สรุปข้อคิดเห็นของ คณาธิป ทองรวีวงศ์ ต่อร่างกฎหมายดักฟัง ในการสัมมนาจัดโดยพลเมืองเน็ต 22 ธค 2557

# ข้อพิจารณา 9 ประการ ต่อข้อเสนอร่างกฎหมายใหม่ที่ให้อำนาจเจ้าพนักงานดักรับข้อมูลการสื่อสาร[1]

คณาธิป ทองรวีวงศ์[2]

จากร่างข้อเสนอแก้ไข ปวิอ โดยเพิ่มบทบัญญัติการให้อำนาจเจ้าพนักงานดักรับข้อมูลการสื่อสาร

มาตรา 131/2 ( https://thainetizen.org/wp-content/uploads/2014/12/criminal-procedure-amendment-info-access-rights-to-silence.pdf )

ผู้เขียนขอเสนอความคิดเห็นทางวิชาการว่า โดยหลักการแล้ว การมีกฎหมายเกี่ยวกับการดักรับข้อมูล สามารถพบได้ทั่วไปในระบบกฎหมายของประเทศต่างๆ โดยกฎหมายการดักรับข้อมูลการสื่อสารอยู่บนพื้นฐานของแนวคิดการควบคุมอาชญากรรม (Crime control) ที่ให้อำนาจเจ้าพนักงานในการรวบรวมพยานหลักฐานอันเกี่ยวกับความผิดโดยเฉพาะในยุคของเทคโนโลยีสารสนเทศซึ่งพยานหลักฐานที่สำคัญของการกระทำผิดมักจะปรากฏในการสื่อสารช่องทางต่างๆ อย่างไรก็ตาม กฎหมายเกี่ยวกับการดักฟังที่จะบัญญัติขึ้นจะต้องหาจุดสมดุลระหว่างการควบคุมอาชญากรรมกับการคุ้มครองสิทธิส่วนบุคคลด้วย เพราะโดยหลักแล้วการดักรับข้อมูลย่อมเป็นการกระทบสิทธิส่วนบุคคลในการสื่อสารโดยตรง

บทบัญญัติของกฎหมายที่จะมีขึ้นจะต้องสะท้อนถึงการประสานสมดุลระหว่างประโยชน์สองประการดังกล่าวข้างต้น โดยผู้เขียนมีข้อพิจารณาว่า กฎหมายที่ให้อำนาจเจ้าพนักงานดักรับข้อมูล อย่างน้อยควรสอดคล้องกับหลักเกณฑ์ 9 ประการตามที่ผู้เขียนเสนอขึ้น โดยวิเคราะห์ขึ้นมาจากแนวทางของกฎหมายประเทศต่างๆ ข้อพิจารณา 9 ประการ มีดังต่อไปนี้

**ประการที่ 1** จะต้องมีการกำหนดกฎหมายวางหลัก ห้ามดักรับข้อมูลการสื่อสาร เป็นการทั่วไป เสียก่อน เพื่อเป็นหลักในการคุ้มครองสิทธิส่วนบุคคล สำหรับกฎหมายการดักรับข้อมูลเพื่อการป้องกันและปราบปรามอาชญากรรม ควรบัญญัติขึ้นในฐานะเป็นข้อยกเว้นของหลักทั่วไปดังกล่าว

หากเปรียบเทียบกับยุโรปจะเห็นได้ว่า มีการกำหนดหลักการคุ้มครองสิทธิส่วนบุคคลในการสื่อสารข้อมูลไว้เป็นหลัก (Right to respect for his correspondence)[3] การดักรับข้อมูลจะมีได้แต่โดยอาศัยอำนาจตามกฎหมายที่มีการบัญญัติไว้ โดยกฎหมายดักรับข้อมูลที่เป็นข้อยกเว้นดังกล่าวจะต้องมีลักษณะและขอบเขตที่จำกัด ทั้งนี้เพื่อเป็นการป้องกันความเสี่ยง

---

1 ข้อพิจารณานี้ผู้เขียนได้นำเสนอในการสัมมนาทางวิชาการ 22 ธันวาคม 2557 จัดโดยเครือข่ายพลเมืองเน็ต ณ คณะเศรษฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์

2 รองศาสตราจารย์ คณะนิติศาสตร์, นักวิชาการด้านกฎหมายสิทธิส่วนบุคคล , kanathip@yahoo.com, www.thaiprivacylaw.com

3 **Article 8 ECHR**

ต่อการใช้อำนาจตามอำเภอใจ ( the risk of arbitrariness) และการใช้อำนาจดังกล่าวไปในทางมิชอบ ( the risk of abuse of phone interceptions )

ทั้งนี้เนื่องจากในปัจจุบัน อาจกล่าวได้ว่า ไทยยังไม่มีกฎหมายที่บัญญัติห้ามการดักรับข้อมูลเป็นการทั่วไปไว้เลย โดย ณ เดือน ธันวาคม 2557 ไม่มีบทบัญญัติรัฐธรรมนูญที่คุ้มครองสิทธิส่วนบุคคลรวมทั้งสิทธิในการติดต่อสื่อสารของประชาชน นอกจากนี้ พระราชบัญญัติต่างๆ ก็ยังไม่มีที่วางหลักห้ามการดักรับข้อมูลเป็นการทั่วไป ในทางตรงข้าม มีพระราชบัญญัติหลายฉบับที่ให้อำนาจเจ้าพนักงานตามกฎหมายนั้น ทำการดักรับข้อมูลหรือได้มาซึ่งข้อมูลเพื่อประโยชน์ในการปฏิบัติการตามกฎหมายนั้นๆ [4] กฎหมายที่อาจกล่าวได้ว่าวางหลักห้ามดักรับข้อมูลโดยตรง มีเพียง พรบ ประกอบกิจการฯ ม 74 แต่ครอบคลุม เฉพาะ ข้อมูลโทรคมนาคม ซึ่งแตกต่างจากกฎหมายสหรัฐอเมริกา ซึ่ง*มีการห้ามดักรับข้อมูลการสื่อสารครบถ้วน ทั้งการสื่อสารด้วยวาจา การสื่อสารทางสาย และการสื่อสารข้อมูลอิเล็กทรอนิกส์ (Oral , wire, electronic communication*) ดังนั้น หากจะมีการบัญญัติกฎหมายให้อำนาจเจ้าพนักงานดักรับข้อมูล ก็ควรบัญญัติในฐานะข้อยกเว้นโดยมีการเพิ่มเติมกฎหมายห้ามดักรับข้อมูลทั่วไปไว้ก่อนดังกล่าว

4 คณาธิป ทองรวีวงศ์ , มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวของผู้ถูกดักฟังการสื่อสารข้อมูล, วารสารกระบวนการยุติธรรม,ปีที่ 6 เล่ม 1 มกราคม-เมษายน 2556.

**ประการที่ 2** กฎหมายที่ให้อำนาจดักรับข้อมูลการสื่อสาร ควรต้องมีลักษณะ เฉพาะเจาะจง ในเชิงมาตรการ (Measures) ตัวอย่างของคดีที่ศาลสิทธิมนุษยชนยุโรปตัดสินไว้ เช่น กฎหมายภายในซึ่งกำหนดให้อำนาจดักรับข้อมูลที่ระบุให้ใช้มาตรการใดๆที่เจ้าหน้าที่เห็นว่าจำเป็น ( 'any investigative measure he considers necessary' ) ขัดต่อมาตรา 8 เนื่องจากมิได้กำหนดมาตรการไว้เฉพาะเจาะจงอย่างเพียงพอ[5]

หากพิจารณากฎหมายไทยที่ให้อำนาจเจ้าพนักงานดักรับข้อมูลหลายฉบับ ผู้เขียนเห็นว่า ให้อำนาจเจ้าพนักงานกระทำการเกี่ยวกับการดักรับข้อมูลไว้ค่อนข้างกว้างและไม่เฉพาะเจาะจง ดังจะเห็นได้จากการใช้ถ้อยคำ "เพื่อให้ได้มาซึ่งข้อมูล..." พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 มาตรา 25[6] พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ.2519 มาตรา 14 จัตวา[7] พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 มาตรา 46 วรรคแรก[8]

ดังนั้น กฎหมายใหม่ที่ให้อำนาจเจ้าพนักงานดักรับข้อมูล ควรพิจารณากำหนดมาตรการให้มีลักษณะชัดเจนและเจาะจงมากกว่าการใช้ถ้อยคำกว้างดังกล่าว สำหรับร่างกฎหมายดักรับข้อมูลที่นำเสนอในการสัมมนานี้ ผู้เขียนเห็นว่าเมื่อพิจารณาเกณฑ์ข้อนี้แล้วน่าจะสอดคล้องกันเนื่องจากมีการกำหนดลักษณะมาตรการไว้เฉพาะเจาะจงซึ่งแตกต่างจากกฎหมายฉบับก่อนๆของไทยดังกล่าวข้างต้น

---

5 KRUSLIN v. FRANCE , 24 April 1990

6 มาตรา 25 วรรคแรก วางหลักว่า " ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เ ป็นคดีพิเศษ พนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษา ศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้"

7 มาตรา 14 จัตวา วรรคแรกวางหลักว่า "ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด เจ้าพนักงาน ซึ่งได้รับอนุมัติจากเลขาธิการเป็นหนังสือ จะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้เจ้าพนักงานได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้

8 มาตรา 46 วรรคหนึ่ง แก้ไขเพิ่มเติมโดยพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (ฉบับที่ 2) พ.ศ. 2551 วางหลักว่า "ในกรณีที่มีพยานหลักฐานตามสมควรว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน พนักงานเจ้าหน้าที่ซึ่งเลขาธิการมอบหมายเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลแพ่ง เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชี ข้อมูลทางการสื่อสาร หรือข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็ได้

**ประการที่ 3** กฎหมายที่ให้อำนาจดักรับข้อมูลการสื่อสาร ควรต้องมีลักษณะ เฉพาะเจาะจง ในแง่ของความผิดที่เข้าข่ายอาจถูกดักรับข้อมูลได้ ทั้งนี้เพื่อสอดคล้องกับหลักการคาดหมายได้ (Forseeability)

สำหรับการกำหนดความผิดที่เข้าข่ายนั้นมีประเด็นว่าจำต้องระบุเฉพาะเจาะจงเป็นรายฐานความผิดเลยหรือไม่ หากพิจารณาแนวทางของกฎหมายประเทศต่างๆ เห็นว่ามีสองแนวทางหลักดังนี้

- แนวทางแรก กำหนดเป็นบัญชีรายชื่อของฐานความผิดที่เฉพาะเจาะจง ซึ่งกรณีนี้จะชัดเจนว่า ความผิดใดที่อาจนำไปสู่อำนาจในการดักรับข้อมูลได้ กฎหมายที่ใช้วิธีการตามแนวทางนี้ เช่น กฎหมายของสหรัฐอเมริกา (Omnibus Crime control Act , section 2516 ) ซึ่งได้ระบุฐานความผิดแยกเป็นรายฐานความผิดว่า ความผิดใดที่อาจถูกดักรับข้อมูลได้
- แนวทางที่สอง มิได้กำหนดฐานความผิดหรือบัญชีรายชื่อฐานความผิด แต่กำหนดเกณฑ์ที่เฉพาะเจาะจงไว้ (Specific criteria) เพื่อนำไปพิจารณาว่า ความผิดในกรณีนั้นๆจะสามารถดักรับข้อมูลได้หรือไม่

ตัวอย่าง ศาลสิทธิมนุษยชนยุโรปเคยตัดสินว่า[9] กฎหมายที่กำหนดให้อำนาจดักรับข้อมูลในความผิด ร้ายแรง ร้ายแรงมาก ร้ายแรงที่สุด นั้น กว้างเกินไป แม้ว่ามีการกำหนดนิยามสำหรับความผิดทั้งสามกรณีดังกล่าว แต่ศาลเห็นว่า ฐานความผิดต่างๆตามกฎหมายอาญาอาจจัดอยู่ในความผิดทั้งสามกลุ่มได้ทั้งสิ้น จึงเห็นว่า การกำหนดความผิดสามกรณีดังกล่าวที่อาจถูกดักรับข้อมูลได้นั้น เป็นการกำหนดที่กว้างเกินไป ไม่สอดคล้องกับอนุสัญญาฯมาตรา 8 ดังนั้น หากร่างกฎหมายใหม่บัญญัติความผิดที่อาจถูกดักรับข้อมูลได้ไว้กว้าง เช่น “ความผิดที่ยุ่งยากซับซ้อน” โดยมิได้กำหนดนิยามหรือขอบเขตว่าความผิดอย่างไรยุ่งยากซับซ้อน อาจทำให้ครอบคลุมความผิดต่างๆในกฎหมายอาญาจำนวนมาก ซึ่งเมื่อเทียบกับกรณีของยุโรปแล้วอาจกล่าวได้ว่ามีลักษณะกว้างเกินไปไม่สอดคล้องกับหลัก “คาดหมายได้” (Forseeability)

**ประการที่ 4** กฎหมายที่ให้อำนาจดักรับข้อมูลการสื่อสาร ควรต้องมีลักษณะ เฉพาะเจาะจง ในแง่บุคคลที่จะตกเป็นเป้าหมายของการดักรับข้อมูล

ตัวอย่างของยุโรปจะเห็นจากคดีที่กฎหมายภายในซึ่งให้อำนาจเจ้าพนักงานดักรับข้อมูลโดยกำหนดกลุ่มเป้าหมายของบุคคลที่จะถูกดักรับข้อมูลไว้ว่า ผู้ต้องสงสัย จำเลย หรือ บุคคลอื่นใดที่อาจเกี่ยวข้องกับการกระทำความผิอาญา (suspect, defendant or other person involved in a criminal offence)[10] นั้น ศาลวินิจฉัยว่าเป็นกฎหมายที่กว้างเกินไปขาดลักษณะเฉพาะเจาะจง โดยเฉพาะกรณี “บุคคลอื่นใดที่อาจเกี่ยวข้องกับการกระทำความผิอาญา” ซึ่งไม่มีคำอธิบายหรือคำนิยามกำหนดขอบเขตของคำดังกล่าวด้วย[11] ดังนั้นศาลเห็นว่ากฎหมายดังกล่าว ไม่สอดคล้องกับอนุสัญญาฯมาตรา 8

---

9 Iordachi v Moldava 10 February 2009

10 Article 156 § 1 of the Criminal Code, Molddava : Iordachi v Moldava 10 February 2009

11 อย่างไรก็ตาม หากกฎหมายนั้นกำหนดเป้าหมายของผู้ถูกดักรับข้อมูลโดยใช้ถ้อยคำกว้าง แต่มีการกำหนดอธิบายขอบเขตนิยามของบุคคลผู้เป็นเป้าหมายไว้ ก็เป็นกฎหมายที่ไม่ขัดแย้งต่ออนุสัญญาฯมาตรา 8 เช่น the Act of 13 August 1968 on Restrictions on the Secrecy of the Mail, Post and Telecommunications (Klass v Germany)

**ประการที่ 5** กฎหมายที่จะกำหนดขึ้นควรมีหลักการหรือมาตรการในการคุ้มครองสิทธิส่วนบุคคลของบุคคลที่สาม (Third party) ซึ่งมิได้มีส่วนร่วมในความผิดที่ดักรับข้อมูล แต่มีส่วนร่วมในการสื่อสารข้อมูลที่ถูกดักรับ กรณีนี้ผู้เขียนเห็นต่อไปว่า อาจต้องมีการจำแนกความแตกต่างระหว่างการดักรับข้อมูลประเภทที่ครอบคลุมการสื่อสารปริมาณมากเกี่ยวข้องกับบุคคลหลายฝ่าย โดยใช้คำสำคัญในการคัดกรองหาคำที่ตั้งโปรแกรมไว้ (Strategic monitoring) กับ การดักรับข้อมูลที่มุ่งหมายถึงการสื่อสารของคู่สนทนาโดยเฉพาะเจาะจง (Individual monitoring )

**ประการที่ 6.** กฎหมายที่ให้อำนาจดักรับข้อมูลจะต้องมีการกำหนดช่วงระยะเวลา (Duration) ในการดักรับข้อมูลที่ชัดเจน ทั้งนี้แม้ว่า กฎหมายดังกล่าวอาจกำหนดให้เจ้าพนักงานยื่นคำขอศาลเพื่อต่อระยะเวลาได้ก็ตาม สำหรับระยะเวลานั้นตามกฎหมายประเทศต่างๆมีความแตกต่างกันไป เช่น สามเดือน[12] สองเดือน[13] เป็นต้น

**ประการที่ 7** กฎหมายที่กำหนดให้อำนาจดักรับข้อมูลจะต้องสอดคล้องกับหลัก "*การเข้าถึงและตรวจสอบได้โดยประชาชน (Public scrutiny)*" กล่าวคือ *คำร้องขอดักรับข้อมูลที่เจ้าพนักงานยื่นขอต่อศาลจะต้องระบุเหตุผลความจำเป็น รายละเอียดประเภทลักษณะข้อมูลที่ต้องการ วิธีการใช้เข้าถึงข้อมูล* หลักดังกล่าวจะเห็นได้จากกรณีของยุโรปในคดีที่ประเด็นพิพาทเกี่ยวข้องกับกฎหมายสหราชอาณาจักรเกี่ยวกับการดักรับข้อมูล[14] ศาลเห็นว่าแม้กฎหมายดังกล่าวจะมีการกำหนดกระบวนการยื่นคำขอเพื่อดักรับข้อมูล แต่มิได้มีการกำหนดให้คำร้องหรือรายละเอียดในการขออนุญาตเพื่อสอดคล้องกับกฎหมายดังกล่าวจะต้องเผยแพร่ต่อสาธารณะด้วย ทั้งนี้แม้ทางฝ่ายรัฐบาลจะแย้งว่า รายละเอียดดังกล่าวมีปรากฏในแนวปฏิบัติภายใน ( internal guidelines) แต่ไม่อาจเผยแพร่ได้เนื่องจากอาจกระทบต่อประสิทธิภาพของมาตรการ แต่ศาลก็ยังเห็นว่า รายละเอียดเกี่ยวกับการดักรับข้อมูลควรเผยแพร่ต่อสาธารณะเพื่อประโยชน์ในการตรวจสอบได้ จะเห็นได้ว่า ในการพิจารณาระหว่าง ความมั่นคง (Public security) และ การตรวจสอบได้จากสาธารณะ (Public scrutiny) นั้น ศาลในคดีนี้ให้น้ำหนักไปในทาง การตรวจสอบจากสาธารณะ

---

12 three months with the possibility of renewal (Weber and Saravia v Germany)

13 two months with the possibility of renewal (Association for European Integration and Ekhimdziev v Bulgaria)

14 CASE OF LIBERTY AND OTHERS v. THE UNITED KINGDOM 1 July 2008

**ประการที่ 8** สำหรับประเด็นที่ว่า ร่างกฎหมายเกี่ยวกับการดักรับข้อมูลนี้ จะซ้ำซ้อนกับกฎหมายที่ให้อำนาจเจ้าพนักงานในการดักรับข้อมูลฉบับอื่นๆที่มีผลบังคับใช้อยู่ในปัจจุบันหรือไม่นั้น ผู้เขียนเห็นว่า เมื่อพิจารณากฎหมายที่ให้อำนาจในการดักรับข้อมูลอื่นๆ (โปรดดูรายละเอียดในบทความตามอ้างอิง)[15] เห็นว่า ร่างกฎหมายใหม่ที่นำเสนอในการสัมมนานี้ โดยหลักแล้วไม่ซ้ำซ้อนกับกฎหมายเหล่านั้น เนื่องจากมีขอบเขตการใช้ที่แตกต่างกัน กล่าวคือ ร่างกฎหมายนี้ให้อำนาจการดักรับข้อมูลเกี่ยวกับฐานความผิดต่างๆตามประมวลกฎหมายอาญา ซึ่งยังไม่มีกฎหมายให้อำนาจในส่วนนี้มาก่อน สำหรับพระราชบัญญัติฉบับอื่นๆที่มีอยู่นั้น จะให้อำนาจเฉพาะในการบังคับใช้กฎหมายเฉพาะนั้นๆ เช่น ความผิดเกี่ยวกับยาเสพติด ความผิดเกี่ยวกับการฟอกเงิน เป็นต้น อย่างไรก็ตาม ผู้เขียนเห็นว่าอาจอาจเกิดปัญหาในบางกรณี เช่น – ข้อมูลการสนทนาหรือการสื่อสารอันหนึ่งเกี่ยวข้องกับทั้งความผิดตามประมวลกฎหมายอาญาและความผิดตามกฎหมายเฉพาะอื่นๆ เช่นนี้จะต้องมีการขออนุญาตในการดักรับข้อมูลโดยอาศัยกระบวนการที่แตกต่างกันเพื่อเข้าถึงข้อมูลการสนทนาอันเดียวกันหรือไม่ นอกจากนี้ ยังอาจเกิดปัญหากรณีข้อมูลที่ได้จากการดักรับอันเกี่ยวข้องกับคดีหนึ่งอาจถูกนำไปใช้กับคดีอื่นๆ ที่การสนทนานั้นเกี่ยวข้องด้วยหรือไม่

ประการที่ 9. ปัญหาการจัดการกับข้อมูลที่ได้รับมาจากการดักรับข้อมูล ทั้งนี้ผู้เขียนเห็นว่า ต้องมีมาตรการคุ้มครองความปลอดภัยของข้อมูล การกำหนดให้ข้อมูลนั้นจะถูกใช้ได้เฉพาะในการสืบสวนสอบสวนตามขอบเขตที่ขออนุญาตศาลในการดักรับข้อมูลเท่านั้น รวมทั้งมีมาตรการป้องกันการหลุดรั่วของข้อมูล (Data leakage) ด้วย ทั้งนี้จะเห็นว่า เมื่อพิจารณาในกรอบของการคุ้มครองข้อมูลส่วนบุคคลแล้ว ในปัจจุบันไทยยังไม่มีกฎหมายเฉพาะในการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป นอกจากนี้ ยังขาดกฎหมายที่วางหลักห้ามดักรับข้อมูลเป็นการทั่วไปด้วย หากมีการบัญญัติเฉพาะกฎหมายที่ให้อำนาจเจ้าพนักงานดักรับข้อมูล จะเกิดปัญหาช่องโหว่ของกฎหมายในการคุ้มครองสิทธิส่วนบุคคล ทั้งนี้เมื่อเปรียบเทียบกับกฎหมายต่างประเทศที่มีกฎหมายให้อำนาจดักรับข้อมูล จะเห็นได้ว่า มีการบัญญัติกฎหมายที่เกี่ยวข้องทั้งกระบวนการ กล่าวคือ ในเบื้องต้น มีกฎหมายคุ้มครองสิทธิส่วนบุคคลโดยบัญญัติห้ามการดักรับข้อมูลเป็นหลัก จากนั้นจึงมีกฎหมายให้อำนาจดักรับข้อมูลเป็นข้อยกเว้น นอกจากนี้ยังมีมาตรการกฎหมายคุ้มครองข้อมูล (data protection) สำหรับปรับใช้กรณีข้อมูลหลุดรั่วอีกด้วย ดังนั้น ผู้เขียนเห็นว่า ควรต้องมีการกำหนดมาตรการทางกฎหมายในการจัดการกับข้อมูลที่ได้รับมาจากการดักรับข้อมูล รวมทั้งกำหนดความผิดเป็นการเฉพาะสำหรับเจ้าพนักงานที่กระทำการเปิดเผยข้อมูลดังกล่าวโดยมิชอบหรือในการใช้ข้อมูลที่ดักรับมาดังกล่าวเกินหรือนอกขอบวัตถุประสงค์

---

15 คณาธิป ทองรวีวงศ์ , มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวของผู้ถูกดักฟังการสื่อสารข้อมูล, วารสารกระบวนการยุติธรรม,ปีที่ 6 เล่ม 1 มกราคม-เมษายน 2556.