมายกำหนดสถานะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ให้ชัดเจนว่าเป็นพยานหลักฐานชนิดใด และจะนำเสนอต่อศาลด้วยวิธีการใด โดยการกำหนดสถานะที่ชัดเจนของข้อมูลอิเล็กทรอนิกส์ให้ชัดเจนก็จะทำให้เข้าใจได้ว่าข้อมูลอิเล็กทรอนิกส์ เป็นวัตถุใดที่พนักงานสอบสวนจะทำการค้นได้ เพราะในการออกหมายอาญาไม่ว่าจะเป็นหมายค้น หรือยึดก็ตาม จำเป็นจะต้องมีการระบุสถานที่ค้น และวัตถุที่ค้นเอาไว้

สำหรับหมายอาญาก็จะต้องระบุเหตุในการค้น และยึด ควรวางหลักกฎหมายให้ชัดเจนโดยจะต้องไม่คลุมเครือ เช่นหมายค้นฮาร์ดแวร์ ซอฟท์แวร์ หรือข้อมูล โดยจะต้องระบุวิธีการ และระยะเวลาในการค้นให้ชัดเจนไม่มากไม่น้อยจนเกินไป รวมทั้งให้อำนาจเจ้าพนักงานสอบสวนทำการกักข้อมูลที่ค้นได้เพื่อใช้ประโยชน์ในการสอบสวนต่อไป ไม่ว่ากรณีใดการค้นข้อมูลอิเล็กทรอนิกส์ก็จะต้องมีหมายค้น แต่เพราะลักษณะของข้อมูลอิเล็กทรอนิกส์ เป็นพยานหลักฐานที่แก้ไขเปลี่ยนแปลงได้ง่าย ดังนั้นจึงควรมีมาตรการทางกฎหมายให้อำนาจเจ้าพนักงาน หรือมีอำนาจมอบหมายให้ผู้เชี่ยวชาญทำการเก็บกู้พยานหลักฐานที่ถูกทำลาย แก้ไขหรือเปลี่ยนแปลงไปให้กลับคืนมา โดยจะต้องวางหลักเกณฑ์ในการกู้ข้อมูลดังกล่าวให้ชัดเจน

ประเทศต่างๆต้องตระหนักถึงปัญหาอาชญากรรมคอมพิวเตอร์ว่าไม่ใช่ปัญหาของประเทศใดประเทศหนึ่ง แต่เป็นปัญหาระหว่างประเทศจึงควรให้ความร่วมมือกับประเทศต่างๆ หรือองค์การระหว่างประเทศในการหามาตรการแก้ไขปัญหา การวางหลักกฎหมายและการรวบรวมพยานหลักฐาน บัญญัติเป็นแนวทางไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา หรือบัญญัติกฎหมายพิเศษขึ้นมาใช้บังคับเป็นการเฉพาะ

ที่สำคัญต้องให้ความรู้แก่ประชาชนถึงปัญหาอาชญากรรมคอมพิวเตอร์ เพื่อให้เกิดความเข้าใจ และใช้คอมพิวเตอร์ได้อย่างถูกต้องและระมัดระวัง ทั้งคอยเป็นหูเป็นตาให้กับทางราชการในการค้นหาผู้กระทำความผิด

DPU

บรรณานุกรม

DPU

บรรณานุกรม

ภาษาไทย

หนังสือ

กุลพล พลวัน. (2538). **พัฒนาการสิทธิมนุษยชน** (พิมพ์ครั้งที่ 6). กรุงเทพฯ : วิญญูชน.

เกียรติขจร วัจนะสวัสดิ์. (2542). **คำอธิบายกฎหมายอาญา ภาค 1** . กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

เกียรติขจร วัจนะสวัสดิ์. (2547). **คำอธิบายหลักกฎหมายวิธีพิจารณาความอาญาว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณาพร้อมด้วยตัวบทและคำอธิบายมาตราที่แก้ไขเพิ่มเติมใหม่** (พิมพ์ครั้งที่ 3 แก้ไขใหม่). กรุงเทพฯ : หจก.จิรรัชการพิมพ์.

เข็มชัย ชุติวงศ์. (2543). **คำอธิบายกฎหมายลักษณะพยาน** (พิมพ์ครั้งที่ 7 ปรับปรุงใหม่). กรุงเทพฯ : นิติบรรณาการ.

คณิต ณ นคร. (2543). **กฎหมายอาญาภาคความผิด** (พิมพ์ครั้งที่ 7). กรุงเทพฯ : มหาวิทยาลัยธรรมศาสตร์.

คณิต ณ นคร. (2546). **กฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม-ปรับปรุงใหม่). กรุงเทพฯ : วิญญูชน.

คนึง ฤาไชย. (2530). **กฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 5). กรุงเทพฯ : มหาวิทยาลัยธรรมศาสตร์.

จีรนิติ หะวานนท์. (2544). **สิทธิทางวิธีพิจารณาความอาญาตามรัฐธรรมนูญ** (พิมพ์ครั้งที่ 2 ปรับปรุงใหม่). กรุงเทพฯ : วิญญูชน.

จิตติ ติงศภัทิย์. (2525). **กฎหมายอาญา ภาค 1**. กรุงเทพฯ : สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตสภา.

ณรงค์ ใจหาญ. (2547). **หลักกฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 7 ปรับปรุงใหม่). กรุงเทพฯ : วิญญูชน.

ทวีเกียรติ มีนะกนิษฐ์. (2543). **กฎหมายอาญา : หลักและปัญหา** (พิมพ์ครั้งที่ 2). กรุงเทพฯ : นิติธรรม.

บรรเจิด สิงคะเนติ. (2543). **หลักพื้นฐานของสิทธิเสรีภาพ และศักดิ์ศรีความเป็นมนุษย์ตามรัฐธรรมนูญ พ.ศ.2540**. กรุงเทพฯ : วิญญูชน.

ปีเตอร์ ที. เดวิส และแบรี่ ดี. เลวิส. (2543). **แรกเริ่มเรียนรู้ เรื่องรักษาความปลอดภัยให้ระบบคอมพิวเตอร์**. แปลจาก Computer Security Dummies โดย เจนศักดิ์ ตั้งพันธ์สุริยะ. กรุงเทพฯ : บริษัท ซีเอ็ดยูเคชั่น จำกัด.

วัชราภรณ์ สุริยาภิวัฒน์. (2543). **คอมพิวเตอร์เบื้องต้นและเทคนิคการเขียนโปรแกรม**. กรุงเทพฯ : ห้างหุ้นส่วนจำกัด ไทยเจริญการพิมพ์.

วาทิน คำทรงศรี. (2539). **การฟอกเงิน**. กรุงเทพฯ : วิญญูชน.

วรพจน์ วิศรุตพิชญ์. (2538). **สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540**. กรุงเทพฯ : วิญญูชน.

วีระ โลจายะ. (2524). **กฎหมายสิทธิมนุษยชน**. กรุงเทพฯ : มหาวิทยาลัยรามคำแหง.

สหัส สิงหวิริยะ. (2547). **คำอธิบายพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542** (พิมพ์ครั้งที่ 2). กรุงเทพฯ : นิติธรรม.

แสวง บุญเฉลิมวิภาส. (2542). **หลักกฎหมายอาญา** (พิพม์ครั้งที่ 2). กรุงเทพฯ : โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลักธรรมศาสตร์.

หยุด แสงอุทัย. (2523). **กฎหมายอาญาภาค 1** (พิพม์ครั้งที่ 14). กรุงเทพฯ : สำนักพิมพ์หาวิทยาลัยธรรมศาสตร์.

หฤทัย หงส์สิริ และมานิตย์ จุมปา. (2542). **คำอธิบายข้อมูลข่าวสารของทางราชการ**. กรุงเทพฯ : นิติธรรม.

อุดม รัฐอมฤต นพนิธิ สุริยะ และบรรเจิด สิงคะเนติ. (2544). **การอ้างศักดิ์ศรีความเป็นมนุษย์หรือใช้สิทธิและเสรีภาพของบุคคลดังกล่าวตามมาตรา 28 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2540**. กรุงเทพฯ : สำนักงานศาลรัฐธรรมนูญ.

บทความ

"การสัมนนาทางวิชาการเรื่อง ศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของบุคคลตามรัฐธรรมนูญ." **วารสารศาลรัฐธรรมนูญ, 1,3.** (2542, กันยายน-ธันวาคม). หน้า 37-48.

กุลพล พลวัน. (2540, มิถุนายน). "กลไกตามรัฐธรรมนูญในการคุ้มครองสิทธิและเสรีภาพของประชาชน." **บทบัณฑิตย์, 52, 2.** หน้า 36-52.

จิรนิติ หะวานนท์. (2527, พฤษภาคม-มิถุนายน). "หลักการไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ : เปรียบเทียบระหว่างกฎหมาย อเมริกา และกฎหมายเยอรมัน." **ดุลพาห, 31, 3.** หน้า 34-52.

นิติ ผดุงชัย. (2532,มิถุนายน). “กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับ Computer.” **วารสารอัยการ**, หน้า 86-88.

ณรงค์ ใจหาญ. (2540, มิถุนายน). “หลักประกันสิทธิของประชาชนในคดีอาญาใหม่ : ปัจจุบันและทศวรรษหน้า 2540-2550.” **บทบัณฑิตย์, 53, 2.** หน้า 64-86.

ประธาน วัฒนวาณิชย์. (2520, พฤศจิกายน). “ระบบความยุติธรรมทางอาญา : แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม.” **วารสารนิติศาสตร์, 9,2**. หน้า 143-156.

สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. (2539, มกราคม-มีนาคม). ”แถลงการณ์เรื่อง การดักฟังทางโทรศัพท์.” **รพีสาร, 14, 4.** หน้า 34- 54.

วิทยานิพนธ์

กิตติพันธุ์ เกียรติสุนทร. (2538). **มาตรการทางอาญาในการคุ้มครองข้อมูลส่วนบุคคล**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

กิตติมา ประคุณคดี. (2533). **การดักฟังทางโทรศัพท์โดยเจ้าพนักงาน**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

กงจักร โพธิ์พร้อม. (2529). **ปัญหากฎหมายมหาชนบางประการเกี่ยวด้วยการควบคุมการใช้ข่าวสารโดยเครื่องคอมพิวเตอร์**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

จงรัก จุทานนท์. (2524). **การคุ้มครองสิทธิของประชาชนต่อการถูกจับและตรวจค้นที่ไม่ชอบธรรม**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

ศุภฤกษ์ ศุกรเสพย์. (2545). **การค้นในที่รโหฐานของเจ้าพนักงานป้องกันและปราบปรามยาเสพติด**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

สุชาติ ตระกูลเกษมสุข. (2543). **การคุ้มครองสิทธิส่วนบุคคลจากการดักฟังทางโทรศัพท์**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

DPU

ภาษาต่างประเทศ

BOOKS

Dando, Shigemitsu. (1965). **Japanese Criminal Procedure**. South Hackensack,NJ: Fred Rothman & Co.

May, Richard. (1999). **Criminal Evidence**. London : Sweet & Maxwell Ltd.

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

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

DPU

บทที่ 2
การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์

ขั้นตอนที่สำคัญขั้นตอนหนึ่งในการดำเนินกระบวนการยุติธรรมทางอาญา นั่นคือการดำเนินคดีอาญาชั้นก่อนฟ้อง (Vorverfahren) คือ การดำเนินการทั้งปวงของเจ้าพนักงานก่อนการยื่นฟ้อง ได้แก่ การสอบสวนของพนักงานสอบสวนและการดำเนินการของพนักงานอัยการก่อนการยื่นฟ้อง [1] และในการดำเนินการสอบสวนก็ครอบคลุมเนื้อหา 2 ประการ ได้แก่ การรวบรวมพยานหลักฐานและการใช้มาตรการบังคับ [2] ดังนั้นการแสวงหาและรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดจึงเป็นขั้นตอนก่อนการฟ้อง เมื่อมีการกระทำความผิดอาญาเกิดขึ้นการที่จะลงโทษผู้กระทำความผิดได้จะต้องมีการรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิด ถ้าไม่มีพยานหลักฐานก็ไม่สามารถที่จะดำเนินกระบวนการยุติธรรมทางอาญาขั้นตอนอื่นๆ ต่อไปได้ เมื่อพยานหลักฐานที่จะนำมาพิสูจน์การกระทำความผิดเป็นส่วนสำคัญของกระบวนการยุติธรรมทางอาญา ผู้กระทำความผิดก็ย่อมที่จะปกปิด ซ่อนเร้น พยานหลักฐานดังกล่าวอยู่ในคอมพิวเตอร์หรือสื่ออิเล็กทรอนิกส์ต่างๆ ซึ่งข้อมูลจากสื่อเหล่านี้อาจใช้เป็นพยานหลักฐานในคดีอาญาได้

ด้วยเหตุนี้กฎหมายวิธีพิจารณาความอาญาจึงต้องมีเครื่องมือในการแสวงหาพยานหลักฐาน ในที่นี้ได้แก่การค้น ซึ่งเป็นมาตรการบังคับในการดำเนินคดีอาญาประการหนึ่ง ซึ่งในที่นี้เป็นการค้นหาพยานหลักฐานจากเครื่องคอมพิวเตอร์หรือสื่ออิเล็กทรอนิกส์ต่างๆ เฉพาะที่เป็นข้อมูลส่วนบุคคล และเป็นมาตรการบังคับที่รุนแรงมาก เพราะเป็นมาตรการบังคับที่กระทบถึงสิทธิและเสรีภาพของบุคคล ดังนั้นจึงจำเป็นที่จะต้องเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ เพื่อประโยชน์ในการแสวงหาพยานหลักฐานที่มีลักษณะดังกล่าวต่อไป

---

[1] คณิต ณ นคร. (2546). **กฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 6, แก้ไขเพิ่มเติม ปรับปรุงใหม่). หน้า 308.

[2] คณิต ณ นคร. เล่มเดิม. หน้า 313.

2.1 ความหมาย ความสำคัญ และประเภท ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

2.1.1 ความหมายของข้อมูลอิเล็กทรอนิกส์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 ให้ความหมายคำว่า "ข้อมูลอิเล็กทรอนิกส์" หมายถึง ข้อความที่ได้ส่ง รับ เก็บรักษาหรือประมวลผลด้วยวิธีการอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์หรือโทรสาร

มาตรา 4 ยังได้ให้คำนิยามคำว่า อิเล็กทรอนิกส์ ข้อความ ระบบข้อมูล การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ ผู้ส่งข้อมูล ผู้รับข้อมูล และบุคคลที่เป็นสื่อกลาง ไว้ดังนี้

"อิเล็กทรอนิกส์" หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่างๆ เช่นว่านั้น

"ข้อความ" หมายความว่า เรื่องราวหรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ

"ระบบข้อมูล" หมายความว่า กระบวนการประมวลผลด้วยเครื่องมืออิเล็กทรอนิกส์สำหรับ สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลข้อมูลอิเล็กทรอนิกส์

"การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์" หมายความว่า การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

"ผู้ส่งข้อมูล" หมายความ บุคคลซึ่งผู้ส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีที่ผู้นั้นกำหนด โดยบุคคลนั้นอาจจะส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

"ผู้รับข้อมูล" หมายความว่า บุคคลซึ่งผู้ส่งข้อมูลประสงค์จะส่งข้อมูลอิเล็กทรอนิกส์ให้และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

"บุคคลที่เป็นสื่อกลาง" หมายความว่า บุคคลซึ่งกระทำการในนามผู้อื่นในการส่ง รับ หรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์อันใดอันหนึ่งโดยเฉพาะ รวมถึงให้บริการอื่นที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น

DPU

นอกจากนี้ยังมีร่างกฎหมายเกี่ยวกับกิจการอินเตอร์เน็ต โดยคณะกรรมการกฎหมายได้เสนอร่างพระราชบัญญัติส่งเสริมกิจการอินเตอร์เน็ต ร่าง 1 ให้นิยามคำว่า คอมพิวเตอร์ อินเตอร์เน็ต ข้อมูลและข้อมูลข่าวสาร[3] ดังนี้

"คอมพิวเตอร์" หมายความว่า อุปกรณ์ที่ใช้ประมวล วิเคราะห์ข้อมูล ซึ่งทำงานด้วยอิเล็กทรอนิกส์แม่เหล็กไฟฟ้าใยแก้ว อิเล็กทรอนิกส์หรืออุปกรณ์ที่เชื่อมต่อ หรือเกี่ยวข้องกับอุปกรณ์ดังกล่าว ซึ่งใช้งานด้วยเหตุผลทางวิทยาศาสตร์ คณิตศาสตร์ เก็บบันทึกและแสดงข้อมูลและหมายรวมถึงการเก็บบันทึกข้อมูลหรือการสื่อสารที่ต่อเชื่อมโดยตรง หรือใช้งานร่วมกับอุปกรณ์นั้นๆ หรืออุปกรณ์ที่เชื่อมต่อระหว่างอุปกรณ์ดังกล่าว แต่ไม่รวมตลอดถึงเครื่องพิมพ์อักษรอัตโนมัติ หรือเครื่องติดตั้งตัวอักษร หรือคำนวณตัวเลขแบบพกพา หรืออุปกรณ์ร่วมทั้งการเผยแพร่ Program ด้วยวิธีใดๆ

"อินเตอร์เน็ต" หมายความว่า ระบบเครือข่ายที่มีเครื่องคอมพิวเตอร์เชื่อมโยงกันทั่วโลก โดยอาศัยการสื่อสารด้วยระเบียบวิธีในการสื่อสารกันระหว่างเครื่องคอมพิวเตอร์ เชื่อมต่อกันในระบบปฏิบัติการแบบมีผู้ใช้หลายคน

"ข้อมูล" หมายความว่า สิ่งที่เป็นข้อเท็จจริง เช่น ข้อความ จำนวนเลข เสียงและภาพ ซึ่งแสดงในรูปแบบที่คอมพิวเตอร์สามารถประมวลผลได้

"ข้อมูลข่าวสาร" หมายความว่า สิ่งที่สื่อความหมาย

และร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ได้ให้ความหมายของคำว่า ระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ ไว้ดังนี้

"ระบบคอมพิวเตอร์" ในพระราชบัญญัตินี้ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดชุดคำสั่งและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ หรือชุดคำสั่ง บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้

เมื่อพิจารณาจากความหมายของคำว่า "ระบบคอมพิวเตอร์" จากร่างพระราชบัญญัติส่งเสริมกิจการอินเตอร์เน็ต ร่าง 1 และร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ข้างต้น "ระบบคอมพิวเตอร์" จึงได้แก่ฮาร์ดแวร์และซอฟต์แวร์ที่พัฒนาขึ้นเพื่อประมวลผลข้อมูลดิจิทัล (digital data) อันประกอบด้วยเครื่องคอมพิวเตอร์ และอุปกรณ์รอบข้าง

---

[3] คณะกรรมการบริหารสมาคมอินเตอร์เน็ตนานาชาติ ประเทศไทย, "ร่างพระราชบัญญัติส่งเสริมกิจการอินเตอร์เน็ต พ.ศ. …….. (ร่าง 1)," <http://www.acm.th.org/law/internetlaw1b.html>

(peripheral) ต่างๆ ในการรับเข้าหรือป้อนข้อมูล (input) นำออกหรือแสดงผลข้อมูล (output) และบันทึกหรือเก็บข้อมูล (store and record) ดังนั้น ระบบคอมพิวเตอร์จึงอาจเป็นอุปกรณ์เพียงเครื่องเดียว หรือหลายเครื่องอันมีลักษณะเป็นชุดเชื่อมต่อกันโดยอาจผ่านระบบเครือข่าย และมีลักษณะการทำงานโดยอัตโนมัติตามโปรแกรมที่กำหนดไว้ และไม่มีการแทรกแซงโดยตรงจากมนุษย์ ส่วนโปรแกรมคอมพิวเตอร์จะหมายถึงชุดคำสั่งที่ทำหน้าที่สั่งการให้คอมพิวเตอร์ทำงาน

ดังนั้นข้อมูลคอมพิวเตอร์ จึงไม่ใช่เฉพาะตัวอักขระ หรือข้อความที่สื่อความหมาย อ่านเข้าใจได้ที่หน้าจอภาพ (monitor) เท่านั้น แต่เป็นข้อมูลดิจิทัลที่อยู่ในระบบคอมพิวเตอร์ และอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้

ตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 มาตรา 4 ให้ความหมายคำว่า “ข้อมูลข่าวสาร” “ข้อมูลข่าวสารส่วนบุคคล” ดังนี้

คำว่า “ข้อมูลข่าวสาร” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

คำว่า “ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

ตามร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. … มาตรา 4 ได้ให้ความหมายคำว่า “ข้อมูลส่วนบุคคล” “บันทึกข้อมูลส่วนบุคคล” ดังนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อเท็จจริงเกี่ยวกับตัวบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม

“บันทึกข้อมูลส่วนบุคคล” หมายความว่า เอกสาร ฐานข้อมูล หรือรูปภาพหรือสิ่งซึ่งแสดงภาพของบุคคลในรูปแบบอื่น ทั้งนี้ไม่รวมถึงสิ่งพิมพ์ซึ่งเผยแพร่ทั่วไปหรือเอกสารที่เก็บไว้ในห้องสมุด หอศิลปะ หรือพิพิธภัณฑ์ เพื่อประโยชน์ในการใช้อ้างอิง การศึกษา การจัดนิทรรศการ หรือเอกสารที่เป็นอนุสรณ์ หรือจดหมายหรือสิ่งอื่นใดที่มีการส่งในทางปกติธุระของการไปรษณีย์ เว้นแต่ข้อความจะกำหนดไว้เป็นอย่างอื่น

เมื่อพิจารณาตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 และร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...ความหมายของคำว่าข้อมูลส่วนบุคคล ควรหมายถึง ข้อมูลข่าวสารที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคล และเป็นข้อมูลที่ได้รับความคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ไม่เปิดเผยต่อผู้ที่ไม่มีสิทธิรับรู้ แม้หลักพื้นฐานของที่สำคัญ 2 ประการของของข้อมูลข่าวสารของราชการนั้น ได้แก่ หลักที่ว่าบุคคลไม่จำต้องเป็นผู้มีส่วนได้เสียกับข้อมูลข่าวสารส่วนที่ขอ และเปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น[4] แต่ในเรื่องข้อมูลข่าวสารส่วนบุคคลนี้ กฎหมายต้องการคุ้มครองความเป็นอยู่ส่วนบุคคลตามที่รัฐธรรมนูญได้บัญญัติไว้ในมาตรา 34 ดังนั้น จึงได้กำหนดหลักการสำคัญแตกต่างไปจากข้อมูลข่าวสารของทางราชการ โดยกำหนดไว้เป็นหลักการว่า "ข้อมูลข่าวสารส่วนบุคคลจะเปิดเผยต่อบุคคลอื่นโดยปราศจากความยินยอมมิได้ เว้นแต่จะเข้าข้อยกเว้น" โดยกฎหมายฉบับนี้ได้บัญญัติเป็นข้อยกเว้นไว้ในมาตรา 24

ข้อมูลข่าวสารส่วนบุคคลนั้นอาจเป็นข้อมูลของบุคคลที่ยังมีชีวิตอยู่ หรือแม้กระทั่งผู้ที่ถึงแก่กรรมไปแล้ว เพราะหากข้อมูลของบุคคลเหล่านั้นถูกเปิดเผยออกไปก็อาจเป็นผลร้ายแก่ชื่อเสียงของผู้ตาย ญาติพี่น้อง หรือวงศ์ตระกูลได้[5]

2.1.2 การประมวลผลข้อมูล (Data Processing) เมื่อมีข้อมูลเกิดขึ้น หรือมีการรวบรวมข้อมูลต่างๆ ขึ้น วิธีการจัดการข้อมูล ไม่ว่าการคำนวณ การเรียงลำดับ หรือการจัดกลุ่ม ต่างก็เป็นการประมวลผล (Processing) ทั้งสิ้น การประมวลผล จึงหมายถึง วิธีการจัดการกับข้อมูล โดยมีจุดมุ่งหมายเพื่อให้ได้ผลลัพธ์อย่างใดอย่างหนึ่ง ข้อสรุปที่ได้ เรียกว่าข้อสนเทศ (Information) ซึ่งสามารถนำไปใช้ในการตัดสินใจต่างๆ ที่เกี่ยวข้อง ขึ้นอยู่กับการนำไปใช้ประโยชน์ของแต่ละคน

ก. ขั้นตอนของการประมวลผลข้อมูล[6] แบ่งเป็น 3 ขั้นตอน ได้แก่

(1) การเตรียมข้อมูล (Input) การเตรียมข้อมูล (Input) คือการเก็บรวบรวมข้อมูลเพื่อรอประมวลผล ซึ่งหมายรวมถึงการเปลี่ยนสภาพข้อมูลให้อยู่ในรูปแบบที่เหมาะสมและพร้อมที่จะประมวลผลต่อไป การเปลี่ยนสภาพข้อมูลประกอบด้วย

- การลงรหัส (Coding) หมายถึงการให้รหัสแทนข้อมูลจริง ทำให้ข้อมูลอยู่ในรูปแบบที่กะทัดรัดสะดวกแก่การประมวลผล ซึ่งรหัสที่ใช้อาจเป็นตัวเลขหรือตัวอักษรก็ได้ เช่น ข้อมูลเพศชาย ใช้แทนด้วยตัว ช. ส่วนเพศหญิงใช้ตัว ญ. เป็นต้น

---

[4] หฤทัย หงส์สิริ และ มานิต จุมปา. (2542). **คำอธิบายข้อมูลข่าวสารของทางราชการ**. หน้า 86.

[5] หฤทัย หงส์สิริ และ มานิต จุมปา. เล่มเดิม. หน้า 19.

[6] วัชราภรณ์ สุริยาภิวัฒน์. (2543). **คอมพิวเตอร์เบื้องต้นและเทคนิคการเขียนโปรแกรม**. หน้า 26-27.

- การบรรณาธิกรณ์ (Editing) หมายถึงการตรวจสอบความถูกต้องและความเป็นไปได้ของข้อมูลและปรับปรุงแก้ไขเท่าที่จะทำได้ เช่น ผู้ให้ข้อมูลเป็นเพศหญิง แต่ตอบว่าเคยเกณฑ์ทหาร ก็ต้องทำการตรวจสอบโดยพิจารณาจากคำตอบที่ได้จากคำถามข้ออื่น หรือไปสอบถามใหม่ แล้วแก้ไข

- การแยกประเภท (Classifying) หมายถึงการจัดประเภทข้อมูลให้เป็นกลุ่มตามลักษณะต่างๆ ของข้อมูล เพื่อสะดวกต่อการประมวลผลต่อไป

- การบันทึกข้อมูลในสื่อ (Media) ที่เหมาะสม หมายถึงการจัดเตรียมข้อมูลให้อยู่ในสื่อหรืออุปกรณ์ที่ใช้ได้กับเครื่องมือการประมวลผลที่มีอยู่ เช่นบันทึกข้อมูลลงแผ่นดิสก์ หรือเทปแม่เหล็กเพื่อนำไปประมวลผลด้วยเครื่องคอมพิวเตอร์ต่อไป

(2) การประมวลผล (Processing) หมายถึงวิธีการจัดการกับข้อมูล ซึ่งอาจเป็นการคำนวณการรวมข้อมูลมากกว่าหนึ่งชุดเข้าด้วยกัน (Merge) การดึงข้อมูลมาใช้ (Retrieve) หรือการเรียงลำดับ (Sort)

(3) การนำเสนอผลลัพธ์ (Output) หมายถึงการนำผลลัพธ์ที่ได้จากการประมวลผลมาแสดงให้ทราบ เช่น แสดงผลสรุปในรูปของตาราง หรือกราฟ

ข. ประเภทของการประมวลผลข้อมูล[7] เมื่อพิจารณาจากอุปกรณ์ที่ใช้เป็นหลัก สามารถแบ่งการประมวลผลข้อมูลได้ 3 ประเภท

(1) การประมวลผลข้อมูลด้วยมือ (Manual Data Processing) เป็นวิธีการประมวลผลข้อมูลที่มีมาแต่เดิม อุปกรณ์ที่ใช้ได้แก่ กระดาษทด เครื่องคิดเลข ลูกคิด ใช้กับข้อมูลที่มีจำนวนน้อยและการคำนวณไม่ยุ่งยาก และเป็นงานที่ไม่รีบเร่ง

(2) การประมวลผลข้อมูลด้วยเครื่องจักรกล (Mechanical Data Processing) เป็นการใช้แรงงานคนร่วมกับเครื่องจักร ที่ใช้กันมากได้แก่ เครื่องจักรทำบัญชี ซึ่งเป็นเครื่องประมวลผลประเภทกึ่งอิเล็กทรอนิกส์ที่เรียกว่า “เครื่อง Unit Record” เช่น เครื่องเจาะบัตร (Card Punch) เครื่องรวมบัตร (Collator) เครื่องเรียงบัตร (Card Sorter) เครื่องแปลบัตร (Interpreter) ฯลฯ เป็นการประมวลผลที่เหมาะกับงานระดับกลางที่มีข้อมูลไม่มากนักและต้องการความรวดเร็วในการทำงานปานกลาง

(3) การประมวลผลข้อมูลด้วยเครื่องคอมพิวเตอร์ (Electronic Data Processing - EDP.) หมายถึงการประมวลผลข้อมูลด้วยเครื่องอิเล็กทรอนิกส์ และเครื่องอิเล็กทรอนิกส์ที่ใช้ก็คือคอมพิวเตอร์นั่นเอง เหมาะกับงานที่มีปริมาณมาก และมีขั้นตอนการทำงานซ้ำๆกัน ต้องการ

---

[7] วัชราภรณ์ สุริยาภิวัฒน์. เล่มเดิม. หน้า 28-29.

ประสิทธิภาพในการทำงาน ให้ผลลัพธ์ที่ถูกต้อง เป็นการคำนวณที่มีสูตรยุ่งยากซับซ้อน และเป็นงานที่ต้องการภาพพจน์ที่ทันสมัย ฯลฯ

2.1.3 ระบบและประโยชน์ของเครือข่ายคอมพิวเตอร์

ก. ระบบเครือข่ายคอมพิวเตอร์ เป็นระบบการสื่อสารที่ประกอบด้วยเครื่องคอมพิวเตอร์หลายเครื่องเชื่อมต่อถึงกันเพื่อให้ผู้ใช้คอมพิวเตอร์สามารถสื่อสารถึงกัน ใช้ข้อมูลร่วมกัน หรือเพื่อแลกเปลี่ยนข้อมูลระหว่างกัน การเชื่อมโยงของระบบเครือข่ายจะผ่านช่องทางการสื่อสารต่างๆ กัน เช่น สายโทรศัพท์ สายไฟฟ้า หรือผ่านสื่อกลาง เช่น ไมโครเวฟ [8] เป็นต้น การแบ่งประเภทระบบเครือข่ายสามารถแบ่งได้จากลักษณะการติดตั้งทางภูมิศาสตร์ แบ่งได้ 3 แบบ ได้แก่

(1) เครือข่ายท้องถิ่น (Local Area Network หรือ LAN) เป็นเครือข่ายระยะใกล้ เช่น ภายในอาคารสำนักงาน เป็นต้น ระบบเครือข่ายชนิดนี้จะช่วยให้สะดวกในการติดต่อ ช่วยลดต้นทุน

(2) เครือข่ายระดับเมือง (Metropolitan Area Network หรือ MAN) เป็นเครือข่ายขนาดกลาง ใช้ภายในเมืองหรือจังหวัด เช่น เคเบิลทีวี

(3) เครือข่ายระดับประเทศ (Wide Area Network หรือ WAN) เป็นเครือข่ายที่มีขนาดใหญ่ ติดตั้งใช้งานในบริเวณกว้าง มีสถานีจุดเชื่อมมากมาย ต้องใช้สื่อกลางหลายชนิด เช่น ระบบคลื่นวิทยุ ไมโครเวฟ หรือดาวเทียม เป็นต้น

(4) ระบบเครือข่ายระหว่างประเทศ (International Network หรือ Inter-Net) เป็นระบบที่ติดต่อข้ามประเทศโดยใช้สายเคเบิล หรือดาวเทียม

จะเห็นได้ว่าระบบเครือข่ายช่วยให้เกิดความรวดเร็วในการติดต่อสื่อสาร ทำให้การส่งข้อมูลข่าวสารในยุคโลกาภิวัฒน์สามารถทำได้สะดวกสบายมากขึ้น ไม่ว่าจะอยู่ในส่วนใดของโลกก็สามารถส่งผ่านข้อมูลข่าวสารถึงกันได้ และแต่ละเครือข่ายก็สามารถเชื่อมกับเครือข่ายอื่นๆ ได้ โดยผ่านคอมพิวเตอร์ขนาดใหญ่ที่มีระบบปฏิบัติงานข่ายงาน (Network Operating System) เป็นซอฟท์แวร์ควบคุมข่ายงาน และมีแผ่นวงจรข่ายงาน (Network Interface Card) คอยควบคุมให้คอมพิวเตอร์ในเครือข่ายเดียวกันทำงานประสานกัน และมีฮาร์ดแวร์ ที่เรียกว่า “เกตเวย์ (Gateway)” คอมพิวเตอร์ในแต่ละจุดจะทำหน้าที่เสมือนเป็นตัวเชื่อมและควบคุม เรียกว่า “สะพาน (Bridge)” มีการเชื่อมคอมพิวเตอร์ให้ถูกต้องตามลักษณะที่เหมาะสม โดยจัดให้มีคอมพิวเตอร์ที่มีความสามารถสูงเครื่องหนึ่ง เป็นเครื่องกลางที่ทำหน้าที่ควบคุมเครือข่ายงานและแฟ้มข้อมูล ลักษณะเหมือนเป็น

---

[8] ระบบไมโครเวฟ เป็นระบบการสื่อสารแบบไม่มีสาย ชนิดที่เป็นคลื่นวิทยุที่มีความถี่ระหว่าง 300 Mhs และ 30 Ghs และเดินทางเป็นเส้นตรง อุปกรณ์ที่ใช้ในการรับส่ง คือ จานสัญญาณไมโครเวฟ ซึ่งมักติดตั้งในที่สูง ข้อดี คือสามารถส่งสัญญาณด้วยความถี่กว้าง และแทบจะไม่มีการรบกวนจากภายนอก ข้อเสียคือถ้าทิศทางการส่งมีสิ่งกีดขวางจะทำให้การส่งสัญญาณทำได้ไม่ดี

DPU

แม่ข่าย หรือตัวบริการแฟ้มข้อมูล (File Server) ให้คอมพิวเตอร์เครื่องอื่นๆ เชื่อมโยงเข้ามาหาคอมพิวเตอร์ที่เป็นแม่ข่ายตัวนี้ ลักษณะการเชื่อมโยงนี้ เรียกว่า "โทโพโลยี (Topology)

ข. ประโยชน์ของเครือข่ายคอมพิวเตอร์ การนำคอมพิวเตอร์เข้ามาประยุกต์ในการดำเนินงานต่างๆ โดยการเชื่อมโยงคอมพิวเตอร์หลายๆ เครื่องเข้าด้วยกัน จัดทำเป็นระบบเครือข่าย ทำให้เกิดความสะดวกสบายและรวดเร็วในการการสื่อสารข้อมูลระหว่างบุคคล เพราะปัจจุบันมีเครือข่ายคอมพิวเตอร์เชื่อมโยงไปทั่วโลก โดยเฉพาะเครือข่ายที่เรียกว่า "อินเตอร์เน็ต (Internet)" ซึ่งมีเครือข่ายเชื่อมโยงคอมพิวเตอร์ครอบคลุมไปทั่วโลกภายใต้มาตรฐานเดียวกัน มาตรฐานดังกล่าวทำให้คอมพิวเตอร์ในเครือข่ายพูดภาษาเดียวกัน ทำให้คนสามารถติดต่อและรับรู้ข่าวสารกันได้รวดเร็ว เป็นประโยชน์อย่างมากในทุกๆ ด้าน เช่น

(1) ด้านธุรกิจ เครือข่ายที่มีประโยชน์ทางธุรกิจ เช่น ธนาคาร มีระบบออนไลน์บนเครือข่ายช่วยให้สามารถสอบถามยอดเงิน หรือโอนเงินได้รวดเร็ว การติดต่อระหว่างสำนักงานใหญ่และสาขาก็สามารถทำได้อย่างสะดวกรวดเร็ว

(2) ด้านการศึกษา มีการศึกษาทางไกล (Tele Education) เป็นการค้นคว้าทางวิชาการ การแบ่งปันหรือถ่ายทอดความรู้ระหว่างบุคคลที่อยู่ห่างไกลกัน

(3) ด้านการแพทย์ มีการแพทย์ทางไกล (Tele Medicine) โดยนำระบบเครือข่ายมาใช้ในการเก็บทะเบียนประวัติคนไข้ โดยใช้ฐานข้อมูลร่วมกัน มีการปรึกษาวินิจฉัยโรค และรักษาผ่านเครือข่ายคอมพิวเตอร์

(4) ด้านความมั่นคงปลอดภัยระหว่างประเทศ เช่น การเก็บประวัติอาชญากรด้วยฐานข้อมูลเดียวกัน โดยทุกสถานีตำรวจมีเครือข่ายคอมพิวเตอร์ที่สามารถเรียกและตรวจสอบข้อมูลได้ ทำให้การปราบปรามอาชญากรรมสามารถทำได้รวดเร็วทันต่อเหตุการณ์

(5) ด้านการสื่อสาร โดยการส่งจดหมายอิเล็กทรอนิกส์ ที่เรียกว่า "E-Mail (Electronic Mail) ซึ่งช่วยให้การสื่อสารทางไกลสะดวกและรวดเร็ว เพราะสามารถสื่อสารกันได้ทั้งจดหมาย ภาพ หรือเสียง นอกจากนี้ยังมีบริการอื่นๆ อีกหลายชนิดบนเครือข่ายอินเตอร์เน็ต เช่น จดหมายข่าว หรือจดหมายเวียน (Mail) การใช้คอมพิวเตอร์บนเครื่องอื่น (Telnet) และการขนถ่ายแฟ้ม (FTP – File Transfer) เป็นต้น

(6) การประชุมทางไกล (Tele Conference) เป็นการประชุมของบุคคลที่อยู่คนละสถานที่และห่างไกลกัน อาจเป็นคนละห้อง คนละตึก คนละจังหวัด คนละประเทศ หรือคนละทวีป โดยอาศัยอุปกรณ์โทรคมนาคมสื่อสารถึงกัน ข่าวสารที่รับส่งถึงได้ทั้งตัวอักษร เสียง และภาพพร้อมๆ กัน โดยทั่วไปการประชุมทางไกลจะแบ่งเป็น 2 ประเภท ได้แก่

- การประชุมทางไกลเฉพาะเสียง (Audio Conference) เป็นการประชุมที่อาศัยระบบโทรศัพท์ หรือวงจรเช่าจากองค์การโทรศัพท์ หรือการสื่อสารแห่งประเทศ เมื่อผู้เข้าประชุมพร้อมจึงเริ่มประชุม โดยผู้เข้าร่วมประชุมทุกคนจะได้ยินเสียงพูดพร้อมๆ กันเสมือนนั่งประชุมอยู่ในที่เดียวกัน และผู้ดำเนินการประชุมเป็นผู้จัดระเบียบการพูด

- การประชุมทางไกลทั้งเสียงและภาพ (Video Conference) เป็นการประชุมที่ใช้สายโทรศัพท์ หรือวงจรพิเศษเป็นสื่อนำภาพ เสียง และข้อมูล ไปยังผู้เข้าร่วมประชุม การใช้บริการสื่อสารรวมระบบดิจิตอล (ISDN – Integrated Service Digital Network) นั้น ช่วยรวมบริการด้านเสียง ภาพ และข้อมูลไว้ในเครือข่ายเดียวกัน โดยใช้เคเบิลใยแก้วนำแสงต่อเข้ากับคู่สายเพียงคู่เดียวก็ทำงานได้ทั้งเสียงและภาพ

2.1.4 การเข้าถึง (Access) ข้อมูล

ก. ความหมายของคำว่า “การเข้าถึง (Access) ข้อมูล”

การเข้าถึง (Access) ข้อมูลเป็นคำที่ไม่ได้มีความหมายเป็นพิเศษสำหรับนักคอมพิวเตอร์โดยทั่วๆไป แต่มีความสำคัญสำหรับการศึกษาถึงการลักลอบเข้าถึงข้อมูลโดยปราศจากอำนาจในทางกฎหมาย ซึ่งถือเป็นการกระทำความผิดทางอาญา

ตามร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... มาตรา 5 ได้กล่าวถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กรณีที่มีการเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหนึ่งเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ

การเข้าถึงตามร่างมาตรา 5 หากเป็นการเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน เป็นความผิดตามร่างมาตรา 7 ในบางกรณีการกระทำความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 7 นี้อาจไม่จำต้องกระทำผิดฐานเข้าถึงระบบคอมพิวเตอร์ตามมาตรา 5 ก่อนก็ได้ เช่น การเอาแผ่นบันทึกข้อมูลของผู้อื่นที่มีการตั้งรหัสผ่านไว้ไปเปิดอ่านในระบบคอมพิวเตอร์ของตนเอง

และถ้าผู้ที่ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ นำมาตรการดังกล่าวไปเปิดเผยโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น เป็นความผิดตามร่างมาตรา 6

เกี่ยวกับความผิดตามร่างมาตรา 5 และมาตรา 7 นี้ มีความเห็นในอีกแง่มุมหนึ่งว่า หากมาตรการป้องกันการเข้าถึงนั้นเป็นมาตรการที่ไม่แน่นหนา ประหนึ่งบ้านที่ใช้กลอนประตูคุณภาพต่ำ การบุกรุกหรือการเข้าถึงกระทำได้ง่ายและอาจไม่ได้เกิดจากความตั้งใจ และเป็นไปได้ที่บุคคลในครอบครัวเดียวกันนั้นเองที่ต้องการใช้เครื่องคอมพิวเตอร์นั้น โดยไม่มีเจตนาร้าย ด้วยเหตุนี้

กฎหมายจึงได้บัญญัติไว้ให้เป็นความผิดอันยอมความได้ และกำหนดโทษไว้ไม่สูงนักและในการประชุมของคณะกรรมการกฤษฎีกา นักวิชาการ-ผู้เชี่ยวชาญทางคอมพิวเตอร์ท่านหนึ่งได้เปรียบเทียบความผิดข้างต้นไว้น่าฟังว่า หากเปรียบระบบคอมพิวเตอร์เป็นบ้านหลังหนึ่ง การเข้าถึงระบบคอมพิวเตอร์อันเป็นความผิดตามร่างมาตรา 5 นั้น ก็เสมือนกับการบุกรุกเข้าไปในบ้านของผู้อื่น การเข้าถึงข้อมูลคอมพิวเตอร์อันเป็นความผิดตามร่างมาตรา 7 ก็เสมือนว่าผู้บุกรุกนั้นนอกจากจะเข้าไปในบ้านหลังนั้นได้แล้ว ยังได้เข้าไปรื้อค้นเอกสารในตู้เก็บเอกสารในนั้นด้วย ส่วนความผิดตามร่างมาตรา ๖ นั้น เสมือนเป็นการนำกุญแจผีที่ไขเข้าไปในบ้านได้ แจกจ่ายให้กับบุคคลอื่นนั่นเอง[9]

กฎหมายของประเทศสหรัฐอเมริกา ได้ให้คำนิยาม คำว่า “การเข้าถึง (Access) ข้อมูล” ไว้ ดังนี้

การเข้าถึง (Access) หมายถึง การเข้าไปสู่ (Approach) สั่ง (Instruct) สื่อสารกับ (Communicate with) ใส่ข้อมูลเข้าไปเก็บไว้ (Store data in) ล้วงข้อมูลมา (Retrieve data from) หรือเอาประโยชน์จาก (Make use of any resources of) เครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์มาใช้

จากคำนิยามดังกล่าวสามารถแยกพิจารณาในส่วนที่สำคัญ ดังนี้

เข้าไปสู่ (Approach) หมายถึง การกระทำที่เป็นการเข้าไปหาสิ่งที่ต้องการ ซึ่งอยู่ภายในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

การสั่ง (Instruct) หมายถึง การกระทำที่เป็นการสั่งให้เครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ทำงานตามที่ต้องการ

การสื่อสาร (Communicate with) หมายถึง การกระทำที่เป็นการติดต่อกับเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ ด้วยวิธีการสื่อสาร เช่น การติดต่อผ่านสายโทรศัพท์ ฯลฯ เพื่อให้ได้ประโยชน์ตามที่ต้องการ

การใส่ข้อมูลเข้าไปเก็บไว้ (Store data in) หมายถึง การกระทำที่เป็นการใส่ข้อมูลเข้าไปเก็บไว้ในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เพื่อประโยชน์ที่จะได้จากการทำงานของเครื่องคอมพิวเตอร์ในภายหลัง

การล้วงข้อมูลมาจาก (Retrieve data from) หมายถึง การกระทำที่เป็นการเอาข้อมูลออกมาจากเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เพื่อประโยชน์ของตน

---

[9] แนวความคิดและหลักการของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ . นายสุนทร เปลี่ยนสี, นิติกร ๕ ฝ่ายกฎหมายกระบวนการยุติธรรมทางอาญา สำนักงานคณะกรรมการกฤษฎีกา

การเอาประโยชน์จาก (Make use of any resources of) หมายถึง การกระทำใดๆ ต่อเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เพื่อประโยชน์ของตน

ดังนั้น การเข้าถึงนี้ อาจเป็นการเข้าถึงโดยผู้กระทำผิดรู้หรือได้รหัสผ่านของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์มาโดยมิชอบ แล้วทำการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น หรืออาจเป็นการเข้าถึงผ่านระบบเครือข่าย ผู้กระทำผิดอาจเป็นผู้มีความรู้ด้านคอมพิวเตอร์ดีพอที่จะเจาะมาตรการป้องกันการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้นได้ สังเกตว่า ร่างกฎหมายฉบับนี้เอาผิดกับผู้ที่พยายามเจาะ (hacking or cracking) เข้าไปในระบบของผู้อื่นเลยทีเดียว ไม่คำนึงว่าเข้าไปโดยประสงค์อย่างไร เพียงแต่เข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงไว้ ก็เป็นความผิดสำเร็จทันที

ข. วิธีการเข้าถึง (Access) ข้อมูล ความเจริญก้าวหน้าด้านเทคโนโลยีในปัจจุบันทำให้ไม่จำเป็นที่จะต้องเข้าไปถึงคอมพิวเตอร์ที่บันทึกข้อมูลหลัก เพียงแต่มีคอมพิวเตอร์ส่วนบุคคล (Personal Computer : PC.) ที่ติดตั้งซอฟต์แวร์ในการติดต่อกับเครือข่ายและโมเด็มที่พ่วงคู่กับสายโทรศัพท์ ที่เรียกว่า “การต่อเชื่อมคอมพิวเตอร์เข้าสู่สายอินเตอร์เน็ต” ก็จะสามารถติดต่อสื่อสารกับคอมพิวเตอร์เครื่องที่ประสงค์จะเข้าถึง และใช้ข้อมูลภายในนั้นได้

ค. มาตรการรักษาความปลอดภัยของข้อมูลในคอมพิวเตอร์ เป้าหมายสำคัญของการรักษาความปลอดภัยที่แท้จริง คือ การปกป้องให้ข้อมูลนั้นเป็นความลับ มีความสมบูรณ์ถูกต้อง และคงอยู่ตลอดเวลาที่เก็บอยู่ในเครื่องคอมพิวเตอร์[10] ระบบการรักษาความปลอดภัยของข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์นั้น โดยทั่วไป อุปกรณ์ต่างๆ ของเครื่องคอมพิวเตอร์จะจำกัดการเข้าถึงโดยผู้ใช้ ซึ่งจะต้องระบุตัวผู้ใช้ (User Identification : User-ID) เอาไว้ โดยใช้รหัสผ่าน (Password) เพื่อใช้เป็นกุญแจในการเข้าสู่ระบบ

2.2 หลักเกณฑ์การคุ้มครองสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล

การให้ความคุ้มครองสิทธิของประชาชนจากการละเมิดสิทธิเสรีภาพของเจ้าพนักงานของรัฐ ไม่ว่าจะเป็นการดำเนินการจับกุม หรือการตรวจค้น ก่อนศตวรรษที่ 18 เป็นเหตุให้เจ้าพนักงานของรัฐมีอำนาจมากในการปฏิบัติหน้าที่โดยไม่มีหลักเกณฑ์ใดมาจำกัดอำนาจของเจ้าพนักงานเหล่านั้นได้ เช่น เจ้าพนักงานของรัฐในประเทศฝรั่งเศสสามารถจับบุคคลไปขังไว้โดยไม่

---

[10] เจนศักดิ์ ตั้งพันธุ์สุริยะ. (2543). **แรกเริ่มเรียนรู้ เรื่องรักษาความปลอดภัยให้ระบบคอมพิวเตอร์.** เรียบเรียงจาก Computer Security for Dummies ของ Peter T. Davis และ Barry D. Lewis. หน้า 27.

แจ้งข้อกล่าวหา และสามารถขังไว้ได้โดยไม่มีกำหนดเวลา[11] ในศตวรรษที่ 8 นักปราชญ์หลายท่าน เช่น มองเตสกิเออ ฯลฯ จึงได้สร้างแนวคิดเกี่ยวกับสิทธิมนุษยชนขึ้น เป็นการนำไปสู่แนวความคิดในการให้ความคุ้มครองสิทธิมนุษยชนมากขึ้นเห็นได้จากการจัดทำเอกสารที่เกี่ยวกับการให้ความคุ้มครองสิทธิของบุคคล เช่น ในประเทศสหรัฐอเมริกามีการจัดทำ The Declaration of Independence[12] และประเทศอังกฤษได้จัดทำ Magna Carta [13]

2.2.1 ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 เดิมการให้ความคุ้มครองสิทธิและเสรีภาพของบุคคลจะเป็นการให้ความคุ้มครองกันภายในรัฐใดรัฐหนึ่งเท่านั้น จนกระทั่งวันที่ 10 ธันวาคม ค.ศ. 1948 องค์การสหประชาชาติได้มีการประชุมและประกาศ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 เป็นการให้ความร่วมมือกันระหว่างประเทศเพื่อให้ความคุ้มครองสิทธิและเสรีภาพของบุคคล และพัฒนาไปในทิศทางเดียว กัน[14]

ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ได้กำหนดหลักเกณฑ์ที่สำคัญเกี่ยวกับการคุ้มครองสิทธิในความเป็นอยู่ทั่วไปของประชาชน ดังนี้ “บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นอยู่ส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือการถูกลบหลู่ในเกียรติยศ และชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับการคุ้มครองจากกฎหมายต่อการแทรกแซงหรือการลบหลู่ดังกล่าวนั้น” จากบทบัญญัติดังกล่าวเป็นการให้ความคุ้มครองความเป็นอยู่ทั่วไปในชีวิตส่วนตัวของบุคคลทั้งที่เป็นการดำเนินชีวิตประจำวัน การติดต่อสื่อสาร เป็นหลัก และยกเว้นในกรณีที่เพื่อประโยชน์สาธารณะ และมีกฎหมายอนุญาตให้ทำได้ แต่ก็ต้องมีการควบคุมมิให้มีการใช้อำนาจที่กระทบกระเทือนต่อสิทธิของประชาชนมากเกินไป สมัชชาสหประชาชาติจึงได้สร้างหลักการควบคุมการใช้อำนาจของรัฐขึ้นมา โดยประกาศใช้ “ประมวลจรรยาบรรณสำหรับเจ้าหน้าที่ผู้มีหน้าที่โดยกฎหมาย” (Code of Conduct for Law Enforcement) ซึ่งข้อที่ 1 บัญญัติให้เจ้าพนักงานผู้มีหน้าที่รักษากฎหมายต้องปฏิบัติตามกฎหมาย โดยมุ่งที่จะให้บริการแก่ประชาชน และคุ้มครองให้ประชาชนปลอดภัยจากการกระทำที่ผิดกฎหมาย และข้อ 2 บัญญัติ ให้เจ้าพนักงานผู้มีหน้าที่รักษา

---

[11] จงรักษ์ จุฑานนท์. (2525). **การคุ้มครองสิทธิของประชาชนต่อการถูกจับและตรวจค้นโดยไม่ชอบธรรม**. หน้า 1.

[12] กุลพล พลวัน. (2538). **พัฒนาการสิทธิมนุษยชน** (พิมพ์ครั้งที่ 3). หน้า 31

[13] กุลพล พลวัน. เล่มเดิม. หน้า 74

[14] กุลพล พลวัน. เล่มเดิม. หน้า 36.

กฎหมาย เมื่อมีการปฏิบัติตามกฎหมายที่เป็นการกระทบกระเทือนถึงสิทธิสิทธิดังกล่าว การกระทำนั้นต้องเคารพ และคุ้มครองศักดิ์ศรีความเป็นมนุษย์ และจะต้องไม่ทำลายล้างหลักสิทธิมนุษยชน[15]

2.2.2 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 นับแต่ประเทศไทยมีการเปลี่ยนแปลงการปกครองจากระบอบสมบูรณาญาสิทธิราชย์ (Absolute Monarchy) มาเป็นระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข (Liberal Democracy with the King as Head of the State) ในปี พ.ศ. 2475 ตั้งแต่นั้นการจัดทำรัฐธรรมนูญแห่งราชอาณาจักรไทยฉบับต่างๆ ก็เหมือนกับรัฐเสรีประชาธิปไตยอื่นๆ คือได้รับแรงบันดาลใจมาจาก "ลัทธิปัจเจกชน" (Individualism)[16] เช่นเดียวกับการจัดทำรัฐธรรมนูญของรัฐเสรีประชาธิปไตย (Liberal and Democratic State) อื่นๆ ซึ่งแนวความคิดของลัทธินี้สอนว่า "มนุษย์ทุกคนเกิดมามีศักดิ์ศรี" นั่นคือ ศักดิ์ศรีความเป็นมนุษย์ (Human Dignity) รัฐธรรมนูญของรัฐเสรีประชาธิปไตยทุกรัฐจึงได้บัญญัติรับรองและให้ความคุ้มครองศักดิ์ศรีความเป็นมนุษย์ของปัจเจกชนไว้อย่างชัดเจนเป็น "สิทธิและเสรีภาพขั้นพื้นฐาน" (Fundamental Rights and Liberties) ซึ่งรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 4 บัญญัติว่า "ศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของบุคคลย่อมได้รับความคุ้มครอง" มาตรา 26 บัญญัติว่า "การใช้อำนาจโดยองค์กรของรัฐทุกองค์กร ต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพตามรัฐธรรมนูญนี้" และมาตรา 27 บัญญัติว่า "สิทธิและเสรีภาพที่รัฐธรรมนูญนี้รับรองไว้โดยชัดแจ้ง โดยปริยาย หรือโดยคำวินิจฉัยของศาลรัฐธรรมนูญ ย่อมได้รับความคุ้มครองและผูกพันรัฐสภา คณะรัฐมนตรี ศาล และองค์กรอื่นของรัฐโดยตรงในการตรากฎหมาย การใช้บังคับกฎหมายและการตีความกฎหมายทั้งปวง" แสดงให้เห็นว่า ไม่ว่าสิทธิหรือเสรีภาพของบุคคลจะต้องอยู่ภายใต้ "ประโยชน์ส่วนรวม" (General Interest) หรือ "ประโยชน์สาธารณะ" (Public Interest) หรือ "ความมั่นคงแห่งชาติ" (National Security)

"สิทธิตามรัฐธรรมนูญ" นั้น ถือว่าเป็น "สิทธิตามกฎหมายมหาชน" (das subjektive oeffentliche Recht) หมายถึงอำนาจตามรัฐธรรมนูญหรือกฎหมายสูงสุดได้บัญญัติให้การรับรองคุ้มครองแก่ปัจเจกบุคคลในอันที่จะกระทำการใด หรือไม่กระทำการใด การให้อำนาจแก่ปัจเจกบุคคลดังกล่าวได้ก่อให้เกิดสิทธิเรียกร้องที่จะไม่ให้บุคคลใดแทรกแซงในสิทธิตามรัฐธรรมนูญของตน โดยเฉพาะอย่างยิ่งเรียกร้องต่อองค์กรของรัฐมิให้แทรกแซงในขอบเขตสิทธิของตน ในบางกรณีการรับรองดังกล่าวได้ก่อให้เกิดสิทธิเรียกร้องให้รัฐดำเนินการอย่างใดอย่างหนึ่ง

---

[15] ศุภฤกษ์ ศุกรเสพย์. (2545). **การค้นในที่รโหฐานของเจ้าพนักงานป้องกันและปราบปรามยาเสพติด**. หน้า 10.

[16] Pierre WIGNY. **Droit constitutionnel : Principle et droit prositif.** Tome premier, Bruxelles, Bruylant, 1952, pp. 257-258.

สิทธิตามรัฐธรรมนูญจึงเป็นความสัมพันธ์ระหว่างปัจเจกบุคคลต่อรัฐ และสิทธิตามรัฐธรรมนูญเป็นสิ่งที่ผูกพันองค์กรผู้ใช้อำนาจรัฐทั้งหลายที่จะต้องให้ความเคารพ ปกป้อง และคุ้มครองสิทธิตามรัฐธรรมนูญดังกล่าว เพื่อให้สิทธิตามรัฐธรรมนูญดังกล่าวมีผลในทางปฏิบัติ[17]

"เสรีภาพตามรัฐธรรมนูญ" หมายถึง อำนาจของบุคคลในอันที่จะกำหนดตนเอง (Self – determination) โดยอำนาจนี้บุคคลย่อมเลือกวิถีชีวิตของตนได้ด้วยตนเองตามใจปรารถนา เสรีภาพจึงเป็นอำนาจที่บุคคลมีอยู่เหนือตนเอง[18]

จะเห็นได้ว่ารัฐธรรมนูญฉบับปัจจุบันมีเจตนารมณ์ที่จะให้ความคุ้มครองสิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์ของประชาชนเป็นสำคัญ ดังจะเห็นได้จากบทบัญญัติในมาตรา 26 บัญญัติว่า "การใช้อำนาจโดยองค์กรของรัฐทุกองค์กร ต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพตามบทบัญญัติแห่งรัฐธรรมนูญนี้"

มาตรา 29 วรรคแรก บัญญัติว่า "การจำกัดสิทธิและเสรีภาพของบุคคลที่รัฐธรรมนูญรับรองไว้จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อการที่รัฐธรรมนูญนี้กำหนดไว้และเท่าที่จำเป็นเท่านั้น และจะกระทบกระเทือนต่อสาระสำคัญแห่งสิทธิและเสรีภาพนั้นมิได้"

และมาตรา 37 วรรคแรก บัญญัติว่า "บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบด้วยกฎหมาย

จากบทบัญญัติดังกล่าวที่กำหนดขึ้นเพื่อปกป้องสิทธิและเสรีภาพของประชาชนมิให้ถูกล่วงละเมิด แม้กฎหมายจะให้การรับรองเสรีภาพอย่างใดอย่างหนึ่งให้แก่บุคคลใดบุคคลหนึ่ง ย่อมมีผลก่อให้เกิดหน้าที่แก่ผู้อื่นด้วยเช่นกัน แต่หน้าที่ที่เกิดขึ้นกับผู้อื่นอันเนื่องมาจากการที่กฎหมายบัญญัติรับรองเสรีภาพให้แก่บุคคลหนึ่งนี้ เป็นแต่เพียงหน้าที่ที่จะต้องเคารพเสรีภาพของผู้ทรงเสรีภาพ และผู้ทรงเสรีภาพเองก็คงมีอำนาจตามกฎหมายแต่เพียงที่จะเรียกร้องให้ผู้อื่นละเว้นจากการรบกวนขัดขวางการใช้เสรีภาพของตนเท่านั้น หาได้มีอำนาจที่จะเรียกร้องให้ผู้อื่นกระทำการอย่างใดอย่างหนึ่งซึ่งมีลักษณะเป็นการส่งเสริมหรือช่วยเหลือการใช้เสรีภาพของตนด้วย

สิทธิและเสรีภาพตามรัฐธรรมนูญนั้นมีผลผูกพันโดยตรงต่ออำนาจนิติบัญญัติ อำนาจบริหารและอำนาจตุลาการ[19] เพราะอำนาจนิติบัญญัติ อำนาจบริหาร และอำนาจตุลาการ ต่างก็เป็น

---

[17] บรรเจิด สิงคะเนติ. (2543). **หลักพื้นฐานของสิทธิเสรีภาพ และศักดิ์ศรีความเป็นมนุษย์ตามรัฐธรรมนูญ พ.ศ. 2540**. หน้า 47.

[18] วรพจน์ วิศรุตพิชญ์. (2543). **สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540**. หน้า 22.

[19] บรรเจิด สิงคะเนติ. เล่มเดิม. หน้า 52.

อำนาจที่มาจากอำนาจอธิปไตย ซึ่งเป็นส่วนหนึ่งที่แสดงออกถึงความเป็นรัฐ นอกจากอาณาเขต และพลเมือง

ปัจจุบันพระราชบัญญัติ การสอบสวนคดีพิเศษ พ.ศ. 2547 มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคลซึ่งมาตรา ๒๙ ประกอบกับมาตรา ๓๑ มาตรา ๓๔ มาตรา ๓๕ มาตรา ๓๖ มาตรา ๓๗ มาตรา ๔๘ มาตรา ๕๘ มาตรา ๒๓๗ และมาตรา ๒๓๘ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย ได้แก่บทบัญญัติต่อไปนี้

มาตรา ๒๔ บัญญัติว่า "เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานสอบสวนคดีพิเศษมีอำนาจดังต่อไปนี้ด้วย

(๑) เข้าไปในเคหสถาน หรือสถานที่ใดๆ เพื่อตรวจค้น เมื่อมีเหตุสงสัยตามสมควรว่ามีบุคคลที่มีเหตุสงสัยว่ากระทำความผิดที่เป็นคดีพิเศษหลบซ่อนอยู่ หรือมีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้ ประกอบกับมีเหตุอันควรเชื่อว่าเนื่องจากการเนิ่นช้ากว่าจะเอาหมายค้นมาได้บุคคลนั้นจะหลบหนีไป หรือทรัพย์สินนั้นจะถูกโยกย้าย ซุกซ่อน ทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิม

(๒) ค้นบุคคล หรือยานพาหนะที่มีเหตุสงสัยตามสมควรว่ามีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้

(๓) มีหนังสือสอบถามหรือเรียกให้สถาบันการเงิน ส่วนราชการ องค์การ หรือหน่วยงานของรัฐ หรือรัฐวิสาหกิจ ส่งเจ้าหน้าที่ที่เกี่ยวข้องมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชีเอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(๔) มีหนังสือสอบถาม หรือเรียกบุคคลใดๆ มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชีเอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(๕) ยึด หรืออายัดทรัพย์สินที่ค้นพบ หรือที่ส่งมาดังกล่าวไว้ใน (๑) (๒) (๓) และ (๔) การใช้อำนาจตามวรรคหนึ่ง ให้พนักงานสอบสวนคดีพิเศษปฏิบัติตามข้อบังคับที่ กคพ. กำหนด เฉพาะการใช้อำนาจตามวรรคหนึ่ง (๑) นอกจากพนักงานสอบสวนคดีพิเศษต้องดำเนินการเกี่ยวกับวิธีการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาแล้ว ให้พนักงานสอบสวนคดีพิเศษแสดงความบริสุทธิ์ก่อนการเข้าค้น รายงานเหตุผลและผลการตรวจค้นเป็นหนังสือต่อผู้บังคับบัญชาเหนือขึ้นไป และบันทึกเหตุสงสัยตามสมควรและเหตุอันควรเชื่อที่ทำให้สามารถเข้าค้นได้เป็นหนังสือให้ไว้แก่ผู้ครอบครองเคหสถานหรือสถานที่ค้น แต่ถ้าไม่มีผู้ครอบครองอยู่ ณ ที่นั้น ให้พนักงาน

สอบสวนคดีพิเศษส่งมอบสำเนาหนังสือนั้นให้แก่ผู้ครอบครองดังกล่าวในทันทีที่กระทำได้ และหากเป็นการเข้าค้นในเวลากลางคืนภายหลังพระอาทิตย์ตก พนักงานสอบสวนคดีพิเศษผู้เป็นหัวหน้าในการเข้าค้นต้องเป็นข้าราชการพลเรือนตำแหน่งตั้งแต่ระดับ ๗ ขึ้นไปด้วย

ให้พนักงานสอบสวนคดีพิเศษผู้เป็นหัวหน้าในการเข้าค้นส่งสำเนาบันทึกเหตุสงสัยตามสมควรและเหตุอันควรเชื่อตามวรรคสาม และสำเนาบันทึกการตรวจค้นและบัญชีทรัพย์ที่ยึดหรืออายัดต่อศาลจังหวัดที่มีอำนาจเหนือท้องที่ที่ทำการค้น หรือศาลอาญาในเขตกรุงเทพมหานครภายในสี่สิบแปดชั่วโมงหลังจากสิ้นสุดการตรวจค้น เพื่อเป็นหลักฐาน

พนักงานสอบสวนคดีพิเศษระดับใดจะมีอำนาจหน้าที่ตามที่ได้กำหนดไว้ตามวรรคหนึ่งทั้งหมดหรือแต่บางส่วน หรือจะต้องได้รับอนุมัติจากบุคคลใดก่อนดำเนินการให้เป็นไปตามที่อธิบดีกำหนดโดยทำเอกสารให้ไว้ประจำตัวพนักงานสอบสวนคดีพิเศษผู้ได้รับอนุมัตินั้นและพนักงานสอบสวนคดีพิเศษผู้นั้นต้องแสดงเอกสารดังกล่าวต่อบุคคลที่เกี่ยวข้องทุกครั้ง

มาตรา 25 ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษพนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

(๑) มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ

(๒) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

(๓) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวันโดยกำหนดเงื่อนไขใดๆ ก็ได้ และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อพนักงานสอบสวนคดีพิเศษได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

บรรดาข้อมูลข่าวสารที่ได้มาตามวรรคหนึ่ง ให้เก็บรักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษซึ่งได้รับอนุญาตตามวรรคหนึ่ง และให้ใช้ประโยชน์ในการสืบสวนหรือใช้เป็นพยานหลักฐานเฉพาะในการดำเนินคดีพิเศษดังกล่าวเท่านั้น ส่วนข้อมูลข่าวสารอื่นให้ทำลายเสียทั้งสิ้น ทั้งนี้ ตามข้อบังคับที่ กคพ. กำหนด

มาตรา 26 ห้ามมิให้บุคคลใดเปิดเผยข้อมูลข่าวสารที่ได้มาเนื่องจากการดำเนินการตามมาตรา 25 เว้นแต่เป็นข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษซึ่งได้รับอนุญาตตามมาตรา 25 และเป็นการปฏิบัติตามอำนาจหน้าที่หรือตามกฎหมายหรือตามคำสั่งศาล

จะเห็นได้ว่าอำนาจที่กฎหมายมอบให้กับพนักงานสอบสวนคดีพิเศษตามบทบัญญัติข้างต้นเป็นการกระทำที่กระทบต่อสิทธิเสรีภาพของประชาชน และจะทำให้เกิดการใช้อำนาจที่ไร้ขอบเขต และประเทศไทยเองก็ยังไม่มีบทบัญญัติของกฎหมายที่ให้การคุ้มครองสิทธิในชีวิตส่วนตัวของบุคคลโดยตรง แต่หากพิจารณาบทกฎหมายที่มีในปัจจุบันแล้วจะพบว่า กฎหมายที่ให้ความคุ้มครองสิทธิส่วนบุคคลมีมากมายพอสมควร ไม่เฉพาะที่ปรากฏอยู่ในประมวลกฎหมายอาญาในความผิดฐานหมิ่นประมาท ความผิดฐานดูหมิ่น ความผิดฐานบุกรุก และความผิดฐานก่อความเดือดร้อนรำคาญเท่านั้น ในประมวลกฎหมายแพ่งและพาณิชย์ ก็มีอยู่ในมาตรา 420 ซึ่งบัญญัติว่า "ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น"

คำว่า "สิทธิอย่างหนึ่งอย่างใด" นี้ก็น่าจะมีความหมายถึง สิทธิในชีวิตส่วนตัวด้วย ซึ่งจะต้องพิจารณากันเป็นกรณีๆ ไป

จะเห็นได้ว่ากฎหมายไทยถือว่าการละเมิดสิทธิในชีวิตส่วนตัวนั้น ถือเป็นความผิดฐานละเมิดตามปกติธรรมดาไม่ได้แยกเป็นพิเศษเหมือนสหรัฐอเมริกา โดยจะต้องพิจารณาถึงเจตนาว่าเป็นการกระทำโดยจงใจหรือประมาทเลินเล่อที่กระทำต่อบุคคลอื่นโดยมิชอบด้วยกฎหมาย แต่การล่วงละเมิดสิทธิในชีวิตส่วนตัวของบุคคลในสหรัฐอเมริกานั้นจะพิจารณาจากผลของการกระทำเป็นสำคัญ และประเทศไทยยังไม่ปรากฏว่ามีคดีเกี่ยวกับการละเมิดสิทธิในชีวิตส่วนตัวขึ้นสู่ศาลดังเช่นที่เกิดขึ้นในประเทศสหรัฐอเมริกา

แม้ว่ารัฐธรรมนูญของประเทศสหรัฐอเมริกาจะไม่มีการกล่าวถึงสิทธิในชีวิตส่วนตัวไว้โดยตรง แต่ศาลสูงของสหรัฐอเมริกาก็ได้วินิจฉัยรับรองว่าสิทธิในชีวิตส่วนตัวเสมือนเป็นสิทธิประการหนึ่งในรัฐธรรมนูญ โดยเฉพาะในคดี Griswold V. Connecticut 381 U.S. 479 (1965) ศาล

สูงสหรัฐได้วินิจฉัยไว้อย่างชัดเจนว่า เจตนารมณ์ของรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 1 เป็นเสมือนศูนย์รวมความรู้ที่ทุกคนไขว่คว้าได้ สิทธิเสรีภาพในการพูด และการพิมพ์โฆษณา ไม่เพียงแต่จะหมายถึงการพูดและการพิมพ์เท่านั้น แต่รวมไปถึงสิทธิในการจำหน่ายจ่ายแจก

ขณะเดียวกันบทบัญญัติรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 3 และ 4 ก็บัญญัติห้ามมิให้บุกรุกเข้าไปในเคหสถานของบุคคลอื่นโดยปราศจากความยินยอม และสิทธิของบุคคลที่จะมีความปลอดภัยในร่างกาย เคหสถาน เอกสาร และทรัพย์สิ่งของจากการตรวจค้น จับกุม ยึดโดยไม่มีเหตุอันสมควร และในบทบัญญัติรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 9 ก็บัญญัติคุ้มครองสิทธิของบุคคลที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองในคดีอาญาและรับรองว่าบรรดาสิทธิต่างๆ ในรัฐธรรมนูญจะตีความให้เป็นการปฏิเสธหรือลิดรอนสิทธิของผู้อื่นไม่ได้

สรุปแล้วบทบัญญัติรัฐธรรมนูญของสหรัฐอเมริกาล้วนแฝงไว้ด้วยสิทธิในชีวิตส่วนบุคคลแทบทั้งสิ้น จึงไม่อาจปฏิเสธได้ว่าสิทธิส่วนบุคคลเป็นสิทธิประการหนึ่ง ซึ่งย่อมได้รับการรับรองโดยกฎหมายโดยชอบ หากผู้ใดละเมิดก็จะมีความผิด โดยยึดถือแนวความคิดคล้ายๆกับการหมิ่นประมาทในตัวของมันเอง (Libel perse)

2.2.3 กฎหมายวิธีพิจารณาความอาญา บทบัญญัติสำคัญของกฎหมายวิธีพิจารณาความอาญาจะอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งเดิมบทบัญญัติที่มีก็เป็นไปเพื่อความสะดวกในการใช้อำนาจของรัฐ การคำนึงถึงสิทธิเสรีภาพส่วนบุคคลมีเพียงส่วนน้อย แต่ได้ให้ความสำคัญมากขึ้นในรัฐธรรมนูญฉบับปัจจุบัน[20]

2.2.3.1 สถานะของผู้ถูกกล่าวหา บทบัญญัติที่ให้ความสำคัญต่อสิทธิเสรีภาพส่วนบุคคลของผู้ถูกกล่าวหา ได้แก่ มาตรา 165 วรรคสาม บัญญัติว่า “ก่อนที่ศาลประทับฟ้องมิให้ถือว่าจำเลยอยู่ในฐานะเช่นนั้น” นั่นคือ ก่อนที่ผู้ที่ถูกผู้เสียหายฟ้องถูกศาลประทับฟ้องยังไม่ถือเป็น “จำเลย” ผู้ถูกกล่าวหาในปัจจุบันจึงไม่ถือเป็นวัตถุแห่งการซักฟอกหรือเป็น “กรรมในคดี” (Prozess-objekt) อีกต่อ แต่เป็น “ประธานในคดี” (Prozess-subjekt) [21] ซึ่งสอดคล้องกับบทบัญญัติในรัฐธรรมนูญมาตรา 241 วรรคหนึ่ง บัญญัติว่า “ในคดีอาญา ผู้ต้องหาหรือจำเลยย่อมมีสิทธิได้รับการสอบสวนหรือการพิจารณาคดีด้วยความเร็ว ต่อเนื่อง และเป็นธรรม”

2.2.3.2 สิทธิของผู้ถูกกล่าวหา สิทธิของผู้ต้องหาที่จะไม่ให้การ เป็นสิทธิของผู้ถูกกล่าวหาในทางอยู่เฉย ซึ่งเป็นสิทธิที่จะตัดสินใจในคดีด้วยตนเอง ในมาตรา 134 บัญญัติว่า “เมื่อผู้ต้องหาเต็มใจให้การอย่างใด ก็ให้จดคำให้การไว้ ถ้าผู้ต้องหาไม่เต็มใจให้การเลยก็ให้บันทึกไว้”

---

[20] คณิต ณ นคร. เล่มเดิม. หน้า 31.

[21] คณิต ณ นคร. เล่มเดิม. หน้า 102.

และในชั้นศาล มาตรา 174 บัญญัติว่า "ถ้าจำเลยไม่ยอมให้การ ก็ให้ศาลจดรายงานไว้และพิจารณาต่อไป" และเพื่อประกันสิทธิในการให้การหรือไม่ให้การของจำเลย มาตรา 135 บัญญัติว่า "ห้ามมิให้พนักงานสอบสวนทำหรือจัดให้ทำการใดๆ ซึ่งเป็นการล่อลวง หรือขู่เข็ญ หรือให้สัญญากับผู้ต้องหาเพื่อจูงใจให้เขาให้การอย่างใดๆ ในเรื่องที่ต้องหานั้น"

การล่อลวง หรือขู่เข็ญ หรือให้สัญญา ซึ่งเป็นการกระทำที่มิชอบด้วยกฎหมายตามที่บัญญัติไว้ในมาตรา 135 นั้น เป็นเพียงการกระทำต้องห้ามที่กฎหมายบัญญัติเป็นตัวอย่างไว้เท่านั้น แต่ความหมายที่บทบัญญัติในมาตรานี้ต้องการแสดงให้ปรากฏก็คือ "การกระทำที่เป็นการละเมิดเสรีภาพในการตัดสินใจของผู้ต้องหา" ทุกสถาน[22]

บทบัญญัติที่ถือว่าขัดแย้งกับบทบัญญัติที่ให้ความคุ้มครองสิทธิของผู้ถูกกล่าวหาในทางอยู่เฉย ได้แก่ มาตรา 132 บัญญัติว่า "เพื่อประโยชน์แห่งการรวบรวมพยานหลักฐาน พนักงานสอบสวนมีอำนาจตรวจค้นผู้ต้องหา จำเลยหรือพิมพ์ลายนิ้วมือ ลายมือหรือลายเท้า" เป็นบทบัญญัติที่แสดงให้เห็นถึงอำนาจของรัฐในการแสวงหาพยานหลักฐานจากผู้ต้องหา หรือจำเลยเพื่อประโยชน์ในการรวบรวมพยานหลักฐาน โดยไม่จำเป็นจะต้องได้รับความยินยอมจากผู้ต้องหาหรือจำเลยดังกล่าว เพียงแต่การตรวจค้นนั้น มาตรา 85 วรรคหนึ่ง บัญญัติว่า "เจ้าพนักงานผู้จับหรือรับตัวผู้ถูกจับไว้ มีอำนาจค้นตัวผู้ต้องหา" และวรรคสอง บัญญัติว่า "การค้นนั้นจักต้องทำโดยสุภาพ ถ้าค้นตัวหญิงต้องให้หญิงอื่นเป็นผู้ค้น" ซึ่งแสดงถึงความเคารพสถานะความเป็นประธานในคดีของผู้ต้องหา

2.2.3.3 สถานะของผู้ต้องหา มาตรา 2 (2) นิยามคำว่า "ผู้ต้องหา" ว่าหมายความถึงบุคคลผู้ถูกหาว่าได้กระทำผิด แต่ยังมิได้ถูกฟ้องต่อศาล จากคำนิยาม บุคคลที่จะมีสถานะเป็นผู้ต้องหาตามกฎหมายจึงต้องเป็นบุคคลที่มีผู้กล่าวหาบุคคลนั้นว่าได้กระทำความผิดอาญาต่อเจ้าพนักงาน หรือเจ้าพนักงานกล่าวหาเอง

ในการกล่าวหาต่อเจ้าพนักงาน มาตรา 2 (7) อาจทำในรูปของคำร้องทุกข์ของผู้เสียหาย หรือตามมาตรา 2 (8) คำกล่าวโทษโดยบุคคลอื่น

2.2.3.4 สถานะของจำเลย มาตรา 2 (3) นิยามคำว่า "จำเลย" ว่าหมายถึงบุคคลซึ่งถูกฟ้องยังศาลแล้วโดยข้อหาว่าได้กระทำความผิด

ดังนั้นจะถือว่าบุคคลซึ่งถูกฟ้องยังศาลแล้วเป็นจำเลยในทันทีที่ยื่นฟ้องจะต้องพิจารณาจากผู้ฟ้องเป็นหลัก หากพนักงานอัยการเป็นผู้ฟ้อง ผู้ถูกฟ้องจะตกเป็นจำเลยทันทีโดยไม่ต้องมีการไต่สวนมูลฟ้องก่อนหรือไม่ แต่ในกรณีที่ผู้เสียหายเป็นผู้ฟ้อง มาตรา 165 วรรคสามตอนท้าย บัญญัติ

---

[22] คณิต ณ นคร. เล่มเดิม. หน้า 105..

ว่า “ก่อนที่ศาลจะประทับฟ้องมิให้ถือว่าจำเลยอยู่ในฐานะเช่นนั้น” ดังนั้นก่อนศาลประทับฟ้องผู้ถูกฟ้องจึงยังไม่ตกเป็นจำเลย

2.2.3.5 การแสวงหาพยานหลักฐาน พยานหลักฐานเป็นเครื่องมือประการหนึ่งในการดำเนินคดีอาญาที่มีความสำคัญมาก ซึ่งในคดีอาญาพยานหลักฐานทุกชนิดรับฟังได้ ดังจะเห็นได้จากมาตรา 226 บัญญัติว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ให้อ้างเป็นพยานหลักฐานได้แต่ต้องเป็นพยานหลักฐานชนิดที่มิได้เกิดจากแรงจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบด้วยประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน”

กระบวนการสำคัญชั้นต้นในการดำเนินคดีอาญา ได้แก่ การสืบสวนและการสอบสวน ซึ่งบทบัญญัติดังกล่าวถือเป็นหลักเบื้องต้นทั่วไปเกี่ยวกับพยานหลักฐานที่แสดงสถานะและความเป็นอิสระในการแสวงหาพยานหลักฐาน แต่สำหรับปัญหาอาชญากรรมที่มีอยู่ในปัจจุบัน เพื่อให้การบังคับใช้กฎหมายป้องกันและปราบปรามอาชญากรรมสำคัญๆ ให้มีประสิทธิภาพมากขึ้นจึงมีการบัญญัติ พระราชบัญญัติ การสอบสวนคดีพิเศษ พ.ศ. 2547 ขึ้น

โดยกฎหมายฉบับนี้ได้กำหนดลักษณะของอาชญากรรมที่เป็นคดีพิเศษแตกต่างไปจากอาชญากรรมธรรมดา เนื่องจากเป็นอาชญากรรมที่มีลักษณะพิเศษ เช่น อาชญากรรมทางเศรษฐกิจหรืออาชญากรรมทางธุรกิจ มีผลกระทบที่รุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของสังคม ประโยชน์ส่วนรวมของประชาชน หรือความมั่นคงของประเทศความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของประเทศ หรือคดีอาญาที่มีผู้มีอิทธิพลเป็นผู้ร่วมกระทำความผิด รวมทั้งอาชญากรรมที่เป็นองค์กรอาชญากรรม และอาชญากรรมข้ามชาติด้วย เป็นอาชญากรรมที่ให้ผลตอบแทนแก่ผู้ประกอบอาชญากรรมเป็นอย่างมาก ทั้งนี้ วิธีการและลักษณะการกระทำความผิดมีความซับซ้อนเป็นการยากที่เจ้าหน้าที่ของรัฐบาลจะเข้าถึงผู้เป็นตัวการที่อยู่เบื้องหลัง เพื่อนำมาดำเนินคดีและลงโทษตามกฎหมายได้ เนื่องจากขาดความรู้ความเชี่ยวชาญและเทคนิคเฉพาะด้านในการสืบสวนสอบสวนเพื่อรวบรวมพยานหลักฐานสำหรับการดำเนินคดี

ดังนั้นจึงมีการกำหนดมาตรการและวิธีการต่างๆ ที่เพิ่มประสิทธิภาพในการปฏิบัติหน้าที่ของพนักงานสอบสวนคดีพิเศษ เช่น การกำหนดให้มีคุณสมบัติเบื้องต้นและคุณสมบัติพิเศษ การผ่านการอบรมตามหลักสูตรที่กำหนด และการผ่านการประเมินความรู้ความสามารถ เป็นต้น นอกจากการเพิ่มประสิทธิภาพให้กับเจ้าหน้าที่สืบสวนสอบสวนโดยเฉพาะแล้ว กฎหมายยังให้อำนาจลักษณะพิเศษไว้ด้วย เพื่อแก้ไขปัญหาความบกพร่องของกระบวนการยุติธรรมให้มีประสิทธิภาพมากขึ้น เนื่องจากระบบการสอบสวนในปัจจุบันยังไม่สามารถแก้ไขปัญหาความบกพร่องของพยานหลักฐานในคดีบางประเภทได้ รวมทั้งระบบการสอบสวนที่มีอยู่แต่เดิม จะเห็น

ได้จากอาชญากรรมที่มีความเชี่ยวชาญในการใช้เทคโนโลยีระดับสูงในการประกอบอาชญากรรม ในขณะเดียวกันก็ใช้ความรู้ความเชี่ยวชาญในการปกปิดซ่อนเร้นทำลายพยานหลักฐาน

เพื่อการแสวงหาพยานหลักฐาน และนำตัวผู้กระทำความผิดมาลงโทษให้ได้ โดยอำนาจหน้าที่หลักของพนักงานสอบสวน ตามมาตรา 2 (6) นิยามว่า "พนักงานสอบสวน หมายความถึงเจ้าพนักงานซึ่งกฎหมายให้อำนาจและหน้าที่ทำการสอบสวน" และมาตรา 121 วรรคหนึ่ง บัญญัติว่า "พนักงานสอบสวนมีอำนาจสอบสวนคดีอาญาทั้งปวง" ซึ่งเป็นบทบัญญัติถึงอำนาจในการสอบสวนของพนักงานสอบสวน

การสอบสวนโดยทั่วไปจะเริ่มเมื่อรู้เรื่องความสงสัยว่ามีการกระทำความผิดอาญาเกิดขึ้น แต่การรู้นั้นสามารถรู้ได้ 2 ทาง ได้แก่ เมื่อมีการร้องทุกข์หรือการกล่าวโทษ และรู้เองซึ่งพิจารณาจากฐานความผิดอาญาประกอบ นั่นคือหากเป็นการกระทำความผิดที่เกี่ยวข้องกับประโยชน์ได้เสียของประชาชนส่วนรวม พนักงานสอบสวนก็ต้องทำการสอบสวนโดยไม่ชักช้า

โดยหลักจุดประสงค์ในการรวบรวมพยานหลักฐานก็เพื่อความน่าเชื่อถือของพยานหลักฐานเหล่านั้น แต่ปัญหาในทางปฏิบัติหรือปัญหาทางเทคนิคของคดีพิเศษคือปัญหาในการแสวงหาพยานหลักฐาน ซึ่งไม่มีประจักษ์พยานเพราะผู้กระทำความผิดจะไม่มีส่วนเกี่ยวข้องกับพยานหลักฐานโดยตรง หรือสามารถทำลายพยานหลักฐานได้โดยง่าย ดังนั้นพนักงานสอบสวนจึงต้องมีความรู้ความเชี่ยวชาญสำหรับวิธีและมาตรการพิเศษที่จะใช้ในการแสวงหาพยานหลักฐานเพื่อนำมาดำเนินคดีกับผู้กระทำความผิดให้ได้

สำหรับ พระราชบัญญัติ การสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 21 (1) บัญญัติว่า

"(๑) คดีความผิดทางอาญาตามกฎหมายที่กำหนดไว้ในบัญชีท้ายพระราชบัญญัตินี้ และที่กำหนดในกฎกระทรวงโดยการเสนอแนะของ กคพ. โดยคดีความผิดทางอาญาตามกฎหมายดังกล่าว จะต้องมีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้

(ก) คดีความผิดทางอาญาที่มีความซับซ้อน จำเป็นต้องใช้วิธีการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเป็นพิเศษ

(ข) คดีความผิดทางอาญาที่มีหรืออาจมีผลกระทบอย่างรุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน ความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของประเทศ

(ค) คดีความผิดทางอาญาที่มีลักษณะเป็นการกระทำความผิดข้ามชาติที่สำคัญ หรือเป็นการกระทำขององค์กรอาชญากรรม หรือ

(ง) คดีความผิดทางอาญาที่มีผู้ทรงอิทธิพลที่สำคัญเป็นตัวการ ผู้ใช้หรือผู้สนับสนุน

ทั้งนี้ ตามรายละเอียดของลักษณะของการกระทำความผิดที่ กคพ. กำหนด

DPU

(๒) คดีความผิดทางอาญาอื่นนอกจาก (๑) ตามที่ กคพ. มีมติด้วยคะแนนเสียงไม่น้อยกว่าสองในสามของกรรมการทั้งหมดเท่าที่มีอยู่

ในคดีที่มีการกระทำอันเป็นกรรมเดียวผิดต่อกฎหมายหลายบท และบทใดบทหนึ่งจะต้องดำเนินการโดยพนักงานสอบสวนคดีพิเศษตามพระราชบัญญัตินี้ หรือคดีที่มีการกระทำความผิดหลายเรื่องต่อเนื่องหรือเกี่ยวพันกัน และความผิดเรื่องใดเรื่องหนึ่งจะต้องดำเนินการโดยพนักงานสอบสวนคดีพิเศษตามพระราชบัญญัตินี้ ให้พนักงานสอบสวนคดีพิเศษมีอำนาจสืบสวนสอบสวนสำหรับความผิดบทอื่นหรือเรื่องอื่นด้วย และให้ถือว่าคดีดังกล่าวเป็นคดีพิเศษ

บรรดาคดีใดที่ได้ทำการสอบสวนเสร็จแล้วโดยพนักงานสอบสวนคดีพิเศษ ให้ถือว่าการสอบสวนนั้นเป็นการสอบสวนในคดีพิเศษตามพระราชบัญญัตินี้แล้ว...”

ดังนั้นคดีพิเศษที่เจ้าพนักงานสอบสวนคดีพิเศษจะทำการสอบสวนได้จะต้องมีลักษณะตามที่กฎหมายบัญญัติเอาไว้ข้างต้น

โดยลักษณะพิเศษของคดีพิเศษทำให้การรวบรวมพยานหลักฐานเป็นไปอย่างยากลำบาก ทำให้การสอบสวนขาดประสิทธิภาพ พยานหลักฐานขาดความน่าเชื่อถือ ตามปกติกฎหมายจึงกำหนดให้พนักงานสอบสวนคดีพิเศษมีอำนาจพิเศษในการแสวงหาพยานหลักฐานดังกล่าวโดยการขออนุญาตต่อศาล เช่นการดักฟังวิทยุหรือโทรศัพท์ การเข้าสู่ข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์

เมื่อกฎหมายให้สิทธิแก่บุคคลหนึ่งก็ย่อมก่อให้เกิดหน้าที่แก่บุคคลอื่นในอันที่จะไม่ก้าวล่วงต่อสิทธิส่วนบุคคลนี้ และหากมีการก้าวล่วงต่อสิทธิส่วนบุคคล เจ้าของสิทธิชอบที่จะได้รับการแก้ไขเยียวยา คือ การเรียกร้องให้ชดใช้ค่าเสียหายหรือกระทำการใดๆ เพื่อทดแทนความเสียหายหรือกำหนดโทษทางอาญาแก่ผู้ที่กระทำความผิดตามบทบัญญัติของกฎหมาย

การที่เจ้าหน้าที่ของรัฐผู้มีอำนาจมีหน้าที่ในการแสวงหา สืบสวน และสอบสวนเพื่อนำตัวผู้ที่กระทำความผิดมาลงโทษ ดังนั้นการปฏิบัติหน้าที่ของเจ้าหน้าที่อาจจะเข้าไปก้าวล่วงในสิทธิส่วนบุคคลของแต่ละคนได้โดยง่าย ดังนั้น การศึกษาในส่วนที่เกี่ยวกับสิทธิส่วนบุคคลจึงเป็นเรื่องที่ไม่อาจมองข้ามไปได้ เพราะเจ้าหน้าที่ของรัฐก็ไม่ใช่บุคคลที่ได้รับการยกเว้นใดๆ จากความรับผิดในการก้าวล่วงต่อสิทธิส่วนบุคคลของผู้อื่น แม้กฎหมายจะให้อำนาจเจ้าหน้าที่ของรัฐในการใช้ดุลพินิจเพื่อเป็นมาตรการเสริมที่จะช่วยในการบังคับใช้กฎหมายให้มีประสิทธิภาพมากยิ่งขึ้น แต่การใช้ดุลพินิจของเจ้าหน้าที่ของรัฐก็เป็นอันตรายต่อสิทธิส่วนบุคคลเช่นกัน การใช้ดุลพินิจของเจ้าหน้าที่ของรัฐจึงต้องอยู่ภายใต้กฎหมาย โดยเฉพาะในเรื่องที่เกี่ยวกับชีวิตส่วนตัวของบุคคลเจ้าหน้าที่ของรัฐอาจมีความผิดฐานละเมิด ดังนั้นเจ้าหน้าที่ของรัฐจึงต้องปฏิบัติหน้าที่ด้วยความระมัดระวังมิให้ผู้อื่นได้รับความเดือดร้อนจากการละเมิดสิทธิส่วนบุคคล

กฎหมายว่าด้วยสิทธิในชีวิตส่วนตัว (Law of Privacy) ของต่างประเทศได้บัญญัติถึงการกระทำบางอย่างซึ่งถึงแม้ว่าจะไม่เป็นถึงกับเป็นการโฆษณาหมิ่นประมาท หรือทำให้บุคคลอื่นเสื่อมเสียเกียรติยศ ชื่อเสียงโดยตรง แต่ก็อาจมีลักษณะที่เป็นการล่วงละเมิดต่อสิทธิเสรีภาพในความเป็นอยู่ส่วนตัวของบุคคลอย่างเห็นได้ชัด เช่น คอยติดตามบุคคลอื่นตลอดเวลาจนก่อให้เกิดความรำคาญ หรือการเข้าตรวจสอบข้อมูลส่วนบุคคลที่บันทึกไว้ในเครื่องคอมพิวเตอร์ ซึ่งเป็นการกระทำความผิดฐานละเมิดตามหลักกฎหมายแพ่งก็ไม่ชัดเจน เพราะผู้กระทำหาได้ทำให้เกิดความเสียหายแก่ร่างกาย เกียรติยศ ชื่อเสียงของบุคคลนั้นโดยมิชอบด้วยกฎหมายไม่ แต่การกระทำดังกล่าวเป็นที่แน่นอนว่าย่อมทำให้บุคลนั้นต้องสูญเสียความเป็นอิสระส่วนตัวไป เพราะการถูกสอดแทรกหรือเกี่ยวข้องจากการกระทำของเจ้าหน้าที่ของรัฐ ซึ่งย่อมต้องขัดกับความต้องการส่วนบุคคลแน่นอน

การพิจารณาเรื่องสิทธิส่วนบุคคลในเบื้องต้น ผู้พิจารณาจะต้องคำนึงถึงอยู่เสมอว่ากฎหมายว่าด้วยสิทธิในชีวิตส่วนตัวไม่มีรูปแบบมาตรฐาน (Uniform) เช่นเดียวกับกฎหมายลักษณะอื่นๆ เพราะลักษณะที่จะถือเป็นการละเมิดสิทธิส่วนบุคคลมีความเห็นหลากหลายแตกต่างกันไปตามสภาพเศรษฐกิจ สังคม และวัฒนธรรมของแต่ละประเทศ เพราะการละเมิดสิทธิส่วนบุคคลเป็นเรื่องเกี่ยวกับความรู้สึกของแต่ละคนอันมีลักษณะทำให้เกิดความเสียหายต่อความเป็นส่วนตัวของเขา ขณะเดียวกันก็ต้องระลึกอยู่เสมอว่าคำพิพากษาหรือกฎหมายที่เกี่ยวกับสิทธิส่วนบุคคลที่มีนั้นเป็นสิ่งที่แสดงออกถึงความพยายามที่จะจุดดุลยภาพระหว่างผลประโยชน์สาธารณะกับสิทธิส่วนบุคคลให้เกิดความพอดี

สิทธิส่วนบุคคล (Right of Privacy) ในความหมายที่แคบที่สุดอาจกล่าวได้ว่า หมายถึงสิทธิที่จะอยู่โดยลำพังปราศจากการรบกวน (The right to be let alone) และเป็นสิทธิที่ได้รับการกล่าวถึงมากที่สุดในช่วงปี ค.ศ. 1980 เพราะเป็นช่วงเวลาที่ประเทศสหรัฐอเมริกาได้รับการขนานนามว่าเป็นสังคมแห่งข่าวสาร กล่าวคือ อิสระของข่าวสารที่ประชาชนหรือสื่อมวลชนจะสามารถเข้าล่วงรู้และนำออกเผยแพร่สู่สาธารณชนได้รับการยอมรับเป็นอย่างมาก ขณะเดียวกันก็เป็นเรื่องยากที่จะเก็บข้อมูลข่าวสารของแต่ละคนไว้โดยปราศจากการแทรกแซงจากเจ้าหน้าที่ของรัฐ หรือเอกชนที่ต่างมุ่งแสวงหาผลประโยชน์ในเชิงธุรกิจของตนเป็นสำคัญ[23]

แต่เนื่องจากลักษณะของการสอบสวนคดีพิเศษต่างๆ จำเป็นที่จะต้องมีระบบการตรวจสอบการใช้อำนาจหน้าที่ของเจ้าพนักงานสอบสวนคดีพิเศษและเจ้าหน้าที่ที่เกี่ยวข้อง รวมทั้งมีการประเมินผลการปฏิบัติหน้าที่เป็นระยะๆ นอกเหนือจากการมีระบบคัดสรรบุคลากรที่เข้มงวด

---

[23] Haroldd L. Nelson & Dwight L. Teeter. (1986). **Law of Mass Communication : Freedom and Control of Print and Broadcast Media** (Fifth Edition). p. 200.

และโปร่งใส เพื่อให้งานสอบสวนคดีพิเศษมีประสิทธิภาพและเป็นอีกส่วนหนึ่งของกระบวนการยุติธรรมในปัจจุบัน

2.3 การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในคดีอาญา

2.3.1 การค้นหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ การค้นเป็นมาตรการบังคับ (Zwangsmassnahme หรือ compulsory measures) ซึ่งเป็นเครื่องมือในการดำเนินคดีอาญาที่สำคัญและจำเป็นต้องมี หากขาดไปการดำเนินคดีอาญาก็ย่อมไม่อาจกระทำได้[24] โดยกำหนดให้เจ้าพนักงานของรัฐ 2 ประเภท เป็นผู้ดำเนินการค้น ได้แก่ พนักงานฝ่ายปกครอง และเจ้าพนักงานตำรวจหรือพนักงานสอบสวน ประชาชนทั่วไปไม่สามารถทำการค้นได้ไม่ว่าจะเป็นกรณีใดก็ตาม[25] และมีเหตุในการออกหมายค้นได้ตามมาตรา 69 (1) – (5)

การค้นจึงเป็นการดำเนินการของเจ้าพนักงานของรัฐที่กฎหมายอนุญาตให้เข้าไปแสวงหาพยานหลักฐานได้ตามสถานที่ต่างๆ หรือจากตัวบุคคลก็ย่อมกระทำได้ เมื่อการค้นเป็นการแสวงหาพยานหลักฐานจากสถานที่ต่างๆ หรือจากตัวบุคคล การค้นของเจ้าพนักงานย่อมเป็นการกระทำที่กระทบกระเทือนต่อสิทธิส่วนบุคคล[26] เสรีภาพในเคหสถาน[27] และสิทธิเสรีภาพในชีวิตและ ร่างกาย[28] และในกรณีที่พยานหลักฐานที่เจ้าพนักงานของรัฐแสวงหามิใช่พยานวัตถุ พยานเอกสาร หรือพยานบุคคล เช่น ข้อมูลอิเล็กทรอนิกส์ ซึ่งกฎหมายไทยมิได้มีการจัดเอาไว้ว่าเป็นพยานหลักฐานประเภทใด และยังมีข้อโต้แย้งกันอยู่ว่าจะเป็นพยานเอกสารหรือพยานวัตถุ

แต่เมื่อพิจารณาจากการแสวงหาพยานหลักฐานดังกล่าวแล้ว อาจทำได้ 2 วิธีได้แก่

(1) เป็นข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ส่วนบุคคลของบุคคลใดบุคคลหนึ่ง ไม่ว่าจะอยู่ที่ใดที่พนักงานของรัฐไม่สามารถใช้เครื่องมือใดๆ เชื่อมเข้าไปในเครื่องคอมพิวเตอร์เพื่อเรียกดูข้อมูลที่ถูกจัดเก็บไว้ในฮาร์ดดิสได้ นอกจากเข้าไปค้นในที่ที่เครื่องคอมพิวเตอร์นั้นอยู่ ซึ่งก็เป็นการบุกรุกเข้าไปในเคหสถานของผู้เป็นเจ้าของ จึงจะได้ข้อมูลที่เป็นพยานหลักฐานมา และ

(2) เป็นการจัดเก็บข้อมูลในรูปของเครือข่าย เช่นเครือข่ายในระบบ LAN (Local Area Network) เป็นระบบเครือข่ายท้องถิ่นภายในอาคารเดียวกัน หรือ ระบบ WAN (Wide Area Network) เป็นระบบเครือข่ายระยะไกลจำกัดเฉพาะกลุ่ม เช่นระบบธนาคาร ใช้เฉพาะกลุ่มธนาคาร

---

[24] คณิต ณ นคร. เล่มเดิม. หน้า 190.

[25] คนึง ฤาไชย. (2540). **กฎหมายวิธีพิจารณาความอาญา เล่ม 1** (พิมพ์ครั้งที่ 6). หน้า 252.

[26] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 34

[27] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 35

[28] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 31

และรวมถึงระบบอินเตอร์เน็ต ซึ่งเจ้าพนักงานของรัฐไม่จำต้องเข้าไปในที่รโหฐานเพื่อค้นหาพยานหลักฐาน แต่อาจใช้เครื่องมือหรือเครื่องคอมพิวเตอร์อีกเครื่องเชื่อมไปที่แม่ข่าย หรือเซิร์ฟเวอร์ (Server) เพื่อเรียกข้อมูลมาตรวจดูก็ได้

2.3.1.1 การค้นพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์ที่อยู่ในที่รโหฐาน ตามคำนิยามของคำว่า "รโหฐาน" ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 2 (13) หมายถึงสถานที่ใดๆ ซึ่งประชาชนไม่มีความชอบธรรมที่จะเข้าไปได้ หรือเป็น "ที่ส่วนตัว" (Private Place) ที่แสดงถึงเจตนาหวงกันของเจ้าของหรือผู้ครอบครอง[29] การคุ้มครองเสรีภาพในเคหสถานของบุคคลตามรัฐธรรมนูญ มาตรา 35 การที่เจ้าพนักงานของรัฐเข้าไปค้นหาข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งอยู่ในที่รโหฐานได้จะต้องเป็นกรณีที่มีกฎหมายบัญญัติไว้ และจะต้องมีหมายค้น ดังที่บัญญัติไว้ตามรัฐธรรมนูญ มาตรา 238[30] ซึ่งจะต้องมีเหตุในการออกหมายค้นตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 69 เว้นแต่เป็นกรณีที่กฎหมายบัญญัติให้มีการค้นได้โดยไม่ต้องมีหมายตามมาตรา 92[31] หากเจ้าพนักงานของรัฐทำการตรวจค้นโดยไม่มีหมาย และไม่เข้ากรณียกเว้น การค้นดังกล่าวก็เป็นการค้นที่มิชอบ เป็นเหตุให้ศาลไม่สามารถรับฟังเป็นพยานหลักฐานได้

ดังนั้นการเข้าตรวจค้นที่รโหฐานเพื่อค้นหาในเครื่องคอมพิวเตอร์ส่วนบุคคล หรือเครื่องคอมพิวเตอร์ที่เชื่อมโยงเครือข่ายในเคหสถานเดียวกันของผู้ต้องสงสัยซึ่งเป็น "สิ่งของที่ใช้ในการกระทำความผิด" เพื่อค้นหาข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นพยานหลักฐานแสดงการกระทำความผิดของผู้ต้องสงสัย เจ้าพนักงานของรัฐจำเป็นจะต้องมีหมายค้นจากศาล ในการรวบรวมพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132[32]

หากพิจารณาจากลักษณะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งสามารถทำลายแก้ไขได้ง่ายโดยใช้เวลาเพียงสั้นๆ แต่การออกหมายค้นจากศาลต้องใช้เวลาพอสมควร หากผู้ต้องสงสัยทราบว่าจะถูกค้น ก็สามารถทำลายหรือแก้ไขได้โดยง่าย ถึงแม้มีความจำเป็นเร่งด่วน จะถือเป็นเข้าเหตุยกเว้นตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92 และใช้อำนาจตามมาตรา 92 วรรคสอง ซึ่งไม่น่าจะยกเป็นเหตุยกเว้นได้ เพราะโดยหลักการค้นจะต้องมีหมาย สำหรับ

---

[29] คณิต ณ นคร. เล่มเดิม. หน้า 220.

[30] ดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 238

[31] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92

[32] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132

การค้นตามมาตรา 92 เป็นการค้นในกรณีพิเศษ จึงต้องมีกฎหมายบัญญัติเอาไว้อย่างชัดแจ้ง ประกอบกับคำวินิจฉัยของคณะกรรมการกฤษฎีกาที่ นร. 0601/618[33] ให้ความเห็นว่า

บทบัญญัติมาตรา 92 วรรคสอง แห่งประมวลกฎหมายวิธีพิจารณาความอาญาในส่วนที่บัญญัติให้พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ค้นด้วยตนเองโดยไม่ต้องมีหมายค้น ในกรณีที่อาจออกหมายค้นได้ ขัดต่อมาตรา 238 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยเป็นอันใช้บังคับมิได้...

ดังนั้น การค้นข้อมูลอิเล็กทรอนิกส์ในกฎหมายไทยปัจจุบันจึงต้องมีหมายค้น เจ้าพนักงานของรัฐจึงจะทำการค้นได้ หากเป็นการค้นโดยไม่มีหมาย ก็ถือว่าพยานหลักฐานที่ได้เป็นพยานหลักฐานที่ได้มาโดยมิชอบ ศาลไม่สามารถนำมาใช้ประกอบการพิจารณาได้

2.3.1.2 การค้นพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์โดยการเชื่อมเข้าระบบ กรณีที่เจ้าพนักงานของรัฐเข้าค้นข้อมูลอิเล็กทรอนิกส์ได้โดยไม่ต้องเข้าไปในที่รโหฐาน แต่ใช้เครื่องคอมพิวเตอร์เชื่อมจากภายนอก ไม่ว่าจะเป็นระบบ LAN, WAN หรือ อินเตอร์เน็ต ลักษณะไม่เป็นการบุกรุกตามประมวลกฎหมายอาญา เพราะไม่ได้เข้าไปยังเคหสถานของผู้อื่น แต่เป็นการละเมิดสิทธิส่วนบุคคลตามรัฐธรรมนูญ มาตรา 34 โดยถือว่าเป็นการค้นเช่นกัน การใช้อำนาจของเจ้าพนักงานของรัฐ ย่อมจะต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของประชาชนตามดังที่บัญญัติไว้ในรัฐธรรมนูญมาตรา 26

ดังนั้น การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN, WAN หรือ อินเตอร์เน็ต แม้ในกฎหมายไทยปัจจุบันยังไม่มีกฎหมายบัญญัติไว้โดยเฉพาะ แต่เมื่อพิจารณาถึงสิ่งที่กฎหมายประสงค์จะให้ความคุ้มครอง นั่นคือสิทธิส่วนบุคคล การค้นจึงต้องมีหมายค้นเช่นเดียวกับการค้นโดยทั่วไป หากเป็นการค้นโดยไม่มีหมาย ก็ถือว่าพยานหลักฐานที่ได้เป็นพยานหลักฐานที่ได้มาโดยมิชอบเช่นกัน และศาลก็ไม่สามารถนำมาใช้ประกอบการพิจารณาได้

2.3.2 การยึดและเก็บรักษาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานที่ไม่มีรูปร่าง ซึ่งจะทำการยึดอย่างเช่นพยานหลักฐานทั่วไป ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 101[34] ไม่ได้ โดยลักษณะของข้อมูลอิเล็กทรอนิกส์ การยึดสามารถกระทำได้โดยการยึดเครื่องคอมพิวเตอร์หรือเครื่องอิเล็กทรอนิกส์ที่มีข้อมูลนั้น หรือการนำฮาร์ดดิสก์ที่มีข้อมูลนั้นเสนอต่อศาล

---

[33] คำวินิจฉัยของคณะกรรมการกฤษฎีกา ตามหนังสือ สำนักงานคณะกรรมการกฤษฎีกาที่ นร. 0601/618 (2542). **วารสารอัยการนิเทศ**, 61, 1. หน้า .183-194.

[34] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 101

กรณีที่เป็นข้อมูลอิเล็กทรอนิกส์ในระบบเครือข่ายอินเตอร์เน็ต ซึ่งต้องมีการเจาะเข้าไปใน E-mail ที่มีข้อมูลส่วนตัว การจะยึดข้อมูลส่วนบุคคลดังกล่าว เจ้าพนักงานของรัฐไม่สามารถทำได้ เพราะเป็นการละเมิดสิทธิส่วนบุคคล สามารถทำได้เพียงการยึดข้อมูลที่มีการเผยแพร่ต่อสาธารณชนเพื่อนำเสนอต่อศาลเท่านั้น

ในการตรวจสอบพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ว่าเกี่ยวข้องกับการกระทำความผิดหรือไม่นั้น ลำพังเจ้าพนักงานของรัฐเองอาจไม่สามารถทำได้ ทำให้ได้ข้อมูลไม่ครบถ้วน จึงจำเป็นต้องมีผู้เชี่ยวชาญ เช่น โปรแกรมเมอร์ที่เป็นผู้เชี่ยวชาญพิเศษโดยเฉพาะเป็นผู้ช่วยเหลือเจ้าพนักงานของรัฐในการปฏิบัติหน้าที่ โดยจะทำหน้าที่เข้าสู่ข้อมูล ตรวจสอบ เก็บข้อมูลหรือพยานหลักฐานให้ครบถ้วน ตลอดจนเก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นให้อยู่ในสภาพที่สามารถใช้ประโยชน์ได้ เพราะวัสดุที่ใช้ในการเก็บรักษาข้อมูล เช่นฮาร์ดดิสก์ เป็นวัสดุที่อาจถูกทำลายได้โดยสภาพแวดล้อมทางธรรมชาติ เช่น ความชื้น ความเย็นจัด ร้อนจัด หรือสนามแม่เหล็ก ทั้งจะต้องทำหน้าที่ยืนยันต่อศาลว่าข้อมูลอิเล็กทรอนิกส์ที่นำเสนอต่อศาลเป็นข้อมูลที่ได้ทำการยึดมา ลักษณะจึงเหมือนกับเป็นพยานผู้เชี่ยวชาญ ผู้ที่จะทำหน้าที่ตรวจสอบพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์อย่างเป็นกลาง และทำหน้าที่เก็บรักษา แต่ขณะนี้ยังไม่มีผู้ที่จะทำหน้าที่ดังกล่าวได้ เพราะไม่มีกฎหมายกำหนดให้มี จึงยังเป็นหน้าที่ของเจ้าพนักงานของรัฐโดยทั่วๆไป ซึ่งไม่ใช่ผู้ที่มีความรู้ความสามารถโดยเฉพาะ

โดยสรุปการตรวจค้น และการยึดข้อมูลอิเล็กทรอนิกส์ เพื่อนำมาเป็นพยานหลักฐานในอาชญากรรมคอมพิวเตอร์นั้น ไม่อาจกระทำได้หากไม่มีหมายค้น บางกรณีก็ไม่สามารถทำได้อย่างทันท่วงที เป็นปัญหาในเรื่องของอำนาจของเจ้าพนักงานของรัฐที่ยังไม่มีกฎหมายให้อำนาจเอาไว้โดยเฉพาะ ตลอดจนการตรวจสอบและการเก็บรักษา ก็ยังต้องใช้วิธีการตามที่บัญญัติเอาไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาเท่านั้น ซึ่งไม่เพียงพอแล้วกับสังคมในปัจจุบัน

บทที่ 3
การเข้าถึงข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในกฎหมายต่างประเทศ

ในบทที่แล้วได้กล่าวถึงความหมาย ลักษณะ และสภาพปัญหาของการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมทางคอมพิวเตอร์รูปแบบต่างๆดังที่ได้กล่าวมาแล้ว ซึ่งปัญหาอาชญากรรมคอมพิวเตอร์นี้ก็มิใช่ว่าจะเกิดแต่เฉพาะในประเทศไทยเท่านั้น แต่ยังส่งผลกระทบต่อกฎหมายอาญาของประเทศอื่นๆ ด้วย ดังนั้นในบทนี้จะกล่าวถึงแนวความคิดในการบัญญัติกฎหมายเพื่อรักษาความปลอดภัยของข้อมูล สภาพปัญหาเกี่ยวกับการปราบปรามอาชญากรรมคอมพิวเตอร์ และมาตรการทางกฎหมายและปัญหาเกี่ยวกับการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์ของประเทศต่างๆ ได้แก่ ประเทศสหรัฐอเมริกา อังกฤษ และญี่ปุ่น โดยการศึกษาถึงแนวความคิด เหตุผล ขั้นตอน วิธีการ และระยะเวลาในการค้น และการรับฟังเป็นพยานหลักฐานในศาลของประเทศต่างๆ เพื่อเป็นแนวทางในการแก้ปัญหาที่เกิดขึ้นในกฎหมายไทยต่อไป

3.1 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาเป็นประเทศหนึ่งที่มีความเจริญก้าวหน้าทางเทคโนโลยีในหลายๆด้าน และมีกฎหมายที่จะใช้ดำเนินคดีกับอาชญากรรมคอมพิวเตอร์มากกว่า 40 ฉบับ เช่น National Stolen Property Act , Copyright Act ฯลฯ จึงต้องพิจารณาว่ากฎหมายที่มีอยู่ทั้ง 40 ฉบับนั้น สามารถนำมาใช้บังคับและครอบคลุมความผิดอาญาเกี่ยวกับคอมพิวเตอร์ได้มากน้อยเพียงใด สำหรับความผิดเกี่ยวกับคอมพิวเตอร์สหรัฐเองก็มีการบัญญัติกฎหมายตั้งแต่ปี ค.ศ. 1984 คือ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA) ซึ่งแบ่งความผิดเกี่ยวกับคอมพิวเตอร์เป็น 3 ลักษณะ ได้แก่

ก. Subsection 1030 (a) (1) ความผิดที่ก่อความเสียหายแก่ความมั่นคงของรัฐโดยตรง

ข. Subsection 1030 (a) (2) ความผิดที่ก่อให้เกิดความเสียหายต่อระบบความเชื่อถือส่วนบุคคลที่มีในสถาบันการเงิน หรือหน่วยงานที่ทำหน้าที่ดูแลประวัติ และผู้บริโภค

ค. Su bsection 1030 (a) (3) ความผิดที่กระทำต่อข้อมูลข่าวสารของเครื่องคอมพิวเตอร์อันก่อให้เกิดความเสียหายต่อรัฐบาลสหรัฐ[1]

และมีการแก้ไขเพิ่มเติมในปี 1988 และ 1990 ตามลำดับเพื่อให้ครอบคลุมความผิดที่เกิดขึ้น สภาคองเกรสได้มีมติให้ออกกฎหมาย The National Information Infrastructure Protection Act of 1996 (NIIPA) [2] และเพิ่มเติมการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ใน U.S. Code title 18 มาตรา 1030 (18 U.S.C.A. section 1030)[3] สำหรับกฎหมายของมลรัฐต่างๆ เริ่มมีใน ค.ศ. 1987 โดยเริ่มมีที่มลรัฐอริโซน่า และมลรัฐฟลอริดา และหลังจากถูกกลุ่มผู้ก่อการร้ายโจมตีตึกเพนทากอนและอาคารเวิลด์เทรดเซ็นเตอร์ เมื่อวันที่ 11 กันยายน ค.ศ. 2001 จึงให้ความสำคัญกับการรักษาความปลอดภัยและความเป็นส่วนตัวกันมากขึ้น และได้จัดสรรเงินเพื่อแก้ปัญหาอาชญากรรม โดยเฉพาะในส่วนที่เกี่ยวกับความปลอดภัยในเครือข่ายคอมพิวเตอร์ (Cyber-security) และการวิจัยเกี่ยวกับการก่อการร้ายในเครือข่ายคอมพิวเตอร์ (Cyber-terrorism) [4]

3.1.1 มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา ประเทศสหรัฐอเมริกาเป็นประเทศแรกที่ประกาศใช้กฎหมายจำกัดการใช้อินเตอร์เน็ตเพื่อความบันเทิงทางเพศ คือกฎหมายควบคุมสื่อลามกและข้อความที่ไม่สมควรทางเพศบนอินเตอร์เน็ต (Communications Decency Act 1996 : CDA.) ซึ่งมีเนื้อหากำกับสิ่งที่ให้บริการทางอินเตอร์เน็ตโดยเฉพาะ โดยกำหนดให้บุคคลที่ส่งภาพหรือข้อความลามกอนาจารหรือไม่เหมาะสมขัดต่อศีลธรรมอันดี แก่ผู้เยาว์อายุต่ำกว่า 18 ปี มีความผิดต้องรับโทษปรับหรือจำคุกไม่เกิน 2 ปี [5] และถ้าผู้ใดอนุญาตให้ผู้เยาว์อายุต่ำกว่า 18 ปี ใช้อินเตอร์เน็ตหรือสถานที่เพื่อการดังกล่าวย่อมมีความผิดด้วย[6] จะเห็นได้ว่ากฎหมายฉบับนี้จำกัดสิทธิเสรีภาพและความเป็นส่วนตัวของบุคคล เมื่อกฎหมายฉบับนี้ใช้บังคับในวันที่ 8 กุมภาพันธ์ 1996 สมาคมสิทธิทางแพ่งของสหรัฐอเมริกัน (ACLU) และ

---

[1] นิติ ผดุงชัย. (2532,มิถุนายน). “กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับ Computer.” **วารสารอัยการ**. หน้า 86-88.

[2] Michael Hatcher , Jay Mc Danell , and Stacy Ostfeld. (1999). “Computer Crimes.” **American Criminal Law Review**. 36 : p.402.

[3] Ibid.p.401.

[4] “The Governance Challenge : Creating a smart and Secure Cyberspace,” Madanmohan Rao report from the ‘New Directions in Internet Policy’ conference in Atlanta, <http://www.indiainfoline.com/nevi/inwi/mm66.html.>,2002.

[5] CDA, Section 223.

[6] CDA, Section 223 (a) (2).

สมาคมห้องสมุด (ALA) ได้ยื่นฟ้องต่อศาลขอประกาศว่ากฎหมายฉบับนี้ขัดต่อรัฐธรรมนูญว่าด้วยการคุ้มครองเสรีภาพในการแสดงออก และสิทธิความเป็นส่วนตัว ตามบทแก้ไขเพิ่มเติมฉบับที่ 1 (First Amendment) และรัฐบาลสหรัฐอเมริกาก็ได้โต้แย้งว่ากฎหมายฉบับนี้บังคับใช้แต่เฉพาะบุคคลที่ไม่สุจริตและรู้ว่าผู้เยาว์ใช้บริการในสถานที่ของตน และยกเว้นบุคคลที่ไม่รู้ว่าข้อความที่ผ่านคอมพิวเตอร์ของตนนั้นเป็นข้อความหรือภาพลามก การจำกัดเสรีภาพจะกระทำต่อเด็กและเยาวชนเท่านั้น ไม่รวมถึงบุคคลทั่วไป แต่ในที่สุดศาลก็ตัดสินให้ระงับใช้กฎหมายฉบับนี้เพราะอาจจะขัดต่อรัฐธรรมนูญ [7]

3.1.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ ในปี ค.ศ. 1986 สภาคองเกรสของสหรัฐอเมริกาได้ออก The Computer Fraud and Abuse Act of 1986 ซึ่งกฎหมายฉบับนี้มีบทบัญญัติที่เปลี่ยนแปลงไปจากกฎหมายที่มีอยู่เดิม ได้แก่

3.1.2.1 ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access)

3.1.2.2 ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration)

3.1.2.3 ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction)

3.1.2.1 ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access) ความผิดฐานเข้าถึงโดยปราศจากอำนาจเป็นความผิดฐานหนึ่ง ที่เป็นการฉ้อโกงหรือกระทำการใดๆ ต่อเครื่องคอมพิวเตอร์โดยเจตนา เป็นการกระทำโดยปราศจากอำนาจ หรือกระทำเกินกว่าอำนาจที่มีอยู่ ได้แก่

(1) เข้าสู่ระบบคอมพิวเตอร์โดยรู้ว่าไม่มีอำนาจ และได้ไปซึ่งข้อมูลนั้น โดยมีเหตุเชื่อได้ว่าข้อมูลนั้นอาจถูกใช้ไปเพื่อการอันเป็นภัยต่อความมั่นคงของประเทศ หรือเพื่อประโยชน์ของชาติอื่น ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 20 ปี

(2) เข้าสู่ระบบคอมพิวเตอร์โดยรู้ว่าไม่มีอำนาจ และได้ไปซึ่งข้อมูลทางการเงินหรือข้อมูลของสถาบันการเงิน ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(3) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ และปลอมแปลงหรือแสร้งว่าเป็นเจ้าหน้าที่ของรัฐเพื่อเปิดระบบประมวลผล ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

---

[7] เลอสรร ธนสุกาญจน์และคณะ. (2541). **กฎหมายสำหรับบริการอินเตอร์เน็ตในประเทศไทย กรอบ ข้อเสนอแนะ และการควบคุมดูแล การให้บริการ**. หน้า 154.

(4) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ เพื่อผลประโยชน์ใดๆ ด้วยเจตนาฉ้อโกงหรือได้ไปซึ่งสิ่งมีค่าใดๆ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(5) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ และได้แก้ไขเปลี่ยนแปลงหรือทำลายข้อมูลที่ได้เข้าถึงนั้นเพื่อผลประโยชน์ใดๆ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(6) รู้และใช้รหัสผ่านโดยปราศจากอำนาจเพื่อเข้าถึงข้อมูลในคอมพิวเตอร์ของรัฐบาลเพื่อการค้าระหว่างรัฐหรือการค้าระหว่างประเทศ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

นอกจากความผิดข้างต้นแล้ว การเข้าถึงข้อมูลในคอมพิวเตอร์โดยปราศจากอำนาจสหรัฐอเมริกาถือเป็นการกระทำที่มิชอบเกี่ยวข้องกับกฎหมายอื่นๆอีก ดังนี้

(1) ประมวลกฎหมายอาญาสหรัฐอเมริกา เนื่องจากการเข้าถึงข้อมูลในคอมพิวเตอร์ถือเป็นการลักขโมยบริการ (Theft of Service) เพราะเป็นการใช้บริการโดยไม่มีอำนาจ แม้ในบางครั้งจะไม่ก่อให้เกิดความเสียหายก็ตาม แต่กฎหมายก็ถือว่ามีความผิด โดยถือว่าเป็นความเสี่ยงต่อการก่อให้เกิดความเสียหายต่อสารสนเทศได้และผู้กระทำย่อมรู้ตัวดี และความเสียหายจะเกิดขึ้นในอนาคต[8] เพราะว่าในการเข้าถึงโดยปราศจากอำนาจ อาจทำให้เจ้าของที่แท้จริงไม่สามารถเข้าสู่ระบบได้ จึงมีการบัญญัติกฎหมายนี้ขึ้นเพื่อคุ้มครองผู้เช่าหรือผู้มีอำนาจใช้สายสื่อสารที่ต่อเชื่อมกับระบบคอมพิวเตอร์ และกรณีของพนักงานของบริษัทที่ใช้คอมพิวเตอร์ทำงานส่วนตัวหรือคัดลอกทำสำเนาข้อมูลโดยไม่ได้รับความยินยอมจากนายจ้าง ที่เรียกว่า “การทำงานกลางคืน” (Moonlight) ก็เป็นการกระทำที่ปราศจากอำนาจ ถือเป็นการลักสิ่งที่มีค่าใดๆ (Thing of Value) อันเป็นความผิดฐานลักทรัพย์ และการกระทำดังกล่าวยังเข้าลักษณะความผิดฐานปลอมแปลงเอกสารและความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญาด้วย ซึ่งจะเห็นได้ว่ามีกฎหมายมากกว่า40 มาตราในบรรพที่ 8 ประมวลกฎหมายอาญาสหรัฐอเมริกาที่บัญญัติถึงการใช้เครื่องคอมพิวเตอร์ในการกระทำความผิดไม่ว่าโดยตรงหรือโดยอ้อม

(2) กฎหมายการสื่อสารทางอิเล็กทรอนิกส์ส่วนบุคคล (The Electronic Communication Privacy Act of 1986) กฎหมายฉบับนี้เป็นกฎหมายที่รับประกันการสื่อสารระหว่างบุคคลที่ผ่านทางโทรศัพท์ในระบบต่างๆ คลื่นวิทยุ การสื่อสารผ่านดาวเทียม และการสื่อสารผ่านทางเครือข่าย

---

[8] สุเนติ คงเทพ . (2541). **เอกสารประกอบการสัมมนาแนวทางในการแก้ปัญหากฎหมายอาชญากรรมยุคไอที เรื่องการไม่มีอำนาจเข้าสู่ระบบประมวลผล**. หน้า 16.

คอมพิวเตอร์ ไปรษณีย์อิเล็กทรอนิกส์ สาระสำคัญของกฎหมายฉบับนี้ คือ คำนิยามและข้อยกเว้นการจำกัดการสื่อสารของภาคเอกชน การเก็บรักษาและการใช้ข้อมูลจากการสื่อสาร การรับจดทะเบียน ฯลฯ

(3) กฎหมายการฉ้อโกงบัตรเครดิต (The Credit Card Fraud Act of 1984) เป็นกฎหมายที่ออกมาเพื่อควบคุมการฉ้อโกงบัตรเครดิตและการปลอมบัตรเครดิต แต่คำนิยามของคำว่า "บัตรเครดิต" ในกฎหมายฉบับนี้ได้ครอบคลุมไปถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ด้วย เช่น การกระทำความผิดที่เข้าถึงสื่อทางคอมพิวเตอร์ หมายความรวมถึงบัตรต่างๆ แผ่นพลาสติก รหัส หมายเลขบัญชี หรือสิ่งอื่นๆของบัญชี และการเข้าถึงให้หมายความถึงการเข้าถึงทางด้านบัญชีและการเข้าถึงสื่อทางคอมพิวเตอร์ อันถือเป็นการกระทำที่ได้ไปซึ่งผลประโยชน์ในด้านต่างๆ ส่วนที่กล่าวถึงการกระทำความผิดเกี่ยวกับเครื่องคอมพิวเตอร์นั้น เป็นการกระทำความผิดฐานฉ้อโกงการทำ ใช้ จำหน่าย ปลอมสื่อทางคอมพิวเตอร์ หรือการเข้าถึงโดยปราศจากอำนาจ ลักษณะของการกระทำความผิดตามกฎหมายฉบับนี้ที่เกิดขึ้นในปัจจุบัน ได้แก่ การลักลอบเข้าสู่ระบบคอมพิวเตอร์เพื่อค้นหา ทดสอบ หรือการแก้ไขเปลี่ยนแปลงข้อมูลต่างๆ เช่น หมายเลขโทรศัพท์ หมายเลขบัญชีธนาคาร หรือรหัสผ่าน

(4) กฎหมายลิขสิทธิ์ (The Copyright Act of 1976) กรณีที่มีการเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์โดยปราศจากอำนาจในลักษณะที่เป็นการลักขโมยโปรแกรมหรือข้อมูลในคอมพิวเตอร์นั้น ถือเป็นการละเมิดลิขสิทธิ์ที่มีโทษทางอาญา ตามรายงานของคณะกรรมาธิการรัฐสภาเกี่ยวกับกฎหมายลิขสิทธิ์ ค.ศ. 1976 หน้า 54 ระบุว่า "งานวรรณกรรม" (Literary Works) ให้รวมถึงฐานข้อมูลทางคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ รวมถึงงานประพันธ์ที่เป็นการแสดงออกถึงความคิดดั้งเดิมของนักเขียนโปรแกรม จึงเป็นสิทธิของผู้เขียนโปรแกรมที่จะปกป้องเอกสารและลายเส้นของรหัสคอมพิวเตอร์จากการคัดลอกหรือทำสำเนา แต่การคุ้มครองดังกล่าวก็มิได้ครอบคลุมถึง "ขั้นตอนวิธี" (Algorithms) ของผู้เขียนโปรแกรมด้วย การกระทำความผิดตามกฎหมายฉบับนี้มีโทษทั้งทางแพ่งและในทางอาญา

(5) กฎหมายการฉ้อโกงทางสายโทรศัพท์ (The Wire Fraud Act) เดิมประมวลกฎหมายสหรัฐอเมริกา มีการยกเว้นการกระทำความผิดทางสายสื่อสารสาธารณะ แต่เมื่อมีการใช้คอมพิวเตอร์จากเครือข่ายทางไกลกระทำการฉ้อโกงทางคอมพิวเตอร์ขึ้นเป็นจำนวนมาก ทั้งเป็นการกระทำความผิดของบุคคลเพียงคนเดียวและหลายคนร่วมมือกัน และผู้ที่กระทำความผิดก็ได้ผลประโยชน์ไปเป็นจำนวนมาก รัฐจึงมีมาตรการออกมาเพื่อปกป้องคุ้มครองการส่งข้อมูลผ่านทางสายสื่อสารสาธารณะดังกล่าว

(6) กฎหมายเกี่ยวกับระเบียบสถาบันทางการเงินและการควบคุมอัตราดอกเบี้ย (The Financial Institutions Regulatory and Interest rate Control Act of 1978 : FIRA) ในส่วนที่เป็นเรื่องการโอนเงินทางอิเล็กทรอนิกส์ (The Electronic Fund Transfer Act) ซึ่งมีการกำหนดคำนิยามและสิทธิส่วนบุคคลของผู้บริโภคที่ได้รับผลกระทบจากการโอนเงินทางอิเล็กทรอนิกส์ โดยกฎหมายฉบับนี้ได้กำหนดให้รัฐบาลกลางออกระเบียบการโอนเงินทางอิเล็กทรอนิกส์ขึ้น

(7) กฎหมายคุ้มครองส่วนบุคคล (The Privacy Act of 1974) กรณีที่เป็นการเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจที่จะกระทำได้ โดยกระทำผ่านฐานข้อมูลในเครื่องคอมพิวเตอร์ เป็นการให้ความคุ้มครองความเป็นส่วนตัวของบุคคล ดังนั้นการเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์โดยปราศจากอำนาจจึงอาจมีความผิดตามกฎหมายฉบับนี้ด้วย

3.1.2.2 ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration) ความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูลตาม The Computer Fraud and Abuse Act 1986 ครอบคลุมถึงการแก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ และข้อมูลที่ถูกจัดเก็บอยู่ในคอมพิวเตอร์ เหตุที่นำความผิดดังกล่าวมาบัญญัติเอาไว้ต่างหาก เนื่องมาจากการกระทำความผิดดังกล่าวมีลักษณะคล้ายกับความผิดฐานปลอมแปลงเอกสาร แต่เมื่อมีการกระทำความผิดเกิดขึ้นกลับไม่สามารถนำบทบัญญัติของกฎหมายในความผิดฐานปลอมแปลงเอกสารมาใช้บังคับได้ เพราะประสบปัญหาการตีความ โดยเฉพาะเรื่องขององค์ประกอบของความผิด ฝ่ายนิติบัญญัติของรัฐบาลกลางและมลรัฐต่างๆ จึงจำเป็นที่จะต้องบัญญัติกฎหมายขึ้นมาใช้บังคับกับความผิดดังกล่าวโดยเฉพาะ

การกระทำที่เป็นการแก้ไขเปลี่ยนแปลงโปรแกรมคอมพิวเตอร์หรือการแก้ไขเปลี่ยนแปลงข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์ ในส่วนที่เกี่ยวกับความผิดฐานปลอมเอกสารนั้นตีความจากคำว่า “เอกสาร” ที่หมายความรวมถึงโปรแกรมคอมพิวเตอร์และข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์

3.1.2.3 ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction) ความผิดฐานทำให้เสียหายหรือทำลายทางคอมพิวเตอร์ตาม The Computer Fraud and Abuse Act 1986 นั้น เป็นการกระทำที่ทำให้เกิดความเสียหายหรือทำลายโปรแกรมคอมพิวเตอร์หรือข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์และการกระทำให้เกิดความเสียหายโดยตรงต่อเครื่องคอมพิวเตอร์รวมทั้งอุปกรณ์ต่างๆของเครื่องคอมพิวเตอร์ที่เรียกว่าฮาร์ดแวร์ (Hardware) ด้วย โดยบัญญัติแยกต่างหากจากความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญา เนื่องจากเห็นว่าเป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายที่ร้ายแรง และก่อให้เกิดความเสียหายต่อเทคโนโลยี

3.1.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ การค้นข้อมูลอิเล็กทรอนิกส์เป็นการค้นที่แตกต่างจากการค้นที่มีอยู่แต่เดิม ซึ่งเมื่อพนักงานสอบสวนเห็นสมควรจะค้นจะต้องมีหมายค้น โดยจะต้องบรรยายสถานที่ที่จะทำการค้นในหมายนั้นด้วย แต่สำหรับการค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์จะต้องทำการค้นหาจากฮาร์ดแวร์หรือฮาร์ดดิสก์

ในการปฏิบัติหน้าที่ของพนักงานสอบสวนของสหรัฐอเมริกาจะต้องเป็นการค้นหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์โดยไม่ขัดต่อหลักการไม่รับฟังพยานหลักฐาน ซึ่งได้มาโดยการค้นที่มิชอบ (Exclusionary Rule) ตามรัฐธรรมนูญสหรัฐอเมริกาแก้ไขเพิ่มเติมฉบับที่ 4 (The Fourth Amendment) บัญญัติว่า "สิทธิของบุคคลที่จะมีความปลอดภัยมั่นคงในร่างกาย เคหสถาน เอกสารและวัตถุสิ่งของ ต่อการค้น การยึด และการจับที่ไม่มีเหตุอันสมควร จะถูกล่วงละเมิดมิได้ และห้ามมิให้มีการออกหมาย เว้นแต่จะโดยมีเหตุอันควร ซึ่งได้มาโดยการสาบาน หรือปฏิญาณตน และหมายนั้นจะต้องระบุเฉพาะเจาะจงถึงสถานที่ที่จะถูกค้น ตัวบุคคลที่จะถูกจับ และสิ่งของที่ถูกยึด"

นอกจากนี้กฎว่าด้วยวิธีพิจารณาความอาญาของสหรัฐได้รับรองหลักของรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่นี้ไว้ในมาตรา 41 (a) ซึ่งบัญญัติว่า "เจ้าพนักงานผู้มีอำนาจหรือพนักงานอัยการต้องขอหมายค้น…

(1) หมายค้นต้องออกโดยศาล Magistrate ของมลรัฐ หรือศาลของสหรัฐ สำหรับการค้นสิ่งของหรือค้นหาบุคคลในเขตอำนาจศาล

(2) หมายค้นออกโดยศาล Magistrate สำหรับกรณีการค้นสิ่งของหรือค้นหาบุคคลในเขตอำนาจศาลหรือค้นสิ่งของที่ถูกโยกย้ายหรือบุคคลหลบหนีออกนอกเขตก่อนจะถูกดำเนินการตามกฎหมาย"

จากกฎหมายดังกล่าวจะเห็นได้ว่าเจ้าหน้าที่ของรัฐจะทำการค้นได้ก็ต่อเมื่อมีหมายค้น และหมายค้นดังกล่าวจะต้องออกโดยผู้พิพากษา แม้ในกรณีของการค้นข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นพยานหลักฐานที่มีลักษณะพิเศษ ที่อาจถูกแก้ไขเปลี่ยนแปลงได้ง่าย เจ้าพนักงานของรัฐก็จะต้องทำการค้นโดยมีหมาย เพราะต้องการจะให้กระบวนการในการออกหมายเป็นมาตรการในการตรวจสอบการใช้ดุลพินิจของเจ้าหน้าที่ (Warrant Process) เพื่อให้เจ้าหน้าที่ปฏิบัติหน้าที่โดยไม่ขัดกับรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 4

ในกรณีที่เจ้าหน้าที่ไม่จำเป็นที่จะต้องเข้าไปค้นในเคหสถานหรือสำนักงานของผู้อื่น แต่สามารถทำการค้นโดยการใช้เครื่องคอมพิวเตอร์หรือเครื่องมืออื่นใดเชื่อมต่อเข้ากับระบบ LAN หรือ WAN ของเคหสถาน หรือสำนักงาน ตลอดจนเครือข่ายอินเตอร์เน็ต โดยไม่มีการบุกรุกเข้าไปทางกายภาพ หากพิจารณาถึงสิทธิที่ได้รับการรับรองคุ้มครองตามรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่

DPU

4 ซึ่งรวมไปถึงสิทธิส่วนบุคคลด้วย การค้นข้อมูลอิเล็กทรอนิกส์ในลักษณะนี้ ก็ถือเป็นการบุกรุกเช่นกัน

3.1.4 การรับฟังเป็นพยานหลักฐานในศาล ภายหลังที่กฎหมายอาชญากรรมคอมพิวเตอร์ในสหรัฐอเมริกาใช้บังคับแล้วยังมีปัญหาที่ตามมาอีกหลายประการ เช่น ปัญหาในการให้คำนิยามคำว่า "อาชญากรรมคอมพิวเตอร์" (Computer crime) การจำกัดการให้ความคุ้มครองที่จำกัดเฉพาะงานของรัฐไม่รวมภาคเอกชน การขาดความชัดเจนในเรื่องของเขตอำนาจศาล และปัญหาเกี่ยวกับวิธีพิจารณาความ เช่น การแสวงหาพยานหลักฐาน และการรับฟังเป็นพยานหลักฐานในศาล ทำให้ไม่สามารถนำผู้กระทำผิดมาลงโทษได้

ศาลของสหรัฐอเมริกาจะไม่รับฟังพยานหลักฐานที่เกิดจากการค้นโดยมิชอบ ดังนั้นในการค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ก็จะต้องเป็นการค้นที่ไม่ขัดต่อหลักการห้ามรับฟังพยานหลักฐานซึ่งได้มาโดยมิชอบ (Exclusionary Rule) ดังนั้นหากเจ้าหน้าที่แสวงหาพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์โดยวิธีการที่มิชอบด้วยกฎหมาย เป็นการล่วงล้ำสิทธิส่วนบุคคล พยานหลักฐานดังกล่าวก็จะถูกตัดออกจากกระบวนการพิจารณาของศาลทันที โดยศาลจะไม่รับฟัง ทำให้ไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้

3.2 ประเทศอังกฤษ

ก่อนที่จะมีกฎหมายอาญาว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือการรักษาความปลอดภัยของข้อมูลในคอมพิวเตอร์นั้น การเข้าถึงข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ในประเทศอังกฤษโดยปราศจากอำนาจไม่ถือเป็นความผิดอาญา โดยพิจารณาเปรียบเทียบจากความผิดฐานบุกรุก (Trespass) ความผิดเกี่ยวกับทรัพย์ (Theft) ที่ผู้กระทำผิดรับผิดแต่เพียงในทางแพ่ง [9] ต่อมาจึงได้บัญญัติ The Computer Misuse Act 1990 เป็นกฎหมายอาญาว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ขึ้นเป็นฉบับแรก ทั้งได้วางมาตรการในการรักษาความปลอดภัยของข้อมูลเอาไว้ด้วย

3.2.1 มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศอังกฤษ วัฒนธรรมของประเทศอังกฤษนั้นให้ความเคารพต่อสิทธิส่วนบุคคล โดยมีคดีตัวอย่างเกี่ยวกับนายจ้างและลูกจ้างที่ศาลตัดสินว่านายจ้างไม่อาจเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง ไม่ว่าข้อมูลนั้นจะเก็บไว้

---

[9] เฉลิมพล ช่อโพธิ์ทอง. (2535). **ความผิดฐานลักทรัพย์และฉ้อโกง : ศึกษาเปรียบเทียบกฎหมายอังกฤษ เยอรมัน และไทย**. หน้า 73.

ในระบบธรรมดาหรือเก็บไว้ในคอมพิวเตอร์ก็ตาม[10] ต่อมารัฐบาลอังกฤษได้พิจารณาถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ว่าควรจะมีกฎหมายคุ้มครอง เพราะจำเป็นต้องดำเนินการให้กฎหมายภายในของอังกฤษสอดคล้องกับอนุสัญญาแห่งสภายุโรปว่าด้วยการให้ความคุ้มครองข้อมูล (The Council of Europe's Data Protection) รัฐสภาของประเทศอังกฤษได้ออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (The Data Protection Act 1984 แก้ไขเพิ่มเติม ค.ศ. 1998) เพราะในการแสวงหาพยานหลักฐานของเจ้าพนักงานของรัฐ โดยล่วงล้ำเข้าไปรับรู้ถึงข้อมูลที่เกี่ยวกับการดำเนินชีวิตของผู้ต้องสงสัยหรือสารสนเทศที่อยู่ในความครอบครองของผู้ใช้ และการแสดงความคิดเห็นส่วนตัว เท่ากับเป็นการล่วงล้ำข้อมูลส่วนบุคคลที่กฎหมายอังกฤษประสงค์จะให้ปกปิด ดังเช่นคดีระหว่างนายจ้างและลูกจ้างข้างต้น การรวบรวมพยานหลักฐานด้วยวิธีการดังกล่าวอาจถูกหาว่าเป็นพยานหลักฐานที่ได้มาโดยมิชอบได้

3.2.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของอังกฤษ คือ The Data Protection Act 1998 และมีมาตรการควบคุม และตรวจสอบการทำงานของเจ้าหน้าที่โดยองค์กรภายนอกไว้อย่างรัดกุม และไม่ทำให้ประสิทธิภาพในการปราบปรามอาชญากรรมของเจ้าหน้าที่ลดลง โดยการให้ดุลพินิจในการปฏิบัติหน้าที่ของเจ้าหน้าที่ ภายใต้กฎเกณฑ์ที่กฎหมายบัญญัติไว้ใน The Police and Criminal Evidence Act 1984

กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ของอังกฤษ คือ The Computer Misuse Act 1990 ที่กำหนดความผิดไว้ 3 รูปแบบ ได้แก่

3.2.2.1 ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access)

3.2.2.2 ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง (Ulterial Hacking Offence หรือ Unauthorized Access with Intent to Commit or Facilitate Commission of Further Offences) และ

3.2.2.3 ความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ (Modification of Computer Material หรือ Unauthorized Modification)

---

[10] Edward Wilding. (1997). **Computer Evidence : A Forensic Investigations Handbook**. London : Sweet & Maxwell Ltd. p.93.

3.2.2.1 ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access) ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 1 บัญญัติว่า

(1) บุคคลจะมีความผิดเมื่อ

(a) บุคคลได้กระทำการให้คอมพิวเตอร์แสดงผล หรือแสดงการทำงานใดๆ ด้วยเจตนาที่จะผ่านสิ่งป้องกันที่มีไว้เพื่อกันการเข้าถึงระบบ และได้ทำการผ่านสิ่งป้องกันเช่นว่านั้นเข้าถึงโปรแกรมคอมพิวเตอร์ใดๆ หรือสารสนเทศที่เก็บไว้ในคอมพิวเตอร์ใดๆ

(b) การผ่านสิ่งป้องกันเข้าไปยังระบบนั้น เป็นการกระทำโดยปราศจากอำนาจ

(c) บุคคลนั้นได้รู้ขณะที่กระทำอยู่แล้วว่า การกระทำอันเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการกระทำนั้นปราศจากอำนาจ

(2) เจตนาของบุคคลที่ได้กระทำความผิดภายใต้มาตรานี้ ไม่จำเป็นต้องเป็นการกระทำที่เป็น

(a) โปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล

(b) โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือ

(c) โปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ

(3) บุคคลที่มีความผิดภายใต้บทบัญญัตินี้ จะต้องถูกพิจารณาคดีแบบรวดรัดและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

จากบทบัญญัติข้างต้นเป็นบทบัญญัติที่ไม่มีความซับซ้อน แสดงถึงการเข้าถึงข้อมูลโดยปราศจากอำนาจ แต่จะเป็นการกระทำที่มีความผิดตามมาตรานี้จะต้องเป็นการทำให้เครื่องคอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ รวมทั้งการสั่งให้เครื่องคอมพิวเตอร์แสดงการทำงานโดยระยะทางไกล (Remote) โดยไม่คำนึงถึงผลของการกระทำ ซึ่งรวมถึงการพยายามกระทำความผิดด้วย แต่ไม่รวมถึงการทำงานทางกายภาพที่กระทำต่อเครื่องหรืออุปกรณ์คอมพิวเตอร์

หากพิจารณาความรับผิดทางอาญาในระบบคอมมอนลอว์ สำหรับความผิดฐานเข้าถึงโดยปราศจากอำนาจ สามารถแยกพิจารณาได้เป็น 2 ส่วน ได้แก่

ก. ส่วนของการกระทำ (Actus Reus) คือการที่ผู้ใดกระทำการอย่างหนึ่งอย่างใดเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ และผู้กระทำต้องรับผิดแม้จะไม่สำเร็จ ทั้งนี้ไม่รวมถึงการกระทำที่เพียงแต่สัมผัสทางกายกับอุปกรณ์หรือเครื่องคอมพิวเตอร์โดยไม่มีการกระทำใดๆต่อเครื่องคอมพิวเตอร์ และการดูข้อมูลที่ปรากฏบนจอภาพ การดักข้อมูล หรือการดักฟังข้อมูล

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) แยกพิจารณาได้ดังนี้

(1) เจตนาที่จะผ่านสิ่งป้องกันที่มีเพื่อเข้าสู่ระบบ เพื่อเข้าสู่ข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ใดๆก็เป็นความผิดแล้ว ไม่จำเป็นจะต้องเป็นเจตนาโดยตรงต่อโปรแกรมหรือข้อมูลใดๆ ตามที่บัญญัติใน (2) แสดงให้เห็นว่าเจตนาของผู้กระทำไม่จำเป็นจะต้องเป็นเจตนาโดยตรงต่อโปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือโปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ ดังนั้น การกระทำโดยประมาทก็อาจมีความผิดตามมาตรานี้ได้

(2) เจตนาภายใน คือผู้กระทำต้องรู้ในขณะที่กระทำว่าตนไม่มีอำนาจที่จะกระทำได้ เป็นการทำให้เครื่องคอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ โดยปราศจากอำนาจ

ดังนั้นในการฟ้องร้องผู้กระทำความผิด โจทก์จะต้องพิสูจน์ให้ศาลเห็นว่าจำเลยมีเจตนาเข้าสู่ระบบและจำเลยรู้ว่าการกระทำของตนเป็นการทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ และเป็นการกระทำโดยปราศจากอำนาจ การพิสูจน์องค์ประกอบภายในทั้ง 2 ประการข้างต้นนี้ถือเป็นหลักในการพิสูจน์ความผิดของผู้กระทำความผิดตามหลักพื้นฐานของคอมมอนลอว์

3.2.2.2 ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง (Ulterial Hacking Offence หรือ Unauthorized Access with Intent to Commit or Facilitate Commission of Further Offences) ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 2 บัญญัติว่า

(1) บุคคลจะมีความผิดภายใต้บทบัญญัตินี้ ถ้าหากว่าเขาได้กระทำความผิดตามมาตรา 1 ข้างต้นโดยมีเจตนา

(a) กระทำความผิดในสิ่งที่มาตรานี้ใช้บังคับ หรือ

(b) ให้ความสะดวกในการกระทำความผิดไม่ว่าจะเป็นการกระทำความผิดของตนเองหรือของผู้อื่น และความผิดที่เขาเจตนากระทำหรือให้ความสะดวกดังจะกล่าวต่อไปในมาตรานี้ให้ถือว่าเป็นผู้กระทำความผิดเช่นเดียวกับผู้ที่กระทำความผิดที่ตนช่วยเหลือ

(2) มาตรานี้ใช้กับความผิด

(a) ความผิดที่บัญญัติไว้ในกฎหมายหรือ

(b) ใช้กับบุคคลที่มีอายุตั้งแต่ 21 ปีขึ้นไป

(3) ภายใต้บทบัญญัติของมาตรานี้ ไม่ว่าการกระทำความผิดของผู้กระทำที่อยู่ระยะไกล (Remote) จะได้กระทำไปในโอกาสที่ปราศจากอำนาจเข้าสู่ระบบหรือไม่ หรือโดยอาศัยโอกาสอื่นใดก็ตาม

(4) บุคคลอาจจะมีความผิดตามมาตรานี้ แม้จะปรากฏข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำที่อยู่ระยะไกลจะไม่ได้กระทำลงก็ตาม

(5) บุคคลผู้กระทำความผิดตามมาตรานี้จะต้อง

(a) ถูกพิจารณาอย่างรวดเร็วและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

จากบทบัญญัติดังกล่าวข้างต้นจะเห็นได้ว่าความผิดฐานนี้เป็นความผิดที่มีความซับซ้อนกว่าและร้ายแรงกว่าความผิดฐานเข้าถึงโดยปราศจากอำนาจ จึงไม่นำมาบัญญัติเอาไว้ต่างหาก เพราะการกระทำความผิดในมาตรานี้จะต้องเป็นการกระทำโดยเจตนาที่จะกระทำความผิดและปราศจากอำนาจที่จะกระทำ หรือเป็นการกระทำเพื่อให้ความสะดวกแก่ผู้กระทำความผิดเพื่อที่จะกระทำความผิดที่ร้ายแรง ข้อแตกต่างระหว่างมาตรา 1 กับมาตรา 2 นี้จึงอยู่ที่การพิสูจน์เจตนาในอนาคต นั่นคือการกระทำความผิดตามมาตรา 1 เป็นการกระทำที่ไม่อาจพิสูจน์เจตนาในอนาคตได้ ซึ่งจะมีโทษเบากว่า โดยถือว่าเป็นความผิดที่เรียกว่า “ความผิดที่ไกลออกไป” (Further Offence) หมายถึงความผิดที่ไม่จำเป็นต้องพิสูจน์ถึงเจตนาของผู้กระทำความผิดว่าได้เกิดขึ้นหรือไม่ แต่ถ้าเป็นกรณีที่สามารถพิสูจน์เจตนาในอนาคตได้ก็จะเป็นการกระทำความผิดตามมาตรา 2 ที่จะมีบทลงโทษผู้กระทำความผิดที่คิดจะกระทำความผิดในอนาคต และถ้าหากไม่สามารถลงโทษผู้กระผิดตามมาตรา 2 นี้ได้ก็สามารถลงโทษได้ตามมาตรา 1 ความผิดที่เกิดขึ้นในลักษณะนี้ ได้แก่ ความผิดฐานฉ้อโกง ความผิดฐานลักทรัพย์ และความผิดฐานยักยอกทรัพย์

การพิจารณาความรับผิดทางอาญาในทางคอมมอนลอว์ สำหรับความผิดฐานนี้สามารถแยกพิจารณาได้ ดังนี้

ก. การกระทำ (Actus Reus) โจทก์ต้องพิสูจน์ให้ได้ว่าจำเลยได้เข้าถึงสาระสำคัญ ได้แก่ โปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์ และ

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) ผู้กระทำมีเจตนาที่จะกระทำความผิดอื่นโดยไม่คำนึงถึงเวลาของการกระทำความผิดอื่นว่าจะกระทำในเวลาใด ไม่ว่าจะเป็นขณะที่เกือบจะเป็นเวลาเดียวกับที่เข้าถึงโดยปราศจากอำนาจ หรือในโอกาสต่อมา นั่นคือหากผู้กระทำความผิดเพียงแต่ได้ข้อเท็จจริงมาโดยตั้งใจที่จะกระทำการเข้าถึงโดยปราศจากอำนาจ แต่ยังไม่ลงมือกระทำก็ถือว่ามีความผิดตาม (4) แล้ว

3.2.2.3 ความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ (Modification of Computer Material หรือ Unauthorized Modification) ความผิดเกี่ยวกับการ

ทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 3 บัญญัติว่า

(1) บุคคลจะมีความผิดถ้า

(a) ผู้นั้นได้กระทำการใดๆ ซึ่งก่อให้เกิดการแก้ไขเปลี่ยนแปลงในเนื้อหาสาระของคอมพิวเตอร์ใดๆ และ

(b) ผู้ที่กระทำการเช่นว่านั้น จะต้องมีเจตนาหรือจะต้องรู้ถึงการกระทำของตนในขณะที่กระทำการนั้น

(2) ภายใต้บทบัญญัติของอนุมาตรา (1) (b) เจตนานั้นจะต้องเป็นเจตนาที่ต้องการแก้ไขเปลี่ยนแปลงเนื้อหาสาระของคอมพิวเตอร์ใดๆ โดยการกระทำ เช่น

(a) ทำให้เกิดความเสียหายต่อการทำงานของเครื่องคอมพิวเตอร์

(b) ขัดขวางหรือทำการกีดกันการเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลในคอมพิวเตอร์หรือ

(c) ทำให้เกิดความเสียหายต่อการทำงานของโปรแกรมคอมพิวเตอร์ หรือทำลายความเชื่อถือของข้อมูล

(3) เจตนาของการกระทำดังกล่าว ไม่จำต้องเป็นเจตนาโดยตรงต่อ

(a) คอมพิวเตอร์เฉพาะเจาะจงใดๆ

(b) โปรแกรมหรือข้อมูลพิเศษเฉพาะเจาะจงใดๆ หรือโปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่งโดยเฉพาะ หรือ

(c) การแก้ไขเปลี่ยนแปลงพิเศษเฉพาะเจาะจงใดๆ หรือการแก้ไขเปลี่ยนแปลงชนิดใดชนิดหนึ่งโดยเฉพาะ

(4) ภายใต้บทบัญญัติของอนุมาตรา (1) (b) ผู้กระทำต้องรู้ว่าการแก้ไขเปลี่ยนแปลงดังกล่าว กระทำไปโดยปราศจากอำนาจ และผู้กระทำมีเจตนาเช่นนั้น

(5) มาตรานี้ไม่ถือวัตถุประสงค์เป็นสิ่งสำคัญ โดยไม่คำนึงถึงการแก้ไขเปลี่ยนแปลงโดยปราศจากอำนาจ หรือผลจากเจตนาที่จะก่อขึ้นตาม (2) ไม่ว่าจะเป็นเจตนาที่จะก่อให้เกิดขึ้นเป็นการถาวรหรือชั่วคราว

(6) การแก้ไขเปลี่ยนแปลงในเนื้อหาสาระของคอมพิวเตอร์ตามกฎหมายฉบับนี้ จะไม่ถือว่าเป็นการก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ใดๆ ตามกฎหมายอาญาเกี่ยวกับการก่อให้เกิดความเสียหายเว้นแต่การกระทำนั้นมีผลทางกายภาพเท่านั้น

(7) บุคคลที่กระทำความผิดตามมาตรานี้จะต้อง

DPU

(a) ถูกพิจารณาอย่างรวดเร็วและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

การพิจารณาความรับผิดทางอาญาในทางคอมมอนลอว์ สำหรับความผิดฐานนี้สามารถแยกพิจารณาได้ ดังนี้

ก. การกระทำ (Actus Reus) มีการกำหนดขอบเขตของการกระทำความผิดไว้ค่อนข้างจำกัด โดยเน้นแต่เฉพาะที่เป็นการแก้ไขเปลี่ยนแปลง (Modification) ในเนื้อหาสาระ (Content) ของคอมพิวเตอร์เท่านั้น และแม้ว่าการกระทำดังกล่าวจะมีความสัมพันธ์กับการก่อให้เกิดความเสียหายทางอาญา แต่ก็ไม่ถือว่าเป็นความผิดตามกฎหมายอาญา เว้นแต่จะเป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายทางกายภาพ

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) ผู้กระทำจะต้องมีเจตนาและรู้อยู่ในขณะที่กระทำการแก้ไขเปลี่ยนแปลง ส่วนผลของการกระทำนั้นจะก่อให้เกิดความเสียหายกับทำให้เกิดความเสียหายต่อการทำงานของเครื่องคอมพิวเตอร์ ขัดขวางหรือทำการกีดกันการเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลในคอมพิวเตอร์ ทำให้เกิดความเสียหายต่อการทำงานของโปรแกรมคอมพิวเตอร์ หรือทำลายความเชื่อถือของข้อมูลเครื่องคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือข้อมูลในเครื่องคอมพิวเตอร์อย่างไรไม่จำต้องนำมาพิจารณา

3.2.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ กฎหมายที่เป็นหลักเกณฑ์ในการค้นหาพยานหลักฐานของอังกฤษ คือ The Police and Criminal Evidence Act 1984 (PACE) มาตรา 1 บัญญัติว่า “การค้นเคหสถานต้องมีเหตุอันควรสงสัยตามสมควร โดยถือมาตรฐานของบุคคลในฐานะและพฤติการณ์เดียวกับผู้ค้นเป็นเกณฑ์” และการค้นจะต้องมีการออกหมายค้นจากศาล (Justice of the peace) โดยศาลจะออกหมายค้นก็ต่อเมื่อเป็นเหตุอันควรเชื่อว่าเป็นความผิดอาญาร้ายแรง (Serious arrestable offence) ดังนั้น จึงต้องพิจารณาว่าอาชญากรรมคอมพิวเตอร์จะถือเป็นความผิดอาญาร้ายแรงที่ศาลสมควรจะออกหมายค้นหรือไม่

การค้นและยึดพยานหลักฐานต่างๆ ตามกฎหมายวิธีพิจารณาความอาญาของประเทศอังกฤษต้องคำนึงถึงแนวความคิดในเรื่องการคุ้มครองสิทธิมนุษยชนในทางอาญา ซึ่งได้บัญญัติรับรองไว้ในกฎบัตรแมคนาคาร์ตา (Magna Carta, 1215) กฎหมายของประเทศอังกฤษได้วางมาตรการควบคุม และตรวจสอบการทำงานของเจ้าพนักงานตำรวจโดยองค์กรภายนอกเอาไว้ ขณะเดียวกันก็ไม่ทำให้ประสิทธิภาพในการดำเนินงานของเจ้าหน้าที่ลดลง โดยให้เจ้าหน้าที่ของรัฐ

ได้แก่ ตำรวจ อัยการ และผู้พิพากษา สามารถใช้ดุลพินิจในการบังคับใช้กฎหมายได้มากขึ้น และในขณะเดียวกันก็มีข้อบังคับที่ตราขึ้นเพื่อควบคุมการปฏิบัติงานเอาไว้โดยละเอียด[11]

การค้นตาม The Police and Criminal Evidence Act 1984 (PACE) สามารถแยกพิจารณาได้ ดังนี้

3.2.3.1 การค้นเครื่องคอมพิวเตอร์พีซีในที่รโหฐาน

3.2.3.2 การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN ระบบ WAN และระบบอินเตอร์เน็ต

3.2.3.3 การยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์

3.2.3.1 การค้นเครื่องคอมพิวเตอร์พีซีในที่รโหฐาน ตาม PACEวางหลักไว้ในมาตรา 1 ว่า การค้นในเคหสถานต้องมีเหตุอันควรสงสัยตามสมควร โดยถือเอามาตรฐานของบุคคลในฐานะและพฤติการณ์เดียวกับผู้ค้นเป็นเกณฑ์ และจะต้องขอหมายค้นจากศาล[12] ดังนั้นในการค้นข้อมูลอิเล็กทรอนิกส์ ไม่ว่าจะอยู่ที่ใดทั้งที่อยู่ในเคหสถาน หรือที่รโหฐานอื่น เจ้าพนักงานตำรวจจะต้องมีเหตุอันควรสงสัยตามสมควรว่าจะมีพยานหลักฐานอยู่ที่นั้น และจะต้องมีศาลเป็นผู้ทำหน้าที่ตรวจสอบการดำเนินงานอีกชั้นหนึ่ง ในการออกหมายค้นนั้นศาลจะออกให้ก็ต่อเมื่อมีเหตุอันควรเชื่อว่ามีความผิดอาญาร้ายแรง (Serious Arrestable Offence) เกิดขึ้นและพยานหลักฐานที่จะพิสูจน์ความผิดได้ถูกเก็บอยู่ในนั้น จึงต้องพิจารณาว่าอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นเป็นความผิดอาญาร้ายแรงที่ศาลจะออกหมายค้นหรือไม่ ถ้าอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นเป็นความผิดอาญาร้ายแรง ศาลก็จะออกหมายค้นให้ และในการเข้าตรวจค้นตามหลักใน PACE มาตรา 16 จะต้องกระทำภายในหนึ่งเดือนนับแต่วันออกหมายค้น โดยจะต้องแจ้งเหตุแห่งการค้น และต้องค้นในเวลาที่เหมาะสม กรณีที่เจ้าของบ้านอยู่ด้วยในเวลาที่ค้น ตำรวจต้องแสดงหมายและมอบสำเนาหมายค้นให้ไว้ แต่ถ้าเจ้าของบ้านไม่อยู่ต้องปิดหมายค้นไว้ในที่ที่เหมาะสม แต่พยานหลักฐานนั้นต้องไม่เป็นพยานหลักฐานที่เป็นความลับตาม PACE มาตรา 15 ,16

กรณีการค้นโดยไม่มีหมายวางหลักไว้ใน PACE มาตรา 17 กำหนดให้ผู้ค้นจะต้องเป็นเจ้าพนักงานตำรวจที่อยู่ในเครื่องแบบ และต้องเป็นการค้นเพื่อช่วยชีวิตบุคคลในเคหสถานนั้น และเพื่อป้องกันการทำลายทรัพย์อย่างร้ายแรง

3.2.3.2 การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN ระบบ WAN และระบบอินเตอร์เน็ต

---

[11]ณรงค์ ใจหาญและคณะ. (2540). **รายงานศึกษาวิจัยฉบับสมบูรณ์ เรื่อง สิทธิผู้ต้องหา จำเลย และผู้ต้องโทษในคดีอาญา (รายงานการศึกษาวิจัยเสนอต่อคณะกรรมการกฤษฎีกา)**. หน้า 23.

[12] ณรงค์ ใจหาญและคณะ. เล่มเดิม. หน้า 51.

ตำรวจอังกฤษจะใช้วิธีนำเครื่องคอมพิวเตอร์หรือเครื่องมืออื่นเชื่อมเข้าไปในระบบเฉพาะของสำนักงาน และระบบเครือข่ายอินเตอร์เน็ต เพื่อเข้าไปตรวจค้นข้อมูลในนั้น จะขอหมายจาก Justice of the Peace ไม่ได้ แต่จะต้องขอจาก Circuit Judge และศาลจะออกหมายให้ต่อเมื่อไต่สวนได้ความว่า "มีเหตุอันควรเชื่อว่าพยานหลักฐานที่เกี่ยวกับการสอบสวนในคดีความผิดเป็น ความผิดอาญาร้ายแรง (Serious Arrestable Offence) ซึ่งเกิดขึ้นในบ้านนี้ และถ้าไม่ค้นบ้านนี้ก็จะไม่ได้มาซึ่งพยานหลักฐานดังกล่าว และในการค้นนั้นจะได้มาซึ่งพยานหลักฐานอันเป็นประโยชน์ต่อสาธารณชน"[13]

3.2.3.3 การยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์ ในการยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์มีบัญญัติอยู่ใน PACE มาตรา 18,19 ดังนี้

มาตรา 18 บัญญัติว่า "เมื่อค้นแล้วตำรวจต้องทำบันทึกการค้นและบันทึกรายการสิ่งของที่ค้นและยึด รายการเหล่านั้นผู้ค้นต้องมอบให้แก่เจ้าของบ้านเมื่อผู้นั้นร้องขอ" และ

มาตรา 19 บัญญัติว่า "กรณีที่ตำรวจยึดวัตถุที่มีเหตุเชื่อได้ว่าเป็นพยานหลักฐานที่เกี่ยวข้องกับการสอบสวน หรือความผิดอื่น หรือมีความผิดอื่นรวมอยู่ด้วย หรือมีความจำเป็นต้องยึดเพื่อป้องกันการเคลื่อนย้าย ซ่อนเร้น หรือทำลายหลักฐาน"

จากบทบัญญัติข้างต้นจะเห็นได้ว่าเครื่องคอมพิวเตอร์ที่ยึดได้นั้นเป็นวัตถุที่ใช้เป็นพยานหลักฐานในการสอบสวนที่เจ้าหน้าที่ตำรวจยึดได้ รวมทั้งข้อมูลที่อยู่ภายในเครื่องด้วย เว้นแต่กรณีที่เป็นข้อมูลที่เป็นความลับ ที่จะต้องพิจารณาตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลประกอบ

3.2.4 การรับฟังเป็นพยานหลักฐานในศาล การรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ของศาลอังกฤษ โดยหลักจะรับฟังแต่พยานหลักฐานโดยตรง พยานบอกเล่า (Hearsay) ถือว่ามีน้ำหนักน้อยหรือไม่รับฟังเลย แต่ The Police and Criminal Evidence Act 1984 เป็นกฎหมายพยานหลักฐานในคดีอาญา ที่มีบทบัญญัติเกี่ยวกับการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์อยู่ เป็นข้อยกเว้นของพยานบอกเล่า (Hearsay) โดยให้รับฟังพยานเอกสารที่เป็นผลจากการประมวลผลหรือคำนวณของเครื่องคอมพิวเตอร์ได้ การค้นและยึดพยานหลักฐานกระทำโดยเจ้าพนักงานตำรวจ กรณีที่ประสบปัญหาการกระทำความผิดทางอินเตอร์เน็ตที่การกระทำอาจเกิดขึ้นในต่างประเทศ อำนาจในการสอบสวนจะสามารถกระทำได้เพียงใด เช่น การกระทำความผิดเกิดขึ้นในประเทศเยอรมนี และผู้กระทำความผิดอยู่ที่ประเทศนั้น แต่เครือข่ายที่ใช้ข้อมูลหรือข้อมูลที่ใช้ผ่านประเทศอังกฤษจะต้องคำนึงถึงข้อตกลงระหว่างประเทศ โดยเฉพาะข้อตกลงระหว่าง

---

[13] ณรงค์ ใจหาญและคณะ. เล่มเดิม. หน้า 52.

ประชาคมยุโรปด้วย แม้ว่าจะต้องคำนึงถึงเรื่องดังกล่าวการดำเนินคดีตามกฎหมายอังกฤษจะถือหลักว่า ถ้าเข้าหลักเกณฑ์ 2 ประการดังต่อไปนี้ประเทศอังกฤษก็อาจจะไม่นำมาดำเนินคดี คือ

ก. ถ้าผู้กระทำความผิดหรือผู้ร่วมกระทำความผิดไม่ใช่พลเมืองของประเทศอังกฤษ หรือ

ข. ความผิดที่เกิดขึ้นไม่ได้บัญญัติไว้ใน The Computer Misuse Act 1990

ศาลที่มีอำนาจในการพิจารณาคดี สามารถแบ่งได้ตามฐานความผิด ดังนี้

(1) ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access) เป็นการกระทำความผิดที่ไม่ซับซ้อน ศาลที่มีอำนาจในการพิจารณาคดีคือศาลแขวง(Magistrate Court) จึงมีกฎหมายที่เกี่ยวข้องอีกฉบับคือ The Magistrate's Court Act 1980 เป็นเรื่องเกี่ยวกับการกำหนดฐานความผิดแก่ผู้ที่ให้ความช่วยเหลือในการกระทำความผิดใน มาตรา 44 (1) ซึ่งบัญญัติว่า "สามารถลงโทษบุคคลที่ให้ความช่วยเหลือผู้ที่กระทำการเข้าถึงโดยปราศจากอำนาจ โดยการให้ความรู้ทางด้านข้อมูล การให้รหัสผ่าน หรือให้วิธีการเข้าสู่ระบบเพื่อผ่านไปยังโปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์"

(2) ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง และความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ ขึ้นอยู่กับความร้ายแรงของการกระทำความผิด หากมีความร้ายแรงมากก็จะอยู่ในอำนาจพิจารณาของศาลสูงคดีอาญา (Crown Court) แต่ถ้าไม่ร้ายแรงมากก็จะอยู่ในอำนาจพิจารณาของศาลแขวง (Magistrate Court)

โดยลักษณะของข้อมูลอิเล็กทรอนิกส์ที่ไม่สามารถพิสูจน์ได้ในทางกายภาพ จึงไม่สามารถนำมาพิสูจน์ในกระบวนพิจารณาคดีอาญาได้ ดังนั้นรายงานที่ประมวลผลจากคอมพิวเตอร์ (Printout) จะเป็นพยานบอกเล่า (Hearsay) เนื่องจากเกิดจากการกระทำของมนุษย์ ต้องห้ามรับฟังตามกฎหมาย Criminal Justice Act 1988 มาตรา 24 แต่จากความสามารถในการทำงานของคอมพิวเตอร์เองที่สามารถใช้เป็นเครื่องกล หรือเครื่องมือในการคำนวณ จึงไม่น่าจะเป็นพยานหลักฐานในรูปพยานบอกเล่าเสมอไป ถ้าอ้างเป็นพยานหลักฐานโดยยืนยันการใช้ที่เป็นธุรกิจปกติ และข้อมูลที่ได้ก็เกิดจากการประมวลผลโดยคอมพิวเตอร์อันเป็นปกติเช่นกัน[14]

3.3 ประเทศญี่ปุ่น

---

[14] Richard May. (1999). **Criminal Evidence. London**. p. 11-36.

รัฐธรรมนูญของประเทศญี่ปุ่นไม่ได้วางหลักคุ้มครองความเป็นอยู่ส่วนตัวไว้โดยชัดแจ้งแต่เป็นหลักที่อาจสังเคราะห์ขึ้นจากหลักเสรีภาพทั่วไปที่บัญญัติไว้ในมาตรา 13[15] ประกอบกับหลักเสรีภาพในการติดต่อสื่อสารกันโดยอิสระในมาตรา 21[16] และหลักเสรีภาพในเคหสถาน ในเอกสาร และทรัพย์สินส่วนตัว ในมาตรา 35[17] ดังนั้นการเข้าไปในเคหสถาน การค้นและการยึดทรัพย์สินจะกระทำมิได้ ยกเว้นมีหมายที่ออกโดยข้าราชการฝ่ายตุลาการ โดยในหมายนั้นจะต้องระบุเหตุผลที่สมควรและกำหนดสถานที่ตรวจค้นและทรัพย์ที่ต้องการยึดไว้โดยชัดแจ้ง

3.3.1 มาตรการเพื่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศญี่ปุ่น การค้นตามกฎหมายวิธีพิจารณาความอาญาของญี่ปุ่นนั้น ให้อำนาจพนักงานอัยการ หรือเจ้าพนักงานตำรวจดำเนินการค้นได้ ภายใต้รัฐธรรมนูญ มาตรา 35 วรรคหนึ่ง ดังนั้นทำการค้นได้ตามกฎหมายญี่ปุ่นต้องมีหมายค้น การค้นข้อมูลอิเล็กทรอนิกส์ก็เช่นกัน ยกเว้นกรณีที่เป็นการกระทำความผิดซึ่งหน้าตามมาตรา 33 ที่ไม่ต้องมีหมายค้น เนื่องจากเป็นการกระทำความผิดหรือถูกจับเนื่องจากการกระทำความผิดซึ่งหน้า รัฐธรรมนูญได้วางหลักเกณฑ์ให้เจ้าพนักงานสามารถค้น และยึดได้ก็ต่อเมื่อมีหมายค้นหรือหมายยึด หรือเป็นกรณีที่เป็นการค้นหรือการยึดที่สืบเนื่องจากการจับกุมตัวผู้กระทำความผิด

สำหรับการค้นเพื่อทำการยึดจดหมายหรือโทรสาร เนื่องจากรัฐธรรมนูญได้ให้ความคุ้มครองสิทธิเสรีภาพในการสื่อสารของบุคคลไว้ใน มาตรา 35 วรรคหนึ่ง ดังนั้นการยึดจดหมายหรือโทรสารที่บุคคลใช้ติดต่อสื่อสารกันย่อมเป็นการกระทำที่ขัดต่อสิทธิเสรีภาพในการสื่อสารที่รัฐธรรมนูญได้บัญญัติรับรองไว้ แต่ถ้าเป็นกรณีที่เจ้าพนักงานกระทำไปเพื่อการแสวงหาพยานหลักฐานในการพิสูจน์ความผิด หรือเพื่อป้องกันอาชญากรรมก็สามารถดำเนินการค้นและยึดได้ [18]

---

[15] มาตรา 13 บัญญัติว่า "ประชาชนทุกคนย่อมได้รับการเคารพในฐานะปัจเจกบุคคล สิทธิของประชาชนในชีวิต เสรีภาพ และการแสวงหาความผาสุกภายในขอบเขตที่ไม่ขัดต่อประโยชน์สุขอันร่วมกันของสาธารณะ ต้องได้รับความเคารพสูงสุดในการออกกฎหมายหรือในการอื่นใดที่เกี่ยวกับการปกครองประเทศ"

[16] มาตรา 21 บัญญัติว่า "เสรีภาพในการชุมนุม การรวมกลุ่ม รวมทั้งการพูด การพิมพ์ และสิ่งใดทั้งปวงที่เป็นการแสดงออกเป็นสิ่งที่ได้รับการคุ้มครอง

[17] มาตรา 35 บัญญัติว่า "บุคคลใดก็ตาม หากไม่มีหมายซึ่งออกโดยเหตุผลอันชอบธรรมและระบุชัดถึงสถานที่ที่จะตรวจค้นและสิ่งของที่จะอายัด สิทธิที่จะไม่ให้เข้าไปในเคหสถาน ไม่ให้ถูกตรวจค้นและอายัดเอกสารและสิ่งของในครอบครอง ย่อมจะไม่ถูกละเมิด เว้นแต่กรณีตามมาตรา 33

การตรวจค้นและอายัดจะดำเนินการโดยหมายแต่ละประเภท ซึ่งออกโดยเจ้าพนักงานกระบวนการยุติธรรมที่มีอำนาจ"

[18] Shigemitsu Dando. (1965). **Japanese Criminal Procedure**. p. 270

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในการประมวลผลด้วยเครื่องคอมพิวเตอร์ของหน่วยงานฝ่ายปกครอง ค.ศ. 1988 รัฐสภาญี่ปุ่นบัญญัติขึ้นโดยอาศัยแนวทางของ Organization for Economic Co-operation and Development (OECD) ที่เสนอให้กำหนดหน้าที่ของหน่วยงานในการรักษาความปลอดภัย วางหลักเกณฑ์ในการเข้าถึงข้อมูล และการแก้ไขข้อมูลให้ถูกต้อง โดยกฎหมายฉบับนี้ได้กำหนดให้หน่วยงานของรัฐจำกัดบทบาทในการรวบรวมข้อมูลข่าวสารส่วนบุคคลและโฆษณาให้สาธารณชนทราบการจัดระบบข้อมูลข่าวสารส่วนบุคคลของหน่วยงาน และห้ามมิให้หน่วยงานของรัฐใช้ข้อมูลของรัฐโดยผิดวัตถุประสงค์ คือห้ามมิให้นำข้อมูลข่าวสารส่วนบุคคลซึ่งจัดเก็บโดยมีวัตถุประสงค์อย่างหนึ่งไปใช้ในวัตถุประสงค์อย่างอื่น

3.3.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ การดักฟังการติดต่อสื่อสารถือเป็นการละเมิดเสรีภาพในการติดต่อสื่อสารซึ่งได้รับความคุ้มครองตามรัฐธรรมนูญ มาตรา 21 วรรคสองตอนท้าย บัญญัติว่า “ความลับในการสื่อสารจะละเมิดมิได้” ดังนั้นโดยหลักแล้วการดักฟังย่อมกระทำมิได้ อย่างไรก็ดีรัฐสภาญี่ปุ่นได้ตรากฎหมายว่าด้วยการดักฟังการสื่อสารทางโทรคมนาคม (Communications Interception Law) ขึ้นใช้บังคับในเดือนสิงหาคม ค.ศ. 1999 ซึ่งให้อำนาจเจ้าพนักงานอัยการหรือตำรวจชั้นผู้ใหญ่ในการดักฟังทางโทรศัพท์หรือการดักจับสัญญาณโทรสารและติดตามเฝ้าดูกฎหมายอิเล็กทรอนิกส์ในการสอบสวนคดียาเสพติด การฆาตกรรม หรือคดีอาญาที่มีการใช้อาวุธ หรือการลักลอบหนีภาษีของชาวต่างชาติ โดยจะต้องได้รับอนุญาตจากศาล และให้มีระยะเวลาดักฟังยาวนานที่สุดไม่เกิน 10 วัน โดยจะขอขยายได้ไม่เกิน 30 วัน

นอกจากนี้ในการดักฟังจะต้องมีบุคคลอื่นที่เป็นบุคคลภายนอก เช่น เจ้าหน้าที่ของบริษัทโทรเลขโทรศัพท์แห่งชาติของญี่ปุ่นร่วมฟังด้วยและภายหลังจากการดักฟังสิ้นสุดลงเจ้าพนักงานตำรวจหรือพนักงานอัยการซึ่งทำหน้าที่ดักฟังจะต้องแจ้งให้ผู้ถูกดักฟังทราบถึงการดักฟังนั้นภายใน 30 วัน

สำหรับสิ่งที่กฎหมายญี่ปุ่นบัญญัติไม่ให้ดำเนินการค้นหรือยึด[19] ได้แก่

ก. เอกสารที่เป็นความลับทางราชการ ซึ่งเจ้าพนักงานจะทำการค้นหรือยึดได้ก็ต่อเมื่อมีคำร้องไปยังหัวหน้าหน่วยงานที่มีเอกสารดังกล่าว และต้องได้รับความยินยอมให้ทำการตรวจค้นหรือยึดเอกสารดังกล่าวจากหัวหน้าหน่วยงานนั้นๆด้วย หากหัวหน้าหน่วยงานดังกล่าวไม่ยินยอมให้ค้นหรือยึดเอกสารนั้น เนื่องจากความมั่นคงของประเทศก็สามารถทำได้

---

[19] Ibid. p.300.

ข. เอกสารหรือสิ่งของที่เป็นความลับของลูกค้าในทางการแพทย์ หรือลูกความ เจ้าพนักงานไม่สามารถเข้าไปค้นหรือยึดได้ เว้นแต่จะได้รับความยินยอมจากบุคคลผู้ครอบครอง หากผู้ครอบครองไม่ยินยอมให้เจ้าพนักงานทำการค้นหรือยึดก็ต้องแจ้งเหตุผลที่ไม่ยินยอมให้เจ้าพนักงานทราบด้วย

3.3.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ รัฐธรรมนูญของประเทศญี่ปุ่นบัญญัติไว้ว่าการค้นจะกระทำได้ก็ต่อเมื่อมีหมายที่ออกโดยศาล และจะต้องเป็นการค้นเพื่อการสืบสวนการกระทำความผิดอาญา เป็นการแสวงหาพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดอาญา ซึ่งการแสวงหาพยานหลักฐานดังกล่าวจะกระทำได้ทั้งก่อน และระหว่างการพิจารณา

3.3.3.1 เหตุแห่งค้น ตามกฎหมายประเทศญี่ปุ่น แบ่งออกเป็น 2 ประเภท ได้แก่

ก. กรณีปกติ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 218 กฎหมายบัญญัติให้อำนาจเจ้าพนักงานของรัฐ ได้แก่ พนักงานอัยการ อัยการผู้ช่วย หรือตำรวจสามารถดำเนินการค้นและยึดได้ แต่ถ้าเป็นการค้นหรือยึดในที่รโหฐานก็ต้องดำเนินการตามหมายค้นหรือยึดที่ออกโดยศาล โดยกำหนดว่าการค้นหรือยึดสิ่งของต่างๆนั้นต้องเป็นไปเพื่อการสืบสวนการกระทำความผิดอาญา การสอบสวนเป็นกระบวนการที่กฎหมายอนุญาตให้เจ้าพนักงานดังกล่าวข้างต้นมีอำนาจในการแสวงหาพยานหลักฐานเพื่อพิสูจน์การกระทำความผิด โดยการแสวงหาพยานหลักฐานนั้นจะต้องกระทำก่อนหรือในระหว่างการพิจารณาคดี[20] เหตุที่เจ้าพนักงานจะขอหมายค้นหรือหมายยึดภายในที่รโหฐานได้ ต้องเป็นกรณีที่มีการแสวงหาพยานหลักฐานที่พิสูจน์การกระทำความผิดกรณีที่พยานหลักฐานดังกล่าวเป็นวัตถุสิ่งของ หากเป็นการค้นหาตัวบุคคลนั้นรัฐธรรมนูญ มาตรา 33 ได้กำหนดว่าเป็นการค้นเพื่อจับกุมผู้กระทำความผิดตามหมายจับ หรือค้นเพื่อหาตัวบุคคลที่ได้กระทำความผิดซึ่งหน้า เจ้าพนักงานสามารถดำเนินการค้นภายในที่รโหฐานได้โดยไม่จำเป็นต้องขอหมายศาล

ข. กรณีพิเศษ เป็นการค้นที่รโหฐานกรณีที่ไม่ต้องมีหมายค้น หรือหมายยึด แต่ก็ต้องเป็นกรณีที่สืบเนื่องมาจากการจับกุม ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 199 บัญญัติหลักเกณฑ์ที่สามารถทำได้ 3 กรณี ได้แก่

(1) การค้นและยึดที่สืบเนื่องจากการจับกุมภายใต้หมายจับที่ออกโดยศาล ตามมาตรา 199 ประกอบมาตรา 220 โดยมาตรา 220 อนุญาตให้เจ้าพนักงานสามารถทำการค้นและยึดสิ่งของกรณีที่เจ้าพนักงานทำการจับกุมผู้ต้องหาที่ศาลออกหมายจับได้ โดยกฎหมายกำหนดให้เจ้าพนักงาน

---

[20] Ibid. p.303.

เหล่านั้นแจ้งต่อศาลว่ามีการกระทำความผิดเกิดขึ้น และเชื่อว่าบุคคลที่จะต้องถูกจับมีความผิดอาญาดังกล่าว

หากเจ้าพนักงานเห็นว่าสิ่งใดสามารถใช้ในการพิสูจน์ความผิดได้ ก็สามารถนำเหตุผลดังกล่าวไปขออนุญาตต่อศาล เพื่อขอหมายค้นเข้าไปค้นหาสิ่งของดังกล่าวมาประกอบการพิจารณาได้ แต่ถ้าเป็นความผิดที่มีอัตราโทษน้อย เช่น โทษปรับไม่เกิน 100 เยน เป็นต้น ไม่จำต้องขอหมายจับจากศาล

3.3.3.2 วิธีการค้น ตามกฎหมายประเทศญี่ปุ่น แบ่งออกเป็น 2 ประเภท ได้แก่

ก.การค้นที่สืบเนื่องจากการจับกุมตามหมายจับ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 201 เมื่อเจ้าพนักงานได้รับหมายจับจากศาลแล้วสามารถไปดำเนินการตามหมายจับดังกล่าวได้เลย หากบุคคลดังกล่าวอยู่ภายในเคหสถาน หรือสถานที่ใดก็ตาม เจ้าพนักงานสามารถเข้าไปได้โดยไม่ต้องมีหมายค้นจากศาล แต่เมื่อพบบุคคลดังกล่าวแล้วก็ต้องแสดงหมายจับให้ดู

ข. การค้นที่สืบเนื่องจากการจับกุมที่ผู้กระทำความผิดได้กระทำความผิดซึ่งหน้า ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 213 บัญญัติให้อำนาจเจ้าพนักงานได้แก่ เจ้าพนักงานอัยการ อัยการผู้ช่วย หรือตำรวจ สามารถทำการจับกุมผู้ที่กระทำความผิดซึ่งหน้าตนได้โดยไม่ต้องมีหมายจับ ถ้าการจับกุมดังกล่าวเกิดขึ้นในที่รโหฐาน เจ้าพนักงานสามารถค้นและยึดสิ่งของภายในสถานที่ดังกล่าวได้โดยไม่ต้องมีหมาย แต่จะต้องเป็นกรณีที่สามารถออกหมายค้นหรือยึดได้ด้วย และเมื่อพบสิ่งที่ต้องการยึดแล้วจะต้องรีบคืนสิ่งของดังกล่าวให้เจ้าของที่แท้จริงโดยด่วน

สำหรับการกระทำความผิดซึ่งหน้านั้น ตามกฎหมายญี่ปุ่น ได้แก่การกระทำความผิดที่บุคคลได้ลงมือกระทำความผิดในขณะนั้น หรือเพิ่งลงมือกระทำความผิด มีลักษณะการกระทำความผิด 4 ประเภท [21] ได้แก่

(1) เมื่อพบเห็นการกระทำความผิดและติดตามจับกุมแบบกระชั้นชิด

(2) เมื่อพบผู้กระทำความผิดครอบครองทรัพย์สิน อาวุธ หรือสิ่งของที่เกี่ยวข้องกับการกระทำความผิด

(3) เมื่อพบว่าร่างกาย หรือเสื้อผ้าของบุคคลดังกล่าวมีร่องรอยการต่อสู้ บาดแผล หรือมีสิ่งที่บ่งบอกว่าได้กระทำความผิดมา

(4) เมื่อเจ้าพนักงานเรียกให้หยุดแต่กลับวิ่งหนี

---

[21] Ibid. p.310.

หากพบเห็นลักษณะของการกระทำประเภทใดประเภทหนึ่งข้างต้นแล้ว ผู้กระทำความผิดได้ถูกจับกุมในเคหสถาน หรือที่รโหฐาน เจ้าพนักงานที่มีอำนาจสามารถทำการตรวจค้นและยึดสิ่งของภายในสถานที่ดังกล่าวได้โดยไม่ต้องมีหมายค้น หรือยึด

ค. การค้นในกรณีฉุกเฉิน เป็นการค้นหรือการยึดในที่รโหฐานที่สืบเนื่องมาจากการจับกุมผู้ต้องหาในกรณีฉุกเฉินตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 210 กรณีที่มีเหตุเพียงพอที่จะเชื่อว่ามีการกระทำความผิดที่มีอัตราโทษจำคุกมากกว่า 3 ปีขึ้นไป โดยเจ้าพนักงานอัยการ อัยการผู้ช่วย หรือตำรวจ แต่ไม่สามารถขอหมายศาลได้ในขณะนั้น เป็นเหตุให้จับกุมโดยไม่มีหมาย เมื่อทำการจับกุมผู้ต้องหาได้แล้วต้องรีบดำเนินการขอหมายศาลทันที เมื่อเจ้าพนักงานทำการจับกุมผู้ต้องหาได้แล้ว เจ้าพนักงานก็สามารถทำการตรวจค้นหรือยึดได้โดยไม่ต้องมีหมายค้น แต่ถ้าศาลไม่ออกหมายจับให้ เจ้าพนักงานผู้ดำเนินการจับกุมก็ต้องปล่อยตัวบุคคลดังกล่าวทันที พร้อมทั้งคืนสิ่งที่ค้นหรือยึดมาด้วย หากศาลออกหมาย[22]

ง.การค้นโดยประชาชนทั่วไป กรณีที่เป็นการกระทำความผิดซึ่งหน้า ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 213 ให้อำนาจประชาชนทั่วไปสามารถจับกุมผู้ที่กระทำความผิดดังกล่าวได้ด้วย แต่กฎหมายไม่อนุญาตให้บุคคลดังกล่าวตรวจค้น หรือยึดสิ่งของ

3.3.3.3 ระยะเวลาในการค้น การที่กฎหมายให้อำนาจเจ้าพนักงานทำการค้นได้ถือเป็นการกระทำที่ละเมิดต่อสิทธิของบุคคลผู้เป็นเจ้าของ เพราะสิ่งที่กฎหมายประสงค์จะคุ้มครอง คือ สิทธิในการครอบครองและการพักอาศัยของบุคคลในเคหสถาน แต่ด้วยเหตุจำเป็นจึงอนุญาตให้ทำได้ อย่างไรก็ตามกฎหมายก็ได้กำหนดระยะเวลาในการค้นเอาไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 116 เนื่องจากเป็นการกระทำที่รบกวนสิทธิของผู้เป็นเจ้าของสถานที่กฎหมายจึงบัญญัติให้ทำการค้นและยึดได้แต่ในเวลากลางวันเท่านั้น ซึ่งเป็นเวลาตั้งแต่พระอาทิตย์ขึ้นจนถึงพระอาทิตย์ตก เพราะในเวลากลางคืนเป็นเวลาพักผ่อนของผู้ครอบครอง

กรณีที่เจ้าพนักงานทำการตรวจค้นในเวลากลางวันแล้วไม่เสร็จในช่วงเวลานั้น ก็สามารถทำการตรวจค้นต่อเนื่องไปในเวลากลางคืนได้ และกฎหมายก็ให้อำนาจทำการค้นในเวลากลางคืนได้ ตามมาตรา 117 กรณีที่ศาลเห็นว่าจำเป็นที่จะต้องทำการค้นในเวลากลางคืน โดยระบุลงไปในหมายไว้ด้วย สถานที่ที่ศาลอนุญาตให้ทำการตรวจค้นในเวลากลางคืนได้ เช่น สถานบันเทิงเริงรมย์ บ่อนการพนัน โรงแรม หรือร้านอาหาร ฯลฯ

---

[22] Ibid. p.316.

3.3.4 การรับฟังเป็นพยานหลักฐานในศาล ศาลสูงสุดของประเทศญี่ปุ่นได้วางมาตรการในการรับฟังพยานหลักฐานสำหรับการค้นเอาไว้เช่นเดียวกับประเทศอื่นๆ คือ ห้ามมิให้รับฟังพยานหลักฐานที่ได้มาจากการค้น โดยไม่มีหมายค้น โดยมาตรการดังกล่าวเป็นเพียงวิธีการในการป้องกันมิให้เจ้าหน้าที่ใช้อำนาจในทางมิชอบเท่านั้น มิใช่ไม่รับฟังพยานหลักฐานดังกล่าวเลย เพราะในทางปฏิบัติของศาลญี่ปุ่นการรับฟังพยานหลักฐานจะพิจารณาถึงความรุนแรงของการกระทำความผิด ประกอบกับความมุ่งหมายของการสอบสวน

จากการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกานั้นไม่ได้มีกฎหมายที่เป็นกลางซึ่งจะวางหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ กฎหมายที่มีผลใช้บังคับอยู่ในปัจจุบันเป็นแต่เพียงกฎหมายที่ให้ความคุ้มครองเฉพาะเรื่อง เช่น การเงิน คอมพิวเตอร์ ฯลฯ ทั้งยังขาดหน่ายงานอิสระที่เป็นองค์กรกลางคอยทำหน้าที่ควบคุม ตรวจตรา และบังคับการให้เป็นไปตามกฎหมาย สำหรับหน่วยงานที่มีอยู่ในปัจจุบันก็ขาดความเป็นอิสระและไม่มีอำนาจเด็ดขาด เนื่องจากเป็นหน่วยงานของฝ่ายบริหาร

สำหรับประเทศอังกฤษซึ่งให้ความเคารพต่อสิทธิส่วนบุคคล และความจำเป็นที่จะต้องดำเนินการให้กฎหมายภายในของตนสอดคล้องกับอนุสัญญาแห่งสภายุโรปว่าด้วยการให้ความคุ้มครองข้อมูล (The Council of Europe's Data Protection) รัฐสภาของประเทศอังกฤษจึงต้องออกกฎหมายเพื่อแสวงหาพยานหลักฐานของเจ้าพนักงานของรัฐ สามารถล่วงล้ำเข้าไปรับรู้ถึงข้อมูลที่เกี่ยวกับการดำเนินชีวิตของผู้ต้องสงสัยหรือสารสนเทศที่อยู่ในความครอบครองของผู้ใช้ และการแสดงความคิดเห็นส่วนตัว เท่ากับเป็นการล่วงล้ำข้อมูลส่วนบุคคลที่กฎหมายอังกฤษประสงค์จะให้ปกปิด ดังเช่นคดีระหว่างนายจ้างและลูกจ้างข้างต้น การรวบรวมพยานหลักฐานด้วยวิธีการดังกล่าวอาจถูกหาว่าเป็นพยานหลักฐานที่ได้มาโดยมิชอบได้ ทั้งกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของอังกฤษ ที่มีมาตรการควบคุม และตรวจสอบการทำงานของเจ้าหน้าที่โดยองค์กรภายนอกไว้อย่างรัดกุม และไม่ทำให้ประสิทธิภาพในการปราบปรามอาชญากรรมของเจ้าหน้าที่ลดลง โดยการให้ดุลพินิจในการปฏิบัติหน้าที่ของเจ้าหน้าที่ ภายใต้กฎเกณฑ์ที่กฎหมายบัญญัติไว้ จึงดูมีความน่าเชื่อถือที่สุด

ประเทศญี่ปุ่นเองก็มีความพยายามที่จะตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลไว้เป็นกฎหมายทั่วไป แต่ก็ไม่ได้วางมาตรการที่ให้ความคุ้มครองที่เคร่งครัดเกินไป เพราะในขณะเดียวกันก็ให้ตรากฎหมายให้อำนาจเจ้าพนักงานของรัฐเข้าสู่ข้อมูลบางประเภทได้ แต่การแสวงหาพยานหลักฐานจากข้อมูลส่วนบุคคลในประเทศญี่ปุ่นเมื่อเทียบกับอีกสองประเทศข้างต้น ก็ยังเป็นเรื่องใหม่ที่ยังต้องรอให้มีการวางมาตรการ บัญญัติกฎหมายลำดับรอง เพื่อบังคับใช้ตามกฎหมายที่มีอยู่ให้มีประสิทธิภาพมากขึ้น เนื่องจากกฎหมายที่มีนั้นยังไม่สามารถนำมาใช้บังคับได้อย่างเต็มที่

อย่างไรก็ดีประสบการณ์ของทั้งสามประเทศต่างก็มีประโยชน์ต่อการนำมาศึกษาเปรียบเทียบกับกฎหมายของไทยที่มีอยู่

DPU

บทที่ 4
วิเคราะห์มาตรการทางกฎหมายในการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในประเทศไทย

ระบบอินเตอร์เน็ตได้รับการพัฒนาขึ้นมาเพื่อประโยชน์ทางด้านการสื่อสารระหว่างมนุษย์ในรูปของสื่อผสม (Multimedia) ซึ่งบุคคลสามารถติดต่อถึงกันได้โดยอาศัยสื่อหลายประเภทผสมกัน ไม่ว่าจะเป็นการรับส่งข้อความธรรมดา การรับส่งภาพ หรือเสียง ตลอดจนข้อมูลอิเล็กทรอนิกส์ เช่น โปรแกรมคอมพิวเตอร์ [1] มีการส่งเสริมให้มีการใช้คอมพิวเตอร์ในประเทศต่างๆ แม้เครื่องมืออิเล็กทรอนิกส์ โดยเฉพาะคอมพิวเตอร์และเครือข่ายอินเตอร์เน็ตนั้นก็มีทั้งคุณและโทษ แต่ก็น่าจะเป็นคุณมากกว่า ประเทศต่างๆจึงให้ความสำคัญ และพยายามที่จะหามาตรการมาแก้ปัญหาที่เกิดขึ้นบนเครือข่ายคอมพิวเตอร์ ประเทศต่างๆ ทั้งในยุโรป อเมริกา ออสเตรเลีย และประเทศในแถบเอเชีย เช่น ญี่ปุ่น ต่างก็พยายามหามาตรการป้องกันและปราบปรามการกระทำความผิดที่เกิดขึ้น แต่การบังคับใช้กฎหมายที่มีอยู่ในปัจจุบันมักไม่มีประสิทธิภาพ และสำหรับอาชญากรรมคอมพิวเตอร์ที่มีการกระทำความผิดที่มิใช่เกิดขึ้นแต่เพียงประเทศใดประเทศหนึ่ง แต่มีลักษณะเป็นอาชญากรรมข้ามชาติ จึงเกิดปัญหาความร่วมมือระหว่างประเทศ มาตรการในการแก้ไขปัญหาระหว่างประเทศในปัจจุบันอยู่ในรูปของความร่วมมือระหว่างประเทศ เพื่อลดช่องว่างที่มีอยู่ให้ลดน้อยลง หรือจัดให้มีความร่วมมือในลักษณะขององค์กรต่อองค์กร หรือประเทศต่อประเทศเพื่อช่วยเหลือซึ่งกันและกันในด้านการสืบสวนสอบสวน

4.1 มาตรการทางกฎหมายในการรับฟังเป็นพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในปัจจุบัน

เมื่อมีการกระทำความผิดเกี่ยวกับข้อมูลส่วนบุคคลที่เก็บอยู่ในเครื่องคอมพิวเตอร์เกิดขึ้น การกระทำดังกล่าวนอกจากจะเป็นอาชญากรรมคอมพิวเตอร์แล้ว การเข้าถึงข้อมูลในคอมพิวเตอร์โดยปราศจากอำนาจตามกฎหมายไทยถือเป็นการกระทำที่มิชอบก่อให้เกิดประเด็น

---

[1] พินัย ณ นคร. (2543, มิถุนายน). “กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์.” **บทบัณฑิตย์, 56, 2**. หน้า 1.

ปัญหา ดังนี้

4.1.1 การรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

4.1.1.1 ประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายวิธีพิจารณาความอาญา หมายถึง กฎหมายที่ว่าด้วยหลักเกณฑ์และวิธีการค้นหาความจริง อันเกี่ยวกับการกระทำความผิด และนำตัวผู้กระทำความผิดต่อกฎหมายอาญามาดำเนินการพิจารณา และลงโทษตามบทบัญญัติของกฎหมาย[2] แม้การกระทำความผิดอาญาจะเป็นการกระทำที่กระทบกระเทือนต่อสังคมโดยรวมก็ตาม แต่การดำเนินคดีอาญาก็ย่อมมีผลกระทบต่อสิทธิและเสรีภาพส่วนบุคคลโดยง่ายด้วย จึงต้องคำนึงถึงกฎหมายวิธีพิจารณาความอาญาที่ให้ความคุ้มครองสิทธิและเสรีภาพส่วนบุคคลในฐานะที่เขาเป็นส่วนหนึ่งของสังคม[3]

ในคดีอาญาพยานหลักฐานทุกชนิดรับฟังได้ ยกเว้นพยานหลักฐานที่ได้มาโดยมิชอบตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 สำหรับข้อมูลอิเล็กทรอนิกส์ ที่ได้มาจากการค้นที่มีหมายพยานหลักฐานดังกล่าวย่อมรับฟังได้ แต่ถ้าหากเป็นการค้นที่ไม่มีหมายพยานหลักฐานที่ได้ก็ไม่สามารถรับฟังได้ เพราะการจะเชื่อถือพยานหลักฐานนั้นเพียงใด ก็ขึ้นอยู่กับการชั่งน้ำหนักพยานหลักฐาน โดยกฎหมายได้วางหลักการชั่งน้ำหนักพยานหลักฐานเอาไว้ในมาตรา 227 คือ หลักพิสูจน์จนสิ้นสงสัย (in dubio pro reo) และได้บัญญัติรับรองไว้ในรัฐธรรมนูญ มาตรา 33 วรรคหนึ่ง ให้สันนิษฐานไว้ก่อนว่าผู้ต้องหาหรือจำเลยไม่มีความผิด โดยความสงสัยนั้นจะต้องเป็นความสงสัยในข้อเท็จจริง ไม่ใช่ความสงสัยในข้อกฎหมาย[4]

สำหรับประเทศไทยมีการให้หลักประกัน โดยบัญญัติรับรองไว้ในรัฐธรรมนูญ ในการให้ความคุ้มครองสิทธิและเสรีภาพเป็นหลัก รัฐจะใช้อำนาจล่วงละเมิดสิทธิเสรีภาพของประชาชนได้เป็นข้อยกเว้นในกรณีที่มีกฎหมายให้อำนาจ และมีเจ้าหน้าที่ของรัฐโดยชัดแจ้ง จะต้องมีกระบวนการควบคุมที่แน่ชัดสามารถตรวจสอบได้ ดังนั้นแม้อาชญากรรมที่เกิดขึ้นในปัจจุบันจะมีความร้ายแรงมาก จำเป็นจะต้องมีวิธีการในการแสวงหาพยานหลักฐานรูปแบบใหม่ๆ ซึ่งเป็นการใช้อำนาจในการปราบปรามอาชญากรรมของเจ้าหน้าที่ของรัฐ ก็ยังคงต้องคำนึงถึงหลักเกณฑ์นี้

การตรวจสอบเพื่อค้นหาข้อมูลในระบบอินเตอร์เน็ตหรือข้อมูลคอมพิวเตอร์นั้นก็เป็นกรณีที่มีความจำเป็นต้องมีหลักเกณฑ์ทางกฎหมายที่เพิ่มจากประมวลกฎหมายวิธีพิจารณาความ

---

[2] ณรงค์ ใจหาญ. (2543). **หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1** (พิมพ์ครั้งที่ 5). หน้า 22.

[3] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. (2539, มกราคม-มีนาคม). "แถลงการณ์เรื่อง การดักฟังทางโทรศัพท์." **รพีสาร, 14, 4**. หน้า 34.

[4] คณิต ณ นคร. เล่มเดิม. หน้า 56.

อาญากำหนดไว้ ซึ่งปัจจุบันยังไม่มีบัญญัติไว้ว่าควรดำเนินการอย่างไร นอกจากมีกำหนดไว้ในกฎหมายพิเศษบางฉบับ เช่นพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542

4.1.1.2 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 การฟอกเงิน (Money Laundering) คือการนำเงินหรือทรัพย์สินที่ได้มาจากการกระทำความผิดหรือได้มาโดยไม่ชอบด้วยกฎหมายมาเปลี่ยนสภาพเป็นเงินหรือทรัพย์สินที่ได้มาอย่างถูกต้อง เป็นการทำเงินสกปรกให้เป็นเงินสะอาด[5] เช่น เอาเงินที่ผิดกฎหมายไปลงทุนทำธุรกิจที่ถูกกฎหมาย โอนเงินออกนอกประเทศ เปิดบัญชีโดยใช้ชื่อปลอม ฯลฯ ไม่ว่าจะเป็นรูปแบบใดการกระทำดังกล่าวก็เพื่อที่จะปกปิดแหล่งที่มา และซุกซ่อนทรัพย์สิน รวมทั้งปกปิดผู้เป็นเจ้าของที่แท้จริง เพื่อทำให้ดูเสมือนว่าเป็นเงินหรือทรัพย์สินที่ถูกต้องตามกฎหมาย

ขั้นตอนของการฟอกเงินไม่ว่าจะเป็นการกระทำรูปแบบใดย่อมเหมือนกัน นั่นคือ ต้องมีการยักย้ายเงินหรือทรัพย์สิน ทำการปกปิดร่องรอยของเงินหรือทรัพย์สินดังกล่าวและนำเงินหรือทรัพย์สินนั้นกลับมาให้เสมือนเป็นเงินหรือทรัพย์สินที่ถูกต้องตามกฎหมาย

เนื่องจากปัจจุบันอาชญากรซึ่งกระทำความผิดกฎหมายบางประเภทได้นำเงินหรือทรัพย์สินที่เกี่ยวกับการกระทำความผิดนั้นมากระทำการในรูปแบบต่างๆ อันเป็นการฟอกเงิน เพื่อนำเงินหรือทรัพย์สินนั้นไปใช้ในการกระทำความผิดต่อไปอีก ทำให้ยากต่อการปราบปรามการกระทำความผิดกฎหมายเหล่านั้น และกฎหมายที่มีอยู่ก็ไม่สามารถปราบปรามการฟอกเงินหรือดำเนินการกับเงินหรือทรัพย์สินนั้นได้เท่าที่ควร ดังนั้นเพื่อเป็นการป้องกันและปราบปรามอาชญากรรม สมควรกำหนดมาตรการต่างๆ ให้สามารถดำเนินการป้องกันและปราบปรามการฟอกเงินให้ได้อย่างมีประสิทธิภาพ

หลักสากลที่นานาประเทศต่างถือเป็นหลักเกี่ยวกับกฎหมายฟอกเงิน ได้แก่ ให้ถือว่ากฎหมายฟอกเงินเป็นความผิดอาญา ที่มีการลงโทษทางอาญาและในขณะเดียวกันก็ให้มีโทษริบทรัพย์ในทางแพ่งด้วย มีวิธีการสืบสวนพิเศษโดยให้สถาบันการเงินจัดให้ลูกค้าแสดงตน ตรวจสอบกิจการของลูกค้า เก็บบันทึกข้อมูล และให้รายงานกิจการที่น่าสงสัยว่าจะเป็นการฟอกเงิน[6] นั่นคือ ธนาคารหรือสถาบันการเงินต้องจัดตั้งระบบการตรวจค้นหาข้อมูลของลูกค้าที่มีเหตุอันควรสงสัย และให้รายงานเหตุอันควรสงสัยนั้นให้เจ้าพนักงานผู้มีอำนาจหน้าที่ทราบ โดยไม่มีความผิดเรื่องเปิดเผยความลับของลูกค้าซึ่งจะเห็นได้ว่าเป็นมาตรการที่สำคัญมากในประเทศสหรัฐอเมริกา[7]

---

[5] สหัส สิงหวิริยะ. (2547). **คำอธิบายพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542** (พิมพ์ครั้งที่ 2). หน้า 3.

[6] สหัส สิงหวิริยะ. เล่มเดิม. หน้า 4.

[7] วาทิน คำทรงศรี. (2539). **การฟอกเงิน**. หน้า 102.

สำหรับกฎหมายไทยตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงินฯ มาตรา 46 ในกรณีที่มีเหตุอันควรเชื่อได้ว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อใช้ประโยชน์ในการกระทำความผิดฐานฟอกเงิน พนักงงานเจ้าหน้าที่ซึ่งเลขาธิการมอบหมายเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลแพ่งเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชี ข้อมูลทางการสื่อสาร เช่น การดักฟังโทรศัพท์ หรือข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็ได้ [8] นั่นคือต้องมีคำสั่งอนุญาตจากศาลแพ่งเสียก่อน จึงจะกระทำการตามมาตรา 46 นี้ได้

ในกรณีตามวรรคหนึ่ง ศาลจะสั่งอนุญาตให้พนักงานเจ้าหน้าที่ผู้ยื่นคำขอดำเนินการโดยใช้เครื่องมือหรืออุปกรณ์ใดๆ ตามที่เห็นสมควรก็ได้ แต่อนุญาตได้ไม่เกิดคราวละ 90 วัน [9]

เมื่อพิจารณาการกระทำความผิดมูลฐานตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542มาตรา 3 (1) ความผิดเกี่ยวกับยาเสพติด[10] ประกอบกับ พระราชบัญญัติมาตรการในการปราบปรามผู้กระทำผิดเกี่ยวกับยาเสพติด พ.ศ. 2534 คำว่า "มีเหตุอันควรสงสัย" ตามกฎหมายดังกล่าวมีขอเขตที่กว้างมาก โดยเริ่มต้นจากมีสิ่งบอกเหตุอย่างใดก็ได้ ไม่ว่าจะเป็นปรากฏการณ์หรือพฤติกรรมใดๆ ก็ได้ จนถึงเหตุที่มีพยานหลักฐานเพียงพอที่จะนำตัวจับกุมไปดำเนินคดี ส่งฟ้องและขอให้ศาลลงโทษ[11] จะเห็นได้ว่าข้อสันนิษฐานดังกล่าวเป็นข้อสันนิษฐานที่เอื้ออำนวยต่อการปฏิบัติหน้าที่ของเจ้าพนักงาน ดังนั้น เหตุอันควรสงสัยจึงไม่ควรเป็นปรากฏการณ์หรือพฤติกรรมใดๆ ก็ได้ แต่ควรจะเป็นปรากฏการณ์หรือพฤติกรรมที่อยู่ในวิสัยของปุถุชนที่สามารถคิดพิจารณาตามสามัญสำนึกว่าการจะเป็นเช่นนั้นได้ เพียงแต่ไม่มีข้อมูลบ่งชี้ จึงยังเป็นที่สงสัย

4.1.2 ปัญหาการรับฟังเป็นพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในศาลไทย

4.1.2.1 สถานะของข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในศาลไทย สภาพปัญหาที่เกิดขึ้นในปัจจุบัน คือ การจะนำเสนอข้อมูลอิเล็กทรอนิกส์เสนอต่อศาล จะนำเสนอในรูปของพยานหลักฐานชนิดใด หากพิจารณาจากลักษณะของพยานหลักฐานต่างๆแล้ว ข้อมูลอิเล็กทรอนิกส์น่าจะมีลักษณะที่สอดคล้องกับพยานหลักฐาน 2 ประเภทได้แก่ พยานเอกสาร หรือพยานวัตถุ ซึ่ง

---

[8] ดู พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, มาตรา 46 วรรคแรก.

[9] ดู พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, มาตรา 46 วรรคสอง.

[10] ดู พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, มาตรา 3 (1).

[11] วาทิน คำทรงศรี . เล่มเดิม. หน้า 73.

จำเป็นที่จะต้องกำหนดลักษณะของข้อมูลอิเล็กทรอนิกส์ให้ชัดเจนว่าเป็นพยานหลักฐานชนิดใด เนื่องจากการนำสืบ และวัตถุประสงค์ในการเสนอพยานหลักฐานทั้ง 2 ชนิดนั้นแตกต่างกัน

(1) เป็นพยานเอกสาร หมายถึง ข้อความในเอกสารที่มีการอ้างความหมายของข้อความเป็นพยาน[12]

พยานเอกสาร หมายถึง สิ่งซึ่งมีการบันทึกตัวอักษร ตัวเลข รูปรอยหรือเครื่องหมายซึ่งสามารถแสดงข้อความหรือความหมายอย่างใดอย่างหนึ่งให้ศาลตรวจดูได้ สิ่งนั้นจะเป็นอะไรก็ได้ และจะบันทึกไว้โดยวิธีเขียนด้วยมือ พิมพ์ พิมพ์ดีด แกะสลัก ถักร้อยหรือวิธีอื่นใดก็ได้[13]

ประมวลกฎหมายวิธีพิจารณาความอาญาและประมวลกฎหมายวิธีพิจารณาความแพ่ง ไม่ได้บัญญัติความหมายของคำว่า "เอกสาร" หรือ "พยานเอกสาร" เอาไว้ แม้จะมีการกล่าวถึงพยานเอกสารเอาไว้หลายชนิดในประมวลกฎหมายทั้ง 2 ฉบับ เช่น เอกสารมหาชน เอกสารราชการ หรือเอกสารเอกชน ความหมายของคำว่า "เอกสาร" นั้น ปรากฏอยู่ในประมวลกฎหมายอาญามาตรา 1 (7) หมายความว่า "กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น"

จะเห็นได้ว่าพยานเอกสารนั้น ประกอบด้วยตัววัตถุที่รองรับข้อความ และข้อความซึ่งเกิดขึ้นจากตัวอักษร ตัวเลข ผัง หรือแผนแบบต่างๆ ไม่ว่าจะโดยการพิมพ์ ถ่ายภาพ หรือวิธีอื่น ลงบนตัววัตถุที่รองรับ

ปกติแล้วพยานเอกสารจึงเป็นการบันทึกข้อความไว้บนกระดาษ โดยสิ่งที่ถูกบันทึกนั้นจะต้องสามารถสื่อความหมาย หรือแสดงข้อเท็จจริงบางอย่างได้ แต่ในบางครั้งก็อาจจะบันทึกลงบนวัสดุอื่นที่ไม่ใช่กระดาษก็ได้ เช่น ผ้า กระดาน แผ่นไม้ แผ่นหิน โลหะ ฯลฯ เพราะสิ่งที่จะพิสูจน์ข้อเท็จจริงคือสิ่งที่บันทึกอยู่บนนั้นเท่านั้น

ดังนั้น ข้อมูลอิเล็กทรอนิกส์ ที่มีลักษณะเป็นพยานเอกสารเมื่ออยู่ในรูปของการพิมพ์ออกมา (Print out)เป็นข้อความที่สื่อได้ด้วยตัวอักษร ตัวเลข หรือแผนแบบต่างๆ บนกระดาษ

ปัญหาที่ต้องพิจารณาต่อมาคือ จะนำเสนอข้อมูลอิเล็กทรอนิกส์ในฐานะ "ต้นฉบับ" หรือ "สำเนา" เพราะสำหรับระบบกฎหมายของประเทศคอมมอนลอว์ ก็จะรับฟังแต่เฉพาะต้นฉบับ โดยถือว่าเป็นพยานหลักฐานที่ถูกต้อง แท้จริงและน่าเชื่อถือที่สุด และหากเป็นสำเนาก็จะถือเป็น

---

[12] เข็มชัย ชุติวงศ์. (2543). **คำอธิบายกฎหมายลักษณะพยาน** (พิมพ์ครั้งที่ 7). หน้า 8.

[13] โสภณ รัตนากร. (2547). **คำอธิบายพยาน** (พิมพ์ครั้งที่ 7). หน้า 22.

พยานบอกเล่า (Hearsay) และสำหรับประเทศไทย แม้ปัญหาดังกล่าวจะไม่มี แต่ก็มีปัญหาในกรณีของคดีแพ่งที่กฎหมายบัญญัติให้ต้องใช้ต้นฉบับในการพิสูจน์ข้อเท็จจริงเท่านั้น

ตามบทบัญญัติของกฎหมายในเรื่องของการทำนิติกรรมสัญญา กฎหมายบัญญัติให้ต้องทำเป็นหนังสือ หรือมีหลักฐานเป็นหนังสือลงลายมือชื่อของผู้ทำนิติกรรมนั้น มิฉะนั้นจะไม่มีผลบังคับกันในทางกฎหมาย แต่ความเจริญก้าวหน้าของเทคโนโลยีในปัจจุบันมีการนำสื่ออิเล็กทรอนิกส์มาใช้ในการทำนิติกรรมสัญญา ได้แก่ โทรเลข เทเล็กซ์ โทรสาร และอินเตอร์เน็ต เรียกว่า "ธุรกรรมทางอิเล็กทรอนิกส์" เป็นการทำนิติกรรมสัญญาในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ไม่ได้ทำลงบนกระดาษเช่นในสมัยก่อน จึงมีการบัญญัติ พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ขึ้นมาใช้บังคับในกรณีนี้โดยเฉพาะ แต่ก็ยังมิได้มีการแก้ปัญหาการรับรองพยานหลักฐานในรูปของข้อมูลอิเล็กทรอนิกส์ในคดีอาญา ว่าเป็นพยานเอกสารหรือไม่แต่อย่างใด

(2) เป็นพยานวัตถุ หมายถึง วัตถุสิ่งของที่คู่ความอ้างเป็นพยาน การอ้างสถานที่ให้ศาลตรวจก็อยู่ในความหมายของพยานวัตถุ[14]

พยานวัตถุ ได้แก่ วัตถุหรือสิ่งใดที่อาจพิสูจน์ความจริงต่อศาลได้ โดยการตรวจดู มิใช่โดยการอ่านหรือการพิจารณาข้อความที่บันทึกไว้[15]

เมื่อพิจารณาเปรียบเทียบกับลักษณะของพยานเอกสารแล้ว จะเห็นว่า เอกสารฉบับหนึ่งอาจเป็นพยานเอกสารหรือพยานวัตถุก็ได้ ขึ้นอยู่กับวัตถุประสงค์ในการอ้าง นั่นคือหากต้องการให้ศาลพิจารณาข้อความในเอกสารนั้นก็เป็นพยานเอกสาร แต่ถ้าเป็นการอ้างเพื่อให้ศาลพิจารณารูปลักษณะของพยานหลักฐานชิ้นนั้นก็เป็นพยานวัตถุ โดยทั่วไปแล้วพยานวัตถุจะมีความสำคัญในคดีอาญามากกว่าในคดีแพ่ง เพราะเป็นพยานที่ดีที่สุดในการพิสูจน์ข้อเท็จจริงบางประการที่เกิดขึ้น ได้แก่ ของกลางต่างๆ

ในความเป็นจริงสื่ออิเล็กทรอนิกส์ไม่จำกัดอยู่แต่เฉพาะคอมพิวเตอร์ แต่มีทั้งกล้องถ่ายภาพ กล้องถ่ายภาพยนตร์ เครื่องบันทึกเสียง ซึ่งต่างก็มีลักษณะเป็นพยานวัตถุ ข้อมูลอิเล็กทรอนิกส์เป็นข้อมูลที่เกิดจากการประมวลผลโดยเครื่องคอมพิวเตอร์ เป็นพยานหลักฐานประเภทหนึ่งเช่นกัน

ดังนั้นการจะพิจารณาว่าสื่ออิเล็กทรอนิกส์เป็นพยานเอกสารหรือพยานวัตถุ จำเป็นที่จะต้องคำนึงถึงวัตถุประสงค์ของการนำสืบพยานหลักฐานชิ้นนั้นว่าจะเป็นการนำสืบตัววัตถุหรือนำ

---

[14] เข็มชัย ชุติวงศ์. เล่มเดิม. หน้า 8.

[15] โสภณ รัตนากร. เล่มเดิม. หน้า 22.

DPU

สืบข้อความ เช่น ต้องการนำสืบข้อเท็จจริงจากข้อความในเอกสารที่ได้พิมพ์ออกมาจากเครื่องคอมพิวเตอร์ ก็เป็นการนำสืบพยานหลักฐานที่เป็นเอกสาร หรือการนำสืบแถบบันทึกเสียงเป็นพยานวัตถุ[16] ศาลฎีกาเคยมีคำพิพากษา แสดงให้เห็นว่าแถบบันทึกเสียงสามารถตรวจสอบได้ด้วยการฟัง เพราะการนำสืบพยานวัตถุเป็นการรับรู้ด้วยประสาทสัมผัส รูป รส กลิ่น เสียง[17]

4.1.2.2 การจำกัดสถานะของพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ปัญหาสถานะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ว่าจะเป็นพยานเอกสารหรือพยานวัตถุนั้น มิได้มีบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา ในขณะที่กฎหมายได้บัญญัติถึงรูปแบบบังคับของการนำพยานหลักฐานเข้าสู่การพิจารณา โดยเรียกว่าเป็น “การจำกัดพยานหลักฐาน” โดยจำกัดสถานะของพยานหลักฐาน และการกำหนดหลักเกณฑ์การรับฟังและการสืบการจำกัดสถานะของพยานหลักฐาน เป็นการกำหนดชนิดของพยานหลักฐานตามที่กฎหมายบัญญัติเอาไว้ ที่จะใช้รับฟังได้ในคดีอาญา สำหรับปัญหาสถานะของพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์นั้น ก็ยังคงเป็นปัญหาที่สรุปไม่ได้ระหว่างพยานเอกสาร กรณีที่ Printout ออกมาเป็นเอกสาร หรือเป็นพยานวัตถุ กรณีที่อยู่ในรูปของฮาร์ดดิสก์

แต่ไม่ว่าจะเป็นพยานเอกสารหรือพยานวัตถุ ต่างก็เป็นพยานหลักฐานที่กฎหมายบัญญัติให้รับฟังได้ในคดีอาญา จึงเห็นว่าไม่น่าจะมีปัญหาในข้อนี้

4.1.2.3 ปัญหาการรับฟังพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ในชั้นศาล ดังได้กล่าวมาแล้วขั้นตอนในการค้น และยึดพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ นั้นต้องกระทำไปภายในขอบเขตที่มีกฎหมายให้อำนาจกระทำได้ เพราะในการดำเนินกระบวนการทางอาญาย่อมต้องก้าวล่วงสิทธิของบุคคลโดยไม่สามารถหลีกเลี่ยงได้ หากในขั้นตอนของการค้น และยึดพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ได้กระทำไปโดยมิชอบแล้วการรับฟังพยานหลักฐานดังกล่าวในศาลไทยก็อาจเกิดปัญหา โดยพิจารณาตามหลักกฎหมายต่อไปนี้

(1) หลักสันนิษฐานไว้ก่อนว่าเป็นผู้บริสุทธิ์ ในคดีอาญาให้สันนิษฐานไว้ก่อนว่าจำเลยหรือผู้ต้องหาไม่มีความผิด [18] โดยมีกฎหมายวิธีพิจารณาความอาญา มาตรา 227 วรรคสอง และรัฐธรรมนูญ มาตรา 33 วรรคหนึ่งที่บัญญัติรับรองหลักนี้ นั่นคือศาลจะต้องรับฟังพยานหลักฐานจนปราศจากความสงสัยอันควรว่าจำเลยได้กระทำผิดจริงจึงจะลงโทษจำเลย มิใช่จะยอมรับบังคับตาม

---

[16] คำพิพากษาฎีกาที่ 7155/2539 (ส่งเสริม) เล่ม 12. หน้า 176.

[17] โสภณ รัตนากร. เล่มเดิม. หน้า 449.

[18] คณิต ณ นคร. เล่มเดิม. หน้า 56.

พยานหลักฐานที่มีเหตุผลมากกว่าอย่างคดีแพ่งเท่านั้น ดังนั้นจึงเกิดหลักดังกล่าว และในกรณีสงสัยก็จะต้องยกประโยชน์แห่งความสงสัย (in dubio pro reo) ให้แก่จำเลย แต่ความสงสัยในที่นี้จำกัดเฉพาะความสงสัยในข้อเท็จจริงเท่านั้น จะไม่ใช้หลักนี้กับความสงสัยในข้อกฎหมาย

(2) หลักการไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ ในการรับฟังพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ไม่ว่าจะเป็นการรับฟังในรูปของพยานเอกสารหรือพยานวัตถุก็ตามรับฟังได้ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 และมีบทบัญญัติรับรองเอาไว้ในรัฐธรรมนูญ และต่างก็มีบทบัญญัติที่เหมือนกันคือยกเว้นไม่รับฟังกรณีที่เป็นพยานหลักฐานที่ได้มาโดยมิชอบ ซึ่งถือเป็นบทตัดพยานในกฎหมายไทย หมายความว่าพยานหลักฐานทุกชนิดที่จะรับฟังได้ จะต้องเป็นพยานหลักฐานที่ได้มาโดยชอบ

ดังนั้น พยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ที่จะใช้รับฟังได้ในศาล จึงต้องเป็นพยานหลักฐานที่ได้มาโดยชอบ ตามนัยของกฎหมาย นั่นคือ กรณีเป็นพยานหลักฐานที่ได้จากการค้นจะต้องมีหมายค้นโดยชอบเสียก่อน เจ้าพนักงานของรัฐจึงจะสามารถเข้าไปค้นข้อมูลอิเล็กทรอนิกส์นั้นๆมาใช้อ้างอิงเป็นพยานหลักฐานได้

(3) การกำหนดหลักเกณฑ์การรับฟังและการนำสืบ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 โดยหลักคือรับฟังพยานหลักฐานที่ได้มาโดยชอบ และยกเว้นไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ และกำหนดขอบเขตในการค้นหาความจริงในคดีอาญา ไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 231 ซึ่งเป็นการห้ามสืบพยานหลักฐานอันจะเป็นการเปิดเผยความลับ มาตรา 234 การให้การเป็นปฏิปักษ์ต่อตนเอง (Self incrimination) และมาตรา 132 การตรวจตัวผู้ต้องหาได้เมื่อเขายินยอม[19]

(4) หลักการพิสูจน์จนสิ้นสงสัย หลักประกันสิทธิของบุคคลตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ข้อ 11 (1) และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง ข้อ 14 (2) และรัฐธรรมนูญ มาตรา 33 การบัญญัติรับรองสถานะของบุคคลที่ยังไม่มีคำพิพากษาของศาลว่ามีความผิด ว่าจะต้องได้รับการปฏิบัติอย่างบุคคลธรรมดาทั่วไป จะปฏิบัติต่อเขาเสมือนกับเป็นผู้ที่กระทำความผิดแล้วมิได้ การจะเข้าค้นข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคล จึงต้องมีเหตุให้ทำการค้นได้ตามที่กฎหมายบัญญัติเอาไว้อย่างชัดเจน สำหรับประเทศไทยก็คือประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 69 เท่านั้น และผลจากหลักสันนิษฐานว่าเป็นผู้บริสุทธิ์จนกว่าศาลจะมีคำพิพากษา ทำให้ต้องมีการพิสูจน์การกระทำความผิดของผู้ถูกกล่าวหาจนสิ้นสงสัยตามมาตรา 227

---

[19] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 231 ,243 วรรคหนึ่ง และ 132

เนื่องจากการค้นข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคล เป็นการกระทำที่ละเมิดต่อสิทธิส่วนบุคคลอย่างร้ายแรง ทำให้ต้องมีเหตุที่กฎหมายบัญญัติเอาไว้อย่างชัดเจน ตามหลักการสันนิษฐานว่าเป็นผู้บริสุทธิ์จนกว่าศาลจะมีคำพิพากษาเสร็จเด็ดขาดว่ามีความผิด โดยจะต้องพิสูจน์จนสิ้นสงสัยโดยการชั่งน้ำหนักพยานหลักฐาน

ที่กล่าวมาล้วนเป็นหลักเกณฑ์การรับฟังและการสืบพยานหลักฐานโดยทั่วๆไปในคดีอาญา ซึ่งผู้เขียนเห็นว่าจะต้องนำมาเป็นหลักเกณฑ์ในการรับฟังและการสืบพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เช่นกัน

4.2 วิเคราะห์ปัญหาที่ไม่อาจคุ้มครองสิทธิในข้อมูลข่าวสารส่วนบุคคลได้อย่างชัดเจน

4.2.1 มาตรการทางกฎหมายในการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ แม้รัฐจะมีองค์กรหลายองค์กรในกระบวนการยุติธรรมที่มีหน้าที่ปราบปรามอาชญากรรม ซึ่งในบางประเทศให้ความสำคัญกับประสิทธิภาพของกระบวนการยุติธรรมที่มุ่งปราบปรามอาชญากรรมมากเกินไป จนทำให้หลักประกันสิทธิส่วนบุคคลน้อยลง แต่บางประเทศก็คำนึงถึงหลักประกันสิทธิส่วนบุคคลมากกว่าประสิทธิภาพของกระบวนการยุติธรรม โดยยอมสละความมีประสิทธิภาพของการปราบปรามอาชญากรรมบางประการไป เพื่อธำรงไว้ซึ่งสิทธิเสรีภาพส่วนบุคคล[20]

กฎหมายวิธีพิจารณาความอาญา หมายถึง กฎหมายที่ว่าด้วยหลักเกณฑ์และวิธีการค้นหาความจริง อันเกี่ยวกับการกระทำความผิดและนำตัวผู้กระทำความผิดต่อกฎหมายอาญามาดำเนินการพิจารณา และลงโทษตามบทบัญญัติของกฎหมาย[21] แม้การกระทำความผิดอาญาจะเป็นการกระทำที่กระทบกระเทือนต่อสังคมโดยรวมก็ตาม แต่การดำเนินคดีอาญาก็ย่อมมีผลกระทบต่อสิทธิและเสรีภาพส่วนบุคคลโดยง่ายด้วย จึงต้องคำนึงถึงกฎหมายวิธีพิจารณาความอาญาที่ให้ความคุ้มครองสิทธิและเสรีภาพส่วนบุคคลในฐานะที่เขาเป็นส่วนหนึ่งของสังคม[22]

สำหรับประเทศไทยมีการให้หลักประกัน โดยบัญญัติรับรองไว้ในรัฐธรรมนูญ ในการให้ความคุ้มครองสิทธิและเสรีภาพเป็นหลัก รัฐจะใช้อำนาจล่วงละเมิดสิทธิเสรีภาพของประชาชนได้เป็นข้อยกเว้นในกรณีที่มีกฎหมายให้อำนาจ และมีเจ้าหน้าที่ของรัฐโดยชัดแจ้ง จะต้องมีกระบวนการควบคุมที่แน่ชัดสามารถตรวจสอบได้ ดังนั้นแม้อาชญากรรมที่เกิดขึ้นในปัจจุบันจะมี

---

[20] ประธาน วัฒนวาณิชย์. (2520, พฤศจิกายน). "ระบบความยุติธรรมทางอาญา : แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม." **วารสารนิติศาสตร์ 9, 2**. หน้า 143.

[21] ณรงค์ ใจหาญ. เล่มเดิม. หน้า 22.

[22] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. แหล่งเดิม. หน้า 34.

ความร้ายแรงมาก จำเป็นจะต้องมีวิธีการในการแสวงหาพยานหลักฐานรูปแบบใหม่ๆ ซึ่งเป็นการใช้อำนาจในการปราบปรามอาชญากรรมของเจ้าหน้าที่ของรัฐ ก็ยังคงต้องคำนึงถึงหลักเกณฑ์นี้

4.2.2 ความจำเป็นในการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลในเครื่องอิเล็กทรอนิกส์ ปัจจุบันประเทศไทยยังไม่มีการวางหลักไว้ในกฎหมายส่วนสารบัญญัติสำหรับอาชญากรรมรูปแบบใหม่ๆ จึงต้องมีการแก้ไขปรับปรุงต่อไป เนื่องจากอาชญากรรมที่เกิดขึ้นในขณะนี้มีลักษณะที่แตกต่างไปจากอาชญากรรมพื้นฐาน หรืออาชญากรรมแบบดั้งเดิม เมื่อมีการกระทำความความผิดเกิดขึ้นแต่ยังไม่มีการบัญญัติกฎหมายเกี่ยวกับการกระทำความผิดดังกล่าวไว้โดยเฉพาะ เช่น อาชญากรรมเศรษฐกิจ ก็จำต้องใช้กฎหมายที่มีอยู่ลงโทษผู้กระทำความผิด ตามประมวลกฎหมายอาญาผู้กระทำความผิดก็อาจรับผิดแต่เพียงในฐานละเมิดต่อผู้เสียหายเท่านั้น แต่ความเสียหายที่เกิดอาจก่อให้เกิดความเสียหายต่อระบบเศรษฐกิจของประเทศ หรือในกรณีอาชญากรรมคอมพิวเตอร์ที่ผู้กระทำความผิดใช้เครื่องคอมพิวเตอร์ในการกระทำความผิด ก็เป็นเพียงการใช้คอมพิวเตอร์ในการกระทำความผิดเท่านั้น แต่การกระทำความเสียหายต่อข้อมูล ระบบโปรแกรม หรือชุดคำสั่ง ทำให้ผู้อื่นเสียหายก็ไม่สามารถนำมาปรับใช้ได้ เพราะอาจขัดกับหลัก “ไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย” อันเป็นหัวใจสำคัญของกฎหมายอาญา

ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานรูปแบบใหม่ที่กระการยุติธรรมจำเป็นต้องให้ความสนใจ เนื่องจากอาชญากรรมรูปแบบใหม่ๆ เช่น อาชญากรรมทางเศรษฐกิจ อาชญากรรมทางคอมพิวเตอร์ และอาชญากรรมบนเครือข่ายอินเตอร์เน็ต ฯลฯ ซึ่งอาชญากรรมเหล่านี้ถือเป็นอาชญากรรมที่มีลักษณะพิเศษ แตกต่างไปจากอาชญากรรมที่มีอยู่แต่เดิม จึงต้องให้ความสำคัญเพราะกฎหมายมักตามไม่เทคโนโลยีที่มีอยู่ ความล้ำหน้าของเทคโนโลยีแม้มีประโยชน์แต่ก็ก่อให้เกิดการกระทำความผิดที่ร้ายแรง เช่น อาชญากรรมทางเศรษฐกิจ ที่มีการแสดงออกไม่รุนแรงแต่กลับก่อให้เกิดความเสียหายในระดับประเทศ

พยานหลักฐานในคดีอาญามีความสำคัญมาก เพราะคดีอาญาต้องตัดสินด้วยพยานหลักฐานเสมอ[23] การแสวงหาพยานหลักฐานจึงมีความจำเป็น แต่พยานหลักฐานบางชนิด เช่น พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เป็นพยานหลักฐานที่ยากต่อการเข้าถึง และรวบรวม บางครั้งผลจากการแสวงหาพยานหลักฐานเหล่านี้อาจกระทบถึงสิทธิเสรีภาพของผู้อื่น ในคดีอาญาพยานหลักฐานทุกชนิดรับฟังได้ แต่ต้องเป็นไปตามหลักเกณฑ์ว่าด้วยการสืบและการรับฟัง[24] ดังนั้น

---

[23] คณิต ณ นคร. เล่มเดิม. หน้า 138.

[24] ดู ประมวลกฎหมายวิธีพิจารณาความอาญา, มาตรา 226.

เจ้าพนักงานของรัฐจึงต้องตระหนักและระมัดระวังทุกขั้นตอนในการแสวงหาพยานหลักฐานว่าจะต้องเป็นไปตามหลักเกณฑ์ว่าด้วยการสืบ เพื่อที่จะรับฟังได้เป็นพยานหลักฐาน

DPU

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

จุดประสงค์ในการแสวงหาพยานหลักฐานในคดีอาญานั้นก็เพื่อจะพิสูจน์ให้ได้ความว่าจำเลยเป็นผู้กระทำความผิดตามที่ถูกฟ้องหรือไม่ มีการกระทำอย่างไร ในเวลาใด สถานที่ใด และมีใครเป็นผู้เกี่ยวข้องบ้าง ซึ่งเป็นหลักเกณฑ์เกี่ยวกับพยานหลักฐานในคดีอาญาที่มีมาแต่เดิม สำหรับอาชญากรรมคอมพิวเตอร์ซึ่งเป็นการกระทำความผิดที่เกิดขึ้นจากความเจริญก้าวหน้าของเทคโนโลยี ไม่ว่าจะเป็นการกระทำความผิดต่อข้อมูลในคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ ซึ่งเป็นสิ่งที่ไม่มีรูปร่าง แตกต่างจากการก่ออาชญากรรมรูปแบบดั้งเดิมที่เป็นการกระทำต่อสิ่งที่มีรูปร่าง การให้ความหมายของคำว่า “อาชญากรรมคอมพิวเตอร์” จึงเป็นการให้ความหมายที่สอดคล้องกับสิ่งที่ผู้ให้ความหมายศึกษาและประสงค์จะให้ความคุ้มครอง ทำให้ไม่มีความหมายที่เป็นสากล แต่ก็มีความเห็นตรงกันประการหนึ่งก็คืออาชญากรรมคอมพิวเตอร์ เป็นการกระทำความผิดที่เกี่ยวเนื่องกับคอมพิวเตอร์ไม่ว่าจะในทางใดก็ตาม

การกระทำความผิดที่เกิดจากอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้น ก่อให้เกิดปัญหากับระบบกฎหมายภายในของประเทศต่างๆทั่วโลก เนื่องจาก การแสวงหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ถือเป็นมาตรการสำคัญ เพราะลักษณะของข้อมูลอิเล็กทรอนิกส์มีลักษณะที่แตกต่างจากพยานหลักฐานทั่วๆไป ก่อให้เกิดปัญหาในการค้น การยึด สถานะในทางพยานหลักฐานและการรับฟังเป็นพยานหลักฐานในศาล ไม่มีกฎหมายใช้บังคับ และไม่มีกฎหมายให้อำนาจเจ้าหน้าที่ของรัฐในการแสวงหาพยานหลักฐานดังกล่าว

ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 34 ได้ให้การรับรองคุ้มครองสิทธิของบุคคลในความเป็นอยู่ส่วนตัว (Right to privacy) ซึ่งไม่ใช่สิทธิในการใช้ชีวิตส่วนตัวเท่านั้น แต่ยังรวมไปถึงสิทธิในข้อมูลข่าวสารส่วนบุคคลด้วย ไม่ว่าข้อมูลนั้นจะจัดเก็บไว้ที่ใด การจะเข้าสู่ข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ โดยหลักแล้วจึงไม่สามารถทำได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เพื่อรักษาความมั่นคงของรัฐ ความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน และการจะจำกัดสิทธิของบุคคลจะต้องทำไปเท่าที่จำเป็น ตามเงื่อนไขที่รัฐธรรมนูญ กำหนดไว้ในมาตรา 29 ด้วย

ในปัจจุบันกฎหมายได้ให้อำนาจเจ้าหน้าที่ของรัฐสามารถเข้าสู่ข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46 และพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม พ.ศ. 2544 มาตรา 14 จัตวา ที่มีบทบัญญัติไปในทำนองเดียวกัน โดยกฎหมายทั้งสองฉบับดังกล่าวได้จำกัดฐานความผิดไว้เฉพาะความผิดฐานฟอกเงิน และความผิดเกี่ยวกับยาเสพติดเท่านั้น ไม่ครอบคลุมไปถึงการกระทำความผิดประเภทอื่นด้วย ดังนั้นการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลโดยประการอื่นนอกจากที่กล่าวมาแล้ว จึงเป็นการกระทำที่มิชอบด้วยกฎหมาย พยานหลักฐานที่ได้มาก็ถือเป็นพยานหลักฐานที่ได้มาโดยมิชอบ และไม่สามารถรับฟังได้ในศาล แต่รูปแบบการประกอบอาชญากรรมในปัจจุบันมีการพัฒนาไปมาก ไม่จำกัดอยู่แต่เฉพาะความผิดฐานฟอกเงิน หรือความผิดเกี่ยวกับยาเสพติด เช่น อาชญากรรมคอมพิวเตอร์ อาชญากรรมทางการเมือง หรือองค์กรอาชญากรรม ฯลฯ ซึ่งการกระทำความผิดดังกล่าวนั้นยากที่จะแสวงหาพยานหลักฐานมาเอาผิดกับผู้กระทำผิดได้ การเข้าสู่ข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ถือเป็นมาตรการพิเศษที่รัฐสามารถจะนำมาใช้แก้ปัญหาในการแสวงหาพยานหลักฐานได้เป็นอย่างดี แต่ก็จะต้องกระทำไปภายในขอบเขตที่รัฐธรรมนูญบัญญัติรับรองให้กระทำได้

เพื่อแก้ปัญหาการแสวงหาพยานหลักฐาน และการให้ความคุ้มครองข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคลในอาชญากรรมคอมพิวเตอร์ ในประเทศต่างๆ เช่น สหรัฐอเมริกา อังกฤษ และญี่ปุ่น ฯลฯ ได้มีการบัญญัติกฎหมายขึ้นมาใหม่ หรือแก้ไขปรับปรุงกฎหมายที่ใช้บังคับอยู่เพื่อแก้ปัญหาดังกล่าว

สำหรับประเทศไทยปัจจุบันยังไม่มีบทบัญญัติในประมวลกฎหมายอาญาให้ดำเนินคดีกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในรูปแบบต่างๆได้ และมาตรการในการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาก็ยังไม่มีบทบัญญัติเอาไว้ มีแต่เพียงกฎหมายพิเศษบางฉบับที่บัญญัติเอาไว้ แต่ก็จำกัดเฉพาะความผิดบางฐานเท่านั้น ไม่ครอบคลุมถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฐานอื่นๆ ด้วย ซึ่งจำเป็นที่จะต้องแก้ปัญหาทั้งการแสวงหาพยานหลักฐาน และการให้ความคุ้มครองข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลส่วนบุคคลในอาชญากรรมคอมพิวเตอร์ ไม่ว่าจะเป็นการบัญญัติกฎหมายขึ้นใหม่หรือแก้ไขปรับปรุงกฎหมายที่ใช้บังคับอยู่เพื่อแก้ปัญหาดังกล่าวดังเช่นในต่างประเทศ

5.2 ข้อเสนอแนะ

เนื่องจากการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ เป็นการกระทำที่ละเมิดสิทธิและเสรีภาพส่วนบุคคลอย่างร้ายแรง จึงจำเป็นที่จะต้องมีมาตรการที่ชัดเจน

โดยกฎหมายจะต้องบัญญัติประเภทของความผิด ที่จำเป็นจะต้องใช้วิธีการนี้ในการแสวงหาพยานหลักฐาน โดยเฉพาะอาชญากรรมคอมพิวเตอร์ เป็นการให้อำนาจเจ้าหน้าที่ในการรวบรวมพยานหลักฐาน และอำนาจที่ให้แก่เจ้าพนักงานสอบสวน เช่น อำนาจในการเชื่อมต่อเข้าไปในเครือข่ายอินเตอร์เน็ตไม่ว่าในกรณีใด เพื่อตรวจสอบเครื่องมือ อุปกรณ์ หรือเครื่องคอมพิวเตอร์ ซึ่งมีเหตุอันควรสงสัยว่าเกี่ยวข้องกับการกระทำความผิดอาชญากรรมคอมพิวเตอร์ ทั้งยังมีอำนาจมอบหมายให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์เหล่านั้น เพื่อช่วยเหลือได้ตามสมควร นั่นคือเจ้าหน้าที่ของรัฐจำเป็นที่จะต้องมีความรู้ในเรื่องคอมพิวเตอร์ดีพอที่จะดำเนินงานได้ และควรจะมีองค์กรกลางที่เป็นอิสระจากพนักงานสอบสวนเป็นผู้ทำหน้าที่ในการรวบรวมพยานหลักฐานประเภทนี้ เพื่อป้องกันการใช้อำนาจในทางมิชอบ

จากลักษณะของข้อมูลอิเล็กทรอนิกส์ ที่แตกต่างจากพยานหลักฐานชนิดอื่นๆ และสามารถเทียบเคียงได้กับพยานเอกสาร และพยานวัตถุ ซึ่งก่อให้เกิดปัญหาการจำแนกสถานะของพยานหลักฐานชนิดนี้ จนนำไปสู่ปัญหาในการนำเสนอต่อศาล จึงควรวางหลักกฎหมายกำหนดสถานะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ให้ชัดเจนว่าเป็นพยานหลักฐานชนิดใด และจะนำเสนอต่อศาลด้วยวิธีการใด โดยการกำหนดสถานะที่ชัดเจนของข้อมูลอิเล็กทรอนิกส์ให้ชัดเจนก็จะทำให้เข้าใจได้ว่าข้อมูลอิเล็กทรอนิกส์ เป็นวัตถุใดที่พนักงานสอบสวนจะทำการค้นได้ เพราะในการออกหมายอาญาไม่ว่าจะเป็นหมายค้น หรือยึดก็ตาม จำเป็นจะต้องมีการระบุสถานที่ค้น และวัตถุที่ค้นเอาไว้

สำหรับหมายอาญาก็จะต้องระบุเหตุในการค้น และยึด ควรวางหลักกฎหมายให้ชัดเจนโดยจะต้องไม่คลุมเครือ เช่นหมายค้นฮาร์ดแวร์ ซอฟท์แวร์ หรือข้อมูล โดยจะต้องระบุวิธีการ และระยะเวลาในการค้นให้ชัดเจนไม่มากไม่น้อยจนเกินไป รวมทั้งให้อำนาจเจ้าพนักงานสอบสวนทำการกักข้อมูลที่ค้นได้เพื่อใช้ประโยชน์ในการสอบสวนต่อไป ไม่ว่ากรณีใดการค้นข้อมูลอิเล็กทรอนิกส์ก็จะต้องมีหมายค้น แต่เพราะลักษณะของข้อมูลอิเล็กทรอนิกส์ เป็นพยานหลักฐานที่แก้ไขเปลี่ยนแปลงได้ง่าย ดังนั้นจึงควรมีมาตรการทางกฎหมายให้อำนาจเจ้าพนักงาน หรือมีอำนาจมอบหมายให้ผู้เชี่ยวชาญทำการเก็บกู้พยานหลักฐานที่ถูกทำลาย แก้ไขหรือเปลี่ยนแปลงไปให้กลับคืนมา โดยจะต้องวางหลักเกณฑ์ในการกู้ข้อมูลดังกล่าวให้ชัดเจน

ประเทศต่างๆต้องตระหนักถึงปัญหาอาชญากรรมคอมพิวเตอร์ว่าไม่ใช่ปัญหาของประเทศใดประเทศหนึ่ง แต่เป็นปัญหาระหว่างประเทศจึงควรให้ความร่วมมือกับประเทศต่างๆ หรือองค์การระหว่างประเทศในการหามาตรการแก้ไขปัญหา การวางหลักกฎหมายและการรวบรวมพยานหลักฐาน บัญญัติเป็นแนวทางไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา หรือบัญญัติกฎหมายพิเศษขึ้นมาใช้บังคับเป็นการเฉพาะ

ที่สำคัญต้องให้ความรู้แก่ประชาชนถึงปัญหาอาชญากรรมคอมพิวเตอร์ เพื่อให้เกิดความเข้าใจ และใช้คอมพิวเตอร์ได้อย่างถูกต้องและระมัดระวัง ทั้งคอยเป็นหูเป็นตาให้กับทางราชการในการค้นหาผู้กระทำความผิด

DPU

บรรณานุกรม

DPU

บรรณานุกรม

ภาษาไทย

หนังสือ

กุลพล พลวัน. (2538). **พัฒนาการสิทธิมนุษยชน** (พิมพ์ครั้งที่ 6). กรุงเทพฯ : วิญญูชน.

เกียรติขจร วัจนะสวัสดิ์. (2542). **คำอธิบายกฎหมายอาญา ภาค 1** . กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

เกียรติขจร วัจนะสวัสดิ์. (2547). **คำอธิบายหลักกฎหมายวิธีพิจารณาความอาญาว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณาพร้อมด้วยตัวบทและคำอธิบายมาตราที่แก้ไขเพิ่มเติมใหม่** (พิมพ์ครั้งที่ 3 แก้ไขใหม่). กรุงเทพฯ : หจก.จิรรัชการพิมพ์.

เข็มชัย ชุติวงศ์. (2543). **คำอธิบายกฎหมายลักษณะพยาน** (พิมพ์ครั้งที่ 7 ปรับปรุงใหม่). กรุงเทพฯ : นิติบรรณาการ.

คณิต ณ นคร. (2543). **กฎหมายอาญาภาคความผิด** (พิมพ์ครั้งที่ 7). กรุงเทพฯ : มหาวิทยาลัยธรรมศาสตร์.

คณิต ณ นคร. (2546). **กฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม-ปรับปรุงใหม่). กรุงเทพฯ : วิญญูชน.

คนึง ฤาไชย. (2530). **กฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 5). กรุงเทพฯ : มหาวิทยาลัยธรรมศาสตร์.

จีรนิติ หะวานนท์. (2544). **สิทธิทางวิธีพิจารณาความอาญาตามรัฐธรรมนูญ** (พิมพ์ครั้งที่ 2 ปรับปรุงใหม่). กรุงเทพฯ : วิญญูชน.

จิตติ ติงศภัทิย์. (2525). **กฎหมายอาญา ภาค 1**. กรุงเทพฯ : สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตสภา.

ณรงค์ ใจหาญ. (2547). **หลักกฎหมายวิธีพิจารณาความอาญา** (พิมพ์ครั้งที่ 7 ปรับปรุงใหม่). กรุงเทพฯ : วิญญูชน.

ทวีเกียรติ มีนะกนิษฐ์. (2543). **กฎหมายอาญา : หลักและปัญหา** (พิมพ์ครั้งที่ 2). กรุงเทพฯ : นิติธรรม.

บรรเจิด สิงคะเนติ. (2543). **หลักพื้นฐานของสิทธิเสรีภาพ และศักดิ์ศรีความเป็นมนุษย์ตามรัฐธรรมนูญ พ.ศ.2540**. กรุงเทพฯ : วิญญูชน.

ปีเตอร์ ที. เดวิส และแบรี่ ดี. เลวิส. (2543). **แรกเริ่มเรียนรู้ เรื่องรักษาความปลอดภัยให้ระบบคอมพิวเตอร์**. แปลจาก Computer Security Dummies โดย เจนศักดิ์ ตั้งพันธ์สุริยะ. กรุงเทพฯ : บริษัท ซีเอ็ดยูเคชั่น จำกัด.

วัชราภรณ์ สุริยาภิวัฒน์. (2543). **คอมพิวเตอร์เบื้องต้นและเทคนิคการเขียนโปรแกรม**. กรุงเทพฯ : ห้างหุ้นส่วนจำกัด ไทยเจริญการพิมพ์.

วาทิน คำทรงศรี. (2539). **การฟอกเงิน**. กรุงเทพฯ : วิญญูชน.

วรพจน์ วิศรุตพิชญ์. (2538). **สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540**. กรุงเทพฯ : วิญญูชน.

วีระ โลจายะ. (2524). **กฎหมายสิทธิมนุษยชน**. กรุงเทพฯ : มหาวิทยาลัยรามคำแหง.

สหัส สิงหวิริยะ. (2547). **คำอธิบายพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542** (พิมพ์ครั้งที่ 2). กรุงเทพฯ : นิติธรรม.

แสวง บุญเฉลิมวิภาส. (2542). **หลักกฎหมายอาญา** (พิพม์ครั้งที่ 2). กรุงเทพฯ : โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลักธรรมศาสตร์.

หยุด แสงอุทัย. (2523). **กฎหมายอาญาภาค 1** (พิพม์ครั้งที่ 14). กรุงเทพฯ : สำนักพิมพ์หาวิทยาลัยธรรมศาสตร์.

หฤทัย หงส์สิริ และมานิตย์ จุมปา. (2542). **คำอธิบายข้อมูลข่าวสารของทางราชการ**. กรุงเทพฯ : นิติธรรม.

อุดม รัฐอมฤต นพนิธิ สุริยะ และบรรเจิด สิงคะเนติ. (2544). **การอ้างศักดิ์ศรีความเป็นมนุษย์หรือใช้สิทธิและเสรีภาพของบุคคลดังกล่าวตามมาตรา 28 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2540**. กรุงเทพฯ : สำนักงานศาลรัฐธรรมนูญ.

บทความ

"การสัมนนาทางวิชาการเรื่อง ศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของบุคคลตามรัฐธรรมนูญ." **วารสารศาลรัฐธรรมนูญ, 1,3.** (2542, กันยายน-ธันวาคม). หน้า 37-48.

กุลพล พลวัน. (2540, มิถุนายน). "กลไกตามรัฐธรรมนูญในการคุ้มครองสิทธิและเสรีภาพของประชาชน." **บทบัณฑิตย์, 52, 2.** หน้า 36-52.

จิรนิติ หะวานนท์. (2527, พฤษภาคม-มิถุนายน). "หลักการไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ : เปรียบเทียบระหว่างกฎหมาย อเมริกา และกฎหมายเยอรมัน." **ดุลพาห, 31, 3.** หน้า 34-52.

นิติ ผดุงชัย. (2532,มิถุนายน). “กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับ Computer.” **วารสารอัยการ**, หน้า 86-88.

ณรงค์ ใจหาญ. (2540, มิถุนายน). “หลักประกันสิทธิของประชาชนในคดีอาญาใหม่ : ปัจจุบันและทศวรรษหน้า 2540-2550.” **บทบัณฑิตย์, 53, 2.** หน้า 64-86.

ประธาน วัฒนวาณิชย์. (2520, พฤศจิกายน). “ระบบความยุติธรรมทางอาญา : แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม.” **วารสารนิติศาสตร์, 9,2**. หน้า 143-156.

สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. (2539, มกราคม-มีนาคม). ”แถลงการณ์เรื่อง การดักฟังทางโทรศัพท์.” **รพีสาร, 14, 4.** หน้า 34- 54.

วิทยานิพนธ์

กิตติพันธุ์ เกียรติสุนทร. (2538). **มาตรการทางอาญาในการคุ้มครองข้อมูลส่วนบุคคล**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

กิตติมา ประคุณคดี. (2533). **การดักฟังทางโทรศัพท์โดยเจ้าพนักงาน**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

กงจักร โพธิ์พร้อม. (2529). **ปัญหากฎหมายมหาชนบางประการเกี่ยวด้วยการควบคุมการใช้ข่าวสารโดยเครื่องคอมพิวเตอร์**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

จงรัก จุทานนท์. (2524). **การคุ้มครองสิทธิของประชาชนต่อการถูกจับและตรวจค้นที่ไม่ชอบธรรม**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

ศุภฤกษ์ ศุกรเสพย์. (2545). **การค้นในที่รโหฐานของเจ้าพนักงานป้องกันและปราบปรามยาเสพติด**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

สุชาติ ตระกูลเกษมสุข. (2543). **การคุ้มครองสิทธิส่วนบุคคลจากการดักฟังทางโทรศัพท์**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์. กรุงเทพฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

DPU

ภาษาต่างประเทศ

BOOKS

Dando, Shigemitsu. (1965). **Japanese Criminal Procedure**. South Hackensack,NJ: Fred Rothman & Co.

May, Richard. (1999). **Criminal Evidence**. London : Sweet & Maxwell Ltd.

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

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

DPU