ปัญหาทางกฎหมายเกี่ยวกับการดักฟังการสื่อสารทางอินเทอร์เน็ต

คธา รักแผน*

ผศ.ดร.กรรภิรมย์ โกมลารชุน**

1.บทคัดย่อ

บทความนี้มีวัตถุประสงค์ในศึกษาถึงการนำมาตรการบังคับทางอาญา (compulsory measures) มาใช้กับการดักฟังการสื่อสารโทรคมนาคมทางอินเทอร์เน็ต โดยศึกษาถึงหลักการและความเหมาะสมของมาตรการบังคับทางอาญากับการนำหลักการดักฟังการสื่อสารโทรคมนาคมตามกฎหมายต่างประเทศมาปรับใช้กับการใช้อำนาจของรัฐในการแสวงหาพยานหลักฐาน กับการคุ้มครองสิทธิความเป็นส่วนตัว (Right to Privacy) และเสรีภาพในการสื่อสารของปัจเจกบุคคลอย่างเหมาะสม เพื่อให้เกิดสมดุลระหว่างการป้องกันและปราบปรามการก่ออาชญากรรมที่นับวันจะยิ่งมีรูปแบบที่ซับซ้อนมากขึ้นอันเกิดมาจากความก้าวหน้าของเทคโนโลยีการสื่อสารไปพร้อมกับการคุ้มครองสิทธิและเสรีภาพของประชาชน

โดยจากการศึกษาพบว่าในต่างประเทศนั้นมีการบัญญัติหลักกฎหมายว่าด้วยมาตรการ ดักฟังการสื่อสารทางโทรคมนาคมทางอินเทอร์เน็ตให้เป็นหลักกฎหมายซึ่งบังคับใช้เป็นการทั่วไปตามประมวลกฎหมายวิธีพิจารณาความอาญา โดยกำหนดถึงกระบวนการ เงื่อนไข และองค์กรที่มีอำนาจใช้มาตรการเอาไว้อย่างชัดเจนแน่นอน ซึ่งส่งผลโดยตรงต่อการคุ้มครองสิทธิและเสรีภาพของบุคคลจากการใช้อำนาจของรัฐอย่างมีภาวะวิสัย (Objectivity) ในส่วนของประเทศไทยพบว่ายังขาดหลักกฎหมายว่าด้วยมาตรการดักฟังการสื่อสารทางอินเทอร์เน็ต โดยไม่มีกฎหมายฉบับใดที่ให้อำนาจในการดักฟังการสื่อสารทางอินเทอร์เน็ตไว้โดยเฉพาะทำให้เจ้าพนักงานปราศจากอำนาจตามกฎหมายในการบังคับใช้มาตรการ ซึ่งที่ผ่านมาหลักการดักฟังการสื่อสารโทรคมนาคมของไทยนั้นกระจัดกระจายอยู่ตามพระราชบัญญัติต่าง ๆ หลายฉบับซึ่งมีสถานะเป็นกฎหมายพิเศษ ส่งผลให้ไม่อาจนำกฎหมายเหล่านั้นมาบังคับใช้ให้ครอบคลุมถึงข้อเท็จจริงที่เกิดขึ้นตามพฤติการณ์แห่งคดีที่มีความแตกต่างกัน รวมทั้งการบังคับใช้กฎหมายพิเศษเหล่านี้ก็กระทำโดยองค์กรที่ต่างกันไปตามแต่วัตถุประสงค์ของกฎหมายพิเศษในแต่ละฉบับ ส่งผลให้ไม่อาจใช้มาตรการบังคับทางอาญาให้อยู่ภายใต้หลักการตีความ กระบวนการ เงื่อนไข และองค์กรที่มีอำนาจอนุมัติให้ใช้มาตรการอย่างแน่นอนชัดเจน ซึ่งส่งผลกระทบโดยตรงต่อการละเมิดต่อสิทธิเสรีภาพและการอำนวยความยุติธรรม

ดังนั้น การแก้ปัญหาทำได้โดยการบัญญัติให้หลักการของมาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตเป็น หลักกฎหมายทั่วไป (Jus Generale) ในประมวลกฎหมายวิธีพิจารณาความอาญา เพื่อให้แนวทางในการบังคับใช้กฎหมายและการตีความกฎหมายของศาลต่อการใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตมีแนวทางปฏิบัติและได้รับการตีความไปด้วยกันอย่างมีเอกภาพ ทั้งนี้ โดยนำหลักกฎหมายต่างประเทศมาสร้างหลักกฎหมายโดยกำหนดกระบวนการในการขอใช้มาตรการ เงื่อนไขต่าง ๆ ไม่ว่าจะเป็น

---

* นักศึกษาหลักสูตรนิติศาสตร์มหาบัณฑิต คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์

** ที่ปรึกษาวิทยานิพนธ์หลัก

ประเภทคดี ฐานความผิด กรอบระยะเวลา ผู้มีอำนาจขอใช้และผู้มีอำนาจอนุมัติให้ใช้มาตรการ การทำลายข้อมูลที่ได้จากการใช้มาตรการ การจัดทำรายงานสรุปการใช้มาตรการเผยแพร่ต่อสาธารณะ ความรับผิดของเจ้าพนักงานต่อการละเมิดหลักการแห่งการใช้มาตรการ รวมทั้งการคุ้มครองบุคคลภายนอกต่อผลกระทบจากการใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตต่อไป

ABSTRACT

The objective of this thesis is to study the compulsory measures used in electronic and internet communication surveillance. The thesis focuses on the principle and appropriation of the compulsory measures and how electronic communication surveillance is used under foreign laws especially when it applies to the acquirement of evidence, right to privacy, and freedom of communication. The focus will be on how to create the balance between protection and prevention of this type of crimes, which have become more complex as a result of communication technological advancement, as well as the protection of rights and freedom of all citizens.

The study shows that in other countries there are provisions of law regarding electronic surveillance procedures in criminal procedural codes. Within the code, the procedures, conditions, and agency that may exercise its authority specifically identified. This results in the direct protection of rights and freedom of citizen from the wrongful exercise of duty objectively. In Thailand, there is still a lack of law regarding digital and electronic surveillance procedures, since there is no specific act authorizes the use of electronic (internet) surveillance.

This creates the situation where the government does not have the authority under the law to conduct surveillance. In the past, the surveillance procedures are scattered in many different acts. These acts are considered special laws and cannot be used to cover different facts in all cases. In addition, the exercise of special laws is carried out by different agencies according to different special act. Due to this fact, it is not possible to have clear interpretation of the law, procedures, conditions, and the agencies that are authorize to exercise these compulsory measures. This creates direct impact to the violation of rights, freedom, and the justice service provided.

Thus, it is suitable to provide a solution by including the principle of electronic surveillance as Jus Generale within the Criminal Procedural Act. This will create unity in court procedures and interpretations. Foreign laws may be applied in creating the principle of laws, by specifying the process on how to receive permission to conduct the survey, conditions such as type of crimes, charges, time line, authorized agency, and authorized entity to grant permission to conduct surveillance, destroy of information obtained from the

surveillance, reporting mechanism to the public, liability of the authority abusing the process, as well as protection of any third party that may be impacted from the electronic surveillance measures.

2.บทนำ

ในปัจจุบันเทคโนโลยีโทรคมนาคมเข้ามามีบทบาทสำคัญต่อการดำเนินชีวิตนอกเหนือจากการติดต่อสื่อสารกันผ่านทางโทรศัพท์ ยังมีวิธีการติดต่อสื่อสารกันโดยอาศัยช่องทางเครือข่ายโทรคมนาคม (Telecommunication) ทางอินเทอร์เน็ตผ่านแอพพลิเคชั่นต่าง ๆ เช่น Line, Whatsapp, Facebook Instant Massager การโทรศัพท์ผ่านอินเทอร์เน็ต (Voice-over-IP–VoIP) หรือการส่งข้อความผ่านระบบการส่งข้อความทันที (Instant Messaging) ซึ่งเนื้อหาของการสื่อสารกันด้วยวิธีการเช่นว่านี้จะถูกเข้ารหัสไว้ ทำให้หน่วยงานที่มีอำนาจสอบสวนคดีอาญาเมื่อต้องการข้อมูลที่จะใช้ในการสืบสวนสอบสวนก็จะได้รับแต่เพียงข้อมูลที่ถูกเข้ารหัสเอาไว้ และการถอดรหัสก็ไม่สามารถทำได้ด้วยวิธีการปัจจุบัน หรือแม้จะทำได้ก็ต้องใช้ค่าใช้จ่ายที่สูง ทำให้ยากต่อการตรวจสอบ ในประเทศเยอรมนีได้มีการแก้ไขเพิ่มเติมหลักการที่เกี่ยวข้องกับการสื่อสารโทรคมนาคมเพื่อเพิ่มประสิทธิภาพการดำเนินคดีอาญา โดยเฉพาะอย่างยิ่งในเรื่องการดักฟังการสื่อสารทางอินเทอร์เน็ต[1]เอาไว้โดยตรงทำให้มาตรการสอบสวนคดีอาญาเท่าทันความก้าวหน้าของเทคโนโลยีสามารถได้มาซึ่งเนื้อหาของการสื่อสารก่อนที่จะเข้ารหัสหรือเนื้อหาหลังจากการถอดรหัสแล้วโดยใช้โปรแกรมพิเศษที่ถูกติดตั้งไว้ที่เครื่องมือหรืออุปกรณ์ปลายทาง (Quellen-TKÜ)[2]

มาตรการนี้เป็นเครื่องมือสำคัญที่รัฐใช้จัดการกับการก่ออาชญากรรมทั้งในรูปแบบปกติและรูปแบบองค์กรอาชญากรรม (Organized Crime) ซึ่งจำเป็นต้องกำหนดเงื่อนไขของมาตรการที่แน่นอนและชัดเจน มีขอบเขตและวิธีการในการใช้มาตรการ เพื่อทำให้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตมีความเป็นภาวะวิสัย เกิดสมดุลในการปราบปรามการกระทำความผิดไปพร้อมกับการคุ้มครองสิทธิและเสรีภาพของบุคคล ที่ผ่านมาประเทศไทยมีกฎหมายเฉพาะ (Jus speciale) ที่ให้อำนาจเจ้าพนักงานในการดักฟังการกระทำความผิดหรือดักรับข้อมูลเกี่ยวกับการกระทำความผิด กระจัดกระจายกันอยู่ในพระราชบัญญัติต่าง ๆ อาทิ พระราชบัญญัติป้องกันและปราบปรามยาเสพ-ติด พ.ศ.2519 มาตรา 14 จัตวา, พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 มาตรา 46, พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 มาตรา 25, พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ฯลฯ เป็นต้น

เมื่อพิจารณาบทบัญญัติเหล่านี้พบว่ามีการบัญญัติหลักเกณฑ์รวมทั้งเงื่อนไขที่แตกต่างกันเพื่อให้เป็นไปตามวัตถุประสงค์ของพระราชบัญญัติแต่ละฉบับ ทำให้เกิดปัญหาการกระจัดกระจายของกฎหมายที่จะใช้บังคับกับข้อเท็จจริงที่เกิดขึ้นส่งผลให้การบังคับใช้กฎหมายที่ใกล้เคียงกันมีการตีความการใช้กฎหมายที่

---

[1] วิธีพิจารณาความอาญาของเยอรมนี § 100a (StPO).

[2] รายงานวิจัยฉบับสมบูรณ์เรื่อง กฎหมายเกี่ยวกับการให้รัฐเข้าถึงและได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน:กรณีศึกษาสหพันธรัฐเยอรมนี, น.9-10, กรรภิรมย์ โกมลารชุน ,(2561),กรุงเทพฯ:สถาบันพระปกเกล้า.

แตกต่างกัน ดังนั้น ควรรวบรวมหลักเกณฑ์และวิธีการให้เป็นหลักเกณฑ์กลางให้เป็น บทกฎหมายทั่วไป[3] (Jus generale) เพื่อเป็นการสร้างหลักกฎหมายให้สอดคล้องกับแนวทางสากลที่กำหนดบทบัญญัติเช่นนี้ไว้ในกฎหมายวิธีพิจารณาความอาญา ทำให้การปฏิบัติหน้าที่ของเจ้าพนักงานมีมาตรฐานเดียวกันได้ แม้ว่าจะมีความพยายามที่จะนำเรื่องการดักฟังและดักรับข้อมูลมาบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา แต่ร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131/2 ก็ยังไม่ครอบคลุมถึงมาตรการดักฟังการสื่อสารทางอินเทอร์เน็ต จึงถือได้ว่าปัจจุบันประเทศไทยยังไม่มีกฎหมายกลางที่รวบรวมหลักเกณฑ์ดังกล่าวเข้าไว้ด้วยกัน ซึ่งบทความนี้จะได้ชี้ให้เห็นถึงหลักกฎหมายของไทยเปรียบเทียบกับหลักการของกฎหมายต่างประเทศต่อไป

3.หลักการเกี่ยวกับการใช้มาตรการบังคับทางอาญาของเจ้าพนักงานในการดักฟังการสื่อสารทางอินเทอร์เน็ตตามกฎหมายต่างประเทศเปรียบเทียบกับประเทศไทย และแนวทางการแก้ปัญหาเกี่ยวกับการใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ต

สำหรับการบัญญัติกฎหมายเรื่องมาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตซึ่งถือเป็น มาตรการบังคับทางอาญา[4] (Compulsory Measure) อย่างหนึ่งเช่นเดียวกับมาตรการบังคับทางอาญาตามกฎหมายวิธีพิจารณาความอาญาของไทย เช่น การจับ การค้น ถือว่าเป็นเครื่องมือสำคัญของเจ้าพนักงานและศาลในการดำเนินคดีอาญาโดยรัฐ (Public Prosecution) กฎหมายต้องกำหนดเงื่อนไขในการใช้มาตรการให้รัดกุม ชัดเจนและแน่นอนเกี่ยวกับวัตถุประสงค์และเงื่อนไขในการใช้มาตรการให้มากที่สุด โดยให้ศาลเป็นผู้อนุมัติ โดยกฎหมายต้องกำหนดระยะเวลาในการใช้มาตรการที่แน่นอน มีขอบเขตและวิธีการใช้มาตรการ รวมทั้งการขยายระยะเวลาก็ควรต้องมีเหตุจำเป็นที่ให้ศาลพิจารณาอนุมัติ ทั้งนี้ เพื่อคุ้มครองสิทธิในการติดต่อสื่อสารของบุคคลให้ไม่ต้องถูกกระทบกระเทือนมากจนเกินไปจากการบังคับใช้กฎหมายอย่างมีภาวะวิสัย (Objectivity) ถือเป็นกระบวนการที่อยู่บนหลักของการตรวจสอบจากภายนอก (Accountability) โดยองค์กรศาลสามารถใช้ดุลพินิจตรวจสอบการใช้อำนาจของเจ้าพนักงานซึ่งเป็นฝ่ายบริหารได้

3.1 เงื่อนไขและความจำเป็นในการขอใช้มาตรการ หลักการในกฎหมายต่างประเทศ ดังนี้

(1) ประเทศสหรัฐอเมริกาตามกฎหมาย The Omnibus Crime Control and Safe Streets Act of 1968 บัญญัติหลักการสำคัญไว้ว่า ห้ามดักฟังการกระทำความผิด เพื่อคุ้มครองสิทธิในการสื่อสาร (Right of Communication) หลักเกณฑ์นี้คล้ายกับมาตรการบังคับ “หมายอาญา” ในส่วนของหมายจับ หมายค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาของไทย

(2) ประเทศเยอรมนี วิธีพิจารณาความอาญาเยอรมนี กำหนดเงื่อนไขสำคัญไว้สองประการด้วยกัน คือ ต้องปรากฏว่ามีความสงสัยว่ามีการกระทำความผิดอาญาเกิดขึ้น โดยจะต้องปรากฏข้อเท็จจริงสนับสนุนว่า

[3] ปรีดี เกษมทรัพย์, กฎหมายแพ่ง:หลักทั่วไป,พิมพ์ครั้งที่ 5(กรุงเทพฯ:หจก.ภาพพิมพ์,2526), น.57-58.

[4] คณิต ณ นคร, กฎหมายวิธีพิจารณาความอาญา,พิมพ์ครั้งที่ 8(กรุงเทพฯ:วิญญูชน,2555), น.266.

มีความสงสัยว่าการกระทำความผิดอาญาในมาตรา 100a II StPO เกิดขึ้นเสียก่อน โดยใช้ระดับความสงสัยเพียงระดับเบื้องต้น (Anfangsverdacht) เท่านั้น โดยในคำร้องขอใช้มาตรการดักการสื่อสารโทรคมนาคมจะต้องบรรยายให้ได้ว่า การสอบสวนโดยไม่ใช่มาตรการดังกล่าวไม่อาจประสบความสำเร็จได้หรืออาจทำได้โดยยากลำบากเพราะเหตุใด

(3) ประเทศฝรั่งเศสเป็นที่มีการบัญญัติกฎหมายว่าด้วยการดักฟังการกระทำความผิด โดยบัญญัติไว้ตามรัฐบัญญัติ เลขที่ 91-646 กำหนดให้ฝ่ายบริหารมีอำนาจอนุญาตให้ทำการดักฟังการติดต่อสื่อสารถึงกันทางโทรคมนาคมเพื่อรักษาความมั่นคงของรัฐ

จะเห็นได้ว่าทุกประเทศล้วนให้ความสำคัญต่อรายละเอียดในการกำหนดเงื่อนไขที่จะขอใช้มาตรการ ดังนั้น ควรกำหนดหลักเกณฑ์สำคัญคือ “ต้องปรากฏว่ามีความสงสัยว่ามีการกระทำความผิดอาญาเกิดขึ้น และเจ้าพนักงานต้องแสดงเหตุต่อศาลให้ได้ว่าการค้นหาความจริงในคดีหรือการทราบถึงสถานที่ที่ผู้ถูกกล่าวหาใช้เป็นที่อาศัยอยู่นั้นทำได้ยากลำบากหรือเป็นไปไม่ได้เลย” โดยความสงสัยใช้ระดับความสงสัยเพียงระดับเบื้องต้นเท่านั้น กล่าวคือ พยานหลักฐานมีความน่าเชื่อเพียงขั้น “น่าจะ” ไม่ใช่ “แน่ใจ” ไม่ต้องมีหลักฐานถึงขนาดปราศจากข้อสงสัยหรือถึงขั้นมีมูลเป็นความผิดเหมือนเช่นในกรณีการลงโทษหรือการไต่สวนมูลฟ้องคดีอาญา[5]

3.2 ฐานความผิดในการขออนุมัติต่อศาลในการใช้มาตรการ ต้องมีการกำหนดฐานความผิดไว้อย่างชัดเจนแน่นอน ดังนี้

(1) ประเทศสหรัฐอเมริกา กำหนดลักษณะของความผิดอาญาบางประเภทที่รัฐสามารถดักฟังการกระทำความผิดได้[6] ต้องเป็นไปเพื่อประโยชน์ในการสืบสวนสอบสวนและป้องกันอาชญากรรม ตามประมวลกฎหมายสหรัฐ (The United State Code/U.S.Code) ยกตัวอย่างเช่น ความผิดที่มีโทษประหารชีวิต หรือจำคุกเกินกว่า 1 ปี ความผิดเกี่ยวกับการก่อวินาศกรรมอุปกรณ์นิวเคลียร์หรือพลังงาน เป็นเฉพาะความผิดอาญาดังที่กล่าวมาข้างต้นนี้เท่านั้นที่จะมีการดักฟังการกระทำความผิดทางโทรศัพท์ได้ ความผิดอาญาอื่น ๆ ไม่อาจใช้การดักฟังการกระทำความผิดเพื่อป้องกันและสอบสวนได้

(2) ประเทศเยอรมนี วิธีพิจารณาความอาญาเยอรมนี มาตรา 100a StPO แบ่งประเภทความผิดออกเป็น 11 กลุ่มความผิด ซึ่งการดักการสื่อสารโทรคมนาคมจะกระทำได้แต่เฉพาะฐานความผิดตามที่ปรากฏในมาตรานี้[7] เท่านั้น โดยมีเจตนารมณ์ในการใช้มาตรการนี้ต่อความผิดอาญาที่เป็นความผิดอาญาร้ายแรง ยกตัวอย่างเช่น กลุ่มความผิดตามประมวลกฎหมายอาญาที่มีความร้ายแรง เช่น ความผิดเกี่ยวกับความมั่นคงของรัฐ การเป็นปรปักษ์ต่อระบอบเสรีประชาธิปไตย ความผิดฐานฆาตกรรม ความผิดเกี่ยวกับการฟอกเงิน กลุ่มความผิดตามพระราชบัญญัติเกี่ยวกับยาเสพติด กลุ่มความผิดตามพระราชบัญญัติควบคุมอาวุธสงคราม กลุ่ม

---

[5] ณรงค์ ใจหาญ, หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1,พิมพ์ครั้งที่ 12,(กรุงเทพฯ:วิญญชน,2556), น.214.

[6] The Omnibus Crime Control and Safe Streets Act of 1968 Section 2516 (1).

[7] วิธีพิจารณาความอาญาของเยอรมนี § 100a II (StPO).

ความผิดตามกฎหมายต่อต้านอาชญากรรมระหว่างประเทศ และกลุ่มความผิดตามพระราชบัญญัติอาวุธ ฯลฯ เหล่านี้เป็นต้น

(3) ประเทศฝรั่งเศส รัฐบัญญัติเลขที่ 91–646 ว่าด้วยการการคุ้มครองความลับของการสื่อสารถึงกันทางโทรคมนาคม กำหนดประเภทความผิดไว้อย่างกว้าง ๆ โดยกำหนดว่าในคดีอาญาซึ่งมีโทษจำคุกขั้นต่ำตั้งแต่ 2 ปีขึ้นไป ผู้พิพากษาไต่สวนมีอำนาจที่จะสั่งให้ดักฟัง บันทึก และถ่ายเป็นลายลักษณ์อักษรซึ่งการติดต่อสื่อสารถึงกันทางโทรคมนาคมของบุคคลและควบคุมตรวจสอบการกระทำดังกล่าว

จากการศึกษาพบว่า การระบุฐานความผิดที่สามารถใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตที่ดีนั้นจะต้องทำให้กฎหมายมีขอบเขตที่ชัดเจนแน่นอน โดยควรกำหนดประเภทของฐานความผิดที่รัฐจะอนุญาตให้ดักฟังการสื่อสารทางอินเทอร์เน็ตเช่นเดียวกับวิธีพิจารณาความอาญาเยอรมนี ระบุฐานความผิดต่าง ๆ โดยพิจารณาถึงกฎหมายพิเศษที่ให้อำนาจในการดักฟังการกระทำความผิด หรือดักรับข้อมูลการกระทำความผิดในพระราชบัญญัติต่าง ๆ ที่มีอยู่ในปัจจุบันเข้ารวมไว้ท้ายประมวลกฎหมายวิธีพิจารณาความอาญา เป็นบัญชีท้ายประมวลกฎหมายวิธีพิจารณาความอาญา

3.3 ระยะเวลาบังคับใช้มาตรการและระยะเวลาสิ้นสุดของการใช้มาตรการ

(1) ประเทศสหรัฐอเมริกาตามกฎหมาย The Omnibus Crime Control and Safe Streets Act of 1968 กำหนดไว้ว่า ระยะเวลาในการดักฟังการกระทำความผิดนั้นศาลจะอนุญาตเกินกว่า 30 วันไม่ได้ หากมีความจำเป็นขอขยายได้อีกไม่เกิน 30 วัน

(2) ประเทศเยอรมนี วิธีพิจารณาความอาญาเยอรมนี มาตรา 100a StPO กำหนดระยะเวลาในการดักฟังการสนทนา ยาวนานที่สุดได้ไม่เกิน 3 เดือน การขยายกระทำได้อีกแต่ไม่เกิน 3 เดือน และในกรณีที่เหตุต่าง ๆ ตามฐานความผิดที่ระบุในมาตรา 100a ไม่มีต่อไปแล้วมาตรการนั้นย่อมตกไป และต้องแจ้งการยกเลิกใช้มาตรการให้ศาลทราบด้วย

(3) ประเทศฝรั่งเศส รัฐบัญญัติเลขที่ 91–646 ว่าด้วยการการคุ้มครองความลับของการสื่อสารถึงกันทางโทรคมนาคม กำหนดว่า การอนุญาตให้ทำการดักฟังการติดต่อสื่อสารทางโทรคมนาคมมีผลบังคับได้นานไม่เกิน 4 เดือน อย่างไรก็ตามการขยายระยะเวลาการอนุญาตย่อมกระทำได้ภายใต้แบบและเงื่อนไขเดิม แต่ทั้งนี้ต้องไม่เกินกว่า 4 เดือน

จากการศึกษาพบว่า ระยะเวลาตามที่กำหนดไว้ในกฎหมายต่างประเทศแม้จะมีความแตกต่างกันอยู่ตามที่แต่ละประเทศจะกำหนดขึ้นก็ตาม แต่ข้อสำคัญก็คือ กฎหมายมีกำหนดระยะเวลาสิ้นสุดไว้อย่างชัดเจน และควรที่จะให้เจ้าพนักงานผู้ขอใช้มาตรการรายงานเรื่องดังกล่าวเข้าสู่สำนวนคดีของศาลด้วย เพื่อให้ศาลสามารถตรวจสอบการใช้อำนาจของเจ้าพนักงานได้ เพื่อให้เป็นไปตามหลักการตรวจสอบภายนอกโดยองค์กรที่มีอิสระ

3.4 องค์กรผู้มีอำนาจอนุญาตให้ใช้มาตรการและองค์กรผู้มีหน้าที่ยื่นคำร้องขอในการใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ต

(1) ประเทศสหรัฐอเมริกา The Omnibus Crime Control and Safe Streets Act of 1968 มาตรา 2518 (1) กำหนดให้องค์กรที่มีอำนาจอนุญาตและพิจารณาคำร้องขอ ได้แก่ ศาลยุติธรรม ที่มีเขตอำนาจ ทั้งนี้ ผู้พิพากษาผู้พิจารณาคำร้องอาจเรียกให้ผู้ยื่นคำร้องแสดงพยานหลักฐานเพิ่มเติมในการพิจารณาสั่งคำร้องได้

(2) ประเทศเยอรมนี วิธีพิจารณาความอาญาเยอรมนีกำหนดว่า การใช้มาตรการดักและบันทึกการสื่อสารโทรคมนาคม โดยหลักกระทำได้แต่โดยคำสั่งศาลเท่านั้น กฎหมายพยายามให้องค์กรที่มีความเป็นอิสระและเป็นกลางเข้ามาควบคุมการใช้มาตรการบังคับทางอาญาโดย เหตุผลก็เนื่องมาจากมาตรการดังกล่าวเกิดขึ้นในทางลับโดยที่ผู้ได้รับผลกระทบจะไม่สามารถปัดป้องหรือขัดขวางไม่ให้การใช้มาตรการเกิดขึ้นได้เลย แต่กฎหมายก็ผ่อนคลายหลักไว้ด้วยว่าในกรณีจำเป็นเร่งด่วน พนักงานอัยการสามารถอนุญาตให้ใช้มาตรการดังกล่าวได้

(3) ประเทศฝรั่งเศส การดักฟังการติดต่อสื่อสารถึงกันทางโทรคมนาคมตามคำสั่งศาล[8] หรือเรียกว่า การดักฟังโดยอำนาจศาล (ecoute judiciares) และการดักฟังการติดต่อสื่อสารถึงกันทางโทรคมนาคมเพื่อการรักษาความมั่นคง เรียกว่า การดักฟังทางปกครอง (ecoute admistratives) โดยคำสั่งนายกรัฐมนตรี ต้องได้รับการตรวจสอบโดย “คณะกรรมการควบคุมการดักฟังการติดต่อสื่อสารถึงกันทางโทรคมนาคมแห่งชาติ”จัดตั้งขึ้นเพื่อควบคุมดูแลให้มีการปฏิบัติตามบทบัญญัติในบรรพ 2 ว่าด้วยการดักฟังการติดต่อสื่อสารถึงกันทางโทรคมนาคมอย่างเคร่งครัด

จากการศึกษาพบว่านอกจากการใช้มาตรการบางกรณีของประเทศฝรั่งเศสแล้ว อำนาจอนุญาตเป็นขององค์กรศาลยุติธรรม เมื่อเปรียบเทียบประเทศไทย พบว่า แม้กฎหมายของไทยจะให้อำนาจนี้เป็นอำนาจของศาลก็ตาม แต่ในส่วนของผู้มีอำนาจยื่นคำร้องขอกลับเป็นของเจ้าพนักงานตำรวจ หรือเจ้าพนักงานฝ่ายบริหารตามกฎหมายพิเศษต่าง ๆ ทำให้การของใช้มาตรการบังคับทางอาญาซึ่งอยู่ในขั้นตอนของการสอบสวนคดีก่อนฟ้องขาดการตรวจสอบกลั่นกรองโดยพนักงานอัยการ ส่งผลให้การคุ้มครองสิทธิและเสรีภาพของบุคคลที่เกี่ยวข้องถูกละเลยไป ดังนี้ ควรกำหนดให้หน้าที่ในการร้องขอใช้มาตรการเป็นอำนาจของพนักงานอัยการเพื่อเป็นการตรวจสอบถ่วงดุลการใช้อำนาจสอบสวนของพนักงานสอบสวน ขณะเดียวกันก็เป็นการคุ้มครองสิทธิและเสรีภาพของประชาชนไปพร้อมกันด้วย

3.5 ข้อยกเว้นอำนาจอนุญาตให้ใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตโดยศาล

(1) ประเทศสหรัฐอเมริกา กำหนดให้บางกรณีที่อาจมีความจำเป็นฉุกเฉินเร่งด่วน กฎหมายให้เจ้าพนักงานของรัฐสามารถทำการดักฟังการกระทำความผิดก่อน โดยหลังจากที่ได้มีการดักฟังการกระทำความผิด

[8] กมลชัย รัตนสกาววงศ์ และวรพจน์ วิศรุตพิชญ์, รายงานการศึกษาวิจัยแนวทางในการยกร่างกฎหมายที่เกี่ยวข้องกับการดักฟังทางโทรศัพท์และการปรับปรุงกฎหมายอื่น ๆ ที่เกี่ยวข้อง, (กรุงเทพฯ:สำนักงานคณะกรรมการวิจัยแห่งชาติ, 2540), น.92-94.

กรณีมีความจำเป็นฉุกเฉินเร่งด่วน เจ้าพนักงานจะต้องขออนุญาตต่อศาลภายใน 48 ชั่วโมง หลังจากเริ่มต้นทำการดักฟัง

(2) ประเทศเยอรมนี วิธีพิจารณาความอาญาเยอรมนี กำหนดให้พนักงานอัยการสามารถอนุญาตให้ใช้มาตรการดังกล่าวได้ หากภายใน 3 วัน ไม่ปรากฏคำสั่งอนุมัติจากศาลให้ดักการสื่อสารโทรคมนาคม ให้ถือว่าการอนุญาตของพนักงานอัยการเป็นอันสิ้นสุดลง

เมื่อศึกษาถึงเหตุอันเกิดจากความจำเป็นเร่งด่วนในการใช้มาตรการตามกฎหมายต่างประเทศแล้ว กรณีวิธีพิจารณาความอาญาของประเทศเยอรมนีกำหนดให้พนักงานอัยการสามารถอนุญาตให้ใช้มาตรการดังกล่าวไปก่อนได้ ถือได้ว่าเป็นแนวทางการแก้ปัญหาการลักลอบใช้มาตรการดักการสื่อสารทางอินเทอร์เน็ตของเจ้าพนักงานโดยการเพิ่มช่องทางให้เจ้าพนักงานสอบสวนสามารถร้องขอต่อพนักงานอัยการซึ่งรวดเร็วกว่าเพื่อให้เท่าทันต่อการปราบปรามการกระทำความผิดที่มีความซับซ้อนมากขึ้นในปัจจุบัน อย่างไรก็ตาม เนื่องจากระบบการพิจารณาคดีในศาลชั้นต้นไทย กำหนดให้การออกหมายอาญากระทำได้ตลอดเวลาไม่มีวันหยุดราชการเสาร์อาทิตย์ โดยผู้พิพากษาเวรสั่ง[9] ดังนั้น กรณีของข้อยกเว้นเพราะเหตุจำเป็นเร่งด่วนหรือเหตุฉุกเฉินอย่างยิ่งที่จะนำมาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตมาใช้ก่อนโดยไม่ต้องขออนุญาตจากศาลนั้นอย่างเช่นในกฎหมายต่างประเทศ จึงไม่มีความจำเป็นต้องบัญญัติไว้แต่อย่างใด

3.6 การทำลายข้อมูลที่ได้จากการดักฟังการสื่อสารทางอินเทอร์เน็ต

การทำลายข้อมูลในเป็นกรณีที่มีความจำเป็นอย่างมาก เพื่อลดปัญหาจากการนำข้อมูลไปใช้ในทางที่ผิด ในขณะเดียวกันก็เป็นการคุ้มครองสิทธิเสรีภาพและความลับของบุคคลที่ต้องถูกละเมิดไปเพื่อไม่ให้ต้องถูกกระทบกระเทือนไปโดยไม่มีที่สิ้นสุด โดยกฎหมายต่างประเทศมีการกำหนดหลักเกณฑ์และวิธีการที่แตกต่างกัน ดังนี้

(1) วิธีพิจารณาความอาญาเยอรมนีได้บัญญัติถึงการใช้และการเก็บรักษาข้อมูลที่ได้จากการใช้มาตรการดักและบันทึกการสื่อสารโทรคมนาคมไว้ในมาตรา 101 และ 101a StPO เป็น “กฎเกณฑ์ในการดำเนินการตามมาตรการที่กระทำโดยลับ” ข้อมูลส่วนบุคคลที่ได้มาจากการใช้มาตรการที่ไม่จำเป็นสำหรับการดำเนินคดีอาญาและการตรวจสอบการใช้มาตรการโดยศาลอีกต่อไปแล้ว กฎหมายกำหนดให้ “ลบเสียโดยไม่ชักช้า” โดยการลบจะต้องถูกบันทึกไว้เป็นลายลักษณ์อักษร

(2) รัฐบัญญัติเลขที่ 91–646 ว่าด้วยการคุ้มครองความลับของการสื่อสารถึงกันทางโทรคมนาคมของประเทศสาธารณรัฐฝรั่งเศส

(ก) การดักฟังการติดต่อสื่อสารถึงกันทางโทรคมนาคมตามคำสั่งศาล กำหนดให้อัยการสูงสุดหรือพนักงานอัยการควบคุมการ “ทำลาย” สิ่งบันทึกการติดต่อสื่อสารถึงกันทางโทรคมนาคมเมื่อคดีอาญานั้นหมดอายุความฟ้องร้องแล้วและให้จัดทำบันทึกการทำลายไว้ด้วย

---

[9] ข้อบังคับประธานศาลฎีกาว่าด้วยหลักเกณฑ์และวิธีการเกี่ยวกับการออกคำสั่งหรือออกหมายอาญา พ.ศ.2548 เรื่อง การร้องขอให้ออกหมายนอกเวลาทำการปกติ ,ประกอบระเบียบคณะกรรมการบริหารศาลยุติธรรมว่าด้วยการจ่ายเงินค่าตอบแทนการปฏิบัติงานนอกเวลาราชการ พ.ศ.2545.

(ข) การดักฟังการติดต่อสื่อสารถึงกันทางโทรคมนาคมเพื่อการรักษาความมั่นคง นายกรัฐมนตรีต้องควบคุมดูแลให้มีการจัดทำรายงานการดักฟังและบันทึกการติดต่อสื่อสารถึงกันทางโทรคมนาคมแต่ละครั้ง โดยให้มีการ “ทำลาย” สิ่งบันทึกการติดต่อสื่อสารถึงกันทางโทรคมนาคมเสียภายใน 10 วัน นับแต่วันที่ได้ทำการบันทึกเป็นอย่างช้า

จากการศึกษาพบว่า ประเทศไทยควรนำหลักการทำลายข้อมูลมาใช้ เพื่อคุ้มครองสิทธิเสรีภาพและความลับของบุคคลที่ต้องถูกละเมิดไป ทั้งนี้ควรกำหนดให้การทำลายข้อมูลนี้อยู่ภายใต้ดุลพินิจของศาลในการพิจารณาถึงความสำคัญของข้อมูล โดยควรกำหนดระยะเวลาให้ข้อมูลส่วนบุคคลที่ได้มาจากการใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตที่ไม่จำเป็นสำหรับการดำเนินคดีอาญาและการตรวจสอบการใช้มาตรการโดยศาลอีกต่อไปแล้ว กฎหมายกำหนดให้ “ลบเสียโดยไม่ชักช้า” เพื่อเป็นการคุ้มครองสิทธิเสรีภาพและความลับของบุคคลที่ต้องถูกละเมิดไปจากการใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ต

3.7 ผลกระทบต่อบุคคลภายนอกเกี่ยวกับการดักฟังการสื่อสารทางอินเทอร์เน็ต

มีเพียงประเทศสหพันธ์สาธารณรัฐเยอรมนีเท่านั้นที่คุ้มครองบุคคลภายนอกไว้ โดยมุ่งคุ้มครองสิทธิและเสรีภาพของบุคคลอย่างแท้จริง เนื่องจากการใช้มาตรการบังคับในการดักการสื่อสารทางอินเทอร์เน็ตนั้น ผู้ถูกผลกระทบจากการใช้มาตรการดังกล่าวจะไม่มีทางรู้ตัวได้เลยว่าเสรีภาพของเขาในการติดต่อสื่อสารและสิทธิในความเป็นส่วนตัวได้ถูกละเมิดโดยรัฐ เพราะฉะนั้นรัฐจึงมีหน้าที่ต้องคัดแยกเนื้อหาของข้อมูลเพื่อแล้วแจ้งข้อมูลดังกล่าวกลับไปยังผู้ที่ได้รับผลกระทบทั้งหมด โดยกฎหมายกำหนดว่า ข้อมูลที่ได้จากการดักการสื่อสารโทรคมนาคมบางประเภทนั้นแม้จะได้มาพร้อมกับการใช้มาตรการแต่รัฐก็ไม่สามารถจะนำมาใช้เป็นพยานหลักฐานได้ หากเป็นข้อมูลเกี่ยวกับ “แกนกลางของการใช้ชีวิตส่วนตัว” และจะต้องถูกลบไปโดยไม่ชักช้าอีกด้วย ทั้งนี้ ข้อมูลที่เกี่ยวกับแกนกลางของการใช้ชีวิตส่วนตัว (Core area of private living) ได้แก่ ข้อมูลที่ได้จากการสนทนาระหว่างผู้ที่ถูกกระทบสิทธิกับสมาชิกในครอบครัว ผู้ให้คำปรึกษาทางโทรศัพท์ ทนายความ หรือแพทย์ เป็นต้น

จากการศึกษาเห็นว่าการบัญญัติให้มาตรการดักฟังการสื่อสารโทรคมนาคมเป็นมาตรการบังคับตามกฎหมายวิธีพิจารณาความอาญาควรจะได้นำหลักการแจ้งผู้ที่ได้รับผลกระทบต่อการใช้มาตรการได้ทราบถึงสิทธิและเสรีภาพที่ตัวเขาเองนั้นถูกละเมิดเพื่อเปิดโอกาสให้ผู้ที่ถูกกระทบสิทธิสามารถปกป้องตนเองจากการถูกละเมิดสิทธิได้ แต่ทั้งนี้กฎหมายควรกำหนดให้เป็นดุลพินิจของศาลที่จะพิจารณาว่าการถูกกระทบสิทธินั้นจะเป็นเรื่องเล็กน้อย หรือเป็นเรื่องกรณีจำเป็นต้องแจ้ง เพื่อไม่ให้เป็นการเพิ่มกระบวนพิจารณาคดีในศาลโดยใช่เหตุ

3.8 ความรับผิดทางอาญาเกี่ยวกับการได้มาโดยมิชอบซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน

พบว่าในกฎหมายต่างประเทศได้มีการกำหนดบทลงโทษเจ้าหน้าที่ของรัฐที่ใช้มาตรการบังคับทางอาญาที่ไม่ชอบด้วยกฎหมายเอาไว้ทั้งที่เป็นโทษทางอาญา และบทลงโทษในเชิงพยานหลักฐานที่ทำให้ข้อมูลที่ได้มาจากการใช้บังคับมาตรการโดยไม่ชอบไม่อาจนำมาใช้เป็นพยานหลักฐานในการพิจารณาพิพากษาคดีได้ดังนี้

(1) ประเทศสหรัฐอเมริกา The Omnibus Crime Control and Safe Streets Act of 1968 กำหนดบทลงโทษสำหรับผู้ดักฟังการกระทำความผิดโดยไม่ชอบ โดยกำหนดโทษผู้ดักฟังการสื่อสารโทรคมนาคมหรือการเข้าถึงข้อมูลอิเล็กทรอนิกส์โดยปราศจากอำนาจไว้ใน ประมวลกฎหมายสหรัฐ ภาค 18 มาตรา 2511 (Interception ad Disclosure of Wire, Oral, or Electronic Communications) อาจถูกระวางโทษจำคุก 5 ปี สำหรับความผิดครั้งแรก และในประมวลกฎหมายสหรัฐภาค 18 มาตรา 2701 (Unlawful Access to Stored Communication) ก็ได้กำหนดให้การกระทำเช่นว่านี้มีโทษทางอาญาด้วยเช่นกัน มีข้อสังเกตว่าในส่วนของการรับฟังพยานหลักฐานที่ได้มาจากการดักฟังการกระทำความผิดโดยมิชอบนั้นข้อมูลที่ได้มาจะถูกห้ามมิให้ใช้เป็นพยานหลักฐานในศาล กล่าวคือ เป็นบทตัดพยาน (Exclusionary Rules) และพยานหลักฐานที่ได้มาจากการดังฟังดังกล่าวก็ห้ามรับฟังเป็นพยานหลักฐานด้วยเช่นกัน

(2) ความรับผิดทางอาญาเกี่ยวกับการได้มาโดยมิชอบซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน บัญญัติไว้ในประมวลกฎหมายอาญาเยอรมนี (Strafgesetzbuch – StGB) ลักษณะที่ 15 ว่าด้วยการล่วงละเมิดพื้นที่ในการใช้ชีวิตส่วนตัวและในความลับ มาตรา 201 ถึง 210 โดยความผิดฐานล่วงล้ำความเป็นส่วนตัวของคำพูดตามมาตรา 201 ดังนั้นในกรณีที่ผู้กระทำมีอำนาจตามกฎหมาย อาทิกฎหมายวิธีพิจารณาความอาญาที่ให้อำนาจเจ้าพนักงานดักการสื่อสารโทรคมนาคมได้ การกระทำจึงไม่เป็นความผิด

ความรับผิดต่อการละเมิดสิทธิความเป็นส่วนตัวนั้นตามประมวลกฎหมายอาญาของไทยยังไม่มีบัญญัติไว้เป็นฐานความผิด แต่กฎหมายต่างประเทศต่างก็ให้ความสำคัญกับเรื่องนี้เป็นอย่างมาก ทั้งนี้ เพื่อให้บทกำหนดโทษฐานละเมิดต่อสิทธิความเป็นส่วนตัว และเสรีภาพในการติดต่อสื่อสารได้รับความคุ้มครองสูงสุดจากการกระทำโดยไม่ชอบด้วยกฎหมาย เพื่อเป็นการป้องปรามมิให้เจ้าพนักงานใช้ดุลพินิจโดยขาดหลักเกณฑ์ และไม่เป็นไปตามเงื่อนไขของกฎหมายอีกด้วย

3.9 กระบวนการเผยแพร่และจัดทำรายงานสรุปผลการใช้มาตรการดักฟังการสื่อสารโทรคมนาคม

ในหัวข้อสุดท้ายนี้จะได้กล่าวถึงกระบวนการในการตรวจสอบการทำงานของเจ้าพนักงานของรัฐในการบังคับใช้กฎหมาย โดยการเปิดเผยข้อมูลดังกล่าวต่อสาธารณชนเพื่อให้ทราบถึงรายละเอียดต่าง ๆ ในรอบปีที่มีการบังคับใช้กฎหมาย จำนวนครั้ง และประเภทของวิธีการ ดังนี้

วิธีพิจารณาความอาญาเยอรมนีกำหนดขั้นตอนสำคัญ โดยให้มลรัฐและอัยการสูงสุดแห่งสหพันธรัฐต้องรายงานเกี่ยวกับการใช้มาตรการตาม มาตรา 100a (StPO) ของหน่วยงานหรือในความรับผิดชอบของตน รายงานต่อสำนักงานกระทรวงยุติธรรมแห่งสหพันธรัฐในทุกปีปฏิทินในแต่ละปี จนถึงวันที่ 30 มิถุนายนของปีถัดจากปีที่รายงาน โดยกฎหมายกำหนดให้สำนักงานกระทรวงยุติธรรมแห่งสหพันธรัฐจัดทำบทสรุปของการใช้มาตรการตามคำสั่งดังกล่าวทั่วทั้งสหพันธรัฐในปีที่จัดทำรายงานและเผยแพร่ข้อมูลดังกล่าวนี้บนอินเทอร์เน็ต[10] รายงานนี้จะต้องระบุถึง จำนวนขั้นตอนและวิธีการในการใช้มาตรการดังฟังการสื่อสารโทรคมนาคมตามมาตรา 100a (StPO) จำนวนคำสั่งในการดักฟังการสื่อสารโทรคมนาคม แยกระหว่าง ก) คำสั่ง

[10] วิธีพิจารณาความอาญาของเยอรมนี § 100b (5)(StPO).

แรกและคำสั่งที่มีการขยายระยะเวลา และ ข) การสื่อสารทางโทรศัพท์ โทรศัพท์เคลื่อนที่ และบนอินเทอร์เน็ต และในประการสุดท้าย รายงานจะต้องระบุถึงการกระทำความผิดอาญาพื้นฐานในแต่ละกรณี ตามรายการที่ระบุไว้ในมาตรา มาตรา 100a (2)(StPO) อีกด้วย[11]

หลักการนี้ควรนำมาใช้เพื่อสร้างหลักการใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตของประเทศไทย เพื่อทำให้การใช้มาตรการดังกล่าวเป็นไปอย่างเปิดเผย โดยบัญญัติให้ “มีการเปิดเผยถึงจำนวนการใช้มาตรการดักฟังการสื่อสารโทรคมนาคมและวิธีการ รวมทั้งฐานความผิดที่นำมาตรการดังกล่าวมาใช้ โดยให้อัยการสูงสุดต้องรายงานเกี่ยวกับการใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตของหน่วยงานหรือในความรับผิดชอบของตน รายงานต่อกระทรวงยุติธรรม ในทุกปีปฏิทินในแต่ละปี จนถึงวันที่ 30 กันยายนของปีถัดจากปีที่รายงาน” โดยให้กระทรวงยุติธรรมจัดทำบทสรุปของการใช้มาตรการตามคำสั่งดังกล่าวทั่วทั้งประเทศในปีที่จัดทำรายงานและเผยแพร่ข้อมูลดังกล่าวนี้บนอินเทอร์เน็ต เพื่อให้ประชาชนทั่วไปได้ทราบ ทั้งนี้ ผลที่ได้จากกระบวนการนี้คือ ทำให้เจ้าพนักงานที่เกี่ยวข้องกับการใช้มาตรการต้องมีการกลั่นกรองเหตุที่จะร้องขอใช้มาตรการอย่างรอบคอบ อีกทั้งย่อมส่งผลให้สิทธิและเสรีภาพของบุคคลต่อการใช้มาตรการได้รับความคุ้มครองตรวจสอบถึงการบังคับใช้กฎหมายของเจ้าพนักงานภายหลังการปฏิบัติหน้าที่ไปแล้วอีกด้วย

4.บทสรุปและข้อเสนอแนะ

โดยสรุปปัญหาของมาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตของประเทศไทยที่มีในปัจจุบันในประการแรกนั้น ประเทศไทยไม่มีบทบัญญัติโดยตรงที่ให้อำนาจเจ้าพนักงานในการใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ต ปัญหาประการต่อมาคือ กฎหมายที่ให้อำนาจแก่เจ้าพนักงานที่มีอยู่ในประเทศไทยมีเพียงกฎหมายที่กำหนดหลักเกณฑ์การดักฟังหรือดักรับข้อมูลการสื่อสารโทรคมนาคมเป็นการทั่วไปตามพระราชบัญญัติต่าง ๆ มีลักษณะเป็นเพียง บทกฎหมายเฉพาะ (Jus special) ไม่อาจนำมาปรับใช้กับข้อเท็จจริงที่เกิดขึ้นได้ในทุกกรณีและไม่มีพระราชบัญญัติที่ใช้บังคับอยู่ในประเทศไทยฉบับใดเลยที่ให้อำนาจเจ้าพนักงานในการดักฟังการสื่อสารทางอินเทอร์เน็ตไว้โดยตรง ซึ่งในทางสากลการดักฟังการสื่อสารทางโทรคมนาคมโดยเฉพาะอย่างยิ่งการสื่อสารทางอินเทอร์เน็ตนั้นจะบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาเนื่องจากเป็นกฎหมายที่มีฐานะเป็น บทบัญญัติทั่วไป (Jus generale) อาทิ ประเทศสหพันธ์สาธารณรัฐเยอรมนีนำหลักการสำคัญเกี่ยวกับมาตรการบังคับทางอาญาที่การบังคับใช้มีผลกระทบต่อสิทธิและเสรีภาพของประชาชนเกี่ยวกับการดักฟังการสื่อสารทางโทรคมนาคมซึ่งมีการแก้ไขเพิ่มเติมให้เจ้าพนักงานมีอำนาจดักฟังการสื่อสารทางอินเทอร์เน็ตมาบัญญัติไว้ในกฎหมายวิธีพิจารณาความอาญา เพื่อให้หลักเกณฑ์ที่สำคัญในการบังคับใช้กฎหมาย และเพื่อให้แนวทางปฏิบัติและการตีความของศาลที่เกี่ยวข้องกันนั้นได้รับการตีความ การวางแนวทางไปด้วยกันอย่างมีเอกภาพ

[11] วิธีพิจารณาความอาญาของเยอรมนี § 100b (6)(StPO).

จากการศึกษาผู้เขียนเสนอแนะการนำหลักกฎหมายต่างประเทศมาสร้างหลักกฎหมายเรื่องมาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตที่มีความเป็นภาวะวิสัย (Objectivity) ดังนี้

1.เงื่อนไขการใช้มาตรการ เพื่อให้การขอใช้มาตรการสามารถคุ้มครองสิทธิและเสรีภาพของบุคคลที่เกี่ยวข้องในการใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ต นอกจากหลักสำคัญที่ว่าเมื่อไม่สามารถรวบรวมพยานหลักฐานได้โดยวิธีการตามปกติแล้ว ควรกำหนดว่า “ต้องปรากฏความสงสัยว่ามีการกระทำความผิดอาญาเกิดขึ้น” (Initial suspicion) ทั้งนี้ เพื่อให้ศาลได้พิจารณาถึงมูลเหตุที่แท้จริงในการขอใช้มาตรการ

2.ฐานความผิด กฎหมายควรบัญญัติระบุฐานความผิดเป็นรายมาตราไว้ในกฎหมาย โดยคำนึงถึงความร้ายแรงแห่งฐานความผิดต่าง ๆ ที่จะต้องเป็นความผิดที่กระทบต่อความมั่นคง หรือสังคมโดยส่วนรวมอย่างมากในวงกว้าง ทั้งนี้เพื่อเกิดความชัดเจนแน่นอนในเงื่อนไขของบทบัญญัติ และลดการใช้ดุลพินิจอย่างกว้างขวางของเจ้าพนักงาน เพื่อคุ้มครองสิทธิและเสรีภาพของบุคคลที่ได้รับผลกระทบ

ทั้งนี้ ควรพิจารณาถึงกฎหมายพิเศษต่าง ๆ ที่เกี่ยวข้องกับการให้อำนาจเจ้าพนักงานในการดักฟังหรือดักรับข้อมูลการกระทำความผิดหรือต่อการติดต่อสื่อสารตามพระราชบัญญัติซึ่งเป็นกฎหมายพิเศษที่มีอยู่ในปัจจุบันนำเข้ารวมไว้ท้ายประมวลกฎหมายวิธีพิจารณาความอาญา ในรูปของ**บัญชีแนบท้าย**ประมวลกฎหมายวิธีพิจารณาความอาญา เพื่อให้มาตรการนี้เป็นหลักเกณฑ์กลางในการใช้มาตรการดักฟังการสื่อสารโทรคมนาคมที่ครอบคลุมพฤติการณ์แห่งคดีอย่างแท้จริง

3.กฎหมายจะต้องกำหนดระยะเวลาในการใช้มาตรการไว้ให้มีความชัดเจนและแน่นอน ทั้งนี้จะต้องมีระยะสูงสุดในการบังคับใช้มาตรการ ควรกำหนด **หลัก** ว่า ให้ศาลมีคำสั่งอนุญาตในการใช้มาตรการนี้เพียงเท่าที่จำเป็นในการแสวงหาพยานหลักฐานเท่านั้น แต่ไม่เกินกว่า 15 วัน โดยกำหนดให้การขอขยายระยะเวลาเป็น**ข้อยกเว้น**ว่า การขอขยายระยะเวลาต้องยื่นคำร้องขอต่อศาลเพื่อให้ศาลพิจารณาถึงเหตุผลและความจำเป็นในการใช้มาตรการเป็นรายครั้ง โดยขยายได้ครั้งละไม่เกิน 15 วัน ทั้งนี้รวมแล้วสูงสุดต้องไม่เกินกว่า 90 วัน อันเป็นระยะเวลาที่เป็นไปตามหลักสากลของกฎหมายต่างประเทศ

4.กฎหมายควรกำหนดถึงการยกเลิกหรือการสิ้นสุดในการใช้มาตรการไว้ด้วย เช่นเดียวกับประเทศเยอรมนี และประเทศสหรัฐอเมริกา เพื่อคุ้มครองสิทธิและเสรีภาพของบุคคลที่อาจต้องเข้ามาเกี่ยวข้องกับการใช้มาตรการให้หลุดพ้นจากมาตรการดังกล่าวไปโดยเร็วที่สุด โดยควรบัญญัติว่า หากเงื่อนไขในการออกคำสั่งอนุญาตให้ใช้มาตรการหมดสิ้นไป ให้มาตรการนั้นสิ้นสุดลงโดยไม่ชักช้า ทั้งนี้ ให้เจ้าพนักงานแจ้งเหตุแห่งการสิ้นสุดไปยังศาลที่อนุญาตโดยทันที

5.ประเทศไทยควรกำหนดให้ผู้มีอำนาจยื่นคำร้องขอต่อศาลในการขอใช้มาตรการเป็นอำนาจของ “พนักงานอัยการที่มีเขตอำนาจ” เนื่องจากการดักฟังการสื่อสารทางอินเทอร์เน็ตเป็นมาตรการบังคับทางอาญาที่ละเมิดต่อสิทธิเสรีภาพของบุคคลเป็นการใช้มาตรการเป็นการกระทำโดยลับ โดยให้เป็นอำนาจของพนักงานอัยการเป็นผู้ยื่นคำร้องขอใช้มาตรการ ไม่ว่าในการสอบสวนเบื้องต้นนั้นเป็นกระทำโดยพนักงานสอบสวนใดก็ตาม เพื่อให้เกิด การตรวจสอบภายนอก (Accountability) โดยองค์กรอัยการเพื่อถ่วงดุลการใช้ดุลพินิจของเจ้าพนักงานฝ่ายสืบสวนสอบสวน

6.หลักการของการบังคับใช้มาตรการบังคับทางอาญา (Compulsory Measures) ไม่ว่าจะเป็นกฎหมายต่างประเทศและของประเทศไทย ผู้มีอำนาจอนุญาตให้ใช้มาตรการคือ ศาล ซึ่งถือว่าเป็นองค์ที่มีความเป็นอิสระแยกต่างหากจากฝ่ายบริหารสามารถพิจารณาโดยใช้ดุลพินิจในการอนุมัติให้ใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ต

7.ข้อยกเว้นอำนาจอนุญาตให้ใช้มาตรการ จากการศึกษาพบว่า ประเทศสหรัฐอเมริกาและประเทศเยอรมนี กำหนดให้หากมีพฤติการณ์ฉุกเฉิน หรือมีความจำเป็นเร่งด่วนในการจะต้องใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตแล้ว กฎหมายอนุญาตให้เป็นอำนาจของพนักงานสอบสวน หรือพนักงานอัยการที่จะอนุญาตให้ใช้มาตรการไปก่อน เพื่อขอคำสั่งศาลในภายหลังได้

แต่เนื่องจากประเทศไทยมีระบบการบริหารจัดการคดีโดยสำนักงานศาลยุติธรรมได้กำหนดให้มี “ผู้พิพากษาเวรสั่ง” ที่สามารถออกหมายอาญาได้ตลอดเวลาโดยไม่มีวันหยุดราชการเสาร์อาทิตย์อย่างเช่นในต่างประเทศ ดังนั้น ข้อยกเว้นเพราะเหตุจำเป็นเร่งด่วนหรือเหตุฉุกเฉินอย่างยิ่งที่จะนำมาตรการดักฟังการสื่อสารทางอินเทอร์เน็ตมาใช้ก่อนโดยไม่ต้องขออนุญาตจากศาลนั้นอย่างในกฎหมายต่างประเทศ จึงอาจไม่มีความจำเป็นต้องบัญญัติไว้แต่อย่างใด

8.ควรกำหนดให้มีการทำลายข้อมูลที่ได้มาจากการใช้มาตรการ หากข้อมูลที่เป็นเนื้อหาของข้อมูลโดยแท้นั้นเป็น ข้อมูลส่วนบุคคลที่มีลักษณะเป็นแกนกลางของการใช้ชีวิตส่วนตัว ทั้งนี้ ข้อมูลที่ไม่มีความจำเป็นสำหรับดำเนินคดีอาญาไม่ว่าจะเป็นข้อมูลส่วนบุคคลหรือไม่ ต้องได้รับการตรวจสอบโดยศาล และให้ศาลมีคำสั่งให้ลบเสียโดยไม่ชักช้า ควรกำหนดว่า หากข้อมูลที่ได้มานั้นเป็นข้อมูลส่วนบุคคลและศาลได้พิจารณาแล้วว่าไม่มีความจำเป็นสำหรับใช้ดำเนินคดีอาญา ให้ศาลมีคำสั่งให้ลบข้อมูลนั้นเสียโดยทันที

9.ควรกำหนดให้ความคุ้มครองผลกระทบที่มีต่อบุคคลภายนอกที่ต้องเข้ามาเกี่ยวข้องกับการใช้มาตรการดักฟังการสื่อสารทางอินเทอร์เน็ต ให้มีการแจ้งต่อศาลว่าการใช้มาตรการทำให้มีผู้ได้รับผลกระทบจากการใช้มาตรการ และให้บุคคลเช่นว่านี้อาจโต้แย้งปกป้องสิทธิของตนต่อศาล ศาลจะพิจารณาว่าการถูกกระทบสิทธินั้นเป็นเรื่องเล็กน้อย หรือเป็นกรณีจำเป็นที่จะต้องแจ้งเรื่องดังกล่าวต่อบุคคลภายนอก เพื่อไม่เป็นการเพิ่มกระบวนการพิจารณาคดีในศาลโดยใช่เหตุ

10.ควรกำหนดความรับผิดทางอาญาเกี่ยวกับการได้มาโดยไม่ชอบซึ่งข้อมูลที่บุคคลสื่อสารถึงกันจากการกระทำในการใช้มาตรการที่ปราศจากอำนาจ ควรกำหนดความรับผิดทางอาญาต่อการละเมิดสิทธิในความเป็นส่วนตัวไว้เป็นฐานความผิดด้วย เพื่อให้บทบัญญัตินี้ช่วยในการป้องปรามมิให้เจ้าพนักงานใช้ดุลพินิจโดยขาดหลักเกณฑ์และเงื่อนไขของกฎหมาย

11.ควรกำหนดให้มีกระบวนการเผยแพร่และจัดทำรายงานสรุปผลการใช้มาตรการดักฟังการสื่อสารทางโทรคมนาคม โดยกำหนดให้กระทรวงยุติธรรมจัดทำบทสรุปของการใช้มาตรการตามคำสั่งดังกล่าวทั่วทั้งประเทศในปีที่จัดทำรายงานและเผยแพร่ข้อมูลดังกล่าวนี้บนอินเทอร์เน็ต เพื่อให้ประชาชนทั่วไปได้ทราบ และต้องทำให้กระบวนการเข้าถึงนั้นเปิดเผย ทั้งนี้ เพื่อสร้างความน่าเชื่อถือในการบังคับใช้กฎหมายของกระบวนการยุติธรรมทางอาญาของไทยให้เกิดความโปร่งใส

บรรณานุกรม

ภาษาไทย

หนังสือ

คณิต ณ นคร. กฎหมายวิธีพิจารณาความอาญา.(พิมพ์ครั้งที่ 8).(กรุงเทพมหานคร:สำนักพิมพ์วิญญูชน.2555).

ปรีดี เกษมทรัพย์. กฎหมายแพ่ง:หลักทั่วไป. (พิมพ์ครั้งที่ 5).(กรุงเทพมหานคร:ห้างหุ้นส่วนจำกัดภาพพิมพ์, 2526)

ณรงค์ ใจหาญ. หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1. (พิมพ์ครั้งที่ 12).(กรุงเทพมหานคร:สำนักพิมพ์วิญญูชน, 2556)

เอกสารอื่น ๆ

กรรภิรมย์ โกมลารชุน. (2561). กฎหมายเกี่ยวกับการให้รัฐเข้าถึงและได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน: กรณีศึกษาสหพันธรัฐเยอรมนี. รายงานวิจัยฉบับสมบูรณ์ สำนักส่งเสริมวิชาการรัฐสภา สถาบันพระปกเกล้า.

กมลชัย รัตนสกาววงศ์ และวรพจน์ วิศรุตพิชญ์. (2540). เรื่องแนวทางในการยกร่างกฎหมายที่เกี่ยวข้องกับการดักฟังทางโทรศัพท์และการปรับปรุงกฎหมายอื่น ๆ ที่เกี่ยวข้อง. (รายงานผลการวิจัย) สำนักงานคณะกรรมการวิจัยแห่งชาติ.