บทที่ 2

ประวัติความเป็นมา ความหมาย และแนวคิดเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

กฎหมายคุ้มครองข้อมูลส่วนบุคคล ถือเป็นกฎหมายใหม่ที่สำคัญสำหรับประเทศไทยเป็นอย่างมาก แต่เนื่องด้วยปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก จนสร้างความเดือดร้อน หรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม จึงกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้นมา โดยมีประวัติความเป็นมา ความหมาย และแนวคิด ที่เกี่ยวข้อง ดังต่อไปนี้

2.1 ประวัติความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ประวัติความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่มีฐานะเป็นกฎหมายกลางกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลในลักษณะทั่วไปครอบคลุมทุกมิติ ซึ่งได้รับอิทธิพลจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ทำให้มีมาตรฐานในการคุ้มครองสิทธิทัดเทียมกับนานาอารยะประเทศ[1]

2.1.1 ประวัติความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในอดีต

การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) ถือเป็นสิทธิมนุษยชนขั้นพื้นฐานประเภทหนึ่งที่นานาประเทศให้ความสำคัญ ซึ่งคำว่า “สิทธิมนุษยชน” หมายถึง สิทธิขั้นพื้นฐาน เป็นมาตรฐานขั้นพื้นฐานที่พึงมี เป็นสิ่งจำเป็นในการดำรงชีวิตอย่างมีศักดิ์ศรีและมีคุณค่า หากมีการล่วงละเมิดต่อสิทธิดังกล่าวย่อมได้รับการรับรองและคุ้มครองโดยกฎหมาย สิทธิมนุษยชนในสมัยโบราณถูกกำหนดขึ้นเพื่อจำกัดสิทธิการใช้อำนาจรัฐแทรกแซงสิทธิของบุคคลอันเป็นที่มา

---

[1] นพดล นิ่มหนู. (2565). หลักการคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเปรียบเทียบพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ.2562กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540. ***วารสารมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยมหาสารคาม***, 41(3). หน้า 51.

ของความเชื่อเรื่องปัจเจกชนนิยม (Individualism) โดยให้คำอธิบายว่า กฎหมายธรรมชาติที่รับรองสิทธิมนุษยชนเป็นกฎหมายศักดิ์สิทธิที่พระเจ้าประทานให้มนุษย์ และ เป็นกฎหมายที่มีอำนาจสูงสุด รัฐจะตรากฎหมายที่ขัดแย้งกฎหมายธรรมชาติไม่ได้ แม้ว่าต่อมาสังคมให้ความสำคัญกับหลักเหตุผลมากกว่าความเชื่อเรื่องสิ่งศักดิ์สิทธิและพระเจ้า กฎหมายธรรมชาติยังได้รับการยอมรับในฐานะกฎของเหตุผลในทางโลกที่มีขึ้นเพื่อปกป้องสิทธิและผลประโยชน์ของบุคคล[2]

Thomas Hobbs กล่าวในหนังสือ Leviathan ไว้ว่า “ในสภาวะที่ยังไม่มีสังคมมนุษย์มีชีวิตอยู่ในธรรมชาติด้วยความหวาดกลัว เห็นแก่ตัวและชอบใช้ความรุนแรง เป็นสภาวะของอนาธิปไตย ด้วยความจำเป็นเพื่อหลีกหนีจากสภาวะอันเลวร้าย มนุษย์จึงรวมตัวกันขึ้นเป็นสังคม และทำความตกลงมอบสิทธิตามธรรมชาติของตนบางส่วนให้กับรัฐควบคุมดูแล เพื่อไม่ให้เกิดสภาวะที่เป็นอนาธิปไตยได้อีก” เช่นเดียวกับ John Locke (1690 cited in Davidson, 1982) กล่าวไว้ในหนังสือ The Second Treaties of Government ไว้ว่า “มนุษย์ ในสภาวะธรรมชาตินั้นเป็นสภาวะแห่งสันติสุข ต่างช่วยเหลือเกื้อกูลกัน มีความเสมอภาคและเป็นอิสระ มีสิทธิที่สำคัญ 3 ประการ คือ สิทธิในชีวิต อิสรภาพ และทรัพย์สิน ภายใต้การควบคุมของกฎแห่งธรรมชาติ การล่วงละเมิดสิทธิที่มนุษย์มีอยู่ตามธรรมชาติจะถูกลงโทษโดยการแก้แค้น ทดแทน จากผู้เสียหายหรือญาติมิตรของผู้เสียหาย” ซึ่ง Locke เรียกว่า “ความยุติธรรมส่วนตัว” (Private Justice) เมื่อมนุษย์มาอยู่รวมกันเป็นสังคมและยินยอมอยู่ใต้อำนาจรัฐซึ่งรับมอบหมายให้ปกป้องคุ้มครองสิทธิในชีวิต เสรีภาพ และทรัพย์สิน มนุษย์จำต้องสละสิทธิตามธรรมชาติบางส่วน ของตนเพื่อให้สังคมเกิดความสงบสุขและคงสิทธิธรรมชาติอื่นไว้ได้ หากรัฐใช้อำนาจละเมิดสิทธิของประชาชนเกินกว่าสิทธิที่ได้รับมอบหมายแล้ว ประชาชนก็มีสิทธิโดยชอบธรรมที่จะล้มล้างรัฐบาล และจัดตั้งรัฐบาลขึ้นใหม่ได้[3]

โดยการคุ้มครองข้อมูลส่วนบุคคลนั้น ถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว (Right of Privacy) เนื่องจากความเป็นอยู่ส่วนตัวนั้น ย่อมหมายความรวมถึง ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) และความเป็นส่วนตัวในเคหสถาน (Territorial Privacy) ซึ่งการคุ้มครองข้อมูลส่วนบุคคลนั้นถือได้ว่าเป็นความส่วนตัว

---

[2] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

[3] พงษ์เทพ สันติกุล. (2562). สิทธิมนุษยชน สิทธิพลเมือง และสิทธิทางสังคม. ***วารสารการเมือง การบริหาร และกฎหมาย***, 11(1). หน้า 37-60.

เกี่ยวกับข้อมูล โดยสิทธิความเป็นส่วนตัวมีการรับรองไว้อย่างชัดเจนในปฏิญญาสากลว่าด้วยสิทธิมนุษยชนข้อ 12[4] ก็ได้บัญญัติให้ความคุ้มครองรับรองสิทธิความเป็นอยู่ส่วนตัวไว้เช่นกัน

ในสังคมยุคปัจจุบัน บรรดาความเป็นส่วนตัวของข้อมูลส่วนบุคคล เป็นเรื่องที่ประเทศส่วนใหญ่ให้ความสำคัญเป็นอย่างมาก ทั้งนี้ เนื่องจากความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศที่เป็นไปอย่างรวดเร็ว การรับรู้ข้อมูลข่าวสารต่างๆ เป็นเรื่องที่สะดวกสบายมากขึ้น เมื่ออินเทอร์เน็ตได้เข้ามาเป็นสื่อที่มีบทบาทสำคัญในการติดต่อ สื่อสารระหว่างกันและเป็นสื่อที่ได้รับความนิยมอย่างแพร่หลาย ทำให้แทบทุกกิจกรรมที่เกิดขึ้น ล้วนแต่มีความเกี่ยวข้องกับอินเทอร์เน็ตทั้งสิ้น ส่งผลให้ธุรกิจและธุรกรรมต่างๆ บนอินเทอร์เน็ต เกิดขึ้นมากมาย ในแต่ละวันข้อมูลนับล้านถูกส่งผ่านเครือข่าย เพื่ออำนวยความสะดวกให้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ต่างๆ อย่างไรก็ตาม ในทางกลับกันเมื่อข้อมูลต่างๆ สามารถเข้าถึงได้ง่าย จึงอาจมีการนำข้อมูลเหล่านี้ไปใช้โดยละเมิดต่อบุคคลอื่น โดยอาจทำให้เกิดความเสียหายหรือสูญหายของข้อมูล หรืออาจถูกนำข้อมูลไปใช้ในทางที่ผิด ไม่ว่าจะโดยเจตนาหรือไม่เจตนาก็ตาม[5]

2.1.2 ประวัติความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

สำหรับประเทศไทยซึ่งเป็นสมาชิกขององค์กรสหประชาชาติ ได้ให้การรับรองและคุ้มครองในเรื่องข้อมูลส่วนบุคคลไว้เช่นเดียวกัน โดยบัญญัติไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทยทั้งในฉบับก่อน คือ ฉบับปี พ.ศ. 2550 ในมาตรา 35 วรรคสาม[6] และตามรัฐธรรมนูญฉบับ

---

[4] มาตรา 12 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการแทรกแซงสิทธิ หรือการลบหลู่ดังกล่าวนั้น

[5] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

[6] มาตรา 35 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ

ปัจจุบัน คือ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 หมวด 3 สิทธิเสรีภาพของปวงชนชาวไทย มาตรา 32[7]

ซึ่งก่อนที่จะมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562ภาครัฐได้มีความพยายามที่จะจัดให้มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขึ้นมาเป็นระยะเวลานานกว่า 10 ปี โดยเล็งเห็นถึงความก้าวหน้าทางเทคโนโลยี การคุ้มครองความเป็นส่วนตัว และแนวโน้มการละเมิดสิทธิในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวที่เพิ่มมากขึ้น โดยเฉพาะการนำข้อมูลส่วนบุคคลไปเปิดเผยโดยมิชอบหรือเปิดเผยโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลเพื่อแสวงหาประโยชน์ต่าง ๆ จึงมีการศึกษาและร่างกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลขึ้น

ต่อมาประเทศไทยได้ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้น โดยมีเหตุผลที่ประกาศใช้พระราชบัญญัติดังกล่าว คือ เนื่องจากประเทศไทยมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก จนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวกและรวดเร็ว ซึ่งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม ประเทศไทยจึงได้ประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูล ส่วนบุคคลที่เป็นหลักการทั่วไป[8]

---

[7] มาตรา 32 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศชื่อเสียงและครอบครัว

การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่งหรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

[8] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

2.2 ความหมายของข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้นิยามความหมายของข้อมูลส่วนบุคคล ไว้ว่า “ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่จะไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรมโดยเฉพาะ[9]”

คำนิยามข้างต้น แสดงให้เห็นได้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับกับข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลธรรมดาคนนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม และไม่ใช้บังคับกับข้อมูลที่สามารถระบุไปยังตัวนิติบุคคลได้

นอกจากนี้แล้วคำนิยามของคำว่า “ข้อมูลส่วนบุคคล”[10] ยังกำหนดกรณีที่เป็นข้อมูลของบุคคลธรรมดาแต่ไม่ถือว่าเป็นข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ด้วย กล่าวคือ ข้อมูลของผู้ที่ถึงแก่ความตายแล้ว จะไม่ถือว่าเป็นข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ ดังนั้น การประมวลผลข้อมูลส่วนบุคคลของผู้ที่ถึงแก่ความตายจึงสามารถกระทำได้โดยไม่ต้องดำเนินการตามหลักเกณฑ์และเงื่อนไขที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

จากนิยามข้างต้นสามารถสรุปได้ว่า “ข้อมูลส่วนบุคคล” ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คือข้อมูลที่มีลักษณะหรือองค์ประกอบ ดังนี้

1) เป็นข้อมูลของบุคคลธรรมดา (Natural Person)

2) เจ้าของข้อมูลส่วนบุคคลยังไม่ถึงแก่ความตาย

3) ข้อมูลนั้นสามารถระบุตัวบุคคลได้ไม่ว่าทางตรง หรือทางอ้อม

ดังนั้น ข้อมูลใดที่ไม่มีลักษณะ 3 ประการดังที่ระบุข้างต้น ข้อมูลนั้นไม่จัดเป็น “ข้อมูลส่วนบุคคล” ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การประมวลผลข้อมูลดังกล่าวจึงไม่ต้องดำเนินการตามหลักเกณฑ์และเงื่อนไขที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โดยมีข้อสังเกตในการพิจารณาข้อมูลส่วนบุคคล[11] ดังนี้

---

[9] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 6 วรรคหนึ่ง.

[10] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 6 วรรคหนึ่ง.

[11] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

1) การจะพิจารณาว่าข้อมูลใดเป็นข้อมูลส่วนบุคคลหรือไม่นั้น ต้องพิจารณาถึงสภาพของข้อมูลส่วนบุคคลและบริบทของการประมวลผลข้อมูลส่วนบุคคลด้วย กล่าวคือ ข้อมูลบางอย่างหากถูกเก็บรวบรวมไว้แยกจากข้อมูลอื่น ๆ ก็จะไม่สามารถระบุตัวบุคคลได้ แต่หากรวมกับข้อมูลอื่น ๆ จะทำให้สามารถระบุตัวบุคคลได้ไม่ว่าจะทางตรงหรือทางอ้อม เช่น อายุ เพศ ศาสนา อาชีพ หากองค์กรใดแยกเก็บข้อมูลส่วนบุคคลเหล่านี้เป็นชุดข้อมูลเดี่ยว ๆ ข้อมูลเหล่านี้ก็จะไม่สามารถระบุตัวบุคคลได้

2) ข้อมูลที่เกี่ยวกับนิติบุคคลบางกรณีอาจเป็น "ข้อมูลส่วนบุคคล" ได้ เช่น หนังสือรับรองบริษัทที่มีรายชื่อกรรมการบริษัทหรือรายชื่อผู้ถือหุ้นบริษัท

3) ประเภทของข้อมูลส่วนบุคคลที่จะถูกจัดเก็บหรือประมวลผลนั้น เป็นไปตามความจำเป็นและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

ทั้งนี้ ข้อมูลส่วนบุคคลบางประเภท เป็นข้อมูลส่วนบุคคลอันมีลักษณะต้องห้ามตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังมีการกำหนดข้อมูลส่วนบุคคลไว้อีกประเภทหนึ่ง เรียกว่า "ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data)" โดยที่ มาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดว่า ข้อมูลอันเกี่ยวกับ เชื้อชาติ เผ่าพันธุ์ ความเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ รวมถึงข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการกำหนด ถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว[12]

2.3 แนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

แนวความคิดของความเป็นส่วนตัวได้มีการพัฒนามาตลอดตั้งแต่สมัยโบราณ แต่จะมากน้อยขึ้นอยู่กับบริบทของสังคมและวัฒนธรรมในช่วงเวลานั้นๆ พัฒนาการครั้งสำคัญที่เห็นว่ามีความชัดเจนในการพัฒนาแนวความคิดการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวมากที่สุดคือ เมื่อมีการเผยแพร่บทความเรื่อง "The Right to Privacy" โดย ซามูเอล ดี. วอร์เรนที่ 2 (Samuel D. Warren) และ Louis D. Brandeis บทความดังกล่าวเป็นผลสะท้อนของการพัฒนาเทคโนโลยีในช่วงปี ค.ศ.1890 การเกิดขึ้นของโทรเลข โทรศัพท์ แท่นพิมพ์หนังสือที่สามารถพิมพ์หนังสือได้รวดเร็ว และการคิดค้นเครื่องมือเครื่องใช้ใหม่ๆ และการพัฒนาระบบธุรกิจซึ่ง Warren และ Brandeis กล่าวว่า ความก้าวหน้าดังกล่าวนี้ทำให้มีความจำเป็นต้องให้ความคุ้มครองแก่บุคคล เพราะพัฒนาการของ

[12] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 26 วรรคหนึ่ง.

เทคโนโลยีดังกล่าวทำให้เกิดการคุกคามสิทธิประโยชน์ของบุคคลอย่างน่ากลัวในบทความ The Right to Privacy ดังกล่าว Warren และ Brandeis อธิบายถึง “สิทธิในความเป็นส่วนตัว (Privacy)” ว่าหมายถึง “สิทธิที่จะอยู่ตามลำพัง (the right to be let alone)” เป็นการมองสิทธิในความเป็นอยู่ส่วนตัวเป็นสองแง่มุม คือ ความเป็นส่วนตัวในแง่นามธรรม ได้แก่การที่บุคคลมีสิทธิและเสรีภาพในการแสดงอารมณ์ ความรู้สึกนึกคิด ตลอดจนความเชื่อถือศรัทธาในลัทธิศาสนา ส่วนความเป็นส่วนตัวในทางรูปธรรม คือ สิทธิที่จะอยู่โดยลำพังปราศจากการรบกวนและการแทรกแซงจากสังคม การอยู่อย่างสันโดษโดยไม่ติดต่อสัมพันธ์กับสังคม[13]

โดยแนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นครั้งแรกในประเทศเยอรมนี โดยกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลฉบับแรก คือ กฎหมายของรัฐ Hessen ซึ่งเป็นกฎหมายที่มีผลบังคับใช้ในระดับรัฐบัญญัติขึ้นในปี ค.ศ. 1970 และต่อมาในปี ค.ศ. 1977 ประเทศเยอรมนีได้บังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับสหพันธรัฐ (Federal Act on Data Protection)(Library of Congress, 2018) และต่อมาประเทศอื่นๆ ก็ได้มีการบัญญัติกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เช่น ประเทศฝรั่งเศส[14] ประเทศสหรัฐอเมริกา[15] นอกจากนี้ประเทศในกลุ่มประชาคมอาเซียน (ASEAN) เช่น ประเทศมาเลเซีย[16] สาธารณรัฐสิงคโปร์ [17] ประเทศฟิลิปปินส์[18] ต่างก็มีกฎหมายซึ่งให้ความคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ

ในปี ค.ศ. 1995 สหภาพยุโรปได้ออกหลักเกณฑ์ คือ Directive95/46/EC ขึ้นมาบังคับใช้ในกลุ่มประเทศสมาชิกของสหภาพยุโรป โดยเป็นบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและเสรีภาพในการเคลื่อนไหวของข้อมูลต่อมาในปี ค.ศ. 2016 รัฐสภาแห่งยุโรปได้ประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ คือ EU General Data Protection Regulation (GDPR) ซึ่งมีผลบังคับใช้แล้วเมื่อปี ค.ศ. 2018 โดยเป็นกฎหมายที่มีสาระสำคัญเกี่ยวกับการคุ้มครองสิทธิของประชาชนในกลุ่มประเทศสมาชิกสหภาพยุโรปเกี่ยวกับข้อมูลส่วนบุคคลและความเป็นส่วนตัว

---

[13] สุขวสา ถมังรักษ์สัตว์. (2562). การคุ้มครองข้อมูลส่วนบุคคลของเด็กบนสื่ออิเล็กทรอนิกส์. ***วารสารเกษมบัณฑิต,*** 20(1). หน้า 131-145.

[14] Act No. 78-17 of 6 January 1978 on information Technology, Data Files and Civil Liberties

[15] การคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาไม่ได้อยู่ในรูปแบบของกฎหมายซึ่งให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป แต่จะเป็นการคุ้มครองข้อมูลส่วนบุคคลภายใต้กฎหมายในเรื่องอื่น เช่น ในกฎหมายระดับสาธารณรัฐ การคุ้มครองข้อมูลส่วนบุคคลจะเป็นไปตามบทบัญญัติของ Federal Trade Commission Act หรือการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายของสถาบันการเงิน คือ Gramm Leach Bliley Act เป็นต้น

[16] Personal Data Protection Act 2010 (PDPA)

[17] Personal Data Protection Act 2012 (No. 26 of 2012)

[18] Data Privacy Act of 2012 (Republic Act No. 10173)

โดยมีหลักเกณฑ์เกี่ยวกับการใช้อำนาจนอกอาณาเขต (Extraterritorial Jurisdiction) คือ ให้ความคุ้มครองต่อข้อมูลส่วนบุคคลของประชาชนในกลุ่มประเทศสหภาพยุโรปไม่ว่าข้อมูลนั้นจะถูกรวบรวมหรือประมวลผลในพื้นที่ใดในโลก กำหนดบทลงโทษแก่ผู้ที่ก่อให้เกิดความเสียหายหรือทำให้ข้อมูลส่วนบุคคลรั่วไหล โดยต้องโทษปรับ 20 ล้านยูโร หรือปรับไม่เกินร้อยละ 4 ของรายได้ทั่วโลกของกิจการนั้น ขึ้นอยู่กับว่าจำนวนใดมากกว่า รวมทั้งกำหนดหลักเกณฑ์เกี่ยวกับการให้ความยินยอมของเจ้าของข้อมูลและการยกเลิกการให้ความยินยอม (European Commission, 2018)[19]

องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organisation for Economic Co-operation and Development หรือ OECD) ซึ่งเป็นองค์การระหว่างประเทศได้จัดทำ Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ซึ่งกำหนดหลักการพื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้ (OECD, 2013)

1) หลักการจัดเก็บรวบรวมข้อมูลส่วนบุคคลโดยจำกัด (Collection Limitation Principle) หมายถึง การจัดเก็บข้อมูลส่วนบุคคลต้องเป็นไปโดยจำกัด และต้องใช้วิธีการโดยชอบด้วยกฎหมายและเป็นธรรม โดยเจตนาของข้อมูลส่วนบุคคลต้องรับรู้และยินยอมให้มีการจัดเก็บข้อมูลส่วนบุคคลนั้น

2) หลักการประมวลผลข้อมูลส่วนบุคคลอย่างมีคุณภาพ (Data Quality Principle) หมายถึง ข้อมูลส่วนบุคคลที่ถูกจัดเก็บรวบรวมต้องเกี่ยวข้องกับวัตถุประสงค์ของการจัดเก็บข้อมูลนั้น และข้อมูลส่วนบุคคลนั้นต้องถูกต้อง สมบูรณ์ และปรับปรุงให้เป็นปัจจุบันเสมอ

3) หลักการระบุวัตถุประสงค์ (Purpose Specification Principle) หมายถึง การจัดเก็บรวบรวมข้อมูลส่วนบุคคลต้องระบุวัตถุประสงค์แห่งการจัดเก็บนั้นก่อน หรือในเวลาที่ทำการจัดเก็บข้อมูล และการใช้ข้อมูลส่วนบุคคลนั้น จะต้องเป็นไปตามวัตถุประสงค์ดังกล่าวเท่านั้น หากวัตถุประสงค์ในการใช้ข้อมูลส่วนบุคคลเปลี่ยนแปลง วัตถุประสงค์ที่เปลี่ยนแปลงไปนั้นจะต้องไม่ขัดหรือแย้งกับวัตถุประสงค์เดิม

4) หลักการใช้ข้อมูลส่วนบุคคลอย่างจำกัด (Use Limitation Principle) หมายถึง ข้อมูลส่วนบุคคลจะต้องไม่ถูกเปิดเผย เข้าถึง หรือใช้สำหรับวัตถุประสงค์เพื่อการอื่นนอกเหนือไปจากวัตถุประสงค์ที่ได้ระบุไว้ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นการใช้ตามที่บทบัญญัติของกฎหมายได้กำหนดไว้

5) หลักการรักษาความปลอดภัยของข้อมูลส่วนบุคคล (Security Safeguards Principle) หมายถึง ข้อมูลส่วนบุคคลจะต้องถูกปกป้องรักษาโดยใช้วิธีการรักษาความปลอดภัยที่

---

[19] ตวงพร ปิยวิทย์. (2564). กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศ***ไทย. วารสารวิชาการ คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏนครราชสีมา***, 1(1). หน้า 83-83.

เหมาะสม โดยต้องป้องกันต่อความเสี่ยงที่ข้อมูลส่วนบุคคลจะสูญหาย ถูกเข้าถึงโดยมิชอบ ถูกทำลาย ถูกใช้ ถูกแก้ไขเปลี่ยนแปลง หรือถูกเปิดเผย

6) หลักความโปร่งใส (Openness Principle) หมายถึง การมีนโยบายเกี่ยวกับความโปร่งใสของ การพัฒนา การปฏิบัติงาน และนโยบายเกี่ยวกับข้อมูลส่วนบุคคลโดยวิธีการนั้น ต้องแสดงให้เห็นถึงการมีอยู่และลักษณะของข้อมูลส่วนบุคคล วัตถุประสงค์หลักของการใช้ รวมถึงชื่อและสถานที่ตั้งของผู้ควบคุมข้อมูลส่วนบุคคล

7) หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle) หมายถึง เจ้าของข้อมูลส่วนบุคคลต้องมีสิทธิดังต่อไปนี้[20]

(1) สิทธิที่จะได้รับการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลว่ามีข้อมูลส่วนบุคคลของตนเองหรือไม่

(2) สิทธิที่จะติดต่อสื่อสารกับผู้ควบคุมข้อมูลส่วนบุคคลภายในระยะเวลาที่เหมาะสม ปราศจากค่าใช้จ่ายหรือเสียค่าจ่ายโดยน้อยที่สุด โดยวิธีการที่เหมาะสม และโดยรูปแบบที่เจ้าของข้อมูลสามารถเข้าใจได้โดยง่าย

(3) สิทธิที่จะได้รับการชี้แจงในกรณีที่ผู้ควบคุมข้อมูลปฏิเสธไม่ปฏิบัติตามสิทธิทั้ง 2 สิทธิข้างต้น และ มีสิทธิที่จะโต้แย้งการปฏิเสธนั้นได้

(4) สิทธิที่จะโต้แย้งการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลของตน และหากการโต้แย้งสำเร็จ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลทำลาย แก้ไขให้ถูกต้อง ทำข้อมูลให้สมบูรณ์ หรือแก้ไขเพิ่มเติมข้อมูลส่วนบุคคลของตน

8) หลักความรับผิดชอบ (Accountability Principle) หมายความว่า ผู้ควบคุมข้อมูลส่วนบุคคลต้องรับผิดชอบต่อการปฏิบัติตามมาตรการต่างๆ เพื่อให้เป็นไปตามหลักการพื้นฐานคุ้มครองข้อมูลส่วนบุคคลข้างต้น

อีกทั้ง แนวความคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) เป็นแนวความคิดที่มีพัฒนาการมาจากการคุ้มครองสิทธิในความเป็นส่วนตัว (Privacy Right) มีพัฒนาการมาเป็นระยะเวลายาวนานแล้วโดยในสมัยโรมันแนวความคิดเกี่ยวกับเรื่องความเป็นส่วนตัวยอมรับว่าบุคคลแต่ละคนมีเขตแดนของตนเอง ในเขตแดนเสมือนเป็นที่พักที่บุคคลไม่เกี่ยวข้องกับกิจกรรมทางสังคมในช่วงเวลาส่วนตัว เป็นดินแดนเฉพาะตัวของแต่ละบุคคลเท่านั้น และเป็นที่ปราศจากการเข้ามาเกี่ยวข้องจากคนอื่น แนวความคิดในการคุ้มครองความเป็นส่วนตัวที่มีความชัดเจนและได้รับการยอมรับมากที่สุดเมื่อมีการเผยแพร่บทความเรื่อง “The Right to Privacy” หรือ “สิทธิในความเป็นส่วนตัว” ของ Samuel D. Warren และ Louis D. Brandies ที่สะท้อนปัญหา

[20] ตวงพร ปิยวิทย์. อ้างแล้วเชิงอรรถที่ 19. หน้า 83-83.

การคุกคามความเป็นส่วนตัวของปัจเจกบุคคลจากการนำเสนอข่าวของสื่อมวลชน ผู้วิจัยอธิบายว่าสิทธิในความเป็นส่วนตัวหมายถึง สิทธิที่จะอยู่โดยลำพัง (Right to be let alone) นอกจากนี้ยังกล่าวด้วยว่าสิทธิในความเป็นส่วนตัวของบุคคลย่อมหมดไปเมื่อบุคคลนั้นเปิดเผยข้อมูลของตนเองสู่สาธารณะหรือด้วยความยินยอมของเจ้าของข้อมูลเองบทความดังกล่าวมีอิทธิพลต่อกฎหมายว่าด้วยการคุ้มครองความเป็นส่วนตัวในบริบทของกฎหมายละเมิดของสหรัฐอเมริกาเป็นอย่างมาก รวมทั้งแสดงให้เห็นถึงการขัดกันระหว่างสิทธิในความเป็นส่วนตัวของปัจเจกบุคคลกับเสรีภาพในการแสดงความเห็นของสื่อมวลชนอีกด้วย ส่วนแนวความคิดในการตรากฎหมายเพื่อคุ้มครองสิทธิในข้อมูลส่วนบุคคลเริ่มจากภาคพื้นยุโรปเป็นที่แรก กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกเกิดขึ้นที่รัฐเฮ็สส์ (Hesse) ประเทศสหพันธ์สาธารณรัฐเยอรมนี ในปี 1970 ตามมาด้วยประเทศสวีเดนในปี 1973 ประเทศสหรัฐอเมริกาในปี 1974 และประเทศฝรั่งเศสในปี 1978[21]

2.4 ประเภทของข้อมูลส่วนบุคคล

การให้ความคุ้มครองข้อมูลส่วนบุคคลสามารถแบ่งความคุ้มครองแก่ข้อมูลออกเป็น 2 ประเภทแตกต่างกัน[22] คือ ข้อมูลทั่วไป[23] (Non-Sensitive Data) และข้อมูลประเภทที่มีความอ่อนไหว[24] (Sensitive Data) โดยข้อมูลแต่ละประเภทมีลักษณะดังต่อไปนี้

2.4.1 ข้อมูลส่วนบุคคลทั่วไป (Non-Sensitive Data)

ข้อมูลส่วนบุคคลทั่วไป (Non-Sensitive Data) คือ ข้อมูลเกี่ยวกับบุคคลผู้เป็นเจ้าของข้อมูลซึ่ง สามารถบ่งชี้เฉพาะเจาะจงไปยังเจ้าของข้อมูลได้ ซึ่งข้อมูลประเภทดังกล่าวเป็นข้อมูลซึ่งมิได้มีความละเอียดอ่อนจนอาจนำมาสู่ปัญหาต่างๆ ได้จึงทำให้ ข้อมูลดังกล่าวเป็นข้อมูลที่อาจเก็บรวบรวม เปิดเผย หรือใช้ได้ ทั้งนี้ ภายใต้หลักเกณฑ์ที่กฎหมายกำหนดไว้

ข้อมูลส่วนบุคคลทั่วไป[25] ได้แก่

---

[21] บรรเจิด ภาคาพันธุ์. (2563). ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในธุรกิจประกันชีวิต. ***วารสารบัณฑิตศึกษานิติศาสตร์,*** 13(1). หน้า 120-135.

[22] วันพิชิต ชินตระกูลชัย. (2564). ***ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหวคืออะไร มีกี่ประเภท มีอะไรบ้าง*** ?. (ออนไลน์). เข้าถึงได้จาก: https://openpdpa.org/personal-data-type/. [2566, 30 มิถุนายน]

[23] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 6.

[24] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 26.

[25] บทความสาระ. (2564). ***PDPA คืออะไร? – สรุป PDPA เกี่ยวกับธุรกิจที่คุณควรรู้! ฉบับเข้าใจง่าย ?.*** (ออนไลน์). เข้าถึงได้จาก: https://easypdpa.com/article/easypdpa-summary-what-is-pdpa [2566,9 กรกฎาคม]

1) ชื่อ-นามสกุล

2) เบอร์โทรศัพท์ อีเมลส่วนตัว ที่อยู่ปัจจุบัน

3) เลขบัตรประชาชน เลขหนังสือเดินทาง เลขใบอนุญาตขับขี่

4) ข้อมูลทางการศึกษา ข้อมูลทางการเงิน ข้อมูลทางการแพทย์

5) ทะเบียนรถยนต์ โฉนดที่ดิน ทะเบียนบ้าน

6) วันเดือนปีเกิด สัญชาติ น้ำหนักส่วนสูง

2.4.2 ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive data)

ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive data) คือ ข้อมูลของบุคคลซึ่งถือเป็นเรื่องเฉพาะตัวของตัวบุคคล เป็นข้อมูลซึ่งมีความละเอียดอ่อนสูง กล่าวคือ ข้อมูลประเภทดังกล่าวเป็นข้อมูลซึ่งหากมีการเปิดเผยอาจก่อให้เกิดผลกระทบที่ไม่พึงประสงค์ตามมา เช่น กระทบต่อความรู้สึกของเจ้าของข้อมูลหรือประชาชนทั่วไปเป็นข้อมูลที่ก่อให้เกิดความขัดแย้งได้ ก่อให้เกิดผลกระทบต่อชื่อเสียงหรือเกียรติคุณของเจ้าของข้อมูล หรือเป็นข้อมูลซึ่งหากมีการเปิดเผยอาจก่อให้เกิดการตั้งข้อรังเกียจหรือเลือกปฏิบัติหรือเกิดอันตรายต่อเจ้าของข้อมูล เป็นต้น โดยข้อมูลประเภทดังกล่าวเจ้าของข้อมูลประสงค์ที่จะเก็บข้อมูลประเภทนี้ไว้เป็นความลับหรือไม่ประสงค์ให้มีการเปิดเผยข้อมูล[26] เช่น

1) เชื้อชาติ เผ่าพันธุ์

2) ความคิดเห็นทางการเมือง

3) ความเชื่อในลัทธิ ศาสนาหรือปรัชญา

4) พฤติกรรมทางเพศ

5) ประวัติอาชญากรรม

6) ข้อมูลด้านสุขภาพ ความพิการ เช่น โรคประจำตัว การฉีดวัคซีน ใบรับรองแพทย์

7) ข้อมูลสหภาพแรงงาน

8) ข้อมูลพันธุกรรม

9) ข้อมูลชีวภาพ เช่น ลายนิ้วมือ แบบจำลองใบหน้า ข้อมูลม่านตา

สำหรับหลักเกณฑ์ในการให้ความคุ้มครองต่อข้อมูลทั้งสองประเภทดังกล่าวมีความแตกต่างกัน เนื่องจากการเก็บรวบรวม เปิดเผย หรือใช้ข้อมูลส่วนบุคคลประเภทที่มีความอ่อนไหว (Sensitive Data) อาจนำมาซึ่งปัญหาต่างๆ ดังที่ได้กล่าวมาแล้ว ดังนั้น ในหลายๆ ประเทศข้อมูลประเภทที่มีความอ่อนไหว (Sensitive Data) จึงถูกกำหนดให้เป็นข้อมูลที่ห้ามทำการเก็บรวบรวม ใช้

---

[26] วันพิชิต ชินตระกูลชัย. (2564). ***ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหวคืออะไร มีกี่ประเภท มีอะไรบ้าง*** ?. (ออนไลน์). เข้าถึงได้จาก: https://openpdpa.org/personal-data-type/. [2566, 30 มิถุนายน]

หรือเปิดเผยข้อมูลโดยเด็ดขาด เว้นแต่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล หรือเป็นกรณีอื่นตามที่กฎหมายกำหนดไว้ เช่น เป็นการปฏิบัติตามกฎหมาย หรือเป็นการจำเป็นเพื่อการดำเนินคดี เป็นต้น แต่ข้อมูลประเภทข้อมูลทั่วไปนั้น (Non-Sensitive Data) กฎหมายกำหนดให้สามารถทำการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลได้ หากได้รับความยินยอมจากเจ้าของข้อมูล

นอกจากนี้ยังสามารถแบ่งประเภทของข้อมูลส่วนบุคคลในประเด็นเกี่ยวกับความอ่อนไหวที่อาจส่งผลกระทบต่อผู้เป็นเจ้าของข้อมูลส่วนบุคคลหากมีการเปิดเผยหรือล่วงรู้ข้อมูลนั้นได้เป็น 3 ระดับ ดังนี้

1) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับต่ำ (Low-Sensitive) ข้อมูลประเภทนี้เป็นข้อมูลที่ความเกี่ยวข้องกับบุคคลเป็นข้อมูลที่มีความอ่อนไหว เนื่องจากข้อมูลเหล่านี้อาจช่วยทำให้ได้มาซึ่งข้อมูลที่มีระดับความอ่อนไหวสูงขึ้น

2) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับปานกลาง (Moderate-Sensitivity) ข้อมูลประเภทนี้เป็นข้อมูลที่มีความอ่อนไหวมาในแง่ที่มีโอกาสที่จะก่อให้เกิดความเสียหาย เมื่อข้อมูลถูกนำเอาไปใช้ในทางที่ผิดอยู่ในระดับสูง ข้อมูลประเภทนี้ครอบคลุมถึงข้อมูลประเภทที่เกี่ยวกับความคิดเห็นของบุคคล ซึ่งมีความครอบคลุมในทุกเรื่องของชีวิต ข้อมูลที่มีความอ่อนไหวระดับปานกลางนี้ มีความสำคัญ เช่น กันกับข้อมูลที่มีความอ่อนไหวระดับสูง และไม่ควรเก็บไว้โดยสิ้นเชิง

3) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับสูง (High-Sensitivity) ข้อมูลประเภทนี้ ได้แก่ ข้อมูลรายละเอียดส่วนตัวของบุคคลในส่วนที่เกี่ยวข้องกับประวัติทางการแพทย์ พฤติกรรมทางเพศ หรือข้อเท็จจริงด้านอื่น ๆ ในชีวิตของบุคคล ซึ่งสามารถกล่าวได้ว่าเป็นเรื่องส่วนตัวหรือลับเฉพาะข้อมูลประเภทนี้มีความอ่อนไหวสูง จึงมีความสำคัญและไม่ควรถูกเก็บรวบรวมไว้โดยสิ้นเชิง[27]

2.5 หลักการทั่วไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลเป็นสิ่งสำคัญในการพัฒนาเศรษฐกิจ การดำเนินธุรกิจล้วนอาศัยข้อมูลเป็นปัจจัยสำคัญ ดังนั้น ประเทศต่างๆ จึงให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลโดยนำหลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งหลักการขององค์การต่างๆ เช่น องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development

[27] เอกณัท สุชาติพันธุ์, ประพันธ์พงษ์ ขาอ่อน. (2562). การคุ้มครองข้อมูลส่วนบุคคลในภาคธุรกิจธนาคาร. ***การประชุมนำเสนอผลงานวิจัยบัณฑิตศึกษาระดับชาติ ครั้งที่ 14 ปีการศึกษาที่ 2562.*** หน้า 202-207.

หรือ OECD) หรือองค์การสหประชาชาติ เป็นต้น มาเป็นแนวทางในการร่างกฎหมาย เพื่อที่จะสามารถทำความเข้าใจกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของนานาประเทศได้ดีจึงควรศึกษาหลักการทั่วไป และหลักการขององค์การต่างๆ

2.5.1 หลักการทั่วไป

1) หลักการคุ้มครองข้อมูลส่วนบุคคลโดยกฎหมายทั่วไป

ในปี ค.ศ. 1970 บัญญัติกฎหมายทั่วไปขึ้นมาฉบับหนึ่งซึ่งเป็นกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลขึ้น ซึ่งนับเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกของโลก ซึ่งในเวลาต่อมาหลายประเทศก็ได้มีการบัญญัติกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยวางหลักการทั่วไปครอบคลุมถึงการเก็บรวบรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคลทั้งของภาครัฐและภาคเอกชน โดยกำหนดให้มีหน่วยงานกลางคอยกำกับดูแลให้มีการปฏิบัติตามกฎหมาย ภาคธุรกิจอุตสาหกรรมอาจกำหนดหลักเกณฑ์ในการคุ้มรองข้อมูลส่วนบุคคลขึ้นเพื่อใช้บังคับกันเองและมีหน่วยงานกลางคอยดูแลให้มีการปฏิบัติตามหลักเกณฑ์ที่กำหนด[28]

2) หลักการคุ้มครองข้อมูลส่วนบุคคลโดยกฎหมายเฉพาะ

การคุ้มครองโดยกฎหมายเฉพาะการบัญญัติกฎหมายเฉพาะเพื่อคุ้มครองข้อมูลส่วนบุคคลเฉพาะกรณีเป็นวิธีการที่นิยมใช้ในบางประเทศ เช่น สหรัฐอเมริกา เป็นการหลีกเลี่ยงการวางหลักทั่วไปโดยมีกฎหมายแต่ละเรื่องไว้เป็นการเฉพาะ[29] เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของเด็กบนเครือข่ายอินเทอร์เน็ต (Children's Online Privacy Act of 1998:COPPA) กฎหมายคุ้มครองข้อมูลส่วนบุคคลในการหาคู่ทางคอมพิวเตอร์ (Computer Matching and Privacy Protection Act of 1998) ข้อดีของการบัญญัติกฎหมายเฉพาะต้องมีการบัญญัติกฎหมาย คือรัฐสามารถวางกฎเกณฑ์เฉพาะเรื่องได้ ส่วนข้อเสียคือการบัญญัติกฎหมายเฉพาะต้องมีการปรับปรุง พัฒนา แก้ไข หรือบัญญัติกฎหมายใหม่เพื่อรองรับให้ทันกับเทคโนโลยีที่มีการเปลี่ยนแปลงตลอดเวลา

3) หลักการคุ้มครองข้อมูลส่วนบุคคลโดยกลไกการกำกับดูแลตนเอง

การใช้กลไกกำกับดูแลตนเอง (Personal Data Protection) ในการคุ้มครองข้อมูลส่วนบุคคลนั้นเป็นการที่ผู้ประกอบการภาคธุรกิจประเภทเดียวกันหรือกลุ่มเดียวกันร่วมกันจัดทำประมวลจริยธรรมเพื่อเป็นระเบียบปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลและร่วมกันดูแล ให้สมาชิกปฏิบัติตามกฎระเบียบปฏิบัตินั้นโดยไม่มีหน่วยงานกลางคอยกำกับดูแล[30]

---

[28] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

[29] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

[30] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

4) การใช้เทคโนโลยี

ในปัจจุบันมีการพัฒนาเทคโนโลยีอย่างรวดเร็วจึงมีการติดต่อสื่อสารผ่านคอมพิวเตอร์[31] เช่น การส่งอิเล็กทรอนิกส์เมล์ (E-mail) หรือ แอพริเคชั่นต่างๆ กันอย่างแพร่หลาย จึงมีผู้คิดค้นเทคโนโลยีเพื่อคุ้มครองข้อมูลส่วนบุคคลในระหว่างการติดต่อสื่อสารในช่องทางดังกล่าวการคุ้มครองข้อมูลส่วนบุคคลนั้นมีหลายรูปแบบโดยหลักเกณฑ์หรือรูปแบบดังกล่าวมีลักษณะมีหลักเกณฑ์หรือหลักปฏิบัติที่แตกต่างกันออกไป เนื่องจากการบังคับใช้กฎหมายในแต่ละประเทศหรือองค์กรนั้นรวมทั้งรูปแบบของข้อมูลที่แตกต่างกัน

2.5.2 การคุ้มครองข้อมูลส่วนบุคคลตามหลักสากล

หลักการพื้นฐานของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในระดับสากลนั้น มีหลักการสำคัญซึ่งเป็นหัวใจของเรื่องอยู่ 9 หลัก[32] ดังต่อไปนี้

1) หลักการจัดเก็บข้อมูลส่วนบุคคลอย่างจำกัด (Collection Limitation Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลอย่างจำกัดเพียงเท่าที่จำเป็นเท่านั้น และการเก็บรวบรวมข้อมูลส่วนบุคคลต้องกระทำโดยวิธีการที่เป็นธรรมและชอบด้วยกฎหมาย นอกจากนี้ ต้องกระทำภายใต้ความรับรู้ และความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลด้วย

2) หลักการประมวลผลข้อมูลส่วนบุคคลอย่างมีคุณภาพและได้สัดส่วน (Data Quality and Proportional Principle)

หลักการดังกล่าวกำหนดให้ข้อมูลส่วนบุคคลที่ทำการประมวลผลนั้นต้องมีความเกี่ยวข้อง เพียงพอ และได้สัดส่วนหรือเกี่ยวเนื่องกับวัตถุประสงค์ที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล นอกจากนี้ ข้อมูลส่วนบุคคลนั้นต้องมีถูกต้องสมบูรณ์และมีการปรับปรุงให้ทันสมัยอยู่ตลอดเวลาเมื่อผู้ควบคุมข้อมูลส่วนบุคคลจะทำการประมวลผลและใช้ข้อมูลส่วนบุคคลนั้น อย่างไรก็ดี หลักการนี้ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลนั้น จัดเก็บและประมวลผลข้อมูลส่วนบุคคลประเภทที่มีความอ่อนไหว (Sensitive Data) เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยชัดแจ้งซึ่ง ข้อมูลประเภทที่มีความอ่อนไหว[33] เช่น ข้อมูลเกี่ยวกับชาติกำเนิด ความเชื่อทางศาสนา หรือความเชื่อทางปรัชญา เป็นต้น

---

[31] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

[32] อธิพร สิทธิธีรรัตน์.(2558). ***ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขาการค้าระหว่างประเทศ, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. หน้า 18-21.

[33] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

3) หลักการระบุวัตถุประสงค์และระยะเวลาในการใช้ข้อมูลส่วนบุคคล (Purpose Specification Principle)

หลักการดังกล่าวกำหนดให้ต้องมีการระบุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลก่อนหรือในขณะที่ทำการประมวลผลข้อมูลส่วนบุคคล การประมวลผลข้อมูลส่วน บุคคลภายหลังสามารถกระทำได้หากเป็นเพียงเพื่อให้สำเร็จตามวัตถุประสงค์ หรือเพื่อการอื่นที่ไม่ขัดหรือแย้งกับวัตถุประสงค์ที่ได้แจ้งไว้ อย่างไรก็ตามหากมีการเปลี่ยนแปลงวัตถุประสงค์ ผู้ควบคุมข้อมูลส่วนบุคคลต้องระบุวัตถุประสงค์การใช้ที่เปลี่ยนแปลงไปนั้นทุกคราวด้วย นอกจากนี้ การเก็บและใช้ข้อมูลส่วนบุคคลนั้นต้องไม่เกินกว่าระยะเวลาที่จำเป็นเพื่อให้วัตถุประสงค์ที่ได้แจ้งไว้สำเร็จลุล่วง[34]

4) หลักการใช้ข้อมูลส่วนบุคคลอย่างจำกัด (Use Limitation Principle)

หลักการดังกล่าวห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยทำให้สามารถเข้าถึงได้หรือนำข้อมูลส่วนบุคคลไปใช้เพื่อการอย่างอื่นนอกจากจากวัตถุประสงค์อื่นซึ่งไม่ขัดหรือแย้งกับวัตถุประสงค์ที่ได้แจ้งไว้ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นการใช้อำนาจตามบทบัญญัติของกฎหมายเพื่อความมั่นคงของประเทศ ความสงบเรียบร้อยของสังคม ประโยชน์สาธารณะ เพื่อการปฏิบัติตามกฎหมาย หรือเพื่อประโยชน์มหาชนอื่นๆ

นอกจากนี้ ยังกำหนดให้บุคคลใดซึ่งมิใช่ผู้จัดเก็บข้อมูลส่วนบุคคลจะนำข้อมูลส่วนบุคคลนั้นไปเปิดเผยโดยเจ้าของมิได้ยินยอมมิได้ แม้ทั้งการเปิดเผยนั้นจะมิได้ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลเลยก็ตาม นอกจากนี้เมื่อเจ้าของข้อมูลส่วนบุคคลอนุญาตให้มีการเปิดเผยแล้ว เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเพิกถอนความยินยอมเพื่อยุติการเผยแพร่ข้อมูลส่วนบุคคลนั้นได้ตลอดเวลา[35]

5) หลักการป้องกันรักษาความปลอดภัยของข้อมูลส่วนบุคคล (Security Safeguard Principle)

หลักการนี้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีระบบการป้องกันรักษาความปลอดภัยของข้อมูลเพื่อมิให้ข้อมูลส่วนบุคคลนั้นสูญหาย ถูกเข้าถึง ถูกทำลาย มีการใช้หรือเปลี่ยนแปลงแก้ไข หรือมีการเปิดเผยข้อมูลโดยบุคคลซึ่งปราศจากอำนาจ

6) หลักเปิดเผยโปร่งใส (Openness Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องประกาศนโยบายในการประมวลผลข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อให้ผู้ที่เกี่ยวข้องทราบถึงการจัดเก็บหรือการ

---

[34] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

[35] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

รวบรวมข้อมูลส่วนบุคคล หรือการนำข้อมูลส่วนบุคคลนั้นไปใช้ ระบบการประมวลผลข้อมูลส่วนบุคคล ต้องสามารถแสดงให้เห็นถึงความมีอยู่และประเภทของข้อมูลส่วนบุคคล วัตถุประสงค์ของการใช้ข้อมูลส่วนบุคคล รวมทั้งชื่อและสถานที่ตั้งของนายทะเบียนผู้ทำหน้าที่ในการประมวลผลข้อมูลส่วนบุคคล

7) หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)

หลักการดังกล่าวกำหนดสิทธิให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นปัจเจกบุคคล ดังต่อไปนี้[36]

(1) ได้รับแจ้งหรือยืนยันจากนายทะเบียนว่าได้ทำการประมวลผล ใช้ หรือโอนข้อมูลส่วนบุคคลของตนหรือไม่

(2) ได้รับการติดต่อจากนายทะเบียนเกี่ยวกับข้อมูลส่วนบุคคลของตน

(2.1) ภายในเวลาอันสมควร

(2.2) อาจมีค่าใช้จ่ายได้แต่ต้องไม่เกินสมควร

(2.3) โดยวิธีที่เหมาะสม

(2.4) โดยรูปแบบที่เจ้าของข้อมูลส่วนบุคคลสามารถเข้าใจได้

(3) ได้รับเหตุผลเมื่อคำร้องตามข้อ 1) และ 2) ถูกปฏิเสธ และมีสิทธิในการอุทธรณ์การปฏิเสธนั้น

(4) คัดค้านการประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับตน และหากการโต้แย้งนั้นรับฟังได้มีสิทธิขอให้ลบหรือทำลายข้อมูลส่วนบุคคล ปรับปรุงหรือแก้ไขเพิ่มเติมเพื่อให้ข้อมูลส่วนบุคคลนั้นถูกต้องและสมบูรณ์

8) หลักข้อจำกัดในการส่งหรือโอนข้อมูลส่วนบุคคลให้แก่บุคคลอื่นข้ามพรมแดน (Restriction on Onward Opposition)

หลักการดังกล่าวมีวัตถุประสงค์เพื่อป้องกันมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับที่อยู่ในประเทศซึ่งปราศจากกฎหมายและวิธีปฏิบัติที่สามารถเป็นหลักประกันการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือมีสัญญาส่งโอนข้อมูลส่วนบุคคลระหว่างกันที่ให้หลักประกันอย่างเพียงพอ[37]

9) หลักความรับผิดชอบของนายทะเบียน (Accountability Principle)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักการที่ 1 ถึง 8 อย่างเคร่งครัด หากฝ่าฝืนหลักการดังกล่าวและก่อให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย ควบคุม ข้อมูลส่วนบุคคล

---

[36] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

[37] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

ต้องรับผิดทั้งในทางแพ่งและทางอาญา และรับผิดในค่าใช้จ่ายเพื่อแก้ไขข้อมูลส่วน บุคคลให้ถูกต้อง รวมไปถึงต้องลบหรือทำลายข้อมูลส่วนบุคคลอีกด้วย[38]

2.6 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และการละเมิดข้อมูลส่วนบุคคลพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ควบคุมการเก็บ รวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามบทบัญญัติ เช่น การนำข้อมูลที่ได้เก็บรวบรวมไว้ไปใช้ผิดจากวัตถุประสงค์ที่ได้รับความยินยอมโดยการนำไปหาประโยชน์ทางการตลาด หรือ การนำไปขายเพื่อประโยชน์ทางธุรกิจ หรือเกิดการละเมิดข้อมูลส่วนบุคคล ย่อมเป็นเหตุให้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลเกิดความรับผิด ซึ่งการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในส่วนของการละเมิดข้อมูลส่วนบุคคล เป็นความผิดที่มีโทษสูงและก่อความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลได้มากหากเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้อธิบายความหมายของการละเมิดข้อมูลส่วนบุคคลเอาไว้โดยเฉพาะ คำอธิบายที่มีอยู่ในกฎหมายต่างประเทศโดยผู้วิจัยยกตัวอย่างจากคำนิยามในกฎหมาย General Date Protection Regulation (GDPR) ของสหภาพยุโรป มาตรา 4 (12) “การละเมิดข้อมูลส่วนบุคคล หมายถึงการละเมิดความปลอดภัยที่นำไปสู่การทำลาย สูญเสีย เปลี่ยนแปลง เปิดเผยโดยไม่ได้รับอนุญาต หรือการเข้าถึงข้อมูลส่วนบุคคลที่ถูกส่ง เก็บรักษา หรือประมวลผล โดยอุบัติเหตุหรือไม่ชอบด้วยกฎหมาย” ศึกษาเทียบเคียงเพราะกฎหมาย GDPR ของสหภาพยุโรปเป็นกฎหมายที่มีความเข้มงวดด้านความเป็นส่วนตัวและมีความปลอดภัยมากที่สุดของโลก การละเมิดข้อมูลส่วนบุคคล อาจเกิดจากการกระทำของบุคคลภายนอก เช่น การขโมยอัตลักษณ์เพื่อการนำไปสวมรอย (identity theft) การลักขโมยอุปกรณ์คอมพิวเตอร์ที่มีข้อมูลส่วนบุคคล เป็นต้น รวมทั้งอาจเกิดจากการกระทำ หรือละเว้นกระทำการของผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วน

[38] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

บุคคลก็ได้ เช่น การส่งข้อมูลส่วนบุคคลผิดตัว ผู้รับการเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต[39]

นอกจากนี้ บทบัญญัติในพระราชบัญญัตินี้ยังกำหนดหน้าที่บางประการแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล เช่น หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลอันเป็นการกำหนดมาตรการเชิงป้องกัน และ หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการบันทึกรายการเพื่อการตรวจสอบ เป็นต้น หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลหากมีการฝ่าฝืนบทบัญญัติจนเป็นเหตุให้เจ้าของข้อมูลได้รับความเสียหาย ก็ถือเป็นการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับผิดมาตรการเชิงป้องกัน การกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า เพราะการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบย่อมเกิดค่าใช้จ่ายแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล[40]

อีกทั้ง การบอกกล่าวการเกิดเหตุละเมิดแก่เจ้าของข้อมูลส่วนบุคคล และการบอกกล่าวการเกิดเหตุละเมิดสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งค่าใช้จ่ายเพื่อการเฝ้าระวัง การเยียวยาแก้ไขการละเมิดข้อมูลส่วนบุคคล ย่อมเกิดเป็นความเสียหายทางการเงินแก่ผู้ประกอบการ และหากไม่ได้รับการเยียวยาก็จะกระทบสิทธิของเจ้าของข้อมูลส่วนบุคคลก็คือประชาชน[41]

---

[39] ปัทมา มัญชุนากร. (2564). ***ปัญหากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในเครือข่ายสังคมออนไลน์: ศึกษา กรณีผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์.

[40] จีระศักดิ์ เสมมีสุข. (2564). การประกันภัยความรับผิดทางไซเบอร์: ศึกษาความคุ้มครองกรณีการละเมิดข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารบัณฑิตศึกษานิติศาสตร์,*** 14(3). หน้า 348-366.

[41] เรื่องเดียวกัน, หน้า 348-366.

2.6.1 ความหมายของเหตุละเมิดข้อมูลส่วนบุคคลการละเมิดตามกฎหมายประมวลกฎหมายแพ่งและพาณิชย์

ละเมิด คือ การกระทำโดยจงใจหรือประมาทเลินเล่อต่อ บุคคลภายนอกโดยผิดกฎหมาย เป็นเหตุให้เขา (ผู้ถูกกระทำ) เสียหายแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดีทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดีกฎหมายถือว่าผู้นั้นทำละเมิดจะต้องรับผิดชอบชดใช้ค่าสินไหมทดแทนเพื่อการละเมิดนั้น ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420[42]

สรุปการกระทำใดจะเป็นละเมิดต้องประกอบด้วย หลัก 3 ประการ

1) กระทำต่อบุคคลอื่นโดยผิดกฎหมาย ซึ่งหมายถึงการประทุษกรรม กระทำต่อบุคคลโดยผิดกฎหมายด้วยอาการฝ่าฝืนต่อความหมายที่ห้ามไว้หรือละเว้นไม่กระทำในสิ่งที่กฎหมายบัญญัติให้กระทำหรือตนมีหน้าที่ตามกฎหมายจะต้องกระทำโดยจงใจหรือประมาทเลินเล่อ เป็นต้น ว่า ฆ่าเขาตายทำร้าย ร่างกายเขา ขับรถโดยประมาทชนคนตายและทรัพย์สินของเขาเสียหาย ฯลฯ

2) กระทำโดยจงใจหรือประมาทเลินเล่อ กระทำโดยจงใจ คือ การะทำโดยรู้สำนึกและในขณะเดียวกัน ก็รู้ว่าจะทำให้เขาเสียหาย เช่น เจตนาฆ่าหรือเจตนาทำร้าย ฯลฯ อย่างไร ก็ดีการกระทำโดยจงใจในเรื่องละเมิดถือหลักเบาบางกว่าทางอาญา สำหรับอาญานั้น ต้องกระทำโดยรู้สึกสำนึกในการที่ทำและในขณะเดียวกันผู้กระทำต้องประสงค์ต่อผลหรือย่อมเล็งเห็นผลด้วย ส่วนจงใจในเรื่องละเมิดบางกรณีไม่ผิดในทางอาญาแต่เป็นละเมิดต้องชดใช้ค่าเสียหายให้แก่เขา เช่น จำเลยรื้อห้องน้ำห้องครัวซึ่งโจทย์ปลูกล้ำออกไปนอกที่เช่าของวัดโดยวัดต้องการจะขุดคูได้บอกให้โจทย์รื้อแล้ว โจทย์ไม่ยอมรื้อการที่จำเลยรื้อแล้วกองไว้หลังบ้านโจทย์มิได้เจตนาชั่วร้ายทำให้ทรัพย์ของโจทย์อันตรายเสียหายไม่เป็นความผิดฐานทำให้เสียทรัพย์แต่เป็นละเมิด เพราะรู้ว่าแล้วว่าการรื้อนั้นจะทำให้ทรัพย์ของโจทย์ เสียหาย (ฎีกาที่ 1617-1618/2500)

คำว่าประมาทเลินเล่อในทางแพ่ง หมายความถึง การกระทำที่ขาดความ ระมัดระวังจนเป็นเหตุให้เกิดความเสียหายนั้นและหมายความถึงการไม่ป้องกัน ผลที่เกิดขึ้นโดยประมาทเลินเล่อแม้ตนเองไม่ได้กระทำให้เกิดผลนั้นขึ้นระดับความระมัดระวังของบุคคลต้องถือระดับบุคคลธรรมดา ตัวอย่าง เช่น นาย ก. ขับรถยนต์ไปในถนนที่มีคนเดินจอแจด้วย ความเร็วและไม่ได้ให้สัญญาณแตรแล้วเฉี่ยวชนถูกคนเดินถนนได้รับบาดเจ็บ ดังนี้ ถือว่า นาย ก. กระทำละเมิดโดยประมาทเลินเล่อ

3) ทำให้บุคคลอื่นเสียหาย โดยปกติผู้กระทำต้องรับผิดเฉพาะการกระทำของตนแต่อย่างไรก็ดี ในเรื่องละเมิดถ้าได้มีการกระทำละเมิดร่วมกันหรือแม้มิได้ร่วมแต่เป็นผู้ยุยง ส่งเสริม

---

[42] ประมาลกฎหมายแพ่งและพาณิชย์.มาตรา420.

หรือช่วยเหลือในการกระทำละเมิดดังนี้บุคคลเหล่านี้จะต้องร่วมกัน รับผิดใช้ค่าสินไหมทดแทนความเสียหายนั้น ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 432[43]

พระราชบัญญัติว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539

การละเมิดตามพระราชบัญญัติว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539[44] เป็นกฎหมายที่ออกมาใช้บังคับด้วยเหตุผลว่า การปฏิบัติงานของเจ้าหน้าที่มิได้เป็นไปเพื่อประโยชน์เฉพาะตัว ในการดำเนินงานบางครั้งอาจเกิดความเสียหายขึ้นโดยความไม่ตั้งใจและผิดพลาดเล็กน้อยแต่กลับต้องรับผิดเป็นการเฉพาะตัว และที่ผ่านมายังใช้หลักของลูกหนี้ร่วมทำให้เจ้าหน้าที่ต้องร่วมรับผิดในการกระทำของผู้อื่น ด้วยซึ่งเป็นระบบที่มุ่งจะให้ได้รับเงินชดใช้ค่าเสียอย่างครบถ้วนโดยไม่คำนึงถึงความเป็นธรรมที่จะมีต่อแต่ละคน จึงก่อให้เกิดความไม่เป็นธรรม และยังเป็นการบั่นทอนขวัญกำลังใจของเจ้าหน้าที่จนบางครั้งเป็นปัญหาในการบริหารงานเพราะเจ้าหน้าที่ไม่กล้าตัดสินใจในการทำงานเท่าที่ควร ดังนั้น กฎหมายฉบับนี้จึงสมควรให้เจ้าหน้าที่รับผิดทางละเมิดในการปฏิบัติหน้าที่เฉพาะเมื่อเป็นการจงใจให้เกิดความเสียหายหรือประมาทเลินเล่ออย่างร้ายแรงเท่านั้น และให้แบ่งแยกความรับผิดของแต่ละคน ทั้งนี้ เพื่อให้เกิดความเป็นธรรมและเพิ่มพูนประสิทธิภาพในการปฏิบัติงานของรัฐ

ดังนั้น การปฏิบัติงานของเจ้าหน้าที่ในหน้าที่ของตนนั้นหากเกิดความเสียหายขึ้น เจ้าหน้าที่ผู้ปฏิบัติงานได้รับการคุ้ม ครองตามกฎหมาย คือ พระราชบัญญัติความรับผิดทาง ละเมิดของเจ้าหน้าที่ พ.ศ. 2539 แต่ความเสียหายที่เกิดขึ้นจากการปฏิบัติหน้าทีนั้นต้องไม่ได้ เกิดจากความจงใจหรือประมาทเลินเล่ออย่างร้ายแรง ของเจ้าหน้าที่ การที่มีกฎหมายให้ค วามคุ้มครองแก่เจ้าหน้าที่ผู้ปฏิบัติงานตามหน้าที่ดังกล่าวนั้นเนื่องจากในการปฏิบัติหน้าที่ราชการ บางกรณีอาจมีโอกาสเสี่ยงที่จะเกิดความผิดพลาดหรือเป็นเหตุสุดวิสัยโดยมิได้เกิดจากความ จงใจหรือประมาทเลินเล่ออย่างร้ายแรงส่งผลให้เกิดความเสียหายพระราชบัญญัติความรับผิด ทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539 จึงบัญญัติคุ้มครองการปฏิบัติหน้าที่ของเจ้าหน้าที่ไว้ ดังนี้

มาตรา 5 วรรคหนึ่ง[45] “หน่วยงานของรัฐต้องรับผิดต่อผู้เสียหายในผลแห่งละเมิดที่เจ้าหน้าที่ของตนได้กระทำในการปฏิบัติหน้าที่ในกรณีนี้ผู้เสียหายอาจฟ้องหน่วยงานของรัฐดังกล่าวได้โดยตรงแต่จะฟ้องเจ้าหน้าที่ไม่ได้”

---

[43] ประมาลกฎหมายแพ่งและพาณิชย์.มาตรา 432.

[44] พระราชบัญญัติว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539.

[45] พระราชบัญญัติความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539. มาตรา 5.

แต่หากเจ้าหน้าที่กระทำการนอกเหนือหรือไม่ได้ปฏิบัติงานในหน้าที่ปกติของตน เช่น เจ้าพนักงานการเงิน ไม่ได้มีหน้าที่ในการขับรถ แต่ได้ขับรถไปซึ่งมิใช่หน้าที่ของตน แล้วเกิดเฉี่ยวชนกับคุคลภายนอกได้รับความเสียหายเป็นต้นย่อมไม่ได้รับการคุ้มครองตามกฎหมาย

มาตรา 6 [46]บัญญัติว่า“ถ้าการกระทาละเมิดของเจ้าหน้าที่มิใช่การกระทาในการปฏิบัติหน้าที่ เจ้าหน้าที่ต้องรับผิดในการนั้น เป็นการเฉพาะตัว ในกรณีนี้ผู้เสียหายอาจฟ้องเจ้าหน้าที่ ได้โดยตรง แต่จะฟ้องหน่วยงานรัฐไม่ได้”

จะเห็นได้ว่าหากเจ้าหน้าที่ปฏิบัติหน้าที่อื่นนอกเหนือหน้าที่ของตนตามที่กฎ ระเบียบกำหนดไว้แล้วรัฐไม่คุ้มครองแต่ถ้าได้ปฏิบัติงานในหน้าที่ของตนโดยชอบแล้วเมื่อเกิดความผิดพลาดไม่ว่าบุคคลใดได้รับความเสียหายหรือทำให้รัฐเองเสียหายก็ตาม หน่วยงานของรัฐ จะต้องเข้ารับผิดชดใช้ค่าเสียหายแทนเจ้าหน้าที่ แต่ก็ต้องพิจารณาต่อไปว่า ความผิดพลาดที่เกิดขึ้นเนื่องมาจากการจงใจหรือประมาทเลินเล่ออย่างร้ายแรงของเจ้าหน้าที่หรือไม่ ตามความที่บัญญัติไว้ใน มาตรา 8 วรรคหนึ่ง ในกรณีที่หน่วยงานของรัฐต้องรับผิดใช้ค่าสินไหมทดแทนแก่ผู้เสียหาย เพื่อการละเมิดของเจ้าหน้าที่ ให้หน่วยงานของรัฐมีสิทธิเรียกให้เจ้าหน้าที่ผู้ทำละเมิดชดใช้ค่า สินไหมทดแทนดังกล่าวแก่หน่วยงานของรัฐได้ ถ้าเจ้าหน้าที่ได้กระทำการอันเป็นไปด้วยความจงใจ หรือประมาทเลินเล่ออย่างร้ายแรง

กรณีจะเป็นประมาทเลินเล่ออย่างร้ายแรงจะต้องเป็นประมาทเลินเล่อเสียก่อนโดย“จะเป็นส่วนที่อยู่กึ่งกลางระหว่างจงใจกับประมาทเลินเล่อธรรมดา” คณะกรรมการกฤษฎีกาเคยตอบข้อหารือกรมบัญชีกลางว่า การที่จะพิจารณาว่ากรณีใดจะเป็นการกระทำด้วยความประมาทเลินเล่ออย่างร้ายแรงของเจ้าหน้าที่หรือไม่นั้น เป็นหน้าที่ของเจ้าหน้าที่ผู้มีอำนาจดำเนินการตามกฎหมายและระเบียบทุกคน จนถึงคณะกรรมการวินิจฉัยร้องทุกข์หรือศาล ส่วนอย่างไรเป็นการประมาทเลินเล่ออย่างร้ายแรงย่อมขึ้นอยู่กับข้อเท็จจริงแต่ละกรณีไปความประมาทเลินเล่ออย่างร้ายแรงจะมีลักษณะไปในทางที่บุคคลนั้นได้กระทำไปโดยขาดความระมัดระวังที่เบี่ยงเบนไปจากเกณฑ์มาตรฐานอย่างมาก เช่น คาดเห็นได้ว่าความเสียหายอาจเกิดขึ้นได้หรือหากใช้ความระมัดระวังสักเล็กน้อย ก็คงได้คาดเห็นการอาจเกิดความเสียหายนั้นนั้นเอง[47]

การละเมิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ตามแนวทางของ General data Protection Regulation (GDPR) เหตุละเมิดข้อมูลส่วนบุคคล มีความหมายดังต่อไปนี้

---

[46] พระราชบัญญัติความรับผิด ทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539. มาตรา 6.

[47] กองกฎหมาย กรมทรัพยากรทางทะเลและชายฝั่ง. ***หลักการกระทำละเมิด ประมวลกฎหมายแพ่งและพาณิชย์.*** (ออนไลน์). เข้าถึงได้จาก: https://dmcrth.dmcr.go.th/lag/detail/1110/

“เหตุการละเมิดข้อมูลส่วนบุคคล” หมายถึง การละเมิดหรือฝ่าฝืนมาตรการความปลอดภัยที่นำไปสู่การทำลายโดยบังเอิญหรือไม่ชอบด้วยกฎหมาย ความเสียหาย การเปลี่ยนแปลง การเปิดเผยโดยไม่มีอำนาจ หรือการเข้าถึง ซึ่งข้อมูลส่วนบุคคลที่มีการส่ง เก็บรักษา หรือประมวลผล

ในส่วนของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37[48] บัญญัติว่า ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ดังนี้ มาตรา 37 (4) “แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมี ความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคล ทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด”

หน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว มีประเด็นที่ต้องพิจารณาทางกฎหมายหลายประการ โดยเฉพาะการเริ่มนับระยะเวลา 72 ชั่วโมงว่าเริ่มเมื่อไหร่ เนื่องจากองค์กรอาจมีความรับผิดทางกฎหมายหากไม่แจ้งภายในระยะเวลาที่กฎหมายกำหนด

2.6.2 หลักการทั่วไปของการแจ้งเหตุละเมิด

หลักการกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุข้อมูลรั่วไหล หรือถูกล่วงละเมิด (Data Breach Notification) โดยแยกเป็น 2 กรณี ดังนี้

1) การแจ้งต่อหน่วยงานกำกับ เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หลักการนี้ปรากฏในกฎหมายสหภาพยุโรปมาตรา 33 (Notification of a personal data breach to the supervisory authority) และการแจ้งเหตุข้อมูลรั่วไหลหรือล่วงละเมิดต่อเจ้าของข้อมูล หลักการนี้ปรากฏในกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรปมาตรา 34 (Communication of a personal data breach to the data subject)

2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (2)[49] ซึ่งจำแนกเป็นการแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและการแจ้งต่อเจ้าของข้อมูล หลักการนี้ส่งผลให้เกิดภาระต้นทุนการทำให้สอดคล้องกับกฎหมาย เช่น ก่อนการแจ้งต้องมีการประเมินสถานการณ์ตรวจสอบข้อเท็จจริงและหลักฐานทางอิเล็กทรอนิกส์ (Forensic) ซึ่งต้องอาศัยงบประมาณและ

[48] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

[49] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

การจ้างผู้เชี่ยวชาญ รวมทั้งต้นทุนในการปฏิบัติการส่งข้อมูลการแจ้งต่าง ๆ[50] และมาตรา 37 (4)[51] "แจ้งเหตุการ ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำ ได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมี ความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคล ทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์ และวิธีการที่คณะกรรมการประกาศกำหนด"[52]

ถ้อยคำหนึ่งในมาตรา 37 (4)[53] ที่เป็นจุดเริ่มต้นสำคัญของการเริ่มนับระยะเวลา คือ "นับแต่ทราบเหตุ" (become aware) ซึ่งต้องทำความเข้าใจทั้งข้อเท็จจริงและข้อกฎหมายประกอบกัน เพื่อทำความเข้าใจจุดเริ่มต้นการนับระยะเวลาดังกล่าวมากขึ้น

ตาม GDPR "นับแต่ทราบเหตุ" ให้เริ่มต้นเมื่อ "ผู้ควบคุมข้อมูลส่วนบุคคล" มีความแน่ใจในว่าเหตุการณ์ข้อมูลรั่วไหลที่เกิดขึ้น (security incident) มีผลทำให้ข้อมูลส่วนบุคคลถูกละเมิด

ในกรณีนี้ต้องทำความเข้าใจก่อนว่าตามแนวทางของ GDPR นั้นไม่ใช่ภัยคุกคามทางไซเบอร์ทุกปะเภทหรือเหตุการณ์ข้อมูลรั่วไหลทุกประเภทจะเข้าเงื่อนไขของ "Data Breach" หรือที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ เรียกว่า "เหตุการละเมิดข้อมูลส่วนบุคคล"

ดังนั้น สิ่งแรกที่องค์กรต้องทำการประเมินก่อน คือ ผลของเหตุการณ์ข้อมูลรั่วไหลนั้นได้ส่งผลกระทบต่อความเสี่ยง หรือความไม่มั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือไม่

วินาทีที่มี "reasonable degree of certainty" คือ จุดเริ่มต้นนับหนึ่งของระยะเวลา ที่ต้องแจ้งอย่างช้าภายใน 72 ชั่วโมงตามเงื่อนไขที่ GDPR กำหนดหากเหตุการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

ดังนั้น กระบวนการตรวจสอบเหตุการณ์ข้อมูลรั่วไหลเบื้องต้น ที่สามารถนำไปสู่ระดับความแน่นอนพอสมควร (reasonable degree of certainty) ว่าข้อมูลส่วนบุคคลได้ถูกทำให้สูญเสียการเป็นความลับ ความถูกต้อง หรือความพร้อมใช้งาน (Security Triad: loss of

---

[50] คณาธิป ทองรวีวงศ์. (2564). ผลกระทบทางลบอันเกิดจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรปและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารรัชต์ภาคย์,*** 15(38). หน้า 42-56.

[51] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

[52] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 34.

[53] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

confidentiality, integrity and/or availability) จึงเป็นเงื่อนไขบังคับก่อนที่สำคัญของการเริ่มต้นนับระยะเวลา

นอกจากนี้ องค์กรยังมีหน้าที่ต้องจัดให้มีมาตรการเชิงเทคนิคและเชิงองค์กรเพื่อให้มั่นใจว่าองค์กรจะสามารถ "ทราบเหตุ"ได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถดำเนินการตามขั้นตอนต่าง ๆ ที่กฎหมายกำหนดอีกด้วย

ทั้งนี้เพื่อป้องกันมิให้องค์กรใช้เป็นข้ออ้างได้ว่า "ไม่สามารถตรวจพบหรือทราบเหตุ" เพราะเมื่อกฎหมายบังคับให้ต้องมีมาตรการที่เหมาะสมแล้ว โดยผลของการจัดให้มีมาตรการดังกล่าว องค์กรจึงมีหน้าที่ต้องรู้หรือควรรู้ว่าเกิดเหตุการละเมิดข้อมูลส่วนบุคคลภายในระยะเวลาที่เหมาะสมอีกด้วย

การพิจารณา "นับแต่ทราบเหตุ" ก็ยังคงเป็นข้อเท็จจริงที่ต้องพิจารณาเป็นรายกรณีไป ในบางกรณีก็อาจจะใช้เวลาพอสมควรเพื่อให้สามารถแน่ใจ (degree of certainty) ว่าเหตุการณ์ข้อมูลรั่วไหล (security incident) หรือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลด้วย ซึ่งมียกตัวอย่างกรณีศึกษาของการพิจารณาไว้ดังนี้[54]

ตัวอย่างที่ 1 กรณี USB key สูญหาย

กรณีที่ USB key ที่ถูกเข้ารหัสไว้สูญหาย กรณีนี้ย่อมมีความไม่แน่นอนว่าผู้ที่ได้ไปจะสามารถเข้าถึงข้อมูลส่วนบุคคลใน USB key หรือไม่และข้อมูลจะสูญเสียการเป็นความลับหรือไม่ (confidentiality breach) แต่ในกรณีนี้ย่อมเป็นที่แน่นอนว่าองค์กรได้สูญเสียความสามารถในการเข้าถึงข้อมูลหรือความพร้อมใช้ของข้อมูลไปแล้ว (availability breach) "นับแต่ทราบเหตุ" จึงเริ่มต้นตั้งแต่องค์กรรู้ว่า USB key ได้หายไป

ตัวอย่างที่ 2 ข้อมูลถูกเปิดเผยไปยังบุคคลภายนอก

มีบุคคลภายนอกได้แจ้งให้องค์กรทราบว่าเขาได้รับข้อมูลส่วนบุคคลของลูกค้าขององค์กรโดยอาจจะเกิดจากการส่งอีเมลผิดหรือจดหมายผิด และบุคคลภายนอกนั้นได้แสดงหลักฐานให้เห็นว่าเขาได้รับข้อมูลมาโดยไม่ถูกต้อง กรณีนี้ต้องถือว่าเกิดการสูญเสียการเป็นความลับของข้อมูลส่วนบุคคลขึ้นแล้ว (confidentiality breach) "นับแต่ทราบเหตุ" [55]จึงเริ่มต้นตั้งแต่องค์กรได้รับทราบหลักฐานของการเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

ตัวอย่างที่ 3 เครือข่ายถูกโจมตีหรือถูกเข้าถึง

---

[54] คณาธิป ทองรวีวงศ์. อ้างแล้วเชิงอรรถที่ 50. หน้า 42-56.

[55] ศุภวัชร์ มาลานนท์. (2565).***การเริ่มนับระยะเวลา แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/columnist/992923 [2566, 27 มิถุนายน]

ในกรณีที่มีตรวจพบว่าอาจจะมีการเข้าถึงเครือข่ายขององค์กร โดยไม่ชอบด้วยกฎหมาย และองค์กรได้ตรวจสอบระบบแล้วพบว่ามีการเข้าถึงโดยไม่ชอบด้วยกฎหมายดังกล่าวได้ส่งผลกระทบต่อข้อมูลส่วนบุคคลในองค์กร "นับแต่ทราบเหตุ" จึงเริ่มต้นตั้งแต่องค์กรสามารถยืนยันว่าข้อมูลส่วนบุคคลได้รับผลกระทบ

ตัวอย่างที่ 4 อาชญากรรมทางคอมพิวเตอร์/การเรียกค่าไถ่

องค์กรถูกเรียกค่าไถ่จากแฮกเกอร์เพื่อแลกกับการไม่เผยแพร่ข้อมูลออกสู่สาธารณะ องค์กรจึงเร่งตรวจสอบระบบของตนเองว่าถูกละเมิดหรือโจมตีโดยบุคคลภายนอกหรือไม่ ข้อเท็จจริงจากการตรวจสอบยืนยันว่ามีการถูกเข้ารหัสข้อมูลโดยบุคคลภายนอกจริง "นับแต่ทราบเหตุ" จึงเริ่มต้นตั้งแต่องค์กรสามารถยืนยันว่าระบบของตนเองถูกโจมตีและมีข้อมูลส่วนบุคคลได้รับผลกระทบ

ตัวอย่างที่ 5 เหตุการละเมิดเกิดจาก "ผู้ประมวลผลข้อมูลส่วนบุคคล"

หน้าที่ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อหน่วยงานบังคับใช้กฎหมายเป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ส่วน "ผู้ประมวลผลข้อมูลส่วนบุคคล" มีหน้าที่แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นเท่านั้น[56]

ใน GDPR ไม่ได้ระบุชัดเจนว่า "นับแต่ทราบเหตุ" จะเริ่มจากการที่ "ผู้ประมวลผลข้อมูลส่วนบุคคล" ทราบเหตุหรือจากการที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งจากผู้ประมวลผลข้อมูลส่วนบุคคล แต่ข้อตกลงในสัญญาระหว่างกัน (Data Processing Agreement) ต้องกำหนดหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้ชัดเจนว่าต้องดำเนินการอย่างไรบ้างเพื่อสนับสนุนและให้ความร่วมมือกับองค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคลขึ้น

ซึ่งเงื่อนไขหนึ่งของหน้าที่ "แจ้ง" ที่กล่าวมาทั้งหมด เป็นเหตุการละเมิดข้อมูลส่วนบุคคลในส่วนของเงื่อนไขการเริ่มนับระยะเวลา 72 ชั่วโมงเท่านั้น การที่ต้องแจ้งหรือไม่ต้องแจ้งและต้องแจ้งใครบ้าง วิธีการแจ้งและมาตรการต่างๆ ที่ต้องดำเนินการเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล ยังมีรายละเอียดที่ต้องพิจารณา จากการประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลประกอบอีกด้วย[57]

2.6.3 ตัวอย่างการละเมิดข้อมูลส่วนบุคคล

กรณีศึกษาที่ 1: การเกิดเหตุละเมิดข้อมูลส่วนบุคคลของ Anthem, Inc. ในปีพ.ศ. 255

---

[56] ปัทมา มัญชุนากร. อ้างแล้วเชิงอรรถที่ 39. หน้า 1.

[57] ศุภวัชร์ มาลานนท์. (2565). ***การเริ่มนับระยะเวลาแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/columnist/992923 [2566, 27 มิถุนายน]

ข้อเท็จจริง

ในปี พ.ศ. 2558 Anthem, Inc. ซึ่งเป็นบริษัทประกันภัยรายใหญ่ของสหรัฐอเมริกาได้ประกาศว่าข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของบริษัทได้ถูกละเมิดไปราว 3.7 ล้านชุดข้อมูล และเป็นข้อมูลส่วนบุคคลของชาวอเมริกันมากกว่า 80 ล้านคน ซึ่งการละเมิดข้อมูลส่วนบุคคลดังกล่าวเกิดขึ้นเนื่องจากถูกแฮกเกอร์ (Hacker) นำข้อมูลส่วนบุคคลไป โดยการละเมิดข้อมูลส่วนบุคคลดังกล่าวนั้นมิได้เกิดขึ้นเพียงครั้งเดียว แต่เกิดขึ้นเรื่อย ๆ ระหว่างช่วงเดือนธันวาคม พ.ศ. 2557 จนถึงเดือนกุมภาพันธ์ พ.ศ. 2558 โดยข้อมูลส่วนบุคคลที่ถูกละเมิดไปนั้นประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่ อีเมล หมายเลขประกันสังคม วันเกิด หมายเลขสมาชิกประกันภัย หมายเลขผู้ป่วย ข้อมูลพนักงาน และรายได้ของบริษัท ซึ่งจากการตรวจสอบพบว่าโดยมากข้อมูลส่วนบุคคลที่ถูกละเมิดไปนั้นได้ถูกนำไปขายต่อให้กับตลาดมืด และไม่ได้มีการนำข้อมูลจำพวกประวัติสุขภาพไปใช้

นอกจากนั้นจากการตรวจสอบยังพบว่าการเกิดเหตุละเมิดนั้นอาจเป็นเพราะว่า Athem, Inc. ไม่ได้มีระบบรักษาความปลอดภัยที่เพียงพอ กล่าวคือ Athem, Inc. ไม่ได้มีมาตรการในการเข้ารหัสข้อมูล (Encryption) ที่มีการจัดเก็บซึ่งอาจทำให้ Hacker สามารถทำลายระบบรักษาความปลอดภัยของข้อมูลส่วนบุคคล และเข้าถึงข้อมูลส่วนบุคคลได้โดยง่าย

บทวิเคราะห์

จากกรณีข้างต้นทำให้เห็นว่าการจัดการเกี่ยวกับระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นเรื่องสำคัญอย่างยิ่งสำหรับผู้ควบคุมข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งผู้ควบคุมข้อมูลส่วนบุคคลที่มีการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว ดังเช่นบริษัทประกันวินาศภัย และบริษัทประกันชีวิต เนื่องจากข้อมูลส่วนบุคคลเหล่านั้นสามารถทำให้เกิดความเสียหาย หรือเกิดผลกระทบกับสิทธิและเสรีภาพของบุคคลได้ง่าย

การเข้ารหัสข้อมูล (Encryption) เป็นวิธีหนึ่งที่จะช่วยให้บริษัทฯ สามารถจัดการกับข้อมูลส่วนบุคคล และป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบได้

ในกรณีนี้ Athem, Inc. ได้มีขั้นตอนการดำเนินการจัดการ และแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่รวดเร็ว และน่านำไปเป็นแบบอย่าง ตามที่เจ้าหน้าที่ FBI ได้กล่าวให้สัมภาษณ์ไว้ โดยเมื่อพนักงานของ Athem, Inc. พบข้อสงสัยเกี่ยวกับฐานข้อมูลของบริษัท บริษัทก็เริ่มดำเนินการตรวจสอบทันที และเมื่อบริษัทหาสาเหตุ และรายละเอียดเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลได้แล้ว บริษัทก็ดำเนินการแจ้ง FBI ของสหรัฐอเมริกา พร้อมทั้งส่งจดหมายแจ้งเจ้าของข้อมูลส่วนบุคคลที่อาจได้รับผลกระทบทันที โดยในการแจ้งรายละเอียดเรื่องการละเมิดข้อมูลส่วนบุคคลนั้นบริษัทได้มีการแจ้งไปถึงประเภทข้อมูลส่วนบุคคลที่ถูกขโมยไป และหลังจากนั้น Athem, Inc. ก็ได้

จ้างบริษัทจัดการด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศหลายรายให้เข้าร่วมจัดการกับระบบรักษาความปลอดภัยของบริษัทเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ

กรณีศึกษาที่ 2 การเกิดเหตุละเมิดข้อมูลส่วนบุคคลของ Capital One[58]

ข้อเท็จจริง

เมื่อเดือนกรกฎาคม พ.ศ. 2562 ที่ผ่านมา Capital One ซึ่งเป็นสถาบันการเงินของสหรัฐอเมริกาได้ถูกแฮกเกอร์ (Hacker) เข้าสู่ระบบฐานข้อมูลแบบ Cloud ของบริษัทโดยที่บุคคลดังกล่าวเป็นพนักงานของบริษัท Amazon Web Services (AWS) ซึ่งเป็นผู้ให้บริการด้านการจัดการข้อมูลบนระบบ Cloud ที่ Capital One ใช้บริการอยู่ โดยที่พนักงานดังกล่าวสามารถเข้าถึงข้อมูลทั้งหมดของ Capital One ได้ และได้นำเรื่องที่ตนสามารถแฮกข้อมูลของ Capital One ได้ไปโพสต์ลงในกรุ๊ปของ Github ซึ่งเป็นเว็บไซต์ที่ให้บริการพื้นที่ทางอินเทอร์เน็ตสำหรับเก็บการควบคุมการปรับปรุงแก้ไขเอกสารออนไลน์โดยใช้กิต (Git)[59] อันทำให้ Capital One ได้รับทราบถึงการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ

ในการแฮกระบบฐานข้อมูลของ Capital One ในครั้งนี้ทำให้ข้อมูลของลูกค้าบัตรเครดิตเป็นจำนวนมากถูกขโมยไป โดยเจ้าของข้อมูลส่วนบุคคลที่ถูกขโมยไปเป็นชาวอเมริกันประมาณ 100 ล้านคน และเป็นลูกค้าชาวแคนาดาอีกประมาณ 6 ล้านคน ซึ่งข้อมูลส่วนบุคคลที่ถูกแฮกไปนั้นประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล วันเกิด หมายเลขประกันสังคม ข้อมูลที่สามารถเชื่อมไปยังบัญชีธนาคาร และสถานะของบัตรเครดิตของลูกค้า

แต่อย่างไรก็ตาม จากการตรวจสอบการละเมิดข้อมูลส่วนบุคคลนี้ พบว่าข้อมูลที่ถูกแฮกไปนั้นไม่ได้ถูกนำไปใช้ หรือเผยแพร่ให้แก่บุคคลอื่นใดเลย เพียงแต่มีการไปโพสต์โดยแฮกเกอร์ว่ามีการเข้าถึงข้อมูลของ Capital One ได้เท่านั้น และนอกจากนั้นจากการตรวจสอบยังทำให้พบอีกว่าการที่พนักงานของ AWS

สามารถเข้าถึงข้อมูลในฐานระบบของ Capital One ได้ทุกข้อมูลนั้นเป็นเพราะการใช้งาน และตั้งค่าระบบ could ที่เหมาะสม ไม่มีการตั้งค่าในเรื่องของสิทธิในการเข้าถึงข้อมูลของ

---

[58] Howard Poston. (2019). ***Lessons learned: The Capital One breach***. (Online). Available: https://resources.infosecinstitute.com/lessons-learned-the-capital-one-breach/ [2023, June 30]

[59] Pakin Phuhinkong. (2017). ***Git คือ Version Control แบบ Distributed ตัวหนึ่ง เป็นระบบที่ใช้จัดเก็บและควบคุมการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ชนิดใดก็ได้ ไม่ว่าจะเป็น Text File หรือ Binary File***. (ออนไลน์). เข้าถึงได้จาก: https://medium.com/@pakin/git-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3-git-is-your-friend-c609c5f8efea [2566, 27 มิถุนายน]

พนักงาน และบุคคลที่เกี่ยวข้องซึ่งโดยทั่วไปแล้วบริษัทควรจะต้องจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของพนักงานเท่าที่จำเป็นตามหน้าที่ของพนักงานแต่ละคนเท่านั้น

บทวิเคราะห์

จากเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของ Capital One ทำให้เห็นว่าการใช้ระบบ Cloud ในการจัดการข้อมูลของบริษัทฯ ต้องใช้ความระมัดระวังอย่างยิ่งเนื่องจากการจัดการรักษาความปลอดภัยของการใช้ระบบ Cloud นั้นอาจไม่เหมือนกับการจัดการระบบรักษาความปลอดภัยของระบบที่ตั้งอยู่ในบริษัทฯ[60]

การกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของพนักงานแต่ละคนให้สอดคล้องกับความจำเป็น และหน้าที่การงานเป็นสิ่งที่สำคัญสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เนื่องจากการให้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลเกินความจำเป็นอาจทำให้เกิดโอกาสสำหรับผู้ที่เข้าถึงข้อมูลในการนำข้อมูลไปใช้โดยมิชอบได้

การจัดให้มีระบบการติดตาม หรือบันทึกการเข้าถึงข้อมูลก็เป็นวิธีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลได้วิธีหนึ่ง เนื่องจากการจัดให้มีระบบติดตาม และบันทึกการเข้าถึงข้อมูลส่วนบุคคลนี้จะทำให้บริษัทฯ สามารถตรวจสอบได้ว่ามีบุคคลใดบ้างที่เข้าถึงข้อมูลส่วนบุคคล และบุคคลใดที่เข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ ซึ่งเนื่องจาก Capital One ไม่ได้จัดให้มีระบบการติดตาม หรือบันทึกการเข้าถึงข้อมูลส่วนบุคคลที่เหมาะสม เพียงพอ ทำให้ Capital One ไม่สามารถตรวจจับการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบได้เลย จนกระทั่งมีการโพสต์ในเรื่องการเข้าถึงข้อมูลของ Capital One ในกลุ่ม Github ซึ่งเป็นการโพสต์โอ้อวดความสามารถของแฮกเกอร์เอง

2.7 ผู้ที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ถือเป็นประเด็นที่ต้องพิจารณาทางกฎหมายหลายประการ โดยมีการกำหนดจากการเริ่มนับระยะเวลา 72 ชั่วโมง เนื่องจากองค์กรอาจมีความรับผิดทางกฎหมายหากไม่แจ้งภายในระยะเวลาที่กฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด[61] ซึ่งในมาตรา มาตรา 37(4)[62] มีการเขียนไว้ว่า การแจ้งเหตุการละเมิดข้อมูลส่วน

---

[60] pornpilast. (2565). ***หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Letter) คืออะไรต้องเขียนอย่างไรบ้าง ?***.(ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/news-article/data-breach-letter/ [2566,30 มิถุนายน]

[61] pornpilast. (2565). ***หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Letter) คืออะไรต้องเขียนอย่างไรบ้าง ?***.(ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/news-article/data-breach-letter/ [2566,30 มิถุนายน]

[62] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

บุคคลแก่สำนักงานโดยไม่ชักช้าภายใน72 ชั่วโมง “ นับแต่ทราบเหตุ” เท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หากกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด ดังนั้น จุดเริ่มต้นสำคัญที่สุดของการเริ่มนับระยะเวลา คือ “นับแต่ทราบเหตุ” (become aware)

2.7.1 ผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล หรือ (DATA CONTROLLER) หากมีการพิจารณาแล้วว่าเหตุการณ์ข้อมูลรั่วไหลที่เกิดขึ้น (security incident)[63] มีผลทำให้ข้อมูลส่วนบุคคลถูกละเมิด ดังนั้น สิ่งแรกที่องค์กรต้องทำการประเมินก่อน คือ อธิบายผลของเหตุการณ์ข้อมูลรั่วไหลนั้นได้ส่งผลกระทบต่อความเสี่ยง หรือความไม่มั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือไม่'[64]

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ดังนี้

มาตรา 37[65] “ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวน มาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษา ความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

(2) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

---

[63] มหาวิทยาลัยมหิดล วิทยาลัยนานาชาติ . (2565). ***ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller).*** (ออนไลน์). เข้าถึงได้จาก: https://muic.mahidol.ac.th/thai/%E0%B8%9C%E0%B8%B9%E0%B9%89%E0%B8%84%E0%B8%A7%E0%B8%9A%E0%B8%84%E0%B8%B8%E0%B8%A1%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84/ [2566,7มิถุนายน]

[64] pornpilast. (2565). ***หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Letter) คืออะไรต้องเขียนอย่างไรบ้าง ?***.(ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/news-article/data-breach-letter/ [2566,30 มิถุนายน]

[65] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

(3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม ข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคล ได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น

การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความใน มาตรา 33 วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(4) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อ สิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพ ของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยา โดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการ ประกาศกำหนด

(5) ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 5 วรรคสอง ต้องแต่งตั้งตัวแทนของ ผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจ ให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 39[66] “มาตรา 39 ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ ก็ได้

(1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูล ส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

---

[66] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 39.

(6) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(7) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง

(8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1) ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 5 วรรคสอง โดยอนุโลม ความใน (1) (2) (3) (4) (5) (6) และ (8) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่ มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพ ของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26”

2.8 บทลงโทษตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ หากฝ่าฝืนจะมีบทลงโทษ โดยมีการกำหนดโทษไว้ถึง 3 ประเภท ได้แก่ ในหมวดที่ 6 ความรับผิดทางแพ่ง หมวดที่ 7 ส่วนที่หนึ่ง โทษอาญา ส่วนที่สองโทษทางปกครอง โดยในส่วนความรับผิดทางแพ่งได้กำหนดให้มีค่าเสียหายเชิงลงโทษและต้องชดใช้ค่าสินไหมทดแทนรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย และในหมวดที่ 7 ส่วนที่สอง โทษทางปกครองซึ่งการกระทำผิดบางฐานกำหนดค่าปรับทางปกครองสูงถึงห้าล้านบาท[67]

2.8.1 โทษอาญา

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้กำหนดโทษ หรือความรับผิดไว้สำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ แต่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจมีความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ในบางกรณี เช่น กรณีที่ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นจากการปฏิบัติหน้าที่ฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและนำข้อมูลเหล่านั้นไปเปิดเผยแก่บุคคลอื่น

---

[67] ฉัตรสุมน พฤฒิภิญโญ. (2565). PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคล. ***วารสารกฎหมายและนโยบายสาธารณสุข,*** 8(1). หน้า 203-214.

"มาตรา 80[68] ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผย ในกรณีดังต่อไปนี้

1) การเปิดเผยตามหน้าที่

2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้า ที่ตามกฎหมาย

4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ"

2.8.2 โทษทางปกครอง

โทษทางปกครองของ PDPA คือโทษปรับเป็นตัวเงิน ซึ่งมีตั้งแต่ 1 ล้านบาทไปจนถึง 5 ล้านบาท โดยกรณีที่จะโดนโทษปรับสูงสุด 5 ล้านบาทนี้ คือกรณีที่มีการฝ่าฝืนข้อกำหนดที่เกี่ยวกับการใช้หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปต่างประเทศในส่วนที่เป็นข้อมูลส่วนบุคคล sensitive และแน่นอนว่า โทษปรับนี้เป็นคนละส่วนต่างหากจากการชดใช้ค่าเสียหายทางแพ่งและโทษปรับทางอาญา[69]

ประกอบด้วยความรับผิดดังนี้

1) ไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศ หรือไม่แจ้งผลกระทบจากการถอนความยินยอม มีโทษปรับทางปกครองไม่เกินหนึ่งล้าน (1,000,000) บาท

2) ขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ ส่ง หรือโอนข้อมูลส่วนบุคคล โดยไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ มีโทษปรับทางปกครองไม่เกินสามล้าน (3,000,000) บาท

---

[68] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 80.

[69] เดต้า ว้าว. (2564). ***บทลงโทษตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ของไทย.*** (ออนไลน์). เข้าถึงได้จาก: https://dporuler.com/%E0%B8%9A%E0%B8%97%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1/%E0%B8%9A%E0%B8%97%E0%B8%A5%E0%B8%87%E0%B9%82%E0%B8%97%E0%B8%A9pdpa/ [2566,7 กรกฎาคม]

3) เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม มีโทษปรับทางปกครองไม่เกินห้าล้าน (5,000,000) บาท

4) ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่ปฏิบัติตามมีโทษปรับทางปกครองไม่เกินหนึ่ง (1,000,000) ล้านบาท

5) ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 40 โดยไม่มีเหตุอันควรหรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา 37 (5) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 38 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้าน (3,000,000) บาท

6) ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรอง หรือไม่มีมาตรการคุ่มครองที่เหมาะสมตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด มีโทษปรับทางปกครองไม่เกินห้าล้าน (5,000,000) บาท

7) ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลหรือตัวแทนผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 39 วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 39 วรรคสอง และมาตรา 41 วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 41 วรรคสี่ ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้าน (1,000,000) บาท

8) ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ มีโทษปรับทางปกครองไม่เกินห้าแสน (500,000) บาท

9) กรณีที่เห็นสมควรคณะกรรมการผู้เชี่ยวชาญจะสั่งให้แก้ไขหรือตักเตือนก่อนก็ได้

บทลงโทษในกรณีที่เกิดความเสียหายหรือการรั่วไหลของข้อมูล (Data Breach) หน่วยงานที่ไม่ปฏิบัติตามข้อกำาหนดจะถูกปรับเป็นจำานวนเงินถึง 20 ล้านยูโร หรือ 2-4% ของรายได้ต่อปีขึ้นอยู่กับว่าวงเงินใดสูงกว่า ซึ่งเป็นโทษปรับสูงสุดในกรณีร้ายแรง เช่น การไม่ขอความยินยอมที่เหมาะสมเพียงพอในการประมวลผลข้อมูล หรือการปฏิบัติขัดหลักการ Privacy by Design บางกรณีมีโทษปรับ 2% เช่น กรณีการไม่มีการบันทึกข้อมูลอย่างเป็นระบบการไม่แจ้ง Supervising Authority และเจ้าของข้อมูลเมื่อเกิดเหตุรั่วไหล หรือการไม่จัดทำา Privacy Impact Assessment

บทกำหนดโทษข้อมูลส่วนบุคคลถือเป็นสิทธิของเจ้าของข้อมูล ดังนั้น การละเมิดสิทธิในข้อมูลส่วนบุคคลจึงเป็นสิ่งต้องห้าม หากผู้ใดละเมิดสิทธิของเจ้าของข้อมูลแล้วผู้นั้นสมควรอย่างยิ่งที่จะได้รับโทษโดยเฉพาะโทษทางอาญา ร่างพระราชบัญญัติฉบับนี้จึงกำหนดให้ผู้ใดก็ ตามที่กระการเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ผู้นั้นต้องรับโทษทาง

อาญา ในส่วนของพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคลพ.ศ.2562 นั้นจะเห็นได้ว่ามีการร่างออกมาเพื่อมุ่งคุ้มครองข้อมูลส่วนบุคคลในหน่วยงานเอกชนโดยตรง ซึ่งไม่ใช่แค่สถาบันทางการเงินอย่างเดียวเหมือน พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545[70] แต่ยังคลอบคลุมไปถึง หน่วยงานภาคเอกชนทั้งหมด ว่าจะต้องได้รับการคุ้มครองข้อมูลส่วนบุคคล ในการจัดเก็บข้อมูลส่วน บุคคล การใช้และการเปิดเผยข้อมูล ซึ่งหากมีการละเมิดข้อมูลส่วนบุคคล หรือปิดเผยโดยเจ้าของ ข้อมูลไม่ได้ให้ความยินยอม ก็จะมีบทโทษสำหรับผู้ที่กระทำความผิดนั้น[71]

[70] พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

[71] จันทร์ทิพย์ แสงแปง. (2559). ***ปัญหาการคุ้มครองข้อมูลส่วนบุคคลศึกษากรณี การจัดเก็บข้อมูลส่วนบุคคลในหน่วยงานเอกชน.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์.