# มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของผู้ถูกดักฟังการสื่อสารข้อมูล

*ผศ. คณาธิป ทองรวีวงศ์* [1]

## ▣ บทนำ

การดักฟังเป็นพฤติกรรมการแสวงหาข้อมูลข่าวสารชนิดหนึ่งซึ่งเป็นการล่วงละเมิดต่อสิทธิในความเป็นอยู่ส่วนตัว (Right of privacy) ในการสื่อสารข้อมูล เนื่องจากเป็นการเก็บข้อมูลการสนทนาระหว่างผู้อื่นโดยมิได้รับความยินยอม ยิ่งไปกว่านั้นผู้ถูกดักฟังอาจมิได้รับรู้ว่ามีการเก็บข้อมูลการสนทนาของตน การดักฟังเกิดขึ้นมาเป็นเวลายาวนานในหลายประเทศ ในระบบกฎหมายคอมมอนลอว์ของประเทศอังกฤษ การลักลอบฟัง (Eavesdropping) ถือเป็นความผิดเกี่ยวกับการรบกวน (Nuisance) สำหรับความหมายของการลักลอบฟังนั้น William Blackstone[2] นิยามว่าหมายถึง การลอบฟังทางกำแพง หน้าต่าง หรือช่องทางต่าง ๆของบ้าน แต่เดิมการดักฟังเป็นการลักลอบฟังการสนทนาทางวาจา ซึ่งบุคคลสามารถหลีกเลี่ยงการดักฟังโดยตรวจสอบว่าไม่มีผู้ใดลอบฟังอยู่ อย่างไรก็ตามเมื่อเทคโนโลยีการสื่อสารพัฒนาขึ้น การดักฟังจึงเปลี่ยนรูปแบบไปตามช่องทางการสื่อสาร ในปี ค.ศ. 1961 ศาลสูงสุดสหรัฐอเมริกาได้อธิบายถึงการกระทำการดักฟังโดยจำแนกความแตกต่างระหว่างพฤติกรรมการดักฟังสองประเภท[3] ได้แก่ (1) การกระทำการดักฟังซึ่งกระทำต่อระบบการสื่อสาร เช่น การดักฟังโทรศัพท์ (Wiretap) (2) การดักฟังการสื่อสารที่กระทำทางกายภาพในลักษณะเดียวกับการ

---

[1] *ผู้ช่วยศาสตราจารย์ประจำคณะนิติศาสตร์, คณบดีคณะนิติศาสตร์ มหาวิทยาลัยเซนต์จอห์น*

[2] *Blackstone, William, Commentaries on the Law of England (1769)*

[3] *Silverman v. United States - 365 U.S. 505 (1961)*

ซ่อนตัวเพื่อแอบฟังการสนทนาในสถานที่ต่าง ๆ[4] (eavesdrop หรือ overhear) การดักฟังลักษณะนี้อาจจำแนกได้อีกสองกรณี คือ การดักฟังที่มีการบุกรุกทางกายภาพ (Eavesdrop accomplished by physical intrusion) และ การดักฟังที่ใช้วิธีการทางอิเล็กทรอนิกส์ (Eavesdrop accomplished by electronic means) ต่อมาในปี ค.ศ. 1967 ศาลมลรัฐ New York ได้จำแนกความประเภทการดักฟังไวสองประเภท[5] ได้แก่ (1) การดักฟังโทรศัพท์หรืออุปกรณ์สื่อสารโดยใช้สาย (Wiretap) เช่น โทรศัพท์ (2) การดักฟังโดยอุปกรณ์อิเล็กทรอนิกส์ที่ไม่ใช้สาย หรือที่เรียกว่า “Bugs” เช่น เครื่องมือขนาดเล็กซึ่งนำไปติดตั้งไว้ในสถานที่ต่าง ๆ

ในปัจจุบันการการสื่อสารในลักษณะไร้สาย (Wireless) แพร่หลายมากขึ้น รวมทั้งพัฒนาการของเทคโนโลยีสารสนเทศทำให้พฤติกรรมการสื่อสารของมนุษย์เปลี่ยนแปลงไป นอกจากการสื่อสารโดยการสนทนาเฉพาะหน้าและโทรศัพท์ที่ใช้สายแล้ว ยังมีการสื่อสารทางเครือข่ายไร้สาย[6] และทางอิเล็กทรอนิกส์มากขึ้น เช่น การสนทนาด้วยการพิมพ์ข้อความ (Texting) ผ่านทางโปรแกรมประยุกต์เพื่อการสนทนาทางโทรศัพท์เคลื่อนที่หรือคอมพิวเตอร์แบบพกพาซึ่งเชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ต การสื่อสารด้วยการส่งข้อความเสียง (Voice mail หรือ Voice message) ข้อความสั้น (Short Message Service หรือ SMS) จดหมายอิเล็กทรอนิกส์ (Electronic mail) การสื่อสารเหล่านี้อาจถูกดักรับข้อมูลได้[7] จะเห็นได้ว่าในปัจจุบันการเข้าไปรับรู้ข้อมูลการสื่อสารของผู้อื่นไม่จำกัดเฉพาะการ “ดักฟัง” แต่รวมถึงการ “ดักรับข้อมูล” การสื่อสารช่องทางต่าง ๆ ด้วย

ดังนั้นผู้เขียนเห็นว่าการดักฟังอาจจำแนกได้สามประเภทดังนี้ (1) การดักฟังการสนทนาด้วยวาจาระหว่างบุคคลที่สื่อสารกันเฉพาะหน้าทางกายภาพ ซึ่งเป็นพฤติกรรมอันมีลักษณะของการดักฟังทางกายภาพ (Eavesdrop) อันอาจจำแนกเป็นกรณีการดักฟังโดยมิได้ใช้อุปกรณ์ใด ๆ ช่วย เช่น การที่บุคคลหนึ่งลอบฟังการสนทนาของผู้อื่น และกรณีการดักฟังโดยใช้อุปกรณ์อิเล็กทรอนิกส์ เช่น การติดตั้งเครื่องดักฟังซ่อนไว้ (2) การดักฟังการสนทนาด้วยวาจาระหว่างบุคคลที่สื่อสารกันทางโทรศัพท์ อาจแยกได้เป็นการดักฟังการสนทนาทางโทรศัพท์ที่ใช้สาย (Wiretap) และการดักฟังการสนทนาทางอิเล็กทรอนิกส์ ซึ่งไม่ใช้

---

[4] *“All that was heard through the microphone was what an eavesdropper, hidden in the hall, the bedroom, or the closet, might have heard”*

[5] *Berger v. New York - 388 U.S. 41 (1967)*

[6] *Matthew, Bierlein, Policing the Wireless World : Access Liability in the Open Wi-Fi Era, Ohio State Law Journal, 2006.*

[7] *Smith, Robert Ellis, Ben Franklin’s Web Site : Privacy and Curiosity from Plymouth Rock to the Internet (2000)*

สาย (Wireless) เช่น ดักฟังการสนทนาทางโทรศัพท์เคลื่อนที่[8] (3) การดักรับข้อมูลการสนทนาทางสื่ออิเล็กทรอนิกส์ เช่น การสื่อสารทางคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ต

หากพิจารณาจากตัวบุคคลผู้กระทำการดักฟังอาจจำแนกได้เป็นสองประเภทคือ (1) การดักฟังที่กระทำโดยเจ้าหน้าที่รัฐ เจ้าหน้าที่ของรัฐอาจทำการดักฟังการสื่อสารของบุคคล ซึ่งส่วนมากจะเป็นการกระทำที่มีวัตถุประสงค์เพื่อแสวงหาพยานหลักฐานในการดำเนินคดี หรือกระทำเพื่อเหตุผลด้านความมั่นคงของรัฐ (2) การดักฟังที่กระทำโดยเอกชนหรือบุคคลทั่วไป ซึ่งอาจทำการดักฟังการสื่อสารของผู้อื่นด้วยวัตถุประสงค์ต่าง ๆ เช่น วัตถุประสงค์ทางการค้า วัตถุประสงค์ในเชิงความสัมพันธ์ส่วนบุคคล วัตถุประสงค์เพื่อการประกอบอาชญากรรม นอกจากเอกชนทั่วไปยังมีการกระทำของสื่อมวลชนเพื่อการแสวงหาข้อมูลข่าวสาร[9] การดักฟังหรือดักรับข้อมูลทางสื่ออิเล็กทรอนิกส์ต่าง ๆที่เกิดขึ้นทั่วไปในปัจจุบันอาจเป็นการกระทำของเอกชนซึ่งมิได้มีวัตถุประสงค์ใด เป็นเพียงความอยากรู้อยากเห็นเท่านั้น[10] การดักฟังไม่ว่าจะกระทำโดยรัฐหรือเอกชน ย่อมส่งผลกระทบต่อสิทธิในความเป็นอยู่ส่วนตัวในการสื่อสารข้อมูลของผู้อื่น สำหรับแนวทางแก้ไขปัญหาการดักฟังโดยใช้มาตรการทางเทคนิคอาจใช้การเข้ารหัสข้อมูล (Encryption) โดยเฉพาะกรณีข้อมูลอิเล็กทรอนิกส์ ทำให้แม้ว่าจะดักรับข้อมูลไปได้แต่ก็ไม่อาจเข้าใจความหมายของข้อมูลได้[11] สำหรับแนวทางแก้ไขทางกฎหมายนั้นหลายประเทศบัญญัติกฎหมายเกี่ยวกับการดักฟังไว้เป็นการเฉพาะ บทความนี้จะได้พิจารณามาตรการทางกฎหมายที่เกี่ยวข้องกับการดักฟัง โดยจะได้พิจารณากฎหมายประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย เพื่อนำมาเปรียบเทียบกับกฎหมายไทยต่อไป

## 1. มาตรการตามกฎหมายต่างประเทศที่เกี่ยวกับการดักฟัง : กฎหมายสหรัฐอเมริกา

กฎหมายเกี่ยวกับการดักฟังของสหรัฐอเมริกาอาจแบ่งออกได้เป็นสองระดับ คือ กฎหมายระดับสหรัฐ (Federal law) และกฎหมายระดับมลรัฐ (State law)

---

[8] *การดักฟังโทรศัพท์เคลื่อนที่อาจมีการดักฟังได้สองลักษณะ กล่าวคือ การดักฟังที่เป็นการแทรกแซงการสื่อสารทางสัญญาณคลื่นความถี่ และ การดักฟังโดยติดตั้งโปรแกรมบางอย่างในเครื่องโทรศัพท์เคลื่อนที่ เช่น ในปัจจุบันมีโปรแกรมการดักฟังโทรศัพท์เคลื่อนที่ (Spy-phone) โดยบุคคลที่ประสงค์ดักฟัง จะนำโทรศัพท์เคลื่อนที่ของบุคคลที่ต้องการดักฟังมาติดตั้งโปรแกรมนี้ ซึ่งหลังการติดตั้ง โปรแกรมดังกล่าวจะซ่อนตัวอยู่และทำการส่งข้อมูลตามที่ผู้ประสงค์ดักฟังต้องการ เช่น ข้อความสั้น (SMS) การโทรเข้าโทรออก เสียงการสนทนา มาให้ผู้ประสงค์ดักฟังทราบ*

[9] *คณาธิป ทองรวีวงศ์, กฎหมายเกี่ยวกับการสื่อสารมวลชน. กรุงเทพฯ:สำนักพิมพ์นิติธรรม. 2555.*

[10] *"People have always been interested in the conversations of others" : Priscilla M. Regan, Legislating Privacy :Technology, Social Value and Public Policy, The University of North Carolina Press, 1995.*

[11] *Whitfield, Diffie and Landau, Susan. Privacy on the Line: The Politics of Wiretapping and Encryption. Cambridge: MIT Press, 1998.*

**1.1 กฎหมายระดับสหรัฐ (Federal law)**

ก่อนปี ค.ศ. 1934 สหรัฐอเมริกายังไม่มีกฎหมายลายลักษณ์อักษรในระดับสหรัฐที่เกี่ยวข้องกับการดักฟังโดยเฉพาะ[12] กฎหมายที่นำมาปรับใช้ได้แก่ รัฐธรรมนูญและคำพิพากษาของศาล โดยรัฐธรรมนูญฉบับแก้ไขครั้งที่ 4 (the fourth amendment) ของสหรัฐอเมริกานั้น รับรองสิทธิในความเป็นส่วนตัว ในส่วนที่เกี่ยวกับตัวบุคคล ทรัพย์สิน ว่าจะไม่ถูกตรวจค้นหรือยึดโดยมิชอบด้วยกฎหมาย สำหรับหมายค้นนั้นจะออกได้ก็แต่โดยการระบุสถานที่และบุคคลที่จะถูกตรวจค้นอย่างเฉพาะเจาะจง[13] จะเห็นได้ว่าเจตนารมณ์ของรัฐธรรมนูญนั้นต้องการให้หลักประกันแก่ประชาชนที่จะไม่ถูกสอดเข้าเกี่ยวข้องและรบกวนความเป็นส่วนตัวจากรัฐโดยมิชอบด้วยกฎหมาย ซึ่งครอบคลุมถึงการดักฟังหรือดักรับข้อมูลการสื่อสารของบุคคลด้วย สำหรับแนวคำพิพากษาศาลนั้น ในปี ค.ศ. 1928 ศาลได้ตัดสินในคดีสำคัญคือ Olmstead v. United States ว่าการดักฟังการสนทนาทางโทรศัพท์ไม่ขัดต่อรัฐธรรมนูญฉบับแก้ไขครั้งที่ 4 เนื่องจากไม่มีการตรวจค้น ยึด ในทางกายภาพ กล่าวคือ เจ้าหน้าที่ไม่ได้กระทำการใด ๆ เข้าไปในสถานที่ของจำเลย พยานหลักฐานที่ได้มา ถือว่าได้มาจากการฟังเท่านั้น[14] จากคำตัดสินจะเห็นได้ว่า การคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวจากการถูกค้นและยึดมีขอบเขตจำกัด เฉพาะกรณีการค้นและยึดทางกายภาพ (physical intrusion) และจับต้องได้ (Tangible) เท่านั้น เช่น การเปิดจดหมายปิดผนึก (sealed letters in the mail) หรือ การบุกเข้าไปในบ้านของผู้อื่น[15]

หลังจาก คดี Olmstead v.United States ดังกล่าว ได้มีการตรากฎหมายลายลักษณ์อักษร เรียกว่า ***รัฐบัญญัติการสื่อสารสหรัฐ (Federal Communications Act)*** ในปี ค.ศ. 1934[16] ซึ่งมีหลักสำคัญในมาตรา 605 ว่า “ห้ามบุคคลซึ่งรับ (receiving) ข้อมูล เนื้อหา หรือความหมาย

---

[12] *สำหรับในระดับมลรัฐนั้น มีบางมลรัฐที่ตรากฎหมายลายลักษณ์อักษรเกี่ยวกับการดักฟังมาก่อนหน้านี้ เช่น มลรัฐ California ตรากฎหมายห้ามการดักฟังทางโทรเลขในปี ค.ศ. 1862 มลรัฐ New York และ Illinois ตรากฎหมายห้ามการดักฟังทางโทรศัพท์ในปี ค.ศ. 1895 ; Matt L. Greenberg, Law Enforcement Officers with Clean Hands May not Make Investigative use of a wiretap that was Illegal acquired by a third party, University of Cincinnati Law Review ,Winter, 2000*

[13] *“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*

[14] *“…there had been no official search and seizure of the person, his papers, tangible material effects, or an actual physical invasion of property…” : Olmstead v. United States, 277 U.S. 438 (1928)*

[15] *อย่างไรก็ตาม ผู้พิพากษา Louis Brandeis ได้เขียนความเห็นแย้งในคำพิพากษาดังกล่าวไว้ว่า เนื่องจากความก้าวหน้าทางเทคโนโลยีส่งผลให้การละเมิดสิทธิส่วนบุคคลกระทำได้ซับซ้อนกว่าเดิม และโดยเจตนารมณ์ของรัฐธรรมนูญที่มุ่งคุ้มครองบุคคลจากการละเมิดสิทธิในความเป็นส่วนตัวแล้ว การเปิดจดหมายกับการดักฟังโทรศัพท์ไม่มีความแตกต่างกันในแง่ของการละเมิดสิทธิส่วนบุคคลดังกล่าว*

[16] *United States Code, Title 47, Chapter 5, Subchapter VI, section 605, Unauthorized publication or use of communication*

ใดๆ จากการสื่อสารทางสายหรือทางวิทยุในการสื่อสารระหว่างรัฐหรือระหว่างประเทศ ทำการเปิดเผยหรือเผยแพร่ข้อมูลดังกล่าว" ผู้ฝ่าฝืนบทมาตราดังกล่าวมีโทษปรับไม่เกิน 2000 เหรียญสหรัฐ หรือจำคุกไม่เกินหกเดือนหรือทั้งจำทั้งปรับ[17] แต่ถ้าผู้นั้นกระทำไปเพื่อวัตถุประสงค์ทางการค้าหรือเพื่อผลประโยชน์ทางการเงินจะต้องระวางโทษปรับไม่เกินห้าหมื่นเหรียญสหรัฐหรือจำคุกไม่เกินสองปีหรือทั้งจำทั้งปรับ[18] หลังจากกฎหมายฉบับนี้มีผลบังคับ ได้มีคดี Nardone v. United States[19] ที่ศาลตัดสินในปี ค.ศ. 1939 วางหลักว่า พยานหลักฐานที่ได้มาโดยการดักฟังอันเป็นการฝ่าฝืนมาตรา 605 ไม่อาจรับฟังเป็นพยานหลักฐานได้ ซึ่งหมายรวมถึงพยานหลักฐานอื่นที่ได้มาโดยอาศัยความรู้จากบทสนทนาดังกล่าว[20]

อย่างไรก็ตาม หลังจากนั้นมีหลายคดีที่ศาลวางหลักว่า การดักฟังไม่ขัดต่อมาตรา 605 เช่น คดี Goldman V United States[21] ศาลตัดสินว่าการที่เจ้าพนักงานติดตั้งอุปกรณ์ที่ผนังห้องเพื่อดักฟังการสนทนาไม่ขัดต่อมาตรา 605 ของรัฐบัญญัติการสื่อสารสหรัฐ เนื่องจากไม่ถือว่าเป็นการดักฟังตามความหมายของกฎหมายดังกล่าว[22] คดี On Lee v. United States[23] เป็นกรณีที่เจ้าพนักงานคนหนึ่งซึ่งมีอุปกรณ์ไมโครโฟนขนาดเล็กในเสื้อโค้ตทำการสนทนากับโจทก์ และส่งสัญญาณการสนทนาไปให้เจ้าหน้าที่อีกคนหนึ่งซึ่งดักฟังอยู่ด้านนอก ศาลตัดสินว่าการกระทำของเจ้าพนักงานยังไม่เป็นการละเมิดต่อมาตรา 605 เนื่องจากมิได้มีการแทรกแซงอุปกรณ์การสื่อสารใดๆ ในคดี Irvine v. California[24] ศาลตัดสินว่า การกระทำของเจ้าหน้าที่ซึ่งติดตั้งอุปกรณ์เพื่อดักฟังการสนทนาของโจทก์ มิใช่การดักฟังดังที่กระทำกันในความหมายปกติ (not a conventional "wire tapping") เนื่องจากเครื่องมือที่เจ้าหน้าที่ใช้ มิได้เชื่อมต่อกับอุปกรณ์โทรศัพท์ไม่มีการกระทำอันเป็นการแทรกแซงระบบการสื่อสาร (no interference with the communication system) จึงไม่เป็นการขัดต่อมาตรา 650 จากคดีดังกล่าวจะเห็นได้ว่า แม้มีกฎหมายลายลักษณ์อักษรคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวจากการดักฟังแล้ว แต่กฎหมายมีขอบเขตจำกัดเฉพาะการ

---

[17] *United States Code, Title 47 , Chapter 5 ,Subchapter VI ,section 605 (e) (1)*

[18] *United States Code, Title 47 ,Chapter 5 ,Subchapter VI , section 605 (e) (2)*

[19] *Nardone v. United States - 308 U.S. 33, (1939)*

[20] *"…This applies not only to the intercepted conversations themselves, but also to evidence procured through the use of knowledge gained from such conversations…"*

[21] *Goldman v. United States - 316 U.S. 129 (1942)*

[22] *"Wire communication" means the transmission of ..signals, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception of such transmission…"*

[23] *On Lee v. United States , - 343 U.S. 747, 1952*

[24] *Irvine v. California - 347 U.S. 128 (1954)*

สื่อสารทางสาย (Wire communication) นอกจากนี้ ศาลยังใช้การตีความตามแบบแผน (conventional) ในการพิจารณาการดักฟัง (Interception) ว่าจะต้องเป็นการดักรับการสื่อสารทางสาย ดังนั้น การลักลอบฟังการสนทนา ที่ไม่ได้ดักฟังการสื่อสารทางสาย (Eavesdrop) เช่น การที่เจ้าหน้าที่นำไมโครโฟนไปซ่อนไว้ หรือการที่ใช้อุปกรณ์รับฟังไปติดไว้ที่ผนังห้อง จะไม่เข้าองค์ประกอบความผิดตามรัฐบัญญัติการสื่อสารสหรัฐ เนื่องจากมิได้ทำการดักฟังการสื่อสารทางสาย (Wiretap) เนื่องจากศาลเห็นว่ากฎหมายนี้มีเจตนารมณ์มุ่งหมายคุ้มครอง “วิธีการสื่อสาร” (Means of communication) มิใช่มุ่งคุ้มครอง “ความลับของการสนทนา” (Secrecy of the conversation)[25]

ในปี ค.ศ. 1967 ศาลได้ตัดสินคดีสำคัญ คือ Katz v. United States ซึ่งเป็นกรณีเจ้าพนักงานติดเครื่องดักฟังไว้ที่ตู้โทรศัพท์สาธารณะ ศาลได้วางหลักว่า แม้ผู้กระทำไม่ได้มีการเข้าไปทางกายภาพอันเป็นการบุกรุก แต่ก็เป็นการกระทำที่ขัดต่อรัฐธรรมนูญฉบับแก้ไขครั้งที่ 4 เนื่องจากรัฐธรรมนูญดังกล่าวมุ่งเน้นที่การคุ้มครองตัวบุคคล มิใช่สถานที่[26] จะเห็นว่าคดีนี้แตกต่างจากคดี Goldman V United States ซึ่งอ้างว่าการดักฟังขัดต่อรัฐบัญญัติการสื่อสารสหรัฐ โดยศาลตีความว่ารัฐบัญญัติดังกล่าวมุ่งคุ้มครอง “วิธีการสื่อสาร” (Means of communication) มิใช่มุ่งคุ้มครอง “ความลับของการสนทนา”[27] ในขณะที่ คดี Katz v.United States มิได้มีประเด็นวินิจฉัยตามรัฐบัญญัติการสื่อสารสหรัฐ แต่เป็นกรณีการอ้างว่าพฤติกรรมการดักฟังขัดต่อรัฐธรรมนูญสหรัฐฉบับแก้ไขครั้งที่ 4 ซึ่งศาลตีความว่ารัฐธรรมนูญดังกล่าวมุ่งให้การคุ้มครองสิทธิของตัวบุคคล มิได้คุ้มครองสถานที่ จะเห็นได้ว่ารัฐบัญญัติดังกล่าวมีขอบเขตที่แคบเนื่องจากจำกัดเฉพาะการดักฟังโดยการแทรกแซงระบบการสื่อสาร ไม่ครอบคลุมถึงกรณีการดักฟังที่มิได้แทรกแซงระบบการสื่อสารโดยตรง เช่น การลักลอบฟัง (Eavesdrop) ทางกายภาพหรือโดยใช้วิธีการติดเครื่องดักฟังไว้ในอาคารสถานที่ต่าง ๆ แต่ศาลตีความว่ารัฐธรรมนูญมุ่งคุ้มครองสิทธิส่วนบุคคลของตัวบุคคลนั้น ไม่ว่าพฤติกรรมการล่วงละเมิดจะเกิดที่ใดก็ตาม อย่างไรก็ตาม ในคดี United States v. Knotts[28] ศาลได้นำหลัก “การคาดหมายความเป็นส่วนตัว” (Expectation

---

[25] *ศาลในคดี Goldman V United States อธิบายว่า “The protection intended by the statute is of the means of communication, and not of the secrecy of the conversation”*

[26] *Katz v. United States, 389 U.S. 347 (1967)*

[27] *ศาลในคดี Goldman V United States อธิบายว่า “The protection intended by the statute is of the means of communication, and not of the secrecy of the conversation”*

[28] *United States v. Knotts, 460 U.S. 276 (1983)*

of privacy) มาพิจารณาการดักฟัง กล่าวคือ หากข้อมูลที่ดักฟังนั้นอาจได้มาโดยการสังเกตด้วยตาเปล่าหรือจากการรับฟังตามปกติอยู่แล้ว การดักฟังหรือดักรับข้อมูลดังกล่าวจะไม่เป็นการขัดต่อรัฐธรรมนูญ เนื่องจากผู้ถูกดักฟังไม่อาจคาดหมายความเป็นส่วนตัวในการสื่อสารดังกล่าวได้[29] แต่ถ้ามีการใช้อุปกรณ์ดักรับข้อมูลซึ่งไม่อาจได้มาโดยการสังเกตด้วยตาเปล่าหรือจากการรับฟังตามปกติ ดังนี้ผู้ถูกดักรับข้อมูลก็ยังสามารถคาดหมายความเป็นส่วนตัวได้ ดังนั้น หากเทียบเคียงเหตุผลของคดี United States v. Knotts กับคดี Katz v. United States จะเห็นได้ว่า การติดเครื่องดักฟังไว้ที่ตู้โทรศัพท์สาธารณะนั้นเป็นการขัดต่อรัฐธรรมนูญเนื่องจากการสนทนาในตู้โทรศัพท์เป็นสถานการณ์ที่บุคคลสามารถคาดหมายความเป็นส่วนตัวได้

หลังจากคดี Katz v. United States ที่ตัดสินในปี ค.ศ. 1967 มีการบัญญัติกฎหมายที่เรียกว่า **"The Omnibus Crime Control and Safe Streets Act"**[30] ในปี ค.ศ. 1968 เพื่อเป็นการแก้ไขเพิ่มเติมรัฐบัญญัติการสื่อสารสหรัฐ (Federal communication Act 1934) โดยในบรรพที่สาม (Title 3) ของกฎหมายนี้วางหลักเกี่ยวกับการดักฟังไว้ จึงมีการเรียกบรรพสามนี้ว่า "กฎหมายเกี่ยวกับการดักฟัง" (Wiretap Act)[31] ซึ่งมาตรา 2511[32] วางหลักห้ามดักฟังการสื่อสารทางสาย (Wire) และทางวาจา (Oral) แต่มีข้อยกเว้นให้ดักฟังได้เพื่อประโยชน์ในการสืบสวนสอบสวนและการป้องกันอาชญากรรมบางประเภท[33] ต่อมาในปี ค.ศ. 1968 มีการบัญญัติกฎหมายที่เรียกว่า **"Electronic Communications Privacy Act of 1986" หรือ ECPA**[34] ขึ้นมาแก้ไขเพิ่มเติม "The Omnibus Crime Control and Safe Streets Act" ให้ครอบคลุมการสื่อสารทางอิเล็กทรอนิกส์ด้วย โดยมาตรา 2511 วางหลักห้ามผู้ใดกระทำการ ดักฟัง (Intercept) ใช้ (Use) อุปกรณ์อิเล็กทรอนิกส์ กลไก หรืออุปกรณ์ใด ๆ ในการดักฟัง เปิดเผย (Disclose) เนื้อหา (contents) ของการสนทนาทาง

---

*[29] คดี United States v. Knotts เป็นกรณีที่เจ้าพนักงานติดตั้งเครื่องส่งสัญญาณในสิ่งของและติดตามรถยนต์โดยอาศัยสัญญาณจากเครื่องดังกล่าว ศาลสูงสุดตัดสินว่า การตรวจสอบติดตามเครื่องส่งสัญญาณนั้น มีลักษณะเหมือนกับการติดตามรถยนต์ที่เคลื่อนที่ไปตามถนนสาธารณะ ซึ่งบุคคลที่ใช้รถยนต์เดินทางในที่สาธารณะนั้นไม่สามารถคาดหมายถึงความเป็นส่วนตัวในการเดินทางดังกล่าวได้*

*[30] Public law. 90-351, June 19, 1968, 82 Stat. 197, 42 U.S.C. § 3711*

*[31] Omnibus Crime Control and Safe Street Act วางหลักเกี่ยวกับการควบคุมอาชญากรรมหลายประการ การดักฟังเป็นเพียงส่วนหนึ่งซึ่งปรากฏอยู่ในบรรพสาม (Title III) ของกฎหมายนี้*

*[32] U.S.C. Title 18, Part 1,Chapter 119, section 2511-2522 [Online] available form, http://www.law.cornell.edu/uscode/text/18/2511*

*[33] กฎหมายฉบับนี้มีวัตถุประสงค์หลักในการควบคุมการกระทำความผิดทางอาญา แต่ในขณะเดียวกันก็มุ่งคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของปัจเจกชนอันอาจได้รับผลกระทบเนื่องจากการควบคุมการกระทำความผิดอาญาด้วย, Charles A. Pulaski, Authorizing Wiretap Applications under Title III: Another Dissent to Giordano and Chavez, University of Pennsylvania Law ReviewApril, 1975*

*[34] Public Law 99-508, 100 Stat. 1848, enacted October 21, 1986 ,18 U.S.C. §§ 2510–2522*

สาย วาจา หรือทางอิเล็กทรอนิกส์ ซึ่งเนื้อหาดังกล่าวเป็นข้อมูลที่ได้รับมาจากการดักฟัง สำหรับข้อยกเว้นที่ทำให้การดักฟังไม่เป็นความผิดนั้น มีดังเช่น

- คู่กรณีหรือบุคคลที่เกี่ยวข้องในการสื่อสารนั้นฝ่ายหนึ่งได้ให้ความยินยอม (one-party consent exception) กล่าวคือ หากบุคคลคนหนึ่งหรือกว่านั้นที่เกี่ยวข้องในการสื่อสารได้ให้ความยินยอมในการบันทึกการสื่อสารนั้น

- หลักการคาดหมายความเป็นส่วนตัว กล่าวคือ การสื่อสารนั้นคู่กรณีอาจคาดหมายความเป็นส่วนตัวได้หรือไม่ หากไม่สามารถคาดหมายได้ การดักฟังนั้นก็ไม่ขัดต่อกฎหมาย สำหรับการตีความว่าผู้ถูกดักฟังคาดหมายความเป็นส่วนตัวได้หรือไม่ ศาลจะใช้แนวการพิจารณาจากคดี Katz กล่าวคือ พิจารณาทั้งด้านอัตวิสัย (ความคาดหมายของตัวผู้ถูกดักฟังเอง) และภววิสัย (ความคาดหมายของสังคมว่ากรณีนั้นอาจคาดหมายความเป็นส่วนตัวได้หรือไม่)

- การดักฟังนั้นกระทำโดยมีหมายศาล (warrant)

- ข้อยกเว้นตามกฎหมายเฉพาะ ในประเทศสหรัฐอเมริกามีกฎหมายเฉพาะอีกหลายฉบับที่ให้อำนาจเจ้าหน้าที่ของรัฐทำการตรวจสอบการสื่อสารข้อมูลของบุคคล โดยเฉพาะทางช่องทางอิเล็กทรอนิกส์ได้มีกฎหมายเกี่ยวกับการสอดส่องทางอิเล็กทรอนิกส์ (electronic surveillance)[35] เช่นในปี ค.ศ. 1978 ได้มีการตารัฐบัญญัติ ว่าด้วยการข่าวกรองต่างประเทศ (“Foreign Intelligence Surveillance Act” หรือ FISA) ซึ่ง ต่อมามีการแก้ไขอีกในปี ค.ศ. 2008 (FISA Amendment Act)[36] กำหนดข้อยกเว้นของหลักการห้ามดักฟัง ตามมาตรา 2511 ของกฎหมาย ECPA โดยกำหนดให้ บุคคลที่ได้มีอำนาจตามกฎหมายในการดักฟังทางสาย การสนทนา การสื่อสารทางอิเล็กทรอนิกส์ หรือทำการสอดส่องทางอิเล็กทรอนิกส์

อาจสรุปได้ว่า หลักสำคัญของกฎหมายลายลักษณ์อักษรระดับสหรัฐเกี่ยวกับการดักฟังนั้น เป็นการวางหลักห้ามการดักฟังการสื่อสารใด ๆ ก็ตาม ทั้งนี้เนื่องจากกฎหมายกำหนดว่า การดักฟัง (Interception) จะเกิดขึ้นเมื่อมีการได้ยินหรือการได้มาซึ่งเนื้อหาข้อมูลทางการสื่อสารโดยใช้สาย (wire) วาจา (oral) ผ่านทางอิเล็กทรอนิกส์หรืออุปกรณ์ใด ๆ[37] ดังนั้นจะเห็นได้ว่า กฎหมายฉบับนี้มิได้จำกัดเฉพาะการ “ดักฟัง” แต่ครอบคลุมการ “ดักรับการสื่อสารข้อมูล” ไม่ว่าจะใช้วิธีการใด ๆ

---

[35] *James G. Carr and Patricia L. Bellia , The Law of Electronic Surveillance, West, 2011*

[36] *FISA (Foreign Intelligence Surveillance Act) Amendments Act of 2008 (Pub. L.110-261; 7/10/2008)*

[37] *interception occurs by the “aural or other acquisition of contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” , 18 U.S.C. §2510(4) (2006)*

**1.2 กฎหมายระดับมลรัฐ (State law)**

นอกจากกฎหมายเกี่ยวกับการดักฟังในระดับสหรัฐ (Federal Wiretap Act) แล้ว ปัจจุบัน 49 มลรัฐได้ตรากฎหมายลายลักษณ์อักษรเกี่ยวกับการดักฟัง หลักสำคัญของกฎหมายระดับมลรัฐมีองค์ประกอบเช่นเดียวกับกฎหมายระดับสหรัฐ เช่น องค์ประกอบเกี่ยวกับความยินยอม กฎหมายระดับมลรัฐส่วนมากกำหนดให้ ความยินยอมจากคู่กรณีฝ่ายหนึ่ง (One party consent) เป็นข้อยกเว้นความรับผิดได้[38] ตัวอย่างเช่น กฎหมายมลรัฐ New York วางหลักว่า บุคคลจะมีความผิดฐานดักฟังเมื่อกระทำการดักฟังโดยปราศจากความยินยอมจากผู้ส่งหรือผู้รับข้อมูล และทำการบันทึกการสื่อสารดังกล่าวไว้ด้วยอุปกรณ์ใด ๆ[39] อย่างไรก็ตาม บางมลรัฐกำหนดองค์ประกอบที่มีความเข้มงวดมากกว่าองค์ประกอบของกฎหมายระดับสหรัฐ เช่น มลรัฐ Pennsylvania กำหนดข้อยกเว้นการดักฟังในกรณีที่คู่กรณีทุกฝ่ายที่เกี่ยวข้องกับการสื่อสารดังกล่าวให้ความยินยอมกับการดักรับข้อมูลการสื่อสาร (All-party consent rule)[40]

**2. มาตรการตามกฎหมายต่างประเทศที่เกี่ยวกับการดักฟัง : กฎหมายออสเตรเลีย**

ประเทศออสเตรเลียได้ตรากฎหมายลายลักษณ์อักษรเกี่ยวกับการดักฟัง คือ พระราชบัญญัติโทรคมนาคม (การดักจับสัญญาณและการเข้าถึง) ค.ศ. 1979 (Telecommunications Interception and Access Act 1979 หรือ TIA) นอกจากนี้ยังมีพระราชบัญญัติโทรคมนาคม ค.ศ. 1997 (Telecommunication Act 1997 หรือ TA) มีหลักการคุ้มครองการสื่อสารข้อมูลซึ่งแยกพิจารณาได้ดังนี้

1. หลักการห้ามดักฟัง ปรากฏอยู่ในกฎหมาย TIA โดยกฎหมายได้นิยามการดักฟังว่า หมายถึงการฟังหรือบันทึกโดยวิธีใด ๆ ซึ่งการสื่อสารในช่องทางระบบโทรคมนาคมโดยปราศจากการรับรู้ของบุคคลที่ทำการสื่อสาร (มาตรา 6) กฎหมาย TIA ได้วางหลักห้ามการดักฟังการสื่อสารที่ทำการสื่อสารผ่านเครือข่ายโทรคมนาคมของออสเตรเลีย (มาตรา 7) เว้นแต่มีหมายดักฟัง (Telecommunication interception warrants) ซึ่งจะออกได้แต่โดยเหตุเพื่อการสืบสวนสอบสวน

---

[38] *Daniel R. Dinger, Should Parents Be Allowed to Record a Child's Telephone Conversations When They Believe the Child Is in Danger: An Examination of the Federal Wiretap Statute and the Doctrine of Vicarious Consent in the Context of a Criminal Prosecution, Seattle University Law Review, 955 (2004-2005)*

[39] *N.Y. Penal Law §250.00(1)*

[40] *"[i]t shall not be unlawful . . . for . . . [a] person, to intercept a wire, electronic or oral communication, where all parties to the communication have given prior consent to such interception.", Pennsylvania Statutes Annotated § 5704(4)*

ความผิดร้ายแรง (Serious offence)[41] หน่วยงานที่มีสิทธิขอออกหมาย เช่น ตำรวจสหพันธ์ออสเตรเลีย (Australian Federal Police หรือ AFP) ผู้มีสิทธิออกหมายได้แก่ ผู้พิพากษาที่มีอำนาจ (Eligible Judge)[42] จากรายงานประจำปี ค.ศ. 2011[43] เกี่ยวกับการบังคับใช้กฎหมาย TIA ชี้ให้เห็นว่าหน่วยงานต่าง ๆขอหมายดักฟัง 3,495 ราย ศาลยกคำขอ 7 ราย ออกหมายดักฟังให้ 3,488 ราย สำหรับระยะเวลาในการดักฟังตามหมายนั้นมีแตกต่างกันไป โดยเฉลี่ยแล้วศาลอนุญาต 56 วัน

2. หลักห้ามเข้าถึงการสื่อสารที่ถูกจัดเก็บไว้ (Stored communication)[44] เว้นแต่มีหมายเข้าถึงข้อมูลการสื่อสารที่ถูกจัดเก็บ (Stored communication warrants) ซึ่งสามารถออกได้แต่โดยเหตุที่เกี่ยวกับการสืบสวนสอบสวน “การฝ่าฝืนกฎหมายอย่างร้ายแรง” (Serious contravention)[45] ผู้มีสิทธิขอออกหมาย ได้แก่ เจ้าหน้าที่บังคับใช้กฎหมาย (Enforcement agency) ซึ่งหมายถึงเจ้าหน้าที่เกี่ยวกับการบังคับใช้กฎหมาย อาญา ผู้มีอำนาจออกหมาย (Issuing authority) ได้แก่ ผู้พิพากษา และ ผู้ซึ่งได้รับการแต่งตั้งจากอัยการสูงสุด จะเห็นได้ว่าหมายการเข้าถึงข้อมูลการสื่อสารที่ถูกเก็บไว้ มีเงื่อนไขในการออกหมายที่กว้างกว่ากรณีหมายดักฟัง จากรายงานประจำปี ค.ศ. 2011[46] เกี่ยวกับการบังคับใช้กฎหมาย TIA ชี้ให้เห็นว่าหน่วยงานต่าง ๆ ขอหมายเข้าถึงข้อมูลการสื่อสารที่ถูกจัดเก็บ 300 ราย ศาลยกคำขอ 2 ราย ออกหมายดักฟังให้ 298 ราย

3. หลักห้ามการเข้าถึงข้อมูลเกี่ยวกับโทรคมนาคม (Telecommunication data) กฎหมาย TA นิยาม ข้อมูลโทรคมนาคม (Telecommunication data) ว่าหมายถึงข้อมูลรายละเอียดเกี่ยวกับวัน เวลา สถานที่ที่บุคคลทำการติดต่อสื่อสาร แต่ไม่รวมถึงเนื้อหา (content) ของการสื่อสารนั้น สำหรับรายละเอียดที่กำหนดหลักและข้อยกเว้นของการเข้าถึง การเปิดเผย จะอยู่ใน

---

*[41] กฎหมายได้นิยาม “ความผิดร้ายแรง” ไว้ในมาตรา 5D เช่น ฆาตกรรม ลักพาตัว ค้ายาเสพติด ก่อการร้าย ความผิดทางเพศซึ่งกระทำต่อเด็ก ความผิดเกี่ยวกับภาพลามกอนาจารของเด็ก ความผิดเกี่ยวกับองค์กรอาชญากรรมข้ามชาติ การฟอกเงิน อาชญากรรมทางคอมพิวเตอร์ ความผิดที่มีโทษจำคุกตั้งแต่เจ็ดปีขึ้นไปในกรณีเกี่ยวกับการทำร้ายร่างกายบุคคล การให้สินบนเจ้าพนักงาน การคอร์รัปชั่น การหนีภาษี เป็นต้น*

*[42] ผู้พิพากษาประจำศาลดังต่อไปนี้มีอำนาจออกหมาย : “The Federal Court of Australia” “The Family Court of Australia” “The Federal Magistrate Court”*

*[43] Telecommunications (Interception and Access) Act 1979, Report for the year 2011 [Online] available from, Australian Attorney-General's Department Website : http://www.ag.gov.au/Publications*

*[44] การสื่อสารที่ถูกเก็บไว้ (Stored communication) หมายถึง การสื่อสารซึ่งได้ทำการสื่อสารผ่านระบบโทรคมนาคมแล้วและทำการเข้าถึงเนื่องจากความช่วยเหลือของผู้ให้บริการโทรคมนาคมโดยปราศจากการรับรู้ของบุคคลที่ทำการสื่อสาร การสื่อสารที่ถูกจัดเก็บไว้รวมถึงจดหมายอิเล็กทรอนิกส์ (Email) ข้อความสั้น (SMS message) ข้อความเสียง (Voice massage) ( มาตรา 108)*

*[45] มีความหมายครอบคลุม “ความผิดร้ายแรง” (Serious offence) ในกรณีของหมายดักฟัง และยังหมายรวมถึงความผิดที่มีโทษจำคุกอย่างน้อยสามปีด้วย*

*[46] Telecommunications (Interception and Access) Act 1979, Report for the year 2011 [Online] available from, Australian Attorney-General's Department Website : http://www.ag.gov.au/Publications*

กฎหมาย TIA ซึ่งมาตรา 172 วางหลักห้ามการเปิดเผยข้อมูลเกี่ยวกับการโทรคมนาคม เช่น ชื่อผู้สมัครใช้งาน หมายเลขโทรศัพท์ที่เกี่ยวข้องกับการสื่อสารวันและเวลาสื่อสาร เลขหมายประจำเครื่องคอมพิวเตอร์ (IP address) ข้อมูลเกี่ยวกับสถานที่ (Location-based information) สำหรับข้อยกเว้นนั้น กฎหมายวางหลักว่า การเข้าถึงข้อมูลเกี่ยวกับโทรคมนาคมนั้นไม่ต้องมีหมาย แต่ใช้วิธีการอนุญาตให้เปิดเผย โดยเจ้าหน้าที่ผู้เกี่ยวข้องกับการบังคับใช้กฎหมายอาญา (criminal law enforcement agency) สามารถขออนุญาตจากหัวหน้าหรือรองหัวหน้าของหน่วยงานตนได้[47] ในปี ค.ศ. 2010 ได้มีการตราพระราชบัญญัติแก้ไข เพิ่มเติมกฎหมายการดักฟังและการข่าวกรอง (The Telecommunications Interception and Intelligence Service Legislation Amendment Act) เพื่อแก้ไขเพิ่มเติมกฎหมาย TIA โดยกำหนดให้เจ้าหน้าที่บังคับใช้กฎหมายสามารถเข้าถึงข้อมูลเกี่ยวกับการโทรคมนาคมเพื่อบ่งระบุสถานที่ของบุคคลที่หายตัวไป ดังนั้นจะเห็นได้ว่า ในกรณีการเข้าถึงข้อมูลเกี่ยวกับการโทรคมนาคมนั้น เจ้าหน้าที่สามารถเข้าถึงได้โดยเงื่อนไขที่เข้มงวดน้อยกว่าการดักฟังที่ต้องขอหมายศาล จากรายงานประจำปี ค.ศ. 2011[48] เกี่ยวกับการบังคับใช้กฎหมาย TIA ชี้ให้เห็นว่าในปี ค.ศ. 2011 เจ้าหน้าที่ผู้มีอำนาจได้อนุญาตให้เข้าถึงข้อมูลเกี่ยวกับการโทรคมนาคมจำนวน 243,631 ราย

จากกฎหมายออสเตรเลีย จะเห็นได้ว่าการสื่อสารข้อมูลของบุคคลได้รับการคุ้มครองถึงสามระดับ กล่าวคือ ในระดับแรก ขณะทำการสื่อสารข้อมูล ในระดับที่สอง เมื่อข้อมูลนั้นถูกสื่อสารแล้วและถูกเก็บรักษาอยู่ในระบบ ในระดับที่สามคุ้มครองรายละเอียดแวดล้อมเกี่ยวกับข้อมูลซึ่งมิใช่ตัวเนื้อหาข้อมูลโดยตรง กล่าวคือ รายละเอียดเกี่ยวกับวัน เวลา สถานที่ในการสื่อสารข้อมูล

### 3. กฎหมายไทยที่เกี่ยวข้องกับการดักฟัง

ในระบบกฎหมายไทยปัจจุบันมีกฎหมายที่มีส่วนเกี่ยวข้องกับการดักฟังและดักรับข้อมูลหลายฉบับ เช่น

**(1) กฎหมายที่คุ้มครองสิทธิในความเป็นอยู่ส่วนตัว กล่าวคือ วางหลักห้ามการดักฟังหรือดักรับข้อมูลการสื่อสารของบุคคล** กฎหมายกลุ่มนี้ได้แก่ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 รับรองเสรีภาพในการสื่อสารถึงกันระหว่างบุคคลในมาตรา 36 ซึ่งวางหลักว่า “บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบ

---

[47] *เจ้าหน้าที่ผู้มีอำนาจสั่งเปิดเผยข้อมูล (authorized officer) ได้แก่ หัวหน้า รองหัวหน้า (Head, Deputy Head) ของหน่วยงานบังคับใช้กฎหมายอาญา*

[48] *Telecommunications (Interception and Access) Act 1979, Report for the year 2011 [Online] available from, Australian Attorney-General's Department Website : http://www.ag.gov.au/Publications*

ด้วยกฎหมาย" เพื่อคุ้มครองเสรีภาพดังกล่าว รัฐธรรมนูญกำหนดห้ามการกระทำที่มีลักษณะเป็นการขัดขวางต่อการสื่อสาร ดังจะเห็นได้จากมาตรา 36 วรรคท้ายที่วางหลักว่า "การตรวจ การกัก หรือการเปิดเผยสิ่งสื่อสารที่บุคคลมีติดต่อถึงกัน รวมทั้ง การกระทำด้วยประการอื่นใดเพื่อให้ล่วงรู้ถึงข้อความในสิ่งสื่อสารทั้งหลายที่บุคคลมีติดต่อถึงกัน จะกระทำมิได้เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เฉพาะเพื่อรักษาความมั่นคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน" แม้รัฐธรรมนูญมิได้ระบุเฉพาะเจาะจงถึง "ดักฟัง" หรือ "ดักรับข้อมูล" แต่จากมาตรา 36 จะเห็นได้ว่า การดักฟังหรือการดักรับข้อมูล จัดเป็น "การกระทำประการอื่นเพื่อให้ล่วงรู้ถึงข้อความในสิ่งสื่อสาร" ซึ่งโดยหลักแล้วต้องห้ามตามรัฐธรรมนูญ

**ประมวลกฎหมายอาญา** ประมวลกฎหมายอาญามิได้มีฐานความผิดเกี่ยวกับการดักฟังหรือดักรับข้อมูลเป็นการเฉพาะ แต่มีฐานความผิดเฉพาะกรณีที่เป็นการกระทำของเจ้าพนักงานผู้มีหน้าที่ในการไปรษณีย์ โทรเลข หรือ โทรศัพท์ กระทำการบางประการในการแทรกแซงข้อมูลข่าวสาร เช่น เปิดจดหมาย หรือสิ่งที่ส่งทางไปรษณีย์ เปิดเผยข้อความที่ส่งทางไปรษณีย์ หรือโทรศัพท์ (มาตรา 163) อย่างไรก็ตาม ข้อจำกัดของประมวลกฎหมายอาญาก็คือ มาตรา 163 มีขอบเขตจำกัดเฉพาะผู้กระทำที่เป็นเจ้าพนักงาน และยังจำกัดว่าจะต้องเป็นเจ้าพนักงานที่มีหน้าที่เกี่ยวข้องกับการสื่อสารข้อมูลบางลักษณะเท่านั้น กล่าวคือ ไปรษณีย์ โทรเลข โทรศัพท์ จึงไม่ครอบคลุมถึงการกระทำที่กระทำโดยเจ้าพนักงานอื่นซึ่งไม่ใช่เจ้าพนักงานที่มีหน้าที่เกี่ยวกับไปรษณีย์ โทรศัพท์ นอกจากนี้ ยังไม่ครอบคลุมถึงกรณีการกระทำดักรับข้อมูลที่กระทำการโดยเอกชนอีกด้วย กล่าวอีกนัยหนึ่งได้ว่า ประมวลกฎหมายอาญามิได้กำหนดฐานความผิดสำหรับการดักรับข้อมูลเป็นการทั่วไปไว้

**พระราชบัญญัติวิทยุคมนาคม พ.ศ. 2498** พระราชบัญญัติวิทยุคมนาคม พ.ศ. 2498 แก้ไขเพิ่มเติม (ฉบับที่ 3) พ.ศ.2535 มาตรา 17 วางหลักว่า "ห้ามมิให้ผู้ใดดักรับไว้ ใช้ประโยชน์ หรือเปิดเผยโดยมิชอบด้วยกฎหมาย ซึ่งข่าววิทยุคมนาคมที่มิได้มุ่งหมายเพื่อประโยชน์สาธารณะ หรือที่อาจก่อให้เกิดความเสียหายแก่ประเทศชาติหรือประชาชน" ข้อจำกัดของกฎหมายฉบับนี้คือ มีขอบเขตเฉพาะการดักรับการสื่อสารโดยช่องทางวิทยุคมนาคม[49] และข้อมูลที่ดักฟังจะต้องเป็นข้อมูลประเภท "ข่าว" ที่มิได้มุ่งหมายเพื่อประโยชน์สาธารณะ

[49] *"วิทยุคมนาคม" หมายความว่า การส่ง หรือการรับเครื่องหมาย สัญญาณ ตัวหนังสือ ภาพ และเสียงหรือการอื่นใดซึ่งสามารถเข้าใจความหมายได้ด้วยคลื่นแฮรตเซียน (มาตรา 4)*

**พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544** มีหลักการห้ามกระทำการดักรับข้อความข่าวสารหรือข้อมูลอื่นใดที่ทำการสื่อสารทางโทรคมนาคม ดังจะเห็นได้จากมาตรา 74 ซึ่งวางหลักว่า "ผู้ใดกระทำด้วยประการใด ๆ เพื่อดักรับไว้ ใช้ประโยชน์ หรือเปิดเผยข้อความข่าวสาร หรือข้อมูลอื่นใดที่มีการสื่อสารทางโทรคมนาคม[50] โดยไม่ชอบด้วยกฎหมาย ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่แสนบาท หรือทั้งจำทั้งปรับ" ดังนั้นจะเห็นได้ว่า การดักรับข้อมูลข่าวสารทางโทรคมนาคม[51] ไม่ว่าจะเป็นการสื่อสารแบบมีสาย หรือ ไร้สาย หากมีการ "ดักรับข้อมูล" ก็เข้าองค์ประกอบความผิดตามพระราชบัญญัตินี้

**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550** สำหรับกรณีการเข้าถึงข้อมูลคอมพิวเตอร์นั้นอาจแยกได้เป็นสองกรณีคือ (1) กรณีแรก การเข้าถึงข้อมูลที่ไม่ได้อยู่ระหว่างการส่ง กล่าวคือ ถูกเก็บอยู่ในระบบคอมพิวเตอร์แล้ว จะเห็นได้จากความผิดตามมาตรา 7[52] ซึ่งเทียบได้กับกรณีการเข้าถึงการสื่อสารที่ถูกจัดเก็บไว้ (Stored communication) ตามกฎหมายประเทศออสเตรเลีย (2) กรณีที่สอง การดักรับข้อมูลคอมพิวเตอร์ระหว่างการส่งในระบบคอมพิวเตอร์ จะเห็นได้จากความผิดตามมาตรา 8[53] เช่น การดักรับข้อมูลการสื่อสารทางการสนทนาออนไลน์ในเว็บไซต์ระหว่างบุคคล กรณีนี้มีลักษณะเช่นเดียวกับการดักฟังนั่นเอง จะเห็นได้ว่าพระราชบัญญัตินี้ วางหลักคุ้มครองบุคคลทั่วไปจากการถูกดักรับข้อมูล แต่ต้องเป็นกรณีข้อมูลคอมพิวเตอร์เท่านั้น

**(2) กฎหมายที่ให้อำนาจเจ้าพนักงานทำการดักฟัง**

จากรัฐธรรมนูญมาตรา 36 จะเห็นได้ว่า การดักฟังหรือการดักรับข้อมูลโดยมิได้รับความยินยอมนั้นไม่อาจทำได้ไม่ว่าจะเป็นการกระทำโดยเจ้าหน้าที่รัฐหรือโดยบุคคลทั่วไป อย่างไรก็ตามรัฐธรรมนูญกำหนดข้อยกเว้นไว้หากมีกฎหมายบัญญัติให้ทำได้ ซึ่งในปัจจุบันมีกฎหมายหลายฉบับที่ให้อำนาจการกระทำการดักรับข้อมูล เช่น **พระราชบัญญัติไปรษณีย์ พ.ศ. 2477** มี

---

*[50] มาตรา 4 ของพระราชบัญญัติ องค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553 นิยามความหมายของ "โทรคมนาคม" ว่าหมายถึง "การส่ง การแพร่ หรือการรับเครื่องหมาย สัญญาณ ตัวหนังสือ ตัวเลข ภาพ เสียง รหัส หรือสิ่งอื่นใดซึ่งสามารถให้เข้าใจความหมายได้โดยระบบคลื่น ความถี่ ระบบสาย ระบบแสง ระบบแม่เหล็กไฟฟ้า หรือระบบอื่น"*

*[51] มาตรา 4 พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 นิยามความหมายของ"กิจการโทรคมนาคม" ไว้ว่า "กิจการโทรคมนาคมตามกฎหมายว่าด้วยองค์กรจัดสรรคลื่นความถี่และกำกับกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม"*

*[52] มาตรา 7 วางหลักว่า "ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ"*

*[53] มาตรา 8 วางหลักว่า ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ*

บทบัญญัติเกี่ยวกับการให้อำนาจเจ้าหน้าที่เปิดตรวจไปรษณียภัณฑ์ได้ ในมาตรา 25[54] ซึ่งการเปิดตรวจก็มีลักษณะเป็นการแทรกแซงข้อมูลระหว่างการส่งเช่นเดียวกับการดักฟัง

**พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2528** ให้อำนาจสำนักข่าวกรองแห่งชาติดำเนินการอันมีผลกระทบต่อข้อมูลข่าวสาร จากการพิจารณามาตรา 4[55] และมาตรา 3[56] ประกอบกันจะเห็นได้ว่าสำนักงานข่าวกรองแห่งชาติมีอำนาจหน้าที่อันเป็นการเก็บข้อมูลการสื่อสารของบุคคลได้ โดยการ “ดักรับข้อมูล” แต่มีข้อจำกัดคือเฉพาะการดักรับข้อมูลด้วยการติดต่อสื่อสารทางสัญญาณวิทยุ และ การดักรับข้อมูลดังกล่าวต้องเป็นไปเพื่อวัตถุประสงค์เกี่ยวกับการข่าวกรองด้านความเคลื่อนไหวของต่างชาติหรือองค์การก่อการร้าย ไม่อาจดักรับข้อมูลเพื่อการสืบสวนสอบสวนความผิดตามกฎหมายอื่น ๆ

**พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547** พระราชบัญญัติฉบับนี้ให้อำนาจพนักงานสอบสวนคดีพิเศษในการดำเนินการเพื่อให้ได้มาซึ่งข้อมูลข่าวสารที่ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ ทั้งนี้ตามเงื่อนไขในมาตรา 25[57]

**พระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548** กฎหมายฉบับนี้ให้อำนาจนายกรัฐมนตรีโดยความเห็นชอบคณะรัฐมนตรีประกาศให้พนักงานเจ้าหน้าที่มีอำนาจออกคำสั่งกระทำการแทรกแซงการสื่อสารใด ๆ ทั้งนี้เมื่อมีการประกาศสถานการณ์ฉุกเฉินที่มีความร้ายแรง[58]

**พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ.2519** มีหลักการที่ให้อำนาจเจ้าพนักงานได้มาซึ่งข้อมูลข่าวสารที่ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด ทั้งนี้ภายใต้

---

*[54] มาตรา 25 วางหลักว่า “ไปรษณียภัณฑ์ใดที่ส่งทางไปรษณีย์เป็นการฝ่าฝืนต่อบทบัญญัติแห่งพระราชบัญญัตินี้ อธิบดีอาจมีคำสั่งตามควรแก่กรณีกล่าวคือ*
*(1) ให้กักไว้หรือส่งต่อไป หรือส่งกลับคืนไปยังผู้ฝาก หรือให้จำหน่ายเป็นอย่างอื่น*
*(2) ให้เปิดตรวจ หรือทำลายเสียได้ ถ้าจำเป็นและเมื่อทำลายแล้ว ให้แจ้งไปให้ผู้ฝากทราบ*
*(3) ให้ส่งตรงไปยังพนักงานเจ้าหน้าที่ เมื่อมีเหตุสงสัยว่าเป็นความผิดอาญา เพื่อจัดการฟ้องร้อง*

*[55] มาตรา 4 กำหนดให้มีสำนักข่าวกรองแห่งชาติ มีอำนาจและหน้าที่ ดังต่อไปนี้ ...(1) ปฏิบัติงานเกี่ยวกับกิจการการข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการสื่อสาร และการรักษาความปลอดภัยฝ่ายพลเรือน*

*[56] มาตรา 3 นิยาม“การข่าวกรองทางการสื่อสาร” ไว้ว่า “การใช้เทคนิคและการดำเนินกรรมวิธีทางเครื่องมือสื่อสารด้วยการดักรับการติดต่อสื่อสารทางสัญญาณวิทยุ เพื่อให้ได้มาซึ่งข่าวเกี่ยวกับความเคลื่อนไหวของต่างชาติหรือองค์การก่อการร้าย อันอาจจะมีผลกระทบกระเทือนต่อความมั่นคงแห่งชาติ”*

*[57] มาตรา 25 วรรคแรกวางหลักว่า “ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ พนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษา ศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้”*

*[58] มาตรา 11 พระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548*

เงื่อนไขที่กำหนดในมาตรา 14 จัตวา[59]

**พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542** ให้อำนาจเจ้าพนักงานที่เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินมอบหมายเป็นหนังสือ มีอำนาจเข้าถึงบัญชี ข้อมูลการสื่อสาร ข้อมูลคอมพิวเตอร์ แต่ต้องยื่นคำขออนุญาตจากศาลก่อน ดังจะเห็นได้จากมาตรา 46[60] ซึ่งมีหลักการคล้ายคลึงกับมาตรา 25 ของพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 และมาตรา 14 จัตวาของพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ.2519 กล่าวคือ ให้อำนาจเจ้าพนักงานกระทำการได้มาซึ่งข้อมูลข่าวสารของผู้อื่น แต่ต้องขออนุญาตศาลก่อนแต่ขออนุญาตจากศาลที่ต่างกัน กล่าวคือ กฎหมายฉบับนี้ให้ขออนุญาตศาลแพ่ง แต่พระราชบัญญัติป้องกันและปราบปรามยาเสพติดกำหนดให้ขออนุญาตจากอธิบดีผู้พิพากษาศาลอาญา

**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550** มาตรา 18 (6) ให้อำนาจเจ้าพนักงานในการ “ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิด...” แต่การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (6) นี้ มาตรา 19 กำหนดเงื่อนไขให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาต ซึ่งเป็นหลักการที่มีลักษณะคล้ายกับกฎหมายของประเทศออสเตรเลียที่ให้ศาลเป็นผู้มีอำนาจอนุญาตให้ทำการดักรับข้อมูล

**ประมวลกฎหมายวิธีพิจารณาความอาญา** ประมวลกฎหมายวิธีพิจารณาความอาญามีบทบัญญัติที่เกี่ยวข้องกับการได้มาซึ่งข้อมูล และผลของการได้มาซึ่งข้อมูลในการพิจารณาคดี (1) ในส่วนที่เกี่ยวกับการได้มาซึ่งข้อมูลข่าวสารในการสืบสวนสอบสวนคดีอาญาก็คือหลักเกณฑ์เกี่ยวกับการค้น ซึ่งมีหลักสำคัญว่า “ห้ามมิให้ค้นในที่รโหฐานโดยไม่มีหมายค้นหรือคำสั่งของศาล” (มาตรา 93) แต่ก็เป็นกรณีการค้นทางกายภาพ กล่าวคือ ค้นบุคคลหรือ

---

*[59] มาตรา 14 จัตวา วรรคแรกวางหลักว่า “ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด เจ้าพนักงานซึ่งได้รับอนุมัติจากเลขาธิการเป็นหนังสือ จะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้เจ้าพนักงานได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้*

*[60] มาตรา 46 วรรคหนึ่ง แก้ไขเพิ่มเติมโดยพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (ฉบับที่ 2) พ.ศ. 2551 วางหลักว่า “ในกรณีที่มีพยานหลักฐานตามสมควรว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน พนักงานเจ้าหน้าที่ซึ่งเลขาธิการมอบหมายเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลแพ่ง เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชี ข้อมูลทางการสื่อสาร หรือข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็ได้*

สถานที่ มิได้มีบทบัญญัติเกี่ยวกับการได้มาซึ่งข้อมูลโดยการเข้าถึงการสื่อสาร ในหมวดสองว่าด้วยการค้นนั้นมีเพียงมาตรา 105[61] ที่เกี่ยวข้องกับข้อมูลในการสื่อสาร แต่เจ้าหน้าที่ต้องขอคำสั่งศาลและมีขอบเขตที่จำกัดเฉพาะเอกสารที่ส่งทางไปรษณีย์เท่านั้น (2) ในส่วนที่เกี่ยวกับผลของการได้มาซึ่งข้อมูลนั้น จะอยู่ในบทบัญญัติที่เกี่ยวกับพยานหลักฐาน ซึ่งมาตรา 226 อันเป็นหลักทั่วไปเกี่ยวกับการอ้างพยานหลักฐานได้วางหลักไว้ว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็น*พยานชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น* และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน” อย่างไรก็ตาม กฎหมายได้กำหนดข้อยกเว้นสำหรับพยานหลักฐานที่เกิดขึ้นโดยชอบแต่ ได้มาโดยมิชอบในมาตรา 226/1 โดยให้ศาลใช้ดุลพินิจรับฟังพยานหลักฐานดังกล่าวหรือไม่ก็ได้

ในกรณีการดักฟังข้อมูลจากการสื่อสารนั้น อาจแยกพิจารณาได้ว่า หากเจ้าพนักงานมีส่วนก่อให้เกิดการสื่อสารดังกล่าวขึ้น ข้อมูลการสนทนานั้นจะเป็นพยานหลักฐานที่เกิดขึ้นโดยมิชอบ (เทียบเคียงคำพิพากษาฎีกาที่ 2429/2551, 4301/2543) แต่หากเจ้าพนักงานดักรับข้อมูลการสื่อสารที่เกิดขึ้นอยู่แล้วโดยมิได้มีส่วนก่อให้เกิดการสื่อสารนั้น ข้อมูลจากการดักรับข้อมูลในลักษณะดังกล่าวมิใช่ข้อมูลที่ “เกิดขึ้นโดยมิชอบ” อันจะต้องห้ามรับฟังตามมาตรา 226 ประเด็นต่อไปก็คือ พยานหลักฐานที่ได้มาจากการดักฟังนั้น จะถือว่าเป็นพยานหลักฐานที่ “ได้มาเนื่องจากการกระทำโดยมิชอบ” หรือไม่ เนื่องจากแม้การเกิดขึ้นของข้อมูลจะเกิดโดยชอบ แต่การที่เจ้าหน้าที่ทำการดักฟังข้อมูลนั้นมาเป็นการกระทำที่ไม่ชอบ ในประเด็นนี้อาจแยกพิจารณาได้สองกรณีคือ (1) หากเจ้าหน้าที่ผู้ดักฟังหรือดักรับข้อมูลนั้นมีอำนาจกระทำการโดยอาศัยบทบัญญัติของกฎหมายฉบับใดฉบับหนึ่ง ดังนี้ก็ไม่ถือว่าเป็นการได้มาโดยการกระทำที่มิชอบ เพราะมีอำนาจกระทำตามกฎหมาย (2) หากเจ้าหน้าที่ผู้ดักฟังไม่อาจอ้างอำนาจตามกฎหมายฉบับใดฉบับหนึ่งได้ ข้อมูลที่ได้จากการดักฟังหรือดักรับนั้นก็เป็นข้อมูลที่ได้จากการกระทำที่ไม่ชอบ โดยหลักแล้ว มาตรา 226/1 ห้ามมิให้ศาลรับฟังพยานหลักฐานลักษณะนี้แต่ให้ศาลใช้ดุลพินิจว่าจะรับฟังหรือไม่ก็ได้ โดยชั่งน้ำหนักระหว่างผลประโยชน์ในการอำนวย

---

[61] *มาตรา 105 วางหลักว่า “จดหมาย ไปรษณียบัตร โทรเลข สิ่งพิมพ์หรือเอกสารอื่นซึ่งส่งทางไปรษณีย์และโทรเลข จากหรือถึงผู้ต้องหาหรือจำเลย และยังมิได้ส่ง ถ้าเจ้าหน้าที่ต้องการเพื่อประโยชน์แห่งการสอบสวน ไต่สวนมูลฟ้อง พิจารณาหรือการกระทำอย่างอื่นตามประมวลกฎหมายนี้ ให้ขอคำสั่งจากศาลถึงเจ้าหน้าที่ไปรษณีย์โทรเลขให้ส่งเอกสารนั้นมา ...บทบัญญัติแห่งมาตรานี้ไม่ใช้ถึงเอกสารโต้ตอบระหว่างผู้ต้องหาหรือจำเลยกับทนายความของผู้นั้น”*

ความยุติธรรมกับสิทธิเสรีภาพของประชาชน ซึ่งสิทธิเสรีภาพของประชาชนนี้ย่อมหมายรวมถึงสิทธิส่วนบุคคล

**4. วิเคราะห์เปรียบเทียบกฎหมายต่างประเทศกับกฎหมายไทย**

หากเปรียบเทียบกับกฎหมายสหรัฐ-อเมริกาจะเห็นได้ว่า รัฐธรรมนูญของทั้งสหรัฐอเมริกาและไทย ต่างมีบทบัญญัติคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวในการสื่อสารข้อมูล สำหรับกฎหมายลายลักษณ์อักษรที่เกี่ยวกับการดักฟังของสหรัฐอเมริกามีลักษณะแตกต่างจากกฎหมายไทย เนื่องจากกฎหมายสหรัฐอเมริกานั้น วางหลักห้ามการดักฟังอันรวมถึงการดักรับข้อมูลทางสื่ออิเล็กทรอนิกส์เป็นการทั่วไป โดยใช้คำว่า “ผู้ใด” ซึ่งครอบคลุมทั้งการกระทำของเอกชนและเจ้าหน้าที่ของรัฐ ในขณะที่กฎหมายไทยมิได้มีบทบัญญัติเป็นการทั่วไปในการห้ามบุคคลดักฟังหรือดักรับข้อมูล กฎหมายไทยหลายฉบับที่เกี่ยวกับการดักฟังนั้นเป็นกรณีการให้อำนาจเจ้าหน้าที่ในการดักฟังหรือดักรับข้อมูลเฉพาะในบางบริบท เช่น เฉพาะการสืบสวนสอบสวนความผิดบางอย่างตามกฎหมายนั้น ๆ มิได้บัญญัติห้ามการดักฟังการสื่อสารเป็นการทั่วไปไว้ นอกจากนี้ กฎหมายไทยมิได้มีกฎหมายเฉพาะฉบับใดให้อำนาจเอกชนในการดักฟังดังเช่นที่ให้อำนาจเจ้าหน้าที่รัฐ ดังนั้นบุคคลที่ดักฟังจึงไม่อาจอ้างอำนาจตามกฎหมายได้ และอาจเป็นความผิดหากเข้าองค์ประกอบกฎหมายที่เกี่ยวข้อง สำหรับกฎหมายที่อาจกล่าวได้ว่าวางหลักทั่วไปในการห้ามดักฟังหรือดักรับข้อมูลนั้น ในปี พ.ศ. 2544 ประเทศไทยได้มีการตราพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มาตรา 74 ซึ่งวางหลักห้าม “ผู้ใด” กระทำด้วยประการใด ๆ เพื่อดักรับไว้ ซึ่งข้อมูลมีการสื่อสารทางโทรคมนาคมโดยไม่ชอบด้วยกฎหมาย ซึ่งกฎหมายฉบับนี้ครอบคลุมทั้งการกระทำการดักรับโดยเจ้าหน้าที่และบุคคลทั่วไป จึงเทียบเคียงได้กับกฎหมายลายลักษณ์อักษรของสหรัฐอเมริกาทั้งระดับสหรัฐและมลรัฐ แต่กฎหมายของไทยฉบับนี้มีขอบเขตเฉพาะการดักรับข้อมูลที่มีการสื่อสารทางโทรคมนาคม เช่น โทรศัพท์ โทรศัพท์เคลื่อนที่ ต่อมาในปี พ.ศ. 2550 ได้มีการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยมาตรา 8 วางหลักห้ามการดักรับข้อมูลคอมพิวเตอร์ระหว่างการส่ง ซึ่งครอบคลุมทั้งการกระทำการดักรับโดยเจ้าหน้าที่และบุคคลทั่วไป จึงอาจกล่าวได้ว่า กฎหมายไทยสองฉบับดังกล่าวมีลักษณะเป็นการวางหลักทั่วไปในการห้ามดักรับข้อมูล โดยกฎหมายแต่ละฉบับมีขอบเขตที่แตกต่างกัน กล่าวคือ พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มีขอบเขตห้ามการดักรับข้อมูลที่สื่อสารทางโทรคมนาคม

ในขณะที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มีขอบเขตห้ามการดักรับข้อมูลคอมพิวเตอร์

นอกจากนี้ ในการวินิจฉัยคดีเกี่ยวกับการดักฟังนั้น ศาลสหรัฐอเมริกานำหลักการคาดหมายความเป็นส่วนตัว (Expectation of privacy) มาพิจารณาว่าการดักฟังลักษณะใดที่ขัดต่อรัฐธรรมนูญ กล่าวคือ หากการดักฟังนั้น เกิดขึ้นในสถานการณ์ที่ผู้ถูกดักฟังไม่อาจคาดหมายความเป็นส่วนตัวได้ การดักฟังนั้นก็ไม่เป็นการขัดต่อรัฐธรรมนูญ ทั้งนี้ศาลได้จำแนกความแตกต่างระหว่างการดักฟังซึ่งมีการติดตั้งอุปกรณ์การดักฟังในสถานที่สาธารณะ[62] ซึ่งโดยทั่วไปแล้วบุคคลไม่อาจคาดหมายความเป็นส่วนตัวได้ และการติดตั้งอุปกรณ์การดักฟังในสถานที่ส่วนบุคคล[63] ซึ่งโดยทั่วไปแล้วบุคคลอาจคาดหมายความเป็นส่วนตัวได้ ในปัจจุบันศาลยังคงนำหลักดังกล่าวมาปรับใช้ในคดีที่เกี่ยวกับการดักฟังหรือติดตามการเคลื่อนไหวของบุคคลด้วยอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ[64] อย่างไรก็ตาม ในประเทศไทยยังไม่พบการนำหลักดังกล่าวมาใช้ในการวินิจฉัยคดีเกี่ยวกับการดักฟัง

หากเปรียบเทียบกับกฎหมายประเทศออสเตรเลียแล้วจะเห็นได้ว่า พระราชบัญญัติโทรคมนาคม (การดักจับสัญญาณและการเข้าถึง) ค.ศ. 1979 (Telecommunications Interception and Access Act 1979 หรือ TIA) ของประเทศออสเตรเลียกำหนดคุ้มครองสิทธิส่วนบุคคลในด้านการสื่อสารข้อมูลถึงสามระดับ กล่าวคือ ในระดับแรก ขณะทำการสื่อสารข้อมูลนั้นมีกฎหมายห้ามการดักฟัง ในระดับที่สอง เมื่อข้อมูลนั้นถูกสื่อสารแล้วและถูกเก็บรักษาอยู่ในระบบ (Stored communication) ก็มีหลักคุ้มครองการเข้าถึงข้อมูลดังกล่าว ในระดับที่สาม คุ้มครองรายละเอียดแวดล้อมเกี่ยวกับข้อมูลซึ่งมิใช่ตัวเนื้อหาข้อมูลโดยตรง กล่าวคือ รายละเอียดเกี่ยวกับวัน เวลา สถานที่ในการสื่อสารข้อมูล ซึ่งกฎหมายดังกล่าวเป็นการกำหนดห้ามการดักฟังเป็นการทั่วไปทั้งกรณีที่กระทำโดยเจ้าหน้าที่ของรัฐและปัจเจกชน หากเปรียบเทียบกับกฎหมายไทยจะเห็นได้ว่า พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 วางหลักคุ้มครองสิทธิส่วนบุคคลในการสื่อสารข้อมูลทางโทรคมนาคมเช่นกัน แต่มิได้จำแนกการเข้าถึงข้อมูลเป็นสามระดับดังกล่าว

---

[62] *United States v. Knotts, 460 U.S. 276 (1983)*

[63] *United States v. Karo, 468 U.S. 705 (1984)*

[64] *ในคดี United States v. Maynard ซึ่งเป็นกรณีที่เจ้าหน้าที่ติดตั้งอุปกรณ์ Global Positioning System (GPS) ในรถของโจทก์ ศาลนำหลักดังกล่าวมาใช้โดยอธิบายว่า บุคคลทั่วไปไม่อาจคาดหมายได้ว่าจะมีการติดตั้งอุปกรณ์ติดตามความเคลื่อนไหวของตนในสถานที่ต่าง ๆ ตลอดเวลาในช่วงระยะเวลาที่ติดตั้งอุปกรณ์นั้น, United States v. Maynard 615 F.3d, 2010, Harvard Law Review, Constitutional Law – Fourth Amendment – D.C. Circuit Deems warrantless use of GPS Device, January, 124 Harvard Law Review. 827, January, 2011*

เนื่องจากมาตรา 74 มุ่งหมายเฉพาะห้ามการดักรับข้อมูลที่มีการสื่อสารทางโทรคมนาคม อันเปรียบเทียบได้กับการคุ้มครองระดับแรกของกฎหมาย TIA อย่างไรก็ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีบทบัญญัติคุ้มครองสิทธิส่วนบุคคลในข้อมูลคอมพิวเตอร์ทั้งสามระดับ กล่าวคือ การดักรับข้อมูลระหว่างการส่ง (มาตรา 8) การเข้าถึงข้อมูลคอมพิวเตอร์ที่ส่งแล้ว (มาตรา 7) อย่างไรก็ตาม สำหรับในระดับที่สาม กฎหมายไทยมุ่งเน้นการเปิดเผยข้อมูลมากกว่าการคุ้มครองสิทธิส่วนบุคคลเนื่องจากพระราชบัญญัติดังกล่าวกำหนดหน้าที่ให้ผู้ให้บริการทำการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (มาตรา 26) ซึ่งเป็นข้อมูลที่มิใช่ตัวเนื้อหาข้อมูลโดยตรง กล่าวคือ รายละเอียดเกี่ยวกับวัน เวลา สถานที่ในการสื่อสารข้อมูลคอมพิวเตอร์ อันมีลักษณะเดียวกับรายละเอียดแวดล้อมข้อมูลตามกฎหมาย TIA อย่างไรก็ตาม ทั้งกฎหมาย TIA และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของไทยต่างมีบทบัญญัติให้อำนาจเจ้าพนักงานเข้าถึงข้อมูลแวดล้อมดังกล่าวโดยขออนุญาตศาลเช่นเดียวกัน

กฎหมาย TIA ของประเทศออสเตรเลียกำหนดข้อยกเว้นสำหรับกรณีที่สามารถดักฟังการสื่อสารและเข้าถึงข้อมูลการสื่อสารที่ถูกจัดเก็บเมื่อมีหมาย (warrant) หากเปรียบเทียบกับกฎหมายไทยจะเห็นได้ว่ามีหลักการคล้ายคลึงกัน กล่าวคือ มีกฎหมายเฉพาะบางฉบับ ที่ให้อำนาจเจ้าหน้าที่ “ได้มาซึ่งข้อมูลข่าวสาร” ซึ่งรวมถึงการดักฟังและการเข้าถึงข้อมูลที่จัดเก็บไว้ แต่ต้องขออนุญาตศาล เช่น พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างไรก็ตาม กฎหมายไทยมีลักษณะกระจัดกระจาย กล่าวคือ หลักกฎหมายที่ให้อำนาจเจ้าหน้าที่ดักฟังโดยต้องขออนุญาตศาลนั้น กำหนดไว้ในกฎหมายที่เกี่ยวข้องกับความผิดบางประเภทเป็นรายฉบับไป มิได้อยู่ในกฎหมายฉบับหลักดังเช่นกฎหมาย TIA ของออสเตรเลีย

หากพิจารณาการดักฟังประเภทต่าง ๆ อาจวิเคราะห์เปรียบเทียบกฎหมายต่างประเทศและกฎหมายไทยสำหรับการดักฟังแต่ละประเภทดังนี้

(1) การดักฟังที่กระทำทางกายภาพ โดยมีการบุกรุกทางกายภาพ (Eavesdrop accomplished by physical intrusion) ซึ่งกรณีนี้ตามกฎหมายสหรัฐอเมริกาหากเป็นการบุกรุกทางกายภาพย่อมขัดต่อรัฐธรรมนูญฉบับแก้ไขครั้งที่ 4 สำหรับกฎหมายไทยจะเห็นได้ว่า หากเป็นการกระทำโดยเจ้าหน้าที่รัฐก็จะต้องพิจารณาว่าเป็นการเข้าไปค้นโดยชอบตามบทบัญญัติ

ว่าด้วยการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาหรือไม่ หากเข้าไปโดยชอบเช่นมีหมายค้น ก็จะไม่เป็นความผิดฐานบุกรุก หากเป็นการเข้าไปโดยเอกชนย่อมเป็นความผิดฐานบุกรุกตามประมวลกฎหมายอาญา

(2) การดักฟังที่กระทำทางกายภาพโดยใช้อุปกรณ์อิเล็กทรอนิกส์ (Eavesdrop accomplished by electronic device) ซึ่งผู้ดักฟังมิได้บุกรุกเข้าไป ตามกฎหมายสหรัฐอเมริกาก่อนปี ค.ศ. 1967 ศาลตัดสินว่าไม่ขัดต่อรัฐธรรมนูญเนื่องจากมิได้มีการบุกรุกเข้าไป ต่อมาในคดี Katz v.United States ซึ่งตัดสินในปี ค.ศ. 1967 ศาลได้วางหลักว่า การดักฟังอันมีลักษณะกระทำทางกายภาพซึ่งใช้วิธีการอิเล็กทรอนิกส์ในการดักฟัง (Eavesdrop accomplished by electronic means) แม้ว่าผู้กระทำไม่ได้มีการเข้าไปทางกายภาพอันเป็นการบุกรุก ศาลก็ยังถือว่าเป็นการกระทำที่ขัดต่อรัฐธรรมนูญฉบับแก้ไขครั้งที่ 4 เนื่องจากรัฐธรรมนูญดังกล่าวมุ่งเน้นที่การคุ้มครองตัวบุคคล มิใช่สถานที่ ต่อมาในคดี United States v.Knotts ศาลได้นำหลัก “การคาดหมายความเป็นส่วนตัว” (Expectation of privacy) มาพิจารณา หากเป็นการกระทำที่ทำให้ได้มาซึ่งข้อมูลอันไม่อาจเห็นด้วยตาเปล่าจากที่สาธารณะดังกล่าว บุคคลก็ยังอาจคาดหมายความเป็นส่วนตัวได้แม้ว่าจะอยู่ในที่สาธารณะ ดังนั้นหากมีประเด็นพิจารณาว่าการดักฟังนั้นขัดต่อรัฐธรรมนูญหรือไม่ ศาลจะนำหลักความคาดหมายความเป็นส่วนตัวมาพิจารณาเป็นกรณีไป หากพิจารณากฎหมายไทยแล้วจะเห็นได้ว่าหากมีกฎหมายเฉพาะให้อำนาจการ “ได้มาซึ่งข้อมูลข่าวสาร” เช่น กฎหมายเกี่ยวกับคดีพิเศษ กฎหมายเกี่ยวกับยาเสพติด กฎหมายเกี่ยวกับการฟอกเงิน ดังนี้การใช้อุปกรณ์ดังกล่าวก็อาจทำได้โดยชอบ หากมิได้มีกฎหมายให้อำนาจ การกระทำดังกล่าวจะต้องพิจารณาพฤติกรรมนั้นว่าเข้าองค์ประกอบความผิดของกฎหมายที่เกี่ยวข้องหรือไม่ หากเป็นการกระทำของปัจเจกชนทั่วไปซึ่งมิได้มีกฎหมายให้อำนาจก็จะต้องพิจารณากฎหมายแพ่งลักษณะละเมิดและกฎหมายอาญาที่เกี่ยวข้อง เช่น หากการติดตั้งอุปกรณ์ดังกล่าวทำให้เกิดความเสียหายต่อทรัพย์สินของผู้อื่น อาจเข้าองค์ประกอบความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญา เป็นต้น

(3) การดักฟังที่กระทำต่อการสื่อสารอันเป็นการแทรกแซงการสื่อสารข้อมูลระหว่างบุคคล (Intercept or Wiretap) เช่น ดักฟังโทรศัพท์ ดักรับข้อมูลอิเล็กทรอนิกส์ ดังนี้ตามกฎหมายสหรัฐอเมริกามีกฎหมายลายลักษณ์อักษรที่เกี่ยวข้องโดยตรง กล่าวคือจะต้องพิจารณารัฐบัญญัติว่าด้วยการสื่อสารสหรัฐ โดยศาลวินิจฉัยว่าการดักฟังสองประเภทดังกล่าวข้างต้นที่มิใช่กระทำต่อระบบการสื่อสารโดยตรง เช่น การติดตั้ง

อุปกรณ์ดักฟังการสนทนาในสถานที่แห่งใดแห่งหนึ่ง (Eavesdrop) ไม่ขัดต่อรัฐบัญญัติดังกล่าว เนื่องจากมิใช่การแทรกแซงระบบการสื่อสาร[65] สำหรับการดักรับข้อมูลทางสาย เช่น โทรศัพท์ หรือการสื่อสารไร้สาย เช่น การสื่อสารข้อมูลอิเล็กทรอนิกส์ จะขัดต่อกฎหมายนี้ สำหรับกฎหมายไทยก็จะต้องพิจารณากฎหมายที่เกี่ยวข้องว่ามีกฎหมายฉบับใดให้อำนาจหรือไม่ซึ่งในกรณีที่เป็นการกระทำโดยเจ้าหน้าที่ของรัฐจะมีกฎหมายหลายฉบับที่ให้อำนาจไว้ แต่ในกรณีบุคคลทั่วไปนั้นมิได้มีกฎหมายให้อำนาจไว้ หากกระทำการดักฟังจะต้องพิจารณาความผิดตามกฎหมายที่เกี่ยวข้อง

**5. สรุป**

ในระบบกฎหมายไทยในปัจจุบันยังไม่มีกฎหมายเฉพาะซึ่งวางหลักคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวจากการถูกดักฟังโดยวางองค์ประกอบความผิดฐานดักฟังเป็นการทั่วไปที่ครอบคลุมตัวผู้กระทำทั้งที่เป็นเจ้าหน้าที่รัฐและเอกชน และครอบคลุมการดักรับข้อมูลการสื่อสารทุกประเภทไว้ในกฎหมายฉบับเดียว แต่การคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวและการให้อำนาจเจ้าพนักงานกระจัดกระจายตามกฎหมายหลายฉบับ ซึ่งอาจแยกสรุปได้ดังนี้

- ในกรณีกฎหมายที่คุ้มครองสิทธิในความเป็นอยู่ส่วนตัวโดยวางหลักห้ามการดักฟังหรือดักรับข้อมูลนั้น จะเห็นได้ว่า กฎหมายบางฉบับ วางหลักห้ามดักรับข้อมูลเฉพาะบางประเภทและมีข้อจำกัดด้านตัวผู้กระทำ เช่น ประมวลกฎหมายอาญา กฎหมายบางฉบับแม้จะวางหลักห้ามการดักรับข้อมูลโดยไม่จำกัดตัวผู้กระทำ กล่าวคือ ครอบคลุมทั้งเจ้าพนักงานและปัจเจกชน แต่ก็วางหลักคุ้มครองการแทรกแซงข้อมูลเฉพาะบางลักษณะ เช่น ทางโทรคมนาคม (พระราชบัญญัติการประกอบกิจการโทรคมคนคม) ทางวิทยุคมนาคม (พระราชบัญญัติวิทยุคมนาคม) ข้อมูลคอมพิวเตอร์ (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์) เมื่อเปรียบเทียบกับกฎหมายต่างประเทศจะเห็นได้ว่า ประเทศไทยยังไม่มีกฎหมายเฉพาะที่วางหลักคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวกรณีการดักฟังหรือดักรับข้อมูลไว้เป็นการทั่วไปที่ครอบคลุมการสื่อสารช่องทางต่าง ๆ

- ในกรณีกฎหมายที่ให้อำนาจเจ้าพนักงานในการดักรับข้อมูล จะเห็นได้ว่า กฎหมายบางฉบับ เช่น พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 แม้ว่ามีองค์ประกอบของการกระทำของเจ้าพนักงานที่กว้าง กล่าวคือ “การได้มาซึ่งข้อมูลข่าวสาร” มีความหมายกว้าง ครอบคลุมลักษณะการ

[65] *Goldman V United States, Irvine v. California, On Lee v. United States*

กระทำทั้ง ดักฟัง ดักรับข้อมูลระหว่างการสื่อสาร เข้าถึงข้อมูลการสื่อสารที่จัดเก็บไว้แล้ว นอกจากนี้ยังครอบคลุมข้อมูลทางสื่อต่าง ๆ ทั้งทางไปรษณีย์ โทรศัพท์ โทรสาร สื่ออิเล็กทรอนิกส์ แต่ก็มีขอบเขตจำกัดคือ จะต้องเป็นการได้มาซึ่งข้อมูลข่าวสารที่เกี่ยวข้องกับความผิดตามกฎหมายนั้น ๆ สำหรับกฎหมายบางฉบับ เช่น พระราช-บัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีองค์ประกอบของการกระทำของเจ้าพนักงานที่แคบกว่า คือ การตรวจสอบและเข้าถึงข้อมูลคอมพิวเตอร์เท่านั้น และมีขอบเขตจำกัด คือ จะต้องเป็นไปเพื่อสืบสวนหาตัวผู้กระทำผิดตามกฎหมายดังกล่าวเท่านั้น จะเห็นได้ว่ากฎหมายของไทยที่ให้อำนาจเจ้าพนักงานในการดักรับข้อมูลมีลักษณะกระจัดกระจาย ซึ่งแตกต่างกับกฎหมายสหรัฐอเมริกาและออสเตรเลียที่มีกฎหมายหลักกำหนดห้ามการดักฟังและกำหนดข้อยกเว้นการดักฟังในกรณีความผิดต่าง ๆ ไว้ในกฎหมายฉบับนั้น

**6. ข้อเสนอแนะ**

จากปัญหาดังที่ได้วิเคราะห์มาดังกล่าว ผู้เขียนจึงมีข้อเสนอแนะการปรับปรุงแก้ไขกฎหมายไทย บนพื้นฐานของตัวแบบกฎหมายต่างประเทศที่ได้ศึกษาในบทความนี้ ดังต่อไปนี้

1. เสนอให้มีการบัญญัติกฎหมายเฉพาะที่วางหลักห้ามการดักฟังเป็นการทั่วไปเพื่อกำหนดฐานความผิดเกี่ยวกับการดักฟังซึ่งครอบคลุมผู้กระทำทั้งเจ้าพนักงานและปัจเจกชน โดยตราเป็นพระราชบัญญัติคุ้มครองความเป็นส่วนตัวในการสื่อสาร มีองค์ประกอบความผิดหลักว่า “ห้ามผู้ใดกระทำการดักฟังการสื่อสารของผู้อื่น” โดยนิยามความหมายของ “การดักฟัง” ตามกฎหมายดังกล่าว ให้ครอบคลุมการสื่อสารข้อมูลช่องทางต่าง ๆ ทั้งการสื่อสารทางสาย ทางอิเล็กทรอนิกส์ และทางวาจา

2. นำหลักการคาดหมายความเป็นส่วนตัว (Expectation of privacy) ของการสื่อสารข้อมูล มาเป็นข้อยกเว้นความผิดกล่าวคือ หากการดักฟังกระทำต่อการสื่อสารที่ผู้ถูกดักฟังไม่อาจคาดหมายความเป็นส่วนตัวได้ การดักฟังนั้นไม่เป็นความผิด

3. กำหนดข้อยกเว้นการดักฟังในกรณีที่คู่กรณีทุกฝ่ายที่เกี่ยวข้องกับการสื่อสารดังกล่าวให้ความยินยอมกับการดักรับข้อมูลการสื่อสาร (All-party consent rule)

4. สำหรับการดักฟังโดยเจ้าพนักงานตามกฎหมายเฉพาะต่าง ๆ นั้น มีข้อเสนอสองแนวทาง กล่าวคือ แนวทางแรก เสนอให้แก้ไขกฎหมายฉบับต่าง ๆ ดังกล่าว โดยยกเลิกบทบัญญัติในส่วนที่ให้อำนาจในการ

ดักฟัง เพื่อให้การดักฟังของเจ้าพนักงานอยู่ภายใต้พระราชบัญญัติคุ้มครองความเป็นส่วนตัวในการสื่อสาร อันเป็นกฎหมายฉบับหลักเพียงฉบับเดียว โดยในพระราชบัญญัตินี้จะกำหนดหลักเกณฑ์และกระบวนการในการดักฟังของเจ้าพนักงานสำหรับความผิดต่าง ๆ เอาไว้ แนวทางที่สอง กำหนดข้อยกเว้นในพระราชบัญญัติคุ้มครองความเป็นส่วนตัวในการสื่อสาร สำหรับกรณีการดักฟังที่กระทำโดยเจ้าพนักงานผู้มีอำนาจตามกฎหมายเฉพาะ โดยไม่จำต้องแก้ไขกฎหมายเฉพาะต่าง ๆ ดังนั้น การดักฟังตามพระราชบัญญัตินี้จะครอบคลุมเฉพาะการดักฟังที่กระทำโดยปัจเจกชนและเจ้าพนักงานที่ไม่มีอำนาจตามกฎหมายเฉพาะ

## ▣ บรรณานุกรม


**ภาษาไทย**

คณาธิป ทองรวีวงศ์, กฎหมายเกี่ยวกับการสื่อสารมวลชน. กรุงเทพฯ:สำนักพิมพ์นิติธรรม. 2555.

**ภาษาอังกฤษ**

Blackstone, William, Commentaries on the Law of England (1769)

Charles A. Pulaski, Authorizing Wiretap Applications under Title III: Another Dissent to Giordano and Chavez, University of Pennsylvania Law Review, April, 1975.

Daniel R. Dinger, Should Parents Be Allowed to Record a Child's Telephone Conversations When They Believe the Child Is in Danger: An Examination of the Federal Wiretap Statute and the Doctrine of Vicarious Consent in the Context of a Criminal Prosecution, Seattle University Law Review, 955, 2004-2005.

Harvard Law Review, Constitutional Law – Fourth Amendment – D.C. Circuit Deems warrantless use of GPS Device, January, 124 Harvard Law Review. 827, January, 2011

James G. Carr and Patricia L. Bellia, The Law of Electronic Surveillance, West, 2011.

Matthew, Bierlein, Policing the Wireless World : Access Liability in the Open Wi-Fi Era, Ohio State Law Journal, 2006.

Matt L. Greenberg, Law Enforcement Officers with Clean Hands May not Make Investigative use of a wiretap that was Illegal acquired by a third party, University of Cincinnati Law Review ,Winter, 2000

Priscilla M. Regan, Legislating Privacy : Technology, Social Value and

Public Policy, The University of North Carolina Press, 1995.

Smith, Robert Ellis, Ben Franklin's Web Site : Privacy and Curiosity from Plymouth Rock to the Internet ,2000.

Telecommunications (Interception and Access) Act 1979, Report for the year 2011 [Online] available from, Australian Attorney-General's Department Website : http:/www.ag.gov.au/Publications

Whitfield, Diffie and Landau, Susan. Privacy on the Line: The Politics of Wiretapping and Encryption. Cambridge: MIT Press, 1998.

**คำพิพากษาศาลต่างประเทศ**

Berger v. New York - 388 U.S. 41 (1967)

Goldman v. United States - 316 U.S. 129 (1942)

Irvine v. California - 347 U.S. 128 (1954)

Katz v. United States, 389 U.S. 347 (1967)

Nardone v. United States - 308 U.S. 33, (1939)

Olmstead v. United States, 277 U.S. 438 (1928)

Silverman v. United States - 365 U.S. 505 (1961)

United States v. Knotts, 460 U.S. 276 (1983)

United States v. Karo, 468 U.S. 705 (1984)

United States v. Maynard 615 F.3d at 558, 2010