การแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญา

ร้อยตรี พิทักษ์พงศ์ ตันบุญเอก

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรนิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ปรีดี พนมยงค์
มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2557

Searching Computer Crime Evidence

Sub. Lt. PHITHAKPHONG TANBOONEK

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Laws

Department of Law

Pridi Banomyong Faculty of Law, Dhurakij Pundit University

2014

หัวข้อวิทยานิพนธ์ การแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญา
ชื่อผู้เขียน ร้อยตรี พิทักษ์พงศ์ ตันบุญเอก
อาจารย์ที่ปรึกษา อาจารย์ ดร.อุทัย อาทิเวช
สาขาวิชา นิติศาสตร์
ปีการศึกษา 2556

บทคัดย่อ

การแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาไทยในปัจจุบันส่วนใหญ่จะใช้วิธีการแสวงหาพยานหลักฐานด้วยวิธีการ เข้าค้น เพื่อยึดพยานเอกสารหรือพยานวัตถุ จากเคหสถานของบุคคล ด้วยวิธีการจับ การค้นเพื่อยึดพยานเอกสารหรือพยานวัตถุจากตัวบุคคล หรือจากร่างกายมนุษย์เท่านั้น ซึ่งยังไม่เพียงพอ เนื่องจากปัจจุบันคอมพิวเตอร์มีส่วนสำคัญในชีวิตประจำวันของมนุษย์โดยเฉพาะในการติดต่อสื่อสารถึงกันซึ่งอาจใช้เป็นสื่อในการติดต่อสื่อสารในการกระทำผิดอาญาร้ายแรงฐานต่างๆ โดยพยานหลักฐานทางคอมพิวเตอร์จำเป็นต้องใช้มาตรการการแสวงหาพยานหลักฐานที่เป็นการใช้มาตรการในการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ ซึ่งประมวลกฎหมายวิธีพิจารณาความอาญาของไทยก็ไม่ได้ระบุเรื่องการแสวงหาพยานหลักฐานทางคอมพิวเตอร์โดยวิธีการดังกล่าวไว้แต่อย่างใดทำให้เจ้าพนักงานเสียโอกาสสำคัญในการที่จะได้มาซึ่งพยานหลักฐานที่จะเอาผิดแก่ผู้กระทำผิดได้ และแม้ว่าประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1 จะเปิดช่องให้รับฟังพยานหลักฐานที่เกิดขึ้นโดยชอบแต่ได้มาโดยมิชอบ ที่ศาลอาจรับฟังได้หากพยานหลักฐานนั้นจะเป็นประโยชน์ต่อการอำนวยความยุติธรรมมากกว่าผลเสีย แต่เพื่อเป็นการอำนวยซึ่งความยุติธรรมของกระบวนการยุติธรรมทางอาญาพยานหลักฐานที่ได้มาโดยมิชอบด้วยกฎหมายไม่ว่าโดยประการใดๆศาลจะต้องปฏิเสธไม่รับฟังโดยถือว่าเป็นหลักการตัดพยานหลักฐาน (Exclusionary Rule) ชนิดหนึ่ง การรับฟังพยานหลักฐานที่ไม่ชอบด้วยกฎหมายเหมือนกับการยอมรับเอาผลไม้ของต้นไม้ที่มีพิษ ศาลจึงไม่รับฟังพยานหลักฐานที่เป็นผลมาจากการกระทำที่ไม่ชอบด้วยกฎหมาย ประกอบกับปัจจุบันมาตรการแสวงหาพยานหลักฐานโดยใช้มาตรการในการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ ก็ได้ถูกบัญญัติไว้ในพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ซึ่งให้อำนาจเจ้าพนักงานคดีพิเศษดำเนินการเพื่อให้ได้มาซึ่งข้อมูลที่เป็นการสื่อสารทางโทรศัพท์รวมทั้งข้อมูลอิเล็กทรอนิกส์โดยมีการตรวจสอบ กลั่นกรองและถ่วงดุลอำนาจดังกล่าวตามบทบัญญัตินี้แต่อำนาจดังกล่าวก็มีเฉพาะในคดีพิเศษตามพระราชบัญญัตินี้เท่านั้นซึ่งไม่ครอบคลุมทุกฐานความผิดในขณะที่

พยานหลักฐานทางคอมพิวเตอร์นั้นอาจเกี่ยวข้องกับฐานความผิดอื่นที่ไม่ใช่การกระทำผิดที่เป็นคดีพิเศษก็ได้เช่นจดหมายอิเล็กทรอนิกส์ที่ใช้ตกลงกันกระทำความผิดทางอาญาฐานต่างๆ ความผิดฐานเรียกค่าไถ่ ความผิดฐานรีดเอาทรัพย์ ความผิดเกี่ยวความมั่นคง เป็นต้น จึงสมควรเพิ่มมาตรการในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์โดยการดักฟังและการได้มาซึ่งข้อมูลอีเล็กทรอนิกส์ ลงในประมวลกฎหมายวิธีพิจารณาความอาญาของไทย ทั้งนี้เพื่อรับรองไว้ให้กระบวนการยุติธรรมนั้นชอบด้วยกฎหมายและเกิดความรวดเร็วความถูกต้องในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์และสามารถเข้าถึงพยานหลักฐานดังกล่าวได้และจะครอบคลุมทุกฐานความผิดไม่ใช่เฉพาะคดีพิเศษเพียงอย่างเดียว

Thesis Title Searching Computer Crime Evidence
Author Sub. Lt. Phithakphong Tanboonek
Thesis Advisor Dr. Utai Athiwet
Department Law
Academic Year 2013

ABSTRACT

Searching evidence according to the present Thai Criminal Procedure Code mostly relies on the method of searching evidence by entering a person's residence to search and confiscate documentary evidence or physical evidence from that person or from human bodies only. This method is not efficient enough since nowadays computers play an important role in human daily life, especially for communication. Thus, computers can become the media of communication in serious criminal offences. In order to search computer evidence, the measure of searching evidence by eavesdropping and acquiring electronic data is required. However, the Thai Criminal Procedure Code does not specify the search computer evidence by such a method. As a result, investigating officers lose their important opportunities to acquire evidence to prosecute the offenders. Besides, even though section 226/1 of the Criminal Procedure Code allows the court to accept the hearing of evidence which occur but are not acquired properly in case that the usefulness of such evidence for the delivery of justice overpowers its negativity. Nevertheless, for the righteousness of criminal justice procedure, the evidence which is unlawfully acquired in any case will be denied by the court according to the exclusionary rule. The hearing of unlawful evidence is like the acceptance of a fruit of a poisonous tree. Consequently, the court denies the hearing of evidence which is the consequences of illegal acts. Also, presently, the measure of searching evidence by eavesdropping and acquiring electronic data is included in the Special Case Investigation Act B.E. 2547, which grants special case officers the power to proceed in order to acquire the data from communication by phone and electronic data. In this case, there will be an investigation, scrutiny and balance of such power according to the act. However, the power is only granted for special cases according to this particular act, not covering all offences. As for computer evidence, they can be related to other

offences which are not special cases; for instance, electronic letters which are used for the agreement to commit various crimes including ransom, extortion and threat to stability. Therefore, it is recommended that the measure of searching computer evidence by eavesdropping and acquiring electronic data is added in the Thai Criminal Procedure Code in order to make the justice procedure lawful and to allow the search computer evidence to be fast, accurate and accessible. Also, this measure should cover all offences, not only special cases.

กิตติกรรมประกาศ

ขอขอบพระคุณ อาจารย์ ดร.อุทัย อาทิเวช ที่ท่านให้โอกาสกระผมได้ทำการศึกษาค้นคว้าในหัวข้อวิทยานิพนธ์ ซึ่งเป็นหัวข้อที่กระผมให้ความสนใจอย่างมากและทุ่มเทในการค้นคว้า และหาข้อมูลต่างๆ เพื่อทำวิทยานิพนธ์ดังกล่าว ซึ่งท่านได้สละเวลาอันมีค่ายิ่งในการให้ความรู้ คำแนะนำติดตามความคืบหน้าในการทำวิทยานิพนธ์และขอขอบพระคุณประธานกรรมการวิทยานิพนธ์ คือ ศาสตราจารย์ ดร. สุรศักดิ์ ลิขสิทธิ์วัฒนกุล ที่ได้สละเวลาเป็นประธานกรรมการวิทยานิพนธ์ฉบับนี้ ตลอดจนขอขอบพระคุณกรรมการวิทยานิพนธ์ คือ ศาสตราจารย์ ดร. ทวีเกียรติ มีนะกนิษฐ และ รองศาสตราจารย์อัจฉรียา ชูตินันทน์ ซึ่งเป็นผู้ที่มีความเชี่ยวชาญอย่างยิ่งเกี่ยวกับกฎหมายวิธีพิจารณาความอาญา สำหรับคำแนะนำต่างๆ ที่ท่านอาจารย์ให้ไว้รวมถึงขอขอบคุณห้องสมุดทุกแห่งที่กระผมได้ไปทำการค้นคว้า โดยเฉพาะห้องสมุดของมหาวิทยาลัยธุรกิจบัณฑิตย์ ที่เป็นแหล่งรวมข้อมูล และมีหนังสือเกี่ยวกับกฎหมายวิธีพิจารณาความอาญาใหม่ๆ อยู่เป็นจำนวนมาก ไม่ว่าจะเป็นหนังสือกฎหมายวิธีพิจารณาความอาญาไทยและหนังสือกฎหมายวิธีพิจารณาความอาญาต่างประเทศ รวมทั้งขอขอบคุณครอบครัวตันบุญเอก และที่ทำงานของกระผมที่เป็นกำลังใจและให้โอกาสกระผมอยู่ตลอดเวลา

อนึ่ง หากวิทยานิพนธ์ฉบับนี้มีคุณค่าและมีประโยชน์ต่อการศึกษาหรือต่อวงการนิติศาสตร์ กระผมขอมอบความดีทั้งหมดให้กับบิดา มารดา และครูบาอาจารย์ทุกๆ ท่าน ที่ประสิทธิ์ประสาทความรู้ให้ส่วนความผิดพลาดและข้อบกพร่องทั้งหมด อันเกิดจากวิทยานิพนธ์ฉบับนี้ กระผมขอน้อมรับไว้แต่เพียงผู้เดียว

ร้อยตรี พิทักษ์พงศ์ ตันบุญเอก

สารบัญ

สารบัญ (ต่อ)

บทที่ **หน้า**

สารบัญ (ต่อ)

บทที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันคอมพิวเตอร์และอินเทอร์เน็ตได้เข้ามาเป็นส่วนหนึ่งที่สำคัญในชีวิตของมนุษย์ และมนุษย์ก็ใช้เวลาหลายชั่วโมงในแต่ละวันอยู่หน้าจอคอมพิวเตอร์เพื่อส่งและรับจดหมายอิเล็กทรอนิกส์ (e-mail) ท่องอินเทอร์เน็ต เก็บข้อมูลในคอมพิวเตอร์ และเข้าร่วมกิจกรรมอื่นๆ อีกมากมาย แต่ในทางกลับกันคอมพิวเตอร์ก็ได้ถูกนำมาใช้ในการกระทำความผิดของอาชญากร ไม่ว่าจะเป็นการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) เพื่อข่มขู่ว่าจะทำอันตรายแก่ชีวิต หรือในบางครั้งคอมพิวเตอร์ก็ถูกใช้เป็นอุปกรณ์อำนวยความสะดวกในการเก็บพยานหลักฐานในการประกอบอาชญากรรมหรือพยานหลักฐานในการเอาผิดแก่ผู้กระทำความผิด เช่น การเก็บข้อมูลเกี่ยวกับการฟอกเงินและการกระทำความผิดอื่นๆ ซึ่งข้อมูลที่อยู่ในคอมพิวเตอร์เหล่านี้ถือว่าเป็นหลักฐานทางอิเล็กทรอนิกส์ (ดิจิตอล) ที่สามารถนำไปใช้ระบุตัวผู้กระทำความผิด ตลอดจนเป็นหลักฐานในชั้นศาลได้[1] และศาลก็สามารถใช้ดุลพินิจรับฟังได้ แต่อย่างไรก็ตาม ด้วยเหตุที่ข้อมูลในคอมพิวเตอร์ที่เป็นหลักฐานดิจิตอลมีความละเอียดอ่อนและความสลับซับซ้อนอย่างมาก การที่จะเข้าถึงหรือทำให้พยานหลักฐานดังกล่าวมีน้ำหนักน่าเชื่อถือได้นั้น ในการแสวงหาพยานหลักฐานจึงจำเป็นที่จะต้องมีวิธีการที่เหมาะสมเพื่อให้ได้มาซึ่งพยานหลักฐานที่มีความแท้จริง ถูกต้องสมบูรณ์ น่าเชื่อถือ และรับฟังเป็นพยานหลักฐานได้ และบุคคลผู้ดูแลหรือเก็บพยานหลักฐานดังกล่าวก็ต้องเป็นผู้เชี่ยวชาญ (Providing Expert) ซึ่งได้รับการฝึกอบรมในด้านนี้โดยมากแล้ว

การแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาไทยในปัจจุบันจะมีเฉพาะการใช้วิธีการแสวงหาพยานหลักฐานด้วยวิธีการ เข้าค้น เพื่อยึดพยานเอกสารหรือพยานวัตถุ จากเคหสถานของบุคคล การใช้วิธีการแสวงหาพยานหลักฐานด้วยวิธีการจับการค้นเพื่อยึดพยานเอกสารหรือพยานวัตถุจากตัวบุคคล การแสวงหาพยานหลักฐานจากร่างกายมนุษย์เท่านั้น โดยเฉพาะในเรื่องการค้นในที่รโหฐานของเจ้าพนักงาน เพื่อให้ได้พยานหลักฐาน

---

[1] Computer Forensic คือ การค้นหาและเก็บหลักฐานทางดิจิตอลที่อยู่ในอุปกรณ์คอมพิวเตอร์ เช่น ไฟล์ที่อยู่ใน พีซี โน้ตบุ๊ก หรือพีดีเอ เป็นต้น หรือหลักฐานดิจิตอลที่ถูกสร้างจากระบบคอมพิวเตอร์ ซึ่งข้อมูลเหล่านี้สามารถนำไปใช้ระบุผู้กระทำผิด จนถึงเป็นหลักฐานในชั้นศาลได้.

ซึ่งถือว่าเป็นการแสวงหาพยานหลักฐานอย่างหนึ่ง แต่การแสวงหาพยานหลักฐานดังกล่าวจะมีลักษณะไปในทางกายภาพเสียมากกว่า กล่าวคือเป็นการค้นเพื่อพบหรือยึดสิ่งของซึ่งจะใช้เป็นพยานหลักฐาน หรือสิ่งของที่มีไว้เป็นความผิดหรือได้มาโดยผิดกฎหมาย หรือมีเหตุอันควรสงสัยว่าได้ใช้หรือตั้งใจจะใช้ในการกระทำผิด หรือเหตุอื่นๆ ตามกฎหมาย แต่การค้นข้อมูลคอมพิวเตอร์ค่อนข้างมีความสลับซับซ้อนและละเอียดอ่อนอย่างมาก ทั้งยังโยงใยหลายเครือข่ายซึ่งข้อมูลนั้นอาจไม่อยู่ในคอมพิวเตอร์นั้นก็ได้ ดังนี้อาจเกิดปัญหาได้ว่าเมื่อเจ้าพนักงานเข้าไปค้นในที่รโหฐานใดเพื่อค้นหาพยานหลักฐานทางอิเล็กทรอนิกส์ (ดิจิตอล) ที่อยู่ในคอมพิวเตอร์ด้วยเหตุที่ว่าคอมพิวเตอร์นั้นสามารถที่จะเก็บข้อมูลได้เป็นจำนวนมากและมีความสลับซับซ้อนเชื่อมโยงหลายเครือข่ายจึงยากแก่การที่จะค้นพบพยานหลักฐานทางอิเล็กทรอนิกส์ (ดิจิตอล) ที่อยู่ในคอมพิวเตอร์นั้นได้และบางครั้งข้อมูลดังกล่าวอาจถูกลบไปโดยผู้กระทำผิด ซึ่งในกรณีที่คอมพิวเตอร์นั้นเชื่อมโยงหลายเครือข่ายข้อมูลนั้นอาจไม่อยู่ในคอมพิวเตอร์นั้นก็ได้ ทำให้ยากต่อการค้นพบจึงเป็นปัญหาอย่างมากในแง่การค้นหาพยานหลักฐาน ยกตัวอย่างเช่น ในกรณีที่มีการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) เพื่อข่มขู่ว่าจะทำอันตรายแก่ชีวิตโดยมิได้ระบุชื่อหรือข้อมูลเกี่ยวกับการกระทำผิดเกี่ยวกับการฟอกเงิน ข้อมูลที่เกี่ยวกับการกระทำผิดทางอาญาอื่นๆ ผู้กระทำผิดอาจลบข้อมูลดังกล่าวไปหรือข้อมูลนั้นอาจไม่ได้อยู่ในคอมพิวเตอร์เครื่องนั้นซึ่งข้อมูลดังกล่าวอาจอยู่ในคอมพิวเตอร์เครื่องอื่นที่เชื่อมโยงหลายเครือข่ายกับคอมพิวเตอร์นั้นทำให้ยากต่อการค้นพบข้อมูลดังกล่าวได้ การที่จะตามยึดเครื่องคอมพิวเตอร์ทุกเครื่องที่อาจเกี่ยวข้องหรือเชื่อมโยงเครือข่ายกับคอมพิวเตอร์ดังกล่าวมาตรวจสอบทุกเครื่องก็ย่อมทำได้ยาก การจะยึดเครื่องคอมพิวเตอร์ดังกล่าวมาตรวจสอบเพียงเครื่องเดียวก็อาจจะไม่เกิดประโยชน์เพราะข้อมูลดังกล่าวก็อาจไม่อยู่ในคอมพิวเตอร์เครื่องนั้นก็ได้ หรือการเข้าไปขอตรวจสอบข้อมูลที่ถูกส่งจากเครื่องคอมพิวเตอร์นั้นไปยังผู้บริหารเครือข่าย (Network Administrator) หรือผู้ให้บริการเครือข่าย ผู้บริหารเครือข่ายหรือผู้ให้บริการเครือข่ายก็อาจไม่ยอมให้ความร่วมมือเพราะเจ้าพนักงานอาจทำให้เกิดความเสียหายแก่ระบบเครือข่ายของเขาก็ได้ และผู้ให้บริการในฐานะบุคคลที่สามเขาก็ไม่กล้าที่จะเปิดเผยข้อมูลของผู้ใช้บริการของตนได้อย่างเต็มที่เพราะอาจถูกผู้ใช้บริการฟ้องคดีทางแพ่งอีก เนื่องจากไปละเมิดสิทธิของเขา ทำให้เป็นปัญหาอย่างมากในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญา โดยในประเทศอเมริกาก็ได้มีหลักเกณฑ์เกี่ยวกับการแสวงหาพยานหลักฐานทางคอมพิวเตอร์โดยกฎหมายของอเมริกาก็มีการเข้าค้นสื่อที่ใช้ในการเก็บข้อมูล (อาทิเช่นคอมพิวเตอร์หรือฮาร์ดแวร์) และเข้ายึดสื่อที่ใช้เก็บข้อมูลคอมพิวเตอร์นั้นหรือทำการสำเนาข้อมูลดังกล่าวไว้ก็ได้[2] และมีการให้อำนาจแก่เจ้าพนักงานในการตรวจสอบการเชื่อมโยงเครือข่ายของคอมพิวเตอร์นั้น

[2] Federal Rules of Criminal Procedure Rule 41 (E) (2) (B).

โดยเจ้าพนักงานอาจแอบติดตั้ง Pen Register และ Trap and Trace โดยขอความร่วมมือจากผู้ให้บริการในการติดตั้งอุปกรณ์ดังกล่าวเพื่อประโยชน์ในการแสวงหาพยานหลักฐาน ซึ่ง Pen Register จะบันทึกข้อมูลทางอิเล็กทรอนิกส์ที่ถูกส่งออกไปและ Trap and Trace จะบันทึกข้อมูลทางอีเล็กทรอนิกส์ที่ถูกส่งเข้ามายังคอมพิวเตอร์ ซึ่งจะเป็นข้อมูลเกี่ยวกับสารสนเทศที่อยู่ที่เป็นแหล่งที่มาของจดหมายอิเล็กทรอนิกส์และเวลาที่ถูกส่งเข้ามาหรือส่งออกไป โดยเจ้าพนักงานอาจแจ้งแก่ผู้ใช้บริการได้ในภายหลังถึงการติดตั้งนั้นก็ได้ โดยอุปกรณ์ดังกล่าวเจ้าพนักงานก็ต้องยื่นคำขอต่อศาลซึ่งหากเจ้าพนักงานทำการฝ่าฝืนก็จะมีโทษทางอาญาและพยานหลักฐานนั้นก็รับฟังไม่ได้และคำสั่งให้ติดตั้งอุปกรณ์ดังกล่าวก็ใช้ได้ทุกเขตอำนาจศาล[3] และการดัก (Sniffer) ข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ (เช่นเนื้อหาจดหมายอิเล็กทรอนิกส์) ก็ทำได้ถ้าได้รับอนุญาตจากศาลหากเป็นความผิดอาญาที่ร้ายแรงซึ่งหากเจ้าพนักงานทำการฝ่าฝืนก็จะมีโทษทางอาญาและพยานหลักฐานนั้นก็รับฟังไม่ได้เช่นกัน[4] นอกจากนี้ยังมีการบังคับโทษทางอาญาที่เข้มงวดในกรณีที่มีการเปลี่ยนแปลงหรือทำลายหลักฐานที่บันทึกไว้ในรูปของเอกสารอิเล็กทรอนิกส์รวมทั้งสื่อที่เก็บข้อมูลอิเล็กทรอนิกส์นั้น[5] ซึ่งถือว่าช่วยเอื้อประโยชน์ในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ของเจ้าพนักงานอย่างมาก

อย่างไรก็ตามในประมวลกฎหมายวิธีพิจารณาความอาญาของไทย ก็ไม่ได้ระบุการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในลักษณะดังกล่าวแต่อย่างใด จึงเห็นได้ว่าการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ของเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญาของไทยนั้น ยังมีปัญหาว่าเจ้าพนักงานนั้นยังไม่อาจเข้าถึงพยานหลักฐานที่เป็นข้อมูลทางคอมพิวเตอร์ได้เพราะข้อมูลคอมพิวเตอร์มีความละเอียดอ่อนและสลับซับซ้อนเชื่อมโยงหลายเครือข่ายมากทำให้การค้นหาพยานหลักฐานดังกล่าวเป็นไปได้ยากและประมวลกฎหมายวิธีพิจารณาความอาญาของไทยก็มิได้กำหนดอำนาจและวิธีการที่เหมาะสมในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์แก่เจ้าพนักงาน ทั้งยังไม่มีบทกฎหมายที่จะช่วยในการแสวงหาพยานหลักฐานดังกล่าวแก่เจ้าพนักงานและบทลงโทษแก่ผู้ที่ทำลายข้อมูลที่อาจใช้เป็นพยานหลักฐานดังกล่าวแต่อย่างใด จึงทำให้มาตรการแสวงหาพยานหลักฐานในคดีอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญาไทยยังไม่เพียงพอที่จะค้นหาพยานหลักฐานทางคอมพิวเตอร์ได้อย่างเต็มที่ ซึ่งอาจทำให้เจ้าพนักงานอาจเสียโอกาสในการได้รับพยานหลักฐาน

---

[3] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3121-3127), The USA Patriot Act 2001.

[4] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2510-2522).

[5] The Sarbanes-oxley act of 2002 (U.S.C. title 18 section 1519).

ที่สำคัญในคดีอาญาซึ่งจะเอาผิดแก่ผู้กระทำผิดได้ และแม้ว่าประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1 จะเปิดโอกาสให้รับฟังพยานหลักฐานที่เกิดขึ้นจากการใช้วิธีการแสวงหาพยานหลักฐานที่ไม่มีกฎหมายรองรับไว้โดยเป็นการละเมิดสิทธิเสรีภาพของบุคคลก็ตาม ซึ่งทำให้พยานหลักฐานที่ได้จากการแสวงหาพยานหลักฐานดังกล่าว เป็นพยานหลักฐานที่เกิดขึ้นมาโดยชอบ แต่ได้มาโดยมิชอบ ที่ศาลอาจรับฟังได้หากหากเข้าข้อยกเว้น โดยที่พยานหลักฐานนั้นจะเป็นประโยชน์ต่อการอำนวยความยุติธรรมมากกว่าผลเสีย แต่เพื่อเป็นการอำนวยซึ่งความยุติธรรม พยานหลักฐานที่ได้มาโดยมิชอบด้วยกฎหมายไม่ว่าโดยประการใดๆ ศาลจะต้องปฏิเสธไม่รับฟัง โดยถือว่าเป็นหลักการตัดพยานหลักฐาน (Exclusionary Rule) ชนิดหนึ่ง การรับฟังพยานหลักฐานที่ไม่ชอบด้วยกฎหมายเหมือนกับการยอมรับเอาผลไม้ของต้นไม้ที่มีพิษ ศาลจึงไม่รับฟังพยานหลักฐานที่เป็นผลมาจากการกระทำที่ไม่ชอบด้วยกฎหมาย จึงสมควรมีมาตรการการแสวงหาพยานหลักฐานทางคอมพิวเตอร์เพื่อรองรับไว้ให้กระบวนการยุติธรรมนั้นชอบด้วยกฎหมาย แต่อย่างไรก็ดีพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 เฉพาะในคดีพิเศษก็ให้อำนาจเจ้าพนักงานคดีพิเศษเพื่อให้ได้มาซึ่งข้อมูลที่เป็นการสื่อสารทางโทรศัพท์รวมทั้งข้อมูลอิเล็กทรอนิกส์[6] โดยมีการตรวจสอบ กลั่นกรองและถ่วงดุลอำนาจดังกล่าวตามบทบัญญัตินี้ บทบัญญัตินี้ถือว่าเป็นการให้อำนาจเจ้าพนักงานในคดีพิเศษในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ซึ่งจะทำให้เจ้าพนักงานคดีพิเศษสามารถเข้าถึงพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์ได้ แต่อำนาจดังกล่าวก็มีเฉพาะในคดีพิเศษตามพระราชบัญญัตินี้เท่านั้น[7] ซึ่งไม่ครอบคลุมทุกฐานความผิดโดยพยานหลักฐานทางคอมพิวเตอร์นั้นอาจเกี่ยวข้องกับฐานความผิดอื่นที่ไม่ใช่การกระทำผิดที่เป็นคดีพิเศษก็ได้เช่นจดหมายอิเล็กทรอนิกส์ที่ใช้ตกลงกันกระทำความผิดทางอาญาฐานต่างๆ ความผิดฐานเรียกค่าไถ่ ความผิดฐานรีดเอาทรัพย์ ความผิดฐานฉ้อโกง เป็นต้น จึงเห็นว่าควรเพิ่มมาตรการในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ลงในประมวลกฎหมายวิธีพิจารณาความอาญาของไทยโดยศึกษาพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และกฎหมายของอเมริกา ในเรื่องของการแสวงหาพยานหลักฐานทางคอมพิวเตอร์มาใช้กับประมวลกฎหมายวิธีพิจารณาความอาญาของไทย เพื่อให้เกิดความรวดเร็วและความถูกต้องในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์และสามารถเข้าถึงพยานหลักฐานดังกล่าวได้และจะครอบคลุมทุกฐานความผิดไม่ใช่เฉพาะคดีพิเศษเพียงอย่างเดียว ทั้งยังเป็นการรับรองให้การแสวงหาพยานหลักฐานทางคอมพิวเตอร์ของเจ้าพนักงานนั้นชอบด้วยกฎหมาย ซึ่งจะเป็นประโยชน์

---

[6] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25.

[7] บัญชีท้ายพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547.

ในเรื่องของการค้นหาพยานหลักฐานในการพิสูจน์ความผิดแก่ผู้กระทำผิดทำให้พยานหลักฐานดังกล่าวมีน้ำหนักน่าเชื่อถือ ถูกต้อง ชัดเจน สมบูรณ์ และรับฟังเป็นพยานหลักฐานได้

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาถึงแนวความคิดและวิวัฒนาการในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญา
2. เพื่อศึกษาถึงหลักการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และกฎหมายของประเทศอเมริกาเพื่อนำมาปรับใช้กับประมวลกฎหมายวิธีพิจารณาความอาญาของไทย
3. เพื่อศึกษาถึงความเหมาะสมของการนำหลักการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และกฎหมายของประเทศอเมริกามาปรับใช้กับประมวลกฎหมายวิธีพิจารณาความอาญาของไทย

1.3 สมมติฐานของการศึกษา

การสอบสวนในคดีอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญาของไทยยังมีปัญหาอย่างมากในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ โดยในคดีพิเศษก็ได้กำหนดวิธีการที่เหมาะสมในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ไว้ แต่ความผิดอาญาร้ายแรงก็ไม่ได้มีเฉพาะคดีพิเศษเพียงอย่างเดียวซึ่งพยานหลักฐานทางคอมพิวเตอร์ก็อาจเกิดขึ้นในคดีอาญาร้ายแรงอื่นๆ ที่ไม่ใช่คดีพิเศษได้เช่นกัน ดังนั้น การกำหนดกลไกในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาของไทยจะทำให้เจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญาสามารถเข้าถึงพยานหลักฐานทางคอมพิวเตอร์ได้ และเป็นการรับรองให้การแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาของเจ้าพนักงานดังกล่าวนั้นชอบด้วยกฎหมาย อันจะทำให้พยานหลักฐานดังกล่าวสามารถรับฟังได้ นอกจากนี้ยังเป็นการป้องกันและปราบปรามอาชญากรรมในสังคมเพื่อให้เกิดความสงบสุขแก่ประชาชนในสังคมอีกด้วย

1.4 ขอบเขตของการศึกษา

จะศึกษาถึงแนวความคิด วิวัฒนาการ และหลักการในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 รวมทั้งการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ตามกฎหมายของประเทศอเมริกามาปรับใช้กับประมวลกฎหมายวิธีพิจารณาความอาญาของไทย

1.5 วิธีดำเนินการศึกษา

การศึกษาวิจัยนี้ จะทำการศึกษาวิจัยเอกสารทั้งที่เป็นภาษาไทยและภาษาต่างประเทศ ตลอดจนตัวบทของกฎหมายไทยและกฎหมายต่างประเทศ ตำรา หรือคำอธิบายกฎหมายและบทความที่เกี่ยวข้องเพื่อนำมาวิเคราะห์ประเด็นปัญหาที่ศึกษาวิจัย

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ทราบถึงความหมาย วิวัฒนาการและสถานะของพยานหลักฐานทางคอมพิวเตอร์
2. ทำให้ทราบถึงปัญหาทางกฎหมายของการแสวงหาพยานหลักฐานทางคอมพิวเตอร์
3. ทำให้ทราบถึงหลักการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และกฎหมายของประเทศอเมริกา

บทที่ 2
แนวคิดที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญา

การแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญานั้น ก่อนอื่นจะต้องศึกษาถึงแนวความคิดที่เกี่ยวกับการแสวงหาพยานหลักฐานในคดีอาญา อีกทั้งหลักการที่เกี่ยวข้องกับการแสวงหาพยานหลักฐาน และความหมายพยานหลักฐานต่างๆ ในคดีอาญา อีกทั้งการคุ้มครองสิทธิเสรีภาพของบุคคลในกฎหมายอาญาว่ามีเพียงใด แนวคิดเกี่ยวกับการตรวจสอบ ถ่วงดุลอำนาจ ดังกล่าวตลอดจนการรับฟังพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาว่าเป็นอย่างไร ซึ่งแนวคิดและหลักการแสวงหาพยานหลักฐานในคดีอาญามีดังนี้

2.1 หลักการแสวงหาพยานหลักฐานในคดีอาญา

ปัจจุบันการแสวงหาพยานหลักฐานในคดีอาญานั้น มีอยู่หลากหลายวิธีไม่ว่าจะเป็นวิธีการค้น การจับ หรือวิธีการอื่นๆ เพื่อให้ได้มาซึ่งพยานหลักฐานในคดีอาญาในการพิสูจน์ความผิดแก่จำเลยในชั้นศาล ซึ่งความหมายของพยานหลักฐานนั้น หมายถึง สิ่งใดๆ ที่แสดงถึงข้อเท็จจริงให้ปรากฏแก่ศาล[8] ที่สามารถแบ่งประเภทตามรูปลักษณะได้ออกเป็น 3 รูปแบบด้วยกันคือ

“พยานบุคคล” หมายถึง ผู้ที่จะต้องเปิดเผยถึงการรับรู้ของตนเกี่ยวกับข้อเท็จจริงโดยการให้ถ้อยคำ

“พยานเอกสาร” หมายถึง ข้อมูลที่บันทึกไว้ในสื่อชนิดใดก็ตามสามารถพิสูจน์ข้อเท็จจริงที่พิพาทในคดีได้และนำสืบชนิดที่บันทึกข้อมูลดังกล่าวนั้นมาใช้เป็นพยานหลักฐานในศาลก็ให้ถือเป็นพยานหลักฐาน และให้รวมถึงสื่อที่บันทึกไว้ในคอมพิวเตอร์หรือสื่อสารสนเทศอื่นๆ ด้วย[9]

---

[8] โสภณ รัตนากร. (2553). *คำอธิบายกฎหมายลักษณะพยาน*. หน้า 19-22.

[9] ปิติกุล จีระมงคลพาณิชย์. (2545, มิถุนายน). “การรับฟังสื่อบันทึกเสียงและภาพในกฎหมายลักษณะพยาน.” *วารสารนิติศาสตร์, 32 (2)*. หน้า 372.

"พยานวัตถุ" หมายความว่า วัตถุอย่างใดๆ อันมิใช่เอกสารซึ่งคู่ความนำส่งเพื่อให้ศาลตรวจ โดยอาจเป็นสิ่งที่มีชีวิต เช่น ร่างกายมนุษย์ สถานที่ สัตว์ หรือเป็นสิ่งที่ไม่มีชีวิตทั้งหลายที่คู่ความ นำมาให้ศาลเห็นได้ด้วยตา หรือให้ศาลไปตรวจดูยังที่ๆ พยานอยู่[10]

จากนิยามของพยานหลักฐานดังกล่าวข้างต้น พยานหลักฐานทางคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ถือว่ามีสถานะเป็นพยานเอกสารอย่างหนึ่ง เนื่องจากเป็นสื่อที่สามารถพิสูจน์ข้อเท็จจริงที่พิพาทในคดีได้และนำสืบชนิดที่บันทึกข้อมูลดังกล่าวนั้นมาใช้เป็นพยานหลักฐานในศาลก็ให้ถือเป็นพยานหลักฐาน และคอมพิวเตอร์ที่บรรจุพยานหลักฐานทางคอมพิวเตอร์ดังกล่าวก็อาจถือได้ว่าคอมพิวเตอร์นั้นเป็นพยานวัตถุอย่างหนึ่งเช่นกัน

นอกจากนี้กระบวนการแสวงหาพยานหลักฐานในขั้นตอนก่อนการพิจารณา อันได้แก่ การสืบสวนสอบสวนที่มีความสำคัญต่อกระบวนการยุติธรรมเป็นอย่างมากในฐานะที่ขั้นตอนดังกล่าวเป็นขั้นตอนแห่งต้นสายของกระบวนการยุติธรรมและเป็นขั้นตอนที่สำคัญที่สุด โดยเฉพาะพนักงานสอบสวนที่มีอำนาจในการรวบรวมพยานหลักฐานได้อย่างกว้างขวางดังบัญญัติไว้ในมาตรา 131[11] แห่งประมวลกฎหมายวิธีพิจารณาความอาญาของไทยอันมีสาระสำคัญในเนื้อหา 2 ประการด้วยกันคือ เนื้อหาในเรื่องของการรวบรวมพยานหลักฐานและเนื้อหาว่าด้วยการใช้มาตรการบังคับ[12] และเมื่อกล่าวถึงการแสวงหาพยานหลักฐานในปัจจุบันเจ้าพนักงานของรัฐอาจทำได้ด้วยวิธี ดังนี้คือ

1) การใช้วิธีการแสวงหาพยานหลักฐานด้วยวิธีการ เข้าค้น เพื่อยึดพยานเอกสารหรือพยานวัตถุ จากเคหสถานของบุคคล

2) การใช้วิธีการแสวงหาพยานหลักฐานด้วยวิธีการจับ การค้นเพื่อยึดพยานเอกสารหรือพยานวัตถุจากตัวบุคคล

3) การแสวงหาพยานหลักฐานจากร่างกายมนุษย์

---

[10] ยิ่งศักดิ์ กฤษณะจินดา และ วุฒิพงษ์ เวชยานนท์. (2541). *คำอธิบายกฎหมายลักษณะพยาน*. หน้า 376-377.

[11] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131 บัญญัติว่า "ให้พนักงานสอบสวนรวบรวมพยานหลักฐานทุกชนิด เท่าที่สามารถจะทำได้ เพื่อประสงค์จะทราบข้อเท็จจริงและพฤติการณ์ต่างๆ อันเกี่ยวกับความผิดที่ถูกกล่าวหา..."

[12] คณิต ณ นคร. (2528). "วิธีพิจารณาความอาญาไทย: หลักกฎหมายกับทางปฏิบัติที่ไม่ตรงกัน." *วารสารนิติศาสตร์, 15 (3)*. หน้า 11.

4) การใช้วิธีการแสวงหาพยานหลักฐานด้วยวิธีการใช้เทคโนโลยีทางอิเล็กทรอนิกส์ในการดักฟัง การติดต่อสื่อสารของบุคคลหรือการใช้อุปกรณ์ดังกล่าวบันทึกเสียงของบุคคลหรือการบันทึกเสียงการสนทนากันระหว่างบุคคล

5) การแสวงหาพยานหลักฐานด้วยวิธีการใช้เทคนิคการสืบสวนสอบสวนพิเศษ ได้แก่ การดักฟังทางโทรศัพท์ การส่งมอบภายใต้การควบคุม การอำพราง การสะกดรอยโดยใช้เครื่องมืออิเล็คทรอนิคส์ การล่อซื้อ ล่อจับ โดยเจ้าพนักงาน เป็นต้น

แต่อย่างไรก็ตามปัจจุบันประมวลกฎหมายวิธีพิจารณาความอาญาของไทย ก็ได้วางหลักการแสวงหาพยานหลักฐานในคดีอาญาไว้เฉพาะการแสวงหาพยานหลักฐานด้วยวิธีการ เข้าค้นเพื่อยึดพยานเอกสารหรือพยานวัตถุ จากเคหสถานของบุคคล วิธีการแสวงหาพยานหลักฐานด้วยวิธีการจับ การค้นเพื่อยึดพยานเอกสารหรือพยานวัตถุจากตัวบุคคล การแสวงหาพยานหลักฐานจากร่างกายมนุษย์ ซึ่งเป็นหลักการแสวงหาพยานหลักฐานโดยทั่วไปในการค้นหาพยานหลักฐานในคดีอาญาได้ในระดับหนึ่ง การแสวงหาพยานหลักฐานทางคอมพิวเตอร์จะต้องมีมาตรการที่พิเศษกว่านั้น โดยประมวลกฎหมายวิธีพิจารณาความอาญาของไทยก็ไม่ได้กำหนดหลักการแสวงหาพยานหลักฐานโดยวิธีการสอบสวนพิเศษ เช่น การดักฟังฯ แต่อย่างใด จึงอาจส่งผลให้การแสวงหาพยานหลักฐานในคดีอาญาของเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญาของไทยไม่สามารถแสวงหาพยานหลักฐานได้อย่างเต็มที่และอาจพลาดโอกาสในการที่จะได้มาซึ่งพยานหลักฐานที่เกิดขึ้นจากการติดต่อสื่อสารทางคอมพิวเตอร์ของอาชญากรซึ่งเป็นพยานหลักฐานที่สำคัญในการเอาผิดแก่ผู้กระทำผิดได้

2.2 หลักการแสวงหาพยานหลักฐานในคดีอาญากับการคุ้มครองสิทธิเสรีภาพขั้นพื้นฐานของบุคคล

ศักดิ์ศรีความเป็นมนุษย์ (Human Dignity) อันเป็นสิทธิขั้นพื้นฐานของสิทธิมนุษยชนที่สำคัญที่สุด รัฐธรรมนูญในฐานะที่เป็นกฎหมายสูงสุดในการปกครองประเทศ[13] ไม่ว่าจะเป็นความสูงสุดในแง่ของกฎหมายที่แสดงถึงที่มาของอำนาจอธิปไตยของประเทศนั้น ซึ่งจะมีการเปลี่ยนแปลงแก้ไขหรือยกเลิกได้ยากกว่ากฎหมายอื่นๆ ทั่วๆ ไป หรือมีความสูงสุดในฐานะที่เป็นกฎหมายที่บทบัญญัติแห่งกฎหมายอื่นๆ และการกระทำใดๆ จะมาขัดหรือแย้งมิได้[14] เหล่านี้ก็จะเห็นได้ว่าการที่รัฐธรรมนูญได้วางหลักการคุ้มครองสิทธิเสรีภาพของบุคคลในเรื่องต่างๆ

---

[13] กมล ทองธรรมชาติ. (2524). *วิวัฒนาการของระบบรัฐธรรมนูญไทย.* หน้า 1.

[14] จรัญ ภักดีธนากุล. (2523, มกราคม-กุมภาพันธ์). “ศาล กับ ความเป็นสูงสุดแห่งรัฐธรรมนูญ.” *ดุลพาห, 27 (1).* หน้า 51.

มากมายก็เพื่อคุ้มครองสิทธิเสรีภาพของประชาชนให้ปลอดพ้นจากการใช้อำนาจที่ไม่เป็นธรรมของรัฐหรือจากผู้อื่น[15]

รัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2550 อันเป็นรัฐธรรมนูญที่ใช้บังคับอยู่ในปัจจุบันก็ได้มีการวางหลัก คุ้มครองสิทธิเสรีภาพขั้นพื้นฐานของบุคคลอันอาจถูกกระทบจากการแสวงหาพยานหลักฐานของเจ้าหน้าที่รัฐ ที่สามารถจำแนกได้ออกเป็น 4 กรณีด้วยกันคือ

2.2.1 หลักการคุ้มครองสิทธิเสรีภาพของบุคคลในเคหสถาน

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 ได้บัญญัติรับรองคุ้มครองสิทธิเสรีภาพของบุคคลในเคหสถานตามมาตรา 33 ที่บัญญัติว่า

"มาตรา 33 บุคคลย่อมมีเสรีภาพในเคหสถานบุคคลย่อมได้รับความคุ้มครองในการที่จะอยู่อาศัยและครอบครองเคหสถานโดยปกติสุข

การเข้าไปในเคหสถานโดยปราศจากความยินยอมของผู้ครอบครองหรือการตรวจค้นเคหสถานจะกระทำมิได้ เว้นแต่มีคำสั่งหรือหมายของศาลหรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ"

จากบทบัญญัติดังกล่าว จะเห็นได้ว่า สิทธิเสรีภาพในเคหสถานของบุคคลตามที่รัฐธรรมนูญฉบับปัจจุบันได้วางหลักไว้เป็นหลักการพื้นฐานที่สำคัญที่จะไม่ถูกล่วงละเมิด ไม่ว่าการล่วงละเมิดนั้น จะเป็นการล่วงละเมิดโดยเอกชนหรือโดยรัฐก็ตาม โดยเฉพาะอย่างยิ่ง รัฐจะต้องให้ความเคารพต่อสิทธิเสรีภาพนี้ด้วยการงดเว้นการล่วงละเมิดต่อสิทธิดังกล่าวเว้นแต่การล่วงละเมิดนั้นจะเป็นกรณีที่กฎหมายได้ให้อำนาจแก่รัฐตามความจำเป็นและในกรอบตามที่กฎหมายบัญญัติให้อำนาจไว้ เช่นในประมวลกฎหมายวิธีพิจารณาความอาญาที่ให้อำนาจแก่เจ้าพนักงานสามารถทำการค้นในที่รโหฐานได้ หากการเข้าค้นดังกล่าวเป็นการค้นโดยมีหมายของศาล หรือเป็นการเข้าค้นโดยไม่มีหมายของศาล แต่ก็จะต้องมีเหตุให้เจ้าพนักงานเข้าค้นได้โดยไม่มีหมาย ดังที่บัญญัติไว้ในมาตรา 92 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา[16] เป็นต้น เพราะเหตุผลสำคัญของการที่กฎหมายกำหนดให้ศาลเท่านั้นเป็นผู้ออกหมายค้น ก็เนื่องด้วยมาจากสาเหตุที่ว่าการค้นในที่รโหฐานถือเป็นการกระทำถือเป็นการกระทบต่อสิทธิส่วนบุคคลซึ่งเป็นสิทธิที่สำคัญของมนุษย์ประการหนึ่ง ฉะนั้นเพื่อเป็นการคุ้มครองสิทธิ เพื่อความเป็นเสรีนิยม นานาอารยประเทศ

---

[15] มานิตย์ จุมปา. (2549). *คำอธิบายรัฐธรรมนูญแห่งราชอาณาจักรไทย (พ.ศ. 2540) รัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช 2549 พร้อมข้อเสนอสำหรับรัฐธรรมนูญแห่งราชอาณาจักรไทย (พ.ศ. 2550) (แก้ไขเพิ่มเติมครั้งที่ 8)*. หน้า 47.

[16] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92.

จึงมอบหมายหน้าที่ให้ศาลเป็นผู้ตรวจสอบอำนาจรัฐเพื่อให้มีความรับผิดชอบที่ตรวจสอบได้ (Accountability)[17]

นอกจากนี้เหตุผลสำคัญที่กฎหมายกำหนดให้ศาลเท่านั้นเป็นผู้ออกหมายค้นก็คือวัตถุประสงค์ในแง่ของการถ่วงดุลและตรวจสอบการใช้อำนาจของเจ้าพนักงานที่เป็นฝ่ายบริหารเพื่อเป็นการคุ้มครองสิทธิเสรีภาพของบุคคลในเคหสถานอีกประการหนึ่งในการป้องกันมิให้เจ้าพนักงานฝ่ายปกครองหรือเจ้าพนักงานตำรวจใช้อำนาจโดยอำเภอใจอันอาจกระทบต่อสิทธิเสรีภาพของบุคคลในเคหสถาน ดังที่รัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2550 ได้บัญญัติไว้ในมาตรา 33 วรรคสาม ที่ใช้บังคับอยู่ในปัจจุบันนั่นเอง

ดังนั้นจึงอาจกล่าวได้ว่าสิทธิเสรีภาพของบุคคลในเคหสถานตามที่บัญญัติในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 จึงเป็นสิทธิขั้นพื้นฐานต่อบุคคลที่สำคัญประการหนึ่งที่รัฐธรรมนูญอันเป็นกฎหมายสูงสุดของประเทศได้ให้การรับรองและคุ้มครองไว้โดยผู้ใดจะมาล่วงละเมิดมิได้

2.2.2 หลักการคุ้มครองสิทธิเสรีภาพของบุคคลในชีวิตและร่างกาย

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 ได้บัญญัติรับรองคุ้มครองสิทธิและเสรีภาพของบุคคลในชีวิต ร่างกายในมาตรา 32 ที่บัญญัติว่า

“มาตรา 32 บุคคลย่อมมีสิทธิและเสรีภาพในชีวิตและร่างกายการทรมาน ทารุณกรรม... ด้วยวิธีการโหดร้ายหรือไร้มนุษยธรรม จะกระทำมิได้...

การจับ และการคุมขังบุคคล จะกระทำมิได้ เว้นแต่จะมีคำสั่งหรือหมายของศาลหรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ

การค้นตัวบุคคล หรือการกระทาใดอันกระทบต่อสิทธิ และเสรีภาพตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่มีเหตุตามที่กฎหมายบัญญัติ”

จากบทบัญญัติดังกล่าวจะเห็นได้ว่า สิทธิเสรีภาพในชีวิตและร่างกายเป็นสิทธิขั้นพื้นฐานที่สำคัญที่สุดโดยเฉพาะความสัมพันธ์กับหลักในเรื่อง ศักดิ์ศรีความเป็นมนุษย์ (Human Dignity) ที่บุคคลใดจะมาล่วงละเมิดไม่ได้โดยเด็ดขาด เว้นแต่จะเป็นการอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายการแสวงหาพยานหลักฐานของเจ้าพนักงานที่มีผลกระทบต่อสิทธิเสรีภาพดังกล่าวเจ้าพนักงานในฐานะที่เป็นตัวแทนของรัฐก็จะต้องดำเนินการตามหน้าที่โดยระมัดระวังภายในกรอบและขอบเขตของกฎหมายที่ให้ไว้ โดยเฉพาะในปัจจุบันอำนาจของเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญาในการดำเนินการตามกฎหมายที่เป็น

---

[17] คณิต ณ นคร. (2544). “บทบาทของศาลในคดีอาญา.” *วารสารกฎหมายธุรกิจบัณฑิตย์, 1 (1)*. หน้า 55.

การกระทบต่อสิทธิ เสรีภาพของบุคคลในร่างกายอยู่หลายกรณีด้วยกัน ไม่ว่าจะเป็นการจับ[18] การค้นตัวบุคคล[19] หรืออำนาจในการตรวจตัวบุคคล[20]

เมื่อกล่าวถึงการจับและการค้นตัวบุคคล อันเป็นวิธีการแสวงหาพยานหลักฐานในทางหนึ่งของเจ้าพนักงานที่กระทบต่อสิทธิเสรีภาพในร่างกายของผู้ถูกจับหรือถูกค้น การใช้อำนาจนี้ก็จะต้องเป็นไปตามที่กฎหมายได้ให้อำนาจไว้ด้วยเช่นเดียวกัน ซึ่งกฎหมายเช่นว่านี้ก็คือ ประมวลกฎหมายวิธีพิจารณาความอาญาที่ให้อำนาจแก่เจ้าพนักงานในการจับ และการค้นตัวของบุคคล โดยเฉพาะอย่างยิ่งเมื่อกล่าวถึงการจับ ที่ถือเป็นมาตรการที่สำคัญประการหนึ่งในกฎหมายวิธีพิจารณาความอาญาในการนำตัวผู้กระทำความผิดมาลงโทษ และเป็นการกระทำที่กระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนมากที่สุดทางหนึ่งเพราะการจับก่อให้เกิดอำนาจในการควบคุมผู้ถูกจับ ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 83 มาตรา 84 มาตรา 84/1 และมาตรา 87 โดยเฉพาะอย่างยิ่งผู้จับมีอำนาจในการค้นตัวผู้ถูกจับ ตามมาตรา 85 วรรคหนึ่งและอำนาจอื่นๆ อีกหลายประการ

มีข้อสังเกตว่าแต่เดิมการจับไม่ว่าจะเป็นการจับโดยมีหมายจับหรือไม่ก็ตามกฎหมายไม่ได้เคร่งครัดว่าจะต้องมีการสืบสวนสอบสวนจนปรากฏพยานหลักฐานก่อนว่า บุคคลที่จะถูกจับนั้นน่าจะได้กระทำความผิดอาญา สังเกตได้จากประมวลกฎหมายวิธีพิจารณาความอาญาเดิมก่อนที่จะมีการแก้ไข ในมาตรา 66 ที่บัญญัติว่า “ถ้าผู้ต้องหาหรือจำเลยไม่มาตามหมายเรียกหรือตามนัดโดยไม่มีข้อแก้ตัวอันควรก็เป็นเหตุที่จะออกหมายจับได้” และมาตรา 7/(4) บัญญัติว่า “ถ้ามีผู้เสียหายซึ่งร้องทุกข์ไว้แล้วขอให้จับบุคคลใด พนักงานฝ่ายปกครองหรือตำรวจมีอำนาจที่จะจับบุคคลนั้นได้โดยไม่ต้องมีหมายจับ” ด้วยเหตุนี้ในทางปฏิบัติจึงทำให้มีการจับกุมผู้ต้องหาไว้ก่อนโดยที่ยังไม่มีพยานหลักฐานเพียงพอ แล้วนำผู้ต้องหานั้นมาสอบสวนเอาข้อเท็จจริงในภายหลังหรือที่เรียกว่า “การแสวงหาพยานหลักฐานเอาจากตัวผู้ต้องหา” ซึ่งเป็นการกระทบต่อสิทธิขั้นพื้นฐานของบุคคลที่ว่าบุคคลมีสิทธิไม่ให้ถ้อยคำอันเป็นปฏิปักษ์ต่อตนเอง อันอาจทำให้ตนถูกฟ้องเป็นคดีอาญา ดังนั้นรัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2540 ตามมาตรา 237 จึงได้วางหลักการใหม่ว่าการจับและคุมขังบุคคลใด จะต้องไปขอหมายจับจากศาลก่อนและหมายจับจะออกได้ต่อเมื่อปรากฏพยานหลักฐานตามสมควรว่า ผู้นั้นน่าจะได้กระทำความผิดอาญาแสดงว่าก่อนมีการจับกุมพนักงานฝ่ายปกครองหรือตำรวจจะต้องมีข้อมูลหรือพยานหลักฐานเพียงพอที่จะเชื่อได้ว่า ผู้นั้นน่าจะได้กระทำความผิดอาญา แม้รัฐธรรมนูญจะกำหนดให้สามารถออกกฎหมายกำหนดข้อยกเว้น

---

[18] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 78.

[19] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 85 และมาตรา 93.

[20] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 (1).

ให้พนักงานฝ่ายปกครองหรือตำรวจจับได้โดยไม่ต้องมีหมายจับหรือคาสั่งของศาลก็ตาม การกำหนดข้อยกเว้นนั้นก็จะต้องคำนึงถึงเจตนารมณ์ของรัฐธรรมนูญดังกล่าวด้วย ซึ่งตามมาตรา 78 (1)-(4) ที่แก้ไขใหม่ ล้วนแต่เป็นกรณีที่เห็นได้ชัดว่ามีพยานหลักฐานตามสมควรว่าบุคคลนั้นน่าจะได้กระทำความผิดอาญา ส่วนกรณีที่มีผู้เสียหายร้องขอให้จับโดยแจ้งว่าได้ร้องทุกข์ไว้แล้วตามมาตรา 78 (4) เดิมนั้น เนื่องจากเป็นการขัดต่อเจตนารมณ์ของรัฐธรรมนูญดังกล่าวข้างต้น จึงถูกตัดออกไป[21]

ในเรื่องของการเข้าค้นตัวบุคคลในที่สาธารณสถานก็เช่นเดียวกัน แม้การเข้าค้นดังกล่าวกฎหมายจะมิได้บังคับว่าจะต้องผ่านการตรวจสอบโดยศาลด้วยการออกหมายค้นก็ตามแต่การที่เจ้าพนักงานได้เข้าค้นเพื่อแสวงหาพยานหลักฐานไม่ว่าจะเป็นพยานหลักฐานหรือพยานวัตถุในตัวบุคคล ต่างก็ถือว่าเป็นการละเมิดต่อสิทธิเสรีภาพในร่างกายของบุคคลโดยทางหนึ่งเช่นเดียวกัน ด้วยเหตุนี้เองกฎหมายวิธีพิจารณาความอาญาของไทยจึงได้กำหนดเงื่อนไขของการใช้อำนาจของเจ้าพนักงานในการกระทำที่กระทบต่อสิทธิเสรีภาพดังกล่าว คือ เงื่อนไขของการมี “เหตุอันควรสงสัย” ว่าบุคคลที่จะถูกค้นนั้น มีสิ่งของเพื่อจะใช้ในการกระทำความผิด หรือ มีสิ่งของที่ได้มาโดยการกระทำความผิด หรือ ซึ่งมีไว้เป็นความผิด ไว้ในครอบครองเป็นเงื่อนไขของกฎหมายที่จะทำให้เจ้าพนักงานมีอำนาจที่จะดำเนินการแสวงหาพยานหลักฐานจากตัวบุคคลที่กระทบต่อเสรีภาพในร่างกาย ซึ่งก็คือ การถูกตรวจค้นนั่นเอง

2.2.3 หลักการคุ้มครองสิทธิของบุคคลที่จะไม่ถูกกักหรือดักการสื่อสารโดยมิชอบตามกฎหมายไทย

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 ที่ใช้บังคับอยู่ในปัจจุบันได้บัญญัติหลักการคุ้มครองสิทธิของบุคคลเกี่ยวกับ สิทธิเสรีภาพในการติดต่อสื่อสารไว้ดังนี้ คือ

มาตรา 35 บัญญัติว่า “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง...

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงหาประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ตามที่กฎหมายบัญญัติ”

มาตรา 36 บัญญัติว่า “บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบด้วยกฎหมาย

การตรวจ การกัก หรือการเปิดเผยสิ่งสื่อสารที่บุคคลมีติดต่อถึงกัน รวมทั้งการกระทำด้วยประการอื่นใด เพื่อให้ล่วงรู้ถึงข้อความในสิ่งสื่อสารทั้งหลายที่บุคคลมีติดต่อถึงกันจะกระทำ

---

[21] ข้อพิจารณาประกอบพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความอาญา (ฉบับที่ 22) พ.ศ. 2547. หน้า 68.

มิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อรักษาความมั่นคงของรัฐหรือเพื่อรักษาความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน”

จากบทบัญญัติดังกล่าว เป็นการวางหลักการคุ้มครองเสรีภาพในการสื่อสาร อันถือว่าเป็นสิทธิส่วนบุคคลหรือเป็นสิทธิในความเป็นส่วนตัว (Right of Privacy) ของบุคคลประเภทหนึ่งที่รัฐธรรมนูญได้ให้การรับรองและคุ้มครองเพื่อมิให้ผู้ใดโดยเฉพาะอย่างยิ่งที่เจ้าพนักงานของรัฐมักจะใช้วิธีการลักลอบดักฟังทางโทรศัพท์ที่ไม่มีกฎหมายให้อำนาจ[22] ในประเด็นปัญหานี้แม้ในปัจจุบันอาชญากรรมในความผิดบางประเภทที่รัฐมีความจำเป็นที่จะต้องใช้เทคโนโลยีในการดักฟังโทรศัพท์ เพื่อให้ได้มาซึ่งข้อมูลอันเป็นประโยชน์ต่อการดำเนินคดี โดยเฉพาะคดีที่มีลักษณะเป็นองค์กรอาชญากรรมที่เป็นเครือข่ายขนาดใหญ่ที่สร้างความเสียหายให้กับประเทศชาติเป็นอย่างมาก เช่น องค์กรค้ายาเสพติด องค์กรก่อการร้าย ฯลฯ ก็ตาม แต่ในขณะเดียวกัน หากการใช้อำนาจรัฐในการดักฟังโทรศัพท์เป็นไปโดยไม่มีหลักเกณฑ์หรือหลักประกันในการควบคุมการใช้อำนาจนั้นแล้ว สิ่งที่เป็นปัญหาซึ่งอาจตามมาก็คือ การใช้อำนาจรัฐก็จะเป็นไปตามอำเภอใจของเจ้าพนักงานผู้ใช้อำนาจนั้นเสียเอง อันอาจส่งผลกระทบต่อประชาชนที่มิได้มีส่วนเกี่ยวข้องกับการประกอบอาชญากรรมให้ต้องได้รับความเสียหายได้ เพราะย่อมเป็นที่รู้กันอยู่ทั่วไปว่า มนุษย์ทุกคนย่อมมีความเป็นส่วนตัว ซึ่งอาจเป็นเรื่องของสิทธิในครอบครัวหรือความลับในทางธุรกิจหรือเรื่องอื่นใดก็ตามที่จำเป็นจะต้องปิดเป็นความลับ ด้วยเหตุนี้รัฐธรรมนูญแห่งราชอาณาจักรไทยจึงได้วางหลักการที่สำคัญไว้ในเรื่องสิทธิของบุคคลที่จะไม่ถูกตรวจหรือกักหรือเปิดเผยสิ่งสื่อสารที่บุคคลติดต่อกันโดยมิชอบ โดยเฉพาะอย่างยิ่งในปัจจุบันส่วนใหญ่ที่มักเป็นปัญหาเกิดขึ้นอยู่เสมอก็คือการลักลอบดักฟังโทรศัพท์ นั่นเอง

ดังนั้นแม้ในบางกรณีการที่รัฐจะต้องแสวงหาข้อมูลต่างๆ ในการสืบสวนสอบสวนของคดีความผิดบางประเภทจำเป็นที่จะต้องมีมาตรการดักฟังโทรศัพท์เข้ามามีส่วนร่วมในการรวบรวมข้อมูลเพื่อสืบหาตัวการใหญ่ในองค์กรอาชญากรรมหรือข้อมูลอื่นใดอันสำคัญหรือเพื่อให้ได้มาซึ่งถ้อยคำที่จะเป็นพยานหลักฐานแก่คดีก็ตาม แต่ในฐานะที่ประเทศไทยก็เป็นประเทศหนึ่งที่ปกครองโดยหลักนิติรัฐ (Legal State) การที่เจ้าพนักงานของรัฐจะกระทำการใดที่กระทบต่อสิทธิเสรีภาพของประชาชนได้ก็ต่อเมื่อมีกฎหมายให้อำนาจ[23] ซึ่งในที่นี้ก็คือการอนุญาตให้เจ้าพนักงานสามารถ

---

[22] กมลชัย รัตนาสกาวงศ์ และวรพจน์ วิศรุตพิชญ์. (2540). *แนวทางในการยกร่างกฎหมายที่เกี่ยวข้องกับการดักฟังทางโทรศัพท์และการปรับปรุงกฎหมายอื่นๆ ที่เกี่ยวข้อง เสนอต่อสานักงานคณะกรรมการวิจัยแห่งชาติ (*รายงานผลการวิจัย). หน้า 38.

[23] มานิตย์ จุมปา. เล่มเดิม. หน้า 76.

ทำการดักฟังทางโทรศัพท์ได้ ภายใต้กรอบและหลักเกณฑ์ตามกฎหมาย ที่ออกโดยผ่านความเห็นชอบของผู้แทนประชาชนเสมอ

2.2.4 หลักการใช้อำนาจของรัฐในการแสวงหาพยานหลักฐาน

ปัจจุบันนานาประเทศส่วนใหญ่จะใช้หลักนิติรัฐในการปกครองกล่าวคือรัฐให้ความสัมพันธ์กับประชาชนและให้หลักประกันแก่สถานะของบุคคล โดยอยู่ภายใต้ระบอบแห่งกฎหมาย ระบอบแห่งกฎหมายนี้จะผูกการกระทำของรัฐไว้ด้วยกฎเกณฑ์ต่างๆ ซึ่งกฎเกณฑ์เหล่านี้ส่วนหนึ่งจะกำหนดสิทธิของประชาชน แต่อีกส่วนหนึ่งจะกำหนดไว้ล่วงหน้าถึงหนทางและวิธีการที่ถูกนำมาใช้เพื่อให้บรรลุจุดประสงค์ในการดำเนินการทางปกครองของรัฐ กฎเกณฑ์สองชนิดนี้มีจุดมุ่งหมายร่วมกันเพื่อจำกัดอำนาจของรัฐ โดยทำให้รัฐอยู่ภายใต้ระเบียบแห่งกฎหมายที่กฎเกณฑ์ทั้งสองชนิดดังกล่าวสร้างขึ้นด้วยเหตุนี้ลักษณะเฉพาะของนิติรัฐที่ชัดเจนอันหนึ่งก็คือในการปฏิบัติต่อผู้ใต้ปกครองฝ่ายปกครองจะใช้วิธีการต่างๆ ได้ก็แต่เฉพาะที่ระเบียบแห่งกฎหมายที่บังคับอยู่ในขณะนั้น เช่น พระราชบัญญัติ พระราชกฤษฎีกา ฯลฯ อนุญาตให้ไว้หลักนิติรัฐรับรองและให้ความคุ้มครองสิทธิเสรีภาพขั้นมูลฐานของประชาชนไว้ในรัฐธรรมนูญ ทั้งนี้เพื่อที่ประชาชนจะได้ใช้สิทธิเสรีภาพเช่นว่านั้นพัฒนาบุคลิกภาพของตนได้ตามที่ตนเองต้องการ

อย่างไรก็ดี การที่รัฐยอมรับรองและให้ความคุ้มครองสิทธิเสรีภาพของประชาชนไว้ในรัฐธรรมนูญนั้น ไม่ได้หมายความว่ารัฐจะยอมให้ประชาชนใช้สิทธิเสรีภาพของตนกระทำการต่างๆ ได้โดยปราศจากการแทรกแซงใดๆ จากเจ้าหน้าที่ของรัฐ ซึ่งรัฐก็มีผลประโยชน์ของส่วนรวมหรือผลประโยชน์สาธารณะ (Public Interest) ที่จะต้องธำรงรักษาไว้ในการธำรงรักษาไว้ซึ่งผลประโยชน์ของส่วนรวมหรือผลประโยชน์สาธารณะนี้ ในบางกรณีรัฐจำต้องบังคับให้ราษฎรกระทำการหรือละเว้นไม่กระทำกาบางอย่าง องค์กรเจ้าหน้าที่ของรัฐจึงสามารถล่วงล้ำเข้าไปในแดนแห่งสิทธิเสรีภาพของประชาชนได้ในบางกรณี แต่รัฐต้องมีหลักประกันต่อประชาชนว่าเจ้าหน้าที่ของรัฐจะล่วงล้ำแดนแห่งสิทธิเสรีภาพของประชาชนได้ ก็ต่อเมื่อมีกฎหมายบัญญัติไว้อย่างชัดแจ้งและเป็นการทั่วไป กล่าวคือ รัฐไม่เพียงมีบทบัญญัติป้องกันมิให้มีการใช้อำนาจเกินขอบเขต แต่ต้องมีบทบัญญัติให้มีรัฐบาลที่สามารถรักษากฎหมายและความสงบเรียบร้อยไว้ได้ตลอดจนรักษาฐานะทางสังคมและเศรษฐกิจได้ด้วย[24] ทั้งนี้ กฎหมายจะให้อำนาจเจ้าหน้าที่ของรัฐล่วงละเมิดสิทธิเสรีภาพของประชาชนได้ก็แต่เพียงเท่าที่จำเป็นแก่การธำรงรักษาไว้ซึ่งผลประโยชน์สาธารณะ บทบัญญัติแห่งกฎหมายที่ให้อำนาจแก่เจ้าหน้าที่ของรัฐเกินเลยกว่าความจำเป็นแก่การธำรงไว้ซึ่งผลประโยชน์ ย่อมขัดต่อเจตนารมณ์ของรัฐธรรมนูญด้วยเหตุนี้ในนิติรัฐ (Legal State) ไม่เฉพาะความสัมพันธ์ระหว่างประชาชนด้วยกันเองเท่านั้นที่จะต้องเป็นความสัมพันธ์ภายใต้

[24] จิตติ ติงศภัทิย์. (2533). *หลักวิชาชีพนักกฎหมาย*. หน้า 60.

กฎหมาย ความสัมพันธ์ระหว่างองค์กรเจ้าหน้าที่ของรัฐกับราษฎรก็จะต้องเป็นความสัมพันธ์ภายใต้กฎหมายด้วยเช่นกัน จึงได้มีผู้กล่าวว่าผู้ปกครองที่แท้จริงในนิติรัฐ คือ กฎหมายที่รัฐตราขึ้นโดยชอบด้วยรัฐธรรมนูญหรือการปกครองที่ถือกฎหมายเป็นใหญ่ (The Rule of Law)[25] ดังนั้นเจ้าหน้าที่ของรัฐไม่ว่าจะอยู่ในลำดับชั้นสูงต่ำอย่างไรก็ตาม ไม่สามารถที่จะรุกล้ำหรือจำกัดสิทธิเสรีภาพของประชาชนได้ตามอำเภอใจตรงกันข้ามอำนาจของเจ้าหน้าที่ของรัฐมีอยู่อย่างจำกัด กล่าวคือ ถ้าเจ้าหน้าที่ของรัฐจะเข้าไปล่วงละเมิดสิทธิเสรีภาพของประชาชนคนใดคนหนึ่ง เจ้าหน้าที่ของรัฐผู้นั้นจะต้องแสดงได้ว่ามีกฎหมายฉบับใดให้อำนาจตนกระทำการเช่นว่านั้น การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ถือเป็นกรณีที่บทบัญญัติของกฎหมายได้จำกัดสิทธิเสรีภาพในการสื่อสารของประชาชนไว้ ทั้งนี้ เพื่อวัตถุประสงค์ในการที่รัฐจะใช้อำนาจดังกล่าวป้องกันและปราบปรามอาชญากรและรักษาไว้ซึ่งความสงบของสังคมส่วนรวม แต่ถึงอย่างไรก็ดี รัฐต้องคำนึงถึงหลักการคุ้มครองสิทธิของประชาชนเป็นหลักเช่นเดียวกัน ในบทนี้ผู้เขียนจึงขอเสนอแนวคิดเรื่องการคุ้มครองสิทธิเสรีภาพของประชาชน และแนวคิดในเรื่องอำนาจรัฐในการรักษาความสงบเรียบร้อยของสังคม เพื่อสร้างความสมดุลระหว่างแนวคิดทั้งสองในการบังคับใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพ

2.2.4.1 แนวคิดเรื่องการคุ้มครองสิทธิเสรีภาพของประชาชน

แนวคิดว่าด้วยการคุ้มครองสิทธิเสรีภาพของประชาชน[26] หรือแนวคิดตามหลักกระบวนการนิติธรรม (Due Process of Law)[27] เป็นหลักที่ห้ามมิให้รับฟังพยานหลักฐานที่เจ้าหน้าที่รัฐได้มาโดยวิธีการจับค้น หรือ การยึด อันมิชอบโดยเด็ดขาด เพื่อคุ้มครองสิทธิและเสรีภาพของประชาชน

สิทธิ (Right) คือ ประโยชน์ที่กฎหมายรับรองและคุ้มครองให้แก่บุคคลในอันที่จะกระทำการเกี่ยวกับทรัพย์สินหรือบุคคลอื่น เช่น สิทธิในทรัพย์สิน สิทธิในชีวิตและร่างกาย เป็นต้น สิ่งใดรัฐธรรมนูญกำหนดเป็นสิทธิ หมายความว่า รัฐให้สิทธิแก่ประชาชน โดยรัฐมีพันธกรณีหรือหน้าที่ที่ต้องทำให้ประชาชนได้รับสิทธินั้น เปรียบเสมือนรัฐเป็นลูกหนี้ ประชาชนเป็นเจ้าหนี้

เสรีภาพ (Liberty) คือ ภาวะของมนุษย์ที่ไม่อยู่ภายใต้การครอบงำของผู้อื่น มีอิสระที่จะกระทำการหรืองดเว้นกระทำการ เช่น เสรีภาพในการติดต่อสื่อสาร เสรีภาพในการเดินทาง เป็นต้น

---

[25] ไพรัช โตสวัสดิ์. (2547). *การตรวจสอบความชอบด้วยกฎหมายของปฏิบัติการทางปกครอง*. หน้า 5.

[26] ประธาน วัฒนพานิช. (2520, กันยายน-พฤศจิกายน). "ระบบความยุติธรรมทางอาญา: แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม." *วารสารนิติศาสตร์, 9 (2)*. หน้า. 151.

[27] เกียรติขจร วัจนะสวัสดิ์. (2521). "หลักการไม่ยอมรับฟังพยานวัตถุ พยานเอกสาร ซึ่งได้มาโดยการจับการค้น การยึดที่ไม่ชอบด้วยกฎหมายในสหรัฐอเมริกา." *วารสารนิติศาสตร์, 9 (3)*. หน้า. 123.

สิ่งใดรัฐธรรมนูญกำหนดเป็นเสรีภาพ หมายความว่า ประชาชนมีเสรีภาพเช่นนั้น โดยรัฐมีหน้าที่โดยทั่วไปที่จะงดเว้นไม่ขัดขวางการให้เสรีภาพนั้นของประชาชน แต่รัฐไม่มีหน้าที่โดยเฉพาะเจาะจงที่จะต้องจัดหาสิ่งที่เป็นเสรีภาพมาให้ เสรีภาพจึงต่างจากสิทธิที่สิ่งใดเป็นสิทธิถือว่าเป็นหน้าที่ของรัฐโดยเจาะจงในการทำให้ประชาชนได้รับสิทธินั้น[28]

เหตุผลในการไม่ยอมรับฟังพยานหลักฐานที่เจ้าหน้าที่รัฐได้มาโดยมิชอบด้วยกฎหมาย มี 3 ประการ คือ

ประการที่ 1 เหตุผลในแง่ของการยับยั้งมิให้เจ้าหน้ารัฐที่กระทำการเช่นนั้นอีก (Deterrent) ในกรณีนี้อาจเป็นการยับยั้งเจ้าหน้าที่รัฐผู้นั้นโดยเฉพาะเจาะจง (Specific Deterrent) หรือยับยั้งเจ้าหน้าที่รัฐผู้อื่นๆ โดยทั่วไป (General Deterrent) ก็ได้ ตัวอย่างเช่น ถ้าเจ้าหน้าที่รัฐทำการดักฟังทางโทรศัพท์โดยไม่ได้รับอนุญาตจากศาล เจ้าหน้าที่รัฐผู้นั้นย่อมตระหนักดีว่าศาลจะไม่ยอมรับฟังพยานหลักฐานที่ได้มาจากการดักฟังเป็นอย่างแน่แท้ ดังนั้นเจ้าหน้าที่รัฐผู้นั้นอาจไม่กล้ากระทำการดักฟังโดยไม่ได้รับอนุญาตจากศาลต่อไปอีก เมื่อจะทำการดักฟังทางโทรศัพท์ในคราวต่อไป จำเป็นจะต้องดำเนินการให้มีการขออนุญาตจากศาลเสียก่อน หลักการเดียวกันนี้ก็มุ่งหวังว่าจะมีผลเป็นการยับยั้งต่อเจ้าพนักงานรายอื่นๆ โดยทั่วๆ ไปด้วย

ประการที่ 2 เหตุผลในแง่ของความบริสุทธิ์ยุติธรรมของศาล (Judicial Integrity) นอกจากเหตุผลในแง่ของการยับยั้งแล้ว ความบริสุทธิ์ยุติธรรมของศาลอาจต้องเสื่อมเสียไป ถ้ายอมรับฟังพยานหลักฐานที่ได้มาโดยวิธีการอันมิชอบ ถ้าศาลรับฟังและใช้พยานหลักฐานดังกล่าวลงโทษจำเลย ก็เท่ากับศาลไร้ความบริสุทธิ์และกลายเป็นหุ้นส่วนในการล่วงละเมิดกฎหมายของเจ้าหน้าที่ด้วยเช่นกัน (Partnership in Official Lawlessness) หลักในเรื่องความยุติธรรมเป็นกลางของศาลที่จะไม่เอียงเอนเข้ากับฝ่ายใด มีผลเป็นการบังคับให้ศาลต้องไม่รับฟังพยานที่ได้มาโดยวิธีการอันมิชอบ ซึ่งก็เท่ากับเป็นการเตือนให้ฝ่ายบริหารผู้ควบคุมเจ้าหน้าที่รัฐให้ได้ตระหนักว่าศาลจะไม่ยอมให้ฝ่ายบริหารได้รับผลประโยชน์ใดๆ จากการกระทำอันมิชอบโดยเจ้าหน้าที่ของฝ่ายบริหารนั้น

ประการที่ 3 เหตุผลในแง่ของสิทธิส่วนบุคคล (Right of Privacy) ของผู้ถูกเจ้าหน้าที่กระทำการอันมิชอบด้วยกฎหมาย

ดังนั้น แนวคิดว่าด้วยการคุ้มครองสิทธิเสรีภาพของประชาชน ก็คือรัฐจะออกกฎหมายหรือบังคับใช้กฎหมายที่เป็นการตัดทอนเอกสิทธิหรือความคุ้มกันหรือรอนสิทธิในชีวิตเสรีภาพ

---

[28] มานิตย์ จุมปา. เล่มเดิม. หน้า 138.

หรือทรัพย์สินของประชาชนโดยไม่ชอบด้วยกระบวนความแห่งกฎหมาย[29] หรือปฏิเสธไม่ให้ความคุ้มครองแห่งกฎหมายโดยเท่าเทียมกัน ย่อมกระทำไม่ได้

2.2.4.2 แนวคิดเรื่องอำนาจรัฐในการรักษาความสงบเรียบร้อยของสังคม

แนวคิดในเรื่องอำนาจรัฐในการรักษาความสงบเรียบร้อย[30] หรือแนวความคิดตามทฤษฎีการควบคุมอาชญากรรม (Crime Control) เป็นแนวความคิดที่ให้ความสำคัญกับการควบคุมปราบปรามอาชญากรรมเพื่อรักษาความสงบเรียบร้อยของสังคมเป็นหลัก ส่วนการคุ้มครองสิทธิเสรีภาพของบุคคลเป็นเรื่องรองลงไป ทั้งนี้เชื่อว่าการที่เจ้าหน้าที่ของรัฐไม่สามารถจะควบคุมและปราบปรามอาชญากรรมหรือจับกุมอาชญากรรมาลงโทษตามกฎหมายได้นั้นย่อมกระทบกระเทือนต่อความสงบเรียบร้อยของสังคมและเสรีภาพของประชาชนผู้สุจริตที่ถูกคุกคามจากภัยอาชญากร[31] แนวคิดในเรื่องอำนาจรัฐในการรักษาความสงบเรียบร้อย หรือแนวความคิดตามทฤษฎีการควบคุมอาชญากรรม จึงมุ่งส่งเสริมประสิทธิภาพของกระบวนการยุติธรรมในด้านการควบคุม ระงับและปราบปรามอาชญากรรมเป็นหลัก โดยการดำเนินงานในกระบวนการยุติธรรมต้องมีความรวดเร็วและแน่นอน ขั้นตอนต่างๆ ในกระบวนทางอาญาจะต้องไม่มีแบบพิธีที่เป็นอุปสรรคต่อการค้นหาข้อเท็จจริง การดำเนินคดีและการพิจารณาพิพากษาคดีตามหลักแนวคิดดังกล่าวกระบวนการการดำเนินคดีทางอาญาจะมีขึ้นเพื่อสร้างความสงบเรียบร้อยขึ้นในสังคมเท่านั้น เจ้าหน้าที่รัฐต้องมีวิธีการใดๆ เพื่อให้ได้มาซึ่งพยานหลักฐานพิสูจน์การกระทำความผิดของอาชญากรและวิธีการค้นหาพยานหลักฐานดังกล่าวอาจเป็นการละเมิดสิทธิเสรีภาพบางส่วนของประชาชนได้ ซึ่งรวมถึงวิธีการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ แต่อย่างไรก็ตามรัฐก็ต้องคำนึงถึงการคุ้มครองสิทธิและเสรีภาพของประชาชนที่บริสุทธิ์ควบคู่กันไปด้วย กล่าวคือ รัฐต้องพยายามในการที่จะให้ความคุ้มครองแก่ประชาชนให้มากที่สุดและจำเป็นที่จะต้องใช้อำนาจในการป้องกันและปราบปรามอาชญากรรมอย่างมีประสิทธิภาพ โดยประชาชนเองจำต้องยอมให้รัฐผลักภาระบางประการให้แก่ประชาชนได้และย่อมส่งผลให้สิทธิบางส่วนของประชาชนจะได้รับความคุ้มครองน้อยลงไปด้วย

ดังนั้น เจ้าหน้าที่รัฐจำเป็นต้องปฏิบัติหน้าที่เพื่อรักษาความสงบเรียบร้อยของสังคมโดยยึดถือหลักสำคัญที่คุ้มครองสิทธิและเสรีภาพของประชาชนที่เรียกว่า “หลักนิติรัฐ” (Legal State

---

[29] จิรนิติ หะวานนท์. (2527, พฤษภาคม-มิถุนายน). “หลักการไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ:เปรียบเทียบระหว่างกฎหมายอเมริกันและกฎหมายเยอรมัน.” *ดุลพาห, 31 (3).* หน้า 36.

[30] กิตติมา ประคุณคดี. (2533). *การดักฟังทางโทรศัพท์โดยเจ้าพนักงาน.* หน้า. 8.

[31] สำนักงานศาลยุติธรรม สถาบันวิจัยรพีพัฒนศักดิ์. (2550). *การออกหมายค้น หมายจับตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540.* หน้า 14.

Principle) ซึ่งมีสาระสำคัญว่ารัฐหรือเจ้าหน้าที่ของรัฐจะกระทำการใดที่กระทบสิทธิหรือเสรีภาพของประชาชนได้ก็ต่อเมื่อมีกฎหมายให้อำนาจควบคู่กันไปด้วย

2.3 การใช้อำนาจดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์

เนื่องจากการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาที่ถือว่าเป็นการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ของผู้อื่นการศึกษาถึงแนวความคิดที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาจึงจำเป็นต้องทราบถึงแนวความคิดพื้นฐานเกี่ยวกับการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลมูลอิเล็กทรอนิกส์ด้วยซึ่งแนวคิดและแนวทางการพัฒนาการใช้อำนาจดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์มีที่มาจากการที่กระบวนการยุติธรรมของนานาประเทศต่างต้องการสืบสวนสอบสวนการกระทำความผิดที่จะเกิดหรือเกิดขึ้นแล้ว เพื่อป้องกันอาชญากรรมร้ายแรงที่เกิดขึ้นภายในประเทศของตนในทุกวิถีทางเพื่อธำรงไว้ซึ่งความสงบสุข ดังนั้นจึงมีความจำเป็นต้องบัญญัติกฎหมายที่ให้อำนาจแก่เจ้าหน้าที่รัฐในการละเมิดสิทธิเสรีภาพส่วนบุคคลเพื่อเข้าถึงข้อมูลข่าวสารที่ติดต่อถึงกันได้ ในขณะเดียวกันก็ต้องคุ้มครองสิทธิเสรีภาพของประชาชนมิให้ถูกล่วงละเมิดจนเกินขอบเขตความเป็นมาของการบัญญัติกฎหมายให้อำนาจแก่เจ้าหน้าที่รัฐในการใช้การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ ประเทศแรกๆ ที่มีการบัญญัติกฎหมายการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ก็คือ ประเทศสหรัฐอเมริกาซึ่งเริ่มในปี ค.ศ. 1928 ศาลสูงของสหรัฐอเมริกาได้พิจารณาบทบัญญัติในรัฐธรรมนูญ แก้ไขเพิ่มเติมฉบับที่ 4 เกี่ยวกับดักฟังทางโทรศัพท์เป็นครั้งแรกในคดี Olmstead v. United States[32] ซึ่งในคดีนี้เจ้าหน้าที่ของรัฐบาลกลางได้ดักฟังการสนทนาที่มีการกล่าวโทษกัน ด้วยการติดอุปกรณ์บนสายโทรศัพท์ (Tapping the Telephone Wires) นอกบ้านพักของจำเลย โดยปราศจากหมายค้นหรือความยินยอมของจำเลย คณะผู้พิพากษาเสียงข้างมากวินิจฉัยว่า การดักฟังทางโทรศัพท์ดังกล่าวไม่ถือเป็นการค้นหรือการยึดในความหมายตามบทบัญญัติในรัฐธรรมนูญ แก้ไขเพิ่มเติมฉบับที่ 4

ด้วยเหตุผลที่ว่าไม่มีการค้นสถานที่เกิดขึ้นในคดีนี้ เนื่องจากเจ้าหน้าที่ของรัฐบาลกลางดักฟังการสนทนา โดยปราศจากการเข้าไปในเคหสถานหรือ สถานที่ทำงานของจำเลย และเสมือนไม่มีการตรวจสอบสถานที่ใดๆ ทั้งยังไม่มีการยึดสิ่งของเกิดขึ้นเพราะการดักฟังการสนทนาไม่ใช่สิ่งของที่จับต้องได้ ศาลจึงเห็นว่าจำเลยได้รับความคุ้มครองสิทธิตามบทบัญญัติในรัฐธรรมนูญแล้ว

---

[32] Olmstead v. United States. 277 U.S. 438. (1928). Retrived October 1. 2008, from *http://www.law.cornell.edu.*

คณะผู้พิพากษาพิจารณาว่าการดักฟังทางโทรศัพท์ไม่เป็นการละเมิดข้อห้ามว่าด้วยการค้นและการจับตามบทบัญญัติรัฐธรรมนูญแห่งสหรัฐอเมริกา แก้ไขเพิ่มเติมฉบับที่ 4 ตราบเท่าที่เจ้าหน้าที่ของรัฐมิได้ล่วงล้ำในทรัพย์สินของบุคคลที่ถูกดักฟังทางโทรศัพท์

แม้ว่ารัฐธรรมนูญแห่งสหรัฐอเมริกา แก้ไขเพิ่มเติมฉบับที่ 4 บัญญัติขึ้นขณะที่เทคโนโลยียังไม่พัฒนาแต่มิได้ละเลยเจตนารมณ์ของรัฐธรรมนูญที่ต้องการคุ้มครองสิทธิและเสรีภาพ โดยเฉพาะสิทธิความเป็นส่วนตัวของบุคคล (Right of Privacy) การไม่ได้รับความยินยอมและการไม่มีหมายให้ดักฟังทางโทรศัพท์โดยไม่จำเป็นต้องคำนึงถึงเรื่องวิธีการหรือสถานที่ที่ถูกเฝ้าสังเกตและติดตาม ย่อมเป็นการฝ่าฝืนต่อบทบัญญัติในรัฐธรรมนูญดังกล่าวในประเด็นผลประโยชน์ส่วนบุคคล

อย่างไรก็ดีศาลสูงของสหรัฐอเมริกาก็ได้ยึดแนวคำวินิจฉัยในคดี Olmstead มาเป็นเวลานานกว่า 40 ปี การดักสัญญาณหรือการดักฟังการติดต่อสื่อสาร (Wiretapping) เจ้าหน้าที่รัฐสามารถกระทำได้ หากไม่มีการล่วงล้ำในทรัพย์สินของบุคคลที่ถูกดักฟัง แต่ถ้าการสืบสวนสอบสวนของเจ้าหน้าที่รัฐไปล่วงล้ำในทรัพย์สินของบุคคลที่ถูกดักฟังทางโทรศัพท์ ศาลก็จะไม่รับฟังพยานหลักฐานที่ได้มาภายใต้ Federal Communications Act of 1934 ซึ่งบัญญัติห้ามดักสัญญาณการสื่อสารของพลเรือนและห้ามเปิดเผยข้อมูลที่ได้จากการดักสัญญาณการสื่อสารของพลเรือน

ต่อมาเมื่อปี ค.ศ. 1967 ศาลสูงของสหรัฐอเมริกาได้กลับแนวคำวินิจฉัยคดี Olmstead ในการพิจารณาคดี Katz v. United States[33] ซึ่งในคดีนี้เจ้าหน้าที่ได้ติดตั้งอุปกรณ์การฟัง (Listening Device) ไว้ด้านนอกตู้โทรศัพท์สาธารณะเพื่อบันทึกเสียงการสนทนาของจำเลย จากนั้นมีการนำข้อมูลที่ได้มาจัดทำเป็นเอกสารในการกล่าวโทษ โดยศาลตัดสินว่าการดักฟังทางโทรศัพท์โดยไม่มีหมายดังกล่าวมานั้น เป็นการกระทำที่ขัดต่อรัฐธรรมนูญ

ศาลสูงของสหรัฐอเมริกาได้พิจารณาว่าบทบัญญัติในรัฐธรรมนูญแห่งสหรัฐอเมริกาแก้ไขเพิ่มเติมฉบับที่ 4 มุ่งคุ้มครองบุคคลมิใช่สถานที่และขยายความคุ้มครองไปยังสถานที่ใดๆที่ปัจเจกบุคคลยังคงเหตุผลในการคาดหวังความเป็นส่วนตัว (Reasonable Expectation of Privacy) โดยศาลเห็นว่าในคดีนี้ จำเลยยังคงเหตุผลในการคาดหวังความเป็นส่วนตัว ทั้งในการสนทนาและในตู้โทรศัพท์สาธารณะที่ใช้ในการสนทนา คดี Katz ทำให้การที่เจ้าหน้าที่รัฐดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ต้องมีการออกหมายอนุญาตให้ดำเนินการให้เป็นไปตามบทบัญญัติในรัฐธรรมนูญแห่งสหรัฐอเมริกา ศาลสูงของสหรัฐอเมริกาได้มีคำวินิจฉัยในการตัดสินคดี Katz แตกต่างไปจากคดี Olmstead ดังกล่าวมาข้างต้น โดยศาลไม่คำนึงถึงแต่เพียงว่ามีการล่วงล้ำ

---

[33] Katz v. United States. 389 U.S. 347. (1967). Retrieved October 1. 2008, from *http://www.uscourts.gov.*

ในทรัพย์สินของบุคคลที่ถูกดักฟังทางโทรศัพท์หรือไม่เท่านั้น หากแต่ศาลคำนึงถึงสิทธิความเป็นส่วนตัวของบุคคลที่ถูกดักฟังทางโทรศัพท์ด้วย ด้วยเหตุผลที่ว่าบุคคลใดต่างก็ต้องการสิทธิความเป็นส่วนตัวของตน

ดังนั้นรัฐจึงมีหน้าที่ต้องให้ความคุ้มครองสิทธิดังกล่าวด้วย หากจะมีการดักฟังทางโทรศัพท์บุคคลใด เจ้าหน้าที่รัฐจะต้องได้รับอนุญาตหรือขอหมายจากศาลก่อน

ต่อมาในปี ค.ศ. 1968 ซึ่งเป็นระยะเวลาหนึ่งปีหลังศาลพิจารณาคดี Katz สภานิติบัญญัติของสหรัฐอเมริกาได้เห็นชอบกับแนวคำวินิจฉัยในคดีดังกล่าว และมีการบัญญัติกฎหมาย Omnibus Crime Control and Safe Street Act of 1968 Title III ว่าด้วยเรื่องการดักฟังการติดต่อสื่อสารโดยตรงและผ่านทางสาย (Interception of wire and oral communications) ทั้งในส่วนของภาครัฐและภาคเอกชนไว้ กล่าวคือ การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูล ทางอิเล็กทรอนิกส์ที่ใช้ในภาครัฐถือเป็นเครื่องมือที่ใช้การสืบสวนสอบสวนการกระทำความผิดทางอาญา แต่ในภาคเอกชนถือเป็นเครื่องมือในการได้มาหรือป้องกันข้อมูลที่มีค่าหรือข้อมูลที่ทำให้เสื่อมเสีย

ต่อไปจะขอกล่าวถึงแนวคิดในประเทศที่ใช้กฎหมายระบบซีวิลลอว์ (Civil Law) หรือระบบประมวลกฎหมายเช่นเดียวกับประเทศไทย ในการบัญญัติกฎหมายเกี่ยวกับการใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ ก็คือ ประเทศเยอรมนีและประเทศฝรั่งเศส

ประเทศเยอรมนีมีการอนุญาตให้ใช้การดักฟังการสนทนาทางโทรศัพท์ เพื่อการสืบสวนการกระทำความผิดในคดีอาชญากรรมสำคัญ ตั้งแต่ปี ค.ศ. 1968 ซึ่งจะใกล้เคียงกับการที่ประเทศสหรัฐอเมริกามีการบัญญัติใช้กฎหมาย Omnibus Crime Control and Safe Street Act มาตรการดักฟังทางโทรศัพท์จะอนุญาตเฉพาะการกระทำความผิดในคดีอาชญากรรมสำคัญที่กำหนดไว้ เช่น ความผิดฐานค้ามนุษย์ การปลอมแปลงเงินตราหรือคดีฆาตกรรม ชิงทรัพย์ ปล้นทรัพย์ จับตัวเรียกค่าไถ่ ค้าทรัพย์สินที่ถูกโจรกรรมหรือคล้ายๆ กับความผิดฐานรับของโจรในประเทศไทย ความผิดฐานฟอกเงิน กฎหมายเกี่ยวกับอาวุธปืนหรือความผิดเกี่ยวกับยาเสพติด ทั้งนี้ กฎหมายจะอนุญาตให้เพียงเพื่อช่วยในการสืบสวน กรณีที่เมื่อเป็นไปไม่ได้หรือเป็นการยากที่จะค้นหาความจริงหรือหาตัวผู้ต้องสงสัยในการกระทำผิดด้วยวิธีการอื่นแล้วเท่านั้นการดักฟังทางโทรศัพท์ของประเทศเยอรมนีสามารถทำได้ทั้งกับผู้ต้องสงสัยในการกระทำความผิดหรือผู้ทำการแทนในนามของผู้กระทำความผิดเอง ผู้นำส่งข้อมูลข่าวสารผู้ทำหน้าที่รับข้อความทางโทรศัพท์แทนผู้กระทำความผิดหรือส่งต่อข้อมูลแทนผู้กระทำความผิดทางโทรศัพท์หรือผู้ที่ติดต่อกับผู้กระทำความผิดทางโทรศัพท์ ตามกฎหมายแล้วมาตรการดังกล่าวต้องมีคำสั่งของศาล โดยข้อมูลที่

ได้มาจะถูกนำมาใช้ เพื่อวัตถุประสงค์ในการเป็นพยานหลักฐานพิสูจน์ความผิดของจำเลยในชั้นศาลเท่านั้น หลังจากนั้นต้องทำลายเมื่อไม่มีความจำเป็นต้องใช้ข้อมูลนั้นในการดำเนินคดี

ความเป็นมาของการบัญญัติกฎหมายในการให้อำนาจแก่เจ้าหน้าที่รัฐในการใช้มาตรการดักฟังทางโทรศัพท์ของประเทศฝรั่งเศส เริ่มจากการที่ประเทศฝรั่งเศสได้ให้สัตยาบันอนุสัญญายุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน ค.ศ. 1950 เมื่อวันที่ 3 พฤษภาคม ค.ศ. 1974 ซึ่งมีการรับรองสิทธิเสรีภาพในการสื่อสารถึงกันของปัจเจกบุคคลและรัฐธรรมนูญแห่งสาธารณรัฐฝรั่งเศส ค.ศ. 1958 มาตรา 55 ก็บัญญัติไว้ว่าสนธิสัญญาหรือความตกลงใดๆ ที่ได้รับการให้สัตยาบันหรือความเห็นโดยชอบ เมื่อได้ประกาศโฆษณาแล้วย่อมมีค่าบังคับสูงกว่ารัฐบัญญัติ ทั้งนี้เมื่อภาคีอีกฝ่ายหนึ่งได้ปฏิบัติตามสนธิสัญญาหรือความตกลงนั้นๆ เช่นเดียวกัน ต่อมาได้เกิดปัญหาในการตีความระหว่าง ศาลฝรั่งเศสและศาลยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน ในคดี Kruslin ผู้พิพากษาสอบสวน (Le Judged'instruction)[34] แห่งเมือง Sain-Gaudens ทำการสอบสวนคดีความผิดฐานฆ่าคนตาย โดยได้มอบหมายให้เจ้าพนักงานตำรวจยุติธรรม (L'officier de police judiciaire) ทำการดักฟังและบันทึกการสนทนาทางโทรศัพท์ของบุคคลที่ใช้เครื่องโทรศัพท์ของนาย Terrieux ในคดี Baron ขณะสนทนากับผู้อื่นระหว่างวันที่ 15-17 มิถุนายน ค.ศ. 1982[35] ในวันสุดท้ายเจ้าพนักงานตำรวจยุติธรรมได้ดักฟังและบันทึกการสนทนาระหว่างนาย Kruslin ซึ่งพักอาศัยอยู่ในบ้านของ นาย Terrieux กับบุคคลอื่นซึ่งใช้โทรศัพท์สาธารณะติดต่อมาถึงนาย Kruslin ในระหว่างการสนทนาบุคคลดังกล่าวได้พูดถึงการปล้นร้านของเครื่องประดับชื่อ La Gerbe d'or ซึ่งตั้งอยู่ในเมือง Toulouse และเจ้าของร้านถูกฆ่าตายระหว่างการปล้นครั้งนั้นต่อมาได้มีการใช้ข้อมูลข่าวสารที่ได้จากการดักฟังและบันทึกการสนทนาทางโทรศัพท์มาดำเนินคดีกับ นาย Kruslin ในความผิดฐานลักทรัพย์โดยมีเหตุอุกฉกรรจ์และฆ่าคนโดยเจตนาแต่นาย Kruslin ได้ต่อสู้คดีว่าข้อมูลข่าวสารที่ได้จากการดักฟังสามารถใช้เป็นหลักฐานดำเนินคดีได้เฉพาะในคดี Baron ซึ่งเป็นมูลเหตุให้เกิดการดักฟังและบันทึกการสนทนาเท่านั้นจะใช้เป็นหลักฐานพิสูจน์ความผิดของตนที่ต้องหาซึ่งเป็นคดีใหม่ไม่ได้ ศาลชั้นต้นฝรั่งเศสพิพากษาว่าข้ออ้างของนาย Kruslin ฟังไม่ขึ้น

นาย Kruslin ได้ฎีกาคัดค้านคำพิพากษาของศาลล่างต่อ Cour de Cassotion โดยอ้างว่าตามบทบัญญัติแห่งอนุสัญญายุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน ค.ศ. 1950 ที่บัญญัติว่าการที่องค์กรหรือเจ้าพนักงานของรัฐแทรกแซงการใช้สิทธิส่วนตัว

---

[34] Code of Criminal Procedure. Retrieved October 10. 2008, from *www.legifrance.gour.fr*

[35] นิยม เติมศรีสุข. (2549). *มาตรา 25 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรการเข้าถึงข้อมูลข่าวสาร ความเป็นมา การบังคับใช้ และข้อเสนอในการพัฒนากฎหมาย.* หน้า 34 – 37.

ชีวิตครอบครัว เคหสถาน และการติดต่อสื่อสารถึงกันของปัจเจกบุคคลจะเป็นมาตรการซึ่งในสังคมประชาธิปไตยแล้ว จำเป็นแก่การป้องกันและปราบปรามการกระทำผิดอาญาได้ก็ต่อเมื่อการกระทำดังกล่าวเป็นไปโดยอาศัยอำนาจตามกฎหมายและกฎหมายนั้นต้องมีลักษณะสองประการดังต่อไปนี้

ประการแรก ต้องมีบทบัญญัติด้วยถ้อยคำที่ชัดแจ้งเพื่อให้ประชาชนได้ทราบล่วงหน้าว่าในกรณีใดและภายใต้เงื่อนไขเช่นไร องค์กรและเจ้าหน้าที่ของรัฐจึงจะมีอำนาจกระทำการซึ่งมีผลกระทบกระเทือนอย่างร้ายแรงต่อสิทธิในชีวิตส่วนตัวและสิทธิเสรีภาพในการติดต่อสื่อสารถึงกัน

ประการที่สอง ต้องมีบทบัญญัติกำหนดขอบเขตอำนาจ กระบวนการและรูปแบบของการใช้อำนาจดังกล่าวไว้อย่างชัดเจนแน่นอน เพื่อเป็นหลักประกันปัจเจกบุคคลจากการใช้อำนาจตามอำเภอใจขององค์กรและเจ้าหน้าที่ของรัฐ

อย่างไรก็ตาม Cour de Cassotion ได้มีคำพิพากษายกฎีกาของนาย Kruslin โดยให้เหตุผลว่าการตรวจการติดต่อสื่อสารถึงกันทางโทรคมนาคมของบุคคลโดยองค์กรและเจ้าหน้าที่ของรัฐที่มีอำนาจหน้าที่สอบสวนคดีอาญาที่ได้ทำลงภายใต้เงื่อนไขบางประการ เป็นการกระทำที่ชอบด้วยกฎหมายภายในและในขณะเดียวกันก็ชอบด้วยอนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานด้วย ข้อมูลข่าวสารที่ได้มาจากการกระทำดังกล่าวอาจใช้พิสูจน์ความผิดของจำเลยได้

ต่อมานาย Kruslin ได้ยื่นฟ้องต่อศาลยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน เพื่อพิจารณาว่ากฎหมายสาธารณรัฐฝรั่งเศสขัดต่ออนุสัญญายุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน

ศาลยุโรปพิจารณาแล้วเห็นว่า บทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาฝรั่งเศส ถือได้ว่าเป็นกฎหมายที่ให้อำนาจผู้พิพากษาสอบสวนหรือเจ้าพนักงานตำรวจยุติธรรมที่ได้รับมอบอำนาจ ทำการดักฟังและบันทึกการสนทนาทางโทรศัพท์ระหว่างบุคคลเพื่อที่จะทราบข้อเท็จจริง หรือพิสูจน์ความผิดและเอาตัวผู้กระทำความผิดมาฟ้องลงโทษ และหลักกฎหมายดังกล่าวก็มีคุณลักษณะสอดคล้องกับหลักการปกครองโดยกฎหมายทุกประการกล่าวคือ บุคคลทั่วไปสามารถรับรู้ได้ อีกทั้งยังมีความแน่นอนชัดเจนเพียงพอที่จะทำให้ปัจเจกบุคคลสามารถคาดหมายได้ล่วงหน้าว่า ในกรณีใดและภายใต้เงื่อนไขเช่นไร ผู้พิพากษาสอบสวนหรือเจ้าพนักงานตำรวจยุติธรรมผู้รับมอบอำนาจ จะทำการดักฟังและบันทึกการสนทนาได้แต่กฎหมายดังกล่าวยังขาดหลักประกันที่สำคัญคือ

1) ไม่ปรากฏว่ามีบทบัญญัติแห่งกฎหมายหรือคำพิพากษาใด ได้กำหนดประเภทของบุคคลที่อาจถูกดักฟังการสนทนาทางโทรศัพท์ และประเภทของความผิดที่อาจใช้มาตราดังกล่าวไว้ ดังนั้นจึงเปิดช่องให้มีการดักฟังการสนทนาทางโทรศัพท์ของปัจเจกบุคคลไว้อย่างกว้างขวาง

2) ไม่ปรากฏว่ามีบทบัญญัติแห่งกฎหมายหรือคำพิพากษาใด กำหนดระยะเวลาขั้นสูงที่จะทำการดักฟังการสนทนาทางโทรศัพท์ของบุคคลเอาไว้

3) ไม่ปรากฏว่ามีบทบัญญัติแห่งกฎหมายหรือคำพิพากษาใด กำหนดเงื่อนไขของการถ่ายการสนทนาเป็นลายลักษณ์อักษร มาตรการรักษาสิ่งบันทึกการสนทนาเพื่อป้องกัน

การตัดต่อหรือทำให้เสียลักษณะดั้งเดิมเอาไว้ ทำนองเดียวกัน กฎหมายฝรั่งเศสก็มิได้กำหนดบังคับให้มีการลบหรือทำลายสิ่งบันทึกการสนทนาเมื่อหมดความจำเป็นต้องใช้เอาไว้ ศาลยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานจึงตัดสินว่าระบอบกฎหมายของฝรั่งเศสที่เกี่ยวกับการตรวจตราการสื่อสารถึงกันทางโทรคมนาคมยังไม่สอดคล้องกับอนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน ค.ศ. 1950 จึงเป็นเหตุปัจจัยสำคัญที่ทำให้สาธารณรัฐฝรั่งเศส ได้ตรารัฐบัญญัติเลขที่ 91-646 ลงวันที่ 10 กรกฎาคม ค.ศ. 1991 ว่าด้วยการคุ้มครองความลับของการสื่อสารถึงกันทางโทรคมนาคมขึ้นใช้บังคับตั้งแต่นั้นเป็นต้นมา โดยมีเนื้อหาของบทบัญญัติว่า ความลับของการสื่อสารถึงกันทางโทรคมนาคมย่อมได้รับความคุ้มครองตามกฎหมาย องค์กรของรัฐจะกระทำการใดๆ ที่มีผลกระทบกระเทือนต่อความลับของการสื่อสารถึงกันได้ ก็เฉพาะแต่ในกรณีที่จำเป็นแก่การธำรงรักษาไว้ซึ่งประโยชน์สาธารณะและภายในขอบเขตที่กำหนดไว้ในกฎหมายนี้เท่านั้น

2.3.1 ความหมายและรูปแบบของการดักฟังทางโทรศัพท์

การดักฟังทางโทรศัพท์ (Wire Tap) หมายถึง การลอบฟังด้วยเครื่องมืออิเล็กทรอนิกส์ประเภทหนึ่งในลักษณะเป็นการดักฟังการสื่อสารทางโทรศัพท์โดยปราศจากความยินยอมของคู่สนทนาทั้งสองฝ่าย

การดักฟังทางโทรศัพท์ คือการติดตามการสนทนาทางโทรศัพท์ (Monitoring of telephone conversations) และทางอินเตอร์เน็ทโดยบุคคลที่สาม ส่วนใหญ่ดำเนินการด้วยวิธีการปกปิดเหตุที่ได้ชื่อว่า “การดักฟังทางโทรศัพท์” เป็นเพราะใช้วิธีการต่อเชื่อมอุปกรณ์ติดตามการสนทนาเข้ากับสายโทรศัพท์ของบุคคลที่จะถูกติดตามการสนทนา และถอนอุปกรณ์ออกหรือการติดอุปกรณ์รับสัญญาณไฟฟ้าขนาดเล็กเพื่อรับฟังการสนทนา[36]

---

[36] Code of Criminal Procedure Retrieved October 10. 2008, from *www.legifrance.gour.fr*

การลักลอบฟังข้อมูลข่าวสารด้วยอุปกรณ์ดักฟัง (Wiretapping) หมายถึง รูปแบบของการลอบฟังทางอิเล็กทรอนิกส์โดยการดักจับข้อมูลหรือแอบฟังทางโทรคมนาคมด้วยวิธีการปกปิดการบันทึกข้อมูลหรือการใช้เครื่องดักฟังการติดต่อสื่อสารผ่านทางสาย[37]

การดักฟัง หมายถึง การลอบฟังการสนทนาด้วยเครื่องมืออิเล็กทรอนิกส์ในลักษณะที่เป็นการดักฟังการสื่อสารทางโทรศัพท์ที่บุคคลอื่นมีถึงกัน โดยมิได้รับความยินยอมจากคู่สนทนานั้นซึ่งการดักฟังไม่จำเป็นจะต้องดักฟังเฉพาะโทรศัพท์เท่านั้น แต่ในความหมายที่แท้จริงการดักฟังเป็นการดำเนินการเพื่อให้ล่วงรู้ข้อมูลของบุคคล โดยใช้เครื่องมืออิเล็กทรอนิกส์ เพื่อให้ได้ข้อมูลข่าวสารซึ่งส่งทางสายหรือคลื่นแม่เหล็กอื่นๆ อาจจะเป็นข้อมูลที่ส่งทางอินเตอร์เน็ต โทรสารโทรพิมพ์หรือการลักลอบดักฟังคลื่นที่ส่งไปในอากาศเพื่อให้ได้ข้อมูลข่าวสาร และปัจจุบันเครื่องมืออิเล็กทรอนิกส์ดังกล่าวก็มีหลากหลายประเภท

ตัวอย่างเครื่องมืออิเล็กทรอนิกส์ที่ใช้ดักฟังการสนทนา เช่น[38]

1) กล้องวงจรปิดซ่อนในฐานโคมไฟ มีเครื่องส่งภาพ วีดีโอไร้สายในตัว เพียงเสียบปลั๊กไฟ ก็สามารถเห็นภาพในจอมอนิเตอร์ด้วยระบบ Infrared ทำให้สามารถเห็นภาพในที่มืดได้

2) กล้องส่องในที่มืดระบบ Infrared สามารถเห็นภาพในเวลากลางคืนได้สว่างเหมือนกลางวัน กล้องจะส่งแสง Infrared ที่มองไม่เห็นด้วยตาเปล่าออกไป สะท้อนกับวัตถุซึ่งอยู่ในที่มืดแสงนั้นจะสะท้อนกลับมายังเครื่องจับแสง Infrared ซึ่งจะทำให้เห็นภาพได้

3) เครื่องดักฟังขนาดเล็กไร้สาย ใช้ระบบคลื่นวิทยุ FM และ UMF ส่งสัญญาณได้ไกลประมาณ 300 เมตร การใช้งานสามารถนำไปวางที่เป้าหมายและเครื่องจะส่งสัญญาณไปยังเครื่องรับ

4) เครื่องบันทึกโทรศัพท์อัตโนมัติ สามารถบันทึกการสนทนาทางโทรศัพท์ได้ เครื่องจะทำงานโดยอัตโนมัติ เมื่อมีสัญญาณโทรเข้าหรือโทรออกและหยุดทำงานเมื่อวางสาย สามารถติดตั้งและเดินสายนำไปซ่อนอำพรางสายตาผู้อื่นได้

5) เครื่องดักฟังโทรศัพท์ เป็นปลั๊กเสียบเข้ากับปลั๊กโทรศัพท์ทั่วไปเพียงนำสายโทรศัพท์มาเสียบก็สามารถฟังคู่สนทนาได้ทั้งสองทาง สามารถฟังได้ทางคลื่นวิทยุ FM

6) เครื่องดักฟังข้ามกำแพง สามารถนำไมโครโฟนไปแนบกำแพงห้อง ซึ่งหนาไม่เกิน 6 นิ้ว เพื่อฟังการสนทนาของอีกห้องหนึ่งได้

7) เครื่องดักฟังโทรศัพท์มือถือ ระบบ 800 MHz และ 900 MHz สามารถดักฟังโทรศัพท์เคลื่อนที่หรือมือถือได้ สำหรับการใช้งานกับโทรศัพท์เคลื่อนที่หรือมือถือที่อยู่ห่างไม่ถึง 10 กิโลเมตร

---

[37] USA: West Publishing. (1997). *West's encyclopedia of American Law.* p. 270.

[38] กมลชัย รัตนสกาววงศ์ และ วรพจน์ วิศรุตพิชญ์. เล่มเดิม. หน้า 24.

สำหรับวิธีการที่ใช้ในการดักฟังทางโทรศัพท์นั้นอาจทำได้หลายวิธี[39] ดังต่อไปนี้

1) Loop Interception คือ การดักฟังทางโทรศัพท์โดยการพ่วงสายหรือ Tap สายโทรศัพท์ที่แยกจากตู้พักสายเดินเข้าอาคารที่ต่อเข้ากับเครื่องโทรศัพท์

2) Trunk Interception คือ การดักฟังทางโทรศัพท์โดยการดักสัญญาณจากสายที่เดินต่อจากชุมสายขนาดใหญ่ ซึ่งใช้ร่วมกันหลายเลขหมาย ต้องใช้ไมโครโปรเซสเซอร์ช่วยเลือกดักฟังเฉพาะหมายเลขโทรศัพท์ที่ต้องการฟัง

3) Microwave Truck คือ การดักฟังทางโทรศัพท์ในกรณีที่เป็นการเชื่อมโยงที่ชุมสายที่อยู่ห่างกัน ตัวอย่างเช่น การโทรศัพท์ทางไกลระหว่างจังหวัดจะใช้จานรับสัญญาณติดในระยะทาง 5 ไมล์จากเครื่องรับปลายทาง เพื่อดูดสัญญาณจากสายอากาศนำเข้าเครื่องแปลงสัญญาณ และทำการดักรับข้อมูลการสื่อสารเฉพาะหมายเลขที่ต้องการ จึงจะบันทึกการสนทนาไว้

4) Satellite Interception คือ การดักฟังทางโทรศัพท์โดยวิธีการเช่นเดียวกับ Microwave Trunk เพียงแต่ใช้จานดาวเทียมแทนชุมสายขนาดใหญ่

5) Fiber Optic Trunk คือ การดักฟังทางโทรศัพท์จากสายเคเบิ้ลใยแก้วนำแสงซึ่งต้องใช้เทคนิคอย่างสูงประกอบกับต้องต่อเพิ่มกับอุปกรณ์อื่น

6) การดักฟังทางโทรศัพท์จากตู้สวิทซ์ที่ชุมสาย วิธีนี้กระทำได้โดยใช้คีมปากปูช่วยในการดักฟังกาสนทนาของบุคคลทางโทรศัพท์บ้านหรือโทรศัพท์ที่ใช้สาย ซึ่งการติดต่อสื่อสารถึงกันจะต้องผ่านชุมสายโทรศัพท์ก่อน จากชุมสายจะผ่านไปยังตู้โทรศัพท์ข้างถนน แล้วจึงแปรสัญญาณคลื่นแม่เหล็กไฟฟ้าเป็นสัญญาณเสียง ระหว่างทำการดักฟัง ผู้ดักฟังจะต้องรู้หมายเลขโทรศัพท์และคู่สายที่ต้องการดักฟังหรือรู้หมายเลขที่ผู้ที่เป็นเป้าหมายแห่งการดักฟังก่อน หลังจากนั้นจึงดำเนินการเปิดตู้เขียวขององค์การโทรศัพท์ ซึ่งตั้งอยู่ริมถนนทั่วไป แล้วนำคีมปากปูไปหนีบตรงคู่สายดังกล่าว ก็จะสามารถฟังการสนทนาทางโทรศัพท์ได้

7) การดักฟังทางโทรศัพท์ที่ชุมสายขององค์การโทรศัพท์ เมื่อทราบหมายเลขของเป้าหมายที่จะทำการดักฟังทางโทรศัพท์แล้ว โดยทั่วไปแต่ละชุมสายขององค์การโทรศัพท์จะมีโปรแกรมซอฟท์แวร์ช่วยในการดักฟังทางโทรศัพท์ เมื่อใช้คีมปากปูคีบชุมสายของหมายเลขเป้าหมายแล้วต่อเข้ากับลำโพงก็จะสามารถฟังการสนทนาได้ที่กล่าวมาข้างต้นเป็นเพียงตัวอย่างของวิธีการที่ใช้ในการดักฟังทางโทรศัพท์เท่านั้นการดักฟังทางโทรศัพท์อาจกระทำด้วยวิธีการอื่นๆ ได้อีกหลากหลายวิธีการและบางวิธีเป็นการดักฟังการสนทนาผ่านทางโทรศัพท์เคลื่อนที่หรือโทรศัพท์มือถือที่นิยมใช้กันอย่างแพร่หลายในปัจจุบันซึ่งจะต้องใช้โปรแกรมซอฟแวร์และเครื่องมือที่มีความก้าวหน้าทางเทคโนโลยีอย่างสูงในการดักข้อมูลการสนทนา

---

[39] แหล่งเดิม. หน้า 25.

ส่วนรูปแบบของการดักฟังทางโทรศัพท์ เราอาจแบ่งรูปแบบความสัมพันธ์ระหว่างผู้ดักฟังการสื่อสารทางโทรศัพท์ได้ 4 รูปแบบดังนี้[40]

รูปแบบที่หนึ่ง องค์กรที่ใช้อำนาจรัฐดักฟังการติดต่อกันทางโทรศัพท์ของเอกชน หมายถึงการที่เอกชนติดต่อกับเอกชนด้วยกันทางโทรศัพท์ หรืออาจจะติดต่อกับหน่วยงานของรัฐก็ได้ แต่องค์กรที่ใช้อำนาจรัฐซึ่งเป็นผู้ดักฟังนั้นได้ดักฟังจากเลขหมายโทรศัพท์ของเอกชนผู้เป็นเจ้าของเลขหมายนั้น และโดยปกติทั่วไปเอกชนก็เป็นผู้ใช้บริการโทรศัพท์เลขหมายนั้นด้วย

รูปแบบที่สอง องค์กรที่ใช้อำนาจรัฐดักฟังเจ้าหน้าที่ของรัฐที่กระทำการในนามของรัฐหรือในระหว่างปฏิบัติหน้าที่ราชการ โดยใช้เครื่องโทรศัพท์ของทางราชการ ซึ่งเจ้าหน้าที่ของรัฐในขณะที่ปฏิบัติหน้าที่ราชการอยู่นั้นอาจจะต้องรับผิดในการปฏิบัติหน้าที่ในฐานะส่วนตัว ไม่ว่าทางอาญาทางวินัยและในทางแพ่งก็ได้

รูปแบบที่สาม เอกชนดักฟังการติดต่อถึงกันทางโทรศัพท์ขององค์กรที่ใช้อำนาจรัฐ หมายถึง กรณีที่เอกชนประสงค์จะทราบข้อมูลหรือความลับของทางราชการ จึงกระทำการดักฟังการติดต่อสื่อสารถึงกันทางโทรศัพท์ขององค์กรที่ใช้อำนาจรัฐ หรือของเจ้าหน้าที่ของรัฐที่มีอำนาจหน้าที่ในการนั้น ไม่ว่าจะเป็นเลขหมายโทรศัพท์ของส่วนราชการหรือเลขหมายโทรศัพท์ส่วนตัวของเจ้าหน้าที่ของรัฐก็ตาม ทั้งนี้จะต้องพิจารณาจากมูลเหตุจูงใจของการดักฟังเพื่อทราบข้อมูลหรือความลับของทางราชการเป็นสาระสำคัญ

รูปแบบที่สี่ เอกชนดักฟังการติดต่อถึงกันทางโทรศัพท์ของเอกชนด้วยกันไม่ว่าจะเป็นเรื่องธุรกิจการค้าหรือเรื่องส่วนตัวอื่นๆ โดยไม่เกี่ยวข้องกับองค์กรที่ใช้อำนาจรัฐอย่างใด

จากรูปแบบของการดักฟังทางโทรศัพท์ทั้ง 4 รูปแบบข้างต้นนี้

รูปแบบแรกและรูปแบบที่สองเป็นการกระทำขององค์กรที่ใช้อำนาจรัฐซึ่งโดยหน้าที่ทั่วไปแล้วจะเป็นการดักฟังเพื่อแสวงหาพยานหลักฐานหรือสอบสวนหาข้อเท็จจริงให้ทราบว่าผู้ใดเป็นผู้กระทำความผิดทางอาญาหรือเกี่ยวข้องกับการกระทำความผิดทางอาญา ไม่ว่าผู้กระทำหรือผู้มีส่วนร่วมในการกระทำความผิดอาญานั้นจะเป็นเอกชนหรือเจ้าพนักงานของรัฐ การกระทำขององค์กรที่ใช้อำนาจรัฐในสองรูปแบบแรกนี้ มิอาจกระทำได้เลยหากไม่มีกฎหมายให้อำนาจและการกำหนดของเขตของการใช้อำนาจ เพราะจะเป็นการกระทำที่ขัดต่อรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 37

รูปแบบที่สามและรูปแบบที่สี่ เป็นการกระทำของเอกชนซึ่งมีบทบัญญัติแห่งกฎหมายบัญญัติเป็นข้อห้ามไว้โดยเด็ดขาดมิให้กระทำ ผู้กระทำการดักฟังการสื่อสารทางโทรศัพท์ย่อมมีความรับผิดทั้งทางแพ่งและทางอาญา ในทางแพ่ง การดักฟังการสื่อสารทางโทรศัพท์ของผู้อื่น

---

[40] แหล่งเดิม. หน้า 21 - 24.

ย่อมเป็นการทำละเมิดผู้กระทำต้องรับผิดชดใช้ค่าสินไหมทดแทนเพื่อความเสียหายที่เกิดจากการกระทำนั้นตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 ส่วนในทางอาญานั้นการดักฟังการสื่อสารทางโทรศัพท์ของผู้อื่นเป็นความผิดตามพระราชบัญญัติโทรเลขและโทรศัพท์ พ.ศ. 2477 มาตรา 24 การดักฟังทางโทรศัพท์ทั้งสองกรณีดังกล่าวกระทำโดยเอกชนซึ่งมีกฎหมายกำหนดความรับผิดและโทษอย่างชัดเจนแล้ว ในรายงานฉบับนี้จึงไม่รวมถึงการดักฟังทางโทรศัพท์รูปแบบที่สามและรูปแบบที่สี่โดยจะศึกษาเฉพาะกรณีที่องค์กรของรัฐเป็นผู้ดักฟังการสื่อสารทางโทรศัพท์ซึ่งอาจมีขึ้นได้ในรูปแบบที่หนึ่งและรูปแบบที่สองคือองค์กรที่ใช้อำนาจรัฐดักฟังการติดต่อถึงกันทางโทรศัพท์ของเอกชนและองค์การที่ใช้อำนาจรัฐดักฟังเจ้าหน้าที่ของรัฐที่กระทำการในนามของรัฐหรือในระหว่างการปฏิบัติหน้าที่ราชการโดยใช้เครื่องโทรศัพท์ของทางราชการเพราะรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 37 วรรคสองให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อรักษาความมั่นคงของรัฐหรือรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

2.3.2 ความหมายของการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์

ในส่วนนี้ถือว่าเกี่ยวข้องกับการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาโดยตรงซึ่งสิ่งแรกที่เราต้องเข้าใจก่อนอย่างแรกกล่าวคือ

คำว่า “ข้อมูลอิเล็กทรอนิกส์” หมายความถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษาหรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ และโทรสาร[41] ในประเทศสหรัฐอเมริกาคณะกรรมาธิการที่ปรึกษา[42] ได้ให้ความหมายของคำว่าข้อมูลคอมพิวเตอร์และสารสนเทศในรูปของดิจิตอลหรืออิเล็กทรอนิกส์อื่นๆ ไว้อย่างกว้างๆ โดยให้มีความหมายรวมถึง แฟ้มไปรษณีย์เสียง (Voice Mail Files) แฟ้มไปรษณีย์เสียงสำรอง (Backup Voice Mail Files) แฟ้มและไปรษณีย์อิเล็กทรอนิกส์หรืออีเมล์ (E-mail Messages and Files) แฟ้มอีเมล์สำรอง (Backup E-mail Files) อีเมล์ที่ถูกลบทิ้ง (Deleted E-mail) แฟ้มข้อมูล (Data Files) แฟ้มโปรแกรม (Program Files) แถบบันทึกสำรองและถาวร (Backup and Archival) แฟ้มข้อมูลชั่วคราว (Temporary Files) แฟ้มประวัติระบบ (System History Files) สารสนเทศของเว็บไซต์ที่เก็บอยู่ในรูปแบบของข้อความ (Texts) รูปภาพ (Graphics) หรือเสียง (Audio) แฟ้มลงบันทึกเข้าออกเว็บไซต์ (Web Site Log Files) แฟ้มแคช (Cache Files)

---

[41] ชัยวัฒน์ วงศ์วัฒนศานต์, ทวีศักดิ์ กออนันตกูล และสุรางคณา แก้วจำนง. (2544). *คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544.* หน้า 16.

[42] ประเสริฐ คันธมานนท์ และ สมชัย จันทรมัสการ. (2549, มีนมคม). “พยานหลักฐานดิจิตอล.” *บทบัณฑิตย์, 6 (1).* หน้า 44.

คุกกี้ (Cookies) และสารสนเทศอื่นๆ ที่บันทึกขึ้นโดยอุปกรณ์อิเล็กทรอนิกส์ข้อมูลทางอิเล็กทรอนิกส์นั้น ย่อมหมายความรวมถึงการได้มาซึ่งหมายเลขโทรศัพท์ที่โทรเข้าหรือโทรออกโดยใช้ Pen register Trap and Trace Device ตามรัฐบัญญัติ The Pen/Trap Statute, amended 2001 โดย 18 U.S.C. ของประเทศสหรัฐอเมริกา มาตรา 3127 (3) ได้นิยาม Pen Register ไว้ว่าหมายถึงอุปกรณ์หรือกระบวนการซึ่งบันทึกหรือถอดรหัสสารสนเทศเกี่ยวกับการโทรศัพท์ การติดต่อ ที่อยู่หรือสัญญาณ ซึ่งมีการส่งโดยใช้อุปกรณ์หรือเครื่องมือที่ส่งตามสายหรือทางอิเล็กทรอนิกส์ อย่างไรก็ตามสื่ออิเล็กทรอนิกส์ดังกล่าวจะต้องไม่มีเนื้อหาของการสื่อสาร[43] ทั้งนี้ Pen Register จะไม่รวมถึงอุปกรณ์หรือกระบวนการที่ใช้ในการเรียกเก็บค่าบริการหรือบัญชีค่าใช้จ่าย (Cost Accounting)

ส่วนนิยามคำว่า อุปกรณ์ Trap and Trace หมายความถึง อุปกรณ์หรือกระบวนการซึ่งจับอิมพัลส์อิเล็กทรอนิกส์หรืออย่างอื่นที่ส่งเข้ามาโดยแสดงข้อมูลทางอิเล็กทรอนิกส์ที่เป็นหมายเลขผู้โทรเข้า หรือการติดต่อ ที่อยู่ หรือสัญญาณ ซึ่งสามารถระบุถึงแหล่งที่มาของการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ที่ให้บริการ อย่างไรก็ตามสื่ออิเล็กทรอนิกส์ดังกล่าว จะต้องไม่มีเนื้อหาของการสื่อสาร

Pen Register and Trap and Trace Device เป็นอุปกรณ์ที่เพียงทำให้ทราบเลขหมายที่มีการติดต่อสื่อสารระหว่างกันเท่านั้น แต่ไม่สามารถทำให้ทราบถึงเนื้อหาในการติดต่อจากการสนทนา รวมทั้งไม่สามารถทำให้ทราบได้ว่าคู่สนทนากันเป็นใคร แต่ถือเป็นการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์อย่างหนึ่ง เป็นเครื่องมือที่ให้ผู้ทำการสืบสวนสอบสวนสามารถมองเห็นภาพความเชื่อมโยงของเส้นทางการติดต่อสื่อสารระหว่างกัน หรือเส้นทางของข้อความจากจุดหนึ่งไปยังจุดหนึ่ง ซึ่งอาจบ่งชี้ได้ถึงกลุ่มคนที่คบค้าสมาคม นิสัย ความสนใจ และกิจกรรมของบุคคลที่เป็นเป้าหมายในการสืบสวนสอบสวนได้ ซึ่งผู้เขียนจะขอกล่าวโดยละเอียดต่อไปในบทที่ 3

ข้อมูลอิเล็กทรอนิกส์สามารถแบ่งออกเป็น 3 ประเภทหลักๆ ได้ดังนี้

ประเภทแรก คือ ข้อมูลอิเล็กทรอนิกส์ที่เพียงจัดเก็บไว้ในระบบคอมพิวเตอร์ซึ่งมนุษย์เป็นผู้สร้างข้อมูลดังกล่าวขึ้น

ประเภทที่สอง คือ ข้อมูลอิเล็กทรอนิกส์ที่สร้างขึ้นโดยระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ ความแตกต่างระหว่างข้อมูลทั้งสองประเภทจะขึ้นอยู่กับว่าข้อมูลอิเล็กทรอนิกส์นั้นมนุษย์หรือเครื่องคอมพิวเตอร์เป็นผู้สร้างข้อความในข้อมูลอิเล็กทรอนิกส์นั้น ฉะนั้น ข้อมูลที่จัดเก็บไว้ในระบบคอมพิวเตอร์ได้แก่ แฟ้มไปรษณีย์เสียง แฟ้มไปรษณีย์สำรองแฟ้ม

---

[43] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. (2002). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (แปลโดย) สำนักงานอัยการสูงสุด*. หน้า 133.

อีเมล์ แฟ้มอีเมล์สำรอง อีเมล์ที่ถูกลบทิ้ง แฟ้มข้อมูลแถบบนทึกสำรองและถาวร และสารสนเทศของเว็บไซต์ที่เก็บอยู่ในรูปแบบของข้อความ รูปภาพ หรือเสียง สำหรับข้อมูลอิเล็กทรอนิกส์ที่สร้างขึ้นโดยระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ได้แก่ แฟ้มโปรแกรม แฟ้มข้อมูลชั่วคราว แฟ้มประวัติระบบ แฟ้มลงบันทึกเข้าออกเว็บไซต์ แฟ้มแคช และคุกกี้เป็นต้น

ประเภทที่สาม คือ ข้อมูลอิเล็กทรอนิกส์ที่ประกอบไปด้วยข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บไว้ในระบบคอมพิวเตอร์และที่สร้างขึ้นโดยระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ทั้งสองประเภท ตัวอย่างเช่น ข้อมูลอิเล็กทรอนิกส์ที่เป็นแผนภูมิ (Chart) ซึ่งเป็นผลลัพธ์ที่ได้จากการทำงานของโปรแกรมตารางการทำงานหรือคำนวณ (Spreadsheet Program) เป็นต้น ข้อมูลอิเล็กทรอนิกส์ดังกล่าวเป็นผลที่ได้จากการที่ระบบคอมพิวเตอร์ประมวลผลข้อมูลตัวเลขต่างๆ ที่มนุษย์ใส่เข้าไปในระบบคอมพิวเตอร์

การได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์นั้นมีหลายวิธี แต่วิธีการได้มาโดยปราศจากการยินยอมของบุคคลคู่สนทนาทั้ง 2 ฝ่ายก็คือ

การดักข้อมูลการดักข้อมูลทางอิเล็กทรอนิกส์นั้นมีทั้งการใช้เครื่องมืออิเล็กทรอนิกส์ในการดักฟังกาสนทนา เพื่อให้ได้มาซึ่งเสียงและเนื้อหาของการสื่อสารและการใช้คอมพิวเตอร์หรือเครื่องมือทางอิเล็กทรอนิกส์ดักข้อมูลที่ส่งผ่านกันทางคอมพิวเตอร์หรือระบบโครงข่ายอินเตอร์เน็ต

การดักข้อมูลคอมพิวเตอร์ คือ การดักข้อมูลคอมพิวเตอร์หรือสิ่งต่างๆ ที่ได้มาจากการปฏิบัติงานของระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ เช่น คลื่นอิเล็กทรอนิกส์ (Electromagnetic Radiation) เป็นต้น การดักข้อมูลคอมพิวเตอร์อาจกระทำได้สองวิธี

วิธีแรก คือ การเข้าถึงระบบคอมพิวเตอร์โดยตรงแล้วจึงดักข้อมูลคอมพิวเตอร์

วิธีที่สอง คือ การใช้เครื่องดักข้อมูล (Electronic Eavesdropping Devices) ซึ่งเป็นการอาศัยเทคโนโลยีสมัยใหม่ดักข้อมูลคอมพิวเตอร์ โดยที่ผู้ดักข้อมูลไม่จำเป็นต้องเข้าถึงระบบคอมพิวเตอร์เลย เพียงแต่วางเครื่องดักข้อมูลไว้ในระยะที่สามารถดักข้อมูลได้ก็พอแล้ว[44] เมื่อพิจารณาถึงลักษณะและวิธีการดักข้อมูลแล้วจะเห็นว่า การดักข้อมูลสามารถกระทำได้โดยง่ายและสะดวกมากกว่าการเข้าถึงคอมพิวเตอร์ และการตรวจพบการกระทำความผิดดังกล่าวก็เป็นเรื่องยาก เนื่องจากผู้กระทำไม่จำเป็นต้องเข้าถึงระบบคอมพิวเตอร์และข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์ก็มิได้ถูกแก้ไขเปลี่ยนแปลง หรือเกิดความเสียหายแต่อย่างใดทำให้ไม่มีร่องรอยการกระทำ

---

[44] องอาจ เทียนหิรัญ. (2546). *อาชญากรรมทางคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์*. หน้า 31.

คำว่า การเข้าถึง หมายถึง การเข้าไป การสั่ง การสื่อสาร การนำข้อมูลเข้าไปเก็บไว้การนำข้อมูลออกมา การใช้ประโยชน์ใดๆ จากข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์

คำว่า การเข้าถึง หมายถึง การเป็นเหตุให้คอมพิวเตอร์ปฏิบัติหน้าที่ใดๆ แก้ไขเปลี่ยนแปลง หรือลบโปรแกรม หรือข้อมูล ทำซ้ำ หรือย้ายโปรแกรม หรือนำข้อมูลไปเก็บไว้ในที่อื่นการใช้โปรแกรมหรือข้อมูลซึ่งนำออกมาจากคอมพิวเตอร์ที่เก็บโปรแกรมหรือข้อมูลนั้นๆ

ข้อมูลคอมพิวเตอร์ หมายถึง การแสดงผลข้อเท็จจริง ข้อความ หรือความเห็นรูปแบบที่เหมาะสมสำหรับใช้ในการประมวลผลโดยระบบคอมพิวเตอร์ รวมทั้งโปรแกรมที่ทำให้ระบบคอมพิวเตอร์ รวมทั้งโปรแกรมที่ทำให้ระบบคอมพิวเตอร์ทำงาน

การเข้าถึง (Access) จะหมายรวมถึงการเข้าถึงทั้งหมดหรือเพียงบางส่วนของระบบคอมพิวเตอร์ซึ่งได้แก่ ฮาร์ดแวร์ (Hardware) ส่วนประกอบต่างๆ (Components) ข้อมูลต่างๆ ที่ถูกเก็บไว้ในคอมพิวเตอร์ แต่ไม่รวมถึงการส่งข้อความทางอิเล็กทรอนิกส์ (E-mail Message) หรือไฟล์ (File) ไปยังระบบคอมพิวเตอร์

การเข้าถึงนี้รวมถึงการเข้าระบบคอมพิวเตอร์ระบบอื่นด้วยในกรณีที่ระบบคอมพิวเตอร์นั้นถูกเชื่อมต่อกับเครือข่ายการติดต่อสื่อสารสาธารณะ (Public Telecommunication Networks) หรือระบบคอมพิวเตอร์ที่อยู่บนเครือข่ายเดียวกันระบบเครือข่ายคอมพิวเตอร์หากจำแนกตามระยะทางของการเชื่อมต่อระหว่างอุปกรณ์สื่อสารสามารถแบ่งได้เป็น 3 ประเภทดังนี้[45]

Local Area Network (LAN)

ระบบเครือข่ายแบบนี้จะเป็นเครือข่ายคอมพิวเตอร์ที่มีการเชื่อมต่ออุปกรณ์สื่อสารในระยะทางที่จำกัดซึ่งมีความเร็วในการแลกเปลี่ยนข้อมูลสูง เป็นเครือข่ายที่ใช้ในหน่วยงานต่างๆ เฉพาะกลุ่มจึงเป็นระบบเครือข่ายแบบปิด (Close Network) เช่น ระบบอินทราเน็ต (Intranet) เป็นต้น

Metropolitan Area Network (MAN)

เป็นระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ครอบคลุมพื้นที่มากกว่าระบบเครือข่ายแบบ LAN เครือข่ายนี้เกิดจากการเชื่อมต่อของเครือข่ายคอมพิวเตอร์แบบ LAN ตั้งแต่ 2 เครือข่ายเข้าด้วยกัน

Wide Area Network (WAN)

เป็นระบบเครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่ประกอบด้วยระบบเครือข่ายคอมพิวเตอร์ทั้งแบบ LAN และเครือข่ายคอมพิวเตอร์แบบ MAN พื้นที่ของเครือข่ายสามารถ

---

[45] ศรีไพร ศักดิ์รุ่งพงศากุล. (2544). *เทคโนโลยีคอมพิวเตอร์และสารสนเทศ*. หน้า 165.

ครอบคลุมพื้นที่ได้ไระดับประเทศหรือระดับโลก และเป็นระบบเครือข่ายแบบเปิด (Open Network) ระบบเครือข่ายอินเตอร์เน็ต (Internet) ก็เป็นระบบเครือข่ายแบบ WAN เช่นกัน

ระบบเครือข่ายอินเตอร์เน็ต (Internet Network)[46] เป็นระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เกิดขึ้นจากการเชื่อมต่อเครือข่ายต่างๆ ไม่ว่าจะเป็น LAN หรือ WAN หลายเครือข่ายเข้าด้วยกัน ทำให้เครื่องคอมพิวเตอร์นับล้านๆ เครื่องทั่วโลกสามารถติดต่อสื่อสารกันได้

เครื่องคอมพิวเตอร์แต่ละเครื่องที่เชื่อมต่อกับเครือข่ายอินเตอร์เน็ตจะใช้มาตรฐานของการสื่อสารแบบเดียวกัน เรียกว่า TCP/IP หรือ Transmission Control Protocol/Internet Protocol และเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่ายอินเตอร์เน็ตจะต้องมีหมายเลขประจำตัวของเครื่องนั้น หรือที่เรียกว่า IP Address ที่ประกอบด้วยเลขฐานสอง 4 ชุด ชุดละ 8 บิต ดังนั้น

เลขหมายของ IP Address จึงมีขนาด 32 บิต ต่อมาเพื่อความสะดวกในการใช้งานได้มีการแปลง IP Address ที่อยู่ในระบบตัวเลขฐานสองเป็นระบบเลขฐานสิบ 4 ชุดเช่นเดิม เนื่องจากเลขหมาย IP Address มีจำนวนมากขึ้น ทำให้ไม่สะดวกต่อการจำเลขหมาย ดังนั้นจึงได้มีการกำหนดชื่อที่เป็นตัวอักษรเพื่อใช้แทนหมายเลข IP Address โดยเรียกชื่อที่ใช้แทนว่า โดเมนเนม (Domain Name) ดังนั้น โดเมนเนม ก็คือชื่อที่เป็นตัวอักษรของเลขหมาย IP Address ของเครื่องคอมพิวเตอร์นั่นเอง

โดเมนเนมจะประกอบด้วยชื่อเครื่องคอมพิวเตอร์ ชื่อเครือข่ายท้องถิ่น ชื่อโดเมนย่อย และชื่อโดเมน

การเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตจำเป็นต้องอาศัยอุปกรณ์พื้นฐานสำคัญๆ ได้แก่ เครื่องคอมพิวเตอร์ โมเด็ม สายโทรศัพท์ โดยเชื่อมต่อระบบอินเทอร์เน็ตผ่านการให้บริการของผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider หรือ ISP)

ทั้งนี้ ในการเชื่อมต่อเครือข่ายอินเตอร์เน็ตจะมีอุปกรณ์สำคัญอีกชนิดหนึ่งซึ่งนับเป็นคอมพิวเตอร์ประเภทหนึ่งใช้ในการจัดหาเส้นทางที่จะเชื่อมระหว่างคอมพิวเตอร์เครื่องหนึ่งกับคอมพิวเตอร์อีกเครื่องหนึ่ง คือ อุปกรณ์จัดเส้นทาง หรือ Router

อย่างไรก็ตาม การเชื่อมต่อกับเครือข่ายอินเตอร์เน็ตมักเป็นการเชื่อมต่อโดยผ่านการให้บริการของผู้ให้บริการอินเตอร์เน็ตหรือ ISP แต่ในบางกรณีก็อาจเป็นการเชื่อมต่อกับเครือข่ายอินเตอร์เน็ตโดยตรง (Direct Internet Access) โดยไม่ผ่านการให้บริการของผู้ให้บริการอินเตอร์เน็ต มักเป็นการเชื่อมต่อกับระบบเครือข่ายอินเตอร์เน็ตโดยหน่วยงานของรัฐหรือสถาบันการศึกษาเป็นต้น

---

[46] ชัยวัฒน์ วงศ์วัฒนศานต์, ทวีศักดิ์ กออนันตกูล และสุรางคณา แก้วจำนง. เล่มเดิม. หน้า 50.

นอกจากการเชื่อมต่อกับอินเตอร์เน็ตที่กล่าวมาข้างต้น โดยทั่วไปแล้วเป็นการติดต่อระหว่างเครื่องคอมพิวเตอร์เท่านั้น ต่อมาจึงเริ่มมีการประยุกต์ให้มีการใช้บริการอินเตอร์เน็ตผ่านระบบโทรศัพท์มือถือได้ด้วย โดยเรียกเทคโนโลยีนี้ว่า WAP หรือ Wireless Application Protocol ที่สามารถใช้โทรศัพท์มือถือเชื่อมต่อกับเครือข่ายอินเตอร์เน็ตได้โดยไม่ต้องอาศัยโมเด็ม (MODEM) และสายโทรศัพท์เช่นเดิม

การใช้จดหมายอิเล็กทรอนิกส์ (Electronic Mail) หรือที่เรียกว่า e-mail นั้นก็เป็นรูปแบบการติดต่อสื่อสารอีกประเภทหนึ่งที่ใช้เครือข่ายอินเตอร์เน็ตเพื่อช่วยให้การติดต่อสื่อสารระหว่างบุคคลสะดวก และรวดเร็วยิ่งขึ้น หากจะเปรียบเทียบระหว่างการส่งจดหมายธรรมดาและจดหมายอิเล็กทรอนิกส์แล้ว โดยปกติในการส่งจดหมายธรรมดานั้น ผู้ส่งจะต้องมีการระบุชื่อและที่อยู่ของผู้รับในการส่งจดหมายอิเล็กทรอนิกส์ก็เช่นเดียวกัน ผู้ส่งจะต้องระบุที่อยู่ของผู้รับจดหมายอิเล็กทรอนิกส์นั้น

ที่อยู่ของผู้ส่งและผู้รับในระบบเครือข่ายอินเตอร์เน็ตนั้นเราเรียกว่า e-mail address เปรียบเสมือนชื่อบุคคล เลขที่บ้าน และที่อยู่ในการส่งจดหมายธรรมดา e-mail address จะประกอบด้วย ชื่อผู้ใช้ (User Name) และชื่อโดเมนเนม (Domain Name)

เนื่องจากกฎหมายของประเทศต่างๆ ส่วนใหญ่กำหนดให้การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเป็นความผิด ดังนั้นหากเจ้าหน้าที่ของรัฐต้องการเข้าถึงข้อมูลทางอิเล็กทรอนิกส์หรือทางคอมพิวเตอร์ ต้องมีกฎหมายให้อำนาจกระทำได้และต้องปฏิบัติตามบทบัญญัติดังกล่าวอย่างเคร่งครัด

การให้ความคุ้มครองความลับในการติดต่อสื่อสารนั้น ในต่างประเทศจะมีกฎหมายให้ความคุ้มครองในเรื่องนี้อยู่ เช่น ประเทศสหรัฐอเมริกามีกฎหมายที่เกี่ยวกับการควบคุมการดักฟังข้อมูลจากระบบการติดต่อสื่อสารต่างๆ เช่น กฎหมายห้ามการดักฟังโทรศัพท์ (Wiretapping) และการดักข้อมูลในระหว่างการติดต่อสื่อสาร (Interception of Data Communications)

2.4 การรับฟังพยานหลักฐานที่ได้มาจากการแสวงหาพยานหลักฐานทางคอมพิวเตอร์

ในเบื้องต้นของการรับฟังพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาจำเป็นต้องทราบความหมายของการรับฟังพยานหลักฐานในคดีอาญาก่อนโดย

การรับฟังพยานหลักฐาน หมายถึง ขั้นตอนในการที่ศาลจะวินิจฉัยหรือคัดเลือกว่าพยานหลักฐานชิ้นใดสามารถนำสืบหรือนาเข้าสู่สำนวนได้โดยชอบด้วยกฎหมาย[47] ซึ่งแตกต่างกับการชั่งน้ำหนักพยานหลักฐาน

---

[47] โสภณ รัตนากร. เล่มเดิม. หน้า. 53, 147.

ในการรับฟังพยานหลักฐานของศาลนั้นมิได้หมายความว่า หากพยานหลักฐานชิ้นใดได้ถูกเสนอต่อศาลแล้ว ศาลจะรับฟังพยานหลักฐานชิ้นนั้นๆ ได้เสมอไป ทั้งนี้เพราะพยานหลักฐานที่ศาลจะรับฟังได้นั้นมีหลักเกณฑ์อันเป็นข้อจำกัดกล่าวคือ ในเบื้องแรก พยานหลักฐานนั้นต้องเป็นพยานหลักฐานที่เกี่ยวข้องกับข้อเท็จจริงอันเป็นประเด็นแห่งคดีเสียก่อน[48] กล่าวอีกนัยหนึ่งก็คือต้องเป็นพยานหลักฐานซึ่งน่าจะพิสูจน์ความผิดหรือความบริสุทธิ์ของจำเลยได้ หรือเป็นพยานหลักฐานอันเกี่ยวกับเหตุลดโทษหรือเหตุบรรเทาโทษหรือเหตุอันควรรอการลงโทษก็ได้ หากพยานหลักฐานชิ้นใดไม่เกี่ยวข้องกับประเด็นหรือไม่ตรงประเด็นดังกล่าวแล้วย่อมเป็นพยานหลักฐานที่รับฟังไม่ได้อยู่เอง ซึ่งในการพิจารณาว่าพยานหลักฐานชิ้นใดเกี่ยวข้องกับประเด็นหรือไม่นั้นเป็นเรื่องของการใช้เหตุผลทางตรรกวิทยา แต่ถ้าพิจารณาได้ในเบื้องแรกว่าพยานหลักฐานนั้นเกี่ยวกับประเด็นแล้ว กรณีก็ยังอยู่ในบังคับแห่งกฎหมายว่าด้วยการรับฟังพยานหลักฐานด้วย หากมิได้ดำเนินการตามกฎหมายว่าด้วยการนี้แล้ว พยานหลักฐานนั้นแม้จะเกี่ยวกับประเด็นก็รับฟังไม่ได้[49] กล่าวโดยสรุปก็คือพยานหลักฐานที่รับฟังได้หมายถึงพยานหลักฐานซึ่งเกี่ยวข้องกับประเด็นแห่งคดีและไม่ถูกห้ามรับฟังโดยกฎหมายหรือกฎเกณฑ์ใดๆ

กฎหมายว่าด้วยการรับฟังพยานหลักฐาน คือบัญญัติว่าพยานหลักฐานอย่างใด รับฟังได้หรือไม่ได้ หรืออีกนัยหนึ่งเป็นการกำหนดว่าพยานหลักฐานใดนาสืบได้พยานหลักฐานใดนำสืบไม่ได้ หลักกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานอาจพิจารณาได้ทั้งทางด้านปฏิฐานอันเป็นทางรับหรืออาจพิจารณาทางด้านปฏิเสธก็ได้ เช่น หลักที่ว่าพยานหลักฐานต้องเกี่ยวกับประเด็นแห่งคดี อาจกล่าวในทางรับว่าพยานหลักฐานที่เกี่ยวกับข้อเท็จจริงในประเด็นรับฟังได้ หรืออาจกล่าวในทางปฏิเสธว่า พยานหลักฐานนอกประเด็นหรือไม่เกี่ยวกับประเด็นรับฟังไม่ได้[50] เป็นต้น

หลักในเรื่องการนำสืบพยานหลักฐานที่เกี่ยวกับประเด็นแห่งคดีนี้เป็นหลักสากลตรงกับกฎหมายคอมมอนลอว์เรื่อง Relevancy กล่าวคือ ในระบบการพิจารณาคดีเพื่อรับฟังพยานหลักฐานจากคู่ความนั้นไม่มีระบบการพิจารณาคดีใดในโลกที่จะยอมให้คู่ความนำเสนอพยานหลักฐานต่อศาลได้โดยไม่จำกัด ศาลย่อมต้องการที่จะรับฟังเรื่องที่เกี่ยวข้องในคดีเท่านั้น คู่ความจะถือโอกาสระบายเรื่องราวต่างๆ ให้ศาลรับรู้ไม่ได้ การพิจารณาว่าพยานหลักฐานใดเกี่ยวถึงข้อเท็จจริงในคดีส่วนใหญ่พิจารณาจากประเด็นข้อพิพาทเป็นหลักซึ่งกฎหมายคอมมอนลอว์เรียกว่า Materiality หรือ In Issue สำหรับพยานหลักฐานที่เกี่ยวกับประเด็นข้อพิพาทนี้อาจมีปัญหาชวนให้คิดว่า ในคดีอาญามีประเด็นเพียงว่าได้มีการกระทำความผิดเกิดขึ้น และจำเลย

---

[48] คนึง ฦาไชย. (2523). *พยาน*. หน้า 47.

[49] แหล่งเดิม. หน้า 45.

[50] โสภณ รัตนากร. เล่มเดิม. หน้า 53.

เป็นผู้กระทำผิดหรือไม่ จึงอาจทำให้สงสัยได้ว่าคู่ความจะเสนอพยานหลักฐานเพื่อประกอบดุลพินิจในการลงโทษได้หรือไม่ ปัญหาดังกล่าวนี้มีหลักว่าการลงโทษผู้กระทำผิดนั้นเกี่ยวเนื่องกับการวินิจฉัยว่าจำเลยมีความผิด ดังนั้นพยานหลักฐานที่นาเสนอเพื่อประกอบดุลพินิจในการลงโทษจึงรับฟังได้[51]

อย่างไรก็ตามแม้ว่าการรับฟังพยานหลักฐานจะกำหนดให้เกี่ยวข้องกับประเด็นแห่งคดีและไม่ถูกห้ามรับฟังแล้ว โดยกฎหมายหรือกฎเกณฑ์ใดๆ แล้วในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์นั้น พยานหลักฐานทางคอมพิวเตอร์ที่ได้มาจากมาตรการแสวงหาพยานดังกล่าวประมวลกฎหมายวิธีพิจารณาความอาญาของไทยก็เปิดโอกาสให้สามารถรับฟังได้แม้ว่าการใช้มาตรการดังกล่าวจะเป็นการละเมิดสิทธิของบุคคลอันเป็นการกระทำที่มิชอบ พยานหลักฐานดังกล่าวจึงเกิดขึ้นมาโดยชอบ แต่ได้มาโดยมิชอบ ซึ่งศาลอาจรับฟังได้หากพยานหลักฐานนั้นจะเป็นประโยชน์ต่อการอำนวยความยุติธรรมมากกว่าผลเสีย ซึ่งมาตรา 226/1 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ได้บัญญัติไว้ว่า

“มาตรา 226/1 ในกรณีที่ความปรากฏแก่ศาลว่า พยานหลักฐานใดเป็นพยานหลักฐานที่เกิดขึ้นโดยชอบ แต่ได้มาเนื่องจากการกระทำโดยมิชอบ หรือเป็นพยานหลักฐานที่ได้มาโดยอาศัยข้อมูลที่เกิดขึ้นหรือได้มาโดยมิชอบ ห้ามมิให้ศาลรับฟังพยานหลักฐานนั้น เว้นแต่การรับฟังพยานหลักฐานนั้นจะเป็นประโยชน์ต่อการอำนวยความยุติธรรมมากกว่าผลเสีย อันเกิดจากผลกระทบต่อมาตรฐานของระบบงานยุติธรรมทางอาญา หรือสิทธิเสรีภาพพื้นฐานของประชาชนในการใช้ดุลพินิจรับฟังพยานหลักฐานตามวรรคหนึ่ง ให้ศาลพิจารณาถึงพฤติการณ์ทั้งปวงแห่งคดีโดยต้องคำนึงถึงปัจจัยต่างๆ ดังต่อไปนี้ด้วย

(1) คุณค่าในเชิงพิสูจน์ ความสำคัญ และความน่าเชื่อถือของพยานหลักฐานนั้น

(2) พฤติการณ์และความร้ายแรงของความผิดในคดี

(3) ลักษณะและความเสียหายที่เกิดจากการกระทำโดยมิชอบ

(4) ผู้ที่กระทำการโดยมิชอบอันเป็นเหตุให้ได้พยานหลักฐานมานั้นได้รับการลงโทษหรือไม่เพียงใด

ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1 เป็นบทบัญญัติที่เจ้าพนักงานของรัฐจะแสวงหาพยานหลักฐานเพื่อพิสูจน์ความผิดของผู้ต้องหาและจำเลย ต้องกระทำไปตามหลักเกณฑ์ที่กฎหมายบัญญัติไว้ แม้การดำเนินคดีอาญาจะเป็นเรื่องการค้นหาความจริงว่าจำเลยกระทำความผิดหรือไม่ แต่ก็ไม่ได้หมายความว่าการค้นหาความจริงดังกล่าวจะกระทำได้ทุกวิถีทางโดยไม่คำนึงถึงสิทธิเสรีภาพของผู้ต้องหาและจำเลยอันเป็นสิทธิขั้นพื้นฐานที่กำหนดไว้ใน

---

[51] พรเพชร วิชิตชลชัย. (2542). *คำอธิบายกฎหมายลักษณะพยาน*. หน้า 106-113.

รัฐธรรมนูญ อย่างไรก็ตามมาตรา 226/1 วรรค 2 บัญญัติข้อยกเว้นให้รับฟังพยานหลักฐานที่ได้มาโดยมิชอบด้วยกฎหมายด้วย จึงมีปัญหาว่าเป็นการทำลายหลักการรับฟังพยานหลักฐานที่ได้มาโดยมิชอบหรือไม่

ดังนั้น จะเห็นได้ว่าการใช้มาตรการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาโดยการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ ที่ไม่มีบทบัญญัติให้อำนาจดังกล่าวไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา ทำให้การแสวงหาพยานหลักฐานดังกล่าว หากกระทำไปจะทำให้พยานหลักฐานดังกล่าวเกิดขึ้นมาโดยชอบ แต่ได้มาโดยมิชอบ เนื่องจากเป็นการกระทำที่กระทบต่อสิทธิเสรีภาพของบุคคลที่ขัดต่อรัฐธรรมนูญ ซึ่งประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1 ก็เปิดโอกาสให้ศาลสามารถรับฟังพยานหลักฐานดังกล่าวได้แม้ว่าการกระทำเพื่อให้ได้มาซึ่งพยานหลักฐานนั้นจะไม่มีกฎหมายรองรับไว้ ศาลอาจใช้ดุลพินิจในการรับฟังได้หากจะเป็นประโยชน์ต่อการอำนวยความยุติธรรมมากกว่าผลเสีย อันเกิดจากผลกระทบต่อมาตรฐานของระบบงานยุติธรรมทางอาญา หรือสิทธิเสรีภาพพื้นฐานของประชาชน โดยศาลจะพิจารณาถึงพฤติการณ์ทั้งปวงแห่งคดี โดยต้องคำนึงถึงปัจจัยต่างๆ ตามที่บัญญัติไว้ในมาตรา 226/1 วรรค 2 (1)-(4)

แม้ว่าประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1 จะเปิดโอกาสให้รับฟังพยานหลักฐานดังกล่าวได้ แต่พยานหลักฐานที่ได้มาโดยมิชอบด้วยกฎหมายไม่ว่าโดยประการใดๆ ศาลจะต้องปฏิเสธไม่รับฟัง โดยถือว่าเป็นหลักการตัดพยานหลักฐาน (Exclusionary Rule)[52] ชนิดหนึ่ง ศาลสหรัฐถือตามแนวคิดนี้โดยเคร่งครัด โดยถือว่ารัฐธรรมนูญได้รับรองสิทธิของจำเลยในคดีอาญาไว้ซึ่งเป็นหลักพื้นฐาน ศาลจึงไม่รับฟังพยานหลักฐานที่ได้มาโดยละเมิดสิทธิของจำเลย และถึงว่าความมีวินัยของตำรวจในการหาพยานหลักฐานในคดีเป็นเรื่องสำคัญ การยอมให้ตำรวจปฏิบัติการอันมิชอบ เป็นความชั่วร้ายยิ่งกว่าการปล่อยอาชญากรไปบ้างในบางครั้งเสียอีก การรับฟังพยานหลักฐานที่ไม่ชอบด้วยกฎหมายเหมือนกับการยอมรับเอาผลไม้ของต้นไม้ที่มีพิษ (Fruit of the poisonous tree)[53] ศาลจึงไม่รับฟังพยานหลักฐานที่เป็นผลมาจากการกระทำที่ไม่ชอบด้วยกฎหมาย ผู้เขียนจึงเห็นว่ากระบวนการยุติธรรมทางอาญาควรจะต้องยึดหลักในความถูกต้องของกฎหมายและใสสะอาด การได้มาซึ่งพยานหลักฐานทางคอมพิวเตอร์ จึงจำเป็นต้อง

---

[52] Jerold H.Isreal, Yale kamisar, Wayne R. LaFave. (1994). *Criminal Procedure and the Costitution Leading Supreme Court Cases and Introductory Text 1994 Edition.* pp. 55 - 56

[53] Hill, Rossen and Sog, (1982). *Criminal Procedure Fourth Edition. p. 90, Wayne R. LaFave. (2000). Criminal Procedure Third Edition.* p. 502

มีบทบัญญัติของกฎหมายรองรับในการแสวงหาพยานหลักฐานดังกล่าว โดยใช้มาตรการพิเศษในการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์

หลัก Exclusionary Rule เกิดจากบรรทัดฐานในคดี Weeks v.United States (1914) [54] โดยให้เหตุผลในการสร้างหลักนี้ว่าเพื่อบังคับบัญชาบทบัญญัติว่าด้วยสิทธิเสรีภาพของประชาชนตามรัฐธรรมนูญให้ใช้ได้เป็นผลอย่างจริงจัง ต่อมาศาลสูงสุดได้หาเหตุผลสนับสนุนเพิ่มเติมขึ้นเรื่อยๆ ได้แก่ คดี Olmstead v.United States (1928)[55] โดยให้เหตุผลว่าเป็นหลักประกันสิทธิส่วนบุคคล คดี Irvine v.California (1954)[56] ว่าเป็นการให้หลักประกันแก่จำเลยว่าจะได้รับการพิจารณาคดีอย่างยุติธรรม คำพิพากษาส่วนมากอ้างว่าเป็นการป้องกันเกียรติยศของศาลที่ไม่เกี่ยวข้องกับการกระทำใดๆ อันมิชอบด้วยกฎหมาย ในคดี Mapp v.Ohio (1961) ก็ให้เหตุผลไว้ว่า “ไม่มีสิ่งใดสามารถบ่อนทำลายรัฐได้รวดเร็วยิ่งไปกว่าการที่เจ้าพนักงานของรัฐไม่ปฏิบัติตามกฎหมาย”[57]

แต่ต่อมาหลัก Exclusionary Rule ได้รับการวิพากษ์วิจารณ์และสถิติอาชญากรรมที่สูงขึ้น จึงมีการปรับปรุงเพื่อแก้ไขสถานการณ์นั้น โดยศาลอุทธรณ์ภาค 5 ของสหรัฐเสนอทางออกไว้ในคดี U.S. v. Williams (1980) โดยเพิ่มข้อยกเว้นเรื่องความสุจริต (Good Faith Exception) ว่าศาลไม่นำ Exclusionary Rule มาใช้บังคับกับกรณีเจ้าพนักงานของรัฐได้พยานหลักฐานมาโดยมิชอบ แต่เชื่อโดยสุจริตใจในขณะนั้นว่ามีอำนาจกระทำได้และต่อมาศาลสูงสุดได้รับรองความเห็นของศาลอุทธรณ์ไว้ในคดี U.S. v. Leon (1984) [58]

จึงเห็นว่าประมวลกฎหมายวิธีพิจารณาความอาญาไทยควรเพิ่มมาตรการในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์โดยการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ เพื่อให้การแสวงหาพยานหลักฐานดังกล่าวของเจ้าพนักงานชอบด้วยกฎหมายและทำให้พยานหลักฐานที่มีความสำคัญในการเอาผิดแก่ผู้กระทำผิดเกิดขึ้นโดยชอบและได้มาโดยชอบด้วย อันเป็นการรับรองการแสวงหาพยานหลักฐานของเจ้าพนักงานดังกล่าว

---

[54] Wayne R. LaFave. Op.cit. p. 112.

[55] Olmstead v. United States. 277 U.S. 438. (1928). Retrived October 1. 2008. from *http://www.law.cornell.edu.*

[56] Jerold H.Isreal, Yale kamisar, Wayne R. LaFave. (1980). Basic Criminal Procedure. p. 37.

[57] Wayne R. LaFave. Op.cit. p.113, *Sanford H. Kadish, Monrad G. Paulsen*. (1975). *Criminal Law and Its Processes Cases and Materials THIRD EDITION.* p. 774.

[58] Wayne R. LaFave. Op.cit. p. 63.

2.5 แนวคิดว่าด้วยการตรวจสอบอำนาจรัฐในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์

แนวความคิดในการดำเนินคดีทางอาญาในรูปแบบต่างๆ เพื่อให้เกิดความสมดุลระหว่างผลประโยชน์ของรัฐและประโยชน์ของประชาชนให้มากที่สุด โดยรูปแบบที่เป็นที่ยอมรับกันทั่วไป คือ รูปแบบตามแนวความคิดของ Herbert Packer ในบทความเรื่อง “Two Model of the Criminal Procedure” ซึ่งได้เสนอว่าการดำเนินคดีอาญานั้นสามารถจัดรูปแบบใหญ่ๆ ได้ 2 รูปแบบคือ รูปแบบซึ่งเน้นในเรื่องการควบคุมอาชญากรรมเพื่อรักษาความเรียบร้อยของบ้านเมือง (Criminal Control Model) หรือแนวคิดเรื่องอำนาจรัฐในการรักษาความสงบเรียบร้อยของสังคมและรูปแบบในเรื่องสิทธิและเสรีภาพของประชาชนเพื่ออำนวยความยุติธรรมให้เกิดกับประชาชน (Due Process Model) หรือแนวคิดในการคุ้มครองสิทธิเสรีภาพของประชาชน แนวคิดทั้งสองรูปแบบนี้มีความแตกต่างอยู่ที่การให้ความสำคัญระหว่างผลประโยชน์ของรัฐและประโยชน์ของประชาชนกล่าวคือ รูปแบบแรกจะให้ความสำคัญของประโยชน์ของรัฐมากกว่าของประชาชนแต่รูปแบบหลังจะให้ความสำคัญของประชาชนมากกว่าของรัฐ แต่อย่างไรก็ตามทั้งสองรูปแบบดังกล่าวก็มีวัตถุประสงค์สุดท้ายเดียวกัน ซึ่งก็คือการทำให้กระบวนการทางอาญาสามารถคุ้มครองผู้บริสุทธิ์และลงโทษคนผิด อันส่งผลให้เกิดความสงบเรียบร้อยในสังคม

จากแนวความคิดดังกล่าว จะเห็นได้ว่าสิทธิเสรีภาพของประชาชนได้รับการยอมรับว่ามีความสำคัญในระดับต่างๆ กัน โดยเฉพาะสิทธิเสรีภาพในส่วนที่จะถูกกระทบกระเทือนจากการกระทำของเจ้าหน้าที่ของรัฐที่มีอำนาจตามกฎหมายที่จะปฏิบัติต่อประชาชน ทำให้เกิดวิวัฒนาการทางแนวความคิดที่จะหาวิธีให้สังคมเกิดการยอมรับและเคารพในสิทธิเสรีภาพของบุคคลจนกระทั่งเป็นแรงผลักดันให้เกิดบทบัญญัติที่ใช้เป็นหลักสากล เพื่อให้มนุษยชาติยอมรับเป็นแนวทางปฏิบัติในเวลาต่อมา

แต่อย่างไรก็ตามมิได้หมายความว่าประชาชนที่มีสิทธิโดยธรรมชาติดังกล่าวแล้วจะต้องมีอำนาจใช้สิทธิของตนได้เต็มที่ แต่ทางตรงกันข้ามกลับเป็นที่ยอมรับกันว่าประชาชนที่อยู่ในสังคมที่เจริญแล้วจำเป็นต้องถูกจำกัดสิทธิและเสรีภาพลงในบางส่วน เพื่อการอยู่ร่วมกันด้วยความสงบสุขในสังคม ทั้งนี้เนื่องจากไม่มีระบบการบริหารความยุติธรรมทางอาญาใดที่สามารถนำตัวผู้กระทำความผิดกฎหมายมารับโทษหรือลงโทษได้อย่างมีประสิทธิภาพเต็มที่โดยไม่กระทบกระเทือนถึงสิทธิและเสรีภาพของประชาชน ดังนั้นรัฐจึงสามารถใช้อำนาจในการรักษาความสงบเรียบร้อยโดยกระทำการในลักษณะที่มีผลกระทบต่อสิทธิและเสรีภาพในด้านต่างๆ ของประชาชนได้ เช่น การที่รัฐใช้อำนาจในการจับกุม การค้น และการดักฟังทางโทรศัพท์ เป็นต้น โดยรัฐจะกระทำการดังกล่าวได้ภายในขอบเขตที่กฎหมายให้อำนาจไว้เท่านั้น

อย่างไรก็ดี ประเทศในโลกเสรีส่วนมากจะปกครองประเทศโดยใช้หลักการแบ่งแยกอำนาจ ซึ่งถือเป็นหลักการตรวจสอบและถ่วงดุลที่มีประสิทธิภาพเป็นอย่างยิ่ง โดยอาจแยกพิจารณาการแบ่งแยกอำนาจในแง่ของความแตกต่างตามภาระหน้าที่ของรัฐซึ่งก่อให้เกิดการแบ่งแยกองค์กรตามขอบเขตภาระหน้าที่ที่แตกต่างกันหรือเรียกกันว่า “การแบ่งแยกอำนาจตามภารกิจ” และ “การแบ่งแยกอำนาจในแง่ของตัวบุคคล” ซึ่งเรียกร้องให้ภาระหน้าที่ของรัฐมีการแบ่งแยกนั้นต้องมีเจ้าหน้าที่ของตนเองอันมิใช่เป็นเจ้าหน้าที่ของรัฐองค์กรอื่นด้วย โดยวิธีการแบ่งแยกอำนาจของรัฐเช่นนี้ รวมทั้งการกำหนดให้องค์กรอื่นๆ เข้าไปมีส่วนร่วมในกระบวนการแต่งตั้งบุคคลเข้าสู่อำนาจนั้นหรือการให้มีสิทธิโต้แย้งคัดค้านอำนาจอื่นหรือสิทธิในการควบคุมตรวจสอบทั้งในแง่ของการแบ่งแยกอำนาจตามภารกิจและในแง่ของตัวบุคคล แล้วกรณีก็จะก่อให้เกิดความสัมพันธ์ระหว่างอำนาจต่างๆ ในการยับยั้งซึ่งกันและกัน และทำให้เกิดความสมดุลระหว่างอำนาจไม่ทำให้อำนาจใดอำนาจหนึ่งอยู่ภายใต้อำนาจอื่นโดยสิ้นเชิง ด้วยสภาพการณ์เช่นนี้จะทำให้สิทธิและเสรีภาพของประชาชนได้รับความคุ้มครองอันเป็นความมุ่งหมายประการสำคัญ[59]

ฝ่ายนิติบัญญัติมีอำนาจหน้าที่โดยตรงในการตรากฎหมายที่มีโทษทางอาญาตามบทบัญญัติกฎหมาย ซึ่งมีผลทำให้มีการบังคับใช้กฎหมายโดยฝ่ายบริหารและฝ่ายตุลาการต่อไป[60]

อย่างไรก็ตาม การที่มีกฎหมายตราบังคับใช้ออกมาเป็นจำนวนมากก่อให้เกิดปัญหาการบังคับใช้แก่เจ้าหน้าที่ฝ่ายบริหารในการติดตามศึกษา การทำความเข้าใจศึกษาและการหยิบยกขึ้นบังคับใช้กับข้อเท็จจริงที่เกิดขึ้น เนื่องจากเจ้าหน้าที่ส่วนใหญ่มิใช่นักกฎหมาย แม้จะเป็นเจ้าหน้าที่ผู้ที่อยู่ในกระบวนการยุติธรรมโดยตรงก็ตาม หากเจ้าหน้าที่ไม่สนใจติดตามหยิบยกกฎหมายขึ้นบังคับใช้ซึ่งส่วนใหญ่ไม่ทราบว่ามีกฎหมายบังคับอยู่ โดยเฉพาะอย่างยิ่งเจ้าหน้าที่ที่มีหน้าที่บังคับการตามกฎหมายทุกฉบับที่มีโทษทางอาญา ย่อมทำให้การบังคับใช้กฎหมายเป็นไปโดยไม่ถูกต้องตามเจตนารมณ์และเป็นไปตามอำเภอใจของเจ้าหน้าที่ ฝ่ายนิติบัญญัติโดยเฉพาะอย่างยิ่งสภาผู้แทนราษฎรจึงมีอำนาจหน้าที่ในการติดตามสอดส่องการบังคับใช้กฎหมายของฝ่ายบริหารและฝ่ายตุลาการต้องมีหน้าที่ในการตรวจสอบและถ่วงดุลการปฏิบัติหน้าที่ของเจ้าหน้าที่ฝ่ายบริหารในกรณีที่กฎหมายให้อำนาจในการออกหมายอาญาและพิจารณาคดีต่างๆ ที่เจ้าหน้าที่ดำเนินการมา การติดตามสอดส่องการบังคับใช้กฎหมายของฝ่ายบริหารและการตรวจสอบถ่วงดุลโดยฝ่ายตุลาการ จึงนับเป็นการควบคุม ตรวจสอบและถ่วงดุลฝ่ายบริหารวิธีการหนึ่งที่มีประสิทธิภาพอย่างยิ่ง

---

[59] บรรเจิด สิงคะเนติ. (2552). *หลักพื้นฐานเกี่ยวกับสิทธิเสรีภาพ และ ศักดิ์ศรีความเป็นมนุษย์*. หน้า 22.

[60] กุลพล พลวัน ก (2538). *พัฒนาการแห่งสิทธิมนุษยชน*. หน้า 133.

ดังนั้น การบังคับใช้กฎหมายโดยฝ่ายบริหารที่อยู่ในกระบวนการยุติธรรมซึ่งเป็นเจ้าหน้าที่ผู้บังคับใช้กฎหมาย (Law Enforcement Officials) จะต้องสอดคล้องกับหลักการคุ้มครองสิทธิเสรีภาพของประชาชนที่รัฐธรรมนูญบัญญัติรับรองไว้ โดยเจ้าหน้าที่ต้องมีความเคารพในหลักการดังกล่าวอย่างเคร่งครัดด้วยเสมอ

วิธีการประการหนึ่งที่จะทำให้หลักนิติรัฐหรือรัฐที่ปกครองโดยยึดหลักกฎหมายซึ่งเป็นระบบที่สร้างขึ้นเพื่อประโยชน์ของประชาชนและเพื่อป้องกัน หรือแก้ไขการใช้อำนาจตามอำเภอใจของเจ้าหน้าที่ของรัฐอย่างมีประสิทธิภาพ ก็คือการให้ขั้นตอนดำเนินการในกระบวนการยุติธรรมทางอาญาทุกขั้นตอนโปร่งใส (Transparency) ทั้งนี้เพื่อนำไปสู่การตรวจสอบการใช้อำนาจของเจ้าหน้าที่ของรัฐด้วย (Accountability) [61]

การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ของบุคคลต้องเป็นมาตรการแก่การรักษาความมั่นคงของรัฐ การรักษาความปลอดภัยในชีวิต ร่างกายและทรัพย์สินของประชาชน การรักษาความมั่นคงทางเศรษฐกิจของประเทศ การรักษาความสงบเรียบร้อยของประชาชนและการป้องกันและปราบปรามการกระทำผิดอาญา การคุ้มครองสุขภาพอนามัยหรือศีลธรรมอันดีของประชาชน หรือการคุ้มครองสิทธิและเสรีภาพของผู้อื่น กล่าวอีกนัยหนึ่งเป็นมาตรการสุดท้าย เมื่อไม่อาจแสวงหาข้อมูลข่าวสารเพื่อคุ้มครองคุณค่าดังกล่าวได้โดยวิธีการอื่นๆ แล้ว เพื่อให้เป็นไปตามนี้การดักฟังและบันทึกการสนทนาทางโทรศัพท์ของบุคคลจะกระทำได้ก็เฉพาะแต่ในกรณีที่ได้มีหรือจะมีการกระทำผิดอาญาที่ร้ายแรงเท่านั้น ยิ่งกว่านั้นยังต้องมีระบบการควบคุมการใช้อำนาจตามอำเภอใจของเจ้าหน้าที่รัฐอย่างรัดกุม ในกระบวนการดักฟังและบันทึกการสนทนาทางโทรศัพท์ทุกขั้นตอน เริ่มตั้งแต่เจ้าหน้าที่รัฐที่ประสงค์ใช้การดักฟังและบันทึกการสนทนาทางโทรศัพท์ของบุคคลจะต้องได้รับอนุญาตจากองค์กรที่มีความเป็นอิสระและเป็นกลาง เช่น ศาล หรือองค์กรที่มีหลักประกันความเป็นอิสระทำนองเดียวกับศาล ทั้งนี้ ต้องมีการกำหนดระยะเวลาขั้นสูงที่จะกระทำการเช่นว่านั้น รวมไปถึงหลักประกันว่าจะไม่มีการตัดต่อการบันทึกเสียงการสนทนา หรือการถ่ายเสียงการสนทนา เป็นลายลักษณ์อักษร ตลอดจนหลักประกันว่าจะมีการทำลายสิ่งบันทึกเสียงการสนทนาเมื่อหมดความจำเป็นต้องใช้แล้ว[62]

ดังนั้น การบัญญัติกฎหมายให้อำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ จึงต้องมีการบัญญัติองค์กรที่ทำหน้าที่ตรวจสอบและถ่วงดุลซึ่งต้องเป็นองค์กรที่มีอำนาจในการอนุญาตให้เจ้าหน้าที่ใช้อำนาจดังกล่าวได้ โดยองค์กรที่ได้รับการยอมรับว่ามีความ

---

[61] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. (2556). *ประมวลกฎหมายวิธีพิจารณาความอาญา ฉบับอ้างอิง*. หน้า 543.

[62] กมลชัย รัตนสกาวงศ์ และ วรพจน์ วิศรุตพิชญ์. เล่มเดิม. หน้า 86.

บริสุทธิ์ ยุติธรรม โปร่งใส ในการใช้ดุลพินิจพิจารณาให้อำนาจเจ้าหน้าที่ในการกระทำที่ต้องละเมิดสิทธิเสรีภาพของประชาชนก็คือ ศาล

แนวคิดที่ให้องค์กรภายนอกที่มิได้มีส่วนได้เสียกับเจ้าหน้าที่ผู้บังคับใช้กฎหมายทำการกลั่นกรองคำร้องขอและอนุมัติให้มีการดักฟังได้ ก็เพื่อให้การกระทำดังกล่าวของเจ้าหน้าที่ต้องใช้ความรอบคอบและละเมิดต่อสิทธิและเสรีภาพของประชาชนให้น้อยที่สุด ท้ายสุดก็คือข้อมูลที่ได้มาจากการดักฟังสามารถใช้เป็นพยานหลักฐานลงโทษผู้กระทำความผิดได้อย่างชัดเจนและโปร่งใส เนื่องจากกระบานการดักฟังดังกล่าวมีองค์กรศาลคอยควบคุมกับดูแลอย่างเคร่งครัด

2.5.1 การตรวจสอบและถ่วงดุลภายในหน่วยงานที่บังคับใช้กฎหมาย

มาตรการควบคุมภายใน (Internal Control) เป็นการควบคุมภายในองค์กรบังคับใช้กฎหมายเอง ทั้งนี้ตามสายงานการบังคับบัญชาตามลำดับชั้นการควบคุมโดยอาศัยการบังคับบัญชา (Controle Hierarchique)

การควบคุมบังคับบัญชา[63] คือ มาตรการหนึ่งของการรวมอำนาจบริหาร (Centralization) ซึ่งเป็นการกำหนดความสัมพันธ์ระหว่างเจ้าหน้าที่ขององค์กรฝ่ายปกครองส่วนกลางด้วยกันเองในรูปของสายการบังคับบัญชา (Hierarchie) กล่าวคือ เป็นกรณีที่ผู้บังคับบัญชาใช้อำนาจทั่วไปซึ่งตนมีอยู่เหนือผู้ใต้บังคับบัญชาของตน ทำการตรวจสอบความชอบด้วยกฎหมายและความเหมาะสมของการกระทำต่างๆ ของผู้ใต้บังคับบัญชาหากเห็นว่าการกระทำใดของผู้ใต้บังคับบัญชาไม่ชอบด้วยกฎหมายหรือชอบด้วยกฎหมายแต่ไม่เหมาะสมผู้บังคับบัญชาย่อมมีอำนาจที่จะสั่งการให้ผู้ใต้บังคับบัญชากระทำการต่างๆ ไปในทิศทางเดียวกันนอกจากนี้ผู้บังคับบัญชายังมีอำนาจการเพิกถอน รวมทั้งมีอำนาจที่จะแก้ไขเปลี่ยนแปลง และอำนาจที่จะสอดเข้าไปใช้อำนาจแทนผู้ใต้บังคับบัญชาได้อีกด้วย

นอกจากนี้ ผู้บังคับบัญชายังมีอำนาจควบคุมบังคับบัญชาตัวผู้ใต้บังคับบัญชาอีกด้วย หมายความว่า การที่ผู้บังคับบัญชาใช้อำนาจบังคับบัญชาของตนเพื่อกระทำการต่างๆ เกี่ยวกับสถานภาพขอผู้ใต้บังคับบัญชา ซึ่งอำนาจการควบคุมของผู้บังคับบัญชาในกรณีดังกล่าวนี้มี 3 ประการด้วยกัน คือ อำนาจที่จะลงโทษทางวินัย อำนาจที่จะโยกย้ายหรือแต่งตั้งให้ดำรงตำแหน่งสูงขึ้น และอำนาจที่จะเลื่อนขั้นเงินเดือน เป็นต้น

การบังคับบัญชาภายในองค์กรของรัฐนั้น ถือเป็นหลักสำคัญในการปฏิบัติงาน ทั้งยังเป็นการตรวจสอบการทำงานของผู้ปฏิบัติ แต่การที่จะมีการตรวจสอบและถ่วงดุลไปพร้อมกันนั้น ผู้ที่ใช้อำนาจและผู้ตรวจสอบควรเป็นผู้ที่มีอำนาจระดับเดียวกันเป็นอย่างน้อยและต้องมีการตรวจสอบขั้นตอนการใช้อำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทาง

---

[63] ไพรัช โตสวัสดิ์. เล่มเดิม. หน้า 14.

อิเล็กทรอนิกส์ตั้งแต่การเริ่มทำคำร้องขอ ซึ่งได้แก่ การตรวจสอบรายงานการสืบสวนไปจนถึงปัญหาที่ผู้ทำคำร้องประสบมาซึ่งเป็นเหตุให้มีการขอใช้อำนาจดังกล่าว ดังนั้นหน่วยหรือส่วนที่มีหน้าที่ในการตรวจสอบและถ่วงดุลจึงต้องมีอำนาจเทียบเท่าหรือมากกว่าหน่วยหรือส่วนที่ใช้อำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์

2.5.2 การตรวจสอบและถ่วงดุลภายนอกหน่วยงานที่บังคับใช้กฎหมาย

มาตรการควบคุมภายนอก (External Control)[64] หน่วยงานที่บังคับใช้กฎหมายเป็นการควบคุมโดยองค์กรอื่นๆ ในกระบวนการยุติธรรม คือ องค์กรตุลาการหรือศาล องค์กรอัยการและทนายความ ในทุกขั้นตอนของการดำ เนินคดี อาทิ การจับ การค้น การควบคุมตัว การสอบสวน ตลอดจนถึงการใช้มาตรการเข้าถึงข้อมูลด้วยการใช้วิธีการดักฟังทางโทรศัพท์ ทั้งนี้เพื่อให้การใช้ดุลพินิจของเจ้าหน้าที่ในการดำเนินคดีอาญาเป็นไปอย่างถูกต้อง โปร่งใสและเป็นธรรมมากที่สุด เพื่อเป็นการรับรองเสรีภาพของบุคคลในการสื่อสารถึงกันโดยมิอาจถูกล่วงละเมิดได้กฎหมายเกี่ยวกับการดักฟังจะต้องบัญญัติให้ชัดเจนว่า โดยหลักแล้วการดักฟังการติดต่อสื่อสารทางโทรคมนาคมมิอาจกระทำได้ เว้นแต่เพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเพื่อรักษาความมั่นคงของรัฐ ทั้งนี้การดักฟังการสื่อสารโทรคมนาคมจะต้องปฏิบัติตามหลักเกณฑ์และเงื่อนไขที่กฎหมายกำหนดไว้

กฎหมายเกี่ยวกับการดักฟังการติดต่อสื่อสารทางโทรคมนาคมจะต้องประสานระหว่างการคุ้มครองสิทธิส่วนบุคคล (Privacy of Individuals)[65] จากการถูกลอบฟังการติดต่อสื่อสารและการให้อำนาจเจ้าหน้าที่ของรัฐในการดักฟังการติดต่อสื่อสารเพื่อให้ได้ข้อมูลที่จำเป็นในการป้องกันมิให้มีการก่ออาชญากรรมและสืบสวนคดีที่มีการกระทำความผิด

ฉะนั้นในการบัญญัติกฎหมายที่ให้อำนาจเจ้าหน้าที่ของรัฐดักฟังทางโทรศัพท์ได้จะต้องกำหนดเงื่อนไขที่จะทำการดักฟังทางโทรศัพท์ไว้เพื่อมิให้เจ้าหน้าที่ของรัฐใช้ดักฟังทางโทรศัพท์ก้าวล่วงกระทบกระเทือนเสรีภาพในการสื่อสารถึงกันของบุคคลโดยไม่มีเหตุอันสมควรระบบการควบคุมการใช้อำนาจตามอำเภอใจของเจ้าหน้าที่รัฐอย่างรัดกุมในกระบวนการดักฟังและบันทึกการสนทนาทางโทรศัพท์ทุกขั้นตอน เริ่มตั้งแต่เจ้าหน้าที่รัฐที่ประสงค์ดักฟังและบันทึกการสนทนาทางโทรศัพท์ของบุคคลจะต้องได้รับอนุญาตจากองค์กรที่มีความเป็นอิสระและเป็นกลาง เช่น ศาล หรือองค์กรที่มีหลักประกันความเป็นอิสระทำนองเดียวกับศาล

---

[64] กุลพล พลวัน ข (2544). *การบริหารกระบวนการยุติธรรม*. หน้า 64.

[65] กมลชัย รัตนสกาวงศ์ และ วรพจน์ วิศรุตพิชญ์. เล่มเดิม. หน้า 111.

2.5.2.1 ศาล

นอกเหนือจากการที่ให้อำนาจศาลในการอนุมัติให้อำนาจแก่เจ้าหน้าที่ในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์แล้วนั้น หากเจ้าหน้าที่ฝ่าฝืนไม่ยอมขออำนาจศาลในการกระทำดังกล่าว พยานหลักฐานที่ได้มาย่อมมิชอบด้วยกฎหมายและศาลย่อมจะไม่รับฟังเป็นพยานหลักฐานลงโทษผู้กระทำความผิด

หลักการรับฟังพยานหลักฐานของศาลนั้น ตามหลักสากลหรือที่เรียกกันว่า Fruit of the Poisonous Tree ในกฎหมายของประเทศสหรัฐอเมริกา ในกรณีที่ความปรากฏแก่ศาลว่าพยานหลักฐานใดเป็นพยานหลักฐานที่เกิดขึ้นโดยชอบแต่ได้มาเนื่องจากการกระทำโดยมิชอบหรือเป็นพยานหลักฐานที่ได้มาโดยอาศัยข้อมูลที่เกิดขึ้นหรือได้มาโดยมิชอบ ห้ามมิให้ศาลรับฟังพยานหลักฐานนั้น

ดังนั้น หากข้อมูลการสื่อสารทางอิเล็กทรอนิกส์ที่ได้มาจากการดักฟังทางโทรศัพท์หรือการเข้าถึงข้อมูลทางคอมพิวเตอร์ โดยไม่ได้รับอนุญาตจากศาลก่อนนั้น ถือเป็นพยานหลักฐานที่ได้มาโดยมิชอบแล้ว ซึ่งอาจส่งผลให้พยานหลักฐานที่ได้มารับฟังไม่ได้ ศาลจะไม่รับฟังทุกกรณี

จะเห็นได้ว่าศาลจะถือหลักการไม่ยอมรับฟังพยานหลักฐานที่ได้มาโดยมิชอบ[66] เพื่อเป็นการลงโทษเจ้าหน้าที่ของรัฐโดยทางอ้อมอีกทางหนึ่ง ให้เจ้าหน้าที่ได้ทราบว่าหากยังคงฝ่าฝืนกฎหมายการดักฟังทางโทรศัพท์หรือการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์นั้น การดักฟังดังกล่าวก็จะไร้ผลเพราะข้อมูลข่าวสารที่ได้มารับฟังไม่ได้ ประกอบกับมีวัตถุประสงค์ให้เจ้าหน้าที่ของรัฐเคารพและปฏิบัติตามกฎหมาย และเป็นการคุ้มครองประชาชนจะมิได้ถูกล่วงละเมิดสิทธิโดยปราศจากเหตุอันควร

ทั้งนี้ ถ้าศาลรับฟังและใช้พยานหลักฐานดังกล่าวลงโทษจำเลย ก็เท่ากับศาลไร้ความบริสุทธิ์และกลายเป็นหุ้นส่วนในการล่วงละเมิดกฎหมายของเจ้าหน้าที่ด้วยเช่นกัน หรือเป็นกรณีที่ผู้พิพากษาซึ่งถือเป็นนักกฎหมาย หากสนับสนุนการใช้กำลังการใช้วิธีนอกกฎหมายย่อมได้ชื่อว่าทรยศต่อวิชาชีพของตน[67] ย่อมเป็นสิ่งที่ไม่ควรเกิดขึ้นในประเทศที่ปกครองโดยใช้หลักการนิติรัฐ

---

[66] เกียรติขจร วัจนะสวัสดิ์. (2551). *คำอธิบาย หลักกฎหมายวิธีพิจารณาความอาญา ว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณา พร้อมด้วย คำอธิบายมาตราที่แก้ไขเพิ่มเติมใหม่ตาม พ.ร.บ. แก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความอาญา ฉบับที่ 25, 26, 27, 28, 29 (เฉพาะขั้นตอนก่อนการพิจารณา).* หน้า 396.

[67] จิตติ ติงศภัทิย์. เล่มเดิม. หน้า 53.

2.5.2.2 อัยการ

องค์กรอัยการเป็นองค์กรที่ทำหน้าที่ในการรวบรวมข้อมูลที่ได้มาจากเจ้าหน้าที่สืบสวนสอบสวน เพื่อประมวลเป็นสำนวนส่งฟ้องผู้กระทำความผิดต่อศาล ดังนั้น อัยการจึงต้องมีบทบาทและอำนาจในการตรวจสอบและถ่วงดุลการกระทำต่างๆ ของเจ้าหน้าที่ในการสืบสวนสอบสวน เพื่อที่ข้อมูลที่ได้มาจะสามารถนำเสนอเป็นพยานหลักฐานในชั้นศาลได้อย่างบริสุทธิ์ชัดเจนอันจะยังประโยชน์ให้แก่กระบวนการยุติธรรมในการนำผู้กระทำความผิดมาลงโทษได้อย่างถูกต้อง ดังนั้นในกรณีการอนุมัติให้มีการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ล่วงหน้าหรือในกรณีฉุกเฉินของบางประเทศ กฎหมายจะให้เป็นอำนาจของอัยการในการอนุมัติให้เจ้าหน้าที่สืบสวนทำการดักฟังไปก่อน แต่ต่อมาต้องรายงานการปฏิบัติต่อศาล ตามขั้นตอนการทำคำร้องขอในกรณีปกติภายใน 48 ชั่วโมง

ดังนั้น อัยการที่จะอนุมัติให้เจ้าหน้าที่ใช้อำนาจดังกล่าวได้ จะต้องมีการตรวจสอบและกลั่นกรองข้อมูลที่ได้มาจากการสืบสวนและปัญหาที่ประสบจนไม่สามารถได้ข้อมูลมาด้วยทางอื่นหรืออาจจะเป็นอันตรายเกินควร จึงถือว่า อัยการเป็นอีกองค์กรที่คอยถ่วงดุลการใช้อำนาจดังกล่าวของเจ้าหน้าที่ให้เป็นไปโดยชอบด้วยกฎหมาย

2.5.2.3 ประชาชน

ในประเทศเยอรมนีการใช้มาตรการการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ในกรณีเพื่อความมั่นคงของรัฐ รัฐจะต้องแจ้งให้กับผู้ถูกกระทบสิทธิโดยตรงจากการถูกใช้มาตรการดังกล่าวนี้ทราบเมื่อสภาพความเป็นอันตรายซึ่งเป็นวัตถุประสงค์ในการจำกัดสิทธิเสรีภาพนั้นหมดสิ้นลง ถ้ายังไม่อาจวินิจฉัยได้ว่าเหตุความเป็นอันตรายนั้นยังมีอยู่หรือไม่ก็ให้แจ้งทันทีที่วินิจฉัยได้ว่าเหตุแห่งความเป็นอันตรายนั้นหมดสิ้นลงแล้ว แต่ไม่จำเป็นต้องแจ้งถ้าไม่ปรากฏเหตุดังกล่าว เมื่อผู้ถูกกระทบสิทธิได้รับการแจ้งถึงการใช้มาตรการดังกล่าวสามารถมีสิทธิฟ้องร้องได้

จะเห็นได้ว่าแนวคิดการตรวจสอบและถ่วงดุลการใช้อำนาจรัฐต่างๆ โดยประชาชนยังเป็นแนวคิดที่ได้รับการยอมรับมานานในโลกยุคเสรีนี้ เนื่องจากประชาชนแต่ละคนมีสิทธิส่วนบุคคลและเสรีภาพในการสื่อสาร ดังนั้น หากเจ้าหน้าที่ได้กระทำการดักฟังจนเป็นการละเมิดสิทธิโดยมิชอบด้วยกฎหมายหรือไม่มีเหตุอันควร ประชาชนย่อมมีอำนาจที่จะทวงคืนซึ่งสิทธิเสรีภาพของตนที่ถูกกระทบกระเทือน และการทวงคืนนั้น รัฐธรรมนูญและกฎหมายของรัฐต่างๆ ก็เปิดช่องให้ประชาชนได้ดำเนินคดีกับเจ้าหน้าที่ผู้กระทำละเมิดได้อย่างชัดเจนและเป็นการทั่วไปอีกด้วย

ปัจจุบันประชาชนสามารถร้องทุกข์กล่าวหาเกี่ยวกับการปฏิบัติหน้าที่โดยมิชอบของเจ้าหน้าที่รัฐได้ โดยร้องทุกข์ไปยังผู้บังคับบัญชาของเจ้าหน้าที่ ผู้บังคับบัญชาระดับสูงขึ้นไป หรือหน่วยงานในระดับสูงขึ้นไปหรือองค์กรที่เจ้าหน้าที่สังกัดอยู่การร้องทุกข์นี้นับว่าเป็นการใช้สิทธิที่สำคัญประการหนึ่งของประชาชน รัฐธรรมนูญหลายประเทศได้บัญญัติรับรองสิทธินี้ไว้ในฐานะที่เป็นสิทธิมูลฐานของพลเมืองการร้องทุกข์มีผลดีหลายประการ ตัวอย่างเช่น

ประการแรก ทำให้ประชาชนผู้อยู่ใต้การปกครองและได้รับความเดือดร้อนหรือการปฏิบัติอย่างไม่เป็นธรรมจากการกระทำของเจ้าหน้าที่รัฐมีโอกาสแจ้งหรือรายงานความเดือดร้อนต่างๆ ให้ฝ่ายบริหารทราบ เพื่อหาทางแก้ไขเยียวยาความเดือนร้อนนั้นได้ทันท่วงที เพราะหากให้ประชาชนให้สิทธิฟ้องร้องต่อศาล ก็อาจใช้เวลานานพอสมควรกว่าจะมีคำพิพากษาอย่างใดอย่างหนึ่งซึ่งอาจจะไม่ทันต่อเหตุการณ์นอกจากนั้นประชาชนจะต้องเสียค่าใช้จ่ายจำนวนมากเพื่อการดำเนินคดีในศาล

ประการที่สอง ทำให้ผู้บังคับบัญชาหรือฝ่ายบริหารได้รับทราบถึงเดือดร้อนของประชาชนเนื่องจากผู้บังคับบัญชาระดับสูงไม่ค่อยมีโอกาสได้ทราบถึงข้อเท็จจริงต่างๆ ที่เกิดขึ้นหากเจ้าหน้าที่ชั้นต้นไม่รายงานขึ้นมา หรือปกปิดข้อเท็จจริง เพื่อที่ผู้บังคับบัญชาหรือฝ่ายบริหารจะได้หาวิธีแก้ไขหรือกำหนดมาตรการเพื่อดำเนินการอย่างเหมาะสมต่อไป[68] อย่างไรก็ดีการตรวจสอบการใช้อำนาจของเจ้าหน้าที่รัฐหรือหน่วยงานบังคับใช้กฎหมาย ประชาชนก็สามารถตรวจสอบการทำงานโดยการกล่าวโทษได้ ในกรณีที่มีการกระทำความผิดต่อตำแหน่งหน้าที่ในการยุติธรรม[69] ตามบทบัญญัติของประมวลกฎหมายอาญาได้อีกทางหนึ่ง

[68] กุลพล พลวัน ข เล่มเดิม. หน้า 187.

[69] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. เล่มเดิม. หน้า 563.

บทที่ 3
กฎหมายที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาของประเทศสหรัฐอเมริกา

การแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาในประเทศสหรัฐอเมริกานั้น ได้มีวิธีการในการเข้าถึงพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาซึ่งเป็นข้อมูลอิเล็กทรอนิกส์ส่วนบุคคล โดยการเข้าถึงพยานหลักฐานดังกล่าวย่อมไปกระทบกระทั่งถึงสิทธิส่วนบุคคลของเจ้าของข้อมูลดังกล่าว แต่อย่างไรก็ดีกฎหมายของสหรัฐอเมริกาก็ได้มีวิธีการในการเข้าถึงพยานหลักฐานดังกล่าวโดยวิธีการที่จะก่อให้เกิดความเสียหายน้อยที่สุด ทั้งนี้เพื่อประโยชน์ของสาธารณชนที่มากกว่าประโยชน์ส่วนบุคคลและไม่เป็นการกระทบกระทั่งถึงประโยชน์ส่วนบุคคลจนมากเกินไป ซึ่งกฎหมายที่เกี่ยวกับการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาของประเทศสหรัฐอเมริกามีดังนี้

3.1 การจับตาโครงข่ายการสื่อสารโดยทางอิเล็กทรอนิกส์

การสอบสวนคดีอาญามักจะเกี่ยวข้องกับการจับตาทางอิเล็กทรอนิกส์ (Electronic Surveillance) ในคดีอาชญากรรมทางคอมพิวเตอร์ เจ้าหน้าที่จะต้องการจับตาดูพฤติกรรมของผู้กระทำผิดที่ใช้คอมพิวเตอร์ในการอำนวยความสะดวกในการกระทำผิดไม่ว่าจะเป็นการรับส่งข้อมูลที่เป็นจดหมายอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการกระทำผิด โดยมีรัฐบัญญัติอยู่ 2 ฉบับที่เกี่ยวข้องกับการจับตาทางอิเล็กทรอนิกส์ในเวลาจริง (Real Time) ในการสอบสวนการกระทำผิดอาญาของสหรัฐ รัฐบัญญัติฉบับแรกซึ่งเป็นฉบับสำคัญที่สุดคือ The Wiretap statute (title 3), amended 1986 ซึ่งอยู่ใน Title 3 ของ Omnibus Crime Control and Safe Streets Act 1968 และรัฐบัญญัติฉบับที่สองได้แก่ The Pen/Trap Statute, amended 2001 ซึ่งกล่าวถึง Pen Register และอุปกรณ์ที่เกี่ยวกับการดักและติดตาม (Trap and Trace Devices) การฝ่าฝืนไม่ปฏิบัติตามรัฐบัญญัติดังกล่าวนี้ จะทำให้ต้องรับผิดทั้งทางแพ่งและทางอาญา และในกรณีการละเมิด Title 3 อาจทำให้ไม่อาจรับฟังพยานหลักฐานที่ได้มานั้น

3.1.1 รัฐบัญญัติ The Wiretap statute (title 3), amended 1986

รัฐบัญญัตินี้จะเกี่ยวข้องกับการดักฟังโดยตรงหรือการดักฟังการสื่อสารทางอิเล็กทรอนิกส์ในเวลานั้นโดยหน่วยงานของรัฐบาล พระราชบัญญัตินี้รู้จักกันในนามของ Title 3 เพราะในครั้งแรกออกมาเป็น Title 3 ของรัฐบัญญัติ The Omnibus Crime Control and Safe Streets ปี 1986[70] ผู้ที่สืบสวนที่จะเข้าสู่คอมพิวเตอร์ที่เป็นเป้าหมายในขณะที่ข้อมูลข่าวสารกำลังส่งจะต้องใช้กฎหมาย the Wiretap statute ซึ่งส่วนมากจะมีใช้กับการสนทนาทางโทรศัพท์[71]

โดยหลักการของ Title 3 จะเรียบง่าย โดยรัฐบัญญัติจะถือเอาว่า การสื่อสารของราษฎรทุกการสื่อสารถือว่าเป็นการติดต่อระหว่างผู้ที่เกี่ยวข้องสองฝ่าย เช่น การโทรศัพท์ติดต่อระหว่าง เอ กับ บี ในขั้นต้นรัฐบัญญัติได้ห้ามไม่ให้บุคคลภายนอก (เช่น รัฐ) ซึ่งไม่ใช่ผู้เกี่ยวข้องเป็นผู้ทำการสื่อสารทำการดักการสื่อสารของบุคคลดังกล่าวโดยใช้ “อิเล็กทรอนิกส์ เครื่องมือหรืออุปกรณ์อย่างอื่น” หากรัฐบัญญัติไม่ได้วางข้อยกเว้นไว้ ซึ่งรัฐบัญญัตินี้จะห้ามการลอบฟังอย่างครอบคลุมในทุกที่ไม่ว่าจะทำโดยบุคคลใดในสหรัฐ ไม่ว่าพนักงานสอบสวนต้องการดำเนินการจับตาที่บ้าน ที่ทำงาน หรือที่ทำการของราชการ ในคุก หรือทางอินเทอร์เน็ต พนักงานสอบสวนนั้นจะต้องมั่นใจว่าการจับตาดังกล่าวเป็นไปตามบทบัญญัติของ Title 3[72] ซึ่งคำนิยามสำคัญที่ปรากฏอยู่ใน Title 3 ก็จะมีดังนี้

การสื่อสารตามสาย (Wire Communication)

โดยทั่วไปแล้วการสื่อสารทางโทรศัพท์เป็นการสื่อสารตามสาย ซึ่งตามมาตรา 2510 (1) “การสื่อสารตามสาย” นั้นหมายถึง “การสื่อสารด้วยวาจาทั้งหมดหรือบางส่วนที่ส่งโดยใช้เครื่องมือที่ช่วยในการส่งการสื่อสาร เช่น ใช้สายโทรศัพท์ เคเบิล หรือสิ่งอื่นๆ ที่ใช้ติดต่อระหว่างผู้ส่งและผู้รับ (เช่น การใช้การติดต่อดังกล่าวในสถานีเปลี่ยนสลับสายหรือ Switching Station) ที่ติดตั้งหรือดำเนินการโดยบุคคลใดๆ ที่เกี่ยวข้องกับการให้บริการหรือบริการเครื่องมือดังกล่าว เพื่อส่งการสื่อสารระหว่างมลรัฐหรือระหว่างประเทศ หรือการสื่อสารที่กระทบต่อการค้าระหว่างมลรัฐหรือระหว่างประเทศ”[73] จึงเห็นว่าตามคำนิยามดังกล่าวนี้ มีหลักเกณฑ์ที่สำคัญคือ เนื้อหาของการสื่อสารจะต้องมีเสียงมนุษย์ หากการสื่อสารไม่มีเสียงมนุษย์ไม่ว่าเป็นเสียงของคนๆ เดียวหรือหลายคนก็จะ

---

[70] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2510-2522)

[71] ไพจิตร สวัสดิสาร. (2549, มกกราคม-เมษายน). “การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์หรือนิติคอมพิวเตอร์ (Computer forensic).” *ดุลพาห, 53 (1).* หน้า 71.

[72] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 135.

[73] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2510 (1)).

ไม่ใช่การสื่อสารตามสาย ซึ่งในคดี S. Rep. No.99-541, at 12 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, United States v. Torres, 751 F.2d 875, 885-86 (7th Cir. 1984) วินิจฉัยว่า การจับตาทางโทรทัศน์ โดยไม่มีเสียงประกอบไม่ใช่เรื่องการดักการสื่อสารตามสายตาม Title 3 เพราะไม่ได้มาซึ่งวาจา

นอกจากนี้หลักเกณฑ์ที่ว่าจะต้องมีการส่งการสื่อสารตามสาย "ทั้งหมดหรือบางส่วนโดยใช้สายโทรศัพท์ เคเบิล หรือสิ่งอื่นที่ใช้ติดต่อ" จะไม่ค่อยมีปัญหาตราบเท่าที่สัญญาณเดินทางผ่านสายบางจุดระหว่างจุดที่ส่งและจุดที่รับการสื่อสาร ก็จะถือว่าเข้าตามหลักเกณฑ์นี้ ตัวอย่างเช่นการส่งเสียงทางโทรศัพท์ทุกประเภท รวมถึงสัญญาณดาวเทียมและโทรศัพท์เคลื่อนที่ (Cellular Phone) ถือเป็นการสื่อสารตามสาย เนื่องจากการส่งดังกล่าวทำโดยทางสายในสถานีเปลี่ยนสลับสายหรือ Switched Stations การส่งดังกล่าวจึงอยู่ในนิยามของการสื่อสารตามสาย มีข้อน่าสังเกตว่า การมีสายอยู่ในอุปกรณ์ที่จุดส่งและรับการสื่อสาร (เช่นโทรศัพท์เคลื่อนที่ส่วนบุคคล) ไม่ถือเป็นเรื่องการสื่อสารที่มีการส่งตามสาย เพราะสายจะต้อง "เป็นสิ่งสำคัญ" ในการส่งการสื่อสารดังกล่าวโดยอยู่นอกอุปกรณ์ที่ใช้ส่งและรับการสื่อสาร แต่อย่างไรก็ตามการสื่อสารตามสายที่ได้เก็บไว้เช่นไปรษณีย์เสียงไม่อยู่ภายใต้รัฐบัญญัตินี้แต่อยู่ใต้รัฐบัญญัติ ECPA ซึ่งจะกล่าวต่อไป[74]

การสื่อสารทางอิเล็กทรอนิกส์

โดยทั่วไปแล้วการสื่อสารทางอินเทอร์เน็ตส่วนใหญ่ เช่น จดหมายอิเล็กทรอนิกส์เป็นการสื่อสารทางอิเล็กทรอนิกส์ ซึ่งตามมาตรา 2510 (12) ได้ให้คำนิยามของคำว่า "การสื่อสารทางอิเล็กทรอนิกส์" ว่าหมายความถึง การส่งเครื่องหมาย สัญญาณ ข้อเขียน ภาพ เสียง ข้อมูล หรือสิ่งที่ใช้แทนธรรมชาติ (Intelligence of Any Nature) โดยส่งทั้งหมดหรือบางส่วนทางสาย วิทยุคลื่นแม่เหล็ก ภาพไฟฟ้า หรือระบบภาพแสง ซึ่งมีผลในการค้าระหว่างมลรัฐหรือระหว่างประเทศแต่ไม่รวมถึง

(1) การสื่อสารใดๆ ตามสายหรือวาจา

(2) การสื่อสารใดๆ ที่กระทำผ่านเครื่องรับส่งข้อความติดตามตัวด้วยเสียง (Tone-only Paging Device)

(3) การสื่อสารใดๆ ที่ได้จากอุปกรณ์ Tracking หรือ

---

[74] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 136.

(4) สารสนเทศการโอนเงินทางอิเล็กทรอนิกส์ ที่สถาบันการเงินเก็บไว้ในระบบการสื่อสารที่ใช้สำหรับเก็บข้อมูลอิเล็กทรอนิกส์และการโอนเงิน[75]

ผู้เขียนเห็นว่าการสื่อสารทางอิเล็กทรอนิกส์เป็นการสื่อสารที่เป็นการรับส่งสัญญาณตามสายที่ส่งเป็น ข้อเขียน ภาพ เสียง ข้อมูล เท่านั้น ไม่รวมถึงการสื่อสารโดยวาจา ที่รับและส่งถึงกันเหมือนการใช้โทรศัพท์ถึงกันผู้เขียนจึงเห็นด้วยกับนิยามดังกล่าว

การดัก (Intercept)

บทบัญญัติของ ECPA และ Title 3 กำหนดคำว่า “ดัก” ใช้ได้เฉพาะกับการสื่อสารที่ได้มาในขณะส่งและไม่การสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ที่เก็บเอาไว้

มาตรา 2510 (4) ได้นิยามคำว่า “ดัก” ว่าหมายถึง “เสียงหรือสิ่งอื่นที่เป็นเนื้อหาของการสื่อสารตามสาย ทางอิเล็กทรอนิกส์ หรือทางวาจาใดๆ โดยใช้อิเล็กทรอนิกส์ กลไก หรือเครื่องมืออื่นๆ” ส่วนคำว่า “การได้มา” นี้ยังไม่ชัดเจนตามคำนิยามนี้ ตัวอย่างเช่น เมื่อเครื่องมือจับตาบันทึกเนื้อหาของการสื่อสารของเจ้าหน้าที่ผู้บังคับใช้กฎหมายอาจ “ได้”การสื่อสารนั้นมา 3 กรณี กรณีแรก เมื่อเครื่องมือได้บันทึกการสื่อสาร กรณีที่สอง เมื่อผู้บังคับใช้กฎหมายได้บันทึกนั้นมาในภายหลัง หรือประการที่สาม เมื่อเจ้าหน้าที่ผู้บังคับตามกฎหมายเปิดบันทึกและได้ยินหรือเห็นเนื้อหาของการสื่อสาร บทบัญญัติในมาตรา 2510 (4) ไม่ได้ระบุว่ากรณีใดที่กล่าวมานี้เป็น “การได้มา” ตาม Title 3

นอกจากนี้นิยามคำว่า “ดัก” ไม่ได้ระบุโดยชัดแจ้งว่าการได้มาจะต้องเกิดขึ้นในขณะที่ส่ง แต่เมื่อดูตามหลักเกณฑ์ของ Title 3 และ ECPA แล้วคำว่า “ดัก” จะต้องเป็นการได้มาซึ่งการสื่อสารในขณะที่ส่ง ตัวอย่างเช่น จดหมายอิเล็กทรอนิกส์หรือไปรษณีย์เสียงอาจอยู่ในที่เก็บข้อมูลอิเล็กทรอนิกส์ก่อนที่ผู้รับจะเรียกดู หากเจ้าหน้าที่ผู้บังคับใช้กฎหมายได้มาซึ่งการสื่อสารจากที่เก็บข้อมูลอิเล็กทรอนิกส์จะไม่ถือว่าเป็นการดักการสื่อสารตามความหมายของ Title 3 เพราะการได้มาซึ่งเนื้อหาของการสื่อสารที่เก็บไว้ทางอิเล็กทรอนิกส์หรือตามสายจะอยู่ภายใต้บทบัญญัติมาตรา 2703 (a) ของ ECPAไม่ใช่ Title3[76]

ศาลส่วนใหญ่ได้นำการตีความนี้ไปใช้และวินิจฉัยว่าจะดักทั้งการสื่อสารตามสายและทาอิเล็กทรอนิกส์ได้เฉพาะในขณะที่มีการส่ง หรืออีกนัยหนึ่งการดักการสื่อสารจะใช้ได้เฉพาะการได้มาซึ่งการสื่อสารในเวลาจริงที่ทำการสื่อสาร[77]

---

[75] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2510 (12)).

[76] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 138.

[77] Konop v. Hawaiiann Airlines, Inc., 2002 WL 1941431, at *7 (9th Cir. Aug. 23, 2002).

อย่างไรก็ตามรัฐบัญญัติ Title 3 ก็ได้มีข้อยกเว้นอยู่ ซึ่งโดยหลักการแล้ว Title 3 ก็จะห้ามไม่ให้มีการดัก ใช้ หรือเปิดเผย การสื่อสารตามสายหรือทางอิเล็กทรอนิกส์โดยเจตนา เว้นแต่มีรัฐบัญญัติได้ยกเว้นไว้โดยเฉพาะ[78] โดยทั่วไปแล้ว ข้อห้ามนี้จะมีผลไม่ให้บุคคลภายนอก (เช่นรัฐ) ที่จะดักโทรศัพท์และติดตั้ง "Sniffers" อิเล็กทรอนิกส์เพื่ออ่านปริมาณการใช้อินเทอร์เน็ต (Internet traffic)

โดยหลักของข้อห้ามตาม Title 3 มีอยู่ว่าการจับตาตาม Title 3 จะชอบด้วยกฎหมายหรือไม่ จะขึ้นอยู่กับว่ารัฐบัญญัติได้กำหนดข้อยกเว้นไว้หรือไม่ Title 3 มีข้อยกเว้นจำนวนมาก ซึ่งอาจนำมาใช้ในกรณีต่างๆ อย่างไรก็ตาม ในคดีอาชญากรรมคอมพิวเตอร์จะมีข้อยกเว้นที่มักจะนำมาใช้อยู่เสมอ 7 ประการ ได้แก่

(1) การดักตามคำสั่งศาล ตามมาตรา 2518

(2) ข้อยกเว้นเรื่อง "ความยินยอม" ตามมาตรา 2511 (2) (c)-(d)

(3) ข้อยกเว้นเรื่อง "ผู้ให้บริการ" ตามมาตรา 2511 (2) (a) (i)

(4) ข้อยกเว้นเรื่อง "ผู้บุกรุกทางคอมพิวเตอร์" ตามมาตรา 2511 (2) (i)

(5) ข้อยกเว้นเรื่อง "โทรศัพท์พ่วง" ตามมาตรา 2510 (5) (a)

(6) ข้อยกเว้นเรื่อง "การได้พยานหลักฐานในคดีอาญามาโดยบังเอิญ" ตามมาตรา 2511 (3) (b) (iv) และ

(7) ข้อยกเว้นเรื่อง "การเข้าถึงสาธารณชน" ตามมาตรา 2511 (2) (g) (i)

1) การดักที่ได้รับอนุญาตโดยคำสั่งศาล ตาม Title 3 ตาม 18 U.S.C. มาตรา 2518

Title 3 ยอมให้เจ้าหน้าที่ผู้บังคับใช้กฎหมายดักการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์โดยคำสั่งศาลตาม 18 U.S.C. มาตรา 2518 คำร้องของสหรัฐในกรณีการดักการสื่อสารตามสายจะต้องได้รับการอนุมัติจากเจ้าหน้าที่ระดับสูงของกระทรวงยุติธรรมและในกรณีการดักการสื่อสารทางอิเล็กทรอนิกส์ จะต้องได้รับการอนุมัติจากผู้กำหนดนโยบายของกระทรวงยุติธรรม (Justice Department Policy) เมื่อได้รับอนุญาตจากกระทรวงยุติธรรมและผู้พิพากษาศาลประจำเขตหรือศาลอุทธรณ์ได้ลงนามในคำสั่งตาม Title 3 เจ้าหน้าที่ผู้บังคับใช้กฎหมายจะสามารถดักการสื่อสารได้นานถึง 30 วัน[79]

มาตรา 2516-2518 ได้กำหนดหลักเกณฑ์ที่เคร่งครัดหลายประการในการที่พนักงานสอบสวนจะต้องปฏิบัติตาม เพื่อจะได้รับคำสั่งศาลตาม Title 3 นี้ คำร้องเพื่อให้ศาลมีคำสั่งดังกล่าวจะต้องแสดงเหตุอันควรเชื่อว่า การดักจะทำให้ได้พยานหลักฐานการกระทำความผิดอาญาร้ายแรง

---

[78] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2511 (1)).

[79] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2518).

ตามบัญชีที่ปรากฏในมาตรา 2516[80] ในกรณีของเจ้าหน้าที่ของสหรัฐ การดักการสื่อสารตามสายจะทำได้เฉพาะความผิดอาญาร้ายแรงที่เชื่อว่าเกิดขึ้นตามที่ระบุไว้ในมาตรา 2516 (1) (a)-(n) สำหรับการดักการสื่อสารทางอิเล็กทรอนิกส์จะทำให้ในกรณีของความผิดอาญาร้ายแรงทุกประเภท[81] อาชญากรรมที่เชื่อว่าเกิดขึ้นที่สหรัฐจะสามารถสอบสวนจะปรากฏตามรายการใน 18 U.S.C. มาตรา 2516 (2) คำร้องเพื่อให้ศาลมีคำสั่งตามTitle 3 นั้นจะต้อง

(1) แสดงให้เห็นว่าไม่สามารถใช้กระบวนการสอบสวนแบบทั่วไปหรือการใช้การสอบสวนแบบทั่วไปไม่น่าจะสำเร็จ หรืออันตรายจนเกินไป[82]

(2) จะต้องมีเหตุอันควรเชื่อว่า มีการใช้เครื่องมือการสื่อสารในการประกอบอาชญากรรม และ

(3) จะต้องแสดงว่า การจับตานั้นจะไม่ไปกระทบการสื่อสารส่วนที่ไม่เกี่ยวกับพยานหลักฐานการกระทำผิดอาญา[83]

จะเห็นได้ว่ากฎหมายดังกล่าวของอเมริกาจะมีกระบวนการต่างๆ ที่จะต้องแสดงเหตุในการใช้มาตรการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ โดยจะต้องเป็นคดีอาญาร้ายแรงและแสดงเหตุผลที่จะใช้มาตรการดังกล่าวแก่ศาล ซึ่งศาลก็จะใช้ดุลพินิจพิจารณาและให้อำนาจดังกล่าวแก่เจ้าพนักงานเพื่อใช้มาตรการดังกล่าวต่อไป

ศาลอุทธรณ์แห่งหนึ่งยังได้วินิจฉัยว่ารัฐจะต้องเปิดเผย “เจตนาที่จะใช้บริการของพลเรือน ในการจับตาการดำเนินการตามกฎหมาย” ตาม Title 3 United States v. Lopez, 2002 WL 1880282, at*7 (1st Cir. Aug. 20, 2002) [84]

ประเทศสหรัฐอเมริกาได้บัญญัติประเภทความผิดที่อนุญาตให้มีการดักฟังทางโทรศัพท์และการเข้าถึงข้อมูลทางอิเล็กทรอนิกส์ไว้ในมาตรา 2516 (1) ของ Omnibus Crime Control and Safe Street Act 1968 ซึ่งลักษณะของความผิดทางอาญาที่จะสามารถดักฟังเพื่อประโยชน์ในการสืบสวนสอบสวนและป้องกันอาชญากรรม มีดังนี้[85]

---

[80] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2518 (3) (a) - (b)).

[81] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2516 (3).

[82] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2518 (1) (c)).

[83] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2518 (5).

[84] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 141.

[85] ธนชัย นักสอน. (2552). *การตรวจสอบและถ่วงดุลการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ ตามมาตรา 25 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547.* หน้า 48-50.

(a) ความผิดที่มีโทษประหารชีวิตหรือจำคุกเกินกว่า 1 ปี ตามมาตรา 2274 ถึง 2277 ของภาค 42 แห่งประมวลกฎหมายสหรัฐเกี่ยวกับการบังคับใช้ The Atomic Energy Act of 1954 มาตรา 2284 ของภาค 42 แห่งประมวลกฎหมายของสหรัฐเกี่ยวกับการก่อวินาศกรรมอุปกรณ์นิวเคลียร์หรือพลังงานความผิดตามภาค 18 แห่งประมวลกฎหมายสหรัฐ ในบทที่ 37 (เกี่ยวกับการจารกรรม) บทที่ 105 (เกี่ยวกับการก่อวินาศกรรม) บทที่ 115 (เกี่ยวกับการก่อกบฏ) บทที่ 102 (เกี่ยวกับการก่อจลาจล) บทที่ 65 (เกี่ยวกับการทำลายทรัพย์สินส่วนตัวโดยมีเจตนาร้ายต่อเจ้าของหรือผู้ครอบครองทรัพย์สินดังกล่าว) บทที่ 111 (เกี่ยวกับการทำลายเรือ) หรือบทที่ 81 (เกี่ยวกับโจรสลัด)

(b) การละเมิดมาตรา 186 หรือมาตรา 501 (c) ของภาค 26 แห่งประมวลกฎหมายของสหรัฐ (เกี่ยวด้วยข้อจำกัดในการจ่ายเงินและกู้ยืมแก่องค์กรผู้ใช้แรงงาน) การปล้นหรือกรรโชกและเป็นความผิดที่มีโทษตามภาค 18

(c) ความผิดต่างๆ ซึ่งต้องถูกลงโทษภายใต้ภาค 18 แห่งประมวลกฎหมายสหรัฐดังต่อไปนี้ มาตรา 201 (การให้สินบนเจ้าพนักงานและพยาน) มาตรา 224 (การให้สินบนในการแข่งขันกีฬา) อนุมาตรา (d) (e) (f) (g) (h) หรือ (i) ของมาตรา 844 (การใช้ระเบิดโดยผิดกฎหมาย) มาตรา 1084 (การใช้ข้อมูลเกี่ยวกับการพนัน) มาตรา 751 (เกี่ยวกับการหลบหนีจากที่คุมขัง) มาตรา 1503 1512 และ 1513 (การข่มขู่หรือทำร้ายเจ้าพนักงาน ลูกขุน หรือพยานทั่วไป) มาตรา 1510 (การขัดขวางการสืบสวนคดีอาญา) มาตรา 1511 (การขัดขวางการบังคับใช้กฎหมายสหรัฐหรือมลรัฐ) มาตรา 1751 (การลอบฆ่า การลักพาตัวประธานาธิบดีและคณะ) มาตรา 1951 (การเข้าไปเกี่ยวข้องทางการค้าโดยข่มขู่หรือใช้ความรุนแรง) มาตรา 1952 (การกระทำเกี่ยวกับการเดินทาง หรือการขนส่งระหว่างมลรัฐโดยจุดมุ่งหมายเพื่อขู่เอาเงินจากกิจการค้า) มาตรา 1958 (การรับจ้างฆาตกรรมโดยใช้เครื่องอำนวยความสะดวกในการพาณิชย์ระหว่างมลรัฐ) มาตรา 1959 (เกี่ยวกับการประกอบอาชญากรรมที่รุนแรงโดยจุดมุ่งหมายการขู่เอาเงิน) มาตรา 1954 (เสนอให้ยอมรับจะให้หรือชักชวนให้มีอิทธิพลหรือต่อการดำเนินการของโครงการผลประโยชน์ของลูกจ้าง) มาตรา 1955 (การห้ามประกอบธุรกิจเกี่ยวกับการพนัน) มาตรา 1956 (การแปรสภาพเครื่องมือเกี่ยวกับการเงิน) มาตรา 1957 (การเกี่ยวข้องกับธุรกิจทางการเงินในทรัพย์สินที่ได้มาจากการกระทำที่ไม่ชอบด้วยกฎหมาย) มาตรา 659 (การลักทรัพย์จากการขนส่งสินค้าระหว่างมลรัฐ) มาตรา 66 (ยักยอกเงินบำนาญหรือเงินสวัสดิการ) มาตรา 1343 (ฉ้อโกงทางสายวิทยุหรือโทรทัศน์) มาตรา 2315 และ 2252 (การกระทำละเมิดทางเพศต่อเด็ก) มาตรา 2312, 2313, 2314 และ 2315 (การขนส่งทรัพย์สินที่ขโมยมาระหว่างมลรัฐ) มาตรา 2321 (เกี่ยวกับการค้าพาหนะที่เป็นเครื่องยนต์หรือส่วนประกอบพาหนะที่เป็นเครื่องยนต์) มาตรา 1203 (เกี่ยวกับการจับคนเป็นตัวประกัน)

มาตรา 1029 (เกี่ยวกับการฉ้อโกงและเกี่ยวกับกิจกรรมที่ใช้เครื่องมือล้วงความลับ) มาตรา 3146 (เกี่ยวกับการลงโทษ การไม่ปรากฏตัว) มาตรา 3521 (b) (3) (เกี่ยวกับการให้พยานย้ายที่อยู่และการช่วยเหลือ) มาตรา 32 (เกี่ยวกับการทำลายเครื่องบินหรือเครื่องอำนวยความสะดวกในเครื่องบิน) มาตรา 1963 (การฝ่าฝืนโดยองค์กรที่ใช้อิทธิพลข่มขู่และให้สินบน) มาตรา 115 (เกี่ยวกับการข่มขู่หรือแก้แค้นต่อเจ้าพนักงานสหรัฐ) มาตราในบทที่ 65 (เกี่ยวกับการทำลายเครื่องมือให้พลังงาน) และมาตรา 1341 (เกี่ยวกับการฉ้อโกงทางไปรษณีย์) มาตรา 351 (การฝ่าฝืนเกี่ยวกับการลอบฆ่าหรือทำร้ายร่างกายสมาชิกรัฐสภา คณะรัฐมนตรีหรือผู้พิพากษาศาลสูง) มาตรา 831 (เกี่ยวกับการห้ามประกอบธุรกิจนิวเคลียร์) มาตรา 33 (เกี่ยวกับการทำลายพาหนะที่เป็นเครื่องยนต์ หรือเครื่องอำนวยความสะดวก) หรือมาตรา 1992 (เกี่ยวกับการทำลายรางรถไฟ)

(d) ความผิดเกี่ยวกับการปลอมแปลงที่ต้องถูกลงโทษภายใต้มาตรา 471 472 หรือ 473 ของภาค 18 นี้

(e) ความผิดเกี่ยวกับการฉ้อโกงเกี่ยวกับคดีความภายใต้ภาค 11 หรือการผลิตการนำเข้า การรับการปกปิด การซื้อ การขาย หรือความผิดในลักษณะอื่นที่เกี่ยวข้องกับยาเสพติดกัญชาหรือยาอันตรายอื่นที่มีโทษตามกฎหมายสหรัฐ

(f) ความผิดต่างๆ โดยรวมถึงกิจการค้าเชื่อ ซึ่งเอาเปรียบภายใต้มาตรา 892, 893 หรือ 894 ของภาค 18 นี้

(g) การฝ่าฝืนมาตรา 532 ของภาค 31 แห่งประมวลกฎหมายสหรัฐ (การรายงานธุรกิจทางการเงิน)

(h) การฝ่าฝืนที่เป็นความผิดตามมาตรา 2511 และ 2512 (เกี่ยวกับการดักฟังทางโทรศัพท์และการเปิดเผยการสื่อสารและเครื่องมือดักฟัง) ของภาค 18 นี้

(i) การฝ่าฝืนบทที่ 71 (เกี่ยวกับการกระทำลามกอนาจาร) ของภาค 18 นี้

(j) การฝ่าฝืนมาตรา 1679 a (c) (2) (เกี่ยวกับการทำลายท่อส่งก๊าซธรรมชาติ) หรืออนุมาตรา (i) หรือ (n) ของมาตรา 1472 (เกี่ยวกับสลัดอากาศ) ของภาค 49 แห่งประมวลกฎหมายสหรัฐ

(k) การฝ่าฝืนทางอาญาในมาตรา 2778 ของภาค 22 (เกี่ยวกับ The Arms Export Control Act)

(l) ผู้ที่ลี้ภัยมาจากการทำความผิดที่ระบุไว้ในมาตรานี้ หรือ (m) การสมคบที่จะกระทำความผิดต่างๆ ที่กล่าวมาข้างต้น

(m) การฝ่าฝืนมาตรา 922 และ 924 ของภาค 18 แห่งประมวลกฎหมายสหรัฐ (เกี่ยวกับอาวุธปืน) และ

(n) การฝ่าฝืนมาตรา 5861 แห่งประมวลรัษฎากรภายใน ค.ศ. 1986 (เกี่ยวกับอาวุธปืน) เป็นต้น ความยินยอมของผู้ที่ทำการสื่อสารตาม 18 U.S.C. มาตรา 2511 (2) (c)-(d)

18 U.S.C. มาตรา 2511 (2) (c) และ (d) กำหนดว่า "(c) ผู้ที่ดำเนินการตามกฎหมายในการดักการสื่อสารตามสาย วาจา หรือทางอิเล็กทรอนิกส์จะไม่มีความผิด เมื่อบุคคลที่ทำการสื่อสารทั้งสองฝ่ายหรือฝ่ายใดฝ่ายหนึ่งได้ให้ความยินยอมในการดักนั้นไว้ล่วงหน้า (d) ผู้ที่ไม่ได้ดำเนินการตามกฎหมายในการดักการสื่อสารตามสาย วาจา หรือทางอิเล็กทรอนิกส์ เมื่อบุคคล ที่ทำการสื่อสารทั้งสองฝ่ายหรือฝ่ายใดฝ่ายหนึ่งได้ให้ความยินยอมในการดักนั้นไว้ล่วงหน้า จะไม่มีความผิด หากไม่ได้ดักการสื่อสารเพื่อกระทำความผิดทางอาญาใดๆ หรือเพื่อละเมิดบทบัญญัติรัฐธรรมนูญหรือกฎหมายของสหรัฐหรือมลรัฐใดๆ " บทบัญญัติในเรื่องนี้ได้ให้อำนาจในการดักการสื่อสารเมื่อผู้ที่ทำการสื่อสารฝ่ายใดฝ่ายหนึ่งได้ให้ความยินยอมในการดัก ตัวอย่างเช่น ถ้าสายลับของรัฐหรือผู้ให้ข้อมูล (Informant) ได้บันทึกการสนทนาทางโทรศัพท์ระหว่างบุคคลดังกล่าวและผู้ต้องสงสัย ความยินยอมในการบันทึกดังกล่าวทำให้เกิดอำนาจในการดัก[86] ในทำนองเดียวกัน หากบุคคลบันทึกการสนทนาของตนเองกับผู้อื่น ความยินยอมของผู้บันทึกจะทำให้การดักนั้นชอบด้วยกฎหมาย เว้นแต่ผู้นั้นมีมูลเหตุจูงใจในการดักการสื่อสารเพื่อทำความผิดทางอาญาหรือทางแพ่ง[87] ความยินยอมนี้อาจทำโดยชัดแจ้งหรือปริยายก็ได้[88] ความยินยอมโดยปริยายจะเกิดขึ้นในกรณีที่ผู้ที่สื่อสารรู้ว่ามีการจับตาและไม่สนใจวิธีการที่ใช้ในการจับตา[89]

ในคดีส่วนใหญ่แล้วปัจจัยสำคัญที่ทำให้เกิดความยินยอมโดยปริยายจะดูได้จาก การที่คู่กรณีได้รับหนังสือแจ้งเรื่องการจับตา แม้จะไม่ได้ใช้ระบบการจับตาตามหนังสือดังกล่าว[90] โดยทั่วไปแล้วการพิสูจน์เรื่องหนังสือแจ้งจะทำให้ได้ข้อสรุปว่า คู่กรณีรู้เรื่องการจับตา[91] หากไม่มีการพิสูจน์เรื่องหนังสือแจ้ง รัฐจะต้องแสดงให้เห็นถึงความยินยอมโดยปริยาย[92]

การจับตาการใช้โครงข่ายคอมพิวเตอร์จะไม่เป็นการละเมิด Title 3 หากผู้ใช้บริการเห็นแถบประกาศของโครงข่าย ที่แจ้งว่า การใช้โครงข่ายเป็นการยินยอมในการจับตา โดยในคดีคอมพิวเตอร์ หลักการเรื่องความยินยอมโดยปริยายจะยอมให้มีการจับตาโครงข่ายคอมพิวเตอร์ที่ได้

---

[86] Obron Atlantic Corp. v. Barr, 990 F.2d 861 (6th Cir.1993).

[87] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 141-142.

[88] United States v. Amen, 831 F.2d 373, 378 (2nd Cir.1987).

[89] United States v. Workman, 80 F.3d 688, 693 (2d Cir. 1996).

[90] Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998).

[91] Workman, 80 F.3d at 693.

[92] United States v. Lanoue, 71 F.3d 966, 981 (1st Cir 1995).

มีการ “ขึ้นแถบประกาศไว้” โดยแถบประกาศจะขึ้นเตือนผู้ใช้เมื่อเข้ามาใช้โครงข่ายว่าอาจมีการจับตาการใช้และการใช้ระบบดังกล่าวจะถือว่าได้รับแจ้งเรื่องการจับตา[93] แต่อย่างไรก็ตามข้อความตามแถบประกาศที่แคบจนเกินไป อาจทำให้สามารถจับตาเพียงบางกรณีข้อความที่กว้างขึ้นก็อาจทำให้จับตาได้มากขึ้น

นอกจากนี้ผู้ที่ทำการสื่อสารในที่นี้ศาลบางศาลได้ให้ความเห็นว่าเจ้าของระบบคอมพิวเตอร์อาจเป็น “ผู้ที่ทำการสื่อสาร” เมื่อผู้ใช้ได้ส่งการสื่อสารไปยังระบบของบุคคลดังกล่าว[94]

2) ข้อยกเว้นเรื่องผู้ให้บริการตาม 18 U.S.C. มาตรา 2511 (20) (a) (i)

ลูกจ้างหรือเจ้าหน้าที่ของผู้ให้บริการสื่อสารอาจดักและเปิดเผยการสื่อสารเพื่อคุ้มครองสิทธิและทรัพย์สินของผู้ให้บริการ ตัวอย่างเช่นโดยทั่วไปแล้วผู้บริหารระบบโครงข่ายคอมพิวเตอร์อาจจับตาการบุกรุกโครงข่ายของแฮ็กเกอร์และเปิดเผยผลของการจับตาแก่เจ้าหน้าที่ผู้บังคับใช้กฎหมายโดยไม่เป็นการละเมิดต่อ Title 3 อย่างไรก็ตามข้อยกเว้นนี้จะเป็นเรื่องของผู้ให้บริการเท่านั้นและไม่รวมถึงเจ้าหน้าที่ผู้บังคับใช้กฎหมาย เมื่อผู้ให้บริการได้แจ้งเรื่องการบุกรุกดังกล่าวทางคอมพิวเตอร์แก่เจ้าหน้าที่ผู้บังคับใช้กฎหมายอาจมีการนำข้อยกเว้นเรื่องผู้บุกรุกทางคอมพิวเตอร์มาใช้ในการจับตาของเจ้าหน้าที่ผู้บังคับใช้กฎหมาย[95]

มาตรา 2511 (2) (a) (i) ยอมให้เจ้าหน้าที่สลับแผงควบคุม หรือ Switchboard หรือเจ้าหน้าที่ ลูกจ้างหรือพนักงานของผู้ให้บริการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ผู้ซึ่งใช้เครื่องมือในการส่งการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ในการดักเปิดเผยหรือใช้การสื่อสารนั้นในทางการที่จ้างในขณะที่ทำการซึ่งจำเป็นในการบริการหรือเพื่อป้องกันสิทธิหรือทรัพย์สินของผู้ให้บริการ เว้นแต่ผู้ให้บริการสื่อสารตามสายแก่สาธารณชนจะไม่อาจใช้บริการติดตามหรือสุ่มจับตาเว้นแต่เพื่อตรวจควบคุมระบบหรือการบริการ

การคุ้มครองสิทธิหรือทรัพย์สินของผู้ให้บริการตามมาตรานี้ ได้ให้สิทธิแก่ผู้ให้บริการในการดักและจับตาการสื่อสารที่พบในระบบของเขาเพื่อปราบปรามการฉ้อโกงและลักทรัพย์ของบริการตัวอย่างเช่นลูกจ้างของของบริษัทโทรศัพท์เคลื่อนที่อาจดักการสื่อสารที่มีการถอดแบบโทรศัพท์เคลื่อนที่โดยไม่ชอบด้วยกฎหมายเพื่อหาที่มาของโทรศัพท์ดังกล่าว[96] ข้อยกเว้นในเรื่องนี้ยังยอมให้ผู้ให้บริการจับตาการกระทำไม่ชอบต่อระบบเพื่อป้องกันระบบจากการถูกทำลาย

---

[93] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 142.

[94] United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993).

[95] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2511 (2) (a) (i).

[96] คดี United States v. Pervaz, 118 F.3d 1, 5 (1st Cir. 1997).

ลักทรัพย์หรือละเมิดสิทธิส่วนบุคคล ตัวอย่างเช่นผู้บริหารระบบสามารถที่จะติดตามร่องรอยของแฮ็กเกอร์ในโครงข่ายเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นในอนาคต[97]

มีข้อสังเกตว่า ข้อยกเว้นดังกล่าวไม่ได้ยอมให้ผู้ให้บริการที่จะจับตาอย่างไม่มีขอบเขต แต่ยอมให้ผู้ให้บริการและพนักงานดำเนินการตามสมควรในการจับตาตามความจำเป็นเพื่อการคุ้มครองสิทธิและทรัพย์สินของผู้ให้บริการโดยพิจารณาเปรียบเทียบกับสิทธิส่วนบุคคลในการสื่อสารของสมาชิก ในการสอบสวนการเข้าใช้ระบบโดยมิชอบดังกล่าวผู้ให้บริการมีอำนาจอย่างกว้างขวางในการจับตาและเปิดเผยพยานหลักฐานการใช้โดยมิชอบตามมาตรานี้แต่ควรพยายามที่จะจำแนกการจับตาและเปิดเผยเพื่อไม่ให้มีการดักและเปิดเผยการสื่อสารของราษฎรที่ไม่เกี่ยวข้องกับการสอบสวน นอกจากนี้ถึงแม้ว่าผู้ให้บริการอาจคุ้มครองสิทธิและทรัพย์สินของตนได้ด้วยการรวบรวมพยานหลักฐานการกระทำผิดอาญาเพื่อการฟ้องร้องดำเนินคดี ผู้ให้บริการไม่สามารถใช้ข้อยกเว้นเรื่องสิทธิหรือทรัพย์สินในการรวบรวมพยานหลักฐานที่ไม่เกี่ยวข้องกับสิทธิหรือทรัพย์สินของเขา[98]

ถึงแม้ว่าข้อยกเว้นดังกล่าวได้ยินยอมให้ผู้ให้บริการดักและเปิดเผยการสื่อสารแก่เจ้าหน้าที่ผู้บังคับใช้กฎหมายเพื่อคุ้มครองสิทธิและทรัพย์สินของตนแต่ก็ไม่ได้ยอมให้เจ้าหน้าที่ผู้บังคับใช้กฎหมายชี้นำหรือขอให้ผู้บริการระบบจับตาตามความต้องการของเจ้าหน้าที่ผู้บังคับใช้กฎหมาย

โดยทั่วไปแล้วเจ้าหน้าที่ผู้บังคับใช้กฎหมายควรจะยอมรับพยานหลักฐานเกี่ยวกับการกระทำความผิดของผู้ต้องสงสัยจากการจับตาของผู้ให้บริการตามมาตรานี้ ที่เกิดขึ้นก่อนที่จะมีการแจ้งเรื่องการสื่อสารให้เจ้าหน้าที่ผู้บังคับใช้กฎหมายทราบอย่างไรก็ตามหลังจากที่ได้รับแจ้งแล้วเจ้าหน้าที่ผู้บังคับใช้กฎหมายควรจะยอมรับผลของการจับตาเฉพาะเมื่อเข้าหลักเกณฑ์ในเรื่องการจับตาและการเปิดเผยเพื่อคุ้มครองสิทธิหรือทรัพย์สินของผู้ให้บริการดังนี้

(1) ผู้ให้บริการเป็นเหยื่อของการกระทำความผิดและต้องการที่จะดักและเปิดเผยเพื่อคุ้มครองสิทธิและสิทธิของตน

(2) เจ้าหน้าที่ผู้บังคับใช้กฎหมายรับรองว่าการจับตาของผู้ให้บริการเกิดขึ้นจากความประสงค์ที่จะคุ้มครองสิทธิและทรัพย์สินของตนไม่ใช่เพื่อช่วยเหลือเจ้าหน้าที่

(3) เจ้าหน้าที่ผู้บังคับใช้กฎหมายไม่ได้ดำเนินการอะไรไม่ได้ชี้นำขอร้องหรือแนะนำการจับตาหรือเปิดเผยเพื่อช่วยเหลือเจ้าหน้าที่ และ

---

[97] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 144.

[98] แหล่งเดิม. หน้า. 145.

(4) เจ้าหน้าที่ผู้บังคับใช้กฎหมายไม่ได้เข้ามีส่วนร่วมหรือควบคุมการจับตาที่เกิดขึ้น ถึงแม้กฎหมายไม่ได้กำหนดไว้[99]

อย่างไรก็ตามข้อยกเว้นเรื่องผู้ให้บริการนี้เจ้าหน้าที่ผู้บังคับใช้กฎหมายกับผู้ให้บริการก็อาจเกี่ยวข้องดำเนินการด้วยกันหากโครงข่ายที่จะคุ้มครองเป็นตัวแทนหรือสาขาของรัฐตัวอย่างเช่น หน่วยงานของสหรัฐเช่น NASA ไปรษณีย์และทหารที่มีทั้งโครงข่ายคอมพิวเตอร์ขนาดใหญ่และเจ้าหน้าที่ผู้บังคับใช้กฎหมาย เนื่องจากทั้งเจ้าหน้าที่ผู้บังคับใช้กฎหมายและผู้บริหารระบบของรัฐต่างมองว่าเป็นทีมเดียวกันจึงเป็นเรื่องยั่วยวนใจสำหรับเจ้าหน้าที่ผู้บังคับใช้กฎหมายที่จะสั่งให้ผู้บริการจับตาและเห็นว่าเป็นเรื่องชอบธรรมที่จะทำเช่นนั้นเพราะการตีความกว้างเรื่องป้องกันสิทธิและทรัพย์สินของผู้ให้บริการ ถึงแม้ว่าศาลจะไม่ได้กล่าวถึงความมีอยู่ของหลักการเรื่องการจัดการของผู้ให้บริการเช่นการตีความแต่โดยความหมายอย่างกว้างอาจไม่เป็นการง่ายที่จะตัดสินคดีด้วยการตีความข้อยกเว้นเรื่องผู้ให้บริการ[100]

3) ข้อยกเว้นเรื่องผู้บุกรุกทางคอมพิวเตอร์ตาม 18 U.S.C. มาตรา 2511 (2) (i)

18 U.S.C. มาตรา 2511 (2) (i) ยอมให้ผู้เสียหายที่ถูกโจมตีทางคอมพิวเตอร์ที่จะอนุญาตให้เจ้าหน้าที่ผู้บังคับใช้กฎหมายดักการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ เจ้าหน้าที่ผู้บังคับใช้กฎหมายอาจดักการสื่อสารของผู้บุกรุกทางคอมพิวเตอร์ ที่ส่งไปยัง ผ่านหรือจากคอมพิวเตอร์ที่มีการคุ้มครองหากเข้าเงื่อนไข 4 ประการ ดังนี้

ประการแรก เจ้าของหรือพนักงานของคอมพิวเตอร์ที่มีการคุ้มครองจะต้องอนุญาตให้ดักผู้บุกรุกการสื่อสาร[101] โดยทั่วไปแล้วถึงแม้ว่ารัฐบัญญัติจะไม่ได้กำหนดหลักเกณฑ์ไว้โดยเฉพาะแต่ในทางปฏิบัติพนักงานสอบสวนก็ควรจะมีหนังสือยินยอมให้ดักของเจ้าของคอมพิวเตอร์หรือพนักงานระดับสูงของเจ้าของคอมพิวเตอร์[102]

ประการที่สอง บุคคลที่ดักการสื่อสารจะต้องเกี่ยวข้องกับการสอบสวนตามกฎหมาย[103]

ประการที่สาม บุคคลซึ่งดักการสื่อสารจะต้อง มีเหตุผลอันควรเชื่อว่าเนื้อหาการสื่อสารของผู้ที่บุกรุกทางคอมพิวเตอร์จะต้องเกี่ยวข้องกับการสอบสวน[104]

---

[99] แหล่งเดิม. หน้า. 146-147.

[100] คดี McLaren, 957 F. Supp. At 219.

[101] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2511 (2) (i) (l)).

[102] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 149.

[103] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2511 (2) (i) (ll)).

[104] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2511 (2) (i) (lll)).

ประการที่สี่ การดักไม่ควรจะได้มาซึ่งการสื่อสารใดๆ ที่ไม่ใช่สิ่งที่ส่งไปยังหรือจากผู้บุกรุกทางคอมพิวเตอร์[105]

ด้วยเหตุนี้พนักงานสอบสวนอาจไม่ไปข้องเกี่ยวกับผู้บุกรุกคอมพิวเตอร์ เว้นแต่ไม่สามารถหลีกเลี่ยงที่จะดักการสื่อสารของผู้ใช้ซึ่งมีอำนาจที่จะใช้และได้ให้ความยินยอมในการดักนั้น

Title 3 ได้ให้ความหมายคำว่า “ผู้บุกรุกทางคอมพิวเตอร์” ไว้ว่าหมายถึง “บุคคลซึ่งเข้าไปในคอมพิวเตอร์ที่ได้รับความคุ้มครองโดยไม่ได้รับอนุญาต ซึ่งนิยามดังกล่าวไม่ได้รวมถึงบุคคลใดๆ ซึ่งเป็นเจ้าของหรือพนักงานซึ่งมีความสัมพันธ์ทางสัญญากับเจ้าของหรือพนักงานเพื่อเข้าถึงคอมพิวเตอร์ที่ได้รับการคุ้มครองทั้งหมดหรือบางส่วน”[106] ตามคำนิยามดังกล่าวลูกค้าของผู้ให้บริการซึ่งละเมิดข้อกำหนดในการบริการที่ผู้ให้บริการได้วางไว้ ไม่ถือเป็นผู้บุกรุกคอมพิวเตอร์และคำนิยามของคำว่า “คอมพิวเตอร์ที่ได้รับความคุ้มครอง” ตาม 18 U.S.C. มาตรา 2030 (e) (2) ว่าให้รวมถึงคอมพิวเตอร์ใดๆ ที่ใช้ในการค้าระหว่างมลรัฐหรือระหว่างประเทศหรือการสื่อสารเช่นเดียวกับคอมพิวเตอร์ส่วนใหญ่ที่ใช้โดยรัฐของสหรัฐหรือองค์กรทางการเงิน ดังนั้นคอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ตจะเป็นคอมพิวเตอร์ที่ได้รับการคุ้มครอง[107]

4) ข้อยกเว้นเรื่องโทรศัพท์พ่วงตาม 18 U.S.C. มาตรา 2510 (5) (a)

ตาม 18 U.S.C. มาตรา 2510 (5) (a) การใช้อุปกรณ์หรือเครื่องมือโทรศัพท์หรือโทรเลขหรือส่วนใดๆ ของโทรศัพท์หรือโทรเลขจะไม่ถือว่าเป็นการละเมิด Title 3 หาก

(1) ผู้ให้บริการติดตั้งแก่สมาชิกหรือผู้ใช้บริการการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ในทางปกติทางการค้าของตนและสมาชิกหรือผู้ใช้ได้ใช้ตามทางปกติทางการค้าหรือสมาชิกหรือผู้ใช้ดังกล่าวติดตั้งเพื่อการติดต่อกับเครื่องมือของบริการดังกล่าวและใช้ตามทางปกติการค้า หรือ

(2) ผู้ให้บริการได้ใช้การสื่อสารหรือเจ้าหน้าที่ผู้บังคับใช้กฎหมายได้ใช้ในการปฏิบัติหน้าที่ตามปกติของตน[108]

ข้อยกเว้นเรื่องโทรศัพท์พ่วง กำหนดไว้ชัดเจนว่าเมื่อบริษัทโทรศัพท์ทำการติดตั้งโทรศัพท์เครื่องพ่วงให้กับนายจ้าง เพื่อวัตถุประสงค์ที่เกี่ยวกับการทำงานที่ชอบด้วยกฎหมายแล้ว

---

[105] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2511 (2) (i) (IV)).

[106] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2510 (21)).

[107] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 149.

[108] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2510 (5) (a)).

การที่นายจ้างจับตาการใช้โทรศัพท์พ่วงของลูกจ้าง เพื่อวัตถุประสงค์ที่เกี่ยวกับการทำงานที่ชอบด้วยกฎหมายนั้นไม่ถือว่าเป็นการละเมิด Title 3[109]

ข้อยกเว้นตาม 18 U.S.C. มาตรา 2510 (5) (a) (ii) ที่ยอมให้พนักงานสอบสวนหรือเจ้าหน้าที่ผู้บังคับใช้กฎหมาย ใช้เครื่องมือ อุปกรณ์โทรศัพท์หรือโทรเลขหรือส่วนใดๆ ของโทรศัพท์หรือโทรเลข ในการปฏิบัติหน้าที่ตามปกติ เป็นที่มาแห่งความสับสน ข้อความดังกล่าวนี้ไม่ได้อนุญาตให้เจ้าหน้าที่ดักการสื่อสารของราษฎรตามหลักการที่ว่าเจ้าหน้าที่ผู้บังคับใช้กฎหมายอาจจำเป็นที่จะดักการสื่อสาร ในการปฏิบัติหน้าที่ตามปกติ ในการปฏิบัติหน้าที่ตามปกติในที่นี้จึงหมายถึงการสอบสวนของเจ้าหน้าที่นั้นเอง[110]

5) ข้อยกเว้นเรื่องการได้มาซึ่งพยานหลักฐานในคดีอาญาโดยไม่ได้ตั้งใจตาม 18 U.S.C. มาตรา 2511 (3) (b) (iv)

18 U.S.C. มาตรา 2511 (3) (b) ได้วางหลักเกณฑ์หลายประการที่ผู้ให้บริการการสื่อสารทางอิเล็กทรอนิกส์แก่สาธารณะในการเปิดเผยเนื้อหาของการสื่อสาร สิ่งที่สำคัญที่สุดของข้อยกเว้นในเรื่องนี้ก็คือ การยอมให้ผู้ให้บริการเปิดเผยเนื้อหาการติดต่อสื่อสารใดๆ ที่ผู้ให้บริการได้มาโดยไม่ตั้งใจ อันเป็นเรื่องเกี่ยวกับการกระทำผิดทางอาญาแก่เจ้าหน้าที่ผู้บังคับใช้กฎหมาย[111] แม้ว่าศาลยังไม่เคยนำข้อยกเว้นเรื่องนี้มาใช้ในคดีเกี่ยวกับคอมพิวเตอร์ที่มีการพิมพ์เผยแพร่ แต่ข้อความตามกฎหมายก็ได้แสดงให้เห็นว่า ยอมให้ผู้ให้บริการรายงานการกระทำความผิดทางอาญา (เช่น พยานหลักฐานที่เป็นแผนการฉ้อโกง หรือภาพลามกอนาจารของเด็ก) ซึ่งไม่เป็นการละเมิดต่อ Title 3[112]

6) ข้อยกเว้นเรื่องการเข้าถึงของสาธารณชนตาม 18 U.S.C. มาตรา 2511 (2) (g) (i)

18 U.S.C. มาตรา 2511 (2) (g) (i) ยอมให้บุคคลใดๆ ดักการสื่อสารทางอิเล็กทรอนิกส์ที่ได้กระทำผ่านระบบ ซึ่งมีการเก็บไว้เพื่อให้สาธารณชนทั่วไปสามารถเข้าถึงโดยง่าย[113] แม้ว่าศาลยังไม่เคยนำข้อยกเว้นเรื่องนี้มาใช้ในคดีเกี่ยวกับคอมพิวเตอร์ที่มีการพิมพ์เผยแพร่แต่ข้อความ

---

[109] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 150.

[110] แหล่งเดิม. หน้า 151.

[111] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2511 (5) (b)).

[112] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 152.

[113] The Wiretap statute (title 3), amended 1986 (U.S.C. title 18 section 2511 (2) (g) (i)).

ตามกฎหมายก็ได้แสดงให้เห็นว่า ยอมให้ดักการสื่อสารทางอิเล็กทรอนิกส์ซึ่งได้ขึ้นไว้บนกระดานข่าวของสาธารณชนหรือห้องคุยของสาธารณชน[114]

3.1.2 รัฐบัญญัติ The Pen/Trap Statute, amended 2001

รัฐบัญญัตินี้ ได้กำหนดรูปแบบการเข้าไปของรัฐที่ล่วงล้ำน้อยกว่าในรัฐบัญญัติ The Wiretap Statute กฎหมายนี้ให้อำนาจในการติดตั้ง Pen Register และ Trap and Trace โดย Pen Register จะบันทึกการหมุนโทรศัพท์ เส้นทางและแสดงข้อมูลที่เกี่ยวกับการสื่อสารอิเล็กทรอนิกส์ที่ออกไป (Outgoing) การสื่อสารอิเล็กทรอนิกส์หมายถึง โทรศัพท์ คอมพิวเตอร์ โทรเลข โทรพิมพ์ ส่วนเครื่องมือ Trap and Trace จะบันทึกข้อมูลเช่นเดียวกันแต่เป็นการสื่อสารที่เข้ามา (Incoming) แต่ข้อเท็จจริงที่สำคัญคือทั้งสองแบบจะไม่บันทึกเนื้อหาของการสื่อสารเพียงแต่บันทึกข้อมูลที่เกี่ยวกับเบอร์โทรศัพท์ทั้งที่เป็นการเรียกออกและเรียกเข้า[115] ซึ่งโดยทั่วไปแล้วรัฐบัญญัติ Pen/Trap จะกล่าวถึงการเก็บสารสนเทศเกี่ยวกับที่อยู่และสารสนเทศที่ไม่ใช่เนื้อหาของการสื่อสารตามสายหรืออิเล็กทรอนิกส์ ส่วน Title 3 จะกล่าวถึงการเก็บตัวเนื้อหาของการสื่อสารตามสายและทางอิเล็กทรอนิกส์ ซึ่งรัฐบัญญัติทั้งสองต้องใช้ควบคู่กันเพราะกฎหมายทั้งสองฉบับนี้กล่าวถึงการเข้าถึงข้อมูลต่างประเภทกัน โดย Title 3 จะยอมให้รัฐได้มาซึ่งเนื้อหาการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ในระหว่างการสื่อสาร ส่วนรัฐบัญญัติ Pen/Trap จะกล่าวถึงการเก็บสารสนเทศประเภทที่อยู่หรือสารสนเทศที่ไม่ใช่เนื้อหาในเวลาจริง[116]

จะเห็นว่าความแตกต่างระหว่างสารสนเทศที่อยู่และสารสนเทศเนื้อหาอย่างชัดเจนในกรณีการสื่อสารแบบเดิมเช่น โทรศัพท์ โดยสารสนเทศที่อยู่ของการโทรศัพท์ก็คือหมายเลขโทรศัพท์ที่โทรออกและหมายเลขโทรศัพท์ที่เป็นสารสนเทศประจำตัวของผู้โทรนั้นเอง โดยจุดแบ่งระหว่างสารสนเทศที่อยู่และสารสนเทศที่เป็นเนื้อหานี้ได้ใช้กับการสื่อสารทางอินเทอร์เน็ต ตัวอย่างเช่น เมื่อเชื่อมต่อคอมพิวเตอร์เข้ากับการสื่อสารอินเทอร์เน็ต จะมีการแบ่งข้อความเป็นส่วนๆ เรียกว่า กลุ่มข้อมูลหรือ Packets และทำการส่งกลุ่มข้อมูลแต่ละส่วนไปยังจุดหมายปลายทาง โดยกลุ่มข้อมูลแต่ละกลุ่มจะมีสารสนเทศที่อยู่ปรากฏอยู่ในส่วนหัวเรื่องของกลุ่ม ตามด้วยข้อความที่เป็นเนื้อหา รัฐบัญญัติ Pen/Trap ยอมให้เจ้าหน้าที่ผู้บังคับใช้กฎหมายได้มาซึ่งสารสนเทศที่อยู่ของการสื่อสารอินเทอร์เน็ต อย่างไรก็ตามการอ่านสารสนเทศทั้งหมดที่อยู่ในกลุ่มข้อมูลจะเป็น

---

[114] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. หน้าเดิม.

[115] ไพจิตร สวัสดิสาร. เล่มเดิม. หน้า 72.

[116] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 129.

เรื่องเกี่ยวกับ Title 3 ข้อแตกต่างเบื้องต้นระหว่างอุปกรณ์ Pen/Trap ที่ใช้กับอินเทอร์เน็ตกับอุปกรณ์จับสารสนเทศที่ใช้กับอินเทอร์เน็ตตาม Title 3 (โดยทั่วไปเรียกว่า Sniffer) ก็คือสิ่งแรกจะเป็นโปรแกรมที่ใช้ในการกักและเก็บสารสนเทศที่อยู่เท่านั้น แต่สิ่งหลังจะเป็นโปรแกรมที่ใช้ในการกักและเก็บสารสนเทศทั้งกลุ่มข้อมูล[117]

โดยหลักเกณฑ์แล้วรัฐบัญญัติ Pen/Trap ยอมให้พนักงานอัยการ (Government Attorney) ขอให้ศาลสั่งอนุญาตให้ติดตั้ง Pen Register หรือ Trap and Trace นานเท่าที่มีความเป็นไปได้ที่สารสนเทศซึ่งเกี่ยวข้องกับการสอบสวนคดีอาญาที่กำลังดำเนินการ[118]

รัฐบัญญัติ Pen/Trap ได้ให้นิยามคำว่า Pen Registers และอุปกรณ์ Trap and Trace อย่างกว้างๆ โดยคำว่า “Pen Register” หมายถึง อุปกรณ์หรือกระบวนการซึ่งบันทึกหรือถอดรหัสสารสนเทศเกี่ยวกับการโทรศัพท์ การติดต่อ ที่อยู่ หรือสัญญาณซึ่งมีการส่งโดยใช้อุปกรณ์หรือเครื่องมือที่ส่งตามสาย หรือทางอิเล็กทรอนิกส์ อย่างไรก็ตามสารสนเทศดังกล่าวจะต้องไม่มีเนื้อหาของการสื่อสาร[119] Pen Register จะไม่รวมถึงอุปกรณ์หรือกระบวนการที่ใช้ในการเรียกเก็บค่าบริการหรือบัญชีค่าใช้จ่าย (Cost Accounting) [120]

คำว่า “Trap and Trace” หมายถึง อุปกรณ์หรือกระบวนการซึ่งจับอิมพัลส์อิเล็กทรอนิกส์หรืออย่างอื่นที่ส่งเข้ามา โดยแสดงสารสนเทศที่เป็นหมายเลขผู้โทรเข้าหรือการติดต่อที่อยู่หรือสัญญาณ ซึ่งสามารถระบุถึงแหล่งที่มาของการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ที่ให้บริการ อย่างไรก็ตามสารสนเทศดังกล่าวจะต้องไม่มีเนื้อหาของการสื่อสาร[121]

เนื่องจากส่วนหัวเรื่องของอินเทอร์เน็ตจะมีสารสนเทศทั้งของ “ผู้รับ” และ “ผู้ส่ง” อุปกรณ์ที่สามารถอ่านส่วนหัวเรื่องทั้งหมด (ยกเว้นเรื่องในส่วนหัวเรื่องของจดหมายอิเล็กทรอนิกส์) จะเรียกว่าอุปกรณ์ Pen/Trap

เหตุผลของการนิยามที่กล่าวมานี้ ก็เนื่องมาจากความแตกต่างของส่วนประกอบของอุปกรณ์โดยประการแรก เครื่องมือหรืออุปกรณ์ที่ใช้ส่งการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์เกี่ยวข้องกับเทคโนโลยีในการสื่อสารหลายประเภท เช่นโทรศัพท์ โทรศัพท์เคลื่อนที่ บัญชีสมาชิกผู้ใช้อินเทอร์เน็ต และบัญชีสมาชิกจดหมายอิเล็กทรอนิกส์ และ

---

[117] แหล่งเดิม. หน้า 130.

[118] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3122 (b) (2)).

[119] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3127 (3)).

[120] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 131.

[121] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3127 (4)).

IP Address ประการที่สอง นิยามดังกล่าวนี้รวมถึง สารสนเทศทุกชนิดเกี่ยวกับการโทรศัพท์การติดต่อ ที่อยู่ หรือสัญญาณที่เป็นสารสนเทศที่ไม่ใช่เนื้อหาเกือบทุกประเภทของการสื่อสาร ประการที่สาม เนื่องจากนิยามของคำว่า Pen Register และ Trap and Trace มีความหมายรวมถึงทั้งอุปกรณ์และกระบวนการ ดังนั้นรัฐบัญญัติฉบับนี้จึงครอบคลุมการทำงานของชุดคำสั่งและตัวอุปกรณ์ดังกล่าว[122]

จะเห็นได้ว่าจากคำนิยามดังกล่าวข้างต้นเป็นการให้คำนิยามถึงลักษณะและคุณสมบัติของ “Pen Register” และ “Trap and Trace” (Pen/Trap) ในความหมายอย่างกว้างโดย Pen/Trap เป็นการเรียกชื่อของกระบวนการและตัวอุปกรณ์ ในการตรวจสอบการติดต่อสื่อสารทั้งขาเข้าและขาออก แต่อย่างไรก็ตามสำหรับชื่อเรียกที่เป็นภาษาไทยของกระบวนการและตัวอุปกรณ์ดังกล่าวในประเทศไทยก็มีการกำหนดไว้ อาทิเช่น ในการใช้มาตรการเข้าถึงข้อมูลการสื่อสารของเจ้าพนักงานในคดียาเสพติด ก็จะเรียก “Pen Register” และ “Trap and Trace” โดยรวมๆ ว่า “ระบบการตรวจสอบการใช้งานโทรศัพท์ ทั้งเข้าและออก”[123] นอกจากนี้ก็ยังมีการเรียกชื่อของกระบวนการและตัวอุปกรณ์ดังกล่าวอย่างอื่นอีกโดยกำหนดให้ “Pen Register” เรียกว่า “อุปกรณ์การบันทึกและถอดรหัสเพื่อระบุจำนวนครั้งที่ใช้” และ “Trap and Trace” เรียกว่า “อุปกรณ์ที่ช่วยระบุเลขหมายของเครื่องต้นทาง”[124] ดังนั้นผู้เขียนเห็นว่าเพื่อให้ง่ายต่อการเรียกชื่อและจดจำและสอดคล้องกับคำนิยามตามรัฐบัญญัติ Pen/Trap จึงสมควรกำหนดชื่อเรียกโดยรวมของ “Pen Register” และ “Trap and Trace” (Pen/Trap) ตามที่เจ้าพนักงานในคดียาเสพติดได้กำหนดไว้โดยเรียกชื่อว่า “ระบบการตรวจสอบการใช้งานโทรศัพท์ทั้งเข้าและออก”

สำหรับคำสั่งเพื่อให้ได้มาซึ่งระบบการตรวจสอบการใช้งานโทรศัพท์ทั้งเข้าและออก (Pen/Trap) ผู้ยื่นคำขอจะต้องระบุถึง สถานะของตนและของหน่วยงานที่ทำการสอบสวนและยืนยันความเชื่อว่า สารสนเทศดังกล่าวเกี่ยวข้องกับการสอบสวนคดีอาญาที่กำลังดำเนินการโดยหน่วยงานนั้น[125] ศาลที่ออกคำสั่งจะต้องมีเขตอำนาจในท้องที่ซึ่งมีการสอบสวน[126] หากคำขอได้ระบุ

---

[122] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 132.

[123] ระเบียบคณะกรรมการป้องกันและปราบปรามยาเสพติดว่าด้วยการได้มา การใช้ประโยชน์และการเก็บรักษาข้อมูลข่าวสาร พ.ศ. 2545.

[124] อรรณพ ลิขิตจิตถะ และคณะ. (2548). *การพัฒนากฎหมายป้องกันและปราบปรามอาชญากรรมข้ามชาติที่มีการจัดตั้งในลักษณะองค์กร (ระยะที่ 2) หัวข้อ เทคนิคการสืบสวนสอบสวนพิเศษ* (รายงานผลการวิจัย). หน้า 16.

[125] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3122 (b) (1)-(2)).

[126] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3127 (2) (2)).

ถึงรายละเอียดเหล่านี้ ศาลจะอนุญาตให้ติดตั้งและใช้ระบบการตรวจสอบการใช้งานโทรศัพท์ทั้งเข้าและออก (Pen/Trap) ไม่ว่าในที่ใดๆ ในสหรัฐ[127] ศาลจะไม่ดำเนินการไต่สวนข้อเท็จจริงที่มีการรับรองดังกล่าวเป็นการเฉพาะต่างหากคำสั่งในการติดตั้ง ระบบการตรวจสอบการใช้งานโทรศัพท์ทั้งเข้าและออก (Pen/Trap) ของสหรัฐ อาจมีผลบังคับใช้ภายนอกเขตท้องที่ของศาลที่ออกคำสั่งในกรณีคำขอของสหรัฐ คำสั่งนั้น จะใช้ได้กับบุคคลหรือองค์กรใดๆ ที่ให้บริการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ในสหรัฐ ที่อาจให้ความช่วยเหลือในการปฏิบัติงานตามคำสั่งนั้น[128] ตัวอย่างเช่น พนักงานอัยการสหรัฐ อาจได้มาซึ่งคำสั่งเพื่อติดตาม (Trace) การใช้โทรศัพท์ที่โทรเข้าเครื่องโทรศัพท์หนึ่ง คำสั่งนั้นไม่เพียงแต่จะใช้กับผู้ให้บริการในท้องถิ่นนั้นแต่ยังใช้ได้กับผู้ให้บริการรายอื่น ที่โทรเข้าหมายเลขโทรศัพท์ผู้ต้องสงสัย ทำนองเดียวกันในกรณีอินเทอร์เน็ต พนักงานอัยการสหรัฐอาจได้มาซึ่งคำสั่งให้ติดตามการสื่อสาร ที่มีถึงคอมพิวเตอร์หรือ IP Address ของผู้เสียหายคนใดคนหนึ่งหากผู้กระทำผิดใช้ช่องทางการสื่อสารโดยผ่านคอมพิวเตอร์หลายเครื่องเป็นทอดๆ คำสั่งดังกล่าวย่อมสามารถนำมาใช้กับคอมพิวเตอร์ทุกเครื่องดังกล่าวได้[129]

รัฐบัญญัติ Pen/Trap ก็ไม่ได้ระบุว่าคำขอหรือคำสั่งในการติดตั้งระบบการตรวจสอบการใช้งานโทรศัพท์ ทั้งเข้าและออก (Pen/Trap) จะต้องระบุชื่อผู้ให้บริการทุกๆ รายที่จะต้องปฏิบัติตามคำสั่งศาล แม้ว่าคำสั่งนั้นจะต้องระบุถึงผู้ให้บริการรายแรก ในการขอความช่วยเหลือจากผู้ให้บริการ พนักงานสอบสวนจะต้องส่งคำสั่งให้แก่ผู้ให้บริการ และเมื่อผู้ให้บริการร้องขอเจ้าหน้าที่ผู้บังคับใช้กฎหมายจะต้องให้ คำรับรองเป็นหนังสือหรืออิเล็กทรอนิกส์ ว่าใช้คำสั่งดังกล่าวกับผู้ให้บริการรายนั้น[130] นอกจากนี้รัฐบัญญัตินี้อาจอนุญาตให้ใช้อุปกรณ์ Pen/Trap เป็นเวลา 60 วันและอาจขยายระยะเวลาไปได้อีก 60 วัน[131] คำสั่งศาลยังอาจสั่งห้ามไม่ให้ผู้ให้บริการเปิดเผยเรื่องการติดตั้งระบบการตรวจสอบการใช้งานโทรศัพท์ ทั้งเข้าและออก (Pen/Trap) แก่บุคคลใดๆ เว้นแต่หรือจนกระทั่งศาลจะสั่งเป็นอย่างอื่น[132] และอาจสั่งให้ผู้ให้บริการการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ ผู้ให้เช่าอสังหาริมทรัพย์ ผู้พิทักษ์ทรัพย์ หรือบุคคลอื่นจัดทำสารสนเทศ เครื่องมือ และสิ่งจำเป็นในการให้ความช่วยเหลือทางเทคนิคทุกชนิดโดยด่วนเพื่อการ

---

[127] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3127 (a) (1)).

[128] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3123 (a) (1)).

[129] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 132-133.

[130] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3123 (a) (1)).

[131] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3123 (c)).

[132] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3122 (d) (2)).

ติดตั้งระบบการตรวจสอบการใช้งานโทรศัพท์ ทั้งเข้าและออก (Pen/Trap)[133] ผู้ให้บริการซึ่งได้รับคำสั่งให้ความช่วยเหลือโดยการติดตั้งระบบดังกล่าว สามารถขอค่าเสียหายตามสมควรจากการใช้จ่ายอย่างสมเหตุสมผลที่เกิดขึ้นในการจัดทำเครื่องมือหรือให้ความช่วยเหลือทางเทคนิคแก่เจ้าหน้าที่ผู้บังคับใช้กฎหมาย[134] การกระทำโดยสุจริตของผู้ให้บริการ ในการปฏิบัติตามคำสั่งศาลโดยให้ความช่วยเหลือตามคำสั่งดังกล่าว สามารถใช้เป็นข้ออ้างเพื่อยกเว้นความผิดจากการถูกฟ้องคดีแพ่งและอาญาใดๆ [135]

รัฐบัญญัตินี้ยังได้กำหนดให้มีการรายงานในกรณีที่เจ้าหน้าที่ได้ติดตั้งระบบการตรวจสอบการใช้งานโทรศัพท์ ทั้งเข้าและออก (Pen/Trap) ของตนบนโครงข่ายที่มีการสลับกลุ่มข้อมูลหรือ Packet Switched ของผู้ให้บริการการสื่อสารทางอิเล็กทรอนิกส์[136] ปกติแล้วเมื่อเจ้าหน้าที่ผู้บังคับใช้กฎหมายจะส่งคำสั่งติดตั้งระบบการตรวจสอบการใช้งานโทรศัพท์ ทั้งเข้าและออก (Pen/Trap) ให้แก่ผู้ให้บริการ จากนั้นผู้ให้บริการจะรวบรวมสารสนเทศที่เกี่ยวข้องและส่งมอบให้เจ้าหน้าผู้บังคับใช้กฎหมาย ในกรณีที่ผู้ให้บริการไม่สามารถทำให้หรือไม่ยอมปฏิบัติตามคำสั่ง รัฐอาจติดตั้งระบบการตรวจสอบการใช้งานโทรศัพท์ ทั้งเข้าและออก (Pen/Trap) เอง เช่น DCS 1000 ของ FBI ในกรณีดังกล่าวรัฐจะต้องให้สารสนเทศดังต่อไปนี้ โดยปิดผนึกแก่ศาลภายใน 30 วันหลังจากคำสั่งสิ้นผล คือ

(1) ชื่อเจ้าหน้าที่ซึ่งติดตั้งและใช้อุปกรณ์

(2) วันและเวลาที่มีการติดตั้ง ใช้ และถอดอุปกรณ์

(3) การปรับแต่งอุปกรณ์ ณ จุดติดตั้ง และการปรับแต่งอุปกรณ์ภายหลังจากนั้นและ

(4) สารสนเทศที่รวบรวมได้จากการใช้อุปกรณ์นั้นๆ [137]

เมื่อรัฐทำการติดตั้งระบบการตรวจสอบการใช้งานโทรศัพท์ ทั้งเข้าและออก (Pen/Trap) รัฐจะต้องใช้ เทคโนโลยีที่สามารถใช้ได้แก่ระบบนั้นตามสมควร เพื่อหลีกเลี่ยงการบันทึกหรือการถอดรหัสเนื้อหาของการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์[138]

นอกจากนี้รัฐบัญญัติยังได้ให้อำนาจแก่ผู้ให้บริการการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ในการใช้ระบบการตรวจสอบการใช้งานโทรศัพท์ ทั้งเข้าและออก (Pen/Trap)

---

[133] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3124 (a) (b)).

[134] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3124 (c)).

[135] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3124 (d) (e)).

[136] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3123 (a) (3) (A)).

[137] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3123 (a) (3)).

[138] The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3123 (c)).

กับโครงข่ายของตนโดยไม่ต้องมีคำสั่งศาลโดย 18 U.S.C. 3121 (b) บัญญัติว่าผู้ให้บริการอาจใช้อุปกรณ์ Pen/Trap โดยไม่ต้องมีคำสั่งของศาลในกรณีดังนี้

(1) เกี่ยงข้องกับการดำเนินการ การดูแลและทดสอบบริการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์หรือการคุ้มครองสิทธิหรือทรัพย์สินของผู้ให้บริการนั้น หรือเพื่อคุ้มครองผู้ใช้จากการให้บริการโดยมิชอบหรือการใช้บริการที่ไม่ชอบด้วยกฎหมาย หรือ

(2) เพื่อบันทึกข้อเท็จจริงว่ามีการติดตั้งหรือทำให้สมบูรณ์ซึ่งการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ เพื่อคุ้มครองผู้ให้บริการนั้นผู้ให้บริการอื่นที่จะทำให้การสื่อสารตามสายบรรลุผลหรือคุ้มครองผู้ใช้บริการจากการฉ้อโกง การให้บริการโดยมิชอบหรือ

(3) ได้รับความยินยอมจากผู้ใช้บริการดังกล่าว

3.1.3 การเยียวยาความเสียหายซึ่งเกิดจากการละเมิด Title 3 และรัฐบัญญัติ Pen/Trap

การละเมิดบทบัญญัติดังกล่าว ทำให้เจ้าหน้าที่และพนักงานอัยการจะต้องรับผิดในทางแพ่งและทางอาญาและพยานหลักฐานที่ได้มาก็ห้ามรับฟัง[139] ในทางปฏิบัติศาลอาจวินิจฉัยว่ามีการละเมิดบทบัญญัติเรื่องการจับตาทางอิเล็กทรอนิกส์ แม้ว่าเจ้าหน้าที่และพนักงานอัยการได้กระทำโดยสุจริตหรือทำตามกฎหมาย เช่น ในบางครั้งราษฎรได้ดักฟังโทรศัพท์ของเพื่อนบ้านและได้นำหลักฐานที่ได้ไปมอบให้แก่ตำรวจหรือเจ้าหน้าที่อาจจะดักการสื่อสารตามคำสั่งศาลที่รู้ในภายหลังว่าใช้บังคับไม่ได้ ทั้งเกิดจากการที่ศาลตีความ Title 3 ไม่ตรงกับเจ้าหน้าที่ที่สืบสวน[140]

สำหรับการเยียวยาโดยไม่รับฟังพยานหลักฐานนั้น Title 3 ได้วางหลักเกณฑ์การไม่รับฟังพยานหลักฐานที่เกิดขึ้นจากการดักการสื่อสารด้วยวาจาและการสื่อสารตามสายที่ได้มาโดยไม่ชอบ แต่ไม่รวมถึงกรณีการสื่อสารทางอิเล็กทรอนิกส์ที่รัฐบัญญัติ Pen/Trap ไม่ได้วางหลักเกณฑ์เรื่องการเยียวยาโดยห้ามไม่ให้รับฟังพยานหลักฐานไว้นอกจากนี้การละเมิดรัฐธรรมนูญอาจจะมีผลให้มีการไม่รับฟังพยานหลักฐานที่ได้มาโดยไม่ชอบเช่นกัน[141]

---

[139] U.S.C. title 18 section 2511 (4), 2520, 3121 (d), 2518 (10) (a).

[140] แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา, สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. เล่มเดิม. หน้า 152-153.

[141] แหล่งเดิม. หน้า. 153.

3.2 กฎหมายอื่นๆ ที่เกี่ยวข้อง

3.2.1 รัฐบัญญัติ The Electronic Communication Privacy Act (ECPA) 1986[142]

รัฐบัญญัตินี้ก็ถือว่าเป็นการแสวงหาพยานหลักฐานทางคอมพิวเตอร์อย่างหนึ่งซึ่งต่างกับการดักฟังทางโทรศัพท์และการได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์ผู้เขียนจึงขอไม่อธิบายอย่างละเอียด โดย ECPA เป็นอำนาจทางกฎหมายในการควบคุมในกรณีของไฟล์คอมพิวเตอร์ที่เก็บไว้ (Stored) ที่ถูกส่งไปยังผู้บริหารเครือข่าย (Network Administrator) ซึ่งต่างจากการดักฟัง (Interception) ที่การสื่อสารเป็นเวลาในขณะนั้นที่อยู่ภายใต้ The Wiretap Statute

ข้อมูลคอมพิวเตอร์ที่เก็บไว้รวมถึง การสื่อสารอินเทอร์เน็ตทั้งหมด เช่นอีเมล์ที่เก็บไว้ในเครื่องแม่ข่ายของผู้ให้บริการ (Internet Service Provider (ISP)) ข้อมูลที่เก็บไว้ในเครือข่ายมีระดับการป้องกันความเป็นส่วนบุคคลในระดับต่างๆ กัน ขึ้นอยู่กับความสำคัญหรือความไวต่อความความรู้สึกของข้อมูล ใน 18 U.S.C. มาตรา 2703 รัฐบัญญัติ ECPA จึงมีระดับอยู่ 5 ระดับ ซึ่งระดับใดที่มีความไวต่อความรู้สึกมากขึ้น ความชอบธรรมที่รัฐบาลต้องแสดงเพื่อให้ได้รับข้อมูลจากบุคคลที่สามก็จะมากขึ้นโดยเฉพาะผู้บริหารระบบ ข้อมูลที่ไวต่อความรู้สึกที่สุดประกอบด้วยเนื้อหาการสื่อสารที่ไม่ได้ถูกนำมาใช้อีก เช่นอีเมล์ที่อยู่ในการเก็บข้อมูลทางอิเล็กทรอนิกส์เป็นเวลา 180 วัน หรือน้อยกว่า แต่หลังจาก 180 วัน ข้อมูลดังกล่าวเป็นข้อมูลที่ไม่สดและไม่ได้รับความคุ้มครองในระดับต้นๆ และไม่ต้องใช้หมายค้นในการเข้าถึงข้อมูลนั้น ส่วนข้อมูลที่ไวต่อความรู้สึกน้อยที่สุดรวมถึงข้อมูลพื้นฐานเท่านั้น เช่น ชื่อของสมาชิก และใบเสร็จจ่ายอย่างไร การได้รับข้อมูลดังกล่าวนี้ รัฐบาลจำเป็นเพียงออกหมายเรียกทางฝ่ายบริหารเท่านั้น หมายเรียกดังกล่าวออกโดยหน่วยงานของรัฐโดยไม่ต้องขออนุญาตศาลก่อน เช่น FBI สามารถออกหมายเรียกในเหตุอันสมควร หากในภายหลังมีการคัดค้านและศาลเห็นว่าไม่มีเหตุสมควร ข้อมูลที่ได้รับภายใต้หมายเรียกก็จะถูกยกเลิกไป

3.2.2 รัฐบัญญัติ The USA Patriot Act 2001[143]

โดยปกติผู้ที่เป็นเป้าหมายในการค้นจะถูกแจ้งให้ทราบในเวลาที่มีการค้นทางกายภาพ แต่รัฐบัญญัตินี้อนุญาตให้มีการแจ้งให้ทราบภายหลัง (Delayed Notification) ซึ่งเป็นบทบัญญัติที่เรียกว่า “แอบมอง”

นอกจากนี้ รัฐบัญญัตินี้ทำให้ผู้ที่ใช้กฎหมายสามารถติดตั้งเครื่องมือการลอบติดตามอิเล็กทรอนิกส์ง่ายขึ้น เดิมคำสั่งการดักฟังหรือคำสั่ง Pen Register ขอออกได้ในเขตอำนาจที่เครื่องมือนั้นติดตั้ง แต่การสื่อสารทางอินเทอร์เน็ตจะเกี่ยวกับผู้ให้บริการอินเทอร์เน็ตตั้งอยู่ใน

---

[142] ไพจิตร สวัสดิสาร. เล่มเดิม. หน้า 70-71.

[143] ไพจิตร สวัสดิสาร. เล่มเดิม. หน้า 72-73.

เขตอำนาจต่างๆ กัน มาตรา 216 และ220 จึงอนุญาตให้มีการติดตั้งเครื่องมือทุกแห่งในสหรัฐอเมริกา

มาตรา 225 มีความสำคัญต่อผู้ที่ทำการสืบสวนทางนิติคอมพิวเตอร์และผู้ให้ข้อมูลแก่รัฐบาล ทั้งให้ภูมิคุ้มกันในการฟ้องร้องคดีทางแพ่งกับบุคคลใดที่ให้ความช่วยเหลือทางเทคนิคหรืออื่นๆ ในการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ตามคำสั่งศาล หรือตามที่ร้องขอตามกฎหมายในการให้ความช่วยเหลือฉุกเฉิน

รัฐบัญญัตินี้บทบัญญัติขยายขอบเขตการสืบสวนออกไป แต่อย่างไรก็ตามยังมีบทบัญญัติการสิ้นสุด หรือ “Sunset Provision” ซึ่งบทบัญญัตินี้จะสิ้นสุดในวันที่ 31 ธันวาคม 2005 ถ้าสภาคองเกรสไม่ขยายเวลาต่อไป แต่บทบัญญัติการสิ้นสุดนี้ไม่ใช้กับรัฐบัญญัติทั้งฉบับส่วนที่สำคัญเช่นการให้อำนาจในการแจ้งการค้นในภายหลังและคำสั่งการดักฟังจะไม่สิ้นสุดโดยอัตโนมัติ

3.2.3 รัฐบัญญัติ The Sarbanes-Oxley Act of 2002[144]

รัฐบัญญัตินี้ออกมาสืบเนื่องจากเหตุการณ์คดี United States of America v. Arthur Andersen LLP ของศาล United States District Court Southern District of Texas กล่าวคือ วันที่ 15 มิถุนายน 2002 แอนเดอร์เสนถูกตัดสินในข้อหาต่อต้านความยุติธรรมโดยทำลายเอกสารที่เกี่ยวกับการตรวจสอบการเงินของลูกค้าเอ็นรอน จึงเป็นผลให้คณะกรรมการหุ้นและหลักทรัพย์ไม่อนุญาตให้แอนเดอร์เสนผู้กระทำการตรวจสอบบริษัทอื่น แอนเดอร์เสนจึงยอมถอนใบอนุญาตและสิทธิในการปฏิบัติการตรวจสอบในวันที่ 31 สิงหาคม ในขณะเดียวกันได้มีการตั้งคณะกรรมการการพิจารณาทางบัญชีที่ผิดพลาดของบริษัทมหาชนหรือ Public Company Accounting Oversight Board (“Oversight Board”)

รัฐบัญญัตินี้ จึงได้ออกมาบังคับเรื่องการกันเอกสารอิเล็กทรอนิกส์ การบังคับโทษทางอาญาที่เข้มงวดในกรณีที่มีการเปลี่ยนแปลงหรือทำลายหลักฐานที่บันทึกไว้ รวมถึงสิ่งที่เก็บในรูปของอิเล็กทรอนิกส์และบังคับเรื่องผลผลิตของหลักฐานที่บันทึกไว้ในรูปแบบอิเล็กทรอนิกส์กับเอกสารอื่น เมื่อเรียกโดยคณะกรรมการการพิจารณาทางบัญชีที่ผิดพลาดของบริษัทมหาชน

จึงเห็นได้ว่ารัฐบัญญัตินี้ช่วยในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์เนื่องจากช่วยให้ผู้กระทำผิดที่ลบข้อมูลที่อาจใช้เป็นพยานหลักฐานนั้นเพื่อปกปิดความผิดของตนได้รับโทษที่หนัก

---

[144] แหล่งเดิม. หน้า 73.

บทที่ 4
วิเคราะห์ความเหมาะสมของการนำหลักการแสวงหาพยานหลักฐานทางคอมพิวเตอร์มาปรับใช้กับประมวลกฎหมายวิธีพิจารณาความอาญาของไทยและการกำหนดฐานความผิดที่เกี่ยวข้อง

จากที่เคยกล่าวมาแล้วในบทที่ 2 นั้นการแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาไทยในปัจจุบันจะมีแค่การใช้วิธีการแสวงหาพยานหลักฐานด้วยวิธีการเข้าค้นเพื่อยึดพยานเอกสารหรือพยานวัตถุ จากเคหสถานของบุคคล การใช้วิธีการแสวงหาพยานหลักฐานด้วยวิธีการจับ การค้นเพื่อยึดพยานเอกสารหรือพยานวัตถุจากตัวบุคคล การแสวงหาพยานหลักฐานจากร่างกายมนุษย์เท่านั้น ซึ่งยังไม่เพียงพอ โดยประมวลกฎหมายวิธีพิจารณาความอาญาของไทยในเรื่องการค้นในที่รโหฐานของเจ้าพนักงาน เพื่อให้ได้พยานหลักฐานซึ่งถือว่าเป็นการแสวงหาพยานหลักฐานอย่างหนึ่ง แต่เนื่องจากลักษณะในการค้นของเจ้าพนักงานนั้นจะมีลักษณะไปในทางกายภาพเสียมากกว่า กล่าวคือเป็นการค้นเพื่อพบหรือยึดสิ่งของซึ่งจะใช้เป็นพยานหลักฐานหรือสิ่งของที่มีไว้เป็นความผิดหรือได้มาโดยผิดกฎหมาย หรือมีเหตุอันควรสงสัยว่าได้ใช้หรือตั้งใจจะใช้ในการกระทำผิด หรือเหตุอื่นๆ ตามกฎหมาย แต่การค้นข้อมูลคอมพิวเตอร์ค่อนข้างมีความสลับซับซ้อนและละเอียดอ่อนอย่างมาก ทั้งยังโยงใยหลายเครือข่ายซึ่งข้อมูลนั้นอาจไม่อยู่ในคอมพิวเตอร์นั้นก็ได้ทำให้เกิดปัญหาอย่างมากในแง่ของการค้นหาพยานหลักฐานดังกล่าวโดยการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ซึ่งถือว่าเป็นการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาอย่างหนึ่งจะช่วยให้เจ้าพนักงานในคดีอาญาสามารถเข้าถึงพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลคอมพิวเตอร์ได้ ซึ่งแม้ว่าพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 เฉพาะในคดีพิเศษจะให้อำนาจเจ้าพนักงานคดีพิเศษเพื่อให้ได้มาซึ่งข้อมูลที่เป็นการสื่อสารทางโทรศัพท์รวมทั้งข้อมูลคอมพิวเตอร์[145] ที่ถือว่าเป็นการให้อำนาจเจ้าพนักงานในคดีพิเศษในการดักฟังและได้มาซึ่งพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์ก็ตาม แต่อำนาจดังกล่าวก็มีเฉพาะในคดีพิเศษตามพระราชบัญญัตินี้เท่านั้น[146] ซึ่งไม่ครอบคลุมทุกฐานความผิดโดยพยานหลักฐาน

---

[145] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547, มาตรา 25.

[146] บัญชีท้ายพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547.

ทางความผิดฐานรีดเอาทรัพย์ ความผิดฐานฉ้อโกง เป็นต้น การนำหลักการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์มาบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาของไทยจึงน่าจะเหมาะสมยิ่งกว่า แต่อย่างไรก็ตามก็ควรต้องวิเคราะห์ถึงความเหมาะสมของการนำหลักการดังกล่าวมาใช้กับประมวลกฎหมายวิธีพิจารณาความอาญาด้วยโดยการนำหลักการถ่วงดุลของการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ของกฎหมายต่างประเทศและกฎหมายไทยมาปรับใช้กับประมวลกฎหมายวิธีพิจารณาความอาญาของไทยด้วยทั้งนี้เพื่อไม่ให้อำนาจดังกล่าวไปล่วงล้ำสิทธิและเสรีภาพของประชาชนจนมากเกินสมควร

4.1 การนำหลักการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาปรับใช้ในประมวลกฎหมายวิธีพิจารณาความอาญาของไทย

กฎหมายว่าด้วยการสอบสวนคดีพิเศษเป็นกฎหมายที่ให้อำนาจแก่เจ้าหน้าที่ในการสืบสวนสอบสวนเอาตัวผู้กระทำความผิดซึ่งเป็นคดีพิเศษมาดำเนินคดีและเพื่อประโยชน์ในการสืบสวนสอบสวน เจ้าหน้าที่สามารถใช้การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ได้ในกรณีที่ไม่สามารถเข้าถึงข้อมูลด้วยวิธีอื่นแล้ว ซึ่งบทบัญญัติตามกฎหมายการสอบสวนคดีพิเศษนี้บัญญัติให้มีอำนาจในการเข้าถึงข้อมูลคล้ายคลึงกับกฎหมายที่ให้อำนาจแก่เจ้าหน้าที่ในการเข้าถึงข้อมูลและสามารถนำข้อมูลที่ได้มาจากการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์เสนอเป็นพยานหลักฐานในชั้นศาลได้คือ พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม ฉบับที่ 4 พ.ศ. 2545 ซึ่งในที่นี้จะขอกล่าวถึงพระราชบัญญัติทั้งสองนี้ในเบื้องต้นก่อนจะนำไปสู่พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547

โดยมาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และที่แก้ไขเพิ่มเติมได้บัญญัติไว้ในมาตรา 46 ซึ่งบัญญัติไว้ว่า[147]

มาตรา 46 กรณีที่มีเหตุอันควรเชื่อได้ว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงินพนักงานเจ้าหน้าที่ซึ่งเลขาธิการมอบหมายเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลแพ่ง เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชี ข้อมูลทางการสื่อสารหรือข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็ได้

---

[147] รายงานการศึกษาวิจัยเพื่อนำเสนอในการประชุมทางวิชาการระดับชาติ ว่าด้วยงานยุติธรรม ครั้งที่ 2. (2547). *มาตรการป้องกันและปราบปรามองค์กรอาชญากรรมและผู้มีอิทธิพล*. หน้า 19-20.

ในกรณีตามวรรคหนึ่ง ศาลจะสั่งอนุญาตให้พนักงานเจ้าหน้าที่ผู้ยื่นคำ ขอดำเนินการโดยใช้เครื่องมือหรืออุปกรณ์ใดๆ ตามที่เห็นสมควรก็ได้ แต่ทั้งนี้ให้อนุญาตได้คราวละไม่เกินเก้าสิบวัน

เมื่อศาลได้สั่งอนุญาตตามความในวรรคหนึ่งหรือวรรคสองแล้ว ผู้เกี่ยวข้องกับบัญชีข้อมูลทางการสื่อสารหรือข้อมูลคอมพิวเตอร์ตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้"

ในกฎหมายฟอกเงิน การเข้าถึงข้อมูลข่าวสารจำกัดเพียงบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน ซึ่งเกี่ยวกับมูลฐานความผิด 21 มูลฐาน คือ ความผิดเกี่ยวกับยาเสพย์ติด ความผิดเกี่ยวกับเพศที่เกี่ยวกับหญิงและเด็กเพื่อการค้าประเวณี ความผิดเกี่ยวกับการฉ้อโกงประชาชน ความผิดเกี่ยวกับการยักยอกทรัพย์หรือฉ้อโกงทรัพย์ที่เกี่ยวกับสถาบันการเงิน ความผิดต่อตำแหน่งหน้าที่ราชการ (คอรัปชั่น) ความผิดเกี่ยวกับกรรโชกหรือรีดเอาทรัพย์โดยอาศัยอำนาจอั้งยี่หรือซ่องโจร (กลุ่มองค์กรอาชญากรรม) ความผิดเกี่ยวกับการลักลอบหนีศุลกากร ความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา ความผิดเกี่ยวกับการพนันตามกฎหมายว่าด้วยการพนัน ความผิดเกี่ยวกับการเป็นสมาชิกอั้งยี่ตามประมวลกฎหมายอาญาหรือการมีส่วนร่วมในองค์กรอาชญากรรมที่มีกฎหมายกำหนดเป็นความผิด ความผิดเกี่ยวกับการรับของโจรตามประมวลกฎหมายอาญา เฉพาะที่เกี่ยวกับการช่วยจำหน่าย ซื้อ รับจำนำ หรือรับไว้ด้วยประการใดซึ่งทรัพย์ที่ได้มาโดยการกระทำความผิดอันมีลักษณะเป็นการค้า ความผิดเกี่ยวกับการปลอมหรือการแปลงเงินตรา ดวงตรา แสตมป์ และตั๋วตามประมวลกฎหมายอาญาอันมีลักษณะเป็นการค้า ความผิดเกี่ยวกับการค้าตามประมวลกฎหมายอาญาเฉพาะที่เกี่ยวกับการปลอม หรือการละเมิดทรัพย์สินทางปัญญาของสินค้า หรือความผิดตามกฎหมายที่เกี่ยวกับการคุ้มครองทรัพย์สินทางปัญญาอันมีลักษณะเป็นการค้า ความผิดเกี่ยวกับการปลอมเอกสารสิทธิ บัตรอิเล็กทรอนิกส์ หรือหนังสือเดินทางตามประมวลกฎหมายอาญาอันมีลักษณะเป็นปกติธุระหรือเพื่อการค้า ความผิดเกี่ยวกับทรัพยากรธรรมชาติหรือสิ่งแวดล้อม โดยการใช้ ยึดถือ หรือครอบครองทรัพยากรธรรมชาติหรือกระบวนการแสวงหาประโยชน์จากทรัพยากรธรรมชาติโดยมิชอบด้วยกฎหมายอันมีลักษณะเป็นการค้า ความผิดเกี่ยวกับการประทุษร้ายต่อชีวิตหรือร่างกายจนเป็นเหตุให้เกิดอันตรายสาหัสตามประมวลกฎหมายอาญา เพื่อให้ได้ประโยชน์ซึ่งทรัพย์สิน ความผิดเกี่ยวกับการหน่วงเหนี่ยวหรือกักขังผู้อื่นตามประมวลกฎหมายอาญาเฉพาะกรณี เพื่อเรียกหรือรับผลประโยชน์ หรือเพื่อต่อรองให้ได้รับผลประโยชน์อย่างใดอย่างหนึ่ง ความผิดเกี่ยวกับการลักทรัพย์ กรรโชก รีดเอาทรัพย์ ชิงทรัพย์ ปล้นทรัพย์ ฉ้อโกงหรือยักยอก ตามประมวลกฎหมายอาญาอันมีลักษณะเป็นปกติธุระ

ความผิดเกี่ยวกับการกระทำอันเป็นโจรสลัดตามกฎหมายว่าด้วยการป้องกันและปราบปรามการกระทำอันเป็นโจรสลัด ความผิดเกี่ยวกับการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายหลักทรัพย์ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ ความผิดเกี่ยวกับอาวุธหรือเครื่องมืออุปกรณ์ของอาวุธที่ใช้หรืออาจนำไปใช้ในการรบหรือการสงครามตามกฎหมายว่าด้วยการควบคุมยุทธภัณฑ์

การดำเนินการเกี่ยวกับการเข้าถึงข้อมูลของพนักงานเจ้าหน้าที่นั้น มีลักษณะดังนี้

1) ต้องมีการดำเนินการสั่งให้ตรวจสอบทรัพย์สินของบุคคลที่จะเข้าถึงข้อมูลข่าวสาร บัญชีหรือคอมพิวเตอร์แล้ว หรือมีบุคคลอื่นที่เกี่ยวข้องเพื่อให้ทราบถึงข้อมูลข่าวสาร บัญชีหรือคอมพิวเตอร์ที่มีความสัมพันธ์กับผู้ที่ถูกตรวจสอบทรัพย์สินนั้น หรือ

2) มีเหตุอันควรเชื่อว่ามีการกระทำความผิดฐานฟอกเงินก็สามารถเข้าถึงข้อมูลข่าวสาร บัญชีหรือคอมพิวเตอร์ได้

3) ต้องได้รับมอบหมายจากเลขาธิการ ป.ป.ง. โดยยื่นต่อศาลแพ่งซึ่งต้องพยานหลักฐานสนับสนุนเพียงพอให้เข้าเหตุอันควรเชื่อด้วย

4) ศาลแพ่งเป็นผู้อนุญาตในการเข้าถึงข้อมูลข่าวสาร บัญชี หรือคอมพิวเตอร์ ครั้งละไม่เกิน 90 วัน

5) ข้อมูลข่าวสาร บัญชี หรือคอมพิวเตอร์ ที่ได้รับสามารถใช้เป็นพยานหลักฐานในศาลได้

ส่วนมาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม ฉบับที่ 4 พ.ศ. 2545 ก็บัญญัติไว้ในมาตรา 14 จัตวา ซึ่งบัญญัติไว้ว่า[148]

“มาตรา 14 จัตวา ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด เจ้าพนักงานซึ่งได้รับอนุมัติจากเลขาธิการเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้เจ้าพนักงานได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญา พิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

---

[148] แหล่งเดิม. หน้า 20-21.

(1) มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดเกี่ยวกับยาเสพติด

(2) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดเกี่ยวกับยาเสพติดจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

(3) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวัน โดยกำหนดเงื่อนไขใดๆ ก็ได้ และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อเจ้าพนักงานได้ดำเนินการตามที่ได้รับอนุญาตแล้วให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

บรรดาข้อมูลข่าวสารที่ได้มาตามวรรคหนึ่งให้เก็บรักษาและใช้ประโยชน์ในการสืบสวนและใช้เป็นพยานหลักฐานในการดำเนินคดีเท่านั้น ทั้งนี้ตามระเบียบที่คณะกรรมการกำหนด

กฎหมายฉบับนี้ให้อำนาจในการดักฟังสื่อที่ส่งทางโทรศัพท์ ไปรษณีย์ โทรเลข เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ซึ่งเป็นการเข้าถึงข้อมูลข่าวสาร และรวมถึงคอมพิวเตอร์เฉพาะฐานความผิดเกี่ยวกับยาเสพย์ติด ซึ่งไม่ใช่ทุกฐานความผิดแต่เป็นการกำหนดเฉพาะฐานความผิดที่สำคัญซึ่งไม่รวมความผิดฐานเสพครอบครอง โดยเน้นไปในเรื่องของลักษณะข่ายงานที่สำคัญ มีการรวมตัวเป็นองค์กรอาชญากรรม

การร้องขอให้มีการดักฟังเป็นการร้องขอจากเจ้าหน้าที่ ที่มีอำนาจจับกุมเกี่ยวกับความผิดยาเสพติดโดยรวบรวมพยานหลักฐาน พฤติการณ์แห่งคดี ประวัติบุคคล ความสัมพันธ์ของกลุ่มข่ายงานหรือองค์กรต่อเลขาธิการ ป.ป.ส. เพื่ออนุมัติให้มีการดักฟัง และต้องมีรายละเอียดเกี่ยวกับค่าใช้จ่ายในการดำเนินการซึ่งต้องเสียให้กับหน่วยงานบริการทางโทรศัพท์ในการติดตั้งเครื่องรับสัญญาณทางโทรศัพท์หรือที่ส่งทางอื่นใด กำหนดระยะเวลาโดยเลขาธิการ ป.ป.ส. จะกลั่นกรองข้อมูลเอกสารที่มีการร้องขอก่อนที่จะอนุมัติ

เมื่อได้รับการอนุมัติแล้วเจ้าหน้าที่ที่ร้องขอก็จะต้องไปดำเนินการร้องขอต่อศาลต่ออธิบดีผู้พิพากษาศาลอาญาเพื่ออนุญาตให้ดักฟัง ซึ่งการอนุญาตก็คงพิจารณาจากความเห็นในการอนุมัติของเลขาธิการ ป.ป.ส. อย่างไรก็ตาม การอนุญาตให้ดักฟังเป็นระยะเวลาเท่าไหร่เป็นดุลพินิจของอธิบดีผู้พิพากษาศาลอาญาในการสั่งให้ตามคำร้องขอและตามระยะเวลาที่กฎหมายให้สูงสุดไม่เกิน 90 วัน และเมื่อครบกำหนดระยะเวลาแล้ว หากการสืบสวนยังไม่ประสบผลสำเร็จเจ้าหน้าที่ผู้ร้องขอก็ร้องขอต่ออธิบดีผู้พิพากษาศาลอาญาอนุญาตอีกเป็นคราวๆ ไปแต่ไม่เกินคราวละ 90 วัน โดยอธิบดีผู้พิพากษาศาลอาญาอาจอนุญาตให้น้อยกว่าที่ร้องขอมาก็ได้

ข้อมูลที่ได้จากการเข้าถึงข้อมูลจะมีการเก็บรักษาและใช้ประโยชน์ในการสืบสวนในทางคดีและเป็นพยานหลักฐานในศาล โดยสำนักงาน ป.ป.ส. เป็นหน่วยงานกลางในการเก็บรักษาข้อมูลเพื่อประโยชน์แห่งกฎหมายฉบับนี้ นอกจากนั้นในกฎหมายได้บัญญัติให้มีระเบียบในการดำเนินตามมาตรานี้ไว้โดยได้กำหนดเป็นระเบียบคณะกรรมการ ซึ่งได้มีการร่างเป็นระเบียบคณะกรรมการป้องกันและปราบปรามยาเสพติดว่าด้วยการได้มา การใช้ประโยชน์และการเก็บรักษาข้อมูลข่าวสาร พ.ศ. 2545

จะเห็นได้ว่าพระราชบัญญัติทั้งสองที่กล่าวเป็นมาตรการในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์อย่างหนึ่งแต่จะแบ่งไปตามประเภทคดีและวิธีการดำเนินการของหน่วยงานที่เกี่ยวข้องกับประเภทคดีที่รับผิดชอบ โดยพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ก็จะกำหนดมาตรการการแสวงหาพยานหลักฐานทางคอมพิวเตอร์เพื่อให้ได้ข้อมูลข่าวสารที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับการฟอกเงิน โดยการเข้าถึงข้อมูลข่าวสาร บัญชีหรือคอมพิวเตอร์ ของบุคคล ซึ่งได้จัดทำธุรกรรมที่มีเหตุอันควรสงสัยว่าเป็นการฟอกเงินจากการได้มาจากการกระทำความผิดตามความผิดมูลฐานที่บัญญัติไว้ในพระราชบัญญัติดังกล่าวทั้ง 21 ฐาน และพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม ฉบับที่ 4 พ.ศ. 2545 ก็จะกำหนดมาตรการการแสวงหาพยานหลักฐานทางคอมพิวเตอร์เพื่อให้ได้ข้อมูลข่าวสารที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับยาเสพย์ติดโดยเฉพาะ ซึ่งทั้งสองพระราชบัญญัติก็มีกระบวนการที่มีส่วนคล้ายคลึงกับพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ไม่ว่าจะเป็นขั้นตอนการใช้มาตรการดักฟังและการได้มาซึ่งข้อมูลอีเล็กทรอนิกส์ที่เป็นมาตรการการแสวงหาพยานหลักฐานทางคอมพิวเตอร์อย่างหนึ่ง การกำหนดระยะเวลาในการใช้มาตรการดังกล่าว การเก็บรักษาและใช้ประโยชน์ ซึ่งข้อมูลที่เข้าถึงดังกล่าว ผู้เขียนจึงเห็นว่าจะศึกษามาตรการในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 เป็นแนวทาง เนื่องจากพระราชบัญญัติดังกล่าวได้กำหนดมาตรการที่ครบถ้วนยิ่งกว่าพระราชบัญญัติ

ทั้งสอง โดยจะนำมาปรับใช้ในประมวลกฎหมายวิธีพิจารณาความอาญาไทย ซึ่งจะขอกล่าวในบทนี้อย่างละเอียด

โดยมาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 นั้น การขออนุญาตใช้การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ก็ต้องผ่านการตรวจสอบและถ่วงดุลจากองค์กรที่เป็นกลางและมีความน่าเชื่อถือ ซึ่งก็คือ ศาล เช่นเดียวกันหากมีการฝ่าฝืนบทบัญญัติกฎหมายหรือเป็นกรณีที่เจ้าหน้าที่รัฐทำการดักฟังทางโทรศัพท์และได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์โดยมิชอบแล้วข้อมูลที่ได้มาย่อมไม่สามารถใช้เป็นพยานหลักฐานในชั้นศาลได้

ดังนั้น การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ซึ่งถือเป็นวิธีการขั้นเด็ดขาดของกรมสอบสวนคดีพิเศษ จึงจำเป็นต้องมีกระบวนการกลั่นกรอง ตรวจสอบและถ่วงดุลกระบวนการในการขออนุญาตใช้มาตรการดังกล่าว ตั้งแต่ขั้นตอนการขออนุญาตตลอดจนไปถึงขั้นตอนการทำลายข้อมูลที่ได้มาจากการใช้มาตรการดังกล่าว ทั้งนี้เพื่อก่อให้เกิดความโปร่งใสในการทำงาน อันเป็นการคุ้มครองซึ่งสิทธิเสรีภาพของประชาชนและบรรลุจุดประสงค์ในการป้องกันและปราบปรามคดีพิเศษที่มีลักษณะซับซ้อนและส่งผลกระทบรุนแรงต่อสังคม

4.1.1 อำนาจของเจ้าพนักงานคดีพิเศษในการดักฟังโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์

บทบัญญัติกฎหมายที่ให้อำนาจแก่เจ้าหน้าที่ในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ เพื่อใช้ในการสืบสวนสอบสวนคดีพิเศษ คือ พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 มีบทบัญญัติว่า

“ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ พนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือจะยื่นคำขอขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญา เพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

(1) มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ

(2) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

(3) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวัน โดยกำหนดเงื่อนไขใดๆ ก็ได้ และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาตหากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไปอธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อพนักงานสอบสวนคดีพิเศษได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

บรรดาข้อมูลข่าวสารที่ได้มาตามวรรคหนึ่ง ให้เก็บรักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษซึ่งได้รับอนุญาตตามวรรคหนึ่ง และให้ใช้ประโยชน์ในการสืบสวนหรือใช้เป็นพยานหลักฐานในการดำเนินคดีพิเศษดังกล่าวเท่านั้น ส่วนข้อมูลข่าวสารอื่นให้ทำลายเสียทั้งสิ้น ทั้งนี้ ตามข้อบังคับที่ กคพ. กำหนด”

จะเห็นได้ว่าบทบัญญัติดังกล่าวให้อำนาจเจ้าพนักงานคดีพิเศษในการเข้าถึงพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ทั้งยังมีการกลั่นกรอง ตรวจสอบ ถ่วงดุล การใช้อำนาจดังกล่าวด้วย

อย่างไรก็ตาม พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 มิได้ให้นิยามความหมายหรือวิธีการได้มาซึ่งข้อมูลทางโทรศัพท์หรือสื่ออิเล็กทรอนิกส์ไว้แต่อย่างใด แต่สามารถตีความได้ว่าวิธีการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์เพื่อให้ได้มาซึ่งข้อมูลนั้น ถือว่าเป็นการได้มาซึ่งข้อมูลข่าวสารซึ่งส่งทางโทรศัพท์ คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใดตามมาตรา 25 นี้แล้ว

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 23 มุ่งหมายให้เจ้าหน้าที่ของรัฐที่เป็นพนักงานสอบสวนคดีพิเศษตามพระราชบัญญัตินี้[149] มีอำนาจในการสืบสวนและสอบสวนการกระทำความผิดทางอาญาที่เป็นคดีพิเศษ โดยสถานะของพนักงานสอบสวนคดีพิเศษเป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวน ตามประมวลกฎหมายวิธี

---

[149] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 14 “ให้กรมสอบสวนคดีพิเศษ มีพนักงานสอบสวนคดีพิเศษ และเจ้าหน้าที่คดีพิเศษ เพื่อทำหน้าที่ดำเนินการเกี่ยวกับคดีพิเศษตามที่กำหนดในพระราชบัญญัตินี้...”

พิจารณาความอาญาแล้วแต่กรณีการดำเนินการใช้วิธีการให้เข้าถึงข้อมูลข่าวสารตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 กฎหมายบัญญัติให้เป็นหน้าที่ของพนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีกรมสอบสวนคดีพิเศษเป็นหนังสือยื่นต่ออธิบดีผู้พิพากษาศาลอาญา

ดังนั้นขอบเขตการให้อำนาจพนักงานสอบสวนคดีพิเศษใช้วิธีการให้เข้าถึงข้อมูลข่าวสารตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 จึงไม่จำกัดอยู่ในขั้นการสืบสวนเท่านั้น แต่สามารถกระทำได้ทั้งในขั้นการสืบสวนและสอบสวนความผิดอาญาที่เป็นคดีพิเศษแล้ว เนื่องจากพนักงานสอบสวนคดีพิเศษเป็นผู้มีอำนาจหน้าที่ตามพระราชบัญญัตินี้โดยมีสถานะเป็นพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

4.1.2 ประเภทความผิดที่อยู่ในอำนาจของเจ้าพนักงานคดีพิเศษ

สำหรับประเภทความผิดที่สามารถขออนุญาตใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ได้มีการบัญญัติไว้ในมาตรา 21 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 กล่าวคือความผิดทางอาญานั้นต้องเป็นคดีพิเศษที่จะต้องดำเนินการสืบสวนและสอบสวนซึ่งแบ่งเป็น 4 ประเภทดังต่อไปนี้

คดีพิเศษประเภทที่หนึ่ง คดีความผิดทางอาญาตามกฎหมายที่กำหนดไว้ในบัญชีท้ายพระราชบัญญัติการสอบสวนคดีพิเศษและที่กำหนดในกฎกระทรวงโดยการเสนอแนะของคณะกรรมการคดีพิเศษโดยคดีความผิดทางอาญาตามกฎหมายดังกล่าว จะต้องมีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้

(1) คดีความผิดทางอาญาที่มีความซับซ้อน จำเป็นต้องใช้วิธีการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเป็นพิเศษ

(2) คดีความผิดทางอาญาที่มีหรืออาจมีผลกระทบอย่างรุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน ความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของประเทศ

(3) คดีความผิดทางอาญาที่มีลักษณะเป็นการกระทำความผิดข้ามชาติที่สำคัญหรือเป็นการกระทำขององค์กรอาชญากรรม

(4) คดีความผิดทางอาญาที่มีผู้ทรงอิทธิพลที่สำคัญเป็นตัวการ ผู้ใช้หรือผู้สนับสนุน

(5) คดีความผิดทางอาญาที่มีพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ซึ่งมิใช่พนักงานสอบสวนคดีพิเศษหรือเจ้าหน้าที่คดีพิเศษเป็นผู้ต้องสงสัยเมื่อมีหลักฐานตามสมควรว่าน่าจะได้กระทำความผิดอาญา หรือเป็นผู้ถูกกล่าวหาหรือผู้ต้องหาทั้งนี้ ตามรายละเอียดของลักษณะของการกระทำความผิดที่คณะกรรมการคดีพิเศษกำหนด

คดีความผิดทางอาญาตามกฎหมายที่กำหนดไว้ในบัญชีท้ายพระราชบัญญัติการสอบสวนคดีพิเศษนั้น มีดังนี้

(1) คดีความผิดตามกฎหมายว่าด้วยการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน

(2) คดีความผิดตามกฎหมายว่าด้วยการแข่งขันทางการค้า

(3) คดีความผิดตามกฎหมายว่าด้วยการธนาคารพาณิชย์

(4) คดีความผิดตามกฎหมายว่าด้วยการประกอบธุรกิจเงินทุน ธุรกิจหลักทรัพย์และธุรกิจเครดิตฟองซิเอร์

(5) คดีความผิดตามกฎหมายว่าด้วยการเล่นแชร์

(6) คดีความผิดตามกฎหมายว่าด้วยการควบคุมการแลกเปลี่ยนเงิน

(7) คดีความผิดตามกฎหมายว่าด้วยความผิดเกี่ยวกับการเสนอราคาต่อหน่วยงานของรัฐ

(8) คดีความผิดตามกฎหมายว่าด้วยการคุ้มครองแบบผังภูมิของวงจรรวม

(9) คดีความผิดตามกฎหมายว่าด้วยการคุ้มครองผู้บริโภค

(10) คดีความผิดตามกฎหมายว่าด้วยเครื่องหมายการค้า

(11) คดีความผิดตามกฎหมายว่าด้วยเงินตรา

(12) คดีความผิดตามกฎหมายว่าด้วยการชดเชยค่าภาษีอากรสินค้าส่งออกที่ผลิตในราชอาณาจักร

(13) คดีความผิดตามกฎหมายว่าด้วยดอกเบี้ยเงินให้กู้ยืมของสถาบันการเงิน

(14) คดีความผิดตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย

(15) คดีความผิดตามกฎหมายว่าด้วยบริษัทมหาชนจำกัด

(16) คดีความผิดตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน

(17) คดีความผิดตามกฎหมายว่าด้วยมาตรฐานผลิตภัณฑ์อุตสาหกรรม

(18) คดีความผิดตามกฎหมายว่าด้วยลิขสิทธิ์

(19) คดีความผิดตามกฎหมายว่าด้วยการส่งเสริมการลงทุน

(20) คดีความผิดตามกฎหมายว่าด้วยการส่งเสริมและรักษาคุณภาพสิ่งแวดล้อม

(21) คดีความผิดตามกฎหมายว่าด้วยสิทธิบัตร

(22) คดีความผิดตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์

(23) คดีความผิดตามประมวลรัษฎากร

(24) คดีความผิดตามกฎหมายว่าด้วยศุลกากร

(25) คดีความผิดตามกฎหมายว่าด้วยภาษีสรรพสามิต

(26) คดีความผิดตามกฎหมายว่าด้วยสุรา

(27) คดีความผิดตามกฎหมายว่าด้วยยาสูบ

(28) คดีความผิดตามกฎหมายว่าด้วยการประกอบธุรกิจของคนต่างด้าว

(29) คดีความผิดตามกฎหมายว่าด้วยประกันวินาศภัย

(30) คดีความผิดตามกฎหมายว่าด้วยประกันชีวิต

(31) คดีความผิดตามกฎหมายว่าด้วยการซื้อขายเกษตรล่วงหน้า

(32) คดีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

(33) คดีความผิดตามประมวลกฎหมายที่ดิน

(34) คดีความผิดตามกฎหมายว่าด้วยป่าไม้

(35) คดีความผิดตามกฎหมายว่าด้วยอุทยานแห่งชาติ

(36) คดีความผิดตามกฎหมายว่าด้วยป่าสงวนแห่งชาติ

(37) คดีความผิดตามกฎหมายว่าด้วยสงวนและคุ้มครองสัตว์ป่า

คดีพิเศษประเภทที่สอง คดีความผิดทางอาญาอื่นนอกจาก (1) ตามที่คณะกรรมการคดีพิเศษมีมติด้วยคะแนนเสียงไม่น้อยกว่าสองในสามของกรรมการทั้งหมดเท่าที่มีอยู่

คดีพิเศษประเภทที่สาม คดีที่มีการกระทำอันเป็นกรรมเดียวผิดต่อกฎหมายหลายบทและบทใดบทหนึ่งจะต้องดำเนินการโดยพนักงานสอบสวนคดีพิเศษตามพระราชบัญญัตินี้หรือคดีที่มีการกระทำความผิดหลายเรื่องต่อเนื่องหรือเกี่ยวพันกัน และความผิดเรื่องใดเรื่องหนึ่งจะต้องดำเนินการโดยพนักงานสอบสวนคดีพิเศษตามพระราชบัญญัตินี้ ให้พนักงานสอบสวนคดีพิเศษมีอำนาจสืบสวนสอบสวนสำหรับความผิดบทอื่นหรือเรื่องอื่นด้วย โดยให้ถือว่าคดีดังกล่าวเป็นคดีพิเศษ

คดีพิเศษประเภทที่สี่ บรรดาคดีที่ได้ทำการสอบสวนเสร็จแล้วโดยพนักงานสอบสวนคดีพิเศษให้ถือว่าการสอบสวนนั้นเป็นการสอบสวนในคดีพิเศษตามพระราชบัญญัตินี้แล้ว ดังนั้นคดีดังกล่าวจึงเป็นคดีพิเศษด้วย

จะเห็นได้ว่าคดีที่เจ้าพนักงานคดีพิเศษจะทำการดักฟังโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ได้นั้น อำนาจดังกล่าวก็จะอยู่ในกรอบของฐานความผิดที่เป็นคดีพิเศษดังกล่าวข้างต้นเท่านั้น ซึ่งเมื่อพิจารณาแล้วความผิดที่มีพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์มาเกี่ยวข้องนั้นอาจเป็นความผิดฐานอื่นที่ไม่ใช่คดีพิเศษก็ได้ ซึ่งอาจเป็นความผิดตามประมวลกฎหมายอาญา อาทิเช่น ความผิดฐานเรียกค่าไถ่ ความผิดฐานฉ้อโกง ความผิดฐานรีดเอาทรัพย์ ความผิดที่เกี่ยวกับความมั่นคง เป็นต้น ซึ่งตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 21 ก็กำหนดลักษณะความผิดตามกฎหมายที่อยู่ในบัญชีท้ายพระราชบัญญัติดังกล่าวที่

เจ้าพนักงานคดีพิเศษจะมีอำนาจในการดักฟังโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์เท่านั้น ซึ่งในคดีอาญาอื่นๆ ที่มีความสำคัญไม่น้อยกว่าคดีพิเศษก็ควรกำหนดอำนาจดังกล่าวด้วยเช่นกัน

4.1.3 กระบวนการขออนุญาตดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์[150]

บทบัญญัติว่าด้วยการใช้การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์นั้น ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 เป็นบทบัญญัติให้อำนาจแก่หน่วยงานและเจ้าหน้าที่ของรัฐกระทำการที่มีผลกระทบต่อสิทธิและเสรีภาพตามรัฐธรรมนูญของประชาชนหรือสร้างเงื่อนไขข้อจำกัดในการใช้เสรีภาพในการกระทำของบุคคลในการติดต่อสื่อสารถึงกัน ในกรณีมีเหตุอันควรเชื่อได้ว่าเอกสาร หรือข้อมูลข่าวสารซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ หากแต่การใช้อำนาจดังกล่าวนั้นเจ้าหน้าที่ต้องปฏิบัติตามบทกฎหมายดังกล่าวอย่างเคร่งครัด กล่าวคือเจ้าหน้าที่จะขออนุญาตใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์เฉพาะกรณีมีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าวและไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าแล้วเท่านั้น

กระบวนการขออนุญาตดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ หัวหน้าคณะพนักงานสอบสวนคดีพิเศษในคดีนั้นๆ ต้องยื่นเอกสารดังต่อไปนี้

1) หนังสือบันทึกข้อความประมวลเรื่องเหตุผลและความจำเป็น พร้อมหมายเลขโทรศัพท์ หรือ ที่อยู่ของจดหมายอิเล็กทรอนิกส์หรืออีเมล์ (E-mail Address) หรือโดเมนเนมหรือ IP Address ที่เป็นของบุคคลเป้าหมายที่ต้องการเข้าถึงข้อมูล

2) คำขอใช้มาตรการเข้าถึงข้อมูลโดยวิธีการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์

3) เอกสารประวัติบุคคลเป้าหมาย

4) หนังสือแจ้งคำสั่งอนุมัติเข้าถึงข้อมูล

5) ข้อมูลที่สนับสนุนเหตุผลในการขอ เช่น รายงานการสืบสวนสอบสวน เป็นต้น

เอกสารทั้งหมดหัวหน้าคณะพนักงานสอบสวนคดีพิเศษต้องยื่นต่อผู้อำนวยการสำนัก (ผู้บัญชาการสำนัก (เดิม)) ที่เป็นผู้รับผิดชอบคดีพิเศษเรื่องนั้นๆ ซึ่งตามกฎกระทรวงแบ่งส่วน

---

[150] ธนชัย นักสอน. เล่มเดิม. หน้า 104-109.

ราชการกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม พ.ศ. 2545 ให้แบ่งส่วนราชการกรมสอบสวนคดีพิเศษ มีจำนวน 9 สำนักที่เกี่ยวข้องกับการสืบสวนสอบสวนคดีพิเศษ ดังนี้

(1) สำนักกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ

(2) สำนักคดีการเงินการธนาคาร

(3) สำนักคดีคุ้มครองผู้บริโภคและสิ่งแวดล้อม

(4) สำนักคดีทรัพย์สินทางปัญญา

(5) สำนักคดีเทคโนโลยีและสารสนเทศ

(6) สำนักคดีภาษีอากร

(7) สำนักคดีอาญาพิเศษ

(8) สำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ

(9) สำนักพัฒนาและสนับสนุนคดีพิเศษ

ในคำขอใช้มาตรการดังกล่าวต่อศาลนั้น ต้องระบุด้วยว่าให้หัวหน้าพนักงานสอบสวนคดีพิเศษในคดีเป็นผู้ปฏิบัติและหากต้องการให้เจ้าหน้าที่คนใดทำหน้าที่ในการดักฟังทางโทรศัพท์หรือการเข้าถึงข้อมูลทางคอมพิวเตอร์ก็สามารถระบุไว้ในคำขอดังกล่าว คำขอให้ได้มาซึ่งข้อมูลข่าวสารด้วยวิธีการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ต้องประกอบด้วย

1) ระบุชื่อส่วนราชการหรือหน่วยราชการของผู้ยื่นคำขอ

2) วันเดือน ปี ที่ทำการขออนุญาต

3) ระบุชื่อและตำแหน่งเจ้าหน้าที่ผู้ขอและผู้ที่จะดำเนินการเข้าถึงข้อมูลข่าวสาร

4) ระบุรายละเอียดเกี่ยวกับบุคคลและสถานที่ ซึ่งต้องถูกดำเนินการเท่าที่จำเป็นหรือพอสมควรแก่อธิบดีผู้พิพากษาศาลอาญาที่จะกำหนดในคำสั่งได้ เหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษ พร้อมรายงานการสืบสวนที่มีรายละเอียดเกี่ยวกับข้อเท็จจริงและพฤติการณ์ของคดี

5) เหตุอันควรเชื่อได้ว่ามีข้อมูลข่าวสารที่มีการติดต่อกันผ่านทางโทรศัพท์หรือทางคอมพิวเตอร์ ซึ่งได้ถูกใช้หรืออาจถูกใช้เพื่อการกระทำความผิดที่เป็นคดีพิเศษและเชื่อได้ว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลดังกล่าว

6) ระบุการอนุมัติของอธิบดีกรมสอบสวนคดีพิเศษและวิธีการเข้าถึงข้อมูล เช่น ระบบการแสดงตำแหน่งของเครื่องมือ ระบบการตรวจสอบการใช้งานโทรศัพท์ ทั้งเข้าและออก (Pen Register, Trap and Trace Device) บันทึกการติดต่อต้นทางปลายทางของระบบโทรคมนาคม ระบบทะเบียนผู้เช่าและผู้ใช้ การบันทึกเสียงการสนทนาของบุคคลทางโทรศัพท์หรือการเข้าถึงข้อมูลด้วยการดักรับข้อมูลทางจดหมายอิเล็กทรอนิกส์ (E-mail) เป็นต้น

7) หมายเลขโทรศัพท์หรือชื่อ ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ โดเมนเนมหรือ IP Address ของบุคคลเป้าหมายที่ต้องการเข้าถึงข้อมูล

8) รายละเอียดเกี่ยวกับพฤติการณ์การกระทำความผิดและเหตุอันไม่สามารถใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าการเข้าถึงข้อมูลข่าวสารด้วยวิธีการดังกล่าว

9) กำหนดระยะเวลาในการขออนุญาตใช้มาตรการดังกล่าว

10) ลายมือชื่อและตำแหน่งผู้ขอหรือผู้ยื่นคำขอการยื่นคำขอต้องประกอบด้วยข้อมูลที่สนับสนุนเหตุผลในการขออนุญาตใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ กล่าวคือข้อมูลที่ได้มาจากการสืบสวนสอบสวนในคดีพิเศษนั้นๆ ทั้งหมด เช่น คำให้การของพยานบุคคล พยานเอกสารพยานวัตถุ ตลอดจนถึงรายงานการสืบสวนในแต่ละวันที่จะแสดงให้ผู้บังคับบัญชาและศาลได้เห็นว่ามีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางโทรศัพท์ โทรสาร คอมพิวเตอร์เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใดซึ่งถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ ประกอบกับมีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษและมีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าวโดยไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่านี้ได้ ทั้งนี้ หัวหน้าคณะพนักงานสอบสวนคดีพิเศษต้องแสดงให้เห็นว่ามีการสืบสวนสอบสวนด้วยวิธีธรรมดาทุกวิธีแล้ว ประกอบกับได้ใช้ระยะเวลาในการสืบสวนสอบสวนมาพอสมควร โดยได้ข้อมูลมาระดับหนึ่งแล้ว แต่ไม่สามารถใช้วิธีการอื่นใดที่จะได้ข้อมูลสำคัญที่เหลืออยู่ เว้นแต่การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ตามมาตรา 25 หรือหากได้ข้อมูลมาก็จะเป็นอันตรายต่อเจ้าหน้าที่หรือสายลับเกินควรหรือจะเป็นไปด้วยความยากลำบากอย่างยิ่ง กล่าวคือ การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์เป็นวิธีการสุดท้าย เพื่อให้ได้มาซึ่งข้อมูลสำคัญในคดีพิเศษนั้นๆ

เมื่อหนังสือและคำขอใช้มาตรการเข้าถึงข้อมูลโดยวิธีการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ผ่านการตรวจสอบและพิจารณาขั้นต้นโดยผู้อำนวยการสำนัก (ผู้บัญชาการสำนัก (เดิม) ที่รับผิดชอบในคดีนั้นๆ แล้ว หนังสือและคำร้องขออนุญาตใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ พร้อมทั้งข้อมูลที่สนับสนุนเหตุผลในการร้องขอทั้งหมดต้องถูกเสนอไปยังอธิบดีกรมสอบสวนคดีพิเศษ โดยจะต้องผ่านการตรวจสอบกลั่นกรองและถ่วงดุลจากรองอธิบดีที่มีความเชี่ยวชาญในการใช้มาตรการดังกล่าวซึ่งได้รับมอบหมายจากอธิบดีให้มีหน้าที่ในการตรวจสอบความชอบด้วยกฎหมายของคำขอและข้อมูลที่ใช้ประกอบทั้งหมดสำหรับการใช้อำนาจในการเข้าถึงข้อมูลตามพระราชบัญญัติการสอบสวนคดีพิเศษ

พ.ศ. 2547 มาตรา 25 โดยเฉพาะหลังจากนั้นรองอธิบดีผู้ซึ่งได้รับมอบหมายจากอธิบดีก็จะมีความเห็นว่าควรอนุมัติให้ใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ในคดีพิเศษที่ขอมาหรือไม่ เสนอไปยังอธิบดีกรมสอบสวนคดีพิเศษเพื่อใช้ดุลพินิจพิจารณาซึ่งเป็นขั้นตอนสุดท้ายสำหรับการขออนุญาตใช้มาตรการดังกล่าวภายในองค์กรกรมสอบสวนคดีพิเศษ หลังจากอธิบดีกรมสอบสวนคดีพิเศษมีคำสั่งเห็นชอบและอนุมัติเป็นหนังสือให้คณะพนักงานสอบสวนคดีพิเศษใช้อำนาจตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 ทำการเข้าถึงข้อมูลด้วยการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ หัวหน้าคณะพนักงานสอบสวนคดีพิเศษในคดีนั้น ต้องเป็นผู้ไปยื่นคำขออนุญาตจากอธิบดีผู้พิพากษาศาลอาญาในการให้ได้มาซึ่งข้อมูลข่าวสารนั้น โดยหัวหน้าคณะพนักงานสอบสวนคดีพิเศษในคดีนั้นมีหน้าที่พิสูจน์ต่อศาลให้ทราบถึงเหตุผลในการยื่นคำขอว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษและมีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว โดยไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่านี้ได้ ทั้งนี้ หัวหน้าคณะพนักงานสอบสวนคดีพิเศษต้องแสดงให้อธิบดีผู้พิพากษาศาลอาญา ปราศจากข้อสงสัยโดยแสดงข้อมูลให้เห็นว่าคณะพนักงานสอบสวนคดีพิเศษทำการสืบสวนสอบสวนด้วยวิธีธรรมดาทุกวิธีและได้ใช้ระยะเวลาในการสืบสวนสอบสวนมานานพอสมควร และต้องนำเสนอข้อมูลที่ได้มาจากการสืบสวนสอบสวนทั้งหมดเชื่อมโยงให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาเห็นว่า เมื่อใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ตามมาตรา 25 แล้ว ต้องได้ข้อมูลสำคัญในคดีพิเศษนั้นๆหรือแสดงให้เห็นว่าข้อมูลมีการผ่านทางโทรศัพท์และคอมพิวเตอร์ของบุคคลเป้าหมายที่ขออนุญาต ทั้งนี้ หัวหน้าคณะพนักงานสอบสวนคดีพิเศษอาจแสดงข้อมูลให้อธิบดีผู้พิพากษาศาลอาญาเห็นว่า หากใช้วิธีการธรรมดาในการสืบสวนสอบสวนจะเป็นอันตรายต่อเจ้าหน้าที่หรือสายลับเกินควรหรือจะเป็นไปด้วยความยากลำบากอย่างยิ่งก็ได้ กล่าวโดยสรุปคือคณะพนักงานสอบสวนคดีพิเศษต้องใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์เป็นวิธีการสุดท้ายเพื่อให้ได้มาซึ่งข้อมูลสำคัญในคดีพิเศษนั้นๆ ในการดำเนินการใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ หัวหน้าคณะพนักงานสอบสวนคดีพิเศษผู้ปฏิบัติตามคำขออาจขอให้บุคคลผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งอนุญาตของอธิบดีผู้พิพากษาศาลอาญา จัดหาให้ซึ่งข้อมูลข่าวสารทั้งหมด สิ่งอำนวยความสะดวกหรือความช่วยเหลือทางด้านเทคนิคที่จำเป็นแก่คณะพนักงานสอบสวนคดีพิเศษ โดยหัวหน้าคณะพนักงานสอบสวนคดีพิเศษจะแสดงคำสั่งของอธิบดีผู้พิพากษาศาลอาญาที่ระบุว่าให้บุคคลดังกล่าวต้องให้ความร่วมมือในการใช้มาตรการดังกล่าวเมื่ออธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตและคณะพนักงานสอบสวนคดีพิเศษ

ได้ดำเนินการเสร็จสิ้นตามที่ได้รับอนุญาตแล้ว หัวหน้าคณะพนักงานสอบสวนคดีพิเศษต้องรายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบโดยการรายงานต้องประกอบด้วย

1) รายงานบันทึกข้อมูลข่าวสาร ซึ่งเป็นการรายงานการดำเนินการตามคำขอเข้าถึงข้อมูลที่ได้รับอนุญาตจากศาล

2) บันทึกถ้อยคำเป็นลายลักษณ์อักษร เป็นการถอดข้อมูลการสนทนาหรือข้อมูลที่ส่งทางคอมพิวเตอร์จากเทปหรือเครื่องบันทึกที่ได้ทำการบันทึกถ้อยคำและข้อมูลโดยต้องเป็นการถอดทุกถ้อยคำที่ทำการดักฟังหรือดักข้อมูล

3) สิ่งที่บันทึกข้อมูลข่าวสาร ตัวอย่างเช่น เทปต้นฉบับหรือเครื่องบันทึกข้อมูลทางคอมพิวเตอร์ที่ทำการดักข้อมูล เจ้าหน้าที่ผู้กระทำการใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ ต้องติดป้ายหรือสติ๊กเกอร์แสดงวันที่ทำการดักฟังหรือดักข้อมูลและปิดผนึกประทับตรา “ลับ” พร้อมการลงลายมือชื่อกำกับ

4) รายงานบันทึกข้อมูลข่าวสารเกี่ยวกับข้อเท็จจริงหรือพฤติการณ์ของบุคคลที่ประมวลได้จากสิ่งที่บันทึกข้อมูลข่าวสาร กล่าวคือ เป็นรายงานสรุปสาระสำคัญของถ้อยคำเฉพาะที่จะใช้ประโยชน์ในคดีพิเศษ

เมื่อคณะพนักงานสอบสวนคดีพิเศษได้ข้อมูลจากการใช้มาตรการดังกล่าว คณะพนักงานสอบสวนคดีพิเศษจะทำการวิเคราะห์ข้อมูลและตัดสิ่งที่ไม่เกี่ยวกับคดีพิเศษที่ซึ่งได้รับอนุญาต และทำการเก็บรักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษและนำมาใช้ประโยชน์ในการสืบสวนหรือใช้เป็นพยานหลักฐานเฉพาะในการดำเนินคดีพิเศษที่ขออนุญาตใช้มาตรการดังกล่าวเท่านั้น ส่วนข้อมูลข่าวสารอื่นคณะพนักงานสอบสวนคดีพิเศษต้องทำลาย ตามข้อบังคับที่คณะกรรมการคดีพิเศษกำหนด

สรุปได้ว่า การใช้กระบวนการอนุญาตให้ใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติการสอบสวนคดีพิเศษพ.ศ. 2547 มาตรา 25 เป็นบทบัญญัติให้ใช้บังคับเฉพาะกรณีมีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าวและไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่า โดยต้องยื่นคำขออนุญาตจากอธิบดีผู้พิพากษาศาลอาญาในการให้ได้มาซึ่งข้อมูลข่าวสารนั้น ซึ่งผู้ยื่นคำขออนุญาตต้องเป็นพนักงานสอบสวนคดีพิเศษที่ได้รับอนุมัติจากอธิบดีเป็นหนังสือ

4.1.4 การกำหนดระยะเวลาในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์

การกำหนดระยะเวลาที่สามารถใช้การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์นั้น อธิบดีผู้พิพากษาศาลอาญาจะสั่งอนุญาตได้ครั้งละไม่เกินเก้าสิบวันและอาจมีกำหนดเงื่อนไขในการดำเนินการใช้มาตรการดังกล่าวด้วยก็ได้ หากภายหลังที่มีคำสั่งอนุญาตปรากฏข้อเท็จจริงว่า เหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร กล่าวคือเมื่อกรณีเหตุแห่งความจำเป็นในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ไม่มีอยู่หรือไม่มีความจำเป็นที่จะเข้าถึงข้อมูลและเอกสารต่างๆ เนื่องจากไม่อาจนำไปใช้ขยายผลหรือติดตามการกระทำความผิดของบุคคลอื่นได้อีกต่อไป หรือศาลพิจารณาพฤติการณ์แล้วเห็นว่าพนักงานสอบสวนคดีพิเศษสามารถสืบสวนสอบสวนเข้าถึงข้อมูลของผู้ต้องสงสัยด้วยวิธีการอื่นได้แล้ว ตลอดจนถึงศาลอาจเห็นว่าการกระทำของผู้ต้องสงสัยไม่มีเหตุอันควรเชื่อว่าจะกระทำ ความผิดที่เป็นคดีพิเศษหรือได้ใช้การสื่อสารดังกล่าวเพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษเป็นต้น ศาลก็สามารถเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควรซึ่งอาจมีคำสั่งให้ยุติการใช้มาตรการดังกล่าวหรือเปลี่ยนแปลงคำสั่งที่ได้อนุญาตไว้นั้นจนเป็นเหตุให้ไม่อาจดำเนินการต่อไปได้

หากการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์นั้น ยังไม่สามารถดักข้อมูลที่สำคัญในคดีที่คณะพนักงานสอบสวนคดีพิเศษนั้นต้องการ คณะพนักงานสอบสวนคดีพิเศษสามารถขอขยายเวลาได้ โดยยื่นต่ออธิบดีผู้พิพากษาศาลอาญา เนื่องจากบทบัญญัติมาตรา 25 ไม่ได้มีการกำหนดข้อห้ามในการขอขยายเวลาแต่อย่างใด ดังนั้นพนักงานสอบสวนคดีพิเศษจึงสามารถขอขยายเวลาได้อย่างไม่จำกัดจำนวนครั้ง แต่อธิบดีผู้พิพากษาศาลอาญาจะอนุญาตให้ใช้มาตรการดังกล่าวได้ครั้งละไม่เกินเก้าสิบวัน

แม้กฎหมายจะมิได้มีการจำกัดจำนวนครั้งไว้สำหรับการใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ แต่การนำเสนอข้อมูลสนับสนุนเหตุผลในการขอขยายเวลาต่อไป คณะพนักงานสอบสวนคดีพิเศษย่อมมีภาระการพิสูจน์มากกว่าในครั้งแรกเนื่องจากคณะพนักงานสอบสวนคดีพิเศษต้องมีการนำเสนอต่อศาลให้เห็นว่าเก้าสิบวันที่ได้ขออนุญาตทำการดักข้อมูลในครั้งแรกนั้น คณะพนักงานสอบสวนคดีพิเศษได้ข้อมูลอะไรมาบ้าง โดยต้องนำเสนอข้อมูลต่อศาลทั้งเก้าสิบวันอย่างละเอียด และต้องแสดงเหตุผลให้ศาลเห็นว่าเหตุใดภายในเก้าสิบวันแรกจึงไม่สามารถดักรับข้อมูลที่สำคัญต่อคดีได้ ซึ่งจะทำให้ศาลเห็นว่าการขออนุญาตในครั้งแรกนั้น คณะพนักงานสอบสวนคดีพิเศษอาจจะไม่มีการวิเคราะห์ข้อมูลที่ได้

จากการสืบสวนสอบสวนมาอย่างดี จึงทำให้การดักข้อมูลในครั้งแรกไม่ประสบผลสำเร็จ และอาจจะทำให้ดุลพินิจของศาลในการพิจารณาข้อมูลที่สนับสนุนการขอขยายเวลาดักฟังในครั้งที่สองหรือครั้งต่อไป ศาลอาจต้องใช้ดุลพินิจพิจารณาหรือตรวจสอบมากกว่าเดิมและศาลอาจมีแนวโน้มในการไม่อนุญาตตามคำขอ ซึ่งย่อมส่งผลให้คณะพนักงานสอบสวนคดีพิเศษมีภาระในการพิสูจน์มากยิ่งกว่าเดิมหลายเท่า

4.1.5 กระบวนการเก็บรักษา ใช้ประโยชน์และทำลายข้อมูลที่ได้มาจากการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์

เมื่ออธิบดีผู้พิพากษาศาลอาญามีคำสั่งอนุญาตให้เข้าถึงข้อมูลข่าวสารด้วยการใช้การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์แล้ว หัวหน้าคณะพนักงานสอบสวนคดีพิเศษหรือพนักงานสอบสวนคดีพิเศษผู้ขอ ต้องนำคำสั่งอนุญาตให้เข้าถึงข้อมูลข่าวสารด้วยการใช้มาตรการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ดังกล่าวรวมทั้งบัญชีแสดงรายการเครื่องมือและอุปกรณ์ที่จะใช้ในการดำเนินการ เสนออธิบดีกรมสอบสวนคดีพิเศษหรือผู้อำนวยการสำนัก (ผู้บัญชาการสำนัก (เดิม)) ที่รับผิดชอบคดีนั้นหรือผู้อำนวยการสำนักซึ่งอธิบดีมอบหมาย เพื่อพิจารณาดำเนินการมีคำสั่งจัดเก็บและให้พนักงานสอบสวนคดีพิเศษที่ได้รับมอบหมายจัดให้มีการบันทึกข้อมูลข่าวสารที่ได้มาในขณะที่ดำเนินการนั้น โดยมิให้มีการเปลี่ยนแปลงหรือแก้ไขโดยง่าย[151]

ในกรณีที่ข้อมูลข่าวสารที่ได้มาโดยการดักฟังทางโทรศัพท์หรือการดักข้อมูลทางคอมพิวเตอร์นั้นเป็นถ้อยคำหรือเสียงของบุคคล หรือการสนทนาระหว่างบุคคลให้พนักงานสอบสวนคดีพิเศษที่ได้รับมอบหมายจากหัวหน้าคณะพนักงานสอบสวนคดีพิเศษ จัดทำบันทึกถ้อยคำเป็นลายลักษณ์อักษรหรือบันทึกเสียงหรือการสนทนาด้วยเครื่องมือทางเทคโนโลยีแล้วแต่กรณี หากถ้อยคำ เสียง หรือการสนทนาดังกล่าวเป็นภาษาต่างประเทศ หรือรหัสที่จำเป็นต้องแปลความหมาย ให้หัวหน้าคณะพนักงานสอบสวนคดีพิเศษมอบหมายเจ้าหน้าที่ที่มีความเชี่ยวชาญหรือผู้เชี่ยวชาญดำเนินการแปลความหมายนั้นไว้ด้วย ทั้งนี้ การบันทึกข้อมูลข่าวสารที่ได้มาต้องมีรายละเอียดเกี่ยวกับวัน เดือน ปี และเวลาในการบันทึกพร้อมทั้งลงลายมือชื่อผู้บันทึก ผู้แปล ล่าม และผู้ถอดรหัสด้วย หลังจากนั้นหัวหน้าคณะพนักงานสอบสวนคดีพิเศษต้องจัดทำรายงานบันทึกข้อมูลข่าวสารเกี่ยวกับข้อเท็จจริงหรือพฤติการณ์ของบุคคลที่ประมวลได้จากสิ่งที่บันทึกข้อมูลข่าวสารที่ได้มาและบันทึกถ้อยคำดังกล่าว เสนอผู้บังคับบัญชาตามลำดับชั้นต่อไป

---

[151] ข้อบังคับ กคพ.ว่าด้วยการเก็บรักษา การใช้ประโยชน์ข้อมูลข่าวสารที่ได้มาและการทำลายข้อมูลข่าวสารอื่น พ.ศ. 2547.

พนักงานสอบสวนคดีพิเศษที่ได้รับมอบหมายจากหัวหน้าคณะพนักงานสอบสวนคดีพิเศษ ต้องส่งรายงานบันทึกข้อมูลข่าวสารที่ได้มาและสิ่งที่บันทึกข้อมูลข่าวสาร บันทึกถ้อยคำที่ทำเป็นลายลักษณ์อักษร ต่ออธิบดีผู้พิพากษาศาลอาญาโดยเร็ว ทั้งนี้ต้องไม่เกินเจ็ดวันนับแต่วันที่ดำเนินการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์เสร็จสิ้น โดยต้องมีการปิดผนึกประทับตราและลงลายมือชื่อกำกับไว้ด้วย

เมื่อคณะพนักงานสอบสวนคดีพิเศษได้ดำเนินการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์จนเสร็จสิ้นกระบวนการดังกล่าวแล้ว ข้อมูลการสนทนาหรือข้อมูลที่ถูกส่งทางคอมพิวเตอร์ที่บันทึกได้ตลอดจนถึงข้อมูลอื่นใดที่ได้มาด้วยการใช้มาตรการดังกล่าวนั้นหัวหน้าคณะพนักงานสอบสวนคดีพิเศษจะต้องนำส่งให้แก่ผู้อำนวยการสำนัก (ผู้บัญชาการสำนักคดี (เดิม)) ที่รับผิดชอบคดีพิเศษนั้นๆ หรือพนักงานสอบสวนคดีพิเศษที่ผู้อำนวยการสำนักรับผิดชอบคดีพิเศษนั้นๆ มอบหมาย เป็นผู้ตรวจสอบและเก็บรักษาเทปหรือเครื่องมือที่ใช้บันทึกข้อมูลตลอดจนถึงข้อมูลอื่นใดที่ได้มาในระหว่างการดำเนินคดีและคดียังไม่ถึงที่สุด เมื่อคดีพิเศษดังกล่าวถึงที่สุดแล้ว ผู้อำนวยการสำนักคดีที่รับผิดชอบต้องส่งมอบให้สำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ ซึ่งมีอำนาจหน้าที่ในการดำเนินการจัดเก็บ การประมวลผล และการใช้ประโยชน์ข้อมูลหรืออุปกรณ์ของกรมสอบสวนคดีพิเศษ[152] เป็นผู้เก็บรักษาข้อมูลข่าวสารที่ได้มาจากการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์

การใช้ประโยชน์ข้อมูลข่าวสารที่ได้มาจากการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ พนักงานสอบสวนคดีพิเศษต้องกระทำด้วยความระมัดระวังเป็นอย่างยิ่ง โดยให้คำนึงถึงความจำเป็นเพื่อประสิทธิภาพในการรักษาความสงบเรียบร้อยและสิทธิเสรีภาพของประชาชนประกอบกันเป็นสำคัญ คำขอใช้ประโยชน์จากเอกสารหรือข้อมูลข่าวสารที่ได้มาโดยการเข้าถึงข้อมูลตามมาตรา 25 ต้องประกอบด้วย

1) ชื่อและสถานที่ตั้งส่วนราชการหรือหน่วยงานที่ต้องการขอใช้ประโยชน์
2) วัน เดือน ปี ที่ขอใช้ประโยชน์ข้อมูล
3) ระบุวัตถุประสงค์ เหตุผลและความจำเป็นในการขอใช้ประโยชน์
4) ระบุประเภทและลักษณะข้อมูลข่าวสารหรือเอกสารที่ต้องการขอใช้ประโยชน์
5) ระยะเวลาที่จะใช้ประโยชน์
6) ลายมือชื่อ ตำแหน่ง ผู้ขอใช้ประโยชน์

---

[152] กฎกระทรวงแบ่งส่วนราชการกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม พ.ศ. 2545 ข้อ 2.

ในกรณีที่ข้อมูลข่าวสารที่ได้มาเป็นข้อมูลข่าวสารที่ไม่ได้ใช้ประโยชน์ในการสืบสวนหรือไม่ได้ใช้เป็นพยานหลักฐานในการดำเนินคดีพิเศษ ให้หัวหน้าคณะพนักงานสอบสวนคดีพิเศษคดีนั้นๆ รายงานเสนออธิบดีกรมสอบสวนคดีพิเศษหรือผู้อำนวยการสำนักคดีที่อธิบดีมอบหมายเพื่อมีคำสั่งให้ทำลายข้อมูลข่าวสารดังกล่าวทั้งหมด การทำลายข้อมูลข่าวสารที่ได้มาจากการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ อธิบดีกรมสอบสวนคดีพิเศษจะแต่งตั้งคณะกรรมการทำลายข้อมูล โดยจะแต่งตั้งจากพนักงานสอบสวนคดีพิเศษในตำแหน่งระดับ 8 หรือระดับชำนาญการขึ้นไป จำนวนสามคน เพื่อทำลายข้อมูลข่าวสาร ตามหลักเกณฑ์ วิธีการและเงื่อนไขที่อธิบดีกำหนด ทั้งนี้คณะกรรมการทำลายข้อมูลเมื่อดำเนินการเสร็จสิ้นแล้ว ต้องทำบันทึกรายงานอธิบดีเพื่อทราบด้วย

4.1.6 บทลงโทษตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 เกี่ยวกับการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์โดยมิชอบ

พระราชบัญญัติการสอบสวนคดีพิเศษเป็นบทบัญญัติที่ห้ามมิให้บุคคลใดเปิดเผยข้อมูลข่าวสารที่ได้มาเนื่องจากการดำเนินการดักฟังตามมาตรา 25 เว้นแต่เป็นข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษ ซึ่งได้รับอนุญาตแล้ว หรือเป็นการปฏิบัติตามอำนาจหน้าที่หรือตามกฎหมายหรือตามคำสั่งศาล[153] หากผู้ใดฝ่าฝืนต้องระวางโทษจำคุกตั้งแต่สามปีถึงห้าปี หรือปรับตั้งแต่หกหมื่นบาทถึงหนึ่งแสนบาทหรือทั้งจำทั้งปรับและหากผู้ฝ่าฝืนเป็นพนักงานสอบสวนคดีพิเศษ เจ้าหน้าที่คดีพิเศษ พนักงานอัยการที่เข้าร่วมสอบสวนหรือเข้าร่วมปฏิบัติหน้าที่หรือผู้เข้าร่วมปฏิบัติหน้าที่ตามมาตรา 25 ผู้กระทำต้องระวางโทษเป็นสามเท่าของโทษที่กำหนดไว้[154]

4.1.7 ความเหมาะสมของการนำหลักการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาปรับใช้กับประมวลกฎหมายวิธีพิจารณาความอาญาของไทย

ดังที่กล่าวมาแล้วข้างต้น พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 นั้นได้กำหนดอำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ไว้ ซึ่งจะทำให้เจ้าพนักงานในคดีพิเศษนั้นสามารถเข้าถึงพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ได้ โดยการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ถือว่าเป็นการล่วงล้ำสิทธิเสรีภาพของประชาชนตามรัฐธรรมนูญ ด้วยเหตุนี้พระราชบัญญัตินี้จึงมีบทบัญญัติที่กำหนดให้มีการตรวจสอบ กลั่นกรองถ่วงดุล อำนาจดังกล่าวด้วย ซึ่งถือว่าเป็นการตั้งกรอบขอบเขตอำนาจแก่เจ้าพนักงานในคดีพิเศษไม่ให้ก้าวล้ำไปถึงสิทธิแสรีภาพของประชาชนจนเกินไปทำให้พระราชบัญญัตินี้มีความสมบูรณ์

---

[153] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547, มาตรา 26.

[154] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547, มาตรา 39.

อยู่เลยทีเดียว แต่อย่างไรก็ตามขอบเขตอำนาจที่จะทำให้เจ้าพนักงานสามารถใช้อำนาจในการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์นั้นก็อยู่ในกรอบของฐานความผิดที่เป็นคดีพิเศษเท่านั้น แต่ไม่มีผลกับคดีอาญาบางคดีที่มีความสำคัญไม่น้อยกว่าเช่นกัน ซึ่งหากนำบทบัญญัติดังกล่าวมาบัญญัติลงในประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งถือว่าเป็นกฎหมายแม่บท ก็จะทำให้อำนาจดังกล่าวครอบคลุมทุกฐานความผิดไม่เฉพาะแต่คดีพิเศษเพียงอย่างเดียว

แต่ทั้งนี้ถ้าพิจารณาถึงในแง่ของสิทธิเสรีภาพของประชาชนนั้น การกำหนดให้มีอำนาจดักฟังทางโทรศัพท์และการได้มาซึ่งอิเล็กทรอนิกส์ที่กว้างขึ้นนี้ก็อาจไปกระทบสิทธิเสรีภาพของประชาชนตามรัฐธรรมนูญจนเกินไปเพราะรัฐจะออกกฎหมายหรือบังคับใช้กฎหมายที่เป็นการตัดทอนเอกสิทธิหรือความคุ้มกันหรือรอนสิทธิในชีวิตเสรีภาพหรือทรัพย์สินของประชาชนโดยไม่ชอบด้วยกระบวนความแห่งกฎหมายไม่ได้ แต่เมื่อพิจารณาถึงอำนาจรัฐในการรักษาความสงบเรียบร้อยของสังคมแล้วนั้นการกำหนดอำนาจดังกล่าวลงในประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งทำให้อำนาจดังกล่าวกว้างขึ้นจะทำให้สามารถป้องกันและปราบปรามการกระทำผิดของอาชญากรได้อย่างเต็มที่เพราะเจ้าหน้าที่รัฐต้องมีวิธีการใดๆ เพื่อให้ได้มาซึ่งพยานหลักฐานพิสูจน์การกระทำความผิดของอาชญากร และวิธีการค้นหาพยานหลักฐานดังกล่าวซึ่งอาจเป็นการละเมิดสิทธิเสรีภาพบางส่วนของประชาชนได้ รัฐต้องพยายามในการที่จะให้ความคุ้มครองแก่ประชาชนให้มากที่สุดและจำเป็นที่จะต้องใช้อำนาจในการป้องกันและปราบปรามอาชญากรรมอย่างมีประสิทธิภาพ โดยประชาชนเองจำต้องยอมให้รัฐผลักภาระบางประการให้แก่ประชาชนได้และย่อมส่งผลให้สิทธิบางส่วนของประชาชนจะได้รับความคุ้มครองน้อยลงไปด้วย ซึ่งเมื่อพิจารณาทั้งสองแง่ประกอบกับการพิจารณาพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 แล้ว กฎหมายฉบับนี้ก็มีบทบัญญัติที่ช่วยในการตรวจสอบ กลั่นกลอง ถ่วงดุล การใช้อำนาจดังกล่าวไว้ในพระราชบัญญัตินี้ ซึ่งทำให้การใช้อำนาจของรัฐไม่เป็นการละเมิดสิทธิของประชาชนจนเกินไป และหากนำมาบัญญัติในประมวลกฎหมายวิธีพิจารณาความอาญาก็ต้องมีการตรวจสอบ กลั่นกรอง ถ่วงดุล อำนาจดังกล่าวเช่นกันเพียงแต่ผลที่ได้มาก็คือ สามารถป้องกันและปราบปรามอาชญากรรมได้อย่างสมบูรณ์ ผู้เขียนจึงเห็นว่าเหมาะสมที่จะนำหลักการการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์มาบัญญัติลงในประมวลกฎหมายวิธีพิจารณาความอาญาของไทย

4.2 การนำหลักการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ของสหรัฐอเมริกามาปรับใช้กับประมวลกฎหมายวิธีพิจารณาความอาญาของไทย

สำหรับกฎหมายที่เกี่ยวกับการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในสหรัฐอเมริกาก็ได้แก่ การดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ ตามรัฐบัญญัติ The Wiretap Statute (title 3), amended 1986 และ The Pen/Trap Statute, amended 2001 ดังที่เคยกล่าวมาแล้วในบทที่ 3 นั้น ถือว่ากฎหมายดังกล่าวของสหรัฐอเมริกานั้นมีส่วนช่วยในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญาซึ่งจะทำให้เจ้าพนักงานสามารถเข้าถึงพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ได้ โดยรัฐบัญญัติ Title 3 ก็ได้กำหนดไว้ว่าโดยหลักแล้วห้ามไม่ให้มีการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์และรัฐบัญญัตินี้ก็ได้แบ่งสิ่งที่จะดักได้ออกเป็น 2 แบบ คือ การดักการสื่อสารตามสาย (เช่นโทรศัพท์) และการดักการสื่อทางอิเล็กทรอนิกส์ (เช่น จดหมายอิเล็กทรอนิกส์) ซึ่งรัฐบัญญัตินี้ก็มีข้อยกเว้นที่จะให้เจ้าพนักงานมีอำนาจในการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ได้โดยบทบัญญัตินี้ก็จะมีข้อยกเว้นต่างๆ อาทิเช่น

(1) การดักตามคำสั่งศาล ตามมาตรา 2518 ซึ่งกำหนดให้เจ้าพนักงานตามกฎหมายสามารถดักการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์โดยคำสั่งศาล โดยคำร้องในกรณีการดักการสื่อสารตามสายจะต้องได้รับอนุมัติจากเจ้าหน้าระดับสูงของกระทรวงยุติธรรม และในกรณีการสื่อสารทางอิเล็กทรอนิกส์ก็ต้องได้รับการอนุมัติจากผู้กำหนดนโยบายของกระทรวงยุติธรรมเมื่อได้รับอนุมัติและผู้พิพากษาศาลประจำเขตหรือศาลอุทธรณ์ได้ลงนามในคำสั่งให้ดักการสื่อสารตามสายและการสื่อสารทางอิเล็กทรอนิกส์แล้วเจ้าหน้าที่ผู้บังคับใช้กฎหมายก็สามารถดักการสื่อสารได้นานถึง 30 วัน และคำร้องดังกล่าวต้องแสดงถึงเหตุอันควรเชื่อว่าการดักจะทำให้ได้พยานหลักฐานการกระทำที่เป็นความอาญาร้ายแรงตามบัญชีที่ปรากฏในมาตรา 2516 ด้วย

(2) ข้อยกเว้นเรื่อง “ความยินยอม” ตามมาตรา 2511 (2) (c)-(d) ในส่วนของเรื่องความยินยอมนั้นถ้าหากผู้ที่ทำการสื่อสารตามสาย วาจา หรือทางอิเล็กทรอนิกส์ทั้งสองฝ่ายหรือฝ่ายใดฝ่ายหนึ่งได้ให้ความยินยอมในการดักนั้นไว้ล่วงหน้า การดักการสื่อสารดังกล่าวจะไม่มีความผิดหากไม่ได้ดักการสื่อสารเพื่อกระทำผิดใดๆ หรือละเมิดบทบัญญัติรัฐธรรมนูญ หรือกฎหมายของสหรัฐหรือมลรัฐใดๆ

(3) ข้อยกเว้นเรื่อง “ผู้ให้บริการ” ตามมาตรา 2511 (2) (a) (i) ข้อยกเว้นนี้จะกำหนดให้ลูกจ้างหรือเจ้าหน้าที่ของผู้ให้บริการการสื่อสารอาจดักและเปิดเผยการสื่อสารเพื่อคุ้มครองสิทธิของผู้ให้บริการ ตัวอย่างเช่นโดยทั่วไปแล้วผู้บริหารระบบโครงข่ายคอมพิวเตอร์อาจจับตาการบุกรุกโครงข่ายของแฮ็กเกอร์ และเปิดเผยผลของการจับตาแก่เจ้าหน้าที่ผู้บังคับใช้กฎหมายโดยไม่

เป็นการละเมิดต่อ Title 3 อย่างไรก็ตามข้อยกเว้นนี้จะเป็นเรื่องของผู้ให้บริการเท่านั้นและไม่รวมถึงเจ้าหน้าที่ผู้บังคับใช้กฎหมาย

(4) ข้อยกเว้นเรื่อง “ผู้บุกรุกทางคอมพิวเตอร์” ตามมาตรา 2511 (2) (i) ที่ยอมให้ผู้เสียหายที่ถูกโจมตีทางคอมพิวเตอร์ ที่จะอนุญาตให้เจ้าหน้าที่ผู้บังคับใช้กฎหมายดักการสื่อสารตามสายหรือทางอิเล็กทรอนิกส์ เจ้าหน้าที่ผู้บังคับใช้กฎหมายอาจดักการสื่อสารของผู้บุกรุกทางคอมพิวเตอร์ ที่ส่งไปยัง ผ่าน หรือจากคอมพิวเตอร์ที่มีการคุ้มครอง

(5) ข้อยกเว้นเรื่อง “โทรศัพท์พ่วง” ตามมาตรา 2510 (5) (a) โดยการใช้อุปกรณ์หรือเครื่องมือโทรศัพท์หรือโทรเลขหรือส่วนใดๆ ของโทรศัพท์หรือโทรเลขจะไม่ถือว่าเป็นการละเมิด Title 3 หากเข้าข้อยกเว้นตามมาตราดังกล่าว

(6) ข้อยกเว้นเรื่อง “การได้พยานหลักฐานในคดีอาญามาโดยบังเอิญ” ตามมาตรา 2511 (3) (b) (iv) ซึ่งยอมให้ผู้ให้บริการเปิดเผยเนื้อหาการติดต่อสื่อสารใดๆ ที่ผู้ให้บริการได้มาโดยไม่ตั้งใจอันเป็นเรื่องเกี่ยวกับการกระทำผิดทางอาญาแก่เจ้าหน้าที่ผู้บังคับใช้กฎหมาย

(7) ข้อยกเว้นเรื่อง “การเข้าถึงสาธารณชน” ตามมาตรา 2511 (2) (g) (i) ซึ่งยอมให้บุคคลใดๆ ดักการสื่อสารทางอิเล็กทรอนิกส์ที่ได้กระทำผ่านระบบ ซึ่งมีการเก็บไว้เพื่อให้สาธารณชนทั่วไปสามารถเข้าถึงโดยง่าย

จึงเห็นได้ว่าโดยหลักแล้วตามกฎหมายของสหรัฐอเมริกา กฎหมายของสหรัฐอเมริกาก็ได้ห้ามการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์แต่ก็มีข้อยกเว้นให้กระทำได้ดังกล่าวข้างต้น ทำให้กำหนดขอบเขตในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ที่ไม่เป็นการเลื่อมล้ำสิทธิ เสรีภาพของประชาชนจนมากเกินสมควรแต่ยังคงไว้ซึ่งการป้องกันและปราบปรามอาชญากรรมในสังคมให้หมดไป

ส่วนรัฐบัญญัติ The Pen/Trap Statute, amended 2001 นี้รัฐบัญญัติต้องใช้ควบคู่กับ Title 3 ซึ่งรัฐบัญญัตินี้ได้กำหนดรูปแบบการเข้าไปของรัฐที่ล่วงล้ำน้อยกว่าในรัฐบัญญัติ The Wiretap Statute กฎหมายนี้ให้อำนาจในการติดตั้งระบบการตรวจสอบการใช้งานโทรศัพท์ทั้งเข้าและออก (Pen Register และ Trap and Trace (Pen/Trap)) โดย Pen Register จะบันทึกการหมุนโทรศัพท์ เส้นทาง และแสดงข้อมูลที่เกี่ยวกับการสื่อสารอิเล็กทรอนิกส์ที่ออกไป (Outgoing) การสื่อสารอิเล็กทรอนิกส์หมายถึง โทรศัพท์ คอมพิวเตอร์ โทรเลข โทรพิมพ์ ส่วน Trap and Trace จะบันทึกข้อมูลเช่นเดียวกันแต่เป็นการสื่อสารที่เข้ามา (Incoming) แต่ข้อเท็จจริงที่สำคัญคือทั้งสองแบบจะไม่บันทึกเนื้อหาของการสื่อสาร เพียงแต่บันทึกข้อมูลที่เกี่ยวกับเบอร์โทรศัพท์ทั้งที่เป็นการเรียกออกและเรียกเข้า

การละเมิดบทบัญญัติดังกล่าว ทำให้เจ้าหน้าที่และพนักงานอัยการจะต้องรับผิดในทางแพ่งและทางอาญาและพยานหลักฐานที่ได้มาก็ห้ามรับฟัง ซึ่งการเยียวยาโดยไม่รับฟังพยานหลักฐานนั้น Title 3 ได้วางหลักเกณฑ์การไม่รับฟังพยานหลักฐานที่เกิดขึ้นจากการดักการสื่อสารด้วยวาจาและการสื่อสารตามสายที่ได้มาโดยไม่ชอบ แต่ไม่รวมถึงกรณีการสื่อสารทางอิเล็กทรอนิกส์ที่รัฐบัญญัติ Pen/Trap ไม่ได้วางหลักเกณฑ์เรื่องการเยียวยาโดยห้ามไม่ให้รับฟังพยานหลักฐานไว้นอกจากนี้การละเมิดรัฐธรรมนูญอาจจะมีผลให้มีการไม่รับฟังพยานหลักฐานที่ได้มาโดยไม่ชอบเช่นกัน การละเมิดบทบัญญัติดังกล่าว ทำให้เจ้าหน้าที่และพนักงานอัยการจะต้องรับผิดในทางแพ่งและทางอาญาและพยานหลักฐานที่ได้มาก็ห้ามรับฟัง

เมื่อพิจารณาถึงรัฐบัญญัติ Title 3 ก็เห็นว่ามีข้อดีอยู่หลายประการ การนำบทบัญญัติบางส่วนของรัฐบัญญัติดังกล่าวของสหรัฐอเมริกามาใช้กับประมวลกฎหมายวิธีพิจารณาความอาญาของไทยนั้น หากพิจารณาถึงเรื่องการคุ้มครองสิทธิเสรีภาพของประชาชนก็จะเห็นได้ว่ากฎหมายของสหรัฐของอเมริกาได้ห้ามการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์โดยสิ้นเชิง แต่ก็กำหนดกรอบข้อยกเว้นไว้หลายประการซึ่งสามารถกระทำได้ หากเป็นกรณีที่มีเหตุสมควรจริงๆ ซึ่งทำให้ประชาชนไม่ถูกล่วงล้ำสิทธิเสรีภาพจนเกินไปแม้ว่าข้อยกเว้นดังกล่าวจะมีอยู่หลายประการแต่ก็อยู่บนฐานของความเหมาะสมในการที่จะอนุญาตให้กระทำการดังกล่าวได้ และเมื่อพิจารณาถึงเรื่องถึงอำนาจรัฐในการรักษาความสงบเรียบร้อยของสังคมการกำหนดให้มีข้อยกเว้นให้มากยิ่งขึ้นก็จะทำให้สามารถป้องกันและปราบปรามอาชญากรรมได้ดียิ่งขึ้นเพราะหากมีข้อยกเว้นให้ทำการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์มากขึ้นก็จะทำให้ได้พยานหลักฐานที่เกี่ยวข้องกับการกระทำผิดทางอาญาได้มากยิ่งขึ้นซึ่งจะสามารถมัดตัวผู้กระทำผิดให้ได้รับโทษทางอาญา ซึ่งการกำหนดข้อยกเว้นดังกล่าวก็ถือว่าเป็นการกลั่นกรองตรวจสอบและถ่วงดุลการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์เช่นกัน นอกจากนี้การกำหนดให้มีการลงโทษทางแพ่งและอาญาแก่เจ้าหน้าที่และพนักงานอัยการในกรณีที่มีการละเมิดรัฐบัญญัติดังกล่าวนี้ก็ถือว่าเป็นการกลั่นกรอง ตรวจสอบและถ่วงดุลเช่นกัน ผู้เขียนจึงเห็นว่าเหมาะสมที่จะนำข้อยกเว้นของรัฐบัญญัติดังกล่าวมาใช้ในประมวลกฎหมายวิธีพิจารณาของไทยด้วย

รัฐบัญญัติ The Pen/Trap Statute, amended 2001 นี้เมื่อพิจารณาแล้วก็พบว่ามีส่วนช่วยในการค้นหาตัวผู้กระทำผิดและแหล่งที่มาของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ด้วย ทั้งเมื่อพิจารณาถึงการคุ้มครองสิทธิและเสรีภาพของประชาชน การนำรัฐบัญญัตินี้มาใช้ในประมวลกฎหมายวิธีพิจารณาของไทยก็ไม่ทำให้ละเมิดสิทธิและเสรีภาพของประชาชนจนเกินไป เพราะโดยลักษณะของบทบัญญัติดังกล่าว ก็เป็นการให้อำนาจเจ้าพนักงานผู้บังคับใช้กฎหมายใน

การเพื่อให้ได้มาซึ่งข้อมูลที่เป็นสารสนเทศประเภทที่อยู่ที่ส่งเข้ามาหรือออกไปเท่านั้น จึงไม่เกี่ยวข้องกับส่วนที่เป็นเนื้อหาของข้อมูลดังกล่าวทำให้ไม่เป็นการละเมิดสิทธิส่วนบุคคลจนเกินไปและหากพิจารณาถึงอำนาจรัฐในการรักษาความสงบเรียบร้อยของสังคมแล้ว การนำรัฐบัญญัตินี้มาใช้กับประมวลกฎหมายวิธีพิจารณาความอาญาของไทยก็จะทำให้สามารถป้องกันและปราบปรามอาชญากรรมได้อย่างดีเพราะสามารถระบุแหล่งที่มาของพยานหลักฐานดังกล่าวเพื่อมัดตัวผู้กระทำผิดไม่ให้ปฏิเสธว่าไม่ใช่เจ้าของของข้อมูลดังกล่าว ทั้งอาจใช้ในการติดตามตัวผู้กระทำผิดมาลงโทษได้ จึงเห็นว่าน่าจะเหมาะสมที่จะนำมาใช้ประมวลกฎหมายวิธีพิจารณาความอาญาของไทย

4.3 การกำหนดฐานความผิดที่จะใช้ในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญา

การกำหนดฐานความผิดสำหรับการใช้อำนาจในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ในคดีอาญานั้นจากการศึกษากฎหมายที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ของประเทศสหรัฐอเมริกา ในประเทศสหรัฐอเมริกาได้บัญญัติประเภทความผิดที่อนุญาตให้มีการดักฟังทางโทรศัพท์และการเข้าถึงข้อมูลทางอิเล็กทรอนิกส์ไว้ในมาตรา 2516 (1) (a)-(n) ของ Omnibus Crime Control and Safe Street Act 1968 ดังที่กล่าวมาแล้วในบทที่ 3 (อาทิเช่น ความผิดเกี่ยวกับการก่อวินาศกรรม การก่อกบฏ การก่อจลาจล โจรสลัด การปล้นและกรรโชก การให้สินบนเจ้าพนักงานและพยาน เป็นต้น) ซึ่งลักษณะของความผิดทางอาญาที่จะสามารถดักการสื่อสารทางอิเล็กทรอนิกส์เพื่อประโยชน์ในการสืบสวนสอบสวนและป้องกันอาชญากรรมจะทำได้ในกรณีของความผิดอาญาร้ายแรงทุกประเภท ทั้งนี้เพื่อมิให้เป็นการละเมิดสิทธิเสรีภาพของประชาชนจนเกินไปจึงจำเป็นต้องกำหนดอำนาจดังกล่าวเฉพาะความผิดที่มีความสำคัญจริงๆ โดยจะต้องเป็นความผิดอาญาที่ร้ายแรงเท่านั้น ดังนั้นการใช้มาตรการในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ อันเป็นมาตรการที่กระทบถึงสิทธิเสรีภาพของประชาชน การจำกัดอำนาจดังกล่าวจึงจำเป็นต้องกระทำโดยเคร่งครัด

อย่างไรก็ตามการกำหนดว่าความผิดอาญาฐานใดเป็นความผิดอาญาที่ร้ายแรงนั้นจะต้องดูจากโทษที่จะลงแก่ผู้กระทำผิดในความผิดอาญาฐานต่างๆ ซึ่งประมวลกฎหมายวิธีพิจารณาความอาญา ก็ไม่ได้บัญญัติไว้ชัดเจนว่าความผิดอาญาที่มีโทษเท่าใดจะเป็นความผิดอาญาร้ายแรง ซึ่งจะพบว่า ประมวลกฎหมายวิธีพิจารณาความอาญา ก็ได้มีการบัญญัติอัตราโทษที่จะใช้มาตรการแสวงหาพยานหลักฐานในคดีอาญาโดยทั่วไปไว้ อาทิเช่น ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 66 (1) ในเรื่องเหตุแห่งการออกหมายจับที่จะต้องมีหลักฐานตามสมควรว่าบุคคลใดน่าจะได้กระทำผิดอาญาซึ่งมีอัตราโทษจำคุกอย่างสูงเกินสามปี ซึ่งจะเห็นได้ว่า ประมวลกฎหมายวิธี

พิจารณาความอาญา มาตรา 66 (1) มีเจตนารมณ์ในการคุ้มครองสิทธิเสรีภาพของบุคคลโดยกำหนดให้เหตุของการออกหมายจับในการที่จะจับบุคคลใด จะต้องมีหลักฐานพอสมควรว่าบุคคลใดน่าจะได้กระทำความผิดอาญา โดยมุ่งไปที่ความผิดอาญาที่มีโทษจำคุกอย่างสูงเกิน 3 ปี การกำหนดโทษเช่นนี้จะหมายถึงความผิดอาญาที่มีโทษจำคุกอย่างสูงเกิน 3 ปี เป็นความผิดอาญาร้ายแรงหรือไม่ ผู้เขียนเห็นว่าเรื่องดังกล่าวเป็นเพียงการแสวงหาพยานหลักฐานโดยทั่วไปไม่ใช่มาตรการพิเศษในการแสวงหาพยานหลักฐาน โดยในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์จะต้องใช้มาตรการพิเศษในการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ที่กระทบต่อสิทธิเสรีภาพของบุคคล การกำหนดโทษดังกล่าวจึงน้อยเกินไป

นอกจากนี้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 176 ได้บัญญัติไว้ว่า

“ในชั้นพิจารณา ถ้าจำเลยให้การรับสารภาพตามฟ้อง ศาลจะพิพากษาโดยไม่สืบพยานหลักฐานต่อไปก็ได้ เว้นแต่คดีที่มีข้อหาในความผิดซึ่งจำเลยรับสารภาพนั้น กฎหมายกำหนดอัตราโทษอย่างต่ำไว้ให้จำคุกตั้งแต่ห้าปีขึ้นไปหรือโทษสถานที่หนักกว่านั้น ศาลต้องฟังพยานโจทก์จนกว่าจะพอใจว่าจำเลยได้กระทำผิดจริง”

เจตนารมณ์ของมาตรานี้ เห็นว่ากฎหมายได้ให้ประโยชน์แก่จำเลยที่รับสารภาพโดยบัญญัติให้ศาลจะต้องรับฟังพยานหลักฐานของโจทย์จนกว่าจะพอใจว่าจำเลยกระทำผิดจริงหากจำเลยรับสารภาพ ซึ่งความผิดนั้นต้องเป็นความผิดที่มีโทษอย่างต่ำให้จำคุกตั้งแต่ห้าปีขึ้นไปหรือโทษหนักกว่านั้น การกำหนดโทษเช่นนี้จะเป็นความผิดอาญาร้ายแรงหรือไม่ เห็นว่าการกำหนดโทษดังกล่าว เป็นเพียงการกำหนดอัตราโทษ ที่จะใช้ประกอบในกระบวนการพิจารณาในชั้นศาลเท่านั้น ซึ่งไม่เกี่ยวข้องกับการใช้มาตรการแสวงหาพยานหลักฐานในคดีอาญาซึ่งเป็นขั้นตอนก่อนที่จะถึงชั้นศาล

อย่างไรก็ตามปัจจุบันประเทศไทยได้ลงนามในอนุสัญญาสหประชาชาติเพื่อการต่อต้านอาชญากรรมข้ามชาติที่ก่อตั้งในลักษณะองค์กร ค.ศ. 2000 (United Nations Convention Against Transnational Organized Crime 2000)[155] เมื่อวันที่ 13 ธันวาคม 2543 ซึ่งได้มีการแก้ไขปรับปรุงกฎหมายที่มีอยู่หรือร่างกฎหมายใหม่เพื่ออนุวัติการตามอนุสัญญาฯ ดังกล่าวและคณะรัฐมนตรีได้มีมติเมื่อวันที่ 26 กันยายน 2543 ให้สำนักงานอัยการสูงสุดเป็นหน่วยงานหลัก เพื่อแก้ไขกฎหมายที่มีอยู่หรือยกร่างขึ้นใหม่รองรับพันธกรณีตามอนุสัญญาฯ โดยสำนักงานอัยการสูงสุดได้ดำเนินการยกร่างพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. .... ไว้ เพื่ออนุวัติการตามอนุสัญญา ฯ และคณะรัฐมนตรีได้มีมติให้เสนอร่างพระราชบัญญัติ

---

[155] United Nations Convention Against Transnational Organized Crime 2000 Article 2 (b).

ดังกล่าวต่อสภาผู้แทนราษฎร[156] ซึ่งต่อมาพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 ก็ได้ประกาศในราชกิจจานุเบกษา เล่ม 130 ตอนที่ 55 ก ลงวันที่ 26 มิถุนายน 2556

หลังจากที่พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 ได้ประกาศในราชกิจจานุเบกษาแล้ว ประเทศไทยได้เข้าเป็นภาคีอนุสัญญาสหประชาชาติเพื่อการต่อต้านอาชญากรรมข้ามชาติที่ก่อตั้งในลักษณะองค์กร ค.ศ. 2000 ซึ่งพระเจ้าหลานเธอ พระองค์เจ้าพัชรกิติยาภา เอกอัครราชทูตผู้แทนถาวรแห่งประเทศไทยประจำสหประชาชาติ ณ กรุงเวียนนา ทรงเป็นผู้แทนรัฐบาลไทยในการยื่นสัตยาบันอนุสัญญาดังกล่าวต่อผู้แทนเลขาธิการสหประชาชาติ ณ นครนิวยอร์ก เมื่อวันที่ 17 ตุลาคม 2556 โดยการยื่นสัตยาบันจะส่งผลให้อนุสัญญา ฯ ดังกล่าว มีผลบังคับใช้กับประเทศไทยในวันที่ 16 พฤศจิกายน 2556 เป็นต้นไป[157]

โดยเนื้อหาของพระราชบัญญัตินี้ ได้ให้ความหมายของ “ความผิดอาญาที่ร้ายแรง” เพื่อให้สอดคล้องกับบทนิยามคำว่า “Serious Crime” ตาม Article 2 (b) ของอนุสัญญาฯ โดยที่อนุสัญญาฯ ได้ให้ความหมายของความผิดอาญาร้ายแรงดังนี้

ความผิดอาญาที่ร้ายแรง (Serious Crime) หมายถึงการกระทำความผิดทางอาญาร้ายแรงที่สามารถลงโทษจำคุกบุคคลนั้นตั้งแต่สี่ปีขึ้นไปจนถึงประหารชีวิต

พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 ก็ได้บัญญัติให้ สอดคล้องกับอนุสัญญาฯ ดังกล่าวโดยกำหนดความหมายของ “ความผิดร้ายแรง” ให้หมายความว่า ความผิดอาญาที่กฎหมายกำหนดโทษจำคุกขั้นสูงตั้งแต่สี่ปีขึ้นไปหรือโทษสถานหนักกว่านั้น

จึงเห็นได้ว่าพระราชบัญญัติฯ และอนุสัญญาฯ ดังกล่าวได้กำหนดความผิดอาญาอาญาที่ร้ายแรงไว้ โดยความผิดอาญาร้ายแรงตามอนุสัญญาฯ ให้ถือว่าเป็นการกระทำความผิดทางอาญาร้ายแรงที่สามารถลงโทษจำคุกบุคคลนั้นตั้งแต่สี่ปีขึ้นไปจนถึงประหารชีวิต และความผิดอาญาที่ร้ายแรงตามพระราชบัญญัติฯ ก็ให้ถือว่าเป็นความผิดอาญาที่กฎหมายกำหนดโทษจำคุกขั้นสูงตั้งแต่สี่ปีขึ้นไปหรือโทษสถานหนักกว่านั้น ซึ่งผู้เขียนเห็นว่าการกำหนดความผิดอาญาร้ายแรงในคดีอาญาของไทยในเมื่อเราได้เข้าลงนามในอนุสัญญาฯ และได้ให้สัตยาบันแก่อนุสัญญาฯ

---

[156] สำนักงานคณะกรรมการกฤษฎีกา. (2555). *บันทึกวิเคราะห์สรุปสาระสำคัญของร่างพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. .... เรื่องเสร็จที่ 614/2555.*

[157] General information from Ministry of Foreign Affairs of The Kingdom of Thailand. 2013, from *http://www.mfa.go.th/main/th/media-center/14/*

ดังกล่าว ประกอบกับพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มีผลบังคับใช้แล้ว การกำหนดความหมายของความผิดอาญาร้ายแรงก็ควรยึดถือตามอนุสัญญาฯ ดังกล่าว

ดังนั้นการกำหนดฐานความผิดทางอาญาที่จะให้อำนาจเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญาในการดักการสื่อสารทางอิเล็กทรอนิกส์จะต้องเป็นความผิดอาญาตามประมวลกฎหมายอาญาที่มีจำคุกขั้นสูงตั้งแต่สี่ปีขึ้นไปหรือโทษสถานหนักกว่านั้น ยกตัวอย่างเช่น

(1) ลักษณะ1 ความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร

1. หมวด 1 ความผิดต่อองค์พระมหากษัตริย์ พระราชินี รัชทายาท และผู้สำเร็จราชการแทนพระองค์ (มาตรา 107-111)

2. หมวด 2 ความผิดต่อความมั่นคงของรัฐภายในราชอาณาจักร (มาตรา 113-117 วรรคแรก)

3. หมวด 3 ความผิดต่อความมั่นคงของรัฐภายนอกราชอาณาจักร (มาตรา 120, 122-129)

4. หมวด 4 ความผิดต่อสัมพันธไมตรีกับต่างประเทศ (มาตรา 130-134)

(2) ลักษณะ 1/1 ความผิดเกี่ยวกับการก่อการร้าย (มาตรา 135/1-135/4)

(3) ลักษณะ 2 ความผิดเกี่ยวกับการปกครอง

1. หมวด 1 ความผิดต่อเจ้าพนักงาน (มาตรา 139-140, 143-144)

2. หมวด 2 ความผิดต่อตำแหน่ง หน้าที่ราชการ (มาตรา 147-164, 166)

(4) ลักษณะ 3 ความผิดเกี่ยวกับการยุติธรรม

1. หมวด 1 ความผิดต่อเจ้าพนักงานในการยุติธรรม (มาตรา 167, 184-185, 188, 191)

2. หมวด 2 ความผิดต่อตำแหน่งหน้าที่ในการยุติธรรม (มาตรา 200-202, 204)

(5) ลักษณะ 5 ความผิดเกี่ยวกับความสงบสุขของประชาชน (มาตรา 209-213)

(6) ลักษณะ 6 ความผิดเกี่ยวกับการก่อให้เกิดภยันตรายต่อประชาชน (มาตรา 217-222, 224-232, 234, 236-238)

(7) ลักษณะ 7 ความผิดเกี่ยวกับการปลอมและการแปลง

1. หมวด 1 ความผิดเกี่ยวกับเงินตรา (มาตรา 240-248)

2. หมวด 2 ความผิดเกี่ยวกับดวงตราแสตมป์และตั๋ว (มาตรา 250-255, 263)

3. หมวด 3 ความผิดเกี่ยวกับเอกสาร (มาตรา 265-266)

4. หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ (มาตรา 269/1-269/5)

5. หมวด 5 ความผิดเกี่ยวกับหนังสือเดินทาง (มาตรา 269/8-269/15)

(8) ลักษณะ 9 ความผิดเกี่ยวกับเพศ (มาตรา 276-286)

(9) ลักษณะ10 ความผิดเกี่ยวกับชีวิตและร่างกาย

1. หมวด 1 ความผิดต่อชีวิต (มาตรา 288-293)

2. หมวด 2 ความผิดต่อร่างกาย (มาตรา 297-298)

3. หมวด 3 ความผิดฐานทำให้แท้งลูก (มาตรา 302-303)

(10) ลักษณะ11 ความผิดเกี่ยวกับเสรีภาพและชื่อเสียง

1. หมวด 1 ความผิดต่อเสรีภาพ (มาตรา 310ทวิ, 312, 312ทวิ, 312ตรี, 313-320)

(11) ลักษณะ12 ความผิดเกี่ยวกับทรัพย์

1. หมวด 1 ความผิดฐานลักทรัพย์และวิ่งราวทรัพย์ (มาตรา 335-336)

2. หมวด 2 ความผิดฐานกรรโชก รีดเอาทรัพย์ ชิงทรัพย์และปล้นทรัพย์ (มาตรา 337-340ตรี)

3. หมวด 3 ความผิดฐานฉ้อโกง (มาตรา 342-343, 347)

4. หมวด 6 ความผิดฐานรับของโจร (มาตรา 357)

5. หมวด 7 ความผิดฐานทำให้เสียทรัพย์ (มาตรา 360-360ทวิ)

6. หมวด 8 ความผิดฐานบุกรุก (มาตรา 365)

การกำหนดฐานความผิดในคดีอาญาดังกล่าวจะเห็นได้ว่าอำนาจในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ (การดักการสื่อสารทางอิเล็กทรอนิกส์) ของเจ้าพนักงานในคดีอาญานั้นการกำหนดกรอบฐานความผิดให้เป็นเฉพาะคดีอาญาที่ร้ายแรงเท่านั้นจะช่วยให้การแสวงหาพยานหลักฐานดังกล่าวไม่เป็นการละเมิดสิทธิและเสรีภาพของประชาชนจนมากเกินไป แต่อย่างไรก็ตามผู้เขียนเห็นว่าถึงแม้จะกำหนดฐานความผิดไว้ก็ตาม แต่ก็ควรมีการตรวจสอบถ่วงดุลย์และกลั่นกรองอำนาจดังกล่าวด้วยโดยคำนึงถึงลักษณะของความผิดว่ามีความสำคัญมากน้อยเพียงใดพอที่จะสมควรให้มีอำนาจในการดักการสื่อสารทางอิเล็กทรอนิกส์หรือไม่ หากเป็นคดีที่ไม่มีความสำคัญเพียงพอถึงแม้ว่าจะเป็นความผิดที่สามารถมีโทษขั้นสูงเกินสี่ปีขึ้นไปก็ตามก็ไม่สมควรให้มีการดักการสื่อสารทางอิเล็กทรอนิกส์ได้ ซึ่งควรจะมุ่งไปถึงความผิดที่เกี่ยวกับความมั่นคงและความสงบสุขของประชาชนเสียมากกว่า ผู้มีอำนาจในการตรวจสอบถ่วงดุลยหรือกลั่นกรองอำนาจดังกล่าวก็ควรใช้ดุลยพินิจในการให้อำนาจดังกล่าวนั้นด้วยโดยคำนึงถึงสิทธิเสรีภาพของประชาชนเป็นหลัก

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

การแสวงหาพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาไทยในปัจจุบันส่วนใหญ่จะใช้วิธีการแสวงหาพยานหลักฐานด้วยวิธีการ เข้าค้น เพื่อยึดพยานเอกสารหรือพยานวัตถุ จากเคหสถานของบุคคล การใช้วิธีการแสวงหาพยานหลักฐานด้วยวิธีการจับการค้นเพื่อยึดพยานเอกสารหรือพยานวัตถุจากตัวบุคคล การแสวงหาพยานหลักฐานจากร่างกายมนุษย์เท่านั้น ซึ่งยังไม่เพียงพอ เนื่องจากปัจจุบันคอมพิวเตอร์มีส่วนสำคัญในชีวิตประจำวันของมนุษย์ การใช้คอมพิวเตอร์ในการติดต่อสื่อสารถึงกันอาจใช้เป็นสื่อในการติดต่อสื่อสารในการกระทำผิดอาญาร้ายแรงฐานต่างๆ โดยพยานหลักฐานทางคอมพิวเตอร์จำเป็นต้องใช้มาตรการการแสวงหาพยานหลักฐานที่เป็นการใช้มาตรการในการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ ซึ่งประมวลกฎหมายวิธีพิจารณาความอาญาของไทย ก็ไม่ได้ระบุการแสวงหาพยานหลักฐานทางคอมพิวเตอร์โดยวิธีการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์แต่อย่างใด หากไม่มีมาตรการดังกล่าวจะทำให้เจ้าพนักงานเสียโอกาสสำคัญในการที่จะได้มาซึ่งพยานหลักฐานที่จะเอาผิดแก่ผู้กระทำผิดได้ และแม้ว่าประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 226/1 จะเปิดช่องให้รับฟังพยานหลักฐานที่เกิดขึ้นจากการใช้วิธีการแสวงหาพยานหลักฐานที่ไม่มีกฎหมายรองรับไว้โดยเป็นการละเมิดสิทธิส่วนบุคคลก็ตาม ทำให้พยานหลักฐานที่ได้จากการแสวงหาพยานหลักฐานดังกล่าว เป็นพยานหลักฐานที่เกิดขึ้นมาโดยชอบ แต่ได้มาโดยมิชอบที่ศาลอาจรับฟังได้หากพยานหลักฐานนั้นจะเป็นประโยชน์ต่อการอำนวยความยุติธรรมมากกว่าผลเสีย แต่เพื่อเป็นการอำนวยซึ่งความยุติธรรมของกระบวนการยุติธรรมทางอาญา พยานหลักฐานที่ได้มาโดยมิชอบด้วยกฎหมายไม่ว่าโดยประการใดๆ ศาลจะต้องปฏิเสธไม่รับฟัง โดยถือว่าเป็นหลักการตัดพยานหลักฐาน (Exclusionary Rule) ชนิดหนึ่งการรับฟังพยานหลักฐานที่ไม่ชอบด้วยกฎหมายเหมือนกับการยอมรับเอาผลไม้ของต้นไม้ที่มีพิษ ศาลจึงไม่รับฟังพยานหลักฐานที่เป็นผลมาจากการกระทำที่ไม่ชอบด้วยกฎหมาย จึงสมควรมีมาตรการการแสวงหาพยานหลักฐานทางคอมพิวเตอร์โดยการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ เพื่อรองรับไว้ให้กระบวนการยุติธรรมนั้นชอบด้วยกฎหมาย

การแสวงหาพยานหลักฐานทางคอมพิวเตอร์โดยการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ตามกฎหมายของสหรัฐอเมริกาและพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ที่จะทำให้เจ้าพนักงานในคดีอาญาสามารถที่จะเข้าถึงพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ได้นั้น สิ่งแรกที่จะต้องคำนึงถึงในการเข้าถึงพยานหลักฐานดังกล่าวได้นั้น กล่าวคือแนวความคิดในการคุ้มครองสิทธิและเสรีภาพของประชาชนซึ่งรัฐจะออกกฎหมายหรือบังคับใช้กฎหมายที่เป็นการตัดทอนเอกสิทธิหรือความคุ้มกันหรือรอนสิทธิในชีวิตเสรีภาพ หรือทรัพย์สินของประชาชนโดยไม่ชอบด้วยกระบวนความแห่งกฎหมายหรือปฏิเสธไม่ให้ความคุ้มครองแห่งกฎหมายโดยเท่าเทียมกัน ย่อมกระทำไม่ได้ โดยการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ถือว่าเป็นการล่วงล้ำสิทธิ และเสรีภาพในความเป็นส่วนตัวของประชาชนตามรัฐธรรมนูญก็จริงอยู่ แต่ถ้าหากเป็นแนวความคิดเรื่องอำนาจรัฐในการรักษาความสงบเรียบร้อย หรือ แนวความคิดตามทฤษฎีการควบคุมอาชญากรรม (Crime Control) ก็เป็นแนวความคิดที่ให้ความสำคัญกับการควบคุมปราบปรามอาชญากรรมเพื่อรักษาความสงบเรียบร้อยของสังคมเป็นหลัก ส่วนการคุ้มครองสิทธิเสรีภาพของบุคคลเป็นเรื่องรองลงไป การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ ก็จะช่วยทำให้สามารถป้องกันและปราบปรามอาชญากรได้เพราะช่วยให้เจ้าพนักงานสามารถแสวงหาพยานหลักฐานในคดีอาญาที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ซึ่งยากแก่การที่จะเข้าถึงได้ง่ายขึ้นและทำให้เกิดความรวดเร็วและมีประสิทธิภาพในการสืบสวนคดีอาญาเพื่อเอาตัวผู้กระทำผิดมาลงโทษ เมื่อพิจารณาถึงทั้งสองแนวความคิดรวมกันแล้วทั้งสองแนวความคิดก็มีจุดประสงค์อันเดียวกันคือการทำให้ประชาชนในสังคมอยู่ร่วมกันอย่างสงบสุขโดยปราศจากอาชญากรรมในสังคม การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์จึงจำเป็นที่จะต้องมีกรอบกฎหมายในการให้อำนาจดังกล่าวเพื่อให้อำนาจดังกล่าวอยู่ในกรอบของกฎหมาย โดยต้องมีการตรวจสอบ กลั่นกรอง และถ่วงดุลการใช้อำนาจดังกล่าวด้วย ไม่ว่าจะโดย ศาล อัยการ ประชาชน

ในการที่เจ้าพนักงานตามกฎหมายจะสามารถเข้าถึงพยานหลักฐานทางคอมพิวเตอร์ซึ่งเป็นข้อมูลอิเล็กทรอนิกส์ที่มีความสลับซับซ้อนเชื่อมโยงหลายเครือข่ายซึ่งยากแก่การค้นหาพยานหลักฐานดังกล่าวได้นั้น ก็จำเป็นที่จะต้องมีกฎหมายในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ที่จะให้อำนาจเจ้าพนักงานในการให้ได้มาซึ่งการสื่อสารที่เป็นการส่งและรับข้อมูลอิเล็กทรอนิกส์เช่นการส่งและรับจดหมายอิเล็กทรอนิกส์ ที่เป็นการใช้คอมพิวเตอร์ในการอำนวยความสะดวกในการกระทำผิดอาญาฐานต่างๆ ตามกฎหมายไทย โดยปัจจุบันกฎหมายไทยที่ให้อำนาจเจ้าพนักงานในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์นั้นก็คือ พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และที่แก้ไขเพิ่มเติม

พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม ฉบับที่ 4 พ.ศ. 2545 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 พระราชบัญญัติทั้งสามนี้ก็มีมาตรการในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ที่เป็นการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ แต่จะแบ่งไปตามประเภทคดีและวิธีการดำเนินการของหน่วยงานที่เกี่ยวข้องกับประเภทคดีที่รับผิดชอบและจากการศึกษาพระราชบัญญัติทั้งสามนี้พบว่า มีมาตรการการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ที่คล้ายคลึงกันเพียงแต่พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 จะมีหลักการแสวงหาพยานหลักฐานทางคอมพิวเตอร์ที่ครบถ้วนยิ่งกว่า ซึ่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 นี้ ก็ให้อำนาจเจ้าพนักงานในคดีพิเศษในกรณีที่มีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใดถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ พนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้ โดยอำนาจดังกล่าวทำให้เจ้าพนักงานคดีพิเศษสามารถทำการดักข้อมูลที่เป็นการติดต่อสื่อสารทางอิเล็กทรอนิกส์ซึ่งรวมถึงข้อมูลคอมพิวเตอร์ด้วยทำให้เจ้าพนักงานคดีพิเศษสามารถเข้าถึงพยานหลักฐานทางคอมพิวเตอร์และพยานหลักฐานทางอิเล็กทรอนิกส์อื่นๆ ด้วย ทั้งกฎหมายนี้ก็มีการตรวจสอบ กลั่นกรอง ถ่วงดุล การใช้อำนาจดังกล่าวไว้ไม่ว่าจะเป็นกำหนดให้มีกระบวนการขออนุญาตดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ไว้การกำหนดให้การอนุญาตตามคำขอให้มีการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์โดยให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นต่างๆ ตามกฎหมายดังกล่าวการกำหนดระยะเวลาในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ กระบวนการเก็บรักษา ใช้ประโยชน์และทำลายข้อมูลที่ได้มาจากการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์บทลงโทษเกี่ยวกับการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์โดยมิชอบอันเป็นการตรวจสอบกลั่นกรองและถ่วงดุลอำนาจดังกล่าวด้วย แต่อย่างไรก็ดีอำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์นั้นขอบเขตของอำนาจดังกล่าวก็สามารถใช้ได้เฉพาะความผิดอาญาที่เป็นคดีพิเศษที่อยู่ในบัญชีท้ายพระราชบัญญัติดังกล่าวเท่านั้น แต่ไม่มีมีผลแก่คดีอาญาอื่นๆ ตามประมวลกฎหมายอาญาที่มีความสำคัญไม่น้อยกว่ากันอาทิเช่นความผิดฐานเรียกค่าไถ่ ความผิดเกี่ยวกับความมั่นคง ความผิดฐานรีดเอาทรัพย์ เป็นต้น ทำให้อำนาจดังกล่าวไม่ครอบคลุมทุกฐานความผิดอำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์จึงไม่อาจนำมาใช้

กับความผิดฐานอื่นที่ไม่ใช่คดีพิเศษได้ นอกจากนี้ในกฎหมายของสหรัฐอเมริกาก็มีกฎหมายที่ช่วยในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์เช่นกันโดยรัฐบัญญัติ The Wiretap Statute (Title 3), amended 1986 (U.S.C. title 18 section 2510-2522) ที่ห้ามไม่ให้มีการดักการสื่อสารตามสายและทางอิเล็กทรอนิกส์เว้นแต่จะเข้าข้อยกเว้นตามกฎหมาย ซึ่งการละเมิดบทบัญญัติดังกล่าวจะทำให้เจ้าพนักงานต้องรับโทษทางแพ่งและทางอาญาและยังมีการเยียวยาความเสียหายโดยการไม่รับฟังพยานหลักฐานด้วยและรัฐบัญญัติ The Pen/Trap Statute, amended 2001 (U.S.C. title 18 section 3121-3127) ที่ให้อำนาจเจ้าพนักงานผู้บังคับใช้กฎหมายในการติดตั้งระบบการตรวจสอบการใช้งานโทรศัพท์ ทั้งเข้าและออก (Pen Register และ Trap and Trace (Pen/Trap)) ในการดักข้อมูลที่เป็นสารสนเทศประเภทที่อยู่ที่ส่งออกและรับเข้ามาที่ไม่ใช่เนื้อหาซึ่งช่วยทำให้ทราบที่อยู่ข้อมูลที่เกี่ยวกับการสื่อสารอิเล็กทรอนิกส์ที่ออกไปและการสื่อสารที่เข้ามาทำให้ทราบถึงแหล่งที่มาของข้อมูลอิเล็กทรอนิกส์ที่อาจใช้เป็นพยานหลักฐานได้ ซึ่งหากเจ้าพนักงานกระการละเมิดบทบัญญัตินี้ก็จะทำให้ต้องรับโทษทั้งทางแพ่งและอาญาเช่นกัน และรัฐบัญญัติ The USA Patriot act 2001 ก็ยังให้อำนาจแก่เจ้าพนักงานผู้บังคับใช้กฎหมายในการที่จะกระทำการตามรัฐบัญญัติ Title 3 และ Pen/Trap โดยอาจแจ้งถึงกระทำการดังกล่าวในภายหลัง ทั้งนี้เพื่อจับตามองการกระทำผิดอาญาของอาชญากร นอกจากนี้รัฐบัญญัติ The Sarbanes-Oxley Act of 2002 (U.S.C. title 18 section 1519) ก็ยังมีการบังคับโทษทางอาญาที่เข้มงวดในกรณีที่มีการเปลี่ยนแปลงหรือทำลายหลักฐานที่บันทึกไว้ในรูปของเอกสารอิเล็กทรอนิกส์รวมทั้งสื่อที่เก็บข้อมูลอิเล็กทรอนิกส์นั้นซึ่งช่วยให้ผู้กระทำผิดที่ใช้คอมพิวเตอร์ในการอำนวยความสะดวกในการกระทำผิดต้องรับโทษที่หนักสำหรับการกระทำที่เป็นการปกปิดความผิดของตนกฎหมายของสหรัฐอเมริกาจึงมีส่วนช่วยในการแสวงหาพยานหลักฐานทางคอมพิวเตอร์แก่เจ้าพนักงานอย่างมาก

การจะทำให้อำนาจในการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ที่จะทำให้เจ้าพนักงานสามารถเข้าถึงพยานหลักฐานทางอิเล็กทรอนิกส์รวมทั้งพยานหลักฐานทางคอมพิวเตอร์โดยที่ทำให้อำนาจดังกล่าวครอบคลุมทุกฐานความผิดและสามารถนำมาใช้กับคดีที่มีความสำคัญในทุกๆ คดีได้นั้นก็จำเป็นที่จะต้องนำบทบัญญัติที่เกี่ยวข้องกับการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์มาบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาของไทยโดยจากการศึกษาพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ในเรื่องการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ บทบัญญัตินี้ก็ได้บัญญัติอำนาจของเจ้าพนักงานคดีพิเศษในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ทั้งยังมีการตรวจสอบ กลั่นกรองและถ่วงดุลอำนาจดังกล่าวไว้อย่างเข้มงวด จึงเห็นว่าบทบัญญัตินี้มีความสมบูรณ์อยู่แล้วเพียงแต่อำนาจนั้นมีขอบเขตที่ใช้ได้เฉพาะคดีพิเศษแต่คดีอื่นๆ ที่มีความสำคัญไม่น้อยกว่ากันกลับไม่ได้

กำหนดอำนาจดังกล่าวนี้ไว้ การนำบทบัญญัติดังกล่าวมาบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาของไทยจึงน่าจะทำให้เกิดประสิทธิภาพในการควบคุมอาชญากรรมเสียมากกว่าเพราะทำให้บทบัญญัติในลักษณะดังกล่าวมีลักษณะเป็นบทบัญญัติให้ใช้ได้ทุกกรณีแต่ก็มีการตรวจสอบกลั่นและถ่วงดุล นอกจากนี้การกำหนดให้การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์เป็นข้อห้ามแต่ก็มีข้อยกเว้นกระทำได้ตามกฎหมายของสหรัฐอเมริกาดังที่กล่าวมาแล้วนั้นการนำกฎหมายดังกล่าวมาใช้ในประมวลกฎหมายวิธีพิจารณาความอาญาของไทยก็น่าจะก่อให้เกิดประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมมากยิ่งขึ้นเช่นกันเพราะกฎหมายดังกล่าวได้กำหนดข้อยกเว้นที่ให้อำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์สำหรับประเภทความผิดที่มีลักษณะร้ายแรงและกำหนดข้อยกเว้นอื่นๆ ที่เหมาะสมจึงน่าจะเกิดประโยชน์ที่จะนำข้อยกเว้นดังกล่าว มาใช้ในประมวลกฎหมายวิธีพิจารณาความอาญาของไทย อย่างไรก็ตามการจะใช้อำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์นั้นก็ต้องคำนึงถึง สิทธิ และเสรีภาพของประชาชนเป็นหลักการใช้อำนาจดังกล่าวและการป้องกันและปราบปรามอาชญากรรมในสังคมเพื่อให้สังคมมีความสงบเรียบร้อยควบคู่กันไปด้วย จึงต้องมีกรอบและขอบเขตในการใช้อำนาจดังกล่าวไว้นั่นเอง

5.2 ข้อเสนอแนะ

ผู้เขียนขอเสนอแนะแนวทางในการแก้ไขปัญหาการแสวงหาพยานหลักฐานทางคอมพิวเตอร์โดยการใช้อำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ตามที่ได้เสนอมาแล้วในบทก่อนหน้านี้ ทั้งนี้ข้อเสนอแนะที่เกิดขึ้นนี้มาจากการวิเคราะห์ปัญหาที่กำลังเกิดขึ้นในปัจจุบันและการป้องกันปัญหาที่อาจเกิดขึ้นในอนาคต เพื่อเป็นประโยชน์ในทางวิชาการและในทางปฏิบัติงานของเจ้าหน้าที่ในการใช้มาตรการดังกล่าวได้อย่างถูกต้องและมีประสิทธิภาพ อันจะทำให้บรรลุวัตถุประสงค์ในการป้องกันและปราบปรามการกระทำความผิดทางอาญาที่มีความร้ายแรงควบคู่ไปกับการคุ้มครองสิทธิเสรีภาพส่วนตัวของประชาชนให้ถูกกระทบจากการใช้มาตรการดังกล่าวน้อยที่สุด

เนื่องจากปัจจุบันการเข้าถึงพยานหลักฐานทางคอมพิวเตอร์ซึ่งเป็นพยานหลักฐานทางอิเล็กทรอนิกส์นั้นเป็นไปได้ยากเพราะ การค้นข้อมูลคอมพิวเตอร์ค่อนข้างมีความสลับซับซ้อนและละเอียดอ่อนอย่างมาก ทั้งยังโยงใยหลายเครือข่ายซึ่งข้อมูลนั้นอาจไม่อยู่ในคอมพิวเตอร์นั้นก็ได้ ดังนี้อาจเกิดปัญหาได้ว่าเมื่อเจ้าพนักงานเข้าไปค้นในที่รโหฐานใดเพื่อค้นหาพยานหลักฐานทางอิเล็กทรอนิกส์ (ดิจิตอล) ที่อยู่ในคอมพิวเตอร์ ด้วยเหตุที่ว่าคอมพิวเตอร์นั้นสามารถที่จะเก็บข้อมูลได้เป็นจำนวนมากและมีความสลับซับซ้อนเชื่อมโยงหลายเครือข่ายจึงยากแก่การที่จะค้นพบ

พยานหลักฐานทางอิเล็กทรอนิกส์ (ดิจิตอล) ที่อยู่ในคอมพิวเตอร์นั้นได้และบางครั้งข้อมูลดังกล่าวอาจถูกลบไปโดยผู้กระทำผิด ซึ่งในกรณีที่คอมพิวเตอร์นั้นเชื่อมโยงหลายเครือข่ายข้อมูลนั้นอาจไม่อยู่ในคอมพิวเตอร์นั้นก็ได้ อาจอยู่ในคอมพิวเตอร์เครื่องอื่นที่เชื่อมโยงกับคอมพิวเตอร์เครื่องนั้นก็ได้ ทำให้ยากต่อการค้นพบจึงเป็นปัญหาอย่างมากในแง่การค้นหาพยานหลักฐาน การที่จะทำให้เจ้าพนักงานสามารถเข้าถึงพยานหลักฐานดังกล่าวได้ก็จำเป็นที่จะต้องมีกฎหมายที่ช่วยในการแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์ ซึ่งก็คือกฎหมายที่เกี่ยวกับการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ ซึ่งปัจจุบันแม้พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 จะให้อำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ไว้ก็ตามแต่อำนาจนี้ก็ไม่ครอบคลุมทุกฐานความผิดที่มีความสำคัญ ปัญหาที่เกิดก็คือเมื่อไม่ครอบคลุมทุกฐานความผิดการป้องกันและปราบปรามอาชญากรรมในสังคมก็จะไม่มีประสิทธิภาพที่ดี ซึ่งกฎหมายของอเมริกาก็ได้กำหนดอำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ไว้ดังที่กล่าวมาแล้วเช่นกัน

ผู้เขียนจึงเสนอแนวทางในการที่จะบัญญัติกฎหมายที่เกี่ยวกับการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และกฎหมายสหรัฐอเมริกาลงในประมวลกฎหมายวิธีพิจารณาความอาญาของไทยโดย

1) การกำหนดให้การดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์เป็นข้อห้ามแต่ให้มีข้อยกเว้นให้กระทำได้

2) ข้อยกเว้นที่จะทำให้เจ้าพนักงานมีอำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ได้นั้นอาจนำข้อยกเว้นตามรัฐบัญญัติ Title 3 ของกฎหมายสหรัฐมาใช้มาใช้ในประมวลกฎหมายวิธีพิจารณาความอาญาของไทย โดยให้แบ่งข้อยกเว้นออกเป็น 1) การดักตามคำสั่งศาล 2) ข้อยกเว้นเรื่อง “ความยินยอม” 3) ข้อยกเว้นเรื่อง “ผู้ให้บริการ” 4) ข้อยกเว้นเรื่อง “ผู้บุกรุกทางคอมพิวเตอร์” 5) ข้อยกเว้นเรื่อง “โทรศัพท์พ่วง” 6) ข้อยกเว้นเรื่อง “การได้พยานหลักฐานในคดีอาญามาโดยบังเอิญ” 7) ข้อยกเว้นเรื่อง “การเข้าถึงสาธารณชน” ดังที่กล่าวมาแล้วในบทที่ 3

ข้อยกเว้นในเรื่องการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์โดยคำสั่งของศาลนี้อาจนำหลักการตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 มาใช้ในประมวลกฎหมายวิธีพิจารณาความอาญาของไทย กล่าวคือคำขอให้มีการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์จะต้องได้รับอนุมัติจากเจ้าหน้าที่ระดับสูงและยื่นคำขอดังกล่าวต่ออธิบดีผู้พิพากษาศาลอาญา เพื่อมีคำสั่งอนุญาตโดยการอนุญาตตามคำขอ

ดังกล่าวอธิบดีผู้พิพากษาศาลอาญาต้องพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นตามมาตรา 25 ดังต่อไปนี้

(1) มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ

(2) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

(3) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้การอนุญาตดังกล่าว ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวัน โดยกำหนดเงื่อนไขใดๆ ก็ได้และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อเจ้าพนักงานได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

บรรดาข้อมูลข่าวสารที่ได้มาให้เก็บรักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดซึ่งได้รับอนุญาตตามวรรคหนึ่งและให้ใช้ประโยชน์ในการสืบสวนหรือใช้เป็นพยานหลักฐานในการดำเนินคดีดังกล่าวเท่านั้น ส่วนข้อมูลข่าวสารอื่นให้ทำลายเสียทั้งสิ้น

นอกจากการนำบทบัญญัติดังกล่าวมาปรับใช้กับประมวลกฎหมายวิธีพิจารณาความอาญานี้แล้วก็ต้องมีการจำกัดอำนาจดังกล่าวให้มีได้เฉพาะคดีที่มีความผิดทางอาญาที่ร้ายแรงด้วยซึ่งผู้เขียนเห็นว่าอาจกำหนดให้มีผลใช้ได้กับความผิดอาญาที่มีโทษจำคุกขั้นสูงตั้งแต่สี่ปีขึ้นไปหรือโทษสถานหนักกว่านั้น โดยอ้างอิงจากความหมายของความผิดอาญาร้ายแรงตามที่อนุสัญญาสหประชาชาติเพื่อการต่อต้านอาชญากรรมข้ามชาติที่ก่อตั้งในลักษณะองค์กร ค.ศ. 2000 (United Nations Convention Against Transnational Organized Crime 2000) ที่ประเทศไทยได้ลงนามในอนุสัญญาฯ และได้ให้สัตยาบัน อีกทั้งพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 ที่สำนักงานอัยการสูงสุดจัดทำขึ้นและมีผลบังคับใช้แล้วที่กำหนดความหมายของ “ความผิดอาญาร้ายแรง”ไว้ โดยได้กำหนดความผิดไว้ตามที่ได้กล่าวไว้ในบทที่ 4 อาทิเช่น ความผิดที่เกี่ยวกับความมั่นคงแห่งราชอาณาจักร (ประมวลกฎหมายอาญา มาตรา 107-133) ความผิดเกี่ยวกับการก่อการร้าย (ประมวลกฎหมายอาญา มาตรา 135/1-135/4) ความผิดเกี่ยวกับความสงบสุขของประชาชน (ประมวลกฎหมายอาญา มาตรา 209, 210 วรรค 2, 213) ความผิดเกี่ยวกับการก่อให้เกิดภยันตรายต่อประชาชน (ประมวลกฎหมายอาญา มาตรา 217-222,

224-225, 230-232, 237-238) ความผิดเกี่ยวกับการปลอมและการแปลงเงินตรา (ประมวลกฎหมายอาญา มาตรา 240-249) ความผิดฐานเรียกค่าไถ่ (ประมวลกฎหมายอาญา มาตรา 313) โดยอาจกำหนดบัญชีประเภทความผิดที่สามารถทำการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ไว้ในบัญชีท้ายประมวลกฎหมายวิธีพิจารณาความอาญาก็ได้

3) กระบวนการเก็บรักษา ใช้ประโยชน์และทำลายข้อมูลที่ได้มาจากการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์และบทลงโทษ เกี่ยวกับการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์โดยมิชอบซึ่งบุคคลใดเปิดเผยข้อมูลข่าวสารที่ได้มาเนื่องจากการดำเนินการดักฟังตามมาตรา 25 ซึ่งไม่ใช่ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ซึ่งไม่มีในประมวลกฎหมายวิธีพิจารณาความอาญา ก็เห็นว่าควรต้องนำมาบัญญัติลงในประมวลกฎหมายวิธีพิจารณาความอาญาด้วยเพราะจะช่วยเป็นการตรวจสอบ กลั่นกรอง และถ่วงดุลการใช้อำนาจในการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์เพื่อไม่ให้การใช้อำนาจดังกล่าวล่วงล้ำไปถึงสิทธิและเสรีภาพของประชาชนจนมากเกินไป

4) การนำหลักการตามรัฐบัญญัติ The Pen/Trap Statute, amended 2001 ของสหรัฐอเมริกา ที่กำหนดให้เจ้าพนักงานในคดีอาญาสามารถติดตั้งระบบการตรวจสอบการใช้งานโทรศัพท์ทั้งเข้าและออก (Pen Register และ Trap and Trace (Pen/Trap)) ในการดักข้อมูลที่เป็นสารสนเทศประเภทที่อยู่ที่ส่งออกและรับเข้ามาที่ไม่ใช่เนื้อหาซึ่งช่วยทำให้ทราบที่อยู่ข้อมูลที่เกี่ยวกับการสื่อสารอิเล็กทรอนิกส์ที่ออกไปและการสื่อสารที่เข้ามาทำให้ทราบถึงแหล่งที่มาของข้อมูลอิเล็กทรอนิกส์ที่อาจใช้เป็นพยานหลักฐานได้ และรัฐบัญญัติ The USA Patriot Act 2001 ที่ให้อำนาจเจ้าพนักงานคดีอาญาในการแอบกระทำการดักฟังและการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ได้โดยแจ้งให้ทราบภายหลังถึงการกระทำดังกล่าว ทั้งการนำรัฐบัญญัติ The Sarbanes-Oxley Act of 2002 โดยกำหนดการบังคับโทษทางอาญาที่เข้มงวดในกรณีที่มีการเปลี่ยนแปลงหรือทำลายหลักฐานที่บันทึกไว้ในรูปของเอกสารอิเล็กทรอนิกส์รวมทั้งสื่อที่เก็บข้อมูลอิเล็กทรอนิกส์นั้นลงในประมวลกฎหมายวิธีพิจารณาความอาญา

5) การบัญญัติบทลงโทษแก่ผู้ที่ทำการดักฟังทางโทรศัพท์และติดตั้งอุปกรณ์ Pen/Trap โดยไม่ได้รับอนุญาตและการเยียวยาความเสียหายซึ่งเกิดจากการกระทำดังกล่าวโดยมิชอบด้วยกฎหมายโดยการไม่รับฟังพยานหลักฐานดังกล่าวที่ได้มา

จึงเห็นว่าหากนำหลักการดังกล่าวข้างต้นมาบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาก็จะทำให้เกิดประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมเพื่อให้เกิดความ

สงบสุขของสังคมและยังไว้ซึ่งการคุ้มครองสิทธิและเสรีภาพของประชาชนไม่ให้ถูกล่วงล้ำจนเกินไปด้วย

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

หนังสือ

กมล ทองธรรมชาติ. (2524). *วิวัฒนาการของระบบรัฐธรรมนูญไทย* (พิมพ์ครั้งที่ 2). กรุงเทพมหานคร: บรรณกิจ.

กมลชัย รัตนสกาววงศ์ และ วรพจน์ วิศรุตพิชญ์. (2540). *แนวทางในการยกร่างกฎหมายที่เกี่ยวข้องกับการดักฟังทางโทรศัพท์และการปรับปรุงกฎหมายอื่นๆ ที่เกี่ยวข้อง (รายงานผลการวิจัย).* กรุงเทพมหานคร: สำนักงานคณะกรรมการวิจัยแห่งชาติ.

กุลพล พลวัน. (2538). *พัฒนาการแห่งสิทธิมนุษยชน* (พิมพ์ครั้งที่ 3). กรุงเทพมหานคร: วิญญูชน.

_____. (2544). *การบริหารกระบวนการยุติธรรม* (พิมพ์ครั้งแรก). กรุงเทพมหานคร: นิติธรรม.

เกียรติขจร วัจนะสวัสดิ์. (2551). *คำอธิบาย หลักกฎหมายวิธีพิจารณาความอาญา ว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณา พร้อมด้วย คำอธิบายมาตราที่แก้ไขเพิ่มเติมใหม่ตาม พ. ร. บ. แก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความอาญา ฉบับที่ 25,26,27,28,29 (เฉพาะขั้นตอนก่อนการพิจารณา).* กรุงเทพมหานคร: จิรรัชการพิมพ์.

คณิต ณ นคร. (2555). *กฎหมายวิธีพิจารณาความอาญา* (พิมพ์ครั้งที่ 8). กรุงเทพฯ: วิญญูชน.

_____. (2556). *ประมวลกฎหมายวิธีพิจารณาความอาญา: หลักกฎหมายและพื้นฐานการเข้าใจ* (พิมพ์ครั้งที่ 2). กรุงเทพฯ: วิญญูชน.

คนึง ฦาไชย. (2523). *พยาน.* กรุงเทพมหานคร: เรือนแก้วการพิมพ์.

_____. (2548). *กฎหมายวิธีพิจารณาความอาญา เล่ม 1* (พิมพ์ครั้งที่ 8). กรุงเทพมหานคร: มหาวิทยาลัยธรรมศาสตร์.

จิตติ ติงศภัทิย์. (2533). *หลักวิชาชีพนักกฎหมาย* (พิมพ์ครั้งที่ 6). กรุงเทพมหานคร: ประกายพรึก.

ชัยวัฒน์ วงศ์วัฒนศานต์ ทวีศักดิ์ กออนันตกูล และ สุรางคณา แก้วจำนง. (2544*). คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544.* กรุงเทพมหานคร: สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ.

นิยม เติมศรีสุข. (2549). *มาตรา 25 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรการเข้าถึงข้อมูลข่าวสาร ความเป็นมา การบังคับใช้ และข้อเสนอในการพัฒนากฎหมาย* (เอกสารไม่ตีพิมพ์). กรุงเทพมหานคร: กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม.

แผนกอาชญากรรมทางคอมพิวเตอร์และทรัพย์สินทางปัญญา สำนักงานคดีอาญา กระทรวงยุติธรรมแห่งสหรัฐอเมริกา. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, 2002 แปลโดย สำนักงานอัยการสูงสุด.*

พรเพชร วิชิตชลชัย. (2542). *คำอธิบายกฎหมายลักษณะพยาน* (พิมพ์ครั้งที่ 4). กรุงเทพมหานคร: เกนโกรว.

มานิตย์ จุมปา. (2549). *คำอธิบายรัฐธรรมนูญแห่งราชอาณาจักรไทย (พ.ศ. 2540) รัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช 2549 พร้อมข้อเสนอสำหรับรัฐธรรมนูญแห่งราชอาณาจักรไทย (พ.ศ. 2550)* (แก้ไขเพิ่มเติมครั้งที่ 8). กรุงเทพมหานคร: นิติธรรม.

ยิ่งศักดิ์ กฤษณะจินดา. (2524). *กฎหมายลักษณะพยานหลักฐาน* (พิมพ์ครั้งที่ 1). กรุงเทพมหานคร: มหาวิทยาลัยธรรมศาสตร์.

ศรีไพร ศักดิ์รุ่งพงศากุล. (2544). *เทคโนโลยีคอมพิวเตอร์ และสารสนเทศ.* กรุงเทพมหานคร: ซีเอ็ดยูเคชั่น.

สำนักงานศาลยุติธรรม สถาบันวิจัยรพีพัฒนศักดิ์. (2550). *การออกหมายค้น หมายจับ ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 (รายงานผลการวิจัย).* กรุงเทพมหานคร: ชวนพิมพ์ 50.

สุรพล ไตรเวทย์. (2547). *การสอบสวนคดีพิเศษ.* กรุงเทพฯ: วิญญูชน.

สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. (2556). *ประมวลกฎหมายวิธีพิจารณาความอาญา ฉบับอ้างอิง* (พิมพ์ครั้งที่ 14). กรุงเทพมหานคร: วิญญูชน.

โสภณ รัตนากร. (2553). *คำอธิบายกฎหมายลักษณะพยาน* (พิมพ์ครั้งที่ 10). กรุงเทพมหานคร: นิติบรรณาการ.

อรรณพ ลิขิตจิตถะ และคณะ. (2548). *การพัฒนากฎหมายป้องกันและปราบปรามอาชญากรรมข้ามชาติที่มีการจัดตั้งในลักษณะองค์กร (ระยะที่ 2) หัวข้อ เทคนิคการสืบสวนสอบสวนพิเศษ* (รายงานผลการวิจัย). กรุงเทพมหานคร: สถาบันกฎหมายอาญา สำนักงานอัยการสูงสุด.

บทความ

เกียรติขจร วัจนะสวัสดิ์. (2521). “หลักการไม่ยอมรับฟังพยานวัตถุ พยานเอกสาร ซึ่งได้มาโดยการจับ การค้น การยึดที่ไม่ชอบด้วยกฎหมายในสหรัฐอเมริกา.” *วารสารนิติศาสตร์, 9 (3).* หน้า 120-136.

คณิต ณ นคร. (2528). “วิธีพิจารณาความอาญาไทย: หลักกฎหมายกับทางปฏิบัติที่ไม่ตรงกัน.” *วารสารนิติศาสตร์, 15 (3).* หน้า 11.

จรัญ ภักดีธนากุล. (2523, มกราคม-กุมภาพันธ์). “ศาล กับ ความเป็นสูงสุดแห่งรัฐธรรมนูญ.” *ดุลพาห, 27 (1).* หน้า 51-88.

จิรนิติ หะวานนท์. (2527, พฤษภาคม-มิถุนายน). “หลักการไม่รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ: เปรียบเทียบระหว่างกฎหมายอเมริกันและกฎหมายเยอรมัน.” *ดุลพาห, 31 (3).* หน้า 34-52.

ประธาน วัฒนพานิช. (2520, กันยายน-พฤศจิกายน). “ระบบความยุติธรรมทางอาญา: แนวความคิดเกี่ยวกับการควบคุมอาชญากรรมและกระบวนการนิติธรรม.” *วารสารนิติศาสตร์, 9 (2).* หน้า. 151.

ประเสริฐ คันธมานนท์ และ สมชัย จันทรมัสการ. (2549, มีนาคม). “พยานหลักฐานดิจิตอล.” *บทบัณฑิตย์, 6 (1).* หน้า 43-45.

ไพจิตร สวัสดิสาร. (2549, มกกราคม-เมษายน). “การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์หรือนิติคอมพิวเตอร์ (Computer Forensic).” *ดุลพาห, 53 (1).* หน้า 63-101.

วิทยานิพนธ์

กิตติมา ประคุณคดี. (2533). *การดักฟังทางโทรศัพท์โดยเจ้าพนักงาน* (วิทยานิพนธ์ปริญญามหาบัณฑิต). กรุงเทพมหานคร: จุฬาลงกรณ์มหาวิทยาลัย.

ธนชัย นักสอน. (2552). *การตรวจสอบและถ่วงดุลการดักฟังทางโทรศัพท์และการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ ตามมาตรา 25 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547* (วิทยานิพนธ์ปริญญามหาบัณฑิต). กรุงเทพมหานคร: มหาวิทยาลัยธรรมศาสตร์.

ไพรัช โตสวัสดิ์. (2547). *การตรวจสอบความชอบด้วยกฎหมายของปฏิบัติการทางปกครอง* (วิทยานิพนธ์ปริญญามหาบัณฑิต). กรุงเทพมหานคร:

องอาจ เทียนหิรัญ. (2546). *อาชญากรรมทางคอมพิวเตอร์:การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์* (วิทยานิพนธ์ปริญญามหาบัณฑิต). กรุงเทพมหานคร: มหาวิทยาลัยธรรมศาสตร์.

กฎหมาย

ข้อบังคับ กคพ. ว่าด้วยการเก็บรักษา การใช้ประโยชน์ข้อมูลข่าวสารที่ได้มาและการทำลายข้อมูลข่าวสารอื่น พ.ศ. 2547

ประมวลกฎหมายวิธีพิจารณาความอาญา.

ประมวลกฎหมายอาญา.

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547.

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และที่แก้ไขเพิ่มเติม.

พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556.

พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 แก้ไขเพิ่มเติม ฉบับที่ 4 พ.ศ. 2545.

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

ระเบียบคณะกรรมการป้องกันและปราบปรามยาเสพติดว่าด้วยการได้มา การใช้ประโยชน์และการเก็บรักษาข้อมูลข่าวสาร พ.ศ. 2545.

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550.

เอกสารอื่น ๆ

รายงานการศึกษาวิจัยเพื่อนำเสนอในการประชุมทางวิชาการระดับชาติ ว่าด้วยงานยุติธรรม ครั้งที่ 2. (2547). *มาตรการป้องกันและปราบปรามองค์กรอาชญากรรมและผู้มีอิทธิพล.* หน้า 19-20.

สำนักงานคณะกรรมการกฤษฎีกา. (2555). *บันทึกวิเคราะห์สรุปสาระสำคัญของร่างพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. .... เรื่องเสร็จที่ 614/2555.*

ภาษาต่างประเทศ

BOOKS

Hill, Rossen and Sog, (1982). *Criminal Procedure Fourth Edition.* USA: West.

Jerold H. Isreal, Yale kamisar , Wayne R. LaFave. (1980). *Basic Criminal Procedure.* USA: West.

Jerold H. Isreal, Yale kamisar , Wayne R. LaFave. (1994). *Criminal Procedure and The Constitution Leading Supreme Court Cases and Introductory Text 1994 Edition.* USA: West.

Office of Legal Education Executive Office for United States Attorneys**. (**2002). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.*

Sanford H. Kadish, Monrad G. Paulsen. (1975). *Criminal Law and Its Processes Cases and Materials Third Edition.* USA: Little, Brown & Company (Canada).

Wayne R. LaFave. (2000). *Criminal Procedure Third Edition*. USA: West Group Basic.

West's encyclopedia of American Law. (1997). USA: West.

LAWS

Federal Rules of Criminal Procedure.

The electronic communication privacy act (ECPA) 1986.

The pen/trap statute, amended 2001.

The Sarbanes-oxley Act of 2002.

The USA Patriot Act 2001.

The Wiretap statute (title 3), amended 1986.

United Nations Convention Against Transnational Organized Crime 2000.

ELECTRONIC SOURCES

Code of Criminal Procedure, Title III, Section III, Subsection 2, Article 100 Retrieved October 10, 2008, from http://www.legifrance.gour.fr.

Code of Criminal Procedure, Title III, Section III, Subsection 2, Article 100-1 Retrieved October 10, 2008, from http://www.legifrance.gour.fr.

Computer Crime & Intellectual Property Section United States Department of Justice "Prosecuting Computer Crimes "Manual"" http://www.cybercrime.gov/index.html.

Computer Forensic: การค้นหา และพิสูจน์หลักฐานดิจิตอล *http://www.thaiadmin.org/board/index.php?topic=45125.0*

General information from Ministry of foreign affairs of the kingdom of Thailand, 2013, from *http://www.mfa.go.th/main/th/media-center/14/*

Katz v. United States. 389 U.S. 347. (1967). Retrieved October 1. 2008, from *http://www.uscourts.gov.*

Olmstead v. United States, 277 U. S. 438, (1928), Retrieved October 1, 2008, from *http://www.law.cornell.edu.*

ประวัติผู้เขียน

ชื่อ – สกุล	ร้อยตรี พิทักษ์พงศ์ ตันบุญเอก
ประวัติการศึกษา	นิติศาสตรบัณฑิต มหาวิทยาลัยหอการค้าไทย
ตำแหน่งและสถานที่ทำงานปัจจุบัน	ประจำแผนกแบบธรรมเนียม กองระเบียบการ กรมเสมียนตรา สำนักงานปลัดกระทรวงกลาโหม