บทที่ 4

วิเคราะห์ปัญหาและแนวทางแก้ไขการบัญญัติกฎหมายคุ้มครองสิทธิส่วนบุคคลจากการล่วงละเมิดโดยใช้แอปพลิเคชันโดยไม่ได้รับอนุญาตในประเทศไทย

การศึกษาในบทที่ 4 นี้ จะได้วิเคราะห์ที่เกี่ยวข้องกับการคุ้มครองสิทธิส่วนบุคคลจากการล่วงละเมิดโดยการใช้แอปพลิเคชัน โดยสารนิพนธ์เล่มนี้ ศึกษาหน่วยงานที่กำกับดูแล การละเมิดสิทธิส่วนบุคคล จากการล่วงละเมิดโดยแอปพลิเคชันเท่านั้น ซึ่งในประเด็นดังกล่าวนี้ จะทำการศึกษาหน่วยงานที่เกี่ยวข้อง ทั้งหน่วยงานของภาครัฐ หน่วยงานภาคเอกชน รวมถึงผู้มีหน้าที่ในการให้บริการเกี่ยวกับแอปพลิเคชัน จะเปรียบเทียบกฎหมายของต่างประเทศเพื่อศึกษาหาหลักเกณฑ์นำมาวิเคราะห์สภาพปัญหาและแนวทางแก้ไขในลำดับต่อไป

4.1ปัญหาของหน่วยงานภาครัฐที่รับผิดชอบในการคุ้มครองสิทธิส่วนบุคคลจากการล่วงละเมิดโดยแอปพลิเคชัน

ปัจจุบันเข้าถึงข้อมูลส่วนบุคคลและสร้างความเสียหายมีแนวโน้มเพิ่มมากขึ้น จากรายงานการประชุมของสำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติ ในการประชุมสมัยที่ 27 วาระที่ 2 และวาระที่ 3เมื่อ 30 มิถุนายน พ.ศ. 2557 ในเรื่องสิทธิความเป็นส่วนตัวในยุคดิจิทัล[1] พบว่ามีการส่งเสริมและคุ้มครองสิทธิในความเป็นส่วนตัว โดยที่เทคโนโลยีการสื่อสารแบบดิจิทัล อย่างเช่น การสื่อสารผ่านอินเทอร์เน็ต สมาร์ทโฟนและอุปกรณ์เชื่อมต่อไวไฟกลายเป็นส่วนหนึ่งของชีวิตประจำวัน โดยนวัตกรรมเทคโนโลยีการสื่อสารเช่นนี้นอกจากทำให้สามารถเข้าถึงข้อมูลและการสื่อสารแบบปัจจุบันได้อย่างรวดเร็วมากขึ้นแล้ว ยังมีส่วนสนับสนุนเสรีภาพในการแสดงออก การแลกเปลี่ยนความเห็นในระดับโลกอีกด้วย แต่ผลที่ตามมาความก้าวหน้าทางเทคโนโลยีส่งผลให้ มีบุคคลในการสอดแนมดักจับ และเก็บรวบรวมข้อมูลรุกล้ำความเป็นส่วนตัว มีเป้าหมายเฉพาะเจาะจงและเป็นไปอย่างกว้างขวางมากกว่าที่เคยเป็นกล่าวอีกอย่างหนึ่งพื้นฐานเทคโนโลยีที่เป็นปัจจัยหนุนเสริมสำคัญมากขึ้นต่อชีวิตทางการเมือง เศรษฐกิจและสังคมในระดับโลก ไม่เพียงจะตกเป็นเป้าหมายของการสอดแนมข้อมูลในวงกว้าง หากยังเป็นปัจจัยหนุนเสริมการสอดแนมอีกด้วย

---

[1]**รายงานการประชุมของข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติ.** (2557). สิทธิความเป็นส่วนตัวในยุคดิจิทัล. สมัยประชุมที่ 27 วาระที่ 2 และ 3.

จากกรณีปัญหาดังกล่าวการล่วงละเมิดข้อมูลส่วนบุคคลผ่านแอปพลิเคชัน ยกตัวอย่างแอปพลิเคชัน LINE จากสถิติของไทยเซิร์ต[2]รายงานการขโมยข้อมูลบัญชีใช้งาน LINE ไว้พอสังเขปดังนี้[3]

(1) เครื่องผู้ใช้งานติดมัลแวร์ (หรือที่คนทั่วไปรู้จักกันในนามของ ไวรัสคอมพิวเตอร์) จากสถิติที่ไทยเซิร์ตได้รับแจ้งเกี่ยวกับการตรวจพบเครื่องคอมพิวเตอร์ในประเทศไทยที่ติดมัลแวร์ประเภทที่มีความสามารถในการขโมยข้อมูลทางการเงิน (Banking Trojan) ระหว่างเดือนมกราคมถึงกันยายน 2557 นับตามจำนวนหมายเลขไอพีที่ไม่ซ้ำในแต่ละวัน มีประเด็นที่น่าสนใจว่าเครื่องคอมพิวเตอร์ไม่น้อยกว่า 10,000 เครื่องในประเทศไทย มีโอกาสเสี่ยงที่จะถูกขโมยข้อมูลบัญชีใช้งานระบบต่างๆ รวมถึงบัญชีใช้งาน LINE ด้วย

(2) ผู้ใช้งานส่งข้อมูลล็อกอินบัญชีใช้งาน LINE ให้กับผู้ไม่หวังดีเอง โดยข้อมูลดังกล่าวไทยเซิร์ตตรวจสอบพบบนเว็บไซต์พันทิปว่ามีผู้หลงเชื่อข้อมูลจากผู้ไม่หวังดี ว่าสามารถโกงไอเท็มของเกมใน LINE ได้ โดยมีการส่งข้อมูลการล็อกอินบัญชีใช้งาน LINE ให้กับผู้ไม่หวังดีเพื่อใช้ในกระบวนการหลอกลวงดังกล่าวและข้อมูลที่พบ ทำให้ทราบว่ายังมีผู้ที่หลงเชื่อกรอกข้อมูลส่งให้ผู้ไม่หวังดีอยู่จริง แสดงให้เห็นว่ากลุ่มผู้ใช้งานอีกส่วนหนึ่งที่ยังคงมีความเสี่ยงในเรื่องของการถูกขโมยข้อมูลจากช่องทางดังกล่าวได้เช่นกัน

(3) ผู้ใช้งานมีการใช้งานรหัสผ่านเดียวกันทุกระบบ หากรหัสผ่านใดรหัสผ่านหนึ่งรั่วไหลหรือถูกขโมยออกไป จะเกิดสถานการณ์ที่ทำให้ผู้ไม่หวังดีสามารถคาดเดารหัสผ่านของบัญชีใช้งาน LINE ได้ทันที ซึ่งกลุ่มเสี่ยงของผู้ใช้งานประเภทนี้ คาดว่าจะมีอยู่เป็นจำนวนหนึ่ง และอาจถูกขโมยด้วยวิธีการต่างๆ นอกเหนือจากข้อ 1 และ 2 เช่น การใช้งาน Wi-Fi สาธารณะและถูกดักข้อมูลการล็อกอิน หรือการตั้งรหัสผ่านที่ง่ายต่อการคาดเดา เป็นต้น โดยยกตัวอย่างกรณีที่เกิดขึ้นในอดีตเมื่อระบบของ Twitter ถูกแฮกทำให้ข้อมูลบัญชีใช้งานถูกขโมยออกไปจำนวนหนึ่ง ส่งผลให้มีผู้ใช้งานจำนวนหนึ่งที่ถูกแฮกอีเมลและบริการอื่นๆเพิ่มเติม

---

[2]ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) จัดตั้งขึ้นในปี พ.ศ. 2543 (ชื่อเดิม ศูนย์ประสานงานรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย)มีภาระหน้าที่หลักเพื่อตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน.

[3]**เตือนภัยแฮกไลน์ (LINE) หลอกให้ซื้อ iTunes Gift Card พร้อมวิธีป้องกันตนเอง.** (2557). (ออนไลน์). เข้าถึงได้จาก: https://www.thaicert.or.th/alerts/user/2014/al2014us018.html#1. [2559,29 กันยายน].

สำหรับประเทศไทยแม้ว่าขณะนี้ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่เสนอโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และยังอยู่ในระหว่างกระบวนการนิติบัญญัติและยังไม่ได้มีผลบังคับใช้ก็ตาม แต่หน่วยงานที่เกี่ยวข้อง เช่น หน่วยงานของรัฐ, ผู้ประกอบธุรกิจด้านเครือข่ายอินเตอร์เน็ตควรคำนึงถึงการให้ความคุ้มครองข้อมูลส่วนบุคคลไม่ให้มีการละเมิดสิทธิส่วนบุคคลเกิดขึ้น โดยอาจจะกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลของตนขึ้นให้มีความสอดคล้องกับกฎหมายระหว่างประเทศหรือกฎหมายของประเทศอื่นๆที่จัดได้ว่ามีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่สูงขึ้นเพื่อให้สอดคล้องกับกฎหมายดังกล่าวจะมีผลใช้บังคับในอนาคตอีกทั้งยังเป็นการสร้างความน่าเชื่อถือให้แก่เว็บไซต์ของผู้ประกอบการอีกทางหนึ่ง ด้วยเนื่องจากการกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการไม่ได้ถูกควบคุมโดยกฎหมายหรือองค์กรใดๆจึงอาจทำให้การกำหนดนโยบายของผู้ประกอบการต่างๆไม่ได้มาตรฐานและไม่อาจคุ้มครองข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการได้จริงดังนั้นจึงมีความจำเป็นที่รัฐจะต้องมีการกำหนดมาตรการบังคับ (Enforcing) โดยการออกกฎหมายภายในเพื่อควบคุมการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ผู้ประกอบการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลตามที่ตนได้ประกาศไว้ด้วยเพื่อให้นโยบายดังกล่าวสามารถบังคับใช้ได้จริงในทางปฏิบัติอย่างมีประสิทธิภาพ

เมื่อวิเคราะห์จากกรณีดังกล่าวจะเห็นว่าปัญหาดังกล่าวส่งผลกระทบต่อสังคมส่วนรวมทั้งทางด้านเศรษฐกิจและสังคมส่วนรวม จึงมีความจำเป็นอย่างยิ่งในการกำหนดหน่วยงานขึ้นมารับผิดชอบให้การคุ้มครองสิทธิส่วนบุคคลจากการล่วงละเมิดโดยการใช้แอปพลิเคชัน ทั้งภาครัฐ และภาคเอกชน รวมถึงผู้ประกอบธุรกิจให้บริการทางด้านเครือข่ายด้วย เพราะถ้าไม่มีหน่วยงานและมีกฎหมายให้อำนาจหน้าที่ในการควบคุมดูแลแล้ว มูลค่าความเสียหายจะมีเพิ่มมากขึ้นในอนาคต และสิทธิส่วนบุคคลย่อมถูกริดรอนไม่ได้รับความคุ้มครองตามหลักปฏิญญาสิทธิมนุษยชนและพลเมืองของสหประชาชาติ ซึ่งเป็นกติกาสากลที่ใช้กันทั่วโลก

จากที่ได้ศึกษามาในบทที่ผ่านมาจะเห็นว่ากฎหมายของประเทศไทยในเรื่องการคุ้มครองสิทธิส่วนบุคคลจากการล่วงละเมิดโดยแอปพลิเคชันนั้นแม้ว่าจะมีหน่วยงานของภาครัฐดูแลในเรื่องดังกล่าวอยู่แล้ว แต่หน่วยงานภาครัฐที่มีหน้าที่กำกับดูแลในเรื่องดังกล่าวยังขาดความชัดเจน ในส่วนของการกำหนดอำนาจหน้าที่ในแต่ละองค์กรกระจัดกระจายกันขอบเขตอำนาจ ทำได้แค่ไหนเพียงไรก็ยังไม่ครอบคลุม เช่น ในกรณีมีความจำเป็นเพื่อรักษาความมั่นคงของชาติ เป็นข้อมูลที่ขัดต่อกฎหมายหรือศีลธรรมอันดีของประชาชนอย่างร้ายแรง ต้องขอโดยหน่วยงานพิเศษตามกฎหมายกำหนด และจะต้องมีการขอคำสั่งจากศาลเท่านั้นอีกด้วย ซึ่งปฏิบัติตามพื้นฐานกฎหมายรัฐธรรมนูญที่กำหนดให้คุ้มครองสิทธิในการสื่อสารของประชาชน และเป็นการคุ้มครองสิทธิขั้นพื้นฐานส่วน

บุคคล ซึ่งรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้รับรองเสรีภาพในการสื่อสารถึงกันระหว่างบุคคลในมาตรา 36 ซึ่งวางหลักว่า "บุคคลย่อมมีเสรีภาพในการติดต่อสื่อสารถึงกันไม่ว่าในทางใดๆ" เพื่อคุ้มครองเสรีภาพดังกล่าว รัฐธรรมนูญกำหนดห้ามการกระทำที่มีลักษณะเป็นการขัดขวางต่อการสื่อสารดังจะเห็นได้จากมาตรา 36 วรรคท้ายที่วางหลักว่า "การตรวจการกักหรือการเปิดเผยข้อมูลที่บุคคลสื่อสารถึงกันรวมทั้งการกระทำด้วยประการใดๆเพื่อให้ล่วงรู้หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันจะกระทำมิได้เว้นแต่มีคำสั่งหรือหมายของศาลหรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ" นอกจากนี้ ยังระบุสิทธิในความเป็นส่วนตัวไว้หลายด้าน ซึ่งผู้วิจัยได้กล่าวไว้แล้วในบทที่ 3 แม้รัฐธรรมนูญมิได้ระบุเฉพาะเจาะจงถึง"การเข้าถึงข้อมูลโดยแอปพลิเคชัน" แต่จากมาตรา 36 จะเห็นได้ว่า การเข้าถึงข้อมูลโดยแอปพลิเคชัน ก็จัดเป็น "การกระทำประการอื่นเพื่อให้ล่วงรู้ถึงข้อความในสิ่งสื่อสาร" ซึ่งโดยหลักแล้วต้องห้ามตามรัฐธรรมนูญ นอกจากนี้ "สิทธิส่วนบุคคล" ยังถูกกำหนดไว้เป็นกติกาสากล ในจากปฏิญญาสิทธิมนุษยชนและพลเมืองของสหประชาชาติที่กำหนดไว้ว่า"บุคคลจะถูกสอดแทรกในชีวิตส่วนตัวครอบครัวเคหสถานการสื่อสารและจะถูกลบหลู่ในเกียรติยศชื่อเสียงโดยพลการมิได้คนทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายจากการสอดแทรกหรือลบหลู่นั้น"[4]ซึ่งอาจกล่าวโดยสรุปว่าสิทธิความเป็นส่วนตัว (Right to Privacy) หมายถึง สิทธิที่จะอยู่ตามลำพัง (Right to be let Alone) โดยปลอดจากการแทรกสอดในความเป็นส่วนตัว ที่ทำให้ได้รับความอับอาย เดือดร้อน รำคาญใจหรือนำภาพหรือชื่อไปใช้ประโยชน์ในทางแสดงหาประโยชน์โดยมิชอบ[5] ซึ่งมีขอบเขตกว้างขวางเป็นสิทธิในชีวิตส่วนตัวของบุคคลที่คาดหมายได้ว่าข้อมูลส่วนบุคคลจะไม่ถูกเปิดเผยต่อบุคคลที่สามหรือต่อสาธารณชนโดยปราศจากความยินยอมซึ่งการเปิดเผยนั้นอาจส่งผลให้บุคคลดังกล่าวได้รับความเดือดร้อนอับอายหรือได้รับความทุกข์ทรมานใจซึ่งข้อมูลข่าวสารส่วนบุคคลนี้หมายความรวมถึงข้อเท็จจริงรูปภาพไม่ว่าจะเป็นภาพถ่ายหรือในลักษณะของวิดีโอเทปหรือความคิดเห็นในลักษณะอื่นๆ เป็นต้น

เมื่อพิจารณาจากขอบเขตของสิทธิดังกล่าวจะพบว่ามีขอบเขตกว้างขวางมากดังนั้นการใช้สิทธิของเอกชน ในการละเมิดข้อมูลของผู้อื่นโดยผ่านทางแอปพลิเคชัน ในบางกรณีจึงอาจกระทบกับสิทธิส่วนบุคคลของผู้อื่นและก่อให้เกิดการละเมิดสิทธิได้ตัวอย่างเช่นการนำภาพหรือชีวิต

---

[4]Universal Declaration of Human Rights 1994, Article 12.อ้างถึงใน. สัมพันธ์ รัตนประดิษฐกุล. (2550). **มาตรการทางกฎหมายในการเยียวยาผู้เสียหายทางแพ่งจากการละเมิดสิทธิส่วนบุคคลโดยสื่อมวลชน.** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขานิติศาสตร์, คณะนิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์. หน้า 25.

[5]กุลพล พลวัน. (2557). **สิทธิในความเป็นอยู่ส่วนตัวกับการคุ้มครองตามกฎหมายไทย.** (ออนไลน์). เข้าถึงได้จาก: http://www.stat.ago.go.th/บทความลงเว็บ/บทที่%2016.html.[2559,14 ตุลาคม]

ส่วนตัวของบุคคลใดบุคคลหนึ่งไปเผยแพร่การเปิดเผยประวัติส่วนตัวของบุคคลการลักลอบฟังการสนทนาทางโทรศัพท์การลักลอบถ่ายภาพของบุคคลการเปิดเผยข้อความหรือจดหมายหรือเอกสารใดๆอันเป็นเรื่องส่วนตัวของบุคคลอื่นการนำภาพของบุคคลหรือชื่อของบุคคลไปใช้ในการโฆษณาสินค้าหรือแม้กระทั่งการสะกดรอยเพื่อเก็บข้อมูลหรือเป็นต้นในต่างประเทศได้ให้ความคุ้มครองกับสิทธิความเป็นอยู่ส่วนบุคคลเป็นอย่างยิ่งและปรากฏข้อเท็จจริงว่ามีการฟ้องร้องคดีเกี่ยวกับการละเมิดสิทธิส่วนบุคคลกันมากซึ่งแตกต่างจากประเทศไทยตรงที่คำว่า "สิทธิส่วนบุคคล" ยังไม่มีการกำหนดเป็นกฎหมายให้ความคุ้มครองที่ชัดเจน และพบว่าแทบจะไม่มีการฟ้องร้องคดีที่เกี่ยวกับการละเมิดสิทธิส่วนบุคคลต่อศาลหรือหากจะมีก็น้อยมากและมักจะมีการเจรจาประนีประนอมยอมความกันเพื่อให้คดียุติก่อนที่ศาลจะมีคำพิพากษาอยู่เสมอเมื่อพิเคราะห์แล้วจะเห็นว่า กฎหมายรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ได้กำหนดเรื่องสิทธิส่วนบุคคลไว้อย่างกว้างๆ แต่หน่วยงานที่กำกับดูแล ในเรื่องการคุ้มครองสิทธิส่วนบุคคลในการคุ้มครองข้อมูลส่วนบุคคลมิให้ถูกล่วงละเมิด ในประเทศไทยกลับไม่มีบัญญัติไว้ชัดเจน

เมื่อวิเคราะห์ต่อมากรณีหน่วยงานของรัฐที่มีหน้าที่เกี่ยวข้องกับการดูแลการล่วงละเมิดสิทธิส่วนบุคคลสรุปปัญหาได้พอสังเขป ได้แก่

1) คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (National Broadcasting and Telecommunication Commission) หรือ กสทช. (NBTC)

ถือเป็นหน่วยงานอิสระของรัฐ มีบทบาทหน้าที่ในการบริหารความถี่วิทยุเพื่อกิจการโทรคมนาคม และกำกับดูแลการประกอบกิจการโทรคมนาคมกสทช.จัดตั้งขึ้นตามพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่ และกำกับกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553 ในส่วนของการดูแลก็มีอำนาจหน้าที่ คุ้มครองสิทธิและเสรีภาพของประชาชนมิให้ถูกเอาเปรียบจากผู้ประกอบกิจการและคุ้มครองสิทธิในความเป็นส่วนตัวและเสรีภาพของบุคคลในการสื่อสารถึงกันโดยทางโทรคมนาคมและส่งเสริมสิทธิเสรีภาพและความเสมอภาคของประชาชนในการเข้าถึงและใช้ประโยชน์คลื่นความถี่ที่ใช้ในกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมเท่านั้น แต่ไม่ได้ครอบคลุมถึงการคุ้มครองสิทธิส่วนบุคคลจากการล่วงละเมิดโดยแอปพลิเคชันแต่อย่างใด

2) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ถือเป็นหน่วยงานที่บังคับใช้กฎหมายที่มุ่งเน้นการอำนวยความยุติธรรม ป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีและบริการประชาชน ให้มีมาตรฐานสากล สร้างความสงบเรียบร้อย มั่นคง แก่ประชาชน สังคมและประเทศชาติ มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวน

สอบสวน ปฏิบัติงานตามประมวลกฎหมาย วิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์ ซึ่งอำนาจหน้าที่หลักก็คือ การรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวน ปฏิบัติงานตามประมวลกฎหมาย วิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์ซึ่งหน่วยงานดังกล่าวก็มุ่งเน้นในการปรามปราม การบังคับใช้กฎหมายในกรณีที่มีการกระทำผิดกฎหมาย แต่ยังไม่มีความชัดจน ในการกำกับดูแลเมื่อมีการล่วงละเมิดสิทธิส่วนบุคคลจากการใช้แอปพลิเคชัน แต่อย่างใด

3) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (Ministry of Digital Economy and Society)

เป็นหน่วยงานที่นำเอาการสื่อสารทางด้านเทคโนโลยีดิจิทัล และการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมเพื่อรองรับการดำเนินกิจกรรมทางเศรษฐกิจ และสังคมเข้ามาช่วยพัฒนาประเทศ เพื่อรองรับการดำเนินกิจกรรมทางเศรษฐกิจ และสังคมในปัจจุบันที่มีการขับเคลื่อนโดยเทคโนโลยีดิจิทัลเป็นหลัก เป็นหน่วยงานภาครัฐทำหน้าที่บูรณาการกลไกต่าง ๆ ทั้งภาครัฐและภาคเอกชนให้มีการดำเนินการไปในทิศทางเดียวกันอันจะเป็นประโยชน์ต่อภาพรวมของการพัฒนาเศรษฐกิจและสังคมของประเทศโดยเน้นให้เทคโนโลยีดิจิทัลเข้าไปมีบทบาทในทุกภาคส่วน ดังนั้นเพื่อให้มีกระทรวงที่มีอำนาจหน้าที่ครอบคลุมถึงเรื่องดิจิทัลเพื่อเศรษฐกิจและสังคม แต่การกำกับดูแลเมื่อมีการล่วงละเมิดสิทธิส่วนบุคคลจากการใช้แอปพลิเคชันยังไม่ได้กำหนดหน้าที่กำกับดูแลอย่างชัดเจน เช่นเดียวกัน

4) หน่วยงานของรัฐที่มีอำนาจหน้าที่ ตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.2540

โดยพระราชบัญญัติฉบับนี้ ถือเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกของประเทศไทยมีลักษณะเป็นกฎหมายกลางแต่ให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลที่อยู่ในความครอบครอง ควบคุม และดูแลขององค์กรภาครัฐเท่านั้นและเป็นกฎหมายฉบับแรกที่ได้กำหนดนิยามของคำว่า ข้อมูลข่าวสารและ “ข้อมูลส่วนบุคคล” ไว้ โดยสรุปพระราชบัญญัตินี้ ให้การคุ้มครองข้อมูลส่วนบุคคลเฉพาะข้อมูลส่วนบุคคลที่จัดเก็บและอยู่ในความครอบครองของหน่วยงานภาครัฐ โดยไม่ครอบคลุมถึงข้อมูลส่วนบุคคลที่อยู่ในความครอบครองขององค์กรภาคเอกชน ในส่วนของข้อมูล จัดเก็บข้อมูลโดยหน่วยงานภาครัฐไม่ว่ากระทำโดยบุคคลหรือ โดยระบบคอมพิวเตอร์อัตโนมัติพระราชบัญญัติฉบับนี้ใช้บังคับกับหน่วยงานของรัฐและส่วนราชการ รวมทั้งส่วนราชการสังกัดรัฐสภาและศาล (เฉพาะที่ไม่เกี่ยวกับการพิจารณาพิพากษาคดี) องค์กรวิชาชีพและองค์กรหรือหน่วยงานอิสระของรัฐ เช่น คณะกรรมการป้องกันและปราบปรามการ

ทุจริตแห่งชาติผู้ตรวจการแผ่นดิน คณะกรรมการสิทธิมนุษย์ชนแห่งชาติ คณะกรรมการการเลือกตั้ง เป็นต้นเมื่อพิเคราะห์แล้วจะเห็นว่าหน่วยงานมีอำนาจบังคับใช้ตามพระราชบัญญัตินี้เท่านั้นจึงไม่ครอบคลุมข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของของเอกชน เช่น การจัดเก็บข้อมูลของ Facebook, LINE เป็นต้น

5) หน่วยงานของรัฐที่มีอำนาจหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

โดยการเข้าถึงข้อมูลมี 2 กรณี คือ กรณีแรกข้อมูลที่อยู่จัดเก็บไว้ในคอมพิวเตอร์ ตามมาตรา 7 [6]และในกรณีที่ 2 การเข้าถึงข้อมูลขณะที่ส่งในระบบคอมพิวเตอร์ตามมาตรา 8[7]ซึ่งในมาตรานี้ ยังได้กำหนดหลักเกณฑ์ขั้นพื้นฐานไม่ให้มีการล่วงละเมิดเข้าถึงข้อมูลการสื่อสารของประชาชนได้ นอกเหนือจากดำเนินการโดยหน่วยงานเฉพาะตามที่กฎหมายได้กำหนดและต้องเป็นเหตุเฉพาะกรณีที่กฎหมายกำหนดเท่านั้นนั่นคือ เฉพาะกรมสอบสวนคดีพิเศษหรือดีเอสไอ เท่านั้นที่มีอำนาจตามกฎหมายดังกล่าว ซึ่งตามพ.ร.บ. การสอบสวนคดีพิเศษ พ.ศ. 2547 (แก้ไขเพิ่มเติม พ.ศ. 2550) มาตรา 25 กำหนดโดยสรุปว่า โดยหลักการไม่มีสิทธิในการละเมิดการสื่อสารของประชาชน การกระทำการอย่างใดเพื่อให้ได้มาซึ่งข้อมูล จะทำได้ก็ต่อเมื่อคดีดังกล่าวอยู่ในความรับผิดชอบของกรมสอบสวนคดีพิเศษ (DSI) ซึ่งDSIจะกระทำได้โดยอาศัยคำสั่งศาล สำหรับคดีบางประเภทที่เป็นคดีพิเศษเท่านั้น[8] เมื่อพิจารณาแล้วพระราชบัญญัตินี้ครอบคลุมข้อมูลส่วนบุคคลที่อยู่ในคอมพิวเตอร์เท่านั้น ไม่ได้ครอบคลุมข้อมูลการสื่อสารที่อยู่ในสื่ออิเล็กทรอนิกส์อย่างอื่นๆ เช่น โทรศัพท์เคลื่อนที่ หรือ สมาร์ทโฟน,แทปเล็ต ฯลฯ แต่อย่างใดเมื่อมีการล่วงละเมิดสิทธิส่วนบุคคลจากการใช้แอปพลิเคชันหน่วยงานที่มีอำนาจหน้าที่โดยตรงในการกำกับดูแล จึงไม่มีความชัดเจน เหตุผลสำคัญประการหนึ่งคือ ปัญหาประเด็นดังกล่าว ต้องพิจารณาว่า ระบบโทรศัพท์เคลื่อนที่อยู่

---

[6]มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

[7]มาตรา 8 ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

[8]อรดา วงศ์อำไพวิทย์. (2557). **สิทธิส่วนบุคคลในการสื่อสารผ่านแอ็ปพลิเคชั่น และเครือข่ายสังคมออนไลน์.** (ออนไลน์). เข้าถึงได้จาก: http://www.thailaw4u.com/ Articles/tabid/83/articleType/ArticleView/articleId/47/-Cry ptography-Law-Steganography-Law-.aspx. [2559,2 ตุลาคม].

ในความหมายของ "ระบบคอมพิวเตอร์" ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือไม่ประเด็นดังกล่าวข้างต้นมีความเห็นทางกฎหมายออกเป็นสองฝ่าย[9]

นักกฎหมายฝ่ายแรก เห็นว่า ระบบโทรศัพท์เคลื่อนที่ ไม่อาจจัดอยู่ในความหมายของคำว่า "ระบบคอมพิวเตอร์" ที่บัญญัติไว้ใน มาตรา 3 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้เนื่องจากกฎหมายดังกล่าวเป็นกฎหมายอาญาและต้องตีความอย่างเคร่งครัด จะตีความขยายความรับผิดทางอาญาเกินกว่าที่กำหมายกำหนดไว้ไม่ได้

นักกฎหมายฝ่ายที่สอง เห็นว่าความหมายของ "ระบบคอมพิวเตอร์" ไม่ได้หมายถึงเฉพาะแต่คอมพิวเตอร์เท่านั้น แต่ยังรวมถึงอุปกรณ์อิเล็กทรอนิกส์ หรืออุปกรณ์สื่อสารทุกประเภทที่มีซอฟแวร์ (Software) เฉพาะที่ทำให้อุปกรณ์ดังกล่าวสามารถประมวลผลข้อมูลได้เหมือนคอมพิวเตอร์ตัวอย่าง เช่น โทรศัพท์เคลื่อนที่ เรื่องคอมพิวเตอร์แบบพกพา (PDA) ประกอบคำพิพากษาศาลอาญาที่ อ.4726/2554 ซึ่งจำเลยได้ใช้โทรศัพท์เคลื่อนที่ของตนเอง พิมพ์ข้อความอันเป็นการจาบจ้วงดูหมิ่นพระมหากษัตริย์และหมิ่นประมาทใส่ความให้ร้ายสมเด็จพระนางเจ้าฯ พระบรมราชินีนาถ ต่อมาจำเลยได้ส่งข้อความดังกล่าวไปยังโทรศัพท์เคลื่อนที่ของอดีตเลขานุการส่วนตัวของอดีตนายกรัฐมนตรี โดยศาลพิพากษาว่า จำเลยมีความผิดตามมาตรา 14 (2),(3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อันเป็นเท็จโดยน่าประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศและมีความผิดฐานนำเข้าระบบคอมพิวเตอร์ซึ่งระบบคอมพิวเตอร์ซึ่งข้อมูลอย่างใดๆอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร

จากกรณีดังกล่าวผู้วิจัยเห็นด้วยกับฝ่ายที่ 2ให้ถือว่าข้อมูลในโทรศัพท์มือถือ Smart Phone เป็นข้อมูลในระบบคอมพิวเตอร์ เช่นเดียวกันSmart Phone หมายถึง[10]โทรศัพท์มือถือที่มีความสามารถพิเศษเพิ่มเติมของ PDA เข้าไป ทำให้สามารถมีประสิทธิภาพมากขึ้น เช่น รับส่งอีเมล์ มีปฏิทิน จัดทำตารางนัดหมาย และ contact เป็นต้น เรียกได้ว่า Smart Phone เป็นคอมพิวเตอร์ขนาดย่อมเลยทีเดียว คุณสมบัติเด่นของ Smart Phoneระบบปฏิบัติการ หรือ OS (Operating System) เป็นระบบที่ช่วยให้การทำงานของโทรศัพท์มีประสิทธิภาพ และเป็นตัวกำหนดว่าโปรแกรมต่างๆ ที่จะสามารถติดตั้งเข้ากับ Smart Phone ได้หรือไม่ด้วย สำหรับระบบปฏิบัติการที่เป็นที่นิยมใช้งานบน Smart Phone ได้แก่ Symbian OS, Windows Mobile, Palm OS หรือแม้กระทั่ง Linux OS ดังนั้นการล่วงละเมิดสิทธิส่วนบุคคล โดยแอปพลิเคชัน ก็ควรอยู่ในระบบคอมพิวเตอร์เช่นเดียวกัน เพราะ

---

[9]ดวงดี วานิชกร. (2556). **ความรับผิดของผู้ให้บริการในการเผยแพร่สิ่งลามกผ่านโทรศัพท์เคลื่อนที่ : ศึกษากรณีเลขหมายพิเศษ.** วิทยานิพนธ์นิติศาสตร, คณะนิติศาสตร์ มหาวิทยาลัยอัสสัมชัญ. หน้า 27-28.

[10]**ประเภทของคอมพิวเตอร์.** (ออนไลน์). เข้าถึงได้จาก:https://sites.google.com/site/namchompoonuch/ team-schedules.[2559,3 ตุลาคม].

การเข้าถึงข้อมูลของ Facebook, LINE ก็สามารถเข้าได้ทั้งในคอมพิวเตอร์และ Smart Phone ได้เช่นเดียวกัน

6) หน่วยงานคณะกรรมการสิทธิมนุษยชนที่รับผิดชอบในการคุ้มครองสิทธิส่วนบุคคลจากการล่วงละเมิดโดยแอปพลิเคชัน

หน่วยงาน คณะกรรมการสิทธิมนุษยชนแห่งชาติ เป็นหน่วยกลางที่มีบทบาทอำนาจหน้าที่เกี่ยวข้องกับสิทธิมนุษยชนกว้างขวางมากตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560คณะกรรมการสิทธิมนุษยชนแห่งชาติมีสถานะเป็น "องค์กรอื่นตามรัฐธรรมนูญ" โดยมีหน้าที่หน้าที่หลักๆก็คือ ตรวจสอบและรายงานการกระทำหรือการละเลยการกระทำอันเป็นการละเมิดสิทธิมนุษยชน หรืออันไม่เป็นตามพันธกรณีระหว่างประเทศเกี่ยวกับสิทธิมนุษยชนที่ประเทศไทยเป็นภาคี และเสนอมาตรการการแก้ไขที่เหมาะสมต่อบุคคล หรือหน่วยงานที่กระทำหรือละเลยการกระทำดังกล่าว เพื่อดำเนินการในกรณีที่ปรากฏว่าไม่มีการดำเนินการตามที่เสนอให้รายงานต่อรัฐสภาและคณะรัฐมนตรีและเผยแพร่ต่อประชาชนเพื่อดำเนินการต่อไป แต่ยังไม่มีอำนาจ หน้าที่ ที่ชัดเจน ที่มาช่วยกำกับดูแลในส่วนของการล่วงละเมิดสิทธิส่วนบุคคลจากการใช้แอปพลิเคชันเลย

โดยสรุปการกำกับดูและของหน่วยงานภาครัฐ เมื่อศึกษา อำนาจหน้าที่ในกรณีที่มีการละเมิดสิทธิส่วนบุคคลจากการใช้แอปพลิเคชันแล้วเห็นว่า แม้จะมีหน่วยงานที่เกี่ยวข้องกับสิทธิส่วนบุคคลหลายหน่วยงาน แต่ยังไม่มีหน่วยงานใดมีอำนาจหน้าที่กำกับดูแลในเรื่องดังกล่าวเป็นการเฉพาะ การกำหนดหน้าที่ผู้รับผิดชอบจึงไม่ครอบคลุม มีความซับซ้อน ซึ่งทั้งที่ปัญหาการละเมิดสิทธิส่วนบุคคลในกรณีดังกล่าวในปัจจุบัน ส่งผลกระทบอย่างมากในสังคมยุคดิจิทัล ความก้าวหน้าทางด้านเทคโนโลยีส่งผลดีในหลายด้าน แต่ก็ส่งผลทางด้านลบด้วยเช่นกัน

เมื่อวิเคราะห์เปรียบเทียบกับต่างประเทศอังกฤษ ในประเด็นดังกล่าว จะเห็นว่า ประเทศอังกฤษ ได้มีการแต่งตั้งคณะกรรมการเรียกว่า "TheLindop Committee" เพื่อศึกษาหาแนวทางต่อการคุ้มครองข้อมูลส่วนบุคคลโดยมีหน้าที่ในคำปรึกษาเสนอแนะต่อรัฐบาลในเรื่องมาตรการใช้เครื่องคอมพิวเตอร์เพื่อเก็บรักษาและใช้ข้อมูลซึ่งเกี่ยวกับตัวบุคคล[11] และประเทศอังกฤษได้ตรากฎหมาย Data Protection Act 1984พระราชบัญญัติฉบับนี้กำหนดหลักการใหม่ซึ่งใช้สำหรับการเก็บรวบรวมข้อมูลและการประมวลผลข้อมูลโดยเครื่องมืออัตโนมัติ นอกจากนั้นยังได้กำหนดให้ผู้ใช้ข้อมูลมีหน้าที่ต้องจดทะเบียนต่อหน่วยงานของรัฐเรียกว่า "The office of The Data Protection Registrar" ผลของการประกาศใช้บังคับ Data Protection Act1984 ทำให้การจัดเก็บรวบรวมข้อมูล

---

[11]กิตติพันธุ์ เกียรติสุนทร. (2538). มาตรการทางอาญาในการคุ้มครองข้อมูลข่าวสาร. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขานิติศาสตร์, คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. หน้า 102.

ทุกประเภทที่เกี่ยวกับบุคคลโดยระบบคอมพิวเตอร์ต้องอยู่ภายใต้บทบัญญัติแห่งพระราชบัญญัตินี้ ไม่ว่าข้อมูลนั้นจะอยู่ภายใต้การควบคุมดูแลของหน่วยงานภาครัฐหรือภาคเอกชนก็ตาม และข้อมูลนั้นต้องสามารถบ่งชี้ตัวบุคคลได้ต่อมาในปี ค.ศ. 1995 The European Commission (EC) ได้ออกมาตรการทางกฎหมายเรียกว่า "The European Data Protection Directive (95/46/EC) on The Protection of Individuals with Regard to The Processing of Personal Data and on The Free Movement of Such Data" ขึ้นเพื่อกำหนดกฎเกณฑ์เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล (Data Processing) ของผู้ควบคุมดูแลข้อมูลให้มีความเหมาะสมและชัดเจนมากยิ่งขึ้น ประเทศอังกฤษเป็นหนึ่งในประเทศสมาชิก European Union จึงได้บัญญัติ Data Protection Act 1998 เพื่อนุวัติการให้เป็นไปตาม The European Data Protection Directive (95/46/EC) หรือ EU Directive การบัญญัติ Data Protection Act 1984 ได้ถูกยกเลิกไปพระราชบัญญัติฉบับนี้มีความละเอียดและสลับซับซ้อนกว่า Data Protection Act 1984 ดังเห็นได้จากการที่พระราชบัญญัติฉบับนี้ใช้บังคับกับข้อมูลที่ถูกประมวลผลด้วยมือซึ่งถูกจัดเก็บไว้ในแฟ้มข้อมูล รวมถึงพระราชบัญญัตินี้ได้กำหนดเงื่อนไขหรือบรรทัดฐานขั้นต่ำของการประมวลผลข้อมูลอันถือว่าเป็นการประมวลผลที่ชอบด้วยกฎหมาย นอกจากนี้มีการจัดประเภทของข้อมูลโดยกำหนดให้มีข้อมูลที่กระทบต่อความรู้สึก (Sensitive Data) ทำให้ผู้ควบคุมดูแลข้อมูลไม่สามารถประมวลผลข้อมูลประเภทนี้ได้ เว้นแต่ได้ปฏิบัติตามเงื่อนไข หรือข้อยกเว้นที่กำหนดไว้โดยเฉพาะและผู้ควบคุมดูแลข้อมูลไม่สามารถประมวลผลข้อมูลได้ เว้นแต่การประมวลผลนั้นได้ปฏิบัติตามเงื่อนไขของการรักษาความปลอดภัยแล้ว

ประเทศแคนาดา มีหน่วยงานภาครัฐจะควบคุมดูแลกฎหมายสิทธิส่วนบุคคล (Privacy Act) เป็นมาตรการทางกฎหมายที่ควบคุมการจัดเก็บ การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยให้สิทธิ์แก่ประชาชนในการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคลที่ตนเห็นว่าไม่ถูกต้อง

สาธารณรัฐฝรั่งเศส จะให้การรับรองและคุ้มครองสิทธิมนุษยชนดังที่ปรากฏในคำประกาศสิทธิมนุษยชนและพลเมืองค.ศ.1789 และรัฐธรรมนูญฉบับปีค.ศ. 1946 ซึ่งตามรัฐธรรมนูญแห่งสาธารณฝรั่งเศสฉบับปัจจุบันได้ให้การยอมรับประกอบกับการที่สาธารณรัฐฝรั่งเศสได้ให้สัตยาบันต่ออนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน สาธารณรัฐฝรั่งเศสจึงมีหน้าที่ต้องให้ความเคารพต่อสิทธิมนุษยชนของประชาชนและจะต้องจัดให้มีมาตรการภายในประเทศในการรับรองและคุ้มครองสิทธิมนุษยชนของประชาชนตามบทบัญญัติในรัฐธรรมนูญและอนุสัญญาดังกล่าวอย่างเคร่งครัด

สาธารณรัฐฝรั่งเศสมีหน่วยงานภาครัฐจะควบคุมดูแลกฎหมายสิทธิส่วนบุคคล โดยรัฐบัญญัติลงวันที่ 6 มกราคม ค.ศ.1978 ดังกล่าวมีวัตถุประสงค์เน้นไปยังเอกสารข้อมูลส่วนบุคคลและได้มีการก่อตั้ง คณะกรรมการข้อมูลข่าวสารและเสรีภาพแห่งชาติ La Cnil (Commission Nationale

de L'Informatique et des Libertés)ขึ้นเป็นคณะกรรมการอิสระไม่อยู่ใต้อำนาจขององค์กรใด ประกอบไปด้วยกรรมการ 17 คนมีวาระการดำรงตำแหน่ง 5 ปีโดยมีกรรมการ 2 คน มาจากสมาชิกสภาผู้แทนราษฎร กรรมการ 2 คน มาจากสมาชิกวุฒิสภา กรรมการ2 คนมาจากสภาเศรษฐกิจและสังคม กรรมการ 2 คนมาจากศาลปกครองสูงสุด กรรมการ 2 คน มาจากศาลฎีกา กรรมการ 2 คนมาจากศาลการคลังและภาษี กรรมการผู้ทรงคุณวุฒิ 2 คน มาจากการแต่งตั้งโดยกฤษฎีกาจากการเสนอของประธานวุฒิสภาและประธานสภาผู้แทนราษฎรและกรรมการอีก3คนมาจากการแต่งตั้งโดยกฤษฎีกาของที่ประชุมคณะรัฐมนตรี

คณะกรรมการ Cnil มีอำนาจหน้าที่หลักๆอยู่หลายประการด้วยกันดังนี้ ประการแรกรายงานการทำงานประจำปีต่อประธานาธิบดีสาธารณรัฐและต่อรัฐสภา ประการที่สอง ประการที่สองทำหน้าที่เป็นองค์กรที่ให้คำปรึกษาคำแนะนำและความเห็นแก่บุคคลที่จัดการเอกสารข้อมูลโดยการเสนอให้มีการปฏิรูปทางกฎหมายหรือกฎเกณฑ์ ประการที่สาม มีอำนาจในการตรากฎเกณฑ์ที่เป็นบรรทัดฐานที่ให้ความมั่นคงแก่ระบบในการจัดเก็บเอกสาร ประการที่สี่ มีอำนาจในการอนุญาตหรือปฏิเสธการจัดเก็บเอกสารที่เป็นอันตรายอย่างยิ่ง ประการที่ห้าอำนาจทั่วไปในการควบคุม เป็นต้น[12]

ระเบียบแห่งสหภาพยุโรปว่าด้วยประเด็นทางกฎหมายพาณิชย์อิเล็กทรอนิกส์ พ.ศ. 2543 (Directive 2003/31/EC of the European Parliament of the Council of 8 June 2000 on Certain Legal Aspect of Information Society Services, in Particular Electronic Commerce, in the Internal Market : Directive on Electronic (Commerce) ก็มีหน่วยงานหรือองค์กรที่มีอำนาจสำหรับการกระทำที่ผิดกฎหมายที่ถูกกล่าวหา หรือข้อมูลของผู้รับบริการ ซึ่งมีหน้าที่ที่จะต้องติดต่อกับหน่วยงานหรือองค์กรที่มีอำนาจ ตามคำร้องขอของผู้ใช้บริการ ในข้อมูลที่สามารถระบุถึงผู้รับบริการกับบุคคลที่มีข้อตกลงในการจัดเก็บข้อมูล ซึ่งถ้าเทียบเคียงกับสำหรับประเทศไทย เห็นว่า หน่วยงานหรือองค์กรที่มีอำนาจดังกล่าว คือคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) นั่นเอง

---

[12]เกรียงไกร เจริญธนาวัฒน์. (2548). เสรีภาพทางกายภาพตามแนวคิดทางกฎหมายของฝรั่งเศส. (ออนไลน์). เข้าถึงได้จาก: http://public-law.net/publaw/view.aspx?id=670&Page=2.[2560,3มิถุนายน].

4.2 ปัญหาของผู้ให้บริการแอปพลิเคชันในการป้องกันการละเมิดสิทธิโดยแอปพลิเคชัน

ปัจจุบันการติดต่อสื่อสารด้วยการรับ – ส่งข้อมูลผ่านโทรศัพท์มือถือ แท็ปเล็ต หรือเครื่องคอมพิวเตอร์โดยใช้ระบบเครือข่ายอินเตอร์เน็ตได้รับความนิยมสูงมาก จึงมีการออกแบบแอปพลิเคชั่น และเครือข่ายสังคมออนไลน์หลายประเภทเพื่อรองรับการใช้งานดังกล่าว เช่น เฟซบุ๊ก (Facebook), ยูทูบ (YouTube), วอทซ์แอพ (WhatsApp), ไลน์ (LINE) เป็นต้นโดยวัตถุประสงค์หลักของการติดต่อสื่อสารในสังคมออนไลน์ ก็เพื่อให้มีการติดต่อสื่อสารอย่างเสรี รวมทั้งผู้ให้บริการในสังคมออนไลน์ยังมีการกำหนดแนวนโยบายที่เป็นหลักสากลในการปกป้องสิทธิเสรีภาพของผู้ใช้บริการ โดยเฉพาะข้อมูลส่วนบุคคลที่มีการติดต่อสื่อสารระหว่างกันด้วย นอกจากเป็นการขอข้อมูลจากภาครัฐอันเนื่องมาจากเหตุผลด้านความมั่นคงของชาติเท่านั้น ซึ่งผู้ให้บริการจะพิจารณาเป็นกรณี เช่น บริษัท Naver ซึ่งเป็นผู้ให้บริการแอปพลิเคชั่น LINE ที่ได้ตั้งบริษัท และ Server อยู่ที่ประเทศญี่ปุ่น ก็มีข้อกำหนดในการรักษาข้อมูลส่วนบุคคลไว้ (LINE Privacy Policy) และได้ระบุข้อยกเว้นของการให้ข้อมูลแก่บุคคลที่สามไว้โดยสรุปคือ เมื่อบริษัทถูกร้องขอให้ความร่วมมือจากสถาบันของรัฐ รัฐบาลท้องถิ่น หรือบุคคล หรือผู้ประกอบการธุรกิจ เพื่อดำเนินการตามกฎหมายหรือกฎเกณฑ์ และเมื่อการให้ผู้ใช้ยินยอมก่อนจะเป็นการกีดขวางการทำงานของเจ้าหน้าที่รัฐเท่านั้น หรือในกรณีของ Facebook ซึ่งเป็นผู้ให้บริการที่ตั้งบริษัท และ Server ที่ประเทศสหรัฐอเมริกา มีกฎเกณฑ์ในการรักษาข้อมูลส่วนบุคคลเช่นเดียวกันกำหนดใน Facebook's Privacy Policy โดยหลักผู้ใช้บริการสามารถเลือกเปิดเผยข้อมูลในกรณีใด หรือกับบุคคลใดได้ หรือให้ข้อมูลเปิดเผยเฉพาะกลุ่มไม่เปิดเผยเป็นการทั่วไป อีกทั้ง Facebook มีข้อกำหนดในการเปิดเผยข้อมูลของระบบกำหนดอยู่ในข้อ 5 ของข้อกำหนดในหัวข้อ How we Share Information ซึ่งนอกเหนือจากกรณีที่ผู้ใช้บริการเลือก หรือเพื่อการปรับปรุงบริการต่างๆ แล้ว จะไม่เปิดเผย โดยมีข้อยกเว้นระบุไว้เฉพาะกรณีโดยสรุป คือ จะเปิดเผยข้อมูลต่อบุคคลที่สามต่อเมื่อ Facebook ได้รับการร้องขอจากองค์กรตามกฎหมาย หรือในกรณีที่มีความจำเป็นเพื่อป้องกันเหตุการณ์ร้ายแรงเท่านั้น[13]

โดยทั่วไปแล้วเอกชนที่เป็นผู้ให้บริการพื้นที่เก็บข้อมูลสำหรับแอปพลิเคชัน (Application Hosting) คือ ผู้ให้บริการพื้นที่ข้อมูลสำหรับโปรแกรมประยุกต์ (Software) และแอปพลิเคชัน (Application) ต่างๆที่ให้บริการพื้นที่แก่นักพัฒนาแอปพลิเคชัน (Application Developer) เพื่อการอัปโหลด (Upload) แอปพลิเคชัน (Application) ของตนเองเข้าสู่พื้นที่บริการดังกล่าวเพื่อให้บุคคลภายนอกสามารถดาวน์โหลด (Download) ไว้เพื่อการใช้งานอย่างใดๆ ซึ่งอาจมีค่าใช้จ่ายหรือไม่ก็ได้ ขึ้นอยู่กับประเภทของแอปพลิเคชันบนโทรศัพท์เคลื่อนที่ (Mobile Application) โดย

---

[13]อรดา วงศ์อำไพวิทย์. อ้างแล้ว เชิงอรรถที่ 8.

หลักการแล้วองค์กรหรือหน่วยงานที่มีอำนาจในการจัดระบบเครือข่าย คือ องค์กรหรือหน่วยงานซึ่งอยู่ต้นสายหรือต้นทางของการให้บริการพื้นที่เชื่อมต่อเข้าสู่ระบบเครือข่ายอินเทอร์เน็ต (Internet) ผูกขาดบริการการติดต่อสื่อสารระหว่างประเทศ และมีอำนาจในการให้ใบอนุญาตตลอดทั้ง ถอดถอนสิทธิในการให้บริการของผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ของประเทศไทย ได้แก่ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ส่วนผู้ให้บริการเข้าใช้เครือข่ายอินเทอร์เน็ต (Internet Access Provider) คือ บุคคลที่ทำหน้าที่ให้บริการเชื่อมต่ออินเทอร์เน็ต (Internet Access Provider) แก่ผู้ใช้บริการ อินเทอร์เน็ต (Internet) โดยตรงโดยที่ผู้ใช้บริการจะต้องเป็นสมาชิกของผู้ให้บริการรายนั้นๆ เสียก่อน เพื่อให้ได้มาซึ่งชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ไว้ใช้ในการเชื่อมต่อเข้าสู่ระบบเครือข่ายอินเทอร์เน็ต (Internet) โดยที่ผู้ใช้บริการดังกล่าวจะต้องได้รับสิทธิตามสัญญาจากองค์กรหรือหน่วยงานที่มีอำนาจในการจัดระบบเครือข่าย จึงจะสามารถดำเนินการให้บริการการเชื่อมต่อของตนเองแก่ผู้ใช้บริการอินเทอร์เน็ต (Internet) ได้

ปัจจุบันการติดต่อสื่อสารผ่านระบบผู้ให้บริการที่มิได้มี Server และไม่มีบริษัทดำเนินการอยู่ในประเทศไทย ก็ยังไม่มีหน่วยงานภาครัฐเข้ามากำกับดูแลได้ ทำให้การกำกับดูแลยังไม่สามารถดำเนินการได้หากไม่ได้รับความร่วมมือ และการอนุญาตจากผู้ให้บริการเท่านั้น โดยในทางสากลนั้นเหตุผลที่แต่ละประเทศจะขอความร่วมมือในการขอข้อมูลจากผู้ให้บริการซึ่งมี Server อยู่ต่างประเทศได้ จะมีเพียงเหตุผลเพราะข้อมูลดังกล่าวมีผลกระทบต่อความมั่นคงปลอดภัยของประเทศนั้นๆ เท่านั้น และเป็นสิทธิเด็ดขาดของผู้ให้บริการที่จะพิจารณาว่าจะอนุญาตให้ข้อมูลหรือไม่ ยกตัวอย่างเช่น ความพยายามในการเข้ามากำกับดูแลควบคุมการติดต่อสื่อสารด้วยแอปพลิเคชั่น LINE ซึ่งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) ได้ออกมาเปิดเผยว่ากองบังคับการได้ส่งทีมงานไปประเทศญี่ปุ่นและเข้าพบผู้บริหารของ Naver ซึ่งเป็นผู้ให้บริการแอปพลิเคชั่น LINE ที่ได้ตั้งบริษัท และ Server อยู่ที่ประเทศญี่ปุ่นเพื่อขอความร่วมมือในการเข้าไปตรวจสอบข้อมูลการสนทนาของผู้ใช้ผ่านแอปพลิเคชั่นดังกล่าวรวมถึงการขอข้อมูลรายชื่อของผู้ใช้บริการรายนั้นๆ ที่อาจส่งผลกระทบต่อความมั่นคงของไทย แต่อย่างไรก็ตามท้ายที่สุดแล้ว Naver ได้แจ้งยืนยันกลับทางหน่วยงานราชการของไทยดังกล่าวแล้วว่าไม่สามารถดำเนินการตามที่ ปอท. ร้องขอได้ ซึ่งเมื่อเราพิจารณาในกรณีของ LINE แล้ว ข้อมูลการติดต่อสื่อสารนอกจากอยู่ที่ผู้ใช้บริการแล้ว ข้อมูลทั้งหมดจะถูกเก็บอยู่ที่ผู้ให้บริการ ซึ่งมีการตั้ง Server อยู่ที่ต่างประเทศ โดยผู้ให้บริการจะสามารถเห็นข้อมูลการสื่อสารทั้งหมด เพราะแม้เป็นข้อมูลสื่อสารส่วนบุคคลแต่ไม่มีการเข้ารหัสลับ หรืออำพรางข้อมูลแต่อย่างใด ข้อมูลดั้งเดิมทั้งหมดจึงถูกเก็บอยู่ที่ผู้ให้บริการ

สำหรับปัญหาของผู้ให้บริการด้านการสื่อสารผ่านแอปพลิเคชันนั้น ปัจจุบันมีปัญหาอย่างมาก เพราะมีการเจาะระบบ (Hacking) หมายถึง การเข้าไปในเครือข่ายคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Unauthorized Access) และเมื่อเข้าไปแล้วก็ทำการสำรวจ ทิ้งข้อความ เปิดโปรแกรม ลบ แก้ไขเปลี่ยนแปลงหรือขโมยข้อมูลการถูกลักลอบเจาะระบบอาจส่งผลให้ความลับทางการค้า ข้อมูลที่สำคัญหรือแม้แต่เงินของหน่วยงานต้องถูกขโมยไป เป็นต้น การกระทำดังกล่าวอาจทำจากคู่แข่งทางการค้า อาชญากรหรือผู้ที่ไม่หวังดี และอาจจะทำจากในหน่วยงานเองหรือจากส่วนอื่นๆ ที่อยู่ห่างไกลออกไป หรือจากนอกประเทศโดยใช้เครือข่ายการสื่อสารสาธารณะหรือโทรศัพท์ นักเจาะระบบอาจได้รหัสการเข้าสู่เครือข่ายโดยการดักข้อมูลทางสายโทรศัพท์ หรือใช้เครื่องมือสื่อสารนำไปติดกับเครื่องคอมพิวเตอร์หรือใช้เครื่องจับการแผ่รังสีจากการส่งผ่านข้อมูลที่ไม่มีการป้องกันการส่งข้อมูล (Unshielded Data Transmission) เพื่อจะได้มาซึ่งรหัสผ่าน (Password)[14] ทำให้เกิดปัญหาทางสังคมมากมาย

กฎหมายของต่างประเทศสำหรับความรับผิดชอบของผู้ให้บริการ มีระเบียบแห่งสหภาพยุโรปว่าด้วยประเด็นทางกฎหมายพาณิชย์อิเล็กทรอนิกส์ (EU Directive 2003/31/EC)ที่ใช้กับภาคีเครือข่ายประเทศสมาชิก ซึ่งมีหลักความรับผิดของผู้ให้บริการที่เป็นสาระสำคัญกล่าวคือถ้าผู้ให้บริการได้ปฏิบัติตามหลักเกณฑ์หรือเงื่อนไขที่กำหนดในระเบียบดังกล่าว ผู้ให้บริการย่อมไม่ต้องรับผิดในเนื้อหาอันมิชอบด้วยกฎหมายที่ผู้ใช้บริการได้กระทำโดยอาศัยระบบเครือข่ายของผู้ให้บริการ แต่ต้องประกอบด้วยไขที่ชัดแจ้งและรัดกุม อาทิเช่น ตามกฎหมายดังกล่าว ได้วางหลักเกณฑ์ ผู้ให้บริการส่งต่อข้อมูลเท่านั้น (Mere Conduit) ตามมาตรา 12 วรรค 1 กรณีของการให้บริการที่ประกอบไปด้วยการส่งข้อมูลของผู้รับบริการผ่านทางระบบเครือข่ายการสื่อสารหรือการให้บริการทางการเข้าถึงระบบเครือข่ายการสื่อสาร รัฐภาคีสมาชิกรับประกันว่าผู้ให้บริการจะไม่มีความรับผิดสำหรับข้อมูลที่ส่งผ่านไประบบเครือข่ายการสื่อสารของตนเองภายใต้เงื่อนไข 3 ประการ คือหนึ่ง ผู้ให้บริการไม่ได้เป็นผู้ซึ่งริเริ่มในการส่งข้อมูลสอง ผู้ให้บริการไม่ได้เลือกผู้รับการส่งข้อมูลและสาม ผู้ให้บริการไม่ได้เลือกหรือแก้ไขดัดแปลงข้อมูลที่ใช้ในการส่งเป็นต้น นอกจากนี้ยังมีข้อพิจารณาตามตามมาตรา 12 วรรค 2 แห่งระเบียบแห่งสหภาพยุโรปว่าด้วยประเด็นทางกฎหมายพาณิชย์อิเล็กทรอนิกส์ หรือ EU Directive 2003/31/EC ได้กำหนดให้การกระทำซึ่งเป็นการส่งข้อมูลทางระบบเครือข่ายการสื่อสาร หรือการให้บริการการเข้าถึงระบบเครือข่ายการสื่อสารตามวรรค 1 ที่มุ่งดูแลเรื่องการจัดเก็บข้อมูลเป็นการชั่วคราวที่อยู่ในระหว่างการส่งผ่านโดย

---

[14]กฎหมายเกี่ยวกับเทคโนโลยีสารสนเทศ. (2554). (ออนไลน์). เข้าถึงได้จาก: http:// kruoong.blogspot.com/2011/06/ blog-post_08.08.html. [2559,28 กันยายน].

อัตโนมัติด้วย เนื่องจาก ในการรับส่งข้อมูลบนระบบเครือข่ายแต่ละครั้ง จะต้องทำงานโดยมีการสำเนาเอกสารและจัดเก็บข้อมูลเอาไว้เป็นการชั่วคราวในคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ทุกเครื่องที่มีการส่งและรับข้อมูล ตลอดจนต้องเปิดดูไฟล์ข้อมูลหรือเอกสารดังกล่าว ซึ่งเป็นการกระทำสำเนาทางเทคนิค เพื่อประโยชน์สำหรับการรับส่งข้อมูลต่อไป อย่างไรก็ตามกระบวนการดังกล่าวจะต้องไม่ใช้ระยะยาวในการจัดเก็บที่นานเกิดสมควร และจะต้องกระทำเพื่อวัตถุประสงค์สำหรับการรับส่งข้อมูลต่อไปเท่านั้น จะกระทำเพื่อวัตถุประสงค์ประการอื่นไม่ได้ จะเห็นว่ากฎหมายในต่างประเทศมีการดูแลรัดกุม เป็นระบบ และมีข้อบังคับที่ชัดเจนในการควบคุมดูแลการสื่อสารผ่านระบบเครือข่าย ซึ่งแตกต่างกับประเทศไทยที่มีกฎหมายแต่มาตรการควบคุมยังขาดความชัดเจนและยังไม่เกิดประสิทธิภาพเท่าที่ควร

กล่าวโดยสรุปจะเห็นว่าการใช้ Social Network สื่อสารกัน ผ่านแอปพลิเคชัน เช่น LINE Facebook ฯลฯ แม้ผู้ประกอบธุรกิจจะการบริหารจัดการ และมีมาตรการควบคุมที่เข้มงวดเพียงใด แต่ก็ปฏิเสธไม่ได้ว่าจะปลอดภัย ร้อยเปอร์เซ็นต์ เนื่องจากข้อมูลการถูกละเมิดสิทธิส่วนบุคคลมีออกมาให้เห็นทางสังคมกันอยู่เป็นประจำจากกระแสข่าวที่มีออกมาอยู่อย่างต่อเนื่อง ไม่ว่าจะเป็นขโมยข้อมูลไปใช้ แอปพลิเคชันปลอมตัวเพื่อไปก่ออาชญากรรม หรือแม้แต่แอบขโมยรูปหรือเบอร์โทรศัพท์เพื่อหวังผลทางธุรกิจ เป็นต้น

4.3 แนวทางแก้ไขปัญหาการป้องกันการละเมิดสิทธิส่วนบุคคลจากการถูกล่วงละเมิดโดยแอปพลิเคชัน

1) แนวทางแก้ไขปัญหาอำนาจหน้าที่ของหน่วยงานภาครัฐขาดความชัดเจน

แนวทางการแก้ไข รัฐบาลควรจะกำหนดองค์กรหรือหน่วยงานขึ้นมามีอำนาจหน้าที่ไว้โดยเฉพาะให้สอดคล้อง ครอบคลุมกับปัญหาที่เกิดขึ้นในปัจจุบัน รวมไปถึงบัญญัติกฎหมายกลางควบคุมดูแลกฎหมายสิทธิส่วนบุคคล (Privacy Act) เป็นมาตรการทางกฎหมายที่ควบคุมการจัดเก็บ การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยให้สิทธิ์แก่ประชาชน เหมือนกับประเทศแคนาดา โดยให้มีความชัดเจนโดยอาจก่อตั้งคณะกรรมการเข้ามาควบคุมดูแลเหมือนกับประเทศอังกฤษ โดยต้องคำนึงถึงการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานหากภาครัฐยึดถือผลประโยชน์ของชาติ (National Interest) เป็นที่ตั้งในการทำงาน และดำรงไว้ซึ่งหลักการของความมั่นคงภายในรัฐ (National Security) เป็นกรอบปฏิบัติ โดยภาครัฐจะต้องมีความสามารถในการสื่อสารถึงเหตุผลและความจำเป็นของการกระทำดังกล่าวให้แก่ภาคประชาชนได้อย่างมีประสิทธิภาพ โดยเหตุผลที่ได้รับการยอมรับในทางสากลและชัดเจน เช่น ภาครัฐมีความจำเป็นที่จะต้องดำเนินการดังกล่าวเพื่อรักษาความมั่นคงภายในรัฐและเพื่อเป็นการป้องปรามภัยคุมคามที่

อาจจะเกิดขึ้นในอนาคต หรือการประนีประนอมขอให้ประชาชนยอมสละสิทธิส่วนบุคคลบางส่วนในเรื่องของการสื่อสาร เพื่อธำรงไว้ซึ่งความมั่นคงแห่งชาติในภาพรวมแต่ถ้าการละเมิดสิทธิส่วนบุคคลเกิดจากเอกชน ต้องมีบทบัญญัติควบคุมอย่างเคร่งครัดและมีหน่วยงานที่ดูแลเรื่องดังกล่าวอย่างชัดเจน นอกจากนี้ควรแต่งตั้งและกำหนดอำนาจหน้าที่ของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ในการประสานงานกับส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานรัฐอื่นๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล จัดทำบัญชีรายชื่อ "ผู้ควบคุมข้อมูล" และติดตามการประเมินผลการทำงานให้ครอบคลุมทุกหน่วยงานที่เกี่ยวข้อง

2) แนวทางแก้ไขปัญหาอำนาจหน้าที่ของหน่วยงานตามรัฐธรรมนูญกับการล่วงละเมิดสิทธิส่วนบุคคลจากแอปพลิเคชัน

กรณีดังกล่าวรัฐบาลควรออกกฎหมายให้อำนาจหน้าที่หน่วยงานตามรัฐธรรมนูญ เช่น คณะกรรมการสิทธิมนุษยชนแห่งชาติ เพราะเป็นองค์กรอื่นตามรัฐธรรมนูญอยู่แล้ว โดยให้กำหนดบทบาทหน้าที่ให้ชัดเจน สอดคล้องกับกฎหมายรัฐธรรมนูญ เช่น ประเทศแคนาดาที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารเล็กทรอนิกส์ (Personal Information Protection and Electronic Documents Act) หรือ PIPEDA เป็นมาตรการทางกฎหมายที่ใช้ควบคุมบริษัทและองค์กรภาคเอกชนซึ่งดำเนินการจัดเก็บภาษี ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับกิจกรรมเชิงพาณิชย์ เป็นต้น

3) แนวทางการแก้ไขปัญหาของผู้ให้บริการด้านการสื่อสารผ่านแอปพลิเคชัน

จากกรณีดังกล่าวผู้ประกอบธุรกิจด้านการให้บริการด้านการสื่อสารผ่านแอปพลิเคชันควรให้ความสำคัญในเรื่องความปลอดภัยของข้อมูลส่วนตัวหรือการคุ้มครองผู้ใช้งานแอปพลิเคชันใน 2 ประเด็นหลัก คือ มาตรการคุ้มครองทางเทคนิคและทางกฎหมาย ดังนี้

(1) มาตรการคุ้มครองทางเทคนิค ที่ต้องมีตลอดการเดินทางของข้อมูล ตลอดวงจรชีวิต (Life Cycle) ของข้อมูล ไม่ว่าจะเป็นในส่วนการรับส่งข้อมูลบนเครือข่าย ความมั่นคงของตัวเครือข่ายเอง การออกแบบแอปพลิเคชัน การจัดเก็บข้อมูล การจัดลำดับชั้นของสิทธิ์ในการเข้าถึงข้อมูล ความเข้มงวดของการยืนยันตัวตน เป็นต้น เพื่อลดโอกาสที่ข้อมูลจะรั่วไหลไปโดยไม่เจตนาหรือถูกเข้าถึงโดยที่เจ้าของไม่ได้อนุญาต รวมทั้งลดความเสียหายในน้อยที่สุดในกรณีที่เกิดการรั่วไหลแล้ว

(2) มาตรการคุ้มครองทางกฎหมาย ไม่ว่าจะเป็นในรูปแบบสัญญาสองฝ่ายระหว่างผู้ให้บริการและผู้ใช้บริการ กฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายเกี่ยวกับการพิจารณาความอาญาและอำนาจในการดักฟัง การกำกับดูแลโดยองค์กรกำกับ เช่น องค์กรสิทธิผู้บริโภค องค์กรกำกับดูแลการสื่อสาร ความเข้มแข็งและความกระตือรือร้นของผู้ประกอบการในการปกป้องสิทธิ

ของลูกค้า เช่น การมีทีมกฎหมายที่พร้อมจะถามถึงความชอบธรรมเหมาะสมในการที่รัฐจะขอข้อมูลผู้ใช้ ทั้งหมดนี้เพื่อลงโทษผู้เปิดเผยข้อมูลหรือละเมิดสิทธิผู้ใช้ ยับยั้งความเสียหายและเยียวยาผู้ถูกละเมิด และเพื่อจูงใจให้ผู้ให้บริการมีวิธีปฏิบัติในการประกอบกิจการที่คุ้มครองข้อมูลของผู้ใช้และจัดให้มีมาตรการทางเทคนิคที่ได้มาตรฐาน[15]

แม้ผู้ให้บริการจะมีระบบรักษาความปลอดภัยเบื้องต้นอยู่แล้วแต่บางครั้งจะเห็นได้จากกรณีที่เกิดขึ้นว่าความผิดพลาดส่วนหนึ่งมาจากเจ้าหน้าที่ของผู้ให้บริการที่สามารถเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้ได้ดังนั้นผู้ให้บริการจำเป็นต้องมีมาตรการควบคุมการเผยแพร่ข้อมูลส่วนบุคคลของผู้ใช้ควรมีการกำหนดระเบียบข้อปฏิบัติและบทลงโทษสำหรับเจ้าหน้าที่ที่ฝ่าฝืนนโยบายความเป็นส่วนตัวจำเป็นต้องมีการแจ้งเตือนผู้ใช้บริการกรณีข้อมูลรั่วไหลและควรแสดงความรับผิดชอบหากเกิดความเสียหายอื่นตามมาจากการรั่วไหลของข้อมูลดังกล่าวนอกจากนี้ผู้ให้บริการควรแจ้งให้ผู้ใช้บริการทราบอย่างชัดเจนว่ามีกระบวนการจัดเก็บและจัดการกับข้อมูลส่วนบุคคลอย่างไรและร่วมกันภายในภาคอุตสาหกรรมเพื่อพัฒนามาตรฐานการคุ้มครองข้อมูลในภาคอุตสาหกรรมนั้นๆ

กล่าวโดยสรุป ปัญหาการละเมิดสิทธิส่วนบุคคลจากการนำแอปพลิเคชันของบุคคลอื่นไปใช้ที่กล่าวมาในข้างต้นอาจจะแบ่งได้เป็น 2 ประเด็นใหญ่ คือ ประการแรก เป็นปัญหาขององค์กรที่มีหน้าที่ควบคุมดูแลในส่วนของภาครัฐเป็นหลัก ประการที่สองเป็นปัญหาของระบบการให้บริการแอปพลิเคชันซึ่งในส่วนนี้ผู้ให้บริการต้องเป็นผู้ดูแล ดังนั้นการแก้ไขปัญหาให้เกิดประสิทธิผลนั้นต้องแก้ไขทั้งองค์กรและระบบให้สอดคล้องกัน จะนำมาซึ่งการแก้ไขปัญหาอย่างได้ผลในทุกมิติ

---

[15]ย้อนไทม์LINE ความพยายามสอดแนมการสื่อสารของรัฐไทย. (2558).(ออนไลน์). เข้าถึงได้จาก:https://thainetizen.org/2015/01/thailand-chat-app-surveillance-timeline/.[2559,28ธันวาคม].