บทที่ 3

กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย เปรียบเทียบกับกฎหมายต่างประเทศ

มาตรการในการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย โดยปรากฏอยู่ในกฎหมายฉบับต่าง ๆ มักจะให้การคุ้มครองสิทธิของบุคคล โดยเฉพาะรัฐธรรมนูญฉบับปัจจุบันซึ่งเป็นหัวใจสำคัญของการคุ้มครองสิทธิมนุษยชนอันเกี่ยวกับสิทธิและเสรีภาพของบุคคล[1] สิทธิอันเกี่ยวกับทรัพย์สิน ชีวิต และร่างกาย ซึ่งได้ปรากฏอยู่ในประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญาให้ความคุ้มครองสิทธิในลักษณะของการแก้ไขเยียวยา เมื่อเกิดความเสียหายกระทบต่อสิทธิความเป็นส่วนตัว (Privacy) นอกเหนือจากการคุ้มครองชีวิต และร่างกาย ทรัพย์สินยังคุ้มครองดังนี้ เช่น สิทธิในการแสดงออกซึ่งความคิดเห็นสิทธิในการชุมนุมอย่างสงบ สิทธิในการสื่อสารถึงกันอย่างอิสระ โดยปัจจุบันการขโมยข้อมูลประจำตัวเป็นปัญหาที่เพิ่มขึ้นในสังคมมากขึ้น ผู้ที่ตกเป็นเหยื่อของการขโมยข้อมูลประจำตัวหลายล้านคนต่อปีและการขโมยข้อมูลส่วนตัวกลายเป็นเรื่องร้องเรียนของผู้บริโภคที่พบบ่อยที่สุด[2] ปัจจุบันสังคมก้าวสู่ยุคดิจิทัลการใช้วิธีการพิสูจน์ตัวตนแบบดั้งเดิมด้วยรหัสผ่านและบัตรประจำตัวยังมีมาตรการการป้องกันยังไม่เพียงพอที่จะมิให้ถูกขโมยข้อมูลประจำตัวและความปลอดภัยได้

มาตรการทางเทคนิคในการตรวจสอบทางวิทยาศาสตร์ ซึ่งส่วนใหญ่ได้รับการสนับสนุนจากระบบชีววิทยานั้นก็คือ “ไบโอเมตริกซ์” (Biometrics) และใช้วิธีการทางวิทยาศาสตร์สารสนเทศที่เรียกว่า (Information Architecture: IA) อันเป็นสถาปัตยกรรมข้อมูล เช่น การประกันข้อมูล การวิเคราะห์และการวัดคุณลักษณะที่โดดเด่นของบุคคลซึ่งประกอบด้วยคุณลักษณะด้านพฤติกรรมและทางกายภาพ การรับรองความถูกต้องทางไบโอเมตริกซ์ เป็นวิธีการส่วนใหญ่ที่ใช้สำหรับการรับรู้หรือการตรวจสอบบุคคล วิธีการระบุและรับรองความถูกต้องที่ทันสมัยของมนุษย์จะเปลี่ยนบัตรประจำตัวประชาชน หรือหมายเลขประจำตัวส่วนบุคคล (PIN) ปัจจัยที่สำคัญที่สุดของชีวมาตรเมื่อเทียบกับบุคคลอื่นจะต้องมีส่วนร่างกายของบุคคลที่ไม่สามารถปลอมแปลง วิธีการ ตรวจสอบ

---

[1] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560.

[2] วลีรัตน์ พันธุวร และวิมลรัตน์ รุกขวรกุล. (2556). ***สรุปสาระสำคัญของการประชุมฯสำนักงานคณะกรรมการคุ้มครองผู้บริโภค.*** (ออนไลน์). เข้าถึงได้จาก: http://www.ocpb.go.th/download/250756.pdf. [2562, 26 กรกฎาคม]

ไบโอเมตริกซ์ของบุคคลนั้น จึงขึ้นอยู่กับข้อเท็จจริงและข้อมูลทางชีวมาตร ซึ่งเป็นสิทธิพื้นฐานที่สำคัญของมนุษย์แต่ละคนจะได้รับการยอมรับอย่างแม่นยำด้วยคุณสมบัติตามธรรมชาติ (พฤติกรรมหรือร่างกาย) ของบุคคลนั้น[3]

ผู้วิจัยจึงได้ศึกษา การระบุตัวบุคคลด้วยการใช้ระบบไบโอเมตริกซ์ เพื่อความเป็นส่วนตัวและเหตุผลด้านความปลอดภัย ซึ่งหน่วยงานรัฐและองค์กรเอกชนที่ครอบครองข้อมูลส่วนบุคคล หรือข้อมูลไบโอเมตริกซ์ที่อยู่ในความครอบครองของตนห้ามขาย หรือให้เช่า หรือแลกเปลี่ยนหรือแสวงหากำไรจากข้อมูลส่วนบุคคล หรือตัวบ่งชี้ทางชีวมาตร หรือข้อมูลทางชีวมาตรของบุคคล หรือข้อมูลของลูกค้าที่เข้าใช้บริการในองค์กรต่าง ๆ เพื่อป้องกันการละเมิดและก่อความเสียหายที่อาจเกิดได้ทั้งปัจจุบันและในอนาคต ดังนี้

3.1 มาตรการทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศไทย

ปัจจุบันการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย ซึ่งอาจต้องมีการจัดเก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลของผู้ใช้บริการในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคล อันเป็นสิทธิขั้นพื้นฐานสำคัญในความเป็นส่วนตัว (Right to privacy) ของประชาชนที่ต้องได้รับการคุ้มครอง อันจะทำให้ประชาชนมีความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์ของบุคคล ย่อมมีเสรีภาพในการสื่อสารถึงกันในทุกช่องทางที่ชอบด้วยกฎหมาย การตรวจ การกัก หรือการเปิดเผยสิ่งสื่อสารที่บุคคลมีการติดต่อถึงกัน รวมทั้งการกระทำด้วยประการอื่นใด เพื่อให้ล่วงรู้ถึงข้อความในสิ่งสื่อสารทั้งหลายที่บุคคลมีการติดต่อถึงกัน จะกระทำมิได้ เว้นแต่ จะอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายให้ไว้เฉพาะเพื่อรักษาความมั่นคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน

3.1.1 มาตรการการคุ้มครองข้อมูลส่วนบุคคลตามรัฐธรรมนูญแห่งราชอาณาจักรไทย

รัฐธรรมนูญแห่งราชอาณาจักรไทยในอดีตก็มีการรับรองสิทธิพื้นฐานของประชาชนไว้ประการหนึ่งดังจะเห็นได้จากรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ที่ได้รับรองสิทธิของบุคคลไว้ในมาตรา 36[4] บัญญัติไว้ว่า บุคคลย่อมมีเสรีภาพในการติดต่อสื่อสารถึงกันไม่ว่าในทางใด ๆ ก็ตาม

---

[3] Thanon Vongprayoon. (2017). ***Information Architecture -เรื่องที่ UX Designer ไม่ควรมองข้าม.*** (ออนไลน์). เข้าถึงได้จาก: https://medium.com/skooldio/information. [2562, 26 กรกฎาคม]

[4] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560.

จากบทบัญญัติดังกล่าวข้างต้น แสดงให้เห็นว่า บุคคลย่อมมีเสรีภาพในการติดต่อสื่อสารระหว่างกัน บุคคลใดจะมาทำการล้วงรู้ข้อมูลส่วนบุคล การดักฟังข้อมูล หรือกระทำการใด เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลย่อมกระทำไม่ได้ เว้นแต่ อาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เช่น เพื่อประโยชน์สาธารณะ เพื่อประโยชน์ส่วนรวม กล่าวคือ เพื่อกิจการทางทหาร อันเป็นการลุกล้ำจำกัดสิทธิเสรีภาพในร่างกายเพื่อประโยชน์ส่วนรวมในการรักษาเอกราชและความมั่นคงของประเทศ[5] เป็นต้น การจำกัดกรอบการใช้อำนาจรัฐในการตรวจ กัก เปิดเผย สิ่งที่สื่อสาร หรือกระทำการเพื่อจะล่วงรู้ข้อความในสิ่งที่สื่อสารของประชาชนว่าเจ้าหน้าที่ของรัฐต้องเป็นไปเพื่อประโยชน์สาธารณะ เว้นแต่จะมีกฎหมายบัญญัติไว้โดยเฉพาะให้สามารถกระทำได้ หรือคำสั่ง หรือหมายของศาล หลักการป้องกันในการสืบค้นข้อมูลส่วนบุคคล อันกระทบกระเทือนต่อสิทธิมนุษยชนขั้นพื้นฐานที่รัฐธรรมนูญรับรองไว้[6]

อย่างไรก็ตาม การที่รัฐยอมรับรองและให้ความคุ้มครองสิทธิเสรีภาพของประชาชนไว้ในรัฐธรรมนูญ ก็มิได้หมายความว่า รัฐจะยอมให้ประชาชนใช้สิทธิเสรีภาพของตนกระทำการต่าง ๆ ได้โดยปราศจากการแทรกแซงจากองค์กร หรือเจ้าหน้าที่ของรัฐ เพราะรัฐมีผลประโยชน์ของส่วนรวมหรือผลประโยชน์สาธารณะ (Public Interest)[7] ที่จะต้องธำรงรักษาไว้และในการธำรงรักษาไว้ซึ่งประโยชน์ของสาธารณะ รัฐจำต้องบังคับให้ประชาชนกระทำการ หรือละเว้นไม่กระทำการบางอย่าง โดยองค์กรเจ้าหน้าที่ของรัฐจึงสามารถล่วงล้ำเข้าไปในแดนแห่งสิทธิเสรีภาพของประชาชนได้บ้าง จึงต้องมีอำนาจมหาชนที่จะให้รัฐมีอำนาจเหนือปัจเจกบุคคล เพื่อดำเนินการให้สำเร็จตามเป้าหมาย จึงมีแนวคิดทางกฎหมายมหาชนมีความสำคัญ 2 ประการ ดังนี้

ประการแรก ในฐานะที่ประโยชน์สาธารณะ เป็นขอบเขตที่กว้างที่สุดของกฎหมายมหาชน และเป็นการกระทำของรัฐ การมีรัฐ หรือฝ่ายปกครองนั้นก็เพื่อดำเนินการในเรื่องที่เป็นประโยชน์ร่วมกันของบุคคลในสังคม แนวคิดในเรื่องประโยชน์สาธารณะเป็นพื้นฐานของแนวคิดทาง

"มาตรา 36 บุคคลย่อมมีเสรีภาพในการติดต่อสื่อสารถึงกันไม่ว่าในทางใด ๆ การตรวจ การกัก หรือการเปิดเผยข้อมูลที่บุคคลสื่อสารถึงกัน รวมทั้งการกระทำด้วยประการใด ๆ เพื่อให้ล่วงรู้ หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันจะกระทำมิได้ เว้นแต่ มีคำสั่ง หรือหมายของศาล หรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ"

[5] พันวิชญ์ โรจนตันติ. (2547). "ประโยชน์สาธารณะกับการจำกัดสิทธิเสรีภาพ". ***วารสารผู้ตรวจการแผ่นดินของรัฐสภา,*** 2(2). หน้า 61.

[6] สุรีรัตน์ เจตน์ตะพุก. (2560). ***ปัญหาสิทธิการติดต่อสื่อสารทางจดหมายของผู้ต้องขังระหว่างพิจารณาตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 105***. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์. หน้า 577.

[7] เอกนิติ นิติทัณฑ์ประภาศ. (2559). ***การกำกับดูแลรัฐวิสาหกิจภายใต้หลักนิติรัฐและหลักนิติธรรม***. เอกสารทางวิชาการวิทยาลัยรัฐธรรมนูญ สำนักงานศาลรัฐธรรมนูญ. หน้า 6.

สารบัญญัติที่สำคัญของกฎหมายมหาชน เช่น ในเรื่องทฤษฎีบริการสาธารณะ (Public Service) ซึ่งการจะพิจารณาว่ากิจกรรมใดเป็นบริการสาธารณะหรือไม่ วัตถุประสงค์ที่เป็นบริการสาธารณะจะต้องมี 3 ลักษณะ เช่น

ลักษณะที่หนึ่ง เพื่อประโยชน์สาธารณะ เพื่อประโยชน์ส่วนรวม หรือประโยชน์มหาชน

ลักษณะที่สอง เพื่อกิจกรรมที่ดำเนินการโดยนิติบุคคลในกฎหมายมหาชน หรืออยู่ภายใต้การควบคุมของนิติบุคคลในกฎหมายมหาชน กล่าวคือ มีการควบคุมโดยตรงจากองค์กรของรัฐ

ลักษณะที่สาม วิธีการที่ใช้ในการดำเนินการต้องเป็นวิธีตามกฎหมายมหาชน ไม่ใช่วิธีการตามกฎหมายทั่วไป

ประการที่สอง ในฐานะที่ประโยชน์สาธารณะเป็นการควบคุมความชอบด้วยกฎหมายต้องมีองค์กรควบคุม คือ ศาลซึ่งมีหน้าที่ควบคุมไม่ให้การกระทำของรัฐดำเนินไปในลักษณะที่นอกเหนือไปจากเพื่อประโยชน์สาธารณะ

ดังนั้น วัตถุประสงค์ของรัฐที่ต้องเป็นไปเพื่อตอบสนองความต้องการของบุคคลส่วนรวม ซึ่งต่างจากวัตถุประสงค์ของเอกชนที่มุ่งตอบสนองความต้องการส่วนบุคคล โดยหลักรัฐสภาและศาลจะเป็นผู้ตีความว่าอะไรคือประโยชน์สาธารณะ

ประเทศไทยได้มีการร่วมลงนาม โดยไม่มีการแบ่งแยกว่าบุคคลนั้น จะมีอายุเท่าไรเพศใด เชื้อชาติใด นับถือศาสนาและภาษาอะไรมีสถานภาพทางกาย หรือฐานะใดหากบุคคลอยู่ในพื้นที่ที่ใช้รัฐธรรมนูญย่อมได้รับความคุ้มครองสิทธิเสรีภาพและมีความเท่าเทียมกันในศักดิ์ศรีความเป็นมนุษย์ด้วยเหตุนี้ ในการปฏิบัติงานตามอำนาจหน้าที่ตลอดจนการตรากฎหมายการตีความและการบังคับใช้กฎหมาย อาจมีการละเมิดสิทธิและเสรีภาพของบุคคลตามรัฐธรรมนูญ หากถูกลิดรอน หรือถูกละเมิดสิทธิมนุษยชนก็สามารถร้องเรียนต่อศาล เพื่อให้ดำเนินคดีได้ตามรัฐธรรมนูญกฎหมายสูงสุดของประเทศได้เขียนบทบัญญัติให้การคุ้มครองสิทธิของประชาชนทุกคนจากบุคคลอื่นที่มาแสวงหาผลประโยชน์ โดยมิชอบในข้อมูลส่วนบุคคลที่เกี่ยวกับประชาชน โดยพิจารณาถึงว่ามีกฎหมายลำดับรอง หรือกฎหมายลูกบัญญัติถึงรายละเอียดเนื้อหาตามกฎหมายดังกล่าว จะให้การคุ้มครองรวมทั้งตลอดจนองค์กรที่จะต้องเข้ามาดูแล และบทลงโทษในกรณีที่มีบุคคลอื่นเข้ามาละเมิดโดยมิชอบในข้อมูลส่วนบุคคลของประชาชน[8]

กฎหมายบัญญัติให้อำนาจ “ในการคุ้มครองสิทธิของบุคคลในความเป็นส่วนตัว เช่น เกียรติยศ ชื่อเสียง และครอบครัว ก็ย่อมได้รับการคุ้มครอง หากมีการกล่าวหรือไขข่าวแพร่หลายซึ่ง

---

[8] สรรชัย อจลานนท์. (2560). ***หลักสิทธิมนุษยชน กับ การปฏิบัติการทางทหาร.*** เอกสารทางวิชาการหลักสูตรนิติธรรมเพื่อประชาธิปไตย. กรุงเทพฯ: สำนักงานศาลรัฐธรรมนูญ. หน้า 1-4.

ข้อความอันฝ่าฝืนต่อความจริง[9] หรือภาพไม่ว่าด้วยวิธีใดก็ตามไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบสิทธิของบุคคลในครอบครัวจะกระทำมิได้" เว้นแต่จะเป็นประโยชน์ต่อสาธารณะ บุคคลนั้นย่อมมีสิทธิได้รับการคุ้มครองการแสวงหาประโยชน์โดยมิชอบ[10]

ในบรรดาสิทธิอันเกี่ยวข้องกับสิทธิมนุษยชนทั้งหมด "ความเป็นส่วนตัว" ถือว่าเป็นสิทธิที่สังคมยุคใหม่เกือบทุกประเทศ ได้ให้ความสำคัญเป็นอย่างมากและเป็นสิทธิลักษณะหนึ่งที่ยากที่สุดในการบัญญัติความหมายเพราะต้องพิจารณาถึงเนื้อหาสภาพของสังคม วัฒนธรรมและพฤติการณ์ในการใช้ชีวิต สภาพแวดล้อมประกอบด้วย ในบางประเทศมีแนวคิดของคำว่า "ความเป็นส่วนตัว" ได้รวมถึงการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นการตีความคำว่า "ความเป็นส่วนตัว" ในด้านการจัดการข้อมูลส่วนบุคคล ซึ่งเป็นคำที่มีความหมายกว้างและครอบคลุมถึงสิทธิต่าง ๆ หลายประการ ซึ่งได้แก่[11]

ประการที่แรก ด้านความเป็นส่วนตัวในด้านข้อมูลส่วนบุคคล (Information privacy) โดยเป็นการคุ้มครองข้อมูลส่วนบุคคล โดยมีการกำหนดหลักเกณฑ์เกี่ยวกับการเก็บ รวบรวม เปิดเผย ใช้ รวมถึงการบริหารจัดการข้อมูลส่วนบุคคล

ประการที่สอง ด้านความเป็นส่วนตัวเกี่ยวกับชีวิตและร่างกาย (Bodily privacy) โดยเป็นการคุ้มครองในชีวิตและร่างกายของบุคคลในด้านทางกายภาพที่จะไม่ถูกดำเนินการใด ๆ อันเป็นการละเมิดในความเป็นส่วนตัว เช่น การทดลองทางพันธุกรรม การทดลองผลิตภัณฑ์ยา เป็นต้น

ประการที่สาม ด้านความเป็นส่วนตัวเกี่ยวกับการติดต่อสื่อสาร (Communication privacy) โดยเป็นการคุ้มครองในด้านความปลอดภัยในการติดต่อสื่อสารในด้านต่าง ๆ เช่น จดหมาย อีเมล โทรศัพท์ ไปรษณีอิเล็กทรอนิกส์ หรือวิธีอื่นใดซึ่งผู้อื่นจะล่วงรู้ไม่ได้

ประการสุดท้าย ด้านความเป็นส่วนในเคหสถาน (Territorial privacy) โดยการกำหนดข้อจำกัดขอบเขต ไม่ให้บุคคลอื่นเข้ามาบุกรุกภายในสถานที่ส่วนตัวได้ ทั้งนี้ รวมถึงการสอดส่องด้วยการติดกล้องวีดีโอ และการตรวจสอบรหัสประชาชนของบุคคล (ID checks)

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 77 โดยเฉพาะในส่วนที่ว่ากฎหมายอาญาต้องมีเฉพาะที่จำเป็น และต้องมีเฉพาะที่ร้ายแรงได้สร้างแนวทางในการออกกฎหมาย

---

[9] ประมวลกฎหมายแพ่งและพาณิชย์. มาตรา 423.

[10] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560. มาตรา 32.

[11] ชุลีพร น่วมทนง. (2557). ***สิทธิมนุษยชนกับการคุ้มครองข้อมูลส่วนบุคคล***. เอกสารทางวิชาการ วิทยาลัยรัฐธรรมนูญ สำนักงานศาลรัฐธรรมนูญ. หน้า 5.

พัฒนากฎหมาย และปรับปรุงแก้ไขกฎหมายเป็นครั้งแรกในระบบกฎหมายไทย ซึ่งมีสาระสำคัญดังนี้[12]

ประการแรก ให้มีกฎหมายเท่าที่จำเป็น

ประการที่สอง ให้ยกเลิก หรือแก้ไขกฎหมายที่ไม่จำเป็น

ประการที่สาม ให้ประชาชนเข้าถึงกฎหมายได้อย่างสะดวก

ประการที่สี่ ก่อนออกกฎหมายให้รับฟังความเห็นผู้เกี่ยวข้อง วิเคราะห์ผลกระทบของกฎหมาย

ประการที่ห้า เมื่อใช้กฎหมายไประยะหนึ่งให้มีการทบทวนว่ากฎหมายนั้น ๆ ยังมีความจำเป็นจะต้องใช้อยู่ หรือควรปรับปรุงแก้ไขอย่างใดให้สอดคล้องกับสถานการณ์

ประการสุดท้าย ให้มีกฎหมายอาญาเฉพาะความผิดร้ายแรง

ดังนั้น ความผิดทางอาญายังมีความจำเป็นอยู่เพราะเป็นเรื่องร้ายแรง เช่น ฆาตกรรม ลักวิ่ง ชิง ปล้นทรัพย์ เป็นต้น ซึ่งเป็นความผิดหลักในประมวลกฎหมายอาญา รวมทั้งการกระทำที่เกี่ยวกับความปลอดภัยสาธารณะ เช่น กฎหมายเกี่ยวกับอาวุธปืน และการกระทำที่กระทบต่อสวัสดิภาพ เศรษฐกิจ สังคม และการสาธารณสุขของส่วนรวม แต่อย่างไรก็ตาม กฎหมายที่ยังจำเป็นต้องมีสภาพบังคับแต่ไม่ร้ายแรงพอที่จะเป็นกฎหมายอาญา จึงควรใช้โทษปรับทางปกครอง หรือจำกัดสิทธิทางปกครองแทน กฎหมายเหล่านี้ก็จะถูกปรับเปลี่ยนในรูปแบบโทษทางปกครอง

---

[12] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560. มาตรา 77

รัฐพึงจัดให้มีกฎหมายเพียงเท่าที่จำเป็น และยกเลิกหรือปรับปรุงกฎหมายที่หมดความจำเป็นหรือไม่สอดคล้องกับสภาพการณ์ หรือที่เป็นอุปสรรคต่อการดำรงชีวิตหรือการประกอบอาชีพโดยไม่ชักช้าเพื่อไม่ให้เป็นภาระแก่ประชาชน และดำเนินการให้ประชาชนเข้าถึงตัวบทกฎหมายต่าง ๆได้โดยสะดวกและสามารถเข้าใจกฎหมายได้ง่ายเพื่อปฏิบัติตามกฎหมายได้อย่างถูกต้อง

ก่อนการตรากฎหมายทุกฉบับ รัฐพึงจัดให้มีการรับฟังความคิดเห็นของผู้เกี่ยวข้อง วิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากกฎหมายอย่างรอบด้านและเป็นระบบ รวมทั้งเปิดเผยผลการรับฟังความคิดเห็นและการวิเคราะห์นั้นต่อประชาชน และนำมาประกอบการพิจารณาในกระบวนการตรากฎหมายทุกขั้นตอนเมื่อกฎหมายมีผลใช้บังคับแล้ว รัฐพึงจัดให้มีการประเมินผลสัมฤทธิ์ของกฎหมายทุกรอบระยะเวลาที่กำหนดโดยรับฟังความคิดเห็นของผู้เกี่ยวข้องประกอบด้วย เพื่อพัฒนากฎหมายทุกฉบับให้สอดคล้องและเหมาะสมกับบริบทต่าง ๆ ที่เปลี่ยนแปลงไป

รัฐพึงใช้ระบบอนุญาตและระบบคณะกรรมการในกฎหมายเฉพาะกรณีที่จำเป็น พึงกำหนดหลักเกณฑ์การใช้ดุลพินิจของเจ้าหน้าที่ของรัฐและระยะเวลาในการดำเนินการตามขั้นตอนต่าง ๆ ที่บัญญัติไว้ในกฎหมายให้ชัดเจน และพึงกำหนดโทษอาญาเฉพาะความผิดร้ายแรง

(Administrativization) เช่น ความผิดเกี่ยวกับการฝ่าฝืนเงื่อนไขในการขออนุมัติอนุญาตดำเนินกิจการทั้งหลายที่ไม่มีผลกระทบกับสังคม[13]

เนื่องจากรัฐบาลโดยกระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อม หรือกระทรวงไอซีที หรือกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้มีการเสนอร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล[14] โดยมีหลักการเพื่อให้ประเทศไทยมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ซึ่งในส่วนเนื้อหาของบทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับปัจจุบัน พุทธศักราช 2562 ได้วางหลักไว้ว่า ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม เว้นแต่บทบัญญัติแห่งพระราชบัญญัติฉบับนี้ หรือกฎหมายอื่นบัญญัติให้กระทำได้ ในการขอความยินยอมจากผู้เป็นเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นด้วย และการขอความยินยอมนั้น ต้องมิใช่เป็นการหลอกลวง การให้ความยินยอมโดยอิสระ หรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ซึ่งเจ้าของข้อมูลส่วนบุคคลจะทำการยกเลิก หรือเพิกถอนความยินยอมในเวลาใดก็ได้[15]

การจัดเก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล อันได้แก่ ประวัติการศึกษา ฐานะทางการเงิน ประวัติการทำงาน ประวัติสุขภาพ หรือลายนิ้วมือ หรือการบันทึกลักษณะเสียง หรือประวัติอาชญากรรม ตลอดจนหมายเลขโทรศัพท์ รหัสประจำตัวประชาชน หรือรูปถ่าย โดยที่เจ้าของข้อมูลส่วนบุคคลนั้นมิได้ให้ความยินยอม ย่อมถือได้ว่าเป็นการกระทำที่ไม่ชอบด้วยกฎหมาย ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายฉบับนี้ ก็ไม่อาจใช้ข้อมูลส่วนบุคคลที่มีอยู่ในความครอบครอง หรืออยู่ในการควบคุมดูแลของตนเอง โดยมิได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลนั้นได้[16]

นอกจากนี้ พระราชบัญญัติฉบับนี้ ยังได้บัญญัติบทลงโทษทางอาญาไว้สำหรับบุคคลที่กระทำการใด ๆ ที่เกี่ยวกับข้อมูลส่วนบุคคล เพื่อให้ตนเอง หรือผู้อื่นได้รับผลประโยชน์อันมิชอบ

---

[13] อิสร์กุล อุณหเกตุ. (2013). ***ปัญหาของระบบค่าปรับทางอาญาในประเทศไทย***. (ออนไลน์). เข้าถึงได้จาก: https://tdri.or.th/2014/03/fine-system/. [2563, 28 มกราคม].

[14] สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (2559). ***ประชาสัมพันธ์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เปิดเวทีรับฟังความคิดเห็นต่อร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ***...(ออนไลน์). เข้าถึงได้จาก: https://www.etcommission.go.th/news-topic-meeting-dp-161159.html. [2562, 29 พฤศจิกายน]

[15] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 21 วรรคสอง.

[16] สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. อ้างแล้วเชิงอรรถที่ 14. (ออนไลน์).

ด้วยกฎหมาย หรือเพื่อให้ผู้อื่นได้รับความเสียหายต้องระวางโทษจำคุกไม่เกิน 1 ปีหรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ[17] ซึ่งสังคมเกิดจากการรวมตัวกันของคนส่วนใหญ่จึงจำเป็นต้องมีการควบคุมความประพฤติของสมาชิกในสังคมเพื่อให้สามารถอยู่ร่วมกันได้โดยสงบสุข หากมีการละเมิดกฎหมายซึ่งถือว่าเป็นความผิด ก็จะต้องมีการลงโทษ การลงโทษจึงเป็นเครื่องมือส่งเสริมประสิทธิภาพของกฎหมายอย่างหนึ่งและเป็นการใช้อำนาจบังคับโดยรัฐอันเป็นมาตรการบังคับทางอาญาตามมาตรา 79 วรรคสอง

ดังนั้น แม้ว่า “ความเป็นส่วนตัว” จะครอบคุลมถึงสิทธิหลายประการแต่ความเป็นส่วนตัวที่นานาประเทศต่าง ๆ ให้ความสำคัญอย่างมากก็คือ “ความเป็นส่วนตัวในข้อมูลส่วนบุคคล” ทั้งนี้เพราะความก้าวหน้าทางเทคโนโลยีที่สามารถประมวลผลได้อย่างรวดเร็วและจัดเก็บข้อมูลได้อย่างเป็นระบบส่งผลให้การติดต่อสื่อสารและการเผยแพร่ข้อมูลสามารถเคลื่อนย้ายและเชื่อมโยงกันได้โดยสะดวกรวดเร็วอย่างไม่จำกัดเวลาและสถานที่อีกต่อไป ซึ่งเป็นไปได้ทั้งโอกาสและภัยคุกคามในขณะเดียวกัน จึงมีความจำเป็นต้องจัดวางกลไกให้มีความสัมพันธ์ระหว่างสิทธิความเป็นส่วนตัวหรือเสรีภาพในการเคลื่อนไหวของข้อมูลและการเปิดเผยข้อมูลให้มีความเหมาะสม เพื่อป้องกันการนำเทคโนโลยีสารสนเทศไปใช้ในทางมิชอบ เช่น การนำข้อมูลส่วนบุคคลไปแสวงหาผลประโยชน์ทางการค้า จากการขายข้อมูลส่วนบุคคลนั้น หรือนำไปใช้ในทางทุจริตจนทำให้บุคคลที่เป็นเจ้าของข้อมูลนั้น ได้รับความเสียหาย อันเป็นการละเมิดและก้าวล่วงในความเป็นส่วนตัวของบุคคลอื่น หรือการแทรกแซงต่อข้อมูลส่วนบุคคล โดยไม่คำนึงถึงสิทธิขั้นพื้นฐานของบุคคลอื่น อันเป็นการคุกคามความเป็นส่วนตัวของบุคคลอื่น ซึ่งอาจส่งผลกระทบต่อความสงบสุขของสังคมได้ในที่สุด

3.1.2 มาตรการการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พุทธศักราช 2540

การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พุทธศักราช 2540 ซึ่งได้บทบัญญัติไว้ในพระราชบัญญัติข้อมูลข่าวสาร ได้มีการกล่าวถึง “ข้อมูลข่าวสาร” ไว้ว่า การสื่อสารหมายถึงเรื่องราวข้อเท็จของข้อมูล หรือสิ่งอื่นใดในการสื่อความหมายได้โดยสภาพไม่ว่าด้วยวิธีใด ๆ หรือไม่ว่าจะอยู่ในรูปแบบเอกสาร แฟ้ม หนังสือ รางาน แผนที่ ภาพเขียน ภาพวาด ภาพฟิล์ม สิ่งบันทึก เสียง โดยระบบคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้ปรากฏได้ “ข้อมูลข่าวสารของราชการ” หมายถึง ข้อมูลข่าวสารต่าง ๆ ที่อยู่ในการครอบครองดูแลของหน่วยงานของรัฐ ให้รวมถึงข้อมูลข่าวสารต่าง ๆ ที่เกี่ยวข้องกับการดำเนินงานของรัฐ หรือข้อมูลข่าวสารที่เกี่ยวข้องกับการดำเนินงานของเอกชนนั้นด้วย

---

[17] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 79 วรรคสอง.

หมายความว่า ข้อมูลข่าวสารที่เกี่ยวข้องกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ประวัติสุขภาพ ฐานะการเงิน ประวัติอาชญากรรม หรือประวัติการทำงานของบุคคลนั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น รูปถ่าย ลายนิ้วมือ แผ่นบันทึกลักษณะเสียง และรวมถึงข้อมูลข่าวสารเกี่ยวข้องกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมไปแล้วด้วย ซึ่งพระราชบัญญัติฉบับนี้หมายถึง เรื่องของข้อมูลประเภทต่าง ๆ ที่ได้กล่าวมาแล้วข้าต้น โดยได้กล่าวถึงคำว่าข้อมูลส่วนบุคคลในมาตรา 4 ยังได้อธิบายไว้อย่างชัดเจนอีกว่า บุคคล หมายถึง อะไร ซึ่งได้วางหลักไว้ว่าดังนี้

เพื่อประโยชน์แห่งหมวดนี้ตามมาตรา 21 “บุคคล” หมายความว่า บุคคลธรรมดาที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทยแต่มีถิ่นที่อยู่ในประเทศไทยและได้บัญญัติหน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลดังนี้[18]

มาตรา 23 หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคล[19] ดังต่อไปนี้

การจัดเก็บข้อมูลข่าวสารต้องกระทำเพียงเท่าที่จำเป็นและเกี่ยวข้องกับบุคคลนั้น เพื่อการดำเนินงานตามอำนาจหน้าที่ของหน่วยงานของรัฐตามวัตถุประสงค์เท่านั้น รวมทั้งทำร้ายข้อมูลที่จัดเก็บเมื่อหมดวัตถุประสงค์

การจัดเก็บข้อมูลข่าวสารต้องกระทำการจัดเก็บเฉพาะข้อมูลจากเจ้าของโดยตรง และต้องไม่ให้กระทบถึงสิทธิและผลประโยชน์ของบุคคลนั้น

การจัดพิมพ์ต้องประกาศในราชกิจจานุเบกษา รวมทั้งต้องตรวจสอบแก้ไขความถูกต้องให้เป็นปัจจุบันอยู่เสมอ ดังต่อไปนี้

ประเภทของบุคคลที่ได้เก็บข้อมูลไว้ ระบบข้อมูลข่าวสารส่วนบุคคลโดยมีลักษณะการใช้ข้อมูลตามปกติ สามารถขอตรวจสอบข้อมูลข่าวสาร วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล แหล่งที่มาของข้อมูลของเจ้าข้อมูล

การตรวจสอบการแก้ไขข้อมูลข่าวสารส่วนบุคคลที่อยู่ในการควบคุมให้มีความถูกต้องเสมอ

การมีมาตรการป้องกันระบบของการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบข้อมูลข่าวสารส่วนบุคคลให้มีความเหมาะสม เพื่อป้องกันมิให้มีการละเมิดที่จะส่งผลร้ายแก่เจ้าของข้อมูล

ในการเก็บข้อมูลข่าวสารจากเจ้าของข้อมูลโดยตรงนั้น โดยหน่วนงานของรัฐจะต้องแจ้งให้เจ้าของข้อมูลได้ทราบล่วงหน้าก่อน หรือพร้อมแจ้งถึงวัตถุประสงค์ในการนำข้อมูลไปใช้ในลักษณะตามปกติ และการให้ข้อมูลโดยความสมัครใจ หรือกรณีตามกฎหมายบังคับ โดย

---

[18] พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พุทธศักราช 2540. มาตรา 21.

[19] พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พุทธศักราช 2540. มาตรา 23.

หน่วยงานของรัฐ หรือเจ้าหน้าที่ของรัฐ อาจมีคำสั่งมิให้เปิดเผยก็ได้ และคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานของรัฐ หรือประโยชน์สาธารณะและประโยชน์ของเอกชนที่มีส่วนเกี่ยวข้องประกอบกัน[20] ดังนี้

สาระสำคัญของการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้มีสามประการ ได้แก่

ประการแรก การกำหนดหน้าที่ต่าง ๆ เกี่ยวกับการจัดระบบข้อมูลส่วนบุคคลของหน่วยงานของรัฐ เพื่อให้การคุ้มครองข้อมูลข่าวสารส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและปลอดภัย

ประการที่สอง การกำหนดข้อห้ามในการเปิดเผยข้อมูลข่าวสารส่วนบุคคล โดยกำหนดให้ต้องได้รับความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลก่อนที่ทำการเปิดเผยข้อมูลนั้น เว้นแต่เป็นกรณีตามที่กฎหมายบัญญัติ

ประการสุดท้าย ให้สิทธิแก่เจ้าของข้อมูลในการตรวจสอบข้อมูลข่าวสารส่วนบุคคลของตนเองที่อยู่ในความครอบครองของหน่วยงานของรัฐ และให้สิทธิในการขอแก้ไขข้อมูลให้ถูกต้องตามความเป็นจริง อีกทั้งให้สิทธิในการอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร[21]

หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบ ในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติและยังได้มีบทบัญญัติห้ามมิให้หน่วยงานรัฐที่ควบคุมดูแลเปิดเผยข้อมูลส่วนบุคคลแก่หน่วยงานอื่น โดยเจ้าของข้อมูลไม่ยินยอมแต่มีข้อยกเว้นตาม มาตรา 24 และมาตรา 25 ในกรณี ดังนี้

เจ้าหน้าที่ในหน่วยงาน เพื่อนำไปใช้ตามอำนาจหน้าที่ การใช้ข้อมูลตามวัตถุประสงค์ของการจัดเก็บ ต่อหน่วยงานที่ทำงานด้านแผน หรือการสถิติ หรือสำมะโนครัว การใช้เพื่อประโยชน์ในการศึกษาวิจัยหอจดหมายเหตุแห่งชาติ เพื่อการตรวจดูคุณค่าในการเก็บรักษา เจ้าหน้าที่เพื่อป้องกันการฝ่าฝืน หรือไม่ปฏิบัติตามกฎหมายกรณีจำเป็นเพื่อป้องกัน หรือระงับอันตรายต่อชีวิต หรือสุขภาพ ศาล และเจ้าหน้าที่หน่วยงาน หรือบุคคลที่มีอำนาจตามกฎหมาย กรณีอื่นตามที่กำหนดไว้ในพระราชกฤษฎีกา[22]

---

[20] สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม. (2558). ***พระราชบัญญัติศูนย์ข้อมูลข่าวสารสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม***. กรุงเทพฯ: สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม. หน้า 4.

[21] พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540. มาตรา 4.

[22] พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พุทธศักราช 2540. มาตรา 24.

กรณีกระทบกระเทือนสิทธิถึงเจ้าของข้อมูลข่าวสารส่วนบุคคลโดยฝ่าฝืนไม่ปฏิบัติตามมาตรา 25 (ยกเว้นเป็นกรณีตามมาตรา 25 วรรคสี่) ย่อมมีสิทธิได้รับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับตน ดังนี้

สิทธิรับรู้ข้อมูลส่วนบุคคลของตน (ขอตรวจดูหรือได้รับสำเนา) สิทธิในการขอแก้ไขเปลี่ยนแปลง หรือลบข้อมูลข่าวสารของตน สิทธิในการอุทธรณ์ กรณีหน่วยงานไม่ลบ หรือเปลี่ยนแปลงตามคำขอ (ภายใน 30 วัน)[23]

ดังนั้น หากพิจารณาคำว่า “ข้อมูลส่วนบุคคล” ซึ่งปรากฏอยู่ในพระราชบัญญัติข้อมูลข่าวสารของราชการ พุทธศักราช 2540 กำหนดไว้ว่า ข้อมูลข่าวสารทั้งหลายที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคล โดยมีชื่อ หรือเลขหมาย หรือ รหัส หรือ สิ่งบอกลักษณะอื่นใดที่ทำให้รู้ตัวผู้นั้นได้[24] ซึ่งได้บัญญัติไว้ในทำนองเดียวกันว่า “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคล ที่ทำให้สามารถระบุตัวของบุคคลนั้นได้ แต่ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐบางแห่งยังไม่ได้รับการคุ้มครอง หรือการเก็บรักษาไว้ดีเท่าที่ควร

โดยพระราชบัญญัติข้อมูลข้อมูลข่าวสารพุทธศักราช 2540 มุ่งหมายที่จะคุ้มครองข้อมูลส่วนบุคคลมิให้ถูกเปิดเผย หรือถูกนำไปใช้อย่างไม่เหมาะสม หรือเป็นผลทำให้เกิดความเสียหายต่อเจ้าของข้อมูล และการเปิดเผยข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูล เว้นแต่จะเป็นการเปิดเผยตามข้อยกเว้นตามที่กฎหมายบัญญัติไว้ อย่างไรก็ตาม พระราชบัญญัติข้อมูลข้อมูลข่าวสารพุทธศักราช 2540 มีจุดมุ่งหมายคุ้มครองข้อมูลส่วนบุคคลที่อยู่ภายในการดูแลของหน่วยงารรัฐ เมื่อพิจารณาตามถ้อยคำของกฎหมายข้อมูลจากลูกค้า หรือผู้รับบริการที่ได้จากการใช้ (Biometrics) แม้จะอยู่ในรูปแบบของรหัสชุด หรือรูปแบบอิเล็กทรอนิกส์ ย่อมเป็นข้อมูลส่วนบุคคลของลูกค้า หรือ ผู้รับบริการทั้งสิ้น เพราะเป็นสิ่งที่ทำให้ธนาคาร หรือผู้ให้บริการสามารถระบุยืนยัน และทราบถึงตัวตนของลูกค้าแต่ละรายได้อย่างถูกต้องก่อนให้บริการ หรืออาจกล่าวได้ว่าข้อมูลไบโอเมตริกซ์ (Biometrics Data) คือ ข้อมูลส่วนบุคคลที่หน่วยงานของเอกชนต้องดูแลตามมาตรฐานที่กฎหมายกำหนด

3.1.3 การคุ้มครองข้อมูลส่วนบุคคลตามประมวลกฎหมายแพ่งและพาณิชย์ พุทธศักราช 2561

ประมวลกฎหมายแพ่งและพาณิชย์ถือได้ว่าเป็นกฎหมายทั่วไปที่นำมาปรับใช้กับกรณีต่าง ๆ ที่ไม่ได้มีการบัญญัติเรื่องนั้น ๆ ไว้เป็นการเฉพาะ หากมีผู้กระทำละเมิดต่อข้อมูลส่วนบุคคลในการธุรกิจ

---

[23] พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พุทธศักราช 2540. มาตรา 25.

[24] สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม. (2558). อ้างแล้วเชิงอรรถที่ 20. หน้า 4.

หรือละเมิดข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชนแล้ว จะมีการนำประมวลกฎหมายแพ่งและพาณิชย์มาปรับใช้กับกรณีที่เกิดทำละเมิดก่อนได้

การคุ้มครองข้อมูลส่วนบุคคลในการทำนิติกรรมต่าง ๆ ผ่านระบบอิเตอร์เน็ตในทางพาณิชย์ที่เกี่ยวข้องในทางธุรกิจ หรือไม่ก็ตาม ผู้ให้บริการล้วนแต่ทราบพฤติกรรมการใช้งานอินเตอร์เน็ตของผู้ใช้บริการทั้งนั้น อาจเกิด “ความเสี่ยง” การถูกละเมิดข้อมูลส่วนบุคคลจากกิจกรรมออนไลน์ประเภทต่าง ๆ ได้ ดังนั้น ตามหลักกฎหมายประมวลแพ่งและพาณิชย์ได้บัญญัติให้มีการคุ้มครองในแง่ของกฎหมายลักษณะการละเมิด ซึ่งเป็นกฎหมายที่เป็นหลักการทั่วไปของการให้ความคุ้มครองสิทธิที่ชอบด้วยกฎหมายของบุคคล โดยมีมาตรา 420 เป็นมาตราของกฎหมายลักษณะละเมิด คือ “ผู้ใดจงใจหรือประมาทเลินเล่อทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดีแก่ร่างกายก็คือนามัยก็ดีเสรีภาพก็ดีทรัพย์สิน หรือสิทธิอย่างใดอย่างหนึ่งก็ดีท่านว่าผู้นั้นทำละเมิดจำต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้น”[25]

หากมีผู้กระทำละเมิดต่อสิทธิของบุคคลโดยผิดกฎหมายไม่ว่าจะด้วยความจงใจ หรือประมาทเลินเล่อย่อมต้องรับผิดชอบชดใช้ค่าสินไหมทดแทนให้แก่ผู้เสียหายซึ่งสิทธิดังกล่าวนี้ เป็นการใช้สิทธิซึ่งมีแต่จะให้เกิดเสียหายแก่บุคคลอื่นตามมาตรา 421 หมายความรวมถึง สิทธิส่วนตัวด้วย ดังนั้น สิทธิส่วนตัวย่อมได้รับความคุ้มครองไม่ให้ใครมาละเมิดจนเกินสมควร เป็นเหตุให้สิทธิของบุคคลนั้น ได้รับความเสียหาย เช่น การนำภาพลับเฉพาะ หรือภาพเปลือยกายของบุคคลใดบุคคลหนึ่งไปเปิดเผยต่อสาธารณชนเป็นต้น บุคคลนั้นย่อมเรียกค่าสินไหมทดแทนจากกระทำละเมิดนั้น ๆ ได้[26]

นอกจากนี้ ในมาตรา 422 และมาตรา 423 ยังสามารถนำมาปรับใช้กับการคุ้มครองข้อมูลส่วนบุคคลได้อีกด้วย ซึ่งทั้งสองมาตราได้วางหลักกฎหมายไว้ว่า หากเกิดความเสียหายแต่การฝ่าฝืนบทบัญญัติแห่งกฎหมายใด ท่านให้สันนิษฐานไว้ก่อนว่าผู้นั้นเป็นผู้ผิดเพื่อจะปกป้องบุคคลอื่น ๆ ฝ่าฝืน หรือ “ผู้ใดกล่าว หรือเปิดเผยข้อความซึ่งฝ่าฝืนต่อความจริง ก่อให้เกิดความเสียหายแก่ชื่อเสียง หรือเกียรติคุณของบุคคลอื่น หรือโดยประการอื่น บุคคลนั้นจำต้องรับผิดใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อความเสียหายอย่างใด ๆ แต่หากผู้รับข่าวสารหรือเปิดเผยนั้น มีทางได้เสียโดยชอบในการนั้น ผู้นั้นก็ไม่ต้องรับผิดค่าสินไหมทดแทน”[27]

อย่างไรก็ตาม แม้ว่าหลักประมวลกฎหมายแพ่งและพาณิชย์จะให้การคุ้มครองข้อมูลส่วนบุคคลไว้ แต่ยังคงขาดหลักเกณฑ์ที่สำคัญเกี่ยวกับวิธีการ เงื่อนไข และมาตรการที่สำคำคัญ ๆ ที่เป็น

---

[25] ประมวลกฎหมายแพ่งและพาณิชย์ พ.ศ.2561. มาตรา 420.

[26] ประมวลกฎหมายแพ่งและพาณิชย์ พ.ศ.2561. มาตรา 421.

[27] ประมวลกฎหมายแพ่งและพาณิชย์ พ.ศ.2561. มาตรา 422 - 423.

การเฉพาะเจาะจงอันเกี่ยวกับหลักประกันในเรื่องการคุ้มครองข้อมูลส่วนบุคคลได้อย่างเพียงพอตามแนวปฏิบัติของหลักสากล ดังจะได้ศึกษาต่อไป

3.1.4 มาตรการทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามประมวลกฎหมายอาญา

กฎหมายพื้นฐานที่สำคัญอีกฉบับ คือ ประมวลกฎหมายอาญามาตรา 163 ถือได้ว่าเป็นอีกฉบับที่สามารถนำมาปรับใช้กับเรื่องการให้การรับคุ้มครองในข้อมูลบุคคลได้ เนื่องจากมีการให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลไว้ซึ่งได้วางหลักไว้ในบทบัญญัติว่า “ผู้ใดเป็นเจ้าพนักงานมีหน้าที่ในการไปรษณีย์โทรเลข หรือโทรศัพท์กระทำการอันมิชอบด้วยหน้าที่ โดยเปิด หรือยอมให้ผู้อื่นเปิดจดหมาย หรือ สิ่งอื่นที่ส่งทางไปรษณีย์ หรือโทรเลขทำให้เสียหายทำลายทำให้สูญหาย หรือยอมให้ผู้อื่นทำให้เสียหายทำลายทำให้สูญหาย ซึ่งจดหมาย หรือสิ่งอื่นที่ส่งทางไปรษณีย์ หรือโทรเลขกักส่งให้ผิดทาง หรือส่งให้แก่บุคคล ที่งรู้ว่ามิใช่เป็นผู้ควรรับซึ่งจดหมาย หรือสิ่งอื่นที่ส่งทางไปรษณีย์ หรือโทรเลข หรือ เปิดเผยข้อความที่ส่งทางไปรษณีย์ทางโทรเลข หรือทางโทรศัพท์” หรือ “ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สามโดยประการที่น่าจะทำให้ผู้อื่นนั้น เสียชื่อเสียงถูกดูหมิ่น หรือ ถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาทต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ”

อย่างไรก็ตาม ประมวลกฎหมายอาญาก็ไม่ได้มุ่งคุ้มครองเฉพาะเรื่องข้อมูลส่วนบุคคลโดยตรง ซึ่งบุคคลที่จะได้รับการคุ้มครองก็ต่อเมื่อเกิดความเสียหายขึ้นแล้วเท่านั้น ทั้งนี้ เนื่องจากหลักการและมาตรการต่าง ๆ ที่กำหนดไว้เป็นการเยียวยาแก่ความเสียหายที่เกิดขึ้นมากกว่าการป้องกันความเสียหาย ซึ่งเป็นหลักการและมาตรการดังกล่าวนี้ ยังมีความขัดแย้งกับหลักการสากลเรื่องการคุ้มครองข้อมูลส่วนบุคคลตามระบบกฎหมายของต่างประเทศที่มุ่งจะให้การคุ้มครองในลักษณะ “ป้องกัน” ทั้งยังขาด หลักเกณฑ์เกี่ยวกับวิธี การเงื่อนไข และมาตรการที่สำคัญจำเป็นและเฉพาะเจาะจง อันเป็นหลักประกันในการให้ความคุ้มครองข้อมูลส่วนบุคคลได้อย่างเพียงพอตามแนวปฏิบัติของหลักสากล[28]

---

[28] พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 26) พุทธศักราช 2560. มาตรา 163.

“ ผู้ใดเป็นเจ้าพนักงาน มีหน้าที่ในการไปรษณีย์ โทรเลข หรือโทรศัพท์ กระทำการอันมิชอบด้วยหน้าที่ดังต่อไปนี้

(1) เปิด หรือยอมให้ผู้อื่นเปิด จดหมาย หรือสิ่งอื่นที่ส่งทางไปรษณีย์ หรือโทรเลข

(2) ทำให้เสียหาย ทำลาย ทำให้สูญหาย หรือยอมให้ผู้อื่นทำให้เสียหาย ทำลายหรือทำให้สูญหาย ซึ่งจดหมาย หรือสิ่งอื่นที่ส่งทางไปรษณีย์ หรือโทรเลข

3.1.5 มาตรการทางกฎหมายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พุทธศักราช 2544 แก้ไขเพิ่มเติม (ฉบับที่ 4) พุทธศักราช 2562

การติดต่อสื่อสารมีแนวโน้วปรับเปลี่ยนวิธีการ โดยอาศัยศักยภาพของการพัฒนาการทางเทคโนโลยีของอิเล็กทรอนิกส์ ซึ่งให้ความสะดวกรวดเร็วและมีการประมวลผลได้อย่างประสิทธิภาพมากขึ้น แต่การทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวนี้ ได้มีความแตกต่างจากวิธีการทำธุรกรรมที่มีกฎหมายให้การรองรับไว้อยู่ในปัจจุบัน ซึ่งเป็นการรองรับสถานะในทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้มีความเสมอเท่ากับการทุรกรรมเป็นหนังสือ หรือการมีหลักฐานเป็นหนังสือ การรับรองด้วยวิธีการส่งข้อมูล และรับข้อมูลทางอิเล็กทรอนิกส์นี้

วิธีการนี้ใช้ลายมือชื่ออิเล็กทรอนิกส์ รวมทั้งเรื่องของการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความที่น่าเชื่อถือ และให้มีผลบังคับในทางกฎหมายเช่นเดียวกับการทำธุรกรรมกับวิธีการทั่วไป เช่นเดียวที่เคยปฏิบัติในรูปแบบของกระดาษกันมา เพื่อส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ ทั้งนี้ เพื่อการส่งเสริมและการพัฒนาการทางเทคโนโลยีให้มีการพัฒนาศักยภาพตลอดและมีมาตรฐานที่น่าเชื่อถือ ตลอดจนสามารถเสนอแนะแนวทางในการแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้องภายในประเทศและระหว่างประเทศด้วยมาตรการในการตรากฎหมายรองรับให้เป็นรูปธรรม และสอดคล้องกับมาตรฐานสากลยอมรับ

นอกจากนี้แล้ว ตามพระราชบัญญัติดังกล่าวยังได้กำหนดให้เพิ่มบทนิยามคำว่า “การพิสูจน์และยืนยันตัวตน” และคำว่า “ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล” ระหว่างบทนิยามคำว่า “ระบบข้อมูล” และคำว่า “ระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติ” ในมาตรา 3 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พุทธศักราช 2544 ซึ่งได้แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พุทธศักราช 2562[29]

---

(3) กัก ส่งให้ผิดทาง หรือส่งให้แก่บุคคลซึ่งรู้ว่ามิใช่เป็นผู้ควรรับซึ่งจดหมาย หรือสิ่งอื่นที่ส่งทางไปรษณีย์ หรือโทรเลข หรือ

(4) เปิดเผยข้อความที่ส่งทางไปรษณีย์ ทางโทรเลข หรือทางโทรศัพท์ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

[29] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พุทธศักราช 2562. มาตรา 3.

ให้เพิ่มบทนิยามคำว่า “ระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติ” ระหว่างบทนิยามคำว่า “ระบบข้อมูล” และคำว่า “การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์” ในมาตรา 4 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พุทธศักราช 2544 “ระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติ ” หมายความว่า โปรแกรมคอมพิวเตอร์หรือวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอัตโนมัติอื่น ที่ใช้เพื่อที่จะทำให้เกิดการกระทำ หรือการตอบสนองต่อข้อมูลอิเล็กทรอนิกส์หรือการปฏิบัติการใด ๆ ต่อระบบข้อมูล ไม่ว่าทั้งหมด หรือแต่บางส่วน โดย

“การพิสูจน์และยืนยันตัวตน” หมายความว่า กระบวนการพิสูจน์และการยืนยันความถูกต้องของตัวบุคคล”

“ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล” หมายความว่า เครือข่ายทางอิเล็กทรอนิกส์ที่เชื่อมโยงข้อมูลระหว่างบุคคลใด ๆ หรือหน่วยงานของรัฐเพื่อประโยชน์ในการพิสูจน์และยืนยันตัวตนและการทำธุรกรรมอื่น ๆ ที่เกี่ยวเนื่องกับการพิสูจน์และยืนยันตัวตน”

พระราชบัญญัติฉบับนี้ ใช้บังคับแก่ธุรกรรมในทางแพ่งและพาณิชย์ที่ดำเนินการ โดยใช้ข้อมูลอิเล็กทรอนิกส์ เว้นแต่ ธุรกรรมที่มีพระราชกฤษฎีกากำหนดมิให้นำพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับ รวมถึงให้ใช้บังคับแก่การทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐด้วย เช่น การประกาศ คำสั่งทางปกครอง คำขอการอนุญาต การจดทะเบียน การชำระเงิน หรือการดำเนินการใด ๆ ของหน่วยงานภาครัฐ หรือโดยได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับกฎหมายในเรื่องนั้นกำหนดตามมาตรา 35

คำว่า “ลายมือชื่ออิเล็กทรอนิกส์” ตามพระราชบัญญัตินี้ หมายความว่า “ตัวอักษร ตัวอักขระ ตัวเลขเสียง หรือสัญลักษณ์อื่นใด ที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์” แล้วสามารถนำมาประกอบใช้กับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงว่าผู้ใช้มีความสัมพันธ์ระหว่างกับข้อมูลอิเล็กทรอนิกส์ เพื่อวัตถุประสงค์ในการระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องและเชื่องโยงกับข้อมูลอิเล็กทรอนิกส์นั้นตามมาตร 3

สรุปลักษณะของความหมาย “ลายมือชื่ออิเล็กทรอนิกส์” ตามกฎหมายฉบับนี้ได้ดังนี้

เป็นลายพิมพ์นิ้วมือ แกงได อักษร อักขระ ตัวเลข เสียง หรือตราประทับ สัญลักษณ์อื่นใดในรูปของอิเล็กทรอนิกส์มีความหมายต่างจากลายมือชื่อตามกฎหมายเดิมคือ ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 9

วัตถุประสงค์หรือหน้าที่ของลายมือชื่ออิเล็กทรอนิกส์ คือ เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้นและเพื่อแสดงว่าบุคคลดังกล่าวยอมรับในข้อมูลอิเล็กทรอนิกส์นั้นแม้ว่าจะมีการใช้ลายมือชื่ออิเล็กทรอนิกส์ข้างต้นก็ตาม แต่ลายมือชื่ออิเล็กทรอนิกส์ที่จะถือเป็นลายมือชื่อที่มีผลทางกฎหมาย จะต้องปฏิบัติตามเงื่อนไขสำคัญ 2 ประการตามมาตรา 9 ดังนี้

ประการที่หนึ่ง ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อและสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตนและ

ปราศจากการตรวจสอบ หรือการแทรกแซงโดยบุคค]ธรรมดาในแต่ละครั้งที่มีการดำเนินการหรือแต่ละครั้งที่ระบบได้สร้างการตอบสนอง”

ประการที่สอง วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อม หรือข้อตกลงของคู่กรณี[30]

ลักษณะของลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือได้ ดังมาตราที่เกี่ยวข้อง คือ มาตรา 25 มาตรา 26 และมาตรา 29 คู่กรณีที่เกี่ยวข้องยังสามารถใช้วิธีการใด ๆ ที่เข้าลักษณะและเงื่อนไขของกฎหมายได้ แม้ว่ากฎหมายจะกำหนดลักษณะของลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือได้ แต่ก็ไม่ควรจำกัดการใช้เทคโนโลยีใดโดยเฉพาะตามหลักการเรื่อง (Technology neutrality) คือ การไม่ถือเอาเทคโนโลยีหนึ่งเทคโนโลยีใดเป็นเกณฑ์พิจารณาความน่าเชื่อถือว่าของลายมือชื่ออิเล็กทรอนิกส์ อีกทั้งบทบัญญัติมาตรา 26 ก็หาได้ระบุจำกัดวิธีการหนึ่งวิธีการใดไว้ไม่

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์เป็นกฎหมายที่มีขึ้นเพื่อรองรับ ในเรื่องตราประทับอิเล็กทรอนิกส์ อันเป็นสิ่งซึ่งสามารถระบุตัวผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ได้เช่นเดียวกันกับลายมือชื่อ โดยหากจะให้เอกสารทางอิเล็กทรอนิกส์ต้องมีการประทับตราในหนังสือย่อมก่อให้เกิดอุปสรรคอย่างมาก นอกจากนี้ พระราชบัญญัติดังกล่าวยังได้กำหนดเรื่องต้นฉบับให้สามารถนำเอกสาร ซึ่งเป็นสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์มาใช้แทนต้นฉบับ หรือเป็นพยานหลักฐานในศาลได้ โดยในเรื่องเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้อาศัยอำนาจตามตามมาตรา 6 มาตรา 8 และ มาตรา 8 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พุทธศักราช 2549 ออกประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ พุทธศักราช 2553 โดยประกาศดังกล่าว สามารถแบ่งสาระสำคัญออกเป็นสองส่วนมีรายละเอียด ดังนี้[31]

---

[30] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พุทธศักราช 2562. มาตรา 9.

[31] พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พุทธศักราช 2549

มาตรา 6 “ในกรณีที่มีการรวบรวมจัดเก็บใช้ หรือเผยแพร่ข้อมูลหรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคลไม่ว่าโดยตรงหรือโดยอ้อมให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย”

มาตรา 7 “แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศและต้องได้รับความเห็นชอบจากคณะกรรมการ หรือหน่วยงานที่คณะกรรมการมอบหมายจึงมีผลใช้บังคับได้

หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ”

มาตรา 8 “ให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติ หรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ไว้เป็นตัวอย่างเบื้องต้นสำหรับการ

โดยประกาศดังกล่าวสามารถแบ่งสาระสำคัญออกเป็นสองส่วนมีรายละเอียด ดังนี้

เพื่อให้ผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐทราบว่าหน่วยงานมีนโยบายในการจัดการข้อมูลส่วนบุคคลอย่างไร และเพื่อให้ผู้ใช้บริการสามารถตัดสินใจเกี่ยวกับข้อมูลส่วนบุคคลของตนเองได้ ประกาศดังกล่าวจึงกำหนดให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ต้องจัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร และต้องมีสาระสำคัญที่จะกล่าวดังต่อไปนี้[32]

การจัดเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด โดยหน่วยงานของรัฐต้องใช้ใช้วิธีที่ชอบด้วยกฎหมายและเป็นธรรม โดยได้รับความยินยอม หรือแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบแล้วแต่กรณี

การจัดเก็บข้อมูลส่วนบุคคลต้องเป็นไปตามวัตถุประสงค์ในการดำเนินงานและตามอำนาจหน้าที่ของหน่วยงานรัฐนั้น

หน่วยงานของรัฐต้องบันทึกวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลในเวลาที่มีการจัดเก็บและรวบรวม รวมถึงการนำข้อมูลไปใช้ภายหลัง ในกรณีที่หน่วยงานของรัฐเปลี่ยนแปลงวัตถุประสงค์ให้หน่วยงานของรัฐต้องทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน

ห้ามหน่วยงานของรัฐเปิดเผย แสดง หรือทำให้ปรากฏโดยประการอื่นซึ่งข้อมูลส่วนบุคคลที่ไม่สอดคล้องกับวัตถุประสงค์ในการเก็บรวบรวมและจัดเก็บข้อมูลส่วนบุคคล เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นกรณีที่มีกฎหมายกำหนดไว้

หน่วยงานของรัฐต้องมีมาตรการในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลเพื่อป้องกันมิให้ข้อมูลนั้นสูญหาย ถูกการเข้าถึง ถูกทำลาย ใช้ แปลง หรือแก้ไข หรือถูกเปิดเผยโดยมิชอบ

หน่วยงานของรัฐต้องดำเนินการให้มีการเปิดเผยการดำเนินการ แนวปฏิบัติ และนโยบายเกี่ยวกับข้อมูลส่วนบุคคล รวมถึงวิธีการที่สามารถตรวจดูความมีอยู่ ลักษณะของข้อมูลส่วนบุคคล วัตถุประสงค์ของการนำข้อมูลไปใช้ ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล

ดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้วหน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบทั้งนี้โดยให้คำนึงถึงความถูกต้องครบถ้วนความน่าเชื่อถือสภาพความพร้อมใช้งานและความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์"

[32] คณะกรรมการธุรกรรมอิเล็กทรอนิกส์. (2553). ***แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ พ.ศ. 2553.*** กรุงเทพฯ: คณะกรรมการธุรกรรมอิเล็กทรอนิกส์. หน้า 31-37.

เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอหน่วยงานของรัฐต้องแจ้งถึงผู้ควบคุมข้อมูลส่วนบุคคลความมีอยู่ หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูล เมื่อได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคลภายในเวลาอันสมควร

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามมาตรการที่ได้กล่าวมาแล้วเพื่อให้การดำเนินตามนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานของประกาศฉบับนี้

หน่วยงานของรัฐต้องจัดให้มีแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อให้บุคคลากรของหน่วยงานนั้นปฏิบัติตาม โดยแนวปฏิบัตินี้ต้องมีสาระสำคัญดังต่อไปนี้ด้วย

ข้อมูลเบื้องต้นประกอบด้วย ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลรายละเอียดการบังคับใช้นโยบายการคุ้มรองข้อมูลส่วนบุคคลนั้น และหากมีการเปลี่ยนแปลงวัตถุประสงค์ หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้หน่วยงานของรัฐแจ้งการเปลี่ยนแปลงให้เจ้าของข้อมูลทราบ และขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนทุกครั้ง เช่น

การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล การแสดงระบุความเชื่อมโยงข้อมูลส่วนบุคคลกับหน่วยงานอื่น

หากหน่วยงานของรัฐได้รวบรวมรวมข้อมูลส่วนบุคคลมาจากหลายแหล่งหน่วยงานของรัฐต้องระบุในนโยบายคุ้มครองข้อมูลส่วนบุคคลถึงเจตนารมณ์การรวมข้อมูล

หากมีบุคคลอื่นใช้ หรือ เปิดเผยข้อมูลแก่บุคคลอื่น หน่วยงานของรัฐต้องระบุว่ามีบุคคลอื่นที่จะเข้าถึง หรือใช้ข้อมูลนั้นได้ และต้องระบุว่าการเข้าถึงใช้ หรือเปิดเผยนั้นสอดคล้องกับข้อกำหนดตามกฎหมายของหน่วยงานรัฐที่ดำเนินการดังกล่าวอีกด้วย

ระบุถึงสิทธิของผู้ใช้บริการที่จะสามารถเลือกว่าจะให้หน่วยงานของรัฐรวบรวม จัดเก็บหรือไม่จัดเก็บ ใช้หรือไม่ให้ใช้ และเปิดเผย หรือไม่ให้เปิดเผยข้อมูลของตนในกรณีที่มีการนำข้อมูลไปใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ของการเก็บรวบรวม

หน่วยงานของรัฐต้องกำหนดวิธีการให้ผู้ใช้สามารถเข้าถึงและแก้ไข หรือปรับปรุงข้อมูลเกี่ยวกับตนเองที่หน่วยงานรวบรวม และจัดเก็บในเว็บไซต์ให้ถูกต้อง

หน่วยงานของรัฐต้องจัดให้มีมาตรรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

หน่วยงานของรัฐต้องระบุข้อมูลติดต่อที่ผู้ใช้บริการสามารถติดต่อกับหน่วยงานของรัฐได้ ซึ่งอย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้ ชื่อและที่อยู่ หมายเลขโทรศัพท์ หมายเลขโทรสาร ที่อยู่จดหมายอิเล็กทรอนิกส์[33]

การยอมรับข้อความในรูปข้อมูลอิเล็กทรอนิกส์ (E-signature) ดังนี้

---

[33] คณะกรรมการธุรกรรมอิเล็กทรอนิกส์. อ้างแล้วเชิงอรรถที่ 32. หน้า 31-37

การสร้าง E-signature ด้วยวิธีการที่ปลอดภัยและน่าเชื่อถือได้ ด้วยเหตุที่กฎหมายรองรับในความน่าเชื่อถือตามมาตรา 9 หลัก (E-signature) และลายมือชื่อที่เชื่อถือได้ตาม (มาตรา 9 ประกอบด้วย 26) ก็เพราะเหตุผลหลักสามประการอันได้แก่[34]

ข้อมูลที่ใช้สร้าง E-signature นั้นเชื่อมโยงไปยังเจ้าของได้ การอยู่ภายใต้การควบคุมของเจ้าของในตอนที่สร้าง และ ผู้เป็นเจ้าของสามารถตรวจพบการเปลี่ยนแปลงหรือการปลอมแปลงใด ๆ ได้ นับจากสร้าง เช่น การสร้าง Digital signature (ที่ใช้เทคโนโลยีเข้ารหัสตามที่ได้กล่าวในข้างต้น) และไบโอเมตริกซ์ (Biometrics)

ตัวอย่างเช่น

การยอมรับลายมือชื่ออิเล็กทรอนิกส์ของกฎหมายว่าเป็น (E-signature) ที่น่าเชื่อถือและปลอดภัย เช่น การใช้ไบโอเมตริกซ์ (Biometrics) เป็น (E-signature) นั้น หากพิจารณาตามองค์ประกอบของกฎหมาย อาจพิจารณาได้สามประการดังนี้

การแปลงอัตลักษณ์ของบุคคลให้อยู่ในรูปแบบอิเล็กทรอนิกส์ ย่อมมีความเชื่อมโยงไปยังเจ้าของอัตลักษณ์เฉพาะของบุคคลนั้นได้ เช่น ลายนิ้วมือ ย่อมอยู่ภายใต้การควบคุมของเราเสมอในเวลาที่สร้าง เพราะแต่ละบุคคลย่อมมีลักษณะเฉพาะดังกล่าวที่แตกต่างกัน

การตรวจสอบการเปลี่ยนแปลงสามารถทำได้เนื่องจากเป็นลักษณะเฉพาะของแต่ละบุคคล โดยซอฟต์แวร์ (Software) ที่ดำเนินการเกี่ยวข้องจะไม่ดำเนินการให้ หากมิใช่เจ้าของอัตลักษณ์นั้น ซึ่งลักษณะดังกล่าวเกิดนับแต่ได้มีการสร้าง ไบโอเมตริกซ์ (Biometrics) นั้น

ดังนั้น แม้ลายมือชื่ออิเล็กทรอนิกส์ (E-signature) จะไม่ได้ทำลงบนกระดาษและอาจไม่มีรูปแบบทางกายภาพ (Physical form) ที่มีการจับต้องได้นั้น อย่างเช่น ลายมือชื่อที่ใช้ปากกา แต่ความน่าเชื่อถือของเอกสารที่ใช้ E-signature ในบางกรณี โดยเฉพาะอย่างยิ่งในรูปแบบที่ใช้วิธีการที่น่าเชื่อถือและปลอดภัย อาจมีมากกว่าการใช้ปากกาเซ็น

พระราชธุรกรรมอิเล็กทรอนิกส์ ฉบับที่ 3 พุทธศักราช 2562 การพิสูจน์ตัวตนผู้ใช้บริการต้องแสดงตนต่อผู้ให้บริการเช่นมีการพิสูจน์ตัวตนการใช้ควายินยอมการลงลายมือชื่อหรือการแสดงเจตนาของผู้ทำธุรกรรม โดยหลักการเพราะระบบธุรกรรมอิเล็กทรอนิกส์ มีดังนี้[35]

ให้มีการพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้โดยให้แจ้งเงื่อนไขเกี่ยวกับความน่าเชื่อถือให้ผู้ใช้บริการทราบล่วงหน้า

ให้มีการตราพระราชกำหนดให้ผู้ให้บริการพิสูจน์และยืนยันตัวตนทางดิจิตอลเป็นธุรกิจที่ต้องขออนุญาตและกำหนดไม่มีคณะกรรมการกำกับดูแลเป็นการเฉพาะก็ได้

---

[34] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พุทธศักราช 2562. มาตรา 9 ประกอบมาตรา 26.

[35] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562 . มาตรา 9.

ผู้ประกอบธุรกิจระบบการพิสูจน์และยืนยันตัวตนทางดิจิตอลที่ไม่ได้รับอนุญาตตามพระราชกฤษฎีกา (ถ้ามี) จะมีโทษทางอาญา

พระราชธุรกรรมอิเล็กทรอนิกส์ (ฉบับที่4) ประกาศเมื่อ 22 พฤษภาคม 2562 โดยพระราชกฤษฎีกากำหนดให้ผู้ให้บริการระบบอิเล็กทรอนิกส์ต้องขออนุญาต (ถ้ามี) กำหนดหลักเกณฑ์เพื่อกำกับดูแลผู้ให้บริการระบบอิเล็กทรอนิกส์เพื่อให้กระบวนการพิสูจน์และยืนยันตัวตนทางดิจิตอลเป็นไปอย่างถูกต้องครบถ้วน

ระบบการพิสูจน์และยืนยันตัวตนทางดิจิตอล (platform)[36]

ผู้ให้บริการของระบบการพิสูจน์และยืนยันตัวตนระหว่างขั้นตอนที่ขอใบอนุญาตจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ระบบทำการแทน (Proxy server)

การให้บริการระบบทำการแทนแก่ผู้ที่ประสงค์จะเข้าสู่แพลตฟอร์ม (platform) แต่ไม่มีมาตรฐานเทคนิคทางเทคโนโลยีเพียงพอ เพื่อให้สามารถเชื่อมต่อกับแพตฟอร์ม (platform) ผ่านระบบทำการแทน หรือระบบ (Proxy server)ได้

การคุ้มครองข้อมูลส่วนบุคคลมาตรฐานการเข้ารหัสข้อมูล หลักเกณฑ์การส่งผ่านข้อมูลระหว่างแพลตฟอร์ม (platform) และรวมถึงอำนาจในการเรียกผู้ที่เกี่ยวข้องมาให้ข้อมูล หรือระบบ (Proxy server) พิจารณาคำอุทธรณ์ของผู้ได้รับความเสียหาย[37]

ดังนั้น พระราชธุรกรรมอิเล็กทรอนิกส์ ไม่ได้กำหนดกรอบขั้นตอนการพิสูจน์และยืนยันตัวตนทางดิจิทัลไว้ แต่เปิดช่องให้สามารถออกพระราชกฤษฎีกาได้ เพื่อให้สอดคล้องกับเทคโนโลยีที่มีความเปลี่ยนแปลงอย่างรวดเร็ว หลักการของ “ลายมือชื่ออิเล็กทรอนิกส์” สิ่งที่ใช้เชื่อมโยงเพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในรูปข้อมูลอิเล็กทรอนิกส์ (E-signature) ตามมาตรา 9 การลงทะเบียนขอใช้ระบบถือเป็นการเชื่อมโยงผู้ใช้กับ (User Account และ Password) ที่ได้รับมาเมื่อผู้ใช้ทำการ (log in) โดยการใช้ (User account และ Password) ระบบจะสามารถระบุว่า ใครทำการยืนยันตัวตนเข้ามาสู่ระบบ โดยข้อสังเกต (User account และPassword) เป็นความลับควรมีเพียงเจ้าของเท่านั้นที่ทราบ

---

[36] ศูนย์วิจัยกสิกรไทย. (2561). ***เผย ร่าง พระราชบัญญัติ Digital ID ปูทางให้ไทยก้าวเข้าสู่ยุคอิเล็กทรอนิกส์อย่างเต็มตัว.*** (ออนไลน์). เข้าถึงได้จาก: https://www.moneyandbanking.co.th. [2562, 29 กรกฎาคม].

[37] เรื่องเดียวกัน, (ออนไลน์).

3.1.6 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562

ภายใต้กฎหมายพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562 ฉบับนี้ เป็นมาตรการป้องกัน และลดความเสี่ยงจากภัยคุมคามที่ส่งผลต่อความมั่นคงของหน่วยงานภาครัฐ เศรษกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ ซึ่งปัจจุบันเทคโนโลยีได้เข้ามามีส่วนร่วมในชีวิตประจำวันของบุคคลทั้งในการทำงาน หรือเรื่องส่วนตัวหากเกิดภัยคุมคามทางไซเบอร์ ที่จะส่งผลต่อความมั่นคงภายในประเทศไม่ว่าจะเป็นหน่วยงานภาครัฐ หรือรวมทั้งองค์กรภาคเอกชน ดังนั้น ประเทศต่าง ๆ รวมทั้งประเทศไทยจึงต้องมีกฎหมายเพื่อรองรับกับปัญหาที่จะเกิดขึ้นอันเป็นมาตรการป้องกัน เมื่อมีเหตุที่ส่งผลกระทบต่อความมั่นคงภายในประเทศ หากมีอาชญากรรมทางคอมพิวเตอร์แฮคเจาะระบบคอมพิวเตอร์เข้าไปควบคุมฐานข้อมูลภายในองค์กรรัฐและหน่วยงานเอกชนก่อให้เกิดความเสียหายต่อประชาชนได้ โดยปกติความปลอดภัยทางไซเบอร์จะเกี่ยวกับทั้งหมดของเทคโนโลยีไม่ว่าจะเป็นทั้งฮาร์ดแวร์ (Hardware) หรือ ซอฟต์แวร์ (Software) ซึ่งความปลอดภัยทางไซเบอร์ (Cyber security) เป็นส่วนหนึ่งของเทคโนโลยี กระบวนการและตัวชี้วัดที่จะออกแบบการป้องกันทั้งรายบุคคล และทั้งองค์กรเพื่อลดความเสี่ยงจากการโจมตีทางไซเบอร์ (Cyber Attack)[38]

ความหมายของ “ภัยคุกคามทางไซเบอร์” ว่าเป็นการกระทำ หรือการดำเนินการใด ๆ โดยมิชอบ ซึ่งใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายก่อให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามกฎหมายเพื่อรักษาสถานะของข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ ที่เกี่ยวข้องกับระบบคอมพิวเตอร์เฉพาะเท่าที่จำเป็น เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

กรณีที่เกี่ยวข้องกับความมั่นคงของรัฐบาล จำกัดเฉพาะภัยคุกคามไซเบอร์ที่มีลักษณะผสมทั้งสองประเภท กล่าวคือ คุกคามต่อความมั่นคงต่อระบบ และส่งผลไปถึงความมั่นคงของรัฐบาลด้วย เช่น ส่งโปรแกรมไป เพราะคำว่า “ข้อมูลคอมพิวเตอร์อันเป็นเท็จ”[39] ตามเจตนารมณ์ หมายถึง การปลอมแปลง

---

[38] ปรัชญา ฮวดปากน้ำ. (2559). ***ยุทธศาสตร์การพัฒนากำลังพลของกองทัพไทยเพื่อต่อต้านภัยคุกคามไซเบอร์ในทศวรรษหน้า.*** เอกสารงานวิจัยวิทยาลัยเสนาธิการทหาร รุ่นที่ ๕๗ สถาบันวิชาการป้องกันประเทศ. หน้า 14.

[39] สฤณี อาชวานันกุล. (2019). ***พ.ร.บ. ไซเบอร์: เมื่อหลักความมั่นคงไซเบอร์แพ้ทัศนคติ “ความมั่นคง 0.4”***. (ออนไลน์). เข้าถึงได้จาก: https://thaipublica.org/2019/03/cybersecurity-principles-lost-national-security/. [2562, 29 กรกฎาคม]

ข้อมูลคอมพิวเตอร์เพื่อหลอกลวง หรือ (Phishing) เท่านั้น แต่ปรากฏว่า“ข้อมูลคอมพิวเตอร์” (Data) หมายถึงข้อความ (Speech) หรือเนื้อหา (Content) ที่ถูกโพสต์ออนไลน์ ซึ่งกลายเป็นบรรทัดฐานในการใช้กฎหมายฉบับนี้

“ภัยคุกคามทางไซเบอร์” ได้นิยามไว้ในมาตรา 3[40] ว่า “การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้

---

[40] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562. มาตรา 3.

ในพระราชบัญญัตินี้

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการ หรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระท าหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติขอดาวเทียม และระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป “หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

“ประมวลแนวทางปฏิบัติ” หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ

เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับสถานการณ์ หรือเหตุการณ์ใดก็ตามที่น่าจะส่งผลกระทบทางลบต่อความมั่นคงปลอดภัยของเครือข่ายและระบบข้อมูล

การกำหนดลักษณะของภัยคุกคามทางไซเบอร์ ซึ่งความชัดเจนพบว่าเป็นภัยคุกคามต่อ “ระบบ” เท่านั้น โดยแบ่งออกเป็น 3 ระดับ ดังต่อไปนี้

ระดับที่หนึ่ง เป็นภัยคุกคามทางไซเบอร์ในระดับเฝ้าระวัง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่อาจก่อให้เกิดความเสียหาย แต่ยังไม่ก่อให้เกิดผลกระทบต่อบุคคล ทรัพย์สิน หรือข้อมูลที่เกี่ยวข้องที่สำคัญในระดับร้ายแรง

ระดับที่สอง เป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามในระดับร้ายแรงที่มีลักษณะดังต่อไปนี้

ภัยคุกคามที่ก่อให้เกิดความเสี่ยงที่จะทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือการให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ภัยคุกคามที่ก่อให้เกิดความเสี่ยงภัยจนอาจทำให้คอมพิวเตอร์ระบบคอมพิวเตอร์ที่ให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เกี่ยวข้องกับภัยคุกคามต่อความมั่นคงของรัฐ การป้องกันประเทศ ความสัมพันธ์ระหว่างประเทศ เศรษฐกิจ การสาธารณสุขความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชน ถูกแทรกแซงอย่างมีนัยสำคัญ หรือถูกระงับการทำงาน

ระดับที่สาม ภัยคุกคามที่มีความรุนแรงที่ก่อ หรืออาจก่อให้เกิดความเสียงภัย หรือความเสียหายต่อบุคคล หรือต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่สำคัญหรือมีจำนวนมาก

ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะดังต่อไปนี้

ภัยคุกคามทางไซเบอร์ หรือเป็นเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ในกรณีฉุกเฉินเร่งด่วน ที่ใกล้จะเกิด และส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศสาธารณูปโภคขั้นพื้นฐาน ความมั่นคงของรัฐ หรือชีวิตความเป็นอยู่ของประชาชน

ภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อความมั่นคงของรัฐ หรือกระทบต่อความสงบเรียบร้อยของประชาชน หรือประเทศอาจตกอยู่ในสภาวะคับขัน หรือมีความจำเป็นต้องมีมาตรการ

ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ”

อย่างเร่งด่วน ในการปฏิบัติตามกฎหมาย เพื่อความปลอดภัยของประชาชนจำต้องแก้ไขเยียวยาความเสียหายที่เกิดจากภัยพิบัติสาธารณะที่ฉุกเฉินและมีความร้ายแรง เพื่อคงรักษาป้องกันความเป็นเอกราชและบูรณภาพแห่งอาณาเขตและผลประโยชน์ของประเทศชาติ[41]

---

[41] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562. มาตรา 60.

"การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์คณะกรรมการจะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้

(3) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

(2) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุขความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหายจนไม่สามารถทำงานหรือให้บริการได้

(3) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การท างานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบ หรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศ หรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้าย ตามประมวลกฎหมายอาญา การรบ หรือการสงคราม ที่จำเป็นต้องมมีมาตรการเร่งด่วนในการรักษาไว้ซึ่งการปกครองประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นพระประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย

การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน

“คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กมช.” หรือ “กกม.” ซึ่งมีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็น เพื่อเป็นการป้องกันการคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการเฝ้าระวังคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง[42]

การตรวจสอบคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

การดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์ เพื่อจัดการข้อบกพร่อง หรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่

การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง”

[42] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562. มาตรา 65.

“ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการ ดังต่อไปนี้

(1) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง

(2) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(3) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่อง หรือกำจัดชุดคำสั่งไม่พึงประสงค์หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่

(4) รักษาสถานะของข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(5) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์ในกรณีมีเหตุจำเป็นที่ต้องเข้าถึงข้อมูลตาม (5) ให้ กกม. มอบหมายให้เลขาธิการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่งดำเนินการตามคำร้องทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

การรักษาสถานะของข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

การเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์ โดยให้ กปช. หรือ กกซ. มอบหมายให้เลขาธิการยื่นคำร้องต่อศาลที่มีเขตอำนาจ เพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง หรือผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่งดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำ หรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรงในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

ในกรณีจำเป็นเร่งด่วน เจ้าหน้าที่สามารถใช้อำนาจได้โดยไม่ต้องขอหมายศาล โดยใช้อำนาจสภาความมั่นคงแห่งชาติในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กปช. หรือ กกซ. มีอำนาจปฏิบัติการ หรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็น เพื่อป้องกันการคุกคามทางไซเบอร์ในเรื่องดังนี้[43]

---

[43] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562. มาตรา 66.

ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ในเรื่องดังต่อไปนี้

(1) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของ หรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(2) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(3) ทดสอบการทำงานของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

(4) ยึด หรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบ หรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์ หรือผู้ครอบครองโดยทันที หลังจากเสร็จสิ้นการตรวจสอบ หรือวิเคราะห์ในการดำเนินการตาม (2) (3) และ (4) ให้ กกม. ยื่นคำร้องต่อศาลที่มี

การเข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของ หรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

การเข้าถึงทรัพย์ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศ หรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้อง หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

การทดสอบการทำงานของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้อง หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายใน หรือใช้ประโยชน์จากคอมพิวเตอร์ หรือระบบคอมพิวเตอร์นั้น

การยึด หรืออายัดคอมพิวเตอร์ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็น ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบ หรือวิเคราะห์ ทั้งนี้ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์ หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบ หรือวิเคราะห์

สำหรับการดำเนินการตาม (3) และ (4) ให้ กปช. หรือ กกซ. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำ หรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรงในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

สำหรับผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้ และในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายนี้

หมวด 4 บทกำหนดโทษ กำหนดข้อปฏิบัติ ข้อห้าม และบทกำหนดโทษสำหรับพนักงานเจ้าหน้าที่และพนักงานสอบสวนรวมถึงหน่วยงานโครงสร้างพื้นฐานและบุคคลที่เกี่ยวข้อง[44]

เขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำ หรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

[44] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562. มาตรา 70.

"ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผย หรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

บทเฉพาะกาลกำหนดให้ในวาระเริ่มแรกที่ยังไม่มีการจัดตั้งสำนักงานให้นายกรัฐมนตรีอาศัยอำนาจตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พุทธศักราช 2562 จัดตั้งสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติชั่วคราว และแต่งตั้งคณะกรรมการผู้ทรงคุณวุฒิ หรือดำเนินการอื่นใดเป็นการชั่วคราวกำหนดให้ กปช. ขอให้ข้าราชการ พนักงาน หรือลูกจ้างของส่วนราชการรัฐวิสาหกิจหรือองค์กรอื่นของรัฐมาปฏิบัติงานในสำนักงานเป็นการชั่วคราวได้ทั้งนี้ เมื่อพระราชบัญญัตินี้ใช้บังคับ ให้รัฐมนตรี (นายกรัฐมนตรี) เสนอคณะรัฐมนตรีดำเนินการเพื่ออนุมัติให้มีการโอนบรรดาอำนาจหน้าที่ กิจการ ทรัพย์สิน สิทธิ หนี้และงบประมาณของบรรดาภารกิจที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติชั่วคราว ไปเป็นของสำนักงานตามพระราชบัญญัตินี้[45]

ความมั่นคงในแง่ไซเบอร์ หมายถึง ความมั่นคงของระบบและข้อมูลและการใช้งานคอมพิวเตอร์ ไว้ตามหลักเกณฑ์ 3 ประการเรียกว่า “CIA”[46] คือ ความลับ (Confidentiality) บูรณภาพ (Integrity) ความพร้อมใช้ (Availability) ภัยคุกคามต่อความมั่นคง คือ การโจมตีใด ๆ ที่กระทบถึงคุณสมบัติการเจาะเข้าถึงฐานข้อมูลของหน่วยงานราชการ กระทบต่อความลับ การส่งมัลแวร์ทำลายหรือแก้ไขข้อมูลกระทบต่อบูรณภาพ การโจมตีทำให้ระบบใช้การไม่ได้ เช่น เว็บล่ม หรือ (DDOS) กระทบต่อความพร้อมใช้

ความมั่นคงไซเบอร์ จึงไม่จำต้องเกี่ยวข้องกับภาครัฐ บุคคลใดที่ใช้คอมพิวเตอร์ก็ย่อมต้องการความมั่นคงของรัฐบาล ภัยคุกคามต่อความมั่นคงประเภทนี้ เกิดจากหลายสาเหตุและไม่จำเป็นต้อง

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือผู้กระท าความผิดตามกฎหมายอื่นหรือเพื่อประโยชน์ในการด าเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ”

[45] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562. มาตรา 78.

“ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วยประธานกรรมการและกรรมการตามมาตรา 5 (1) (2) และให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นกรรมการและเลขานุการเพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อน และให้ดำเนินการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของคณะกรรมการตามมาตรา 5 (3) ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

ในการแต่งตั้งกรรมการผู้ทรงคุณวุฒิตามวรรคหนึ่ง รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอาจเสนอรายชื่อบุคคลต่อคณะรัฐมนตรี เพื่อพิจารณาแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิดังกล่าวด้วยได้”

[46] คณาธิป ทองรวีวงศ์. (2562). ***ตอบทุกข้อสงสัย พระราชบัญญัติมั่นคงไซเบอร์ นิยามความมั่นคงคืออะไร คุกคามเสรีภาพจริงหรือไม่ แล้วทำไมคนมากมายถึงต้องกังวล***. (ออนไลน์). เข้าถึงได้จาก: https://thestandard.co/thailands-cyber-law/. [2562, 29 กรกฎาคม]

เกี่ยวกับไซเบอร์ หรือระบบคอมพิวเตอร์ก็ได้ เช่น การก่อการร้ายแบบวางระเบิด การจลาจลแบบใช้อาวุธ หรือส่งโปรแกรมไปควบคุมเครื่องบินที่คณะรัฐมนตรีโดยสารให้ตกทะเล เป็นต้น

ดังนั้น เมื่อพิจารณาตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562 ในการให้อำนาจเจ้าหน้าที่องค์กรที่ได้จัดตั้งขึ้น ตามพระราชบัญญัติฉบับนี้ โดยการอิงการป้องกัน “ภัยคุกคามทางไซเบอร์” การมีอำนาจดังกล่าว จึงกลายเป็นการล้วงล้ำความไม่ปลอดภัยในสิทธิความเป็นส่วนตัวของประชาชนจนเกินไป จากคำนิยามของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562 หมายถึง การโจมตีระบบคอมพิวเตอร์เท่านั้น แต่ปรากฏว่ามาตรา 25 ได้บัญญัติขยายความหมายของภัยคุกคามไซเบอร์กว้างขึ้น โดยแบ่งเป็น 3 ระดับ ได้แก่[47]

ระดับแรก ระดับการเฝ้าระวัง เป็นภัยคุกคามไซเบอร์ที่ทำให้ระบบคอมพิวเตอร์ใช้คอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของหน่วยงานรัฐด้อยประสิทธิภาพลง

ระดับสอง ระดับร้ายแรงเป็นภัยคุกคามไซเบอร์ที่มีการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ที่มีผลทำให้ระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการให้บริการด้านความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณสุข หรือความสงบสุขเรียบร้อยของประชาชน ไม่สามรถทำงาน หรือให้บริการได้

ระดับสุดท้าย ระดับวิกฤตเป็นภัยคุกคามจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ที่ส่งผลกระทบรุนแรงเป็นวงกว้าง ทำให้หน่วงงานของรัฐ การให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐควบคุมไม่ได้ อันกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศ หรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน โดยจะแบ่งตามระดับความรุนแรงดังกล่าวนี้ ซึ่งจะมีผลทำให้เจ้าหน้าที่รัฐมีอำนาจเพิ่มขึ้นด้วยเช่นกัน

หากเจ้าหน้าที่ผู้ไม่มีเจตนาดี อาจตีความคำว่า “ภัยคุกคามไซเบอร์” ครอบคลุมถึงประเด็น “เนื้อหา” ในระบบบนโลกออนไลน์มากว่าเรื่องการคุกคามในระบบคอมพิเตอร์ โดยที่เจ้าหน้าที่รัฐสามารถขอดูข้อมูล เอกสาร หรือสำเนาข้อมูลที่อยู่ในการครบครองของผู้อื่นได้ ซึ่งไม่สอดคล้องกับสัญญาการให้บริการ ซึ่งจะระบุชัดเจนว่า ห้ามไม่ให้ผู้ให้บริการเปิดเผยข้อมูลลับกับบุคคลอื่น เท่ากับว่าเป็นข้อยกเว้นหลักสัญญาและกฎหมายละเมิด แม้ว่าจะเป็นข้อยกเว้นความผิดในกฎหมายไทยก็ตาม แต่ขณะเดียวกันอาจผิดต่อกฎหมายสัญญาอื่นนอกเหนือนจากสัญญาในประเทศไทย

---

[47] อนุรักษ์ นิยมเวช. (2562). ***การรักษาความมั่นคงปลอดภัยไซเบอร์ที่ภาคธุรกิจและประชาชนควรรู้***. (ออนไลน์). เข้าถึงได้จาก: http://www.anurakbusinesslaw.com/www.anurakbusinesslaw.com/Article_files/Articles/2015/18_CYBER.html . [2562, 28 พฤศจิกายน]

อาจผิดต่อสัญญาผู้ประกอบการธุรกิจต่างประเทศได้ ผู้วิจัยเห็นว่ากฎหมายฉบับนี้ กระทบต่อสิทธิมนุษยชนและสิทธิส่วนบุคคล เพราะกฎหมายไซเบอร์ได้ให้อำนาจในการล้วงรู้ข้อมูลส่วนบุคคล การดักฟังและฐานข้อมูลไซเบอร์ หรือขอให้ผู้ให้บริการส่งข้อมูลต่าง ๆ ให้แก่รัฐได้ หากผู้บังคับใช้กฎหมายมีลักษณะอำนาจนิยมอาจสอดส่องพฤติกรรมต่าง ๆ ของประชาชน ซึ่งการเก็บข้อมูลไบโอเมตริกซ์ได้ถูกเก็บไว้ในฐานข้อมูลออนไลน์นั้นอาจส่งผลกระทบภาคธุรกิจได้

3.1.7 มาตรการทางกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562

"การคุ้มครอง" ข้อมูลส่วนบุคคลในความสำคัญของกฎหมายฉบับนี้ อันเป็นการจัดการข้อมูลส่วนบุคคลอย่างเหมาะสมและเพียงพอ ข้อมูลทั้งหมดจะต้องได้รับการประมวลผลอย่างเป็นธรรมและถูกต้องตามกฎหมายข้อมูลที่ได้รับจะต้องเป็นไปตามวัตถุประสงค์ที่ระบุไว้อย่างถูกต้องตามกฎหมายและจะไม่สามารถดำเนินการในลักษณะใดก็ตามที่เป็นกันขัดต่อวัตถุประสงค์ดังกล่าว การเก็บรวมรวมข้อมูลจะต้องมีความเกี่ยวข้องอย่างเพียงพอและไม่มากเกินไป ซึ่งจะต้องสัมพันธ์กับวัตถุประสงค์เดิมที่เป็นเหตุผลในการเก็บรวบรวมข้อมูลเหล่านั้นเป็นข้อมูลที่มีความถูกต้องและเป็นปัจจุบัน ไม่ควรเก็บข้อมูลไว้นานเกินความจำเป็น หากข้อมูลได้ทำหน้าที่ตามวัตถุประสงค์เป็นที่เรียบร้อยแล้ว ข้อมูลจะต้องถูกลบ หรือถูกทำลาย ยกเว้นในกรณีที่มีเหตุผลอื่น ๆ ที่จำเป็นจะต้องเก็บรักษา ซึ่งจะต้องเป็นไปตามที่กฎหมายกำหนดเป็นการประมวลผลข้อมูลตามสิทธิประโยชน์ของแต่ละบุคคล ข้อมูลจะต้องถูกเก็บไว้ในที่ ๆ ปลอดภัย จากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหาย หรือถูกทำลายโดยไม่ตั้งใจ

เมื่อมีความจำเป็นต้องขอใช้ข้อมูลส่วนบุคคล ทั้งนี้ ก็เพื่อป้องกันความเสี่ยงที่จะมีผลกระทบไปถึงการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ที่ก่อให้เกิดแนวโน้มให้เกิดผลกระทบเชิงลบหรือความเสียหายในระดับบุคคล หรือองค์กร ความน่าเชื่อถือในมาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศมีผลกระทบต่อการค้าระหว่างประเทศและการทำธุรกิจระหว่างประเทศ หากประเทศไทยไม่มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ย่อมทำให้เสียโอกาสและความเชื่อมั่นจากกลุ่มประเทศต่าง ๆ และอาจรวมไปถึงการตื่นตัวเรื่อง (Data Protection)[48] เพราะเหตุการณ์ใหญ่ ๆ ที่เกิดขึ้นแล้ว เช่น การรั่วไหลของข้อมูลส่วนบุคคลของผู้ใช้เฟซบุ๊กหลายล้านบัญชี เป็นต้น

---

[48] Ingram Micro Thailand. (2018). ***Data Protection – ความสำคัญของการป้องกันข้อมูล.*** (ออนไลน์). เข้าถึงได้จาก: https://medium.com/ingrammicroth/data-protection. [2562, 29 กรกฎาคม]

กฎระเบียบใหม่ที่สหภาพยุโรปกำหนดนั้น แสดงให้เห็นถึงการป้องกันข้อมูล (Data protection) โดยการโอนอำนาจจาก “ผู้ควบคุมข้อมูล” (Data Controller) และ “ผู้ประมวลผลข้อมูล” (Data Processor) ให้เป็น “บุคคลที่เป็นเจ้าของข้อมูล” (Data Subject) สำหรับวิธีการที่จะนำมาใช้ในการประมวลผลข้อมูลโดยเจ้าของข้อมูลเอง และข้อมูลใดบ้างที่เจ้าของข้อมูลจะสามารถรวบรวมและเก็บไว้ได้[49]

หากพิจารณาข้อมูลส่วนตัวดังกล่าวนี้ สามารถพิจารณาได้ทั้งในด้านสิทธิตามกฎหมายหรือสิทธิตามหลักศีลธรรม จริธรรม รวมถึงความเป็นส่วนตัวดังต่อไปนี้ เช่น

ด้านความเป็นส่วนตัวในร่างกาย เช่น การใช้ประโยชน์จากการโยกย้ายถ่ายเทจากอวัยวะเนื้อเยื่อ ของเหลวที่ได้จากร่างกายของตนโดยปราศจากการได้ยิน

ด้านความเป็นส่วนตัวในพฤติกรรมครอบคลุมถึงพฤติกรรมการกระทำทั้งในที่ลับและที่แจ้งของตน เช่น การลักลอบบันทึกเสียงในห้องน้ำหญิงซึ่งไม่มีความผิดในทางกฎหมาย เพราะเครื่องบันทึกเป็นของส่วนตัวไม่มีกฎหมายอาญาใดที่จะเอาโทษจากการบันทึกเสียงในกรณีดังกล่าว จึงไม่มีความผิดทางกฎหมาย แต่การเอาข้อความในคลิปเสียงมาเผยแพร่ ถ้าข้อความนั้นก่อให้เกิดความเสียหายต่อบุคคลนั้นผิดฐานหมิ่นประมาท[50]

ด้านความเป็นส่วนตัวในการติดต่อสื่อสารกับบุคคลอื่นผ่านทางสื่อต่าง ๆ อย่างเป็นอิสระโดยไม่ถูกลักลอบดักฟัง หรืออยู่ในสายตาหน่วยงานองค์กรนิติบุคคลใด ๆ หรือปัจเจกบุคคล เช่น การลักลอบดักฟังทางโทรศัพท์

ด้านความเป็นส่วนตัวในข้อมูล ชื่อ ที่อยู่ ข้อมูลสุขภาพ ข้อมูลการเงิน ข้อมูลไบโอเมตริกซ์ เป็นต้น อันเป็นการบ่งชี้ถึงความเป็นตัวตนของปัจเจกบุคคลย่อมต้องเป็นสมบัติของบุคคลนั้น จะต้องไม่ถูกเผยแพร่ต่อบุคคลอื่นหน่วยงาน หรือสาธารณชนและบุคคลนั้นย่อมมีสิทธิที่จะควบคุมการใช้ประโยชน์แก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคลของตนเองได้

การที่จะนำข้อมูลไบโอเมตริกซ์มาใช้ เพื่อบ่งชี้ความเป็นตัวตนที่แท้จริงของบุคคลมากขึ้นในปัจจุบัน จึงเกิดความเสี่ยงในการถูกคุกคามความเป็นส่วนตัวก็มากขึ้นได้เช่นกัน เช่น การดำเนินชีวิตประจำวันสามารถถูกตรวจสอบได้ง่ายว่าได้กระทำกิจกรรมอะไรบ้างในแต่ละวัน นอกจากนี้ข้อมูลในรูปแบบของดิจิทัลสามารถกระทำซ้ำ หรือถูกถ่ายโอนผ่านเครือข่ายระบบคอมพิวเตอร์ไปสู่

---

[49] ETDA สพธอ. (2018). ***GDPR: Practical Guideline เพื่อปรับตัวให้เข้ากับแนวทางการคุ้มครองข้อมูลส่วนบุคคลในกระแสโลก***. (ออนไลน์). เข้าถึงได้จาก: https://www.etda.or.th/content/gdpr-practical-guideline-knowledge-sharing-class.html. [2562, 29 กรกฎาคม].

[50] ประมวลกฎหมายอาญา. มาตรา 326.

บุคคลอื่นหรือไปสู่สาธารณชนได้ง่ายขึ้น ซึ่งไวต่อการเสียหายมากกว่าข้อมูลรูปแบบอื่น ๆ สาระสำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 มีดังต่อไปนี้[51]

นิยามคำว่า “ข้อมูลส่วนบุคคล” หมายถึง สิ่งที่ระบุข้อมูลที่ทำให้ระบุ หรืออาจระบุตัว ของบุคคลนั้น (Identified and Identifiable) ได้ไม่ว่าจะทางตรง หรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

การกำหนดสิทธิเจ้าของข้อมูล ให้ผู้ใช้มีสิทธิเข้าถึงข้อมูลส่วนตัวของตน พร้อมเปิดเผยที่มาของข้อมูล รวมถึงมีสิทธิแก้ไขข้อมูลให้ถูกต้อง และให้สิทธิ์เจ้าของข้อมูลระงับการใช้ข้อมูล หรือทำลายข้อมูลของตนได้

เมื่อมีการละเมิดข้อมูลส่วนบุคคล โดนแฮคเกอร์ หรือข้อมูลรั่วไหล ผู้ให้บริการต้องรีบแจ้งให้เจ้าของข้อมูลทราบ พร้อมรายงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลถึงมาตรการเยียวยา

3.1.7.1 มาตรการในการคุ้มครองข้อมูลส่วนบุคคล

หลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลไว้ว่า การเก็บรวมรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลของผู้ใด จะทำได้ก็ต่อเมื่อเจ้าของข้อมูลได้ให้ความยินยอมไว้ โดยการขอความยินยอมต้องทำเป็นหนังสือ อาจจะทำผ่านระบบอิเล็กทรอนิกส์ก็ได้ ต้องมีแบบหรือมีข้อความที่เข้าใจได้ใช้ภาษาอ่านง่าย ให้เจ้าของข้อมูลมีอิสระในการตัดสินใจว่าจะยินยอมให้เก็บข้อมูล หรือนำข้อมูลไปใช้ได้ หรือไม่ โดยไม่เป็นเงื่อนไขในการให้บริการผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อน หรือในขณะนั้น เว้นแต่ บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้[52]

---

[51] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 6.

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคล หรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคล หรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลทั้งนี้ บุคคล หรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“บุคคล” หมายความว่า บุคคลธรรมดา

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

[52] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 19.

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบ หรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวง หรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว

การขอความยินยอมต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลให้เจ้าของข้อมูลทราบด้วย และตามมาตรา 21 ก็กำหนดว่า ผู้ควบคุมข้อมูลจะต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเฉพาะตามวัตถุประสงค์ที่ได้แจ้งไว้ สำหรับเจ้าของข้อมูลที่ได้ให้

"ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำโดยชัดแจ้งเป็นหนังสือ หรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบ หรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวง หรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมาย หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้ว โดยชอบตามที่กำหนดไว้ในหมวดนี้

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ในหมวดนี้ ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้"

ความยินยอมไปแล้ว ถ้าหากเปลี่ยนใจจะถอนความยินยอมของตนเมื่อใดก็ได้ตามมาตรา 23[53] โดยต้องแจ้งผลกระทบในการถอนคำยินยอมเมื่อเจ้าของข้อมูลไม่ประสงค์จะดำเนินการใด ๆ อีกไปตามมาตรา 19 วรรคหก

แม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ได้วางหลักการไว้ว่าเจ้าของข้อมูลต้องให้ “ความยินยอม” ทุกกรณีบุคคลอื่นถึงจะสามารถเข้ามาเกี่ยวกับข้อมูลได้ แต่ขณะเดียวกันก็ยังได้กำหนดข้อยกเว้นไว้ โดยเฉพาะกิจประการสำคัญ ๆ ของรัฐซึ่งสามารถที่เข้ามายุ่งเกี่ยวกับข้อมูลของประชาชนได้รับการยกเว้นไว้ โดยไม่ต้องขอความยินยอมจากประชาชนก่อน และกลับกลายเป็นการเข้าถึงข้อมูลโดยไม่ต้องขอความยินยอมที่มีกฎหมายรองรับด้วย โดยการกำหนดข้อยกเว้นแบ่งได้เป็น 3 ระดับ ดังนี้

ระดับหนึ่ง ยกเว้น ไม่ต้องถูกบังคับโดยกฎหมายฉบับนี้ ดังบัญญัติไว้ในมาตรา 4 กำหนดประเภทกิจการที่พระราชบัญญัตินี้จะไม่ใช้บังคับไว้ 6 ประเภท ดังนี้[54]

---

[53] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 23.

“ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(1) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้ หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา 24 ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา หรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม”

[54] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 4.

“พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตน หรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

ประเภทที่หนึ่ง การเก็บข้อมูล การใช้ข้อมูล และการเปิดเผยข้อมูล เพื่อประโยชน์ของตัวเองหรือกิจกรรมในครอบครัว

ประเภทที่สอง การดำเนินงานของหน่วยงานของรัฐที่มีหน้าที่รักษาความมั่นคงของรัฐ ซึ่งรวมถึง ความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับ การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

ประเภทที่สาม การเปิดเผยข้อมูลส่วนบุคคลเพื่อกิจการสื่อมวลชน ศิลปกรรม หรือวรรณกรรมตามจริยธรรมของวิชาชีพเพื่อประโยชน์สาธารณะ

ประเภทที่สี่ การทำงานของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา ในการพิจารณาตามอำนาจหน้าที่ ซึ่งองค์กรของรัฐสภามีอำนาจหน้าที่พิจารณาให้ความเห็นชอบบุคคลเพื่อดำรงตำแหน่งสำคัญ ๆ ด้วย

ประเภทที่ห้า การพิจารณาคดีของศาล และเจ้าหน้าที่ในกระบวนการยุติธรรม

ประเภทที่หก การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิก[55]

ดังนั้น จะเห็นว่า กิจการที่ไม่ต้องอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นมีมาก ซึ่งเรียกได้ว่า ข้อมูลของประชาชนที่เกี่ยวกับข้อมูลของตัวเองบนโลกออนไลน์ซึ่งได้รับการยกเว้น ที่ไม่ต้องปฏิบัติตามกฎหมายฉบับนี้ ถูกบัญญัติไว้แล้ว ไม่ว่าจะเป็นงานสอดส่องประชาชนของหน่วยงานความมั่นคง หรือการเปิดเผยข้อมูลโดยสื่อมวลชน ซึ่งบุคคลที่เกี่ยวข้องสามารถเข้ามาเก็บข้อมูลของประชาชนและนำไปใช้ได้โดยไม่ต้องขอความยินยอมก่อน และเจ้าของข้อมูลก็ไม่อาจจะทราบเลยก็ได้ว่า ข้อมูลของตัวเองถูกนำไปใช้อย่างไรบ้าง โดยเฉพาะกิจการที่ไม่ต้องอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นมีหลากหลาย โดยทั่วไป การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วน

---

(3) บุคคล หรือนิติบุคคลซึ่งใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น

(4) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าวซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎรวุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดีการบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต”

[55] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 4.

บุคคล ส่วนใหญ่มักจัดทำขึ้นเพื่อประโยชน์ในการใช้ในธุรกรรมของนิติบุคคล หรือการให้บริการของภาครัฐ เช่น

ผู้ให้บริการในทางด้านโทรคมนาคม จะต้องทำการเก็บข้อมูลที่เกี่ยวข้องและเชื่อมโยงไปยังตัวของบุคคล เช่น ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ หรือข้อมูลส่วนบุคคลอื่น ๆ ที่จำเป็นเพื่อประโยชน์ในการเรียกชำระเงิน หรือให้บริการทางด้านโทรศัพท์ หรือบริการด้านอื่น ๆ ได้โดยหน่วยงาน หรือบริษัทเหล่านี้ มักจะมีลักษณะการเก็บ รวบรวมข้อมูลที่เรียกว่า "(Customer Identifiable)" กล่าวคือ ข้อมูลที่มีการเชื่อมโยงไปถึงตัวบุคคลนั้น โดยตามความเข้าใจของบุคคลโดยทั่วไปแล้ว ผู้ใช้บริการทางอิเล็กทรอนิกส์นั้น ว่าข้อมูลนั้นเป็นของตนจะไม่ถูกนำไปเผยแพร่ หรือนำไปใช้เพื่อวัตถุประสงค์อย่างอื่น เช่น ชื่อ นามสกุล ที่อยู่ เลขประจำตัวประชาชน หมายเลขโทรศัพท์ รวมถึงข้อมูลที่เกี่ยวข้องกับกิจกรรมทางด้านธุรกรรมออนไลน์ของตน เช่น การขออีเมล์ฟรี การใช้บริการในการสั่งซื้อสินค้า การโอนเงินผ่านสมาร์ทโฟน หมายเลขโทรศัพท์ฟรี แต่ปรากฏว่า ข้อมูลส่วนบุคคลต่าง ๆ เหล่านี้ ในความเป็นจริงล้วนแล้วเป็นข้อมูลที่เกี่ยวข้องและเชื่อมโยงมาถึงยังตัวขอลบุคคลได้ทั้งนั้น โดยอาจถูกล่วงละเมิดสิทธิเหล่านี้ได้ ซึ่งผู้เป็นเจ้าของข้อมูลเองก็ไม่อาจทราบได้

ระดับที่สอง ข้อยกเว้นการให้เก็บข้อมูล ใช้ข้อมูล โดยไม่ต้องขอความยินยอมก่อน ตามข้อยกเว้นในมาตรา 4[56] ได้ให้ไว้นั้น ไม่ต้องปฏิบัติตามกฎหมายนี้แล้ว แต่ยังคงมีกิจการของภาครัฐที่แทบจะไม่ต้อง "ขอความยินยอม" เมื่อกระทำการใช้ข้อมูล เพราะมาตรา 24[57] และ มาตรา 27[58]

---

[56] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 4.

[57] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 24.

"ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลท าการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย หรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามค าขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีค วามสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล"

ข้อยกเว้นไว้ว่า การเก็บข้อมูลและใช้ข้อมูลในกิจการต่อไปนี้ ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลก็ได้ ไว้ 6 ประเภท ดังนี้

ประเภทที่หนึ่ง เพื่อการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิของเจ้าของข้อมูล

ประเภทที่สอง เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

ประเภทที่สาม เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูล

ประเภทที่สี่ เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

ประเภทที่ห้า เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าว จะมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานที่มีอยู่ในข้อมูลของเจ้าของข้อมูลส่วนบุคคล

ประเภทที่หก เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

สำหรับข้อยกเว้นนั้น เพื่อป้องกันอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ เป็นเรื่องที่จำเป็นในกรณีที่ต้องช่วยชีวิตของบุคคลนั้น ๆ อาจมีความจำเป็นจะต้องเข้าถึงข้อมูลที่เกี่ยวข้องทางด้านสุขภาพ เช่น ประวัติของการแพ้ยา กรุ๊ปเลือด เป็นต้น แต่มาตรา 24 ได้บัญญัติเปิดช่องไว้โดยใช้คำว่า “สุขภาพของบุคค” ไม่ได้คุ้มครองเฉพาะ “สุขภาพของเจ้าของข้อมูล” ซึ่งเป็นเรื่องของตนเอง ดังนั้นมาตรา 24 ก็เปิดช่องให้นำข้อมูลของบุคคลหนึ่ง นำไปใช้เพื่อประโยชน์ทางสุขภาพของบุคคลอื่นได้ด้วยนั้นเอง

สำหรับข้อยกเว้น เมื่อพิจารณาจากถ้อยคำที่ว่า “การดำเนินภารกิจเพื่อประโยชน์สาธารณะ” หรือ “ปฏิบัติหน้าที่ในการใช้อำนาจรัฐ” หรือ “การปฏิบัติตามกฎหมาย” ดังจะเห็นได้ว่าความหมายอย่างกว้าง เพราะกิจการของรัฐทุกประเภทก็จะเป็นกิจการเพื่อประโยชน์สาธารณะและ

---

[58] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 27.

“ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

บุคคล หรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการตามมาตรา 39”

เป็นการปฏิบัติหน้าที่ตามที่กฎหมายให้อำนาจไว้ทั้งหมด ในส่วนการ “ปฏิบัติหน้าที่ในการใช้อำนาจรัฐ” นั้นยังรวมถึงกิจการที่ภาครัฐมอบอำนาจให้เอกชนเข้าร่วมดำเนินการบางประเภทด้วย เช่นเดียวกัน จึงหมายถึงกิจการของรัฐและที่รัฐได้มอบหมายให้เอกชนกระทำการแทนทั้งหมด หรือบางส่วนก็ได้รับการยกเว้น การเก็บข้อมูลและการใช้ข้อมูลไม่ต้องขอความยินยอมจากเจ้าของข้อมูลก่อนได้[59]

อย่างไรก็ตาม หากเจ้าของข้อมูลไม่ต้องการถูกเก็บข้อมูล หรือถูกใช้ข้อมูลโดยกิจการของภาครัฐก็อาจต้องยกข้อต่อสู้ว่า การเข้ามายุ่งเกี่ยวกับข้อมูลส่วนบุคคลนั้น ๆ “เป็นการจำเป็น” หรือไม่ และกฎหมายที่ให้อำนาจในการปฏิบัตินั้น การกำหนดขอบเขตการเก็บข้อมูลไว้ชัดเจน หรืออย่างกว้าง หรือไม่เพียงใด เมื่อเทียบกับหลักการทั่วไปในมาตรา 19 ของกฎหมายฉบับนี้

ระดับที่สาม สำหรับข้อมูลที่อ่อนไหว ยกเว้นไว้ให้เพื่อ “ประโยชน์สาธารณะที่สำคัญ”

สำหรับข้อมูลส่วนบุคคลบางประเภทที่มีความอ่อนไหวพิเศษ เพราะการที่บุคคลอื่นเข้าถึงข้อมูลเหล่านี้อาจจะนำไปสู่อันตรายต่อเจ้าของข้อมูล หรือนำไปสู่การเลือกปฏิบัติ อาจเกิดการกีดกันที่ไม่เป็นธรรมได้ เช่น ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ เป็นต้น ซึ่งเป็นข้อมูลที่มีความอ่อนไหวง่ายจะต้องได้รับการคุ้มครองอีกระดับหนึ่งเป็นพิเศษ

ข้อมูลประเภทที่มีความละเอียดอ่อนตามมาตรา 26 ได้บัญญัติให้ความคุ้มครองไว้เพียงว่าผู้อื่นจะเก็บข้อมูลเหล่านี้นั้น ได้ต้องได้รับ “ความยินยอมโดยชัดแจ้ง” จากเจ้าของข้อมูลก่อน ซึ่งกฎหมายยังมิได้ให้คำนิยามเอาไว้ว่า ความยินยอมโดยชัดแจ้งต่างจากความยินยอมในกรณีปกติอย่างไร เพราะการยินยอมในกรณีปกติก็ต้องเป็นการยินยอมที่ต้องทำเป็นหนังสือเช่นเดียวกัน

แต่อย่างไรก็ตาม ในมาตรา 26 และมาตรา 27 ได้บัญญัติข้อยกเว้นไว้อีกหลายประการ เช่น การเก็บข้อมูลและการใช้ข้อมูลที่มีความอ่อนไหวพิเศษในกิจการต่อไปนี้ โดยไม่ต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลแต่อย่างไร

กรณีเพื่อป้องกัน หรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ไม่ว่าด้วยเหตุใด ๆ ก็ตาม

การดำเนินกิจการขององค์กรไม่แสวงหาผลกำไร เช่น มูลนิธิ สมาคม ที่ทำงานด้านการเมือง ศาสนา ปรัชญา สหภาพแรงงานให้แก่สมาชิก หรือผู้ที่ติดต่ออย่างสม่ำเสมอ และองค์กรนั้น ๆ

---

[59] ยลพรรณ สีตะระโส. (2559). ***ปัญหาการคุ้มครองข้อมูลพันธุกรรมมนุษย์ในประเทศไทย.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. หน้า 44.

วัตถุประสงค์ดังกล่าวเป็นไปโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร

กรณีเป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลเอง

กรณีมีความจำเป็นเพื่อก่อตั้งสิทธิเรียกร้อง หรือการดำเนินคดี การต่อสู้คดีตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

กรณีจำเป็นในการปฏิบัติตามกฎหมาย เพื่อประเมินความสามารถของลูกจ้างในการทำงาน การวินิจฉัยโรคทางการแพทย์ การให้บริการสุขภาพ การรักษาทางการแพทย์ การป้องกันโรคติดต่อ การคุ้มครองแรงงาน สวัสดิการรักษาพยาบาล การวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ เป็นต้น และเพื่อประโยชน์สาธารณะที่สำคัญ โดยจัดให้มีมาตรการคุ้มครองข้อมูลที่เหมาะสม[60] เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพ หรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพ หรือวิชาชีพ หรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์ เช่น

การป้องกันด้านสุขภาพจากโรคติดต่ออันตราย หรือโรคระบาดที่อาจติดต่อ หรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐาน หรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสม และเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลไว้ โดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่ หรือตามจริยธรรมแห่งวิชาชีพ

การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิ หรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลตามที่

---

[60] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 26.

คณะกรรมการประกาศกำหนด โดยประโยชน์สาธารณะที่สำคัญ ต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ข้อมูลชีวภาพตามวรรคหนึ่งให้หมายถึงข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิค หรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ

ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม ต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด[61]

3.1.7.2 สิทธิของเจ้าของข้อมูลส่วนบุคคล

กฎหมายได้บัญญัติการรับรองสิทธิเจ้าของข้อมูลให้สามารถถึงเข้าข้อมูลของตนได้ เพื่อแก้ไขข้อมูลที่ไม่ถูกต้อง หรือแจ้งให้หน่วยงานที่ดูแลควบคุมข้อมูลดังกล่าวดำเนินการแก้ไขเพิ่มเติม ที่ไม่ถูกต้อง หรือไม่เป็นปัจจุบันครบถ้วนสมบูรณ์ภายใต้กำหนดของกฎหมาย[62]

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอมตามมาตรา 30

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอตามวรรคหนึ่ง จะปฏิเสธคำขอได้เฉพาะในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล และการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

เมื่อเจ้าของข้อมูลส่วนบุคคลนั้น มีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม่อาจปฏิเสธคำขอนั้นได้ตามวรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่ได้รับคำขอ[63]

เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ตามมาตรา 32 ดังต่อไปนี้

กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 (4) หรือ (5) เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่า

---

[61] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 26.

[62] ชนาเทพ คิ้วเที่ยง. (2555). ***การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกิจ***.วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขาวิชากฎหมายธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม. หน้า 75.

[63] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 30.

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลได้แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อวัตประสงค์เกี่ยวกับการตลาดแบบตรง

กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไปได้ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติโดยแยกส่วนออกจากข้อมูลอื่นอย่างชัดเจนในทันทีเมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งการคัดค้านให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ[64]

3.1.7.3 ผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลข้อมูลส่วนบุคคลมีหน้าที่แจ้งและจัดให้มีมาตรรักษาด้านความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าว เมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ต่อสำนักงานโดยไม่ชักช้า ภายใน 72 ชั่วโมง เว้นแต่ การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลตามมาตรา 37[65]

---

[64] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 32.

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

" ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

(4) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่ การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิด

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ตาม มาตรา 40 ดังต่อไปนี้

การดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ รวมทั้งแจ้งให้ตผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

การจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม (1) สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

ความใน (3) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่ มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของผู้เป็นเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีหน้าที่ดังต่อไปนี้

หน้าที่ต้องแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานทราบ ตามมาตรา 41 วรรคห้า โดยคณะกรรมการอาจกำหนดคุรสมบัติของเจ้าที่คุ้มครองข้อมูลส่วนบุคคลได้ โดยคำนึงถึงความรู้ หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 41 วรรคหก[66]

ให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด”

[66] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 41.

คำจำกัดความและหน้าที่ของผู้เกี่ยวข้องกับการประมวลผลข้อมูลหลักไว้ 3 ประเภท ดังนี้[67]

ประเภทที่หนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคล (Controller) คือ กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล ซึ่งโดยส่วนมากจะเป็นผู้ขอความยินยอมจากเจ้าของข้อมูล เช่น ผู้ให้บริการเว็บไซต์ต่าง ๆ

ประเภทที่สอง ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor) คือ ผู้ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์และวิธีการของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งในทางปฏิบัติอาจเป็นบุคคลเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลก็ได้ อนึ่ง “การประมวลผลข้อมูล” (Processing) นี้ไม่ใช่เพียงแค่การวิเคราะห์ หรือจัดการข้อมูลแบบทั่วไปเท่านั้น แต่ให้รวมถึงการบันทึกและจัดเก็บข้อมูลด้วย

ประเภทที่สาม เจ้าของข้อมูลส่วนบุคคล (Data Subject)

ดังนั้น การประมวลผลของข้อมูลจะชอบด้วยกฎหมายหรือไม่นั้น จำต้องพิจารณาจาก “ความยินยอม” (Consent) ซึ่งเป็นหัวใจสำคัญของการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ฉบับนี้

3.1.7.4 บทกำหนดโทษแพ่งและโทษทางอาญา

ข้อมูลส่วนบุคคลก็คือทรัพย์สิน ไม่ว่าจะเป็น ชื่อ นามสกุล บ้านเลขที่ หมายเลขโทรศัพท์ และเรื่องราวทั้งหมดของบุคคลหนึ่งล้วนเป็นทรัพย์สินของคน ๆ นั้น เมื่อสำคัญเช่นนี้แล้วจึงมีประเด็นว่าจะคุ้มครองอย่างไรไม่ให้ใครสามารถเอาข้อมูลส่วนตัวไปใช้โดยไม่แจ้งเจ้าของข้อมูล และถ้าได้ไปแล้ว เช่น รัฐเอาข้อมูลส่วนบุคคลไปแล้วจะมีมาตรการดูแลปกป้องอย่างไร ว่าจะใช้ไปในทางที่ชอบ หรือผู้มีหน้าที่จัดเก็บต้องรักษามาตรฐานความปลอดภัย และเมื่อมีความเสี่ยง หรือเกิดความเสียหายจะต้องได้รับผลอย่างไรนั้น ดังได้บัญญัติบทลงโทษไว้ในมาตราดังต่อไปนี้ เช่น

ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืน หรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจ หรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ตามมาตรา 77 ว่า[68]

---

[67] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2012). ***กฎหมาย GDPR ฉบับรวบรัด.*** (ออนไลน์). เข้าถึงได้จาก: https://www.etda.or.th/content/gdpr-in-a-nutshell. [2562, 29 พฤศจิกายน]

[68] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 77.

ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำ หรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็น เพื่อใช้ในการป้องกันความเสียหายที่กำลังจะเกิดขึ้น หรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่ง หรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5,000,000 บาท หรือทั้งจำทั้งปรับตามมาตรา 79[69]

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่ง หรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเอง หรือผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับความผิดตามมาตรานี้เป็นความผิดอันยอมความได้

ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ฉบับนี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับตามมาตรา 80

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผย ในกรณีดังต่อไปนี้[70]

การเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐในประเทศ หรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

3.1.7.5 โทษทางปกครอง

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 26 วรรคหนึ่ง หรือวรรคสาม หรือฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 หรือส่ง หรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่ง หรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาทตามมาตรา 84[71]

---

[69] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 79.

[70] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 80.

[71] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 84.

ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดส่ง หรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 วรรคหนึ่ง หรือวรรคสาม โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่ง หรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาทตามมาตรา 87[72]

ด้วยเหตุดังกล่าวนี้ แม้ว่าจะได้มีบทบัญญัติได้ให้การคุ้มครองข้อมูลชีวมาตร Biometrics ตามมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 แต่ยังมีประเด็นในการบังคับใช้กับหน่วยงานของรัฐ เนื่องจากปัจจุบันมีหน่วยงานรัฐหลายแห่งมีการใช้อำนาจรัฐในการบังคับการเก็บข้อมูลชีวมาตรของประชาชนทุกคน โดยที่ไม่ได้มีการพิจารณาเหตุผลและความจำเป็นอย่างรอบคอบและอาจจะมิได้มีการคำนึงถึงผลกระทบที่จะเกิดกับเจ้าของข้อมูลชีวมาตรส่วนบุคคลในกรณีที่เกิดการรั่วไหลหรือถูกนำไปใช้ในทางที่มิชอบโดยเจ้าหน้าที่ของรัฐเอง นอกจากนี้ ยังพบว่าหน่วยงานรัฐที่มีการบังคับเก็บข้อมูลชีวมาตรของประชาชนได้มีการสัมปทานให้แก่บริษัทเอกชนเข้ามาเป็นผู้บริหารจัดการฐานข้อมูลชีวมาตรที่อยู่ในความรับผิดชอบของหน่วยงานของภาครัฐ ซึ่งอาจทำให้มีความสุ่มเสี่ยงที่เอกชน ที่ได้รับการสัมปทานอาจมีการนำข้อมูลเหล่านี้ ไปหาประโยชน์ในทางมิชอบ ซึ่งผลกระทบในกรณีที่มีการรั่วไหล หรือละเมิดข้อมูลชีวมาตรที่อยู่ในความรับผิดชอบของหน่วยงานภาครัฐ ซึ่งไม่ได้มีเพียงแค่ผลกระทบต่อเจ้าของข้อมูลชีวมาตรเท่านั้น แต่ยังรวมไปถึงผลกระทบต่อความน่าเชื่อถือและภาพพลักษณ์ของประเทศ ในด้านความมั่นคงของประเทศและผลกระทบต่อนโยบายการขับเคลื่อนเศรษฐกิจดิจิทัลของรัฐบาลได้ ดังจะได้พิจารณาบทกำหนดโทษดังนี้

สำหรับโทษในกรณีไม่ปฏิบัติตามพระราชบัญญัติฉบับนี้แบ่งได้ 3 ประเภท ได้แก่ โทษทางปกครอง โทษทางแพ่ง และโทษทางอาญา

โทษทางแพ่ง กล่าวคือ เป็นค่าเสียหายที่ผู้ประกอบธุรกิจอาจต้องชดใช้ให้แก่เจ้าของข้อมูลในกรณีที่การไม่ปฏิบัติตามพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ทั้งนี้แม้ว่า การกระทำนั้นจะไม่ได้เกิดจากความจงใจหรือประมาทเลินเล่อก็ตาม เว้นแต่ผู้ประกอบธุรกิจจะสามารถยกข้อต่อสู้ตามกฎหมายขึ้นอ้างได้ ศาลสั่งให้ผู้ประกอบธุรกิจชำระค่าเสียหายเพิ่มเติมเป็นค่าเสียหายเชิงลงโทษได้ตามที่ศาลเห็นสมควรแต่ไม่เกิน 2 เท่าของค่าเสียหายที่แท้จริง และหากเป็นกรณีที่มีผู้เสียหายหลายคนจากเหตุการณ์เดียวกัน เช่น กรณีข้อมูลของผู้ใช้บริการมีจำนวนมาก ข้อมูลรั่วไหล ผู้ใช้บริการเหล่านี้อาจรวมตัวกันและใช้วิธีการพิจารณาคดีแบบกลุ่ม (Class Action) หากศาลพิจารณาว่ามีความเสียหายจากการรั่วไหลของข้อมูลเกิดขึ้น และกำหนดค่าเสียหายให้คนละ 1 ล้านบาท ค่าเสียหายทั้งหมดที่ผู้ประกอบธุรกิจจะต้องรับผิดชอบก็จะสูงเท่ากับจำนวนบุคคลที่ได้รับความเสียหายตามคำสั่งศาล[73]

---

[72] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 87.

[73] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 77 ประกอบมาตรา 78.

โทษทางอาญา กล่าวคือ ซึ่งมีทั้งโทษจำคุกและโทษปรับ โดยโทษจำคุกสูงสุดหนึ่งปีและโทษปรับสูงสุด 1 ล้านบาท ขึ้นอยู่กับความร้ายแรงของการกระทำความผิด และในกรณีที่ผู้ประกอบธุรกิจเป็นนิติบุคคล กรรมการ ผู้จัดการ หรือ ผู้ที่รับผิดชอบการดำเนินงานของนิติบุคคลนั้น อาจจะต้องรับผิดเป็นส่วนตัวสำรับการกระทำความผิดนั้น ๆ ด้วย[74]

โทษทางปกครอง กล่าวคือ เป็นการกำหนดมาตรการไว้ในพระราชบัญญัติฉบับนี้ คือ โทษปรับทางปกครองที่คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งปรับได้ตามความร้ายแรงของการกระทำความผิด ทั้งนี้โทษปรับสูงสุดถึง 5 ล้านบาท ทั้งนี้ คณะกรรมการผู้เชี่ยวชาญอาจสั่งให้ผู้กระทำความผิดแก้ไข หรือ ตักเตือนก่อนที่จะมีคำสั่งปรับได้[75] ผู้วิจัยได้พิจารณาแล้วว่า เนื้อหาไม่ได้สอดคล้องกับแนวปฏิบัติตามหลักสากล ซึ่งยังมีความขัดแย้งและไม่สอดคล้องกันเองในบทบัญญัติฉบับปัจจุบันนี้ ดังจะได้วิเคราะห์ในบทต่อไป

3.2 มาตรการทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ

การกำหนดการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation: GDPR) เป็นกฎหมายเกี่ยวกับความเป็นส่วนตัวของพลเมืองสหภาพยุโรป (EU) ที่จะมีผลต่อธุรกิจทั่วโลก โดยมีผลบังคับใช้ในวันที่ 23 ตุลาคม 2018 เป็นต้นมา โดยจะกำหนดวิธีการที่องค์กรใด ๆ ก็ตามที่ติดต่อสื่อสารรับ หรือส่งข้อมูลกับประเทศสมาชิกสหภาพยุโรป ต้องปฏิบัติตามมาตรการการคุ้มครองที่เหมาะสมในการใช้ข้อมูลส่วนบุคคลของบุคคลที่อยู่ในสหภาพยุโรป ซึ่งมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของอียู (EU) หรือ (General Data Protection Regulation: GDPR) แทนหลักเกณฑ์ (EU Data Protection Directive) เดิมที่มีการบังคับใช้มาตั้งแต่ปี 1995 เพื่อยกระดับการคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค โดยเฉพาะในธุรกิจบริการทางอินเทอร์เน็ต[76]

ระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation: GDPR) เป็นบทบัญญัติหลักภายในพระราชบัญญัติคุ้มครองข้อมูล (DPA) กฎนี้เขียนขึ้นเพื่อช่วยปกป้องข้อมูลทางดิจิทัลของพลเมืองของสหภาพยุโรปและเพื่อให้มั่นใจได้ว่าธุรกิจที่ใช้ข้อมูลเหล่านั้นมีความโปร่งใสและปลอดภัยในการรวบรวมและประมวลผลข้อมูล[77] ข้อมูลส่วนบุคคล คือ ข้อมูล

---

[74] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตร 79.

[75] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. มาตรา 84 ประกอบมาตรา 90.

[76] สำนักเจรจาการค้าบริการและการลงทุนกรมเจรจาการค้าระหว่างประเทศ. (2561). ***สรุปสาระสำคัญของ GDPR (General Data Protection Regulation)***. กรุงเทพฯ: กระทรวงพาณิชย์. หน้า 1.

[77] Sean Allan. (2019). ***Aware Academy: ทำไม GDPR จึงสำคัญสำหรับธุรกิจ?*** (ออนไลน์). เข้าถึงได้จาก: https://www.aware.co.th. [2562, 12 กรกฎาคม].

ใด ๆ ที่สามารถระบุ หรือยืนยันความเป็นตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม หากกระทำการรวบรวม เปลี่ยนแปลง แก้ไข ส่งต่อ ทำลาย ใช้ หรือเก็บข้อมูลส่วนบุคคลของพลเมือง(EU) จะต้องปฏิบัติตามกฎ (GDPR) การยินยอมที่ตรวจสอบได้ต้องมีการบันทึกเป็นลายลักษณ์อักษร ว่าเกิดขึ้นเมื่อใดและอย่างไรที่บุคคลนั้น ๆ ตกลงที่จะให้นำข้อมูลส่วนบุคคลของนั้นไปใช้ ต้องระบุไว้อย่างชัดเจน ว่าจะนำข้อมูลไปใช้ทำอะไรเพื่อวัตถุประสงค์ใด การให้ความยินยอมต้องมีความชัดเจนด้วยภาษาที่อ่านเข้าใจง่าย[78]

เนื่องจากสหภาพยุโรปมีลักษณะเป็นองค์กรบริหารเหนือรัฐ (Sup national) โดยประเทศสมาชิกตกลงยินยอมถ่ายโอนอำนาจอธิปไตยบางส่วนให้กับองค์กรกลางของประชาคม ซึ่งอำนาจพื้นฐานของประชาคมมีกฎหมายรับรองในรูปแบบของสนธิสัญญา รวมทั้งมาตรการทางกฎหมายในรูปแบบของข้อกำหนดบังคับ (Directives) และระเบียบ (Regulations) คำสั่ง (Decisions) ในการออกนโยบายและมาตรการทางกฎหมาย แม้ว่าสหภาพยุโรปจะเป็นการรวมกลุ่มของรัฐ หรือ เป็นองค์กรระหว่างประเทศ แต่อย่างไรก็ตาม โครงสร้างของสหภาพยุโรปนั้นเป็นลักษณะ “เหนือชาติ” (Supranational trait) ได้อย่างชัดเจน ด้วยเหตุเพราะบรรดารัฐสมาชิกไม่ใช่เพียงแค่รวมตัวกันเท่านั้น หากแต่ยังได้ร่วมกันสร้างสรรค์สถาบัน หรือหน่วยงานภายใน ซึ่งมีอำนาจเหนือรัฐสมาชิกรัฐใดรัฐหนึ่งโดยเฉพาะ อันประกอบไปด้วย สภายุโรป คณะมนตรี คณะกรรมาธิการ และศาลยุติธรรม[79]

โดยสมาชิกคณะมนตรี ประกอบไปด้วยรัฐมนตรี หรือผู้แทนรัฐบาลจากทุกประเทศสมาชิกในการประชุมแต่ละครั้งจะมีรัฐมนตรีผู้รับผิดชอบเรื่องนั้น ๆ เข้าร่วมรวมทั้งสิ้น 27 ท่าน[80] เช่น การต่างประเทศ เกษตรกรรม คมนาคม เศรษฐกิจและการเงิน และพลังงาน เป็นต้น หากมีการประชุมในการตัดสินใจประเด็นสำคัญ ๆ ก็จะเป็นการประชุมในระดับประมุขของประเทศ โดยจะมีการประชุมสุดยอด 4 ครั้ง ต่อปี เพื่อที่จะกำหนดทิศทางนโยบายของสหภาพยุโรป โดยแต่ละประเทศจะมีเสียงโหวตแตกต่างกันตามสัดส่วนจำนวนของประชากร ซึ่งการตัดสินใจส่วนใหญ่ใช้แบบเสียงข้างมาก และในขณะที่ประเด็นสำคัญจะใช้ระบบการโหวตแบบเอกฉันท์

---

[78] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. อ้างแล้วเชิงอรรถที่ 67. (ออนไลน์).

[79] สำนักงานต่างประเทศ. (2557). ***กฎหมายประชาคมยุโรป***. รายงานวิจัยหลักสูตรกฎหมายประชาคมยุโรป ณ มหาวิทยาลัยไลเดน ราชอาณาจักรเนเธอร์แลนด์ ระหว่างวัน ที่ ๑๖ - ๒๗ มิถุนายน ๒๕๕๗. หน้า 12-13.

[80] กรมยุโรป กระทรวงการต่างประเทศ. (2561). ***สหภาพยุโรป (The European Union - EU).*** (ออนไลน์). เข้าถึงได้จาก: http://www.mfa.go.th/europetouch/th/other/8331/89715%E0%B8%AA%E0%B8%AB%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%A2%E0%B8%B8%E0%B9%82%E0%B8%A3%E0%B8%9B-(The-European-Union---EU).html. [2563, 27 มกราคม]

รัฐสหภายุโรปได้ออกกฎหมาย (GDPR) ซึ่งได้กำหนดให้ข้อมูลไบโอเมตริกซ์ (Biometrics)ไว้เฉพาะเจาะจงว่า “เป็นข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิคเฉพาะที่เกี่ยวข้องกับลักษณะทางกายภาพสรีรวิทยา หรือพฤติกรรมของบุคคลธรรมดาซึ่งอนุญาต หรือยืนยันเอกลักษณ์เฉพาะของบุคคลธรรมดา เช่น ใบหน้า ภาพ หรือข้อมูลลายนิ้วมือ (Dactyloscopic)” ซึ่ง (GDPR) ระบุว่าข้อมูลไบโอเมตริกซ์เป็นหมวดหมู่ใหม่ของ “ข้อมูลพิเศษ” อย่างชัดเจนของข้อมูลไบโอเมตริกซ์นั้นเกิดจากการถูกใช้เพื่อจุดประสงค์ในการระบุตัวตนและการเปิดเผยข้อมูลไบโอเมตริกซ์ โดยไม่ได้รับอนุญาต หรือโดยไม่ได้ตั้งใจอาจก่อให้เกิดความเสี่ยงร้ายแรงต่อการขโมยข้อมูลประจำตัว คุณสมบัติของข้อมูลไบโอเมตริกซ์เป็นหมวดหมู่ของ “ข้อมูลพิเศษ” นำไปสู่ผลลัพธ์หลายประการสำหรับผู้ที่ต้องการประมวลผลข้อมูลประเภทนี้และใช้เทคโนโลยีไบโอเมตริกซ์ ตามกฎ (GDPR) จะห้ามมิให้มีการประมวลผลข้อมูลไบโอเมตริกซ์ เว้นแต่ จะมีข้อยกเว้นไว้เฉพาะ เช่น บริษัทเอกชน โดยปกติส่วนใหญ่จะต้องอยู่ภายใต้ความยินยอมในการประมวลผลข้อมูลโอเมตริกซ์ (แต่ระวังว่าพนักงานไม่สามารถให้ความยินยอมได้ตามปกติ) ในขณะที่บางองค์กร เช่น ประกันสังคม หรือการจ้างงาน หรือโรงพยาบาลอาจใช้กฎหมายอื่น ๆ สำหรับการประมวลผลข้อมูลไบโอเมตริกซ์[81]

รัฐสภายุโรปมีมติในการสร้างฐานข้อมูลชีวภาพส่วนกลางขนาดใหญ่ โดยรัฐสภายุโรปกล่าวว่า “ระบบจะสามารถทำให้ระบบสารสนเทศของสหภาพยุโรปนำมาใช้ในการรักษาความปลอดภัยชายแดนและการจัดการการโยกย้ายทำงานร่วมกันช่วยให้การแลกเปลี่ยนข้อมูลระหว่างระบบ” ที่หน่วยงานบังคับใช้กฎหมายของรัฐสมาชิกใด ๆ ที่สามารถเข้าถึงได้ (มีข้อจำกัดบางอย่าง) แม้ว่ากฎหมายปัจจุบันส่วนใหญ่จะรวมฐานข้อมูลชีวภาพที่มีอยู่ของประเทศในสหภาพยุโรปที่มีอยู่แล้ว แต่ก็ยังสามารถเพิ่มความเสี่ยงของการแฮคได้ในขณะที่เสรีภาพทางแพ่งอ้างว่ากฎหมายใหม่สามารถขยายได้ในอนาคตเพื่อครอบคลุมการใช้งานอื่น ๆ สมาชิกบางส่วนของ (EP) ได้พยายามมาหลายปีเพื่อให้นักท่องเที่ยวรัฐสมาชิกสหภาพยุโรปตกอยู่ภายใต้ฐานข้อมูลนี้[82]

---

[81] Legal ICT Biometric data processing raeds:

“Automated monitoring and recognition of employees’ facial features and expressions, is generally considered unlawful. Using biometrics for access control in the workspace, such as facial, iris, or finger print scanners, appears problematic as well, as employers cannot rely on consent, and no other exception to the general prohibition to process biometric data appears applicable. Member states are permitted to create their own rules concerning biometric data, however”.

[82] Fatema Patrawala, (2019), EU parliament votes to amass the largest biometric database on earth. reads:

“The European Parliament says “the system will make EU information systems used in security, border and migration management interoperable enabling data exchange between the systems.”

ฐานข้อมูลใหม่ ถูกเรียกว่า (Common Identity Repository: CIR)[83] และมีเป้าหมายที่จะรวมระเบียนของพลเมือง 350 ล้านคนจากสหภาพยุโรป (CIR) ได้รับข้อมูลพลเมือง เช่น ชื่อ วันเดือนปีเกิด หมายเลขหนังสือเดินทาง รวมถึงข้อมูลไบโอเมตริกซ์ เช่น ลายนิ้วมือและการสแกนใบหน้า ข้อมูลทั้งหมดนี้จะมีไว้สำหรับหน่วยงานบังคับใช้กฎหมายทั้งหมดจาก 27 ประเทศสมาชิกสหภาพยุโรป ฐานข้อมูลนี้ คือ การทำให้งานของตัวแทนผู้รักษากฎหมาย รวมถึงการป้องกันชายแดนซึ่งตอนนี้ต้องใช้ผ่านฐานข้อมูลของแต่ละประเทศที่เกี่ยวข้องเมื่อต้องการค้นหาข้อมูลเกี่ยวกับบุคคล ข้อมูลจะมาจากฐานข้อมูลอื่น ๆ เช่น ระบบข้อมูลเชงเก้น (Schengen Information System Eurodac) ระบบข้อมูลวีซ่า (VIS) และสามระบบใหม่ เป็นระบบบันทึกความผิดทางอาญาแห่งยุโรปสำหรับประเทศที่สาม (ECRIS-TCN) ระบบเข้า หรือออก (EES) และสารสนเทศและการอนุมัติระบบการเดินทางยุโรป (ETIAS) ตามที่เจ้าหน้าที่ของสหภาพยุโรป (CIR) ผ่านรัฐสภายุโรปเมื่อวันจันทร์ที่ 16 เมษายน 2019 ด้วยคะแนนเสียงสองเสียงแยกกัน กฎ (CIR) สำหรับชายแดนและการตรวจสอบวีซ่าได้รับการรับรองโดย 511 ถึง 123 และงดออกเสียงเก้าครั้งในขณะที่กฎหมาย (CIR) สำหรับตำรวจและความร่วมมือด้านการพิจารณาคดีการขอลี้ภัยและการโยกย้ายได้รับการอนุมัติ 510 ถึง 130 และงดออกเสียง 9 ท่าน[84]

สิทธิของบุคคลตาม (GDPR) ยังระบุถึงสิทธิส่วนบุคคลของเจ้าของข้อมูล พลเมืองของสหภาพยุโรปมีสิทธิที่จะขอรายละเอียดเกี่ยวกับวิธีการที่จะนำข้อมูลส่วนบุคคลเหล่านั้นไปใช้ และมีสิทธิขอให้เจ้าของข้อมูลกระทำบางอย่างได้เกี่ยวกับข้อมูลของตน ตามคำขอของเจ้าของข้อมูลอย่างรวดเร็ว ผู้ใช้มีสิทธิที่จะขอให้แก้ไขข้อมูลส่วนตัวให้ถูกต้องได้ ขอให้ให้หน่วยงานที่เก็บข้อมูลส่งข้อมูลของตัวเองไปให้หน่วยงานอื่น ๆ ได้ ขอห้ามมิให้ใช้ข้อมูลในงานบางอย่างก็ได้ หรือขอให้ทำลายข้อมูลอย่างสมบูรณ์ได้ จึงเป็นมาตรการในการให้ความคุ้มครองข้อมูลส่วนบุคคลเพื่อความมั่นคงปลอดภัยแก่เจ้าของข้อมูล ซึ่งจะได้ทำการศึกษาต่อไป[85]

---

[83] Lucian Armasu. (2019). EU Common Identity Repository (CIR). Raeds:

"The new database will be called the Common Identity Repository (CIR), and it aims to unify the records of 350 million citizens from the EU. CIRcontains citizen information such as names, dates of birth, passport numbers, as well as biometric data such as fingerprints and facial scans. All of this data will be made available to all law enforcement agencies from the 27 EU member states".

[84] Katrien Luyten, Sofija Voronova. (2019). ***Members' Research ServiceInteroperability between EU border and security information systems***. pp. 10-11.

[85] GDPR Preamble raeds:

3.2.1 คำสั่ง Directive 2002/58 on Privacy and Electronic Communications

Directive 2002/58 on Privacy and Electronic Communications[86]ถูกนำมาบังคับใช้เมื่อวันที่ 12 กรกฎาคม คริสต์ศักราช 2002 และมีการแก้ไขเพิ่มเติมเรื่อยมาซึ่งการแก้ไขครั้งล่าสุดมีขึ้นเมื่อวันที่ 6 เมษายน2015 เป็นบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลและความเป็นส่วนตัวในยุคดิจิตอล ซึ่งมีสาระสำคัญหลายประการเช่น การคุ้มครองข้อมูลซึ่งเป็นความลับ รวมถึงการคุ้มครองการเก็บรวบรวมข้อมูลจากแสปมหรือคุกกี้ สาเหตุประการหนึ่งของการบังคับใช้ (E-Privacy Directive) นี้มาจากการติดตามพฤติกรรมของบุคคลบนอินเตอร์เน็ต

กฎที่แตกต่างใน (PECR) ถูกนำไปใช้ในวิธีที่ต่างกันโดยใช้คำศัพท์ได้กำหนดไว้หลากหลายคำศัพท์เหล่านี้ได้มีการอธิบายที่เกี่ยวข้องกับหลักแนวความคิด ได้แก่ [87]

ผู้ให้บริการ ให้บริการโทรศัพท์หรืออินเทอร์เน็ต ผู้ให้บริการเครือข่าย จัดหาอุปกรณ์เครือข่ายพื้นฐานสมาชิก บุคคลที่มีชื่ออยู่ในใบเรียกเก็บเงิน และผู้ใช้ บุคคลใดก็ตามที่ใช้โทรศัพท์หรือการเชื่อมต่ออินเทอร์เน็ต

E-Privacy Directive ได้ให้คำนิยามความหมายดังต่อไปนี้

“ผู้ใช้” หมายถึง บุคคลผู้ที่ใช้บริการการสื่อสารทางอิเล็กทรอนิกส์ที่ทำเปิดเผยต่อสาธารณชน เพื่อวัตถุประสงค์ส่วนตัว หรือธุรกิจโดยไม่จำเป็นต้องสมัครใช้บริการนี้[88]

---

(1): “The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8 (1) of the Charter of Fundamental Rights of the European Union …provide that everyone has the right to protection of personal data concerning him or her.”

[86] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[87] Different rules in PECR apply in different ways, using a variety of defined terms. Many of these terms are explained where relevant throughout this guide. The main concepts include: reads:

1.service provider: provides telephone or internet services;

2.network provider: provides the underlying network equipment;

3.subscriber: the person whose name is on the bill; and

4. user: any individual using the phone or internet connection.

[88] Directive 2002/58 on Privacy and Electronic Communications reads:

“subscriber” means a person who is party to a contract with a provider of public electronic communications services for the supply of such services;

“user” means any individual using a public electronic communications service.

“การสื่อสาร” หมายถึง ข้อมูลใด ๆที่ถูกแลกเปลี่ยน หรือถ่ายโอนระหว่างกลุ่มบุคคลซึ่งมีจำนวนจำกัดโดยผ่านบริการสื่อสารอิเล็กทรอนิกส์สาธารณะ แต่ไม่รวมถึงข้อมูลซึ่งถ่ายโอนโดยเป็นส่วนหนึ่งของการบริการทางโปรแกรม เว้นแต่ข้อมูลนั้นสามารถเชื่อมโยงไปยังสมาชิกหรือผู้ใช้ที่อาจถูกระบุตัวได้จากการรับข้อมูลนั้น[89]

“ผู้ให้บริการการสื่อสาร” ได้ให้คำนิยามไว้ตาม Section 405 ของ (Communication Act 2003 (c)) ได้ให้คำนิยามไว้หมายถึง บุคคลผู้ซึ่งให้บริการการเครือข่ายการสื่อสารทางอิเล็กทรอนิกส์หรือให้บริการการสื่อสารทางอิเล็กทรอนิกส์[90]

“เครือข่ายการสื่อสารทางอิเล็กทรอนิกส์” ได้ถูกกำหนดไว้ในมาตรา 151 ตามคำนิยามที่กำหนดไว้ใน section 32 ของ (Communication Act 2003 (b)) ได้ให้ความหมายไว้ว่า หมายถึง[91] ระบบการสื่อสารเพื่อการถ่ายโอนสัญญาณโดยวิธีอิเล็กทรอนิกส์ หรือแม่เหล็ก หรือพลังแม่เหล็กไฟฟ้าบุคคลซึ่งจัดเตรียมระบบหรือเกี่ยวข้องกับระบบนั้นได้ใช้สิ่งดังต่อไปนี้เพื่อการถ่าย

---

[89] Communication Act 2003 raeds:

(d) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

[90] Communication Act 2003 Section 405 (c) reads:

A ‘communications provider’ is defined in section 405 of the Communications Act 2003 as someone who provides an electronic communications network or electronic communications service. So, this term is broad and includes any organisation that operates a network or service, even if it is a private network or service not available to the public.

[91] Communication Act 2003 section 32 (b) reads:

“(a) a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description; and

(b) such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals

(i) apparatus comprised in the system;

(ii) apparatus used for the switching or routing of the signals;

(iii) software and stored data; and

(iv) (except for the purposes of sections 125 to 127) other resources, including network elements which are not active.”

โอนสัญญาณคือ อุปกรณ์ซึ่งประกอบอยู่ในระบบอุปกรณ์ซึ่งใช้เพื่อการสลับ หรือจัดเส้นทางของสัญญาณ และซอร์ฟแวร์และข้อมูลที่ได้ถูกจัดเก็บไว้

"บริการการสื่อสารทางอิเล็กทรอนิกส์" มีความหมายตามที่กำหนดไว้ใน Section 32 ของ (Communication Act 2003) ได้ให้ความหมายไว้ว่า หมายถึง บริการซึ่งมี หรือประกอบด้วยลักษณะการส่งสัญญาณทางเครือข่ายการสื่อสารอิเล็กทรอนิกส์เว้นแต่เป็นการให้บริการทางเนื้อหา

"อีเมล" หมายถึง ตัวอักษรใด ๆ เสียงพูด เสียง หรือข้อความรูปภาพที่ถูกส่งบนเครือข่ายการสื่อสารอิเล็กทรอนิกส์สาธารณะซึ่งสามารถที่จะถูกเก็บรักษาบนเครือข่าย หรือบนอุปกรณ์ปลายทางของผู้รับจนกระทั่งผู้รับได้รับ รวมถึงข้อความที่ถูกส่งโดยอาศัยบริการข้อความสั้น

"บุคคล" หมายถึง ปัจเจกบุคคล และรวมถึงหน่วยงานซึ่งยังมิได้จดทะเบียนของบุคคลดังกล่าว

ข้อมูลตำแหน่ง "(Location data)" หมายถึง ข้อมูลใด ๆ ซึ่งถูกประมวลในเครือข่ายการสื่อสารอิเล็กทรอนิกส์หรือโดยบริการการสื่อสารอิเล็กทรอนิกส์ระบุถึงตำแหน่งทางภูมิศาสตร์ของอุปกรณ์ปลายทางของผู้ใช้บริการการสื่อสารอิเล็กทรอนิกส์สาธารณะ โดยให้รวมถึงข้อมูลดังต่อไปนี้[92]

ละติจูด ลองติจูด หรือระดับความสูงของอุปกรณ์ปลายทาง ทิศทางการเดินทางของผู้ใช้ เวลาซึ่งข้อมูล (location) ได้ถูกบันทึกไว้

"การละเมิดข้อมูลส่วนบุคคล" หมายถึง การละเมิดความปลอดภัยซึ่งนำไปสู่การทำลาย การสูญหาย การเปลี่ยนแปลง การเปิดเผยโดยไม่ได้รับอนุญาต หรือการเข้าถึงข้อมูลส่วนบุคคล การถ่ายโอน การเก็บรักษา หรือการประมวลผลโดยประการอื่นตามบทบัญญัติเกี่ยวกับบริการสื่อสารอิเล็กทรอนิกส์สาธารณะ ทั้งนี้ไม่ว่าการกระทำดังกล่าวจะเกิดขึ้นโดยอุบัติเหตุหรือการกระทำโดยจงใจก็ตาม[93]

---

[92] Communication Act 2003 Section 32 reads:

(c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

[93] Communication Act 2003 section 32 reads:

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

“ผู้ให้บริการการสื่อสารสาธารณะ” หมายถึง ผู้ให้บริการการเครือข่ายการสื่อสารอิเล็กทรอนิกส์สาธารณะ หรือผู้ให้บริการการสื่อสารอิเล็กทรอนิกส์สาธารณะ

“ผู้ให้บริการเครือข่ายอิเล็กทรอนิกส์สาธารณะ” ให้มีความหมายตามที่กำหนดใน Section 151 ของ (Communication Act 2003 (g)) ได้ให้ความหมายไว้ว่าหมายถึง บริการสื่อสารอิเล็กทรอนิกส์สาธารณะใด ๆ ซึ่งสามารถใช้ได้โดยสาธารณะ

“เครือข่ายการสื่อสารอิเล็กทรอนิกส์สาธารณะ” ให้มีความหมายตามที่กำหนดใน Section 151 ของ (Communication Act 2003) ได้ให้ความหมายไว้ว่า เครือข่ายบริการสื่อสารอิเล็กทรอนิกส์ซึ่งให้บริการทั้งหมด หรือโดยหลักเพื่อวัตถุประสงค์เพื่อให้บริการการสื่อสารอิเล็กทรอนิกส์สาธารณะสามารถเข้าถึงได้โดยสาธารณะ

“สมาชิก” หมายถึง บุคคลซึ่งเป็นคู่สัญญากับผู้ให้บริการสื่อสารอิเล็กทรอนิกส์สาธารณะเพื่อการให้บริการดังกล่าว

เครือข่ายข้อมูล “(Traffic Data)” หมายถึง ข้อมูลซึ่งถูปะมวลผลเพื่อวัตถุประสงค์ในการถ่ายโอนการสื่อสารทางเครือข่ายการสื่อสารอิเล็กทรอนิกส์ หรือเพื่อการเรียกเก็บเงินเกี่ยวกับการสื่อสารนั้นรวมถึงข้อมูลเกี่ยวกับการกำหนดเส้นทาง ระยะเวลา หรือเวลาในการสื่อสาร

“ผู้ใช้” หมายถึง บุคคลใด ๆ ซึ่งใช้บริการสื่อสารอิเล็กทรอนิกส์สาธารณะ

ข้อมูลสื่อสารอิเล็กทรอนิกส์ส “(E-privacy directive)” ได้มีการกำหนดให้ผู้ให้บริการสื่อสารอิเล็กทรอนิกส์สาธารณะต้องมีมาตรการทางเทคนิคและมาตรการในทางองค์กร เพื่อรักษาความปลอดภัยของการให้บริการมาตรการดังกล่าว ต้องก่อให้เกิดความมั่นใจว่าข้อมูลส่วนบุคคลนั้น จะถูกเข้าถึงได้เพียงเฉพาะบุคคลที่ได้รับอนุญาตและเพื่อวัตถุประสงค์ที่ชอบด้วยกฎหมายเท่านั้น และมาตรการนี้ต้องป้องกันข้อมูลส่วนบุคคลที่ถูกเก็บรักษา หรือถูกโอนมิให้ถูกทำลายโดยอุบัติเหตุ หรือโดยมิชอบด้วยกฎหมาย การสูญหายโดยอุบัติเหตุ หรือการเปลี่ยนแปลง หรือการเก็บรักษาโดยบุคคลซึ่งไม่มีอำนาจ หรือไม่ชอบด้วยกฎหมาย การประมวลผล การเข้าถึง หรือการเปิดเผย หากภายหลังการบังคับใช้มาตรการดังกล่าวแล้ว ยังมีความเสี่ยงที่มีนัยสำคัญต่อความปลอดภัยของบริการสื่อสารอิเล็กทรอนิกส์สาธารณะ ผู้ให้บริการต้องแจ้งให้สมาชิกทราบถึงลักษณะของความเสี่ยง มาตรการที่เหมาะสม ซึ่งสมาชิกอาจได้รับเพื่อป้องกันความเสี่ยงและค่าใช้จ่ายที่อาจเกิดขึ้นต่อสมาชิกในการใช้มาตรการดังกล่าว[94]

---

[94] Communication Act 2003 section 32 reades:

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคลผู้ให้บริการต้องแจ้งการละเมิดต่อ (Information commissioner) โดยไม่ชักช้าโดยจะต้องแจ้งถึงลักษณะของการละเมิด ผลจากการละเมิด และมาตรการที่ถูกใช้ หรือจะใช้เพื่อแจ้งการละเมิด และหากการละเมิดนั้นน่าจะก่อให้เกิดผลกระทบต่อข้อมูลส่วนบุคคล หรือความเป็นส่วนตัวของสมาชิก หรือผู้ใช้ ผู้ให้บริการต้องแจ้งการละเมิดนั้นแก่สมาชิก หรือผู้ใช้โดยไม่ช้าซึ่งการแจ้งดังกล่าวต้องระบุถึงลักษณะของการละเมิดข้อมูล เพื่อให้สมาชิก หรือผู้ใช้สามารถติดต่อผู้ให้บริการ เพื่อข้อมูลเพิ่มเติม และคำแนะนำเกี่ยวกับมาตรการเพื่อให้สมาชิกบรรเทาผลกระทบที่อาจเกิดขึ้นจากการละเมิดนั้น อย่างไรก็ตาม ผู้ให้บริการได้รับการยกเว้น ไม่ต้องแจ้งเตือนสมาชิก หรือผู้ใช้ในกรณีที่ผู้ให้บริการมีมาตรการเทคโนโลยีป้องกันที่เหมาะสม ซึ่งก่อให้บุคคลผู้ไม่ได้รับอนุญาตให้เข้าถึงข้อมูลนั้น ไม่สามารไม่สามารถเข้าใจข้อมูลนั้นได้ และมาตรการนั้นได้ ถูกนำมาใช้แก่ข้อมูลที่ถูกละเมิด

การให้ความคุ้มครองแก่การเก็บรวบรวม หรือการเข้าถึงข้อมูลส่วนบุคคล (E-privacy) ได้กำหนดว่านอกจากจะเป็นการเก็บรวบรวม หรือการเข้าถึงข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เพื่อการถ่ายโอนข้อมูลการสื่อสารผ่านเครือข่ายการสื่อสารอิเล็กทรอนิกส์ หรือการเก็บรวบรวม หรือการสื่อสารนั้นจำเป็นอย่างยิ่งเพื่อข้อกำหนดของบริการสังคมข้อมูลข่าวสาร ซึ่งร้องขอโดยสมาชิก หรือผู้ใช้บุคคลจะต้องไม่ทำการเก็บรักษา หรือเข้าถึงข้อมูลส่วนบุคคล ซึ่งถูกเก็บรักษาไว้ในอุปกรณ์ปลายทางของสมาชิก หรือผู้ใช้ เว้นแต่ สมาชิก หรือผู้ใช้ได้รับข้อมูลที่ชัดแจ้งและเข้าใจได้เกี่ยวกับวัตถุประสงค์ของการเก็บรวบรวม หรือการเข้าถึงข้อมูลนั้น

ในกรณีของการประมวลผลข้อมูลส่วนบุคคล (E-Privacy Directive ข้อ 7) กำหนดให้เครือข่ายข้อมูล (Traffic data) ของสมาชิก หรือผู้ใช้ซึ่งถูกประมวลผล หรือเก็บรักษาโดยผู้ให้บริการสื่อสารสาธารณะ หากข้อมูลนั้นไม่จำเป็นอีกต่อไป ผู้ให้บริการสื่อสาธารณะจะต้องลบ หรือทำการแก้ไขเปลี่ยนแปลงข้อมูลนั้น เพื่อไม่ให้สามารถเชื่อมโยงตัวเจ้าของได้ สำหรับความคุ้มครอง ข้อมูลตำแหน่ง (Location data) ได้ถูกกำหนดไว้ในข้อ 14 เรื่องข้อจำกัดของการประมวลผลข้อมูลตำแหน่ง (Location data) โดยกำหนดห้ามผู้ประกอบการสื่อสารอิเล็กทรอนิกส์ หรือผู้ให้บริการเครือข่ายการสื่อสารอิเล็กทรอนิกส์ประมวลผลข้อมูลเกี่ยวกับข้อมูลตำแหน่ง (Location data) ของสมาชิก หรือผู้ใช้ โดยมีข้อยกเว้นให้สามารถกระทำการประมวลผลได้ หากสมาชิก หรือผู้ใช้ไม่สามารถถูกระบุตัวโดยข้อมูลนั้น หรือเป็นการจำเป็นแก่การให้บริการเสริม (Value added service) โดยได้รับความยินยอมจากผู้ใช้

ดังนั้น นอกจากที่กล่าวมาแล้ว (E-privacy directive) ยังมีบทบัญญัติเกี่ยวกับการทำการตลาดแบบตรงผ่านโทรศัพท์ โทรสาร และอีเมล โดยใน (E-privacy directive) ได้กำหนดห้ามบุคคลกระทำ

การส่ง หรือสนับสนุนการส่งการสื่อสารที่ไม่พึงประสงค์ ซึ่งมีวัตถุประสงค์ เพื่อการตลาดผ่านทางอีเมล เว้นแต่ จะได้รับความยินยอมจากผู้รับไว้ล่วงหน้า

3.2.2 ข้อบังคับกฎระเบียบการคุ้มครองข้อมูลทั่วไปของรัฐสภายุโรปและสภา (REGULATION (EU) 2016/679 (General Data Protection Regulation) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016)

ข้อบังคับกฎระเบียบการคุ้มครองข้อมูลทั่วไปของรัฐสภายุโรปและสภา (REGULATION (EU) 2016/679 of the European Parliament and of the Council) หรือ กฎความคุ้มครองข้อมูลทั่วไป (The General Data Protection Regulations: GDPR) เมื่อวันที่ 27 เมษายน 2016 ซึ่งมีผลใช้บังคับตั้งแต่วันที่ 25 พฤษภาคม 2018 รัฐสภายุโรปได้มีการแก้ไขและกำหนดกรอบการทำงานใหม่สำหรับการจัดการและคุ้มครองข้อมูลส่วนบุคคลของพลเมืองผู้อยู่อาศัยในสหภาพยุโรป โดยมีผลบังคับใช้กับทุกหน่วยงานที่มีการประมวลผลข้อมูลส่วนบุคคลของพลเมืองผู้อยู่อาศัยในสหภาพยุโรป ไม่ว่าการประมวลผลจะทำในสหภาพยุโรป หรือไม่ก็ตาม (GDPR) ใหม่แทนที่กฎระเบียบการคุ้มครองข้อมูลที่ล้าสมัยซึ่งประกาศย้อนกลับไปในปี 1995 ซึ่งแตกต่างจากกฎระเบียบข้อบังคับอนุญาตให้สมาชิก 28 ประเทศ ประเด็นปัญหาของข้อบังคับ (Directive) กล่าวคือ บทบัญญัติดังกล่าวนั้นไม่มีความสอดคล้องเกี่ยวข้องกับยุคดิจิตอลในปัจจุบันอีกต่อไป ข้อบังคับ (Directive) ฉบับเดิมมิได้ให้การคุ้มครองในการจัดการกับวิธีการจัดเก็บรวบรวมและถ่ายโอนข้อมูลในยุคปัจจุบัน ซึ่งเป็นยุคดิจิตอล เช่นเดียวกับกฎระเบียบและกฎเกณฑ์ต่าง ๆ ทั่วทั้งสหภาพยุโรปและกฎระเบียบเหล่านี้ ไม่สามารถก้าวทันระดับความก้าวหน้าทางเทคโนโลยี[95]

ข้อบังคับ (EU Directive 95/46) ได้ใช้บังคับมานานกว่า 20 ปี โดยที่สังคมโลกมีการเปลี่ยนแปลงอย่างมากในปัจจุบัน โดยเฉพาะบริบทการสื่อสารผ่านทางอิเล็กทรอนิกส์ ที่มีการเติบโตพัฒนาอย่างรวดเร็วมาก จึงมีการปรับปรุงแก้ไข (Directive) ดังกล่าว ซึ่งในที่สุดรัฐสภาแห่งยุโรปก็ได้เห็นชอบข้อกำหนดการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation: GDPR) เมื่อวันที่ 14 เมษายน คริสตศักราช2016 และมีผลบังคับใช้ในวันที่ 25 พฤษภาคม คริสตศักราช 2018

ข้อกำหนดการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation 2016) กฎข้อบังคับ (Regulation 2016/679) ซึ่งได้แทนที่กฎข้อบังคับ (Data Protection Directive 1995) ข้อบังคับ (Directive 95/46/EC) EU Commission ได้รับรองเมื่อวันที่ 27 พฤษภาคม คริสต์ศักราช 2016 แต่ยังมิใช้บังคับกับประเทศสมาชิก (EU) จนกระทั่งมีผลบังคับใช้วันที่ 25 พฤษภาคม คริสตศักราช 2018 เพื่อให้

---

[95] สกล หาญสุทธิวารินทร์. (2561). ***กรุงเทพธุรกิจ: การคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป***. (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/blog/detail/645890. [2562, 2 ตุลาคม]

สอดคล้องกับกฎหมายความเป็นส่วนตัวของข้อมูลทั่วยุโรปอันเป็นการปกป้องและให้อำนาจความเป็นส่วนตัวของพลเมืองในสหภาพยุโรปทั้งหมดและการปรับเปลี่ยนวิธีการขององค์กรต่าง ๆ

โดยรัฐสภายุโรปได้มีการเปลี่ยนแปลงดังนี้

ข้อบังคับ (Directive (EU) 2016/679) การคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation) ในเรื่องการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลและการเคลื่อนไหวของข้อมูลดังกล่าวฟรีและยกเลิก Directive 95/46 / EC (OJ L 119, 4.5.2016, pp. 1–88)[96]

ข้อบังคับ (Directive (EU) 2016/680) ในเรื่องการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล โดยเจ้าหน้าที่เป็นผู้มีอำนาจเพื่อวัตถุประสงค์ในการป้องกันสืบสวนสอบสวนความผิด หรือดำเนินคดีอาญา หรือการดำเนินการลงโทษทางอาญาและการเคลื่อนย้ายข้อมูลดังกล่าวอย่างอิสระ และยกเลิกการตัดสินใจของกรอบการทำงานของสภา 2008/977 / JHA[97] ทั้งนี้ กฎข้อบังคับ (Regulation (EU) 2016/679) ซึ่งเป็นกฎหมากลางของสหภาพยุโรปในการให้ความคุ้มครองข้อมูลส่วนบุคคล รวมถึงได้มีการบัญญัติให้ความคุ้มครองข้อมูลไบโอเมตริกซ์ (Biometrics) โดยมีผลบังคับใช้กับประเทศสมาชิก ซึ่งตัวบทจะมีความเหมาะสมกว่ากับสภาพในปัจจุบัน รวมถึงเทคโนโลยีที่ใช้กันอยู่ ณ ตอนนี้โดยมีสาระสำคัญดังนี้

การบังใช้กฎระเบียบฉบับนี้ ได้บัญญัติไว้ในมาตรา 3[98] ไม่ได้บังคับใช้เฉพาะองค์กรที่ตั้งอยู่ในสหภาพยุโรปเท่านั้น แต่บังคับใช้ถึงองค์กรที่ตั้งอยู่นอกสหภาพยุโรปด้วย หากองค์กรเหล่านั้น

---

[96] Regulation (EU) 2016/679 of the European parllament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[97] Directive (EU) 2016/680 of the European parllament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[98] Regulation (EU) 2016/679 (General Data Protection Regulation) Article 3 Territorial scope reads:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

เสนอขายสินค้าหรือบริการต่อพลเมืองของสหภาพยุโรป หรือที่เฝ้าตรวจสอบติดตามพฤติกรรมของผู้บริโภคในสหภาพยุโรปด้วย และบังคับใช้กับบรรดาบริษัททั้งหลายที่ประมวลผลและเก็บรักษาข้อมูลส่วนบุคคลของพลเมืองผู้บริโภคชาวสหภาพยุโรปด้วย แม้บริษัทเหล่านั้นจะตั้งอยู่นอกสหภาพยุโรปก็ตาม แม้การประมลผลและส่งข้อมูลนั้นได้ทำข้ามแดนสหภาพยุโรปไปเก็บรักษาที่ประเทศอื่น หรือไม่ก็ตาม หากได้มีการกระทำนั้นเกิดขึ้นภายใต้ดินแดนแห่งรัฐสมาชิกของสหาภาพยุโรป หรือผู้ควบคุมข้อมูลส่วนบุคคลนั้นมิได้อยู่ภายใต้บังคับ หรือกฎหมายขัดกับ กฎข้อบังคับ (Regulation (EU) 2016/679) ก็ให้นำกฎข้อบังคับ Regulation ((EU) 2016/679) มาใช้บังคับเพื่อปฏิบัติตามกฎของสภายุโรป (EU) 2016/679 (General Data Protection Regulation) ตามมาตรา 4 ได้ให้คำนิยามศัพท์ที่สำคัญไว้ดังนี้

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใด ๆ ก็ตามที่เกี่ยวข้องถึงการบ่งชี้ตัวบุคคลธรรมดาหรือที่อาจบ่งชี้ได้ถึงตัวบุคคลธรรมดาไม่ว่าโดยทางตรงหรือทางอ้อม โดยเฉพาะการอ้างอิงถึงตัวบ่งชี้ เช่นชื่อ หรือตัวบ่งชี้ที่เป็นรหัสหมายเลขประจำคัวบุคคล ข้อมูลเกี่ยวกับสถานที่ตั้งตัวบ่งชี้ทางระบบออนไลน์ หรือด้วยองค์ประกอบอย่างใดอย่างหนึ่งหรืออย่างที่เจาะจงถึงกายภาพ สรีรวิทยา พันธุกรรม สภาพจิตใจ เศรษฐกิจ วัฒนธรรม หรือสถานะทางสังคมของบุคคลนั้น ที่เกี่ยวข้องกับบุคคลที่สามารถระบุตัวตน หรือลักษณะของบุคคลนั้นได้[99]

“การประมวลผล” หมายถึง การดำเนินการใด ๆ ก็ตามเกี่ยวกับการดำเนินการกับข้อมูลส่วนบุคคลหรือข้อมูลส่วนบุคคลไม่ว่าจะด้วยวิธีการอัตโนมัติ เช่น การรวบรวม การบันทึก องค์กรที่การจัดเก็บ การแก้ไข หรือการเปลี่ยนแปลง การใช้ การเปิดเผย โดยการส่ง การเผยแพร่ หรือการทำให้พร้อมใช้งาน การจัดตำแหน่ง หรือการรวมกันข้อ จำกัด การลบ หรือการทำลาย[100]

---

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

[99] Regulation (EU) 2016/679 (General Data Protection Regulation) Article 4 Definitions reads:

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

[100] Regulation (EU) 2016/679 Art. 4 GDPR Definitions reads:

(2) “processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation,

“การทำโปรไฟล์” หมายถึง การประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติในรูปแบบใด ๆ ก็ตาม ซึ่งประกอบด้วย การใช้ข้อมูลส่วนบุคคลเพื่อประเมินลักษณะส่วนบุคคลบางประการที่เกี่ยวข้องกับบุคคลโดยเฉพาะอย่างยิ่งในการวิเคราะห์ หรือคาดการณ์ด้านต่าง ๆ ที่เกี่ยวข้องกับการทำงานของบุคคล ความชอบส่วนบุคคล ความสนใจ ความน่าเชื่อถือ พฤติกรรม ตำแหน่ง หรือการเคลื่อนไหว[101]

“ผู้ควบคุม” หมายถึง บุคคลธรรมดา หรือนิติบุคคล หรือหน่วยงานของรัฐ หรือตัวแทน บริษัท หรือหน่วยงานอื่นใดมีวัตถุประสงค์ร่วมกันกับผู้อื่น หรือโดยลำพัง หรือร่วมกับผู้อื่น ในกรณีที่มีวัตถุประสงค์และวิธีการประมวลผลดังกล่าวถูกกำหนดโดยกฎหมายสหภาพ หรือรัฐสมาชิก ผู้ควบคุม หรือเกณฑ์เฉพาะสำหรับการแต่งตั้งโดยกฎหมายสหภาพ หรือกฎหมายรัฐสมาชิก[102]

“ความยินยอม” หมายถึง การแสดงเจตนาโดยอิสระมีลักษณะเฉพาะเจาะจงชัดแจ้งและไม่คลุมเครือเป็นลายลักษณ์อักษณ์ หรือตามสัญญาตามวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลได้ความยินยอมให้ทำการประมวลผลข้อมูลส่วนบุคคลนั้น[103]

“การละเมิดข้อมูลส่วนบุคคล” หมายถึง การละเมิดความปลอดภัยที่นำไปสู่การทำลายโดยมิชอบโดยมิชอบ หรือผิดกฎหมายการสูญเสียการเปลี่ยนแปลงการเปิดเผยข้อมูล หรือการเข้าถึงข้อมูลส่วนบุคคลที่ถูกส่งไป จัดเก็บ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต[104]

---

structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”

[101] Regulation (EU) 2016/679 Art. 4 GDPR Definitions reads:

(6) “filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis”

[102] Regulation (EU) 2016/679 Art. 4 GDPR Definitions reads:

(7) “controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”

[103] Regulation (EU) 2016/679 Art. 4 GDPR Definitions reads:

(11) “consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”

[104] Regulation (EU) 2016/679 Art. 4 GDPR Definitions reads:

“ข้อมูลทางพันธุกรรม” หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับลักษณะทางพันธุกรรมของบุคคลธรรมดาซึ่งได้รับ หรือสืบทอดมา โดยข้อมูลนี้นี้มีเอกลักษณ์พิเศษเกี่ยวกับสรีรวิทยา หรือสุขภาพของบุคคลนั้น โดยแสดงผลจากการวิเคราะห์ตัวอย่างทางชีวภาพของบุคคลนั้น[105]

“ข้อมูลไบโอเมตริกซ์” หมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิคเฉพาะที่เกี่ยวข้องกับลักษณะทางกายภาพสรีรวิทยา หรือพฤติกรรมของบุคคลนั้น ซึ่งทำให้บ่งชี้ลักษณะเฉพาะของบุคคล เช่น ภาพใบหน้า ลายนิ้ว หรือข้อมูลลายนิ้วมือ (dactyloscopic)[106]

“ข้อมูลสุขภาพ” หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสุขภาพร่างกาย หรือจิตใจของบุคคลธรรมรวมถึงการให้บริการด้านการดูแลสุขภาพซึ่งเปิดเผยข้อมูลเกี่ยวกับสถานะสุขภาพของบุคคลนั้น[107]

กฎระเบียบว่าด้วยเรื่องการคุ้มครอง “ข้อมูลส่วนบุคคล” นั้น ในการนำข้อมูลส่วนบุคคลไปใช้จะต้องอยู่ภายใต้เงื่อนไขต่อไปนี้ ตามมาตรา 6[108]

---

(12) “personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”

[105] Regulation (EU) 2016/679 Art. 4 GDPR Definitions reads:

(13) “genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question”

[106] Regulation (EU) 2016/679 Art. 4 GDPR Definitions reads:

(14) “biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data”

[107] Regulation (EU) 2016/679 Art. 4 GDPR Definitions reads:

(15) “data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”

[108] Regulation (EU) 2016/679 (General Data Protection Regulation) Article 6 Lawfulness of processing reads:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

เจ้าของข้อมูลได้ให้คำยินยอมให้นำข้อมูลไปใช้สำหรับจุดประสงค์ใดจุดประสงค์หนึ่งหรือหลาย ๆ จุดประสงค์

การใช้ข้อมูลส่วนบุคคลเพื่อทำสัญญา หรือมีความจำเป็นต้องใช้ข้อมูลส่วนบุคคลเพื่อเตรียมสัญญา โดยเจ้าของข้อมูลเป็นคู่สัญญา

ผู้ที่ต้องการข้อมูลส่วนบุคคลนั้นมีความจำเป็นต้องใช้ข้อมูลส่วนบุคคล เนื่องจากกฎหมายกำหนดไว้

มีความจำเป็นต้องใช้ข้อมูลส่วนบุคคล เพื่อผลประโยชน์ต่อชีวิตของเจ้าของข้อมูล หรือเพื่อปกป้องผลประโยชน์ของผู้อื่น

มีความจำเป็นต้องใช้ข้อมูลส่วนบุคคล เพื่อปฏิบัติภารกิจที่มีผลต่อความมั่นคงและความปลอดภัยของสาธารณะ

มีความจำเป็นที่สมเหตุสมผลที่ต้องใช้ข้อมูลส่วนบุคคล โดยการใช้ข้อมูลส่วนบุคคลนั้นต้องไม่ขัดต่อผลประโยชน์ สิทธิและอิสรภาพขั้นพื้นฐานของเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งถ้าบุคคลผู้นั้นเป็นผู้เยาว์

การประมวลผลในภายภาคหน้าต้องสอดคล้องกับวัตถุประสงค์ที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล โดยการประมวลผลนั้นจะสอดคล้องกับวัตถุประสงค์ หรือไม่ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณาในกรณีดังต่อไปนี้ เว้นแต่ ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

กรณีแรก มีความเชื่อมโยงระหว่างวัตถุประสงค์ที่ข้อมูลนั้น จะถูกเก็บ รวบรวม และวัตถุประสงค์ที่จะทำการประมวลผลต่อไป

กรณีที่สอง ในกรณีข้อมูลส่วนบุคคลนั้นจะถูกเก็บรวบรวมไว้ในฐานข้อมูล

กรณีที่สาม ลักษณะของข้อมูลส่วนบุคคลที่จะทำการประมวลผล โดยเฉพาะอย่างยิ่งเป็นข้อมูลที่มีลักษณะพิเศษ

กรณีที่สี่ ผลที่อาจเกิดจากการประมวลที่จะทำต่อไป อันจะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

กรณีสุดท้าย มีมาตรการป้องกันที่มีความเหมาะสม

ดังนั้น หากข้อมูลส่วนบุคคลที่จะทำการประมวลผลต่อไปขัดกับวัตถุประสงค์ในตอนแรกที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลคนเดียวกัน การประมวลผลต่อไปนั้นอย่างน้อยต้องมีหลักการตามที่กล่าวมาไม่น้อยกว่า 1 ข้อ การประมวลผลเพื่อประโยชน์ของผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคลที่สามซึ่งขัดกับวัตถุประสงค์ในตอนแรก จะถือว่าชอบด้วยกฎหมายต่อเมื่อประโยชน์นั้น สำคัญกว่าประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

หลักความยินยอม ได้บัญญัติไว้ในมาตรา 7[109] โดยในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคลและข้อมูลลักษณะพิเศษภายใต้ความยินยอมของเจ้าของข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลต้องสามารถแสดงว่าเจ้าของข้อมูลส่วนบุคคลมีการให้ความยินยอม “โดยชัดแจ้ง” ในกรณีที่ความยินยอมจะต้องแจ้งเป็นลายลักษณ์อักษรซึ่งมีเรื่องอื่น ๆ รวมอยู่ด้วย การขอความยินยอมต้องแยกออกมาอย่างเด่นชัดจากเรื่องอื่น ๆ และอยู่ในรูปแบบที่สามารถเข้าใจได้ เข้าถึงได้ง่าย และใช้ภาษาที่ง่ายและชัดเจน นอกจากนี้เจ้าของข้อมูลส่วนบุคคลยังมีสิทธิเพิกถอนความยินยอมได้ตลอดเวลาไม่ว่าในเวลาใด ๆ โดยการเพิกถอนนั้นจะไม่กระทบความชอบด้วยกฎหมายในการประมวลผลข้อมูลก่อนมีการเพิกถอนความยินยอม ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งสิทธิในการเพิกถอนความยินยอมแก่เจ้าของข้อมูลด้วย

หลักการประมวลผลข้อมูลนามแฝง (Pseudonymous) ในการประมวลผลข้อมูลนั้นไม่จำเป็นต้องระบุตัวเจ้าของข้อมูลส่วนบุคคลอีกต่อไป ผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่เก็บรักษาหรือเพิ่มเติมข้อมูล หรือไม่ต้องประมวลผลเพิ่มเติมตามระเบียบกฎเกณฑ์ฉบับนี้ หากผู้ควบคุม

---

[109] Regulation (EU) 2016/679 (General Data Protection Regulation) Article 7 Conditions for consent reads:

1.Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

ข้อมูลส่วนบุคคลได้มีการกระทำการก่อให้สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลนั้นได้เจ้าของข้อมูลส่วนบุคคลดังกล่าวมีสิทธิตามกฎเกณฑ์ดังนี้

สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคลมาตรา 15[110] กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลภายในเวลาอันสมควร โดยไม่มีค่าใช้จ่ายแสดงว่าข้อมูลส่วนบุคคลนั้นได้ถูกประมวลผลหรือไม่ก็ตาม หรือมีการประมวลผลใด ๆ เกิดขึ้น และมีสิทธิเข้าถึงข้อมูล ดังต่อไปนี้

---

[110] Regulation (EU) 2016/679 (General Data Protection Regulation) Article 15 Right of access by the data subject reads:

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ผู้รับข้อมูดังกล่าวอาจถูกเปิดเผยโดยเฉพาะอย่างยิ่งผู้รับซึ่งอยู่ในประเทศที่สาม หรือ เป็นองค์การระหว่างประเทศ แจ้งระยะเวลาในการเก็บรักษาข้อมูลนั้น สิทธิในการขอให้แก้ไข หรือลบข้อมูลส่วนบุคคล หรือการคัดค้านการประมวลผล สิทธิในการร้องเรียนต่อเจ้าหน้าที่

กรณีข้อมูลนั้นมิได้รับมาโดยตรงจากเจ้าของข้อมูลส่วนบุคคลนั้น ๆ จะต้องแจ้งถึงที่มาของข้อมูลนั้น

กรณีที่มีการประมวลผลโดยระบบอัตโนมัติ ให้รวมถึงการทำโปรไฟล์ (Profiling) ต้องแจ้งข้อมูลที่เกี่ยวข้องด้วย ซึ่งอาจเกิดจากการประมวลผลนั้นด้วย

สิทธิในการแก้ไขข้อมูลส่วนบุคคล (Right to rectification) ตามมาตรา 16[111]

กรณีข้อมูลส่วนบุคคลนั้นไม่ถูกต้อง หรือไม่เป็นปัจจุบัน เจ้าของข้อมูลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการแก้ไขข้อมูลให้ถูกต้องโดยไม่ชักช้า โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งการแก้ไขให้แก่บุคคลอื่น ซึ่งข้อมูลส่วนบุคคลนั้นถูกเปิดเผย เว้นแต่ ไม่สามารถกระทำได้

สิทธิในการขอให้ลบข้อมูลส่วนบุคคล หรือ “สิทธิที่จะถูกลืม” (Right to be forgotten) ตามมาตรา 17

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการลบข้อมูลโดยไม่ชักช้า โดยเฉพาะข้อมูลที่เก็บรวบรวมในขณะที่เจ้าของข้อมูลส่วนบุคคลเป็นเด็ก และเจ้าของข้อมูลมีสิทธิขอให้ผู้ควบคุมข้อมูลลบข้อมูลในกรณีดังต่อไปนี้ด้วย

กรณีแรก ข้อมูลนั้นไม่จำเป็นอีกต่อไปเมื่อพิจารณาถึงวัตถุประสงค์ที่ทำการเก็บรวบรวม หรือ

กรณีที่สอง เจ้าของข้อมูลส่วนบุคคลเพิกถอนความยินยอมและไม่มีพื้นฐานกฎหมายรองรับการประมวลผลอีกต่อไป หรือ

กรณีที่สาม เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านโต้แย้งการประมวลผลข้อมูลตามมาตรา 18 (a) และไม่มีเหตุอันชอบด้วยกฎหมายที่สำคัญกว่าในการประมวลผลต่อไป หรือเจ้าของข้อมูลคัดค้านการประมวลผลตามมาตรา 18 (b)

---

[111] Regulation (EU) 2016/679 (General Data Protection Regulation) Article 16 Right to rectification reads:

“The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the daa subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.”

กรณีที่สี่ ข้อมูลถูกประมวลผลโดยไม่ชอบด้วยกฎหมาย หรือ

กรณีสุดท้าย ข้อมูลนั้นจำเป็นต้องถูกลบเพื่อปฏิบัติตามกฎหมายที่ควบคุมผู้ควบคุมข้อมูลส่วนบุคคล

เมื่อเจ้าของข้อมูลส่วนบุคคลนั้นได้ขอใช้สิทธิแล้วผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการขอใช้สิทธิลบข้อมูลให้แก่บุคคลอื่นซึ่งข้อมูลส่วนบุคคลนั้นถูกเปิดเผย เว้นแต่ไม่สามารถกระทำได้

สิทธิในการยับยั้งการประมวลผลข้อมูลส่วนบุคคล (Right to processing data) ตามมาตรา 18

สิทธิดังกล่าวได้กำหนดไว้ในมาตรา 18[112] ให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการยังยั้งการประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลใน 3 กรณี กล่าวคือ

กรณีแรก เจ้าของข้อมูลส่วนบุคคลคัดค้านความถูกต้องของข้อมูลส่วนบุคคลกรณีเช่นนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องยับยั้งการประมวลผลข้อมูลนั้นภายในกำหนดเวลาสำหรับการตรวจสอบความถูกต้องของข้อมูลนั้น หรือ

กรณีที่สอง ผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องมีข้อมูลส่วนบุคคลนั้น เพื่อการประมวลผลแต่เป็นการจำเป็นสำหรับเจ้าของข้อมูลเพื่อการก่อตั้ง ใช้สิทธิ หรือต่อสู้คดี หรือ

---

[112] Regulation (EU) 2016/679 (General Data Protection Regulation) Article 18 Right to restriction of processing reads:

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

กรณีสุดท้าย เจ้าของข้อมูลส่วนบุคคลคัดค้านวัตถุประสงค์ของการประมวลผลตามมาตรา 18 ผู้ควบคุมข้อมูลส่วนบุคคลต้องยับยั้งการประมวลข้อมูลนั้นจนกระทั่งมีการยืนยันว่าเหตุผลอันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลเหนือกว่าเจ้าของข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการจำกัดการประมวลผลให้แก่บุคคลอื่นซึ่งข้อมูลส่วนบุคคลนั้นถูกเปิดเผยตามมาตรา 19 เว้นแต่ไม่สามารถกระทำได้ หรือเป็นการใช้ความพยายามเกินสมควร

สิทธิในการโอนข้อมูลส่วนบุคคล (Right to data portability) ตามมาตรา 20

สิทธิดังกล่าวก่อให้เจ้าของข้อมูลส่วนบุคคลสามารถรับข้อมูลเกี่ยวกับตน ซึ่งได้ให้ไว้แก่ผู้ควบคุมข้อมูลส่วนบุคคลในรูปแบบที่เป็นแบบแผนใช้งานได้ และสามารถอ่านได้โดยเครื่อง (machine-readable) และมีสิทธิที่จะโอนข้อมูลนั้นไปยังผู้ควบคุมข้อมูลอื่น เว้นแต่ การประมวลผลนั้น เป็นความยินยอมของเจ้าของข้อมูลส่วนบุคคล หรือเป็นไปตามสัญญา หรือเป็นการประมวลผลโดยวิธีอัตโนมัติ แต่หากการใช้สิทธินี้นำมาซึ่งการละเมิดลิขสิทธิ์ในการประมวลผลข้อมูลส่วนบุคคลเจ้าของข้อมูลส่วนบุคคลไม่สามารถใช้นี้ได้

สิทธิในการคัดค้าน (Right to object) ตามมาตรา 21 ในการประมวลผลข้อมูลส่วนบุคคล[113]

---

[113] Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 21 GDPR Right to object reads:

1.The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. 2The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or de fence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall

สิทธิดังกล่าวได้บัญญัติไว้ในมาตรา 21 ผู้เป็นเจ้าของบุคคลมีสิทธิคัดค้านได้ เมื่อมีสถานการณ์พิเศษต่อเจ้าของข้อมูลส่วนบุคคล ในการประมวลผลข้อมูลส่วนบุคคลที่เป็นการจำเป็นเพื่อการปฏิบัติภารกิจอันเกี่ยวกับสาธารณประโยชน์ หรือเป็นการใช้อำนาจรัฐเหนือผู้ควบคุมข้อมูลส่วนบุคคล หรือเป็นการประมวลผลที่จำเป็นโดยมีวัตถุประสงค์เพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคลที่สาม โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่ประมวลผลข้อมูลนั้น เว้นแต่ จะแสดงได้ว่ามีกฎหมายบังคับนั้นเหนือกว่าประโยชน์ หรือสิทธิเสรีภาพของเจ้าของของมูลเพื่อการก่อตั้ง ใช้สิทธิ หรือการต่อสู้คดีหากข้อมูลส่วนบุคคลนั้นถูกประมวลผลเพื่อการตลาดเจ้าของข้อมูลมีสิทธิคัดค้านและหากมีการคัดค้านดังนั้นแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่ประมวลผลต่อไป ในกรณีที่ข้อมูลส่วนบุคคลนั้นถูกประมวลผลเพื่อวัตถุประสงค์ทางประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์ เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านได้ เว้นแต่ จำเป็นเพื่อประโยชน์สาธารณะ

สิทธิเกี่ยวกับการตัดสินใจโดยวิธีการอัตโนมัติ (Automated individual decision-making, including profiling) ตามมาตรา 22

บทบัญญัติเกี่ยวกับการตัดสินใจโดยวิธีอัตโนมัติได้ถูกบัญญัติไว้ในมาตรา 22[114] เป็นการคุ้มครองเจ้าของข้อมูลมิให้ตกอยู่ภายใต้การตัดสินใจโดยระบบอัตโนมัติเพียงอย่างเดียว ซึ่งรวมถึง

---

have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

[114] Regulation (EU) 2016/679 (General Data Protection Regulation). Article 22.

Automated individual decision-making, including profiling reads:

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

การทำโปรไฟล์ (Profiling) โดยเฉพาะอย่างยิ่งเมื่อการประมวลผลนั้น อาจทำให้เกิดผลทางกฎหมายอย่างมีนัยสำคัญแก่บุคคลดังกล่าว อย่างไรก็ตาม การตัดสินใจโดยวิธีอัตโนมัตินี้มีข้อยกเว้น 3 กรณีคือ

กรณีแรก เป็นการจำเป็นเพื่อการเข้าทำสัญญา หรือการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคล

กรณีที่สอง ได้รับอนุญาตตามกฎหมายของสหภาพยุโรป หรือกฎหมายของรัฐสมาชิก ซึ่งต้องมีมาตรการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลที่เหมาะสม

กรณีสุดท้าย เป็นการกระทำภายใต้ความยินยอมโดยจัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

ข้อบังคับ (Regulation (EU) 2016/679) ได้มีมาตรการและแนวทางในการปกป้องข้อมูลไบโอเมตริกซ์ (Biometrics) ในสหภาพยุโรป หากพิจารณาถึงข้อมูลไบโอเมตริกซ์ (Biometrics) ก็จะเป็นหนึ่งใน “หมวดหมู่พิเศษของข้อมูลส่วนบุคคล” (Processing of special categories of personal data) ที่ถูกบัญญัติไว้ตามมาตรา 9 ในภายในกฎข้อบังคับ (Regulation (EU) 2016/679) ดังนี้

ให้คำจำกัดความของข้อมูลไบโอเมตริกซ์ตาม Article 4 (14) เพื่อให้เป็นไปตาม Article 9[115] การประมวลผลข้อมูลส่วนบุคคลที่เปิดเผยเกี่ยวกับเชื้อชาติ หรือเผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา หรือปรัชญา หรือการเป็นสมาชิกสหภาพแรงงานและการประมวลผลข้อมูลพันธุกรรมข้อมูลไบโอเมตริกซ์เพื่อจุดประสงค์ในการระบุบุคคลธรรมดาข้อมูลเกี่ยวกับสุขภาพ หรือข้อมูลที่เกี่ยวข้องชีวิต ทางเพศของบุคคลธรรมดา หรือรสนิยมทางเพศจะต้องห้าม เว้นแต่จะเป็นข้อยกเว้นตามกฎหมายที่กำหนดไว้เฉพาะโดยมี 10 เงื่อนไขตาม Article 9 ดังนี้

เจ้าของข้อมูลได้ให้ความยินยอมโดยชัดแจ้ง เว้นแต่ การยินยอมนั้นต้องห้ามโดยกฎหมาย

การประมวลผลเป็นการจำเป็นเพื่อวัตถุประสงค์ในการปฏิบัติตามหน้าที่ หรือใช้สิทธิเฉพาะเจาะจงของผู้ควบคุมข้อมูลส่วนบุคคล หรือของเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับการจ้างงาน ประกันสังคม ทั้งนี้ เท่าที่ชอบด้วยกฎหมายของประเทศนั้น ๆ

---

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9 (1), unless point (a) or (g) of Article 9 (2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

[115] Regulation (EU) 2016/679 (General Data Protection Regulation). Article 9.

Processing of special categories of personal data reads:

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

การประมวลผลจำเป็นในการปกป้องประโยชน์ของเจ้าของข้อมูลส่วนบุคคล หรือของบุคคลอื่นในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สมารถให้ความยินยอมทางทางกายภาพ หรือตามกฎหมายได้

การประมวลผลนั้นเป็นกิจกรรมที่ชอบด้วยกฎหมายและมีมาตรการป้องกันโดยองค์กรสมาคม หรือบุคคลซึ่งไม่แสวงหากำไร โดยมีวัตถุประสงค์ในทางการเมือง ปรัชญา ศาสนา หรือสหภาพแรงงาน ภายใต้เงื่อนไขว่าต้องเป็นการประมวลผลข้อมูลของสมาชิก หรือบุคคลที่เคยเป็นสมาชิกและไม่เปิดเผยข้อมูลนั้น

เป็นข้อมูลส่วนบุคคลที่ถูกเปิดเผยไว้เป็นสาธารณะโดยเจ้าของข้อมูลส่วนบุคคล

การประมวลผลนั้นเพื่อการก่อตั้ง การใช้สิทธิ หรือการต่อสู้คดี หรือการปฏิบัติหน้าที่ของศาล

การประมวลผลนั้นจำเป็นเพื่อวัตถุประสงค์ในทางประโยชน์สาธารณะโดยประเทศต้องมีมาตรการป้องกันประโยชน์ของเจ้าของข้อมูลด้วย

การประมวลผลนั้นจำเป็นเพื่อวัตถุประสงค์ทางการแพทย์

การประมวลนั้นจำเป็นเพื่อประโยชน์สาธารณะเกี่ยวกับสุขภาพของประชาชน เช่น การป้องกันอันตรายร้ายแรงที่ข้ามพรมแดน หรือเพื่อให้มีมาตรฐานความปลอดภัยและคุณภาพทางสาธารณสุขที่สูง

การประมวลผลจำเป็นเพื่อประโยชน์สาธารณะ เช่น ประวัติศาสตร์ สถิติวิทยาศาสตร์ โดยมีมาตรการป้องกันความปลอดภัยของรัฐ

หลักการสำคัญของกฎหมายตามข้อบังคับ (Regulation (EU) 2016/679) การคุ้มครองข้อมูลส่วนบุคคลทั่วไป (General Data Protection Regulation) ของสหภาพยุโรปที่สำคัญดังนี้

การคุ้มครองข้อมูลส่วนบุคคลและเพิ่มเติมสิทธิของเจ้าของข้อมูลอย่างเข้มงวด ข้อมูลส่วนบุคคลที่จัดเก็บต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยอิสระและชัดแจ้ง ต้องมีการแจ้งวัตถุประสงค์ในการนำข้อมูลไปใช้ที่เข้าใจง่าย เจ้าของข้อมูลต้องสามารถแจ้งแก้ไข ลบ หรือให้หยุดการประมวลผลข้อมูลได้ เมื่อไม่มีความจำเป็นต้องเก็บข้อมูล หรือเมื่อไม่ประสงค์จะให้นำข้อมูลไปใช้ เจ้าของข้อมูลสามารถขอให้โอนย้ายข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นได้ ผู้ควบคุมข้อมูลต้องจัดทำระบบให้เจ้าของข้อมูลสามารถเข้าถึงข้อมูลของตนได้อย่างรวดเร็ว

กำหนดให้ผู้ควบคุมข้อมูลต้องมีมาตรการทางเทคนิคที่เหมาะสมและเป็นระบบ เพื่อให้มั่นใจและเพื่อแสดงได้ว่าการประมวลผลข้อมูลเป็นไปตามข้อกำหนดของกฎข้อบังคับ (Regulation (EU) 2016/679: GDPR)

การกำหนดให้ผู้ควบคุมข้อมูลจะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer) ที่มีความเชี่ยวชาญด้านการจัดเก็บข้อมูล เพื่อควบคุมดูแลข้อมูลส่วนบุคคลไว้โดยเฉพาะ สำหรับกรณีการประมวลผลข้อมูลในบางกรณี เช่น กรณีที่ผู้ควบคุมข้อมูลประกอบด้วยการประมวลผลข้อมูลส่วนบุคคลขนาดใหญ่ที่ต้องมีการควบคุมดูแลอย่างสม่ำเสมอและอย่างเป็นระบบ เป็นต้น

เพิ่มมาตรการในการแจ้งเหตุกรณีได้มีการละเมิดข้อมูลส่วนบุคคล (Data Breach Notification) โดยผู้ควบคุมข้อมูลภายใน 72 ชั่วโมง พร้อมระบุรายละเอียดแก่หน่วยงานผู้รับผิดชอบและเจ้าของข้อมูลส่วนบุคคลตามเงื่อนไขที่ข้อบังคับ (Regulation (EU) 2016/679: GDPR) กำหนดไว้[116]

มีการกำหนดบทลงโทษ หรือการกำหนดค่าปรับตามความร้ายแรง หรือหนักเบาของการกระทำที่ไม่ปฏิบัติตามที่ข้อบังคับ (Regulation (EU) 2016/679: GDPR) กำหนดไว้[117]

การประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษ ข้อบังคับ(Regulation (EU) 2016/679: GDPR) ได้ให้การควบคุมที่แข็งแกร่งยิ่งขึ้นในการประมวลผลข้อมูลหมวดหมู่พิเศษ ในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษที่มีความละเอียดอ่อนจะต้องตอบสนองเงื่อนไขตามข้อ (10) ในการประมวลผลข้อมูลส่วนบุคคลของประเทศสมาชิกจะต้องมีอย่างน้อยหนึ่งประเภทต่อไปนี้[118]

---

[116] Regulation (EU) 2016/679: GDPR reads:

(85) "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay"

[117] มัณฑณา ศรีพงษ์พันธ์. (2561). ***ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเฉพาะกรณีข้อมูลตำแหน่งของผู้ใช้บริการ***. สารนิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม. หน้า 45.

[118] เรื่องเดียวกัน, หน้า 45.

ประเภทแรก การยินยอมอย่างชัดเจนจากเจ้าข้อมูลส่วนบุคคลนั้น ได้ให้ความยินยอมอย่างชัดเจน อย่างไรก็ตามกฎหมายสหภาพ หรือรัฐสมาชิกอาจจำกัดสถานการณ์ที่สามารถให้ความยินยอมได้

ประเภทที่สอง ภาระผูกพันทางกฎหมายที่เกี่ยวข้องกับการจ้างงาน หรือการดำเนินการเป็นสิ่งจำเป็นสำหรับภาระผูกพันทางกฎหมายในด้านการจ้างงานและกฎหมายประกันสังคม หรือข้อตกลงร่วม

ประเภทที่สอง การดำเนินการเป็นสิ่งจำเป็นเพื่อปกป้องผลประโยชน์ที่สำคัญของบุคคลหรือของบุคคลอื่น โดยทั่วไปจะจำกัดการประมวลผล ยกเว้น จำเป็นสำหรับกรณีฉุกเฉินทางการแพทย์

ประเภทที่สี่ ไม่ใช่สำหรับองค์กรที่แสวงหาผลกำไร หรือดำเนินการในกิจกรรมที่ชอบด้วยกฎหมายขององค์กรที่ไม่แสวงหาผลกำไรและเกี่ยวข้องกับสมาชิก หรือบุคคลที่เกี่ยวข้องเท่านั้นและจะไม่เปิดเผยข้อมูลส่วนบุคคลภายนอกโดยไม่ได้รับความยินยอม

ประเภทที่ห้า ข้อมูลสาธารณะ หรือการประมวลผลเกี่ยวข้องกับข้อมูลส่วนบุคคลซึ่งเป็นการเปิดเผยต่อสาธารณะ

ประเภทที่หก การเรียกร้องทางกฎหมาย หรือการดำเนินการเป็นสิ่งที่จำเป็นสำหรับการดำเนิดการทางแพ่ง หรือการป้องกันข้อเรียกร้องทางกฎหมาย หรือการปฏิบัติตามอำนาจหน้าที่ของศาล

ประเภทที่เจ็ด ผลประโยชน์สาธารณะที่สำคัญ หรือการดำเนินการเป็นสิ่งจำเป็นสำหรับเหตุผลของผลประโยชน์สาธารณะที่สำคัญบนพื้นฐานของกฎหมายสหภาพ หรือรัฐสมาชิก

ประเภทที่แปด การดูแลสุขภาพ หรือการประมวลผลมีความจำเป็นสำหรับวัตถุประสงค์ด้านการดูแลสุขภาพและอยู่ภายใต้การป้องกันที่เหมาะสม

ประเภทที่เก้า สาธารณสุข หรือการประมวลผลมีความจำเป็นสำหรับวัตถุประสงค์ด้านสุขภาพและเป็นไปตามกฎหมายของสหภาพ หรือรัฐสมาชิก

ประเภทสุดท้าย การเก็บ รวบรวม หรือการประมวลผลที่จำเป็นสำหรับการเก็บถาวรวัตถุประสงค์การวิจัยทางวิทยาศาสตร์ หรือประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติและเป็นไปตามกฎหมายของสหภาพ หรือรัฐสมาชิกสามารถแนะนำเงื่อนไขเพิ่มเติมเกี่ยวกับสุขภาพ พันธุกรรม หรือข้อมูลไบโอเมตริกซ์ได้

ดังนั้น หากพิจารณาถึงข้อมูลไบโอเมตริกซ์เป็นข้อมูลที่อ่อนไหวพิเศษภายใต้ (GDPR) แต่ถ้าใช้เพื่อจุดประสงค์ในการ “ระบุตัวตน” โดยไม่ซ้ำใครตามมาตรา 9 (1) ภาพถ่ายจำนวนมากที่อัพโหลดไปยังฐานบริการคลาวด์จะไม่ถือเป็นข้อมูลที่มีความละเอียดอ่อน แต่หากใช้เพื่อจุดประสงค์ในการระบุตัวตน เช่น หนังสือเดินที่จดจำลักษณะบุคคลจากภาพที่ถือว่าเป็นอุปสรรคด้านความปลอดภัยของ

สนามบิน[119] ข้อมูลประเภทนี้มีความอ่อนไหวมากขึ้น เนื่องจากข้อมูลประเภทนี้สามารถสร้างความเสี่ยงที่มีนัยสำคัญยิ่งขึ้นต่อสิทธิและเสรีภาพของบุคคล (GDPR) ตระหนักถึงสิ่งนี้และวางขั้นตอนเพิ่มเติม สำหรับผู้ที่ต้องการประมวลผลข้อมูลส่วนบุคคล เพื่อให้แน่ใจว่าได้รับการคุ้มครองมากขึ้น ในการประมวลผลข้อมูลที่สำคัญในหกฐานที่ถูกต้องตามกฎหมายที่ระบุไว้ในมาตรา 6 ของ (GDPR) ตามรายละเอียดข้างต้น นอกจากนี้ยังแสดงให้เห็นถึงหนึ่งในพื้นฐานที่เพิ่มเติมที่มีอยู่ภายในมาตรา 9 (2) ของ (GDPR) ที่ใช้บังคับในการยินยอมอย่างชัดเจนในการปฏิบัติตามกฎหมายการจ้างงาน สิ่งนี้จะได้รับการคุ้มครองข้อมูลไบโอเมตริกซ์ โดยพื้นฐานและผลประโยชน์ที่สำคัญของพนักงาน

3.2.3 มาตรการทางกฎหมาย (Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018)

พระราชบัญญัติคุ้มครองข้อมูลทั่วไป (General Data Protection Act: GDPR) และพระราชบัญญัติคุ้มครองข้อมูล (The Data Protection Act 2018) ชื่ออย่างเป็นทางการของระเบียบ (EU) 2018/1725[120] ซึ่งแทนที่ Regulation (EC) No 45/2001 ยังเรียกว่า “(GDPR)” ของรัฐสภายุโรปและสภา 23 ตุลาคม 2018เกี่ยวกับการคุ้มครองบุคคลธรรมดาที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลโดยสถาบันสหภาพหน่วยงานสำนักงานและหน่วยงานอิสระและการเคลื่อนไหวของอิสระดังกล่าว ระเบียบนี้ถือเป็น “ภาคคู่” ของ (GDPR)[121] โดยนำไปใช้กับทุกบริษัท และองค์กรที่ประมวลผลข้อมูลส่วนบุคคลภายในสหภาพยุโรปและดำเนินการในภาคเอกชน บทบาทสำคัญ เช่น ผู้ควบคุมข้อมูลและผู้ประมวลผลถูกกำหนดในระเบียบเช่นเดียวกับกรณีของ (GDPR) วัตถุประสงค์ของกฎใหม่นี้ เพื่อให้พลเมืองของสหภาพยุโรปมีสิทธิเช่นเดียวกับที่ได้รับภายใต้ (GDPR)

---

[119] Phil Lee. (2016). ***Article Privacy, Security and Information Law***. reads:

“Biometric data is sensitive data under the GDPR: WRONG (ISH)! You can be forgiven for thinking this. Biometric data can be sensitive data under the GDPR - but only if used for the purpose of “uniquely identifying” someone (Art. 9 (1). A bunch of photographs uploaded onto a cloud service would not be considered sensitive data, for example, unless used for identification purposes - think, for instance, of airport security barriers that recognize you from your passport photograph.

[120] Regulation (EU) 2018/1725 of the European parllament and of the council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No1247/2002/EC (Text with EEA relevance).

[121] Novelties. (2019). ***Deloitte’s view on the implementation of Regulation*** (EU) 2018/1725. (Online). Available: https://www2.deloitte.com/be/en/pages/risk/articles/gdpr-for-eu-institutions.html. [2562, 7 October]

ข้อมูลและยกเลิกกฎระเบียบ (EC) หมายเลข 45/2001 และหมายเลข 1247/2002 / EC ในการคุ้มครองบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล การคุ้มครองข้อมูลส่วนบุคคลตาม (EU) Directive 95/46 เกิดขึ้นในปี 1995 เป็นบทบัญญัติที่มีผลบังคับระหว่างประเทศฉบับแรกที่ให้ความคุ้มครองข้อมูลส่วนบุคคที่ถูกสร้างขึ้นโดยประเทศสมาชิกสหภาพยุโรป ข้อบังคับนี้ให้การคุ้มครองข้อมูลส่วนบุคคลและเสรีภาพในการเคลื่อนไหวของข้อมูลและยกเลิกกฎระเบียบ (EC) หมายเลข 45/2001 และ 1247/2002 / EC (ข้อความที่มีความเกี่ยวข้องกับ EEA) ทั้งนี้ ยังให้การรับรองว่าข้อมูลจะได้รับการคุ้มครองอย่างเท่าเทียมกันตลอดทั้งภาคยุโรป เพื่อให้ทันสังคมโลกมีการเปลี่ยนแปลงอย่างมากในปัจจุบัน โดยเฉพาะบริบทการสื่อสารผ่านทางอิเล็กทรอนิกส์ ที่มีการเติบโตพัฒนาอย่างรวดเร็วมาก จึงมีการปรับปรุงแก้ไข ซึ่งมีดังนี้

คำสั่ง (Directive 2002/58 / EC) ซึ่งแก้ไขเพิ่มเติมโดยคำสั่ง (Directive 2009/136 / EC) ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลและการปกป้องความเป็นส่วนตัวในภาคการสื่อสารอิเล็กทรอนิกส์

คำสั่ง (Directive 2006/24 / EC) เกี่ยวกับการเก็บรักษาข้อมูลที่สร้างขึ้นจากการประมวลผลที่เกี่ยวข้องกับการให้บริการการสื่อสารอิเล็กทรอนิกส์ที่เปิดเผยต่อสาธารณชนหรือเครือข่ายการสื่อสารสาธารณะ

การประมวลผลข้อมูลส่วนบุคคลไม่ว่าด้วยเหตุใด ๆ จะต้องดำเนินการภายใต้มาตรา 6 ของ (GDPR) นอกจากนี้ การประมวลผลเกี่ยวข้องกับข้อมูลหมวดหมู่พิเศษซึ่งรวมถึงข้อมูลไบโอเมตริกซ์จะมีเหตุยกเว้น ตามมาตรา 9 บทบัญญัติตามมาตรา 6 (1) แสดงถึงพื้นฐานสำหรับการประมวลผล ในบริบทของการเฝ้าระวังวิดีโอฐานที่ใช้บังคับรวมถึงความยินยอมของบุคคลที่เกี่ยวข้องกับมาตรา 6 (1) (a) สำหรับความยินยอมอย่างอิสระที่ถูกต้องตามกฎหมายได้รับการแจ้งในการประมวลผลที่เฉพาะเจาะจงและไม่เป็นที่น่าสงสัยก่อนจะมีการประมวลผล หรือความจำเป็นสำหรับผลประโยชน์ที่ชอบด้วยกฎหมายที่ดำเนินการโดยผู้ควบคุมมาตรา 6 (1) (f) การดำเนินการเพื่อจุดประสงค์ของ “ผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ควบคุม” จะถูกต้องตามกฎหมายเว้นแต่ผลประโยชน์นั้นจะถูกแทนที่ด้วยสิทธิขั้นพื้นฐานและเสรีภาพของแต่ละบุคคล

โดยมีหลักการที่เป็นสาระสำคัญตาม (EU Directive 95/46) คือ[122]การรักษาคุณภาพของข้อมูล มาตรการของการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย ข้อกำหนดในการประมวลผลข้อมูลพิเศษ หรือข้อมูลที่อ่อนไหว (Sensitive Data) สิทธิในการได้รับแจ้งการเก็บข้อมูล สิทธิในการ

---

[122] นคร เสรีรักษ์. (2561). ***บทความ GDPR คือ อะไร สำคัญอย่างไร? ทำไมจึงต้องเข้าใจ GDPR?***. (ออนไลน์). เข้าถึงได้จาก: https://www.matichon.co.th/article/news_902461. [2562, 29 กรกฎคม]

เข้าถึงข้อมูล สิทธิในการคัดค้านการประมวลผล การรักษาความปลอดภัยในการประมวลผลข้อมูล การส่งผ่านข้อมูลส่วนบุคคลไปยังประเทศที่สาม

นอกจากการควบคุมการส่งข้อมูลภายในประเทศสมาชิกแล้ว สำหรับประเทศที่ไม่ได้เป็นสมาชิกสหภาพยุโรป หากจะทำการติดต่อรับ หรือส่งข้อมูลกับประเทศสมาชิกสหภาพยุโรป จะต้องมีมาตรการการคุ้มครองข้อมูลที่เหมาะสมเป็นที่พอใจแก่สหภาพยุโรปด้วย เช่นกัน ซึ่งมาตรการที่เหมาะสมที่อียู (EU) ได้ตั้งไว้ แม้กระทั่งประเทศสหรัฐอเมริกา ที่มีการค้าและการลงทุนกับประเทศสมาชิกสหภาพยุโรปมากที่สุด และมีการเคลื่อนไหวของข้อมูลข่าวสารมากที่สุด ยังคงต้องพยายามหาวิธีการประนีประนอม เพื่อเป็นทางออกและแก้ไขปัญหาความขัดแย้งของทั้งสองฝ่าย

มาตรการและแนวทางในการปกป้องข้อมูลไบโอเมตริกซ์ (Biometrics) ในสหภาพยุโรป

หากการประมวลผลข้อมูลส่วนบุคคลเกี่ยวข้องกับข้อมูลหมวดหมู่พิเศษ นอกเหนือจากการประมวลผลข้อมูลทั่วไปตามกฎหมายแล้ว ภายใต้มาตรา 6 แล้วจะต้องมีการยกเว้นในบทบัญญัติมาตรา 9 เพื่อการประมวลผล ทางเทคโนโลยีในการจดจำข้อมูลส่วนบุคคลให้รวมถึงข้อมูลประเภทหมวดหมู่พิเศษคือข้อมูลไบโอเมตริกซ์หากสามารถระบุตัวบุคคลได้ถึงเอกลักษณ์ของบุคคลนั้น ข้อมูลไบโอเมตริกซ์เกี่ยวข้องกับลักษณะทางกายภาพสรีรวิทยา หรือ พฤติกรรมของบุคคล ดังนั้นหากเทคโนโลยีการจดจำใบหน้าใช้เพื่อระบุบุคคลใดบุคคลหนึ่งโดยเฉพาะเมื่อเทียบกับประเภทของบุคคล เช่น การจัดทำโปรไฟล์ของลูกค้าตามเชื้อชาติ เพศ อายุ สิ่งนี้จะเป็นการประมวลผลข้อมูลไบโอเมตริกซ์

กฎหมายความเป็นส่วนตัวของข้อมูลในสหภาพยุโรปได้กำหนด “ข้อมูลไบโอเมตริกซ์” (Biometrics) เป็น “หมวดหมู่ข้อมูลส่วนบุคคลพิเศษ” และห้าม “การประมวลผล” ข้อมูลไบโอเมตริกที่แม่นยำมาจากข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิคเฉพาะที่เกี่ยวข้องกับลักษณะทางกายภาพสรีรวิทยา หรือพฤติกรรมของบุคคลธรรมดาซึ่งช่วย หรือการยืนยันระบุเอกลักษณ์ของบุคคลธรรมดานั้น เช่น ภาพใบหน้าหรือข้อมูล (Dactyloscopic) สำหรับผู้ประมวลผล “ไม่ประมวลซ้ำกับบุคคลธรรมดา” เป็นสิ่งต้องห้าม

การนำมาบังคับใช้แก่การประมวลผลข้อมูลส่วนบุคคลทั้งหมด หรือบางส่วนโดยวิธีอัตโนมัติแต่จะไม่นำมาบังคับใช้แก่การประมวลผลข้อมูลส่วนบุคคล ซึ่งไม่ได้ตกอยู่ภายใต้กฎหมายแห่งประชาคมยุโรป (Directive 95/46/EC) ให้นิยามที่สำคัญของข้อมูลส่วนบุคคลไว้ใน Article 4 ซึ่งมีสาระสำคัญดังต่อไปนี้

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลที่ถูกระบุตัว หรือ บุคคลที่อาจถูกระบุตัวตนได้ โดยบุคคลซึ่งถูกระบุตัวตนได้โดยตรง หรือโดยอ้อม โดยเฉพาะอย่างยิ่งจาก

การอ้างอิงโดยเลขบัตรประชาชน หรือลักษณะอื่น ซึ่งบ่งเฉพาะทางร่างกาย สรีรวิทยา จิตใจ เศรษฐกิจ วัฒนธรรม หรือ อัตลักษณ์ทางสังคม[123]

"การประมวลผลข้อมูลส่วนบุคคล" หมายถึง การดำเนินการต่าง ๆ หรือชุดของการดำเนินการซึ่งกระทำต่อข้อมูลส่วนบุคคล ไม่ว่าจะเป็นไปโดยวิธีอัตโนมัติ หรือไม่ก็ตาม เช่น การเก็บรวบรวม การบันทึก การจัดระเบียบ การเก็บรักษา การเปลี่ยนแปลง หรือปรับปรุง การกู้คืน การใช้ การเปิดเผยโดยการส่ง การเผยแพร่ หรือการทำให้สามารถเข้าถึงได้โดยประการอื่น การจัดหรือการรวม การปิดกั้น การลบ หรือ การทำลาย[124]

"ผู้ควบคุม" หมายถึง บุคคลธรรมดา หรือนิติบุคคล หน่วยงานรัฐ ตัวแทน หรือบุคคลอื่นใด ไม่ว่าโดยตนเองหรือโดยร่วมกับบุคคลอื่นกำหนดวัตถุประสงค์และวิธีในการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่วัตถุประสงค์และวิธีในการประมวลผลข้อมูลส่วนบุคคลกำหนดโดยกฎหมาย หรือกฎของประเทศ หรือประชาคม ผู้ควบคุมข้อมูลส่วนบุคคล หรือหลักเกณฑ์เฉพาะเพื่อการแต่งตั้งผู้ควบคุมข้อมูลให้กำหนดโดยกฎหมายของประเทศหรือประชาคม[125]

---

[123] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018.

Article 3. Definitions reads:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

[124] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

Article 3 Definition reads:

(3)'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

[125] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018.

Article 3. Definition reads:

(8)'controller' means the Union institution or body or the directorate-general or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law;

“การทำโปรไฟล์” หมายถึง การประมวลผลข้อมูลโดยระบบอัตโนมัติโดยการใช้ข้อมูลเหล่านั้นประเมินมุมมองของบุคคล โดยเฉพาะอย่างยิ่งการวิเคราะห์และประเมินประสิทธิภาพเกี่ยวกับการทำงาน สถานะทางเศรษฐกิจ สุขภาพ ความชอบ ความสนใจ ความน่าไว้วางใจ พฤติกรรม หรือการเคลื่อนไหว[126]

“การละเมิดข้อมูลส่วนบุคคล” หมายถึง การละเมิดความปลอดภัยที่นำไปสู่การทำลายโดยมิชอบ หรือกระทำผิดกฎหมาย การแก้ไข การเปลี่ยนแปลง การเปิดเผยข้อมูล หรือ การเข้าถึงข้อมูลส่วนบุคคล การส่งออกไป การจัดเก็บ หรือดำเนินการใด ๆ ก็ตามโดยมิได้รับอนุญาต[127]

“ความยินยอมของเจ้าของข้อมูลส่วนบุคคล” หมายถึง การแสดงเจตนาโดยอิสระมีลักษณะเฉพาะเจาะจงและบ่งบอกถึงวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลแสดงถึงความยินยอมให้ทำการประมวลผลข้อมูลส่วนบุคคล การบังคับใช้คำสั่ง (Directive 95/46/EC) กำหนดให้รัฐสมาชิกต้องนำบทบัญญัติแห่ง (Directive) นี้มาใช้บังคับแก่การประมวลผลข้อมูลส่วนบุคคลซึ่งผู้ควบคุมข้อมูลตั้งอยู่ในดินแดนของรัฐสมาชิก ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลตั้งอยู่ในหลายดินแดนของรัฐสมาชิก ผู้ควบคุมข้อมูลต้องปฏิบัติตามกฎหมายของแต่ละประเทศด้วย หรือ ผู้ควบคุมข้อมูลส่วนบุคคลมิได้ตั้งอยู่ในดินแดนของรัฐสมาชิก แต่กฎหมายของรัฐสมาชิกนั้นถูกนำมาใช้บังคับต่อผู้ควบคุมข้อมูลส่วนบุคคล และในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกดินแดนของสหภาพยุโรป แต่วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลใช้อุปกรณ์ โดยระบบอัตโนมัติ หรือไม่ก็ตามซึ่งตั้งอยู่ในดินแดนแห่งรัฐสมาชิก เว้นแต่ อุปกรณ์นั้นใช้เพื่อวัตถุประสงค์ในการส่งข้อมูลข้ามดินแดนเท่านั้น ซึ่งในกรณีดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลต้องตั้งตัวแทนในดินแดนของรัฐสมาชิก[128]

---

[126] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018.

Article 3 Definition reads:

(5) ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyses or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

[127] Regulation (EU) 2018/1725 Article 3 Definition reads:

(16) “personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”

[128] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

Article 3 Definition reads:

“ข้อมูลทางพันธุกรรม” หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับพันธุกรรมของบุคคลธรรมดา ซึ่งได้รับ หรือ สืบทอดมา โดยข้อมูลนี้นี้มีเอกลักษณ์พิเศษเกี่ยวกับสรีรวิทยา หรือ สุขภาพของบุคคลนั้น โดยแสดงผลจากการวิเคราะห์ตัวอย่างทางชีวภาพของบุคคลนั้น[129]

“ข้อมูลไบโอเมตริกซ์” หมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิคเฉพาะที่เกี่ยวข้องกับลักษณะทางกายภาพสรีรวิทยา หรือพฤติกรรมของบุคคลธรรมดาซึ่งอนุญาตหรือการระบุอัตลักษณ์ของบุคคลนั้น เช่น ภาพใบหน้า หรือข้อมูลลายนิ้วมือ (Dactyloscopic)[130]

“ข้อมูลสุขภาพ” หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสุขภาพกาย หรือสุขภาพจิตของบุคคลธรรมดารวมถึงการให้บริการด้านการดูแลสุขภาพ หรือเพศ ซึ่งเปิดเผยข้อมูลเกี่ยวกับสถานะสุขภาพของบุคคล[131]

“ผู้ใช้” หมายถึง บุคคลธรรมดาที่ใช้เครือข่าย หรืออุปกรณ์ปลายทางที่ดำเนินการภายใต้การควบคุมของสถาบัน หรือองค์กรของสหภาพ[132]

---

(15) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

[129] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

Article 3 Definition reads:

(17) ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

[130] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

Article 3 Definition reads:

(18) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

[131] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

Article 3 Definition reads:

(19) ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status;

[132] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

Article 3 Definition reads:

(23) ‘user’ means any natural person using a network or terminal equipment operated under the control of a Union institution or body;

“เครือข่ายการสื่อสารทางอิเล็กทรอนิกส์” หมายถึง ระบบส่งสัญญาณไม่ว่าจะอยู่บนพื้นฐานของโครงสร้างพื้นฐานถาวร หรือความสามารถในการบริหารจัดการแบบรวมศูนย์และในกรณีที่มีการปรับเปลี่ยนหรือ กำหนดเส้นทางอุปกรณ์และทรัพยากรอื่น ๆ รวมถึงองค์ประกอบเครือข่ายที่ไม่ได้ใช้งาน โดยสายสัญญาณวิทยุออปติคอล หรือ แม่เหล็กไฟฟ้าอื่น ๆ รวมถึงเครือข่ายดาวเทียมคงที่ (วงจร - และแพ็คเก็ต - สวิทซ์รวมถึงอินเทอร์เน็ต) และเครือข่ายภาคพื้นดินมือถือ ระบบสายไฟฟ้าที่ใช้สำหรับการส่งสัญญาณ ใช้สำหรับการกระจายเสียงวิทยุและโทรทัศน์และเครือข่ายเคเบิลทีวีโดยไม่คำนึงถึงประเภทของข้อมูลที่สื่อความหมาย[133]

ภายใต้กฎหมาย (GDPR) ได้สร้างมาตรฐานการปกป้องข้อมูลไบโอเมตริกซ์ สำหรับการรวบรวมข้อมูลที่ละเอียดอ่อนเป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้จริงของบุคคลที่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ ตาม Article 10 ถือว่า “การประมวลผลข้อมูลพันธุกรรม ข้อมูลไบโอเมตริกซ์ เพื่อจุดประสงค์ในการระบุตัวตนของบุคคลที่เป็นเอกลักษณ์เฉพาะ” เป็นสิ่งต้องห้ามโดยปริยาย เว้นแต่ จะเป็นข้อยกเว้นตามกฎหมายที่กำหนดไว้เฉพาะ ซึ่งประกอบด้วยข้อมูลที่เกี่ยวข้องกับบุคคล ห้ามมิให้มีการประมวลผลข้อมูลส่วนบุคคลดังนี้[134]

เชื้อชาติหรือเผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา หรือ ความเชื่ออื่นที่มีลักษณะคล้ายคลึงกัน สมาชิกสหภาพแรงงาน สุขภาพ หรือสภาพร่างกาย หรือจิตใจ ชีวิต เพศ

---

[133] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

Article 3 Definition reads:

(25) ‘electronic communications network’ means a transmission system, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

[134] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

Article 10 Processing of special categories of personal data reads:

1.Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

และรสนิยมทางเพศ ข้อมูลทั่วไปและข้อมูลไบโอเมตริกซ์ สำหรับการประมวลผลข้อมูลส่วนบุคคลได้มี 6 กรณี[135] ดังนี้

กรณีแรก กระทำต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

กรณีที่สอง จำเป็นเพื่อปฏิบัติตามสัญญา ซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาในสัญญานั้น หรือเป็นการปฏิบัติตามขั้นตอนก่อนมีการเข้าทำสัญญาโดยคำร้องขอของเจ้าของข้อมูลส่วนบุคคล

กรณีที่สาม การประมวลผลเป็นการจำเป็นเพื่อปฏิบัติหน้าที่ตามกฎหมาย

กรณีที่สี่ การประมวลผลเป็นการจำเป็นเพื่อการปกป้องผลประโยชน์สำคัญของเจ้าของข้อมูลส่วนบุคคล

กรณีที่ห้า การประมวลผลจำเป็นเพื่อการปฏิบัติหน้าที่อันเป็นประโยชน์สาธารณะ หรือเป็นการใช้อำนาจขององค์กรรัฐต่อผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคลที่สาม ซึ่งข้อมูลนั้นถูกเปิดเผย หรือ

กรณีสุดท้าย การประมวลผลเป็นการจำเป็นเพื่อวัตถุประสงค์เกี่ยวกับผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคลที่สาม เว้นแต่ ผลประโยชน์ที่ทับซ้อนกับประโยชน์เกี่ยวกับสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล ซึ่งต้องได้รับการคุ้มครอง

ใน Regulation (EU) 2018/1725 มาตรา 5 ได้กำหนดเรื่องคุณภาพของข้อมูล โดยกำหนดให้ข้อมูลส่วนบุคคลต้องประมวลผลโดยชอบด้วยกฎหมาย หรือ เป็นธรรม การเก็บรวบรวมข้อมูลส่วนบุคคลต้องมีวัตถุประสงค์ที่ชัดแจ้ง ชอบด้วยกฎหมาย และต้องไม่ประมวลผลนอกเหนือจากวัตถุประสงค์ที่ระบุไว้แต่การประมวลเพื่อประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์ ไม่ถือเป็นการขัดกับวัตถุประสงค์[136]

---

[135] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

Article 10 Processing of special categories of personal data reads:

(b) the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

[136] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

Article 5 Lawfulness of processing reads:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body;

(b) processing is necessary for compliance with a legal obligation to which the controller is subject;

หากรัฐสมาชิกมีมาตรการการคุ้มครองที่เพียงพอ ข้อมูลส่วนบุคคลนั้นต้องเกี่ยวข้อง และไม่เกินความจำเป็นต่อวัตถุประสงค์ซึ่งข้อมูลส่วนบุคคลนั้นถูกเก็บรวบรวมและหรือประมวลผลในภายหน้า นอกจากนี้ ข้อมูลส่วนบุคคลนั้นต้องถูกต้องเป็นปัจจุบันและมีมาตรการเพื่อทำให้แน่ใจว่าข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์จะถูกทำลายหรือแก้ไขให้ถูกต้อง หรือสมบูรณ์ และการเก็บรักษาข้อมูลนั้น จะต้องเก็บไว้เท่าระยะเวลาที่จำเป็นเพื่อการประมวลผลตามวัตถุประสงค์นั้น

เมื่อมีการเก็บรวบรวมข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลว่าได้ข้อมูลนั้นมาจากบุคคลใด รวมทั้งต้องแจ้งถึงตัวผู้ควบคุมข้อมูลและตัวแทน (ถ้ามี) วัตถุประสงค์ในการประมวลข้อมูล และข้อมูลอื่น ๆ เช่น ผู้รับหรือประเภทของผู้รับข้อมูลส่วนบุคคล สิทธิในการเข้าถึงและแก้ไขข้อมูล หากข้อมูลส่วนบุคคลนั้นผู้ควบคุมข้อมูลส่วนบุคคลมิได้เก็บรวบรวมโดยตรงจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเจ้าของข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคลและเสรีภาพในการเคลื่อนไหวของข้อมูล ทั้งยังให้การรับรองว่าข้อมูลจะได้รับการคุ้มครองอย่างเท่าเทียมกัน โดยมีหลักการที่เป็นสาระสำคัญดังนี้ คือ[137]

(c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(e) processing is necessary in order to protect the vital interests of the data subject or of another natural person.

2. The basis for the processing referred to in points (a) and (b) of paragraph 1 shall be laid down in Union law.

[137] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 reads:

(29) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection, as the context of their processing could create significant risks to the fundamental rights and freedoms. Such personal data should not be processed unless the specific conditions set out in this Regulation are met. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. In addition to the specific requirements for processing of sensitive data, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs, in

มาตรการการรักษาคุณภาพของข้อมูลในการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย ข้อกำหนดในการประมวลผลข้อมูลพิเศษ หรือข้อมูลที่อ่อนไหว (Sensitive data) สิทธิในการได้รับแจ้งการเก็บข้อมูลต่าง ๆ สิทธิในการเข้าถึงข้อมูล สิทธิในการเข้าถึงข้อมูล สิทธิในการคัดค้านการประมวลผล การรักษาความปลอดภัยในการประมวลผลข้อมูล

การพิจารณาถึงความเหมาะสมที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลนั้นต้องพิจารณาถึงความเสี่ยงที่เกิดขึ้นจากการประมวลผล และลักษณะของข้อมูลที่ทำการประมวลผลโดยสรุปข้อกำหนดของ (EU) ได้กำหนดให้รัฐสมาชิกอนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลภายใต้หลักทั่วไป ดังนี้

ความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล Regulation (EU) 2016/679 มาตรา 4 (1) ได้บัญญัติให้ความคุ้มครอง ข้อมูลส่วนบุคคลให้หมายความรวมถึงอัตลักษณ์ออนไลน์ หรือ สิ่งที่สามารทำให้ระบุตัวตนในทางออนไลน์ได้ด้วย (Online identifier) ซึ่งในส่วนอารัมภบท ข้อที่ 30[138] บัญญัติไว้ว่า ข้อมูลส่วนบุคคลอาจเชื่อมโยงกับตัวบุคคลในออนไลน์ที่มีการจัดเตรียมโดยอุปกรณ์หรือด้วยแอปพลิเคชัน เช่น ระบบอินเตอร์เน็ตโปรโตคอล ตัวระบุคุกกี้ (Cookies identifiers) หรือตัวระบอื่น ๆ ที่อาจทิ้งร่องรอยไว้ได้ โดยเฉพาะอย่างยิ่งข้อมูลอัตลักษณ์ของบุคคลที่ได้รับจากเซิร์ฟในการสร้างโปรไฟล์ของบุคคลนั้น และสามารถใช้ระบุตัวบุคคลได้ เช่น คดีตัวอย่าง ความยินยอมในการใช้ (Cookies)

คดี Planet 49[139]

ประเด็น การให้ความยินยอม เมื่อวันอังคาร ที่ 1 ตุลาคม 2562 โดยศาลยุติธรรมแห่งสหภาพยุโรปได้มีคำวินิจฉัยปัญหาข้อกฎหมายเบื้องต้นในคดี C-673/17[140] ตามที่ศาลยุติธรรมแห่งสหพันธ์

---

particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

[138] Regulation (EU) 2016/679 of the European Parliament and of the Council of 23 October 2018 reads:

Acting in accordance with the ordinary legislative procedure Whereas reads: (30) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union law should provide for specific and suitable measures so as to protect fundamental rights and the personal data of natural persons.

[139] Planet49: CJEU Rules on Cookie Consent.

สาธารณรัฐเยอรมนีขอให้มีคำวินิจฉัยในคดีพิพาทระหว่างสหพันธ์องค์กรผู้บริโภคเยอรมนี (The Federation of German Consumer Organisations) สหพันธ์และบริษัท Planet 49 ซึ่งเป็นผู้ให้บริการเกมออนไลน์ โดยสหพันธ์ฯ เห็นว่าการที่ Planet49 ขอความยินยอมให้ใช้คุกกี้บนเว็บไซต์ของตนเองโดยใช้ (Pre-ticked check) นั้นไม่ชอบด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคลตาม Directive 95/46 ซึ่งใช้บังคับอยู่ ณ ขณะนั้น ก่อนบังคับใช้ (GDPR) แต่ในการพิจารณาข้อพิพาทดังกล่าว ศาลได้พิจารณา (GDPR) ประกอบด้วย เนื่องจาก Directive 95/46 นั้นได้ถูกยกเลิกแล้วโดย (GDPR) โดยข้อพิพาทระหว่างสหพันธ์สาธารณรัฐเยอรมนี ในฐานะผู้ฟ้องคดีแทนผู้บริโภคและ Planet49 เกิดขึ้นเมื่อวันที่ 23 กันยายน 2556 เมื่อ Planet 49 จัดให้มีการเสี่ยงโชคออนไลน์ในเว็บไซต์ของตนโดยในการเสี่ยงโชคดังกล่าว ผู้ใช้บริการต้องกรอกข้อมูลส่วนบุคคลหลาย ๆ ประการ เช่น ชื่อ ที่อยู่ รหัสไปรษณีย์ เป็นต้น โดยการใช้คุกกี้ ทางเว็บไซต์ได้มีการเลือกมาให้แล้ว ในการยินยอม ว่ามีการยินยอมให้ใช้คุกกี้ได้ติ๊กไว้ล่วงหน้า (Pre-select tick)[141]

คำวินิจฉัยของศาลยุติธรรมแห่งสหภาพยุโรปส่วนที่เกี่ยวกับความยินยอมศาลได้วางหลักการที่สำคัญไว้ 2 ประการดังนี้[142]

ประการแรก การให้ความยินยอมเพื่อประมวลผล เก็บ รวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลนั้น (GDPR) มาตรา 4 (11) กำหนดว่า ความยินยอมนั้นต้องเป็นความ

---

[140] ennart Schüßler, James Fenelon. (2019). Planet49: CJEU Rules on Cookie Consent reads:

Background facts:

Planet49 ('Planet49') ran a promotional lottery on its website.

As part of entering the lottery users were presented with two tick-boxes. The first was an unchecked tick-box to receive third party advertising. In order to enter the competition, users needed to tick this box.

The second was a pre-ticked box allowing Planet49 to set cookies to track the user's behaviour online. The German Federation of Consumer Organisations (the 'Federation') claimed that these two check-boxes did not satisfy German law requirements, and sought an injunction requiring Planet49 to cease using them. The case ultimately reached the German Federal Court of Justice (the 'Bundesgerichtshof'), which in turn referred the case to the CJEU for preliminary ruling. (Online). Available: https://www.twobirds.com/en/news/articles /2019/global/planet49-cjeu-rules-on-cookie-consent. [2019, 18 December]

[141] Gabriela Zanfir-Fortuna. (2019). ***Planet49 CJEU Judgment brings some 'Cookie Consent' Certainty to Planet Online Tracking.NEWS AND COMMENTS ON EU LAW***. (Online). Available: https://europeanlawblog.eu/2019/ 10/08/planet49-cjeu-judgment-brings-some-cookie-consent-certainty-to-planet-online-tracking/.[2019, 18 December]

[142] ศุภวัชร์ มาลานนท์. (2019). ***คุกกี้และความยินยอมตากฎหมาย.*** คณะนิติศาสตร์ มหาวิทยาลัยสงขลานครินทร์. หน้า 45.

ยินยอมโดยอิสระ ชัดเจน ได้รับแจ้งข้อมูลที่เพียงพอต่อการตัดสินใจ ไม่สร้างความสับสนหลงผิด และต้องมีการแสดงออกของการกระทำโดยชัดแจ้งว่ามีการให้ความยินยอม (Active consent) โดยอารัมภบทข้อ 32 อธิบายเพิ่มเติมว่า หากเป็นกรณีที่ได้เลือกมาให้แล้ว (Pre-select tick) กรณีนี้จะถือไม่ได้ว่าได้มีการให้ความยินยอม (Silence pre-ticked boxes or inactivity should not therefore constitute consent.)

ประการสุดท้าย ข้อมูลที่ Planet 49 ต้องให้แก่ผู้ใช้บริการโดยชัดแจ้งรวมถึงระยะเวลาที่คุกกี้จะถูกเก็บไว้และใช้ประโยชน์ด้วย และต้องแจ้งให้ทราบด้วยว่าจะมีการให้สิทธิบุคคลที่สามในการเข้าถึงคุกกี้หรือไม่

ดังนั้น Planet 49 มาตรการในการให้ความยินยอมใช้คุกกี้ ใน “ความยินยอม” ใด ๆ ที่ได้รับจากการใช้คุกกี้ หรือ เทคโนโลยีที่คล้ายคลึงกัน บนอุปกรณ์ของผู้ใช้จะต้องเป็นไปตามเงื่อนไขหากไม่พบหนึ่งในนั้นความยินยอมดังกล่าวนั้น เป็นการไม่ถูกต้อง

การประมวลผลจะทำได้เท่าที่จำเป็นในการทำนิติกรรมสัญญาใด ๆ จากเจ้าของข้อมูลเท่านั้น

การประมวลผลจะต้องอยู่ภายใต้กรอบของกฎหมาย

การประมวลผลจะต้องกระทำเพื่อปกป้องผลประโยชน์สำคัญของผู้เป็นเจ้าของข้อมูล การประมวลผลจำเป็นที่จะต้องกระทำเพื่อผลประโยชน์ของสาธารณะหรือในการดำเนินงานของหน่วยงานของรัฐที่ได้รับมอบหมายให้เป็นผู้ควบคุมข้อมูล หรือเปิดเผยข้อมูลต่อบุคคลที่สาม

การประมวลผลที่จำเป็นและอยู่ภายใต้กรอบของกฎหมายจะต้องไม่กระทบต่อผลประโยชน์หรือสิทธิขั้นพื้นฐานของผู้เป็นเจ้าของข้อมูล

นอกจากนี้ ข้อตกลงนี้ยังได้ให้ความสำคัญเกี่ยวกับความลับ ความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล รวมถึงข้อยกเว้น ในการเปิดเผยข้อมูลกรณีที่ไม่ได้นำข้อมูลไปใช้ประโยชน์สาธารณะ แต่นำไปใช้เพื่อประโยชน์ส่วนตัว และกำหนดเกี่ยวกับเรื่องความเสียหายที่เกิดขึ้นต่อข้อมูลเมื่อมีการประมวลผลโดยไม่ชอบด้วยกฎหมาย และการเปิดเผยข้อมูลจะต้องไม่ละเมิดต่อความมั่นคงของรัฐ

การส่งข้อมูลส่วนบุคคล หรือทำการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศนั้น ข้อตกลงดังกล่าวนี้ ห้ามไม่ให้ทำการส่งข้อมูลส่วนบุคคล หรือ ทำการโอนข้อมูลส่วนบุคคล หรือเพื่อทำการประมวลผล หรือมีเจตนาที่จะส่งไปยังต่างประเทศไม่ได้เป็นประเทศสมาชิกของสหภาพยุโรป เว้นแต่ ประเทศที่ได้รับข้อมูลส่วนบุคคลนั้น จะมีระดับการให้การคุ้มครองข้อมูลส่วนบุคคลในระดับที่มาตรฐานพอ อย่างไรก็ตาม ภายใต้ข้อตกลงฉบับนี้ ยังได้มีการกำหนดข้อยกเว้นไว้เฉพาะเช่น กรณีได้มีการยินยอมจากผู้เป็นเจ้าของข้อมูลไว้อย่างชัดแจ้ง หรือการส่งข้อมูลส่วนบุคคล หรือ

การโอนข้อมูลส่วนบุคคลนั้นมีความจำเป็น เพื่อปฏิบัติตามสัญญาที่เจ้าของข้อมูลและผู้ควบคุมข้อมูลมีสัญญาระหว่างกัน หรือ เพื่อปฏิบัติการให้เป็นไปตามข้อตกลงก่อนเข้าทำสัญญาตามคำร้องขอของเจ้าของข้อมูลนั้นโดยมี 10 เงื่อนไขตาม Article 9 ที่ทำให้การประมวลผลข้อมูลส่วนบุคคล “หมวดหมู่พิเศษ”เป็นหมวดกฎหมายที่คุ้มครองข้อมูลส่วนบุคคลเกี่ยวข้องกับพนักงานในการที่จะถูกนำข้อมูลไบโอเมตริกซ์ไปใช้มากที่สุด คือ “ความยินยอมอย่างชัดเจน” ซึ่งหมายความว่าคุณไม่สามารถใช้ระบบจดจำลายนิ้วมือได้โดยไม่ต้องขอความยินยอมจากพนักงานที่จะเก็บลายนิ้วมือนั้นได้

สิทธิและขอบเขตของเจ้าของข้อมูล ตามระเบียบข้อตกลงฉบับนี้ได้บัญญัติให้สิทธิของเจ้าของข้อมูลตาม Article 15 ดังนี้

สิทธิในการได้รับแจ้งข้อมูล (Right to be informed) เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการแจ้งข้อมูลจากผู้ควบคุมข้อมูลว่าข้อมูลส่วนบุคคลของตนถูกนำไปใช้เพื่อการใด มีข้อมูลใดถูกนำไปใช้บ้าง ข้อมูลที่ถูกรวบรวมไปจะถูกเก็บไว้ที่ใดบ้างและนานเท่าใด[143]

สิทธิในการเข้าถึงข้อมูล (Right of access by the data subject) เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอว่าข้อมูลส่วนบุคคลของตนถูกประมวลผลอย่างไร[144]

สิทธิในการแก้ไขข้อมูลให้ถูกต้อง (Right to rectification) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้องและเป็นปัจจุบัน[145]

สิทธิในการลบ (Right to Erasure) สิทธินี้รู้จักกันในชื่อ “สิทธิในการถูกลืม (Right to be forgotten)” คือ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลลบข้อมูลส่วนบุคคลของตน โดยแนวคิดนี้เกิดจากที่ชาวยุโรปคนหนึ่งเคยถูกตัดสินว่ามีความผิดและได้รับการลงโทษทาง

---

[143] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 Reads:

Article 17 Right of access by the data subject

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 48 relating to the transfer.

[144] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

Article 17 Right of access by the data subject Reads:

[145] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 Reads:

Section 3 Rectification and erasure. Article 18 Right to rectification

“The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.”

กฎหมายด้วยการจำคุกไปแล้ว แต่ประวัติของตนยังมีบันทึกความผิดเดิมอยู่ จึงได้เรียกร้องขอให้ลบบันทึกนั้นออก[146]

สิทธิในการจำกัดการประมวลผลข้อมูล (Right to restriction of processing) เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการร้องขอให้องค์กรจำกัดการประมวลผลข้อมูล โดยผู้เก็บข้อมูลสามารถเก็บข้อมูลส่วนบุคคลต่อไปได้ แต่ไม่สามารถนำไปประมวลผลข้อมูลได้อีกต่อไป เว้นแต่เจ้าของข้อมูลจะให้ความยินยอม หรือได้รับการยกเว้นตามที่กฎหมายกำหนด[147]

สิทธิในการโอนย้ายข้อมูล (Right to data portability) เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการได้รับข้อมูลส่วนบุคคลของตนเองที่เคยให้แก่ผู้ควบคุมข้อมูล ในรูปแบบที่สามารถอ่านและ

---

[146] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 Reads:

Article 19 Right to erasure (‘right to be forgotten’)

[147] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 Reads:

Article 20Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 23 (1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject’s consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

4. In automated filing systems restriction of processing shall in principle be ensured by technical means. The fact that the personal data are restricted shall be indicated in the system in such a way that it becomes clear that the personal data may not be used.

เข้าใจได้อย่างแพร่หลาย และมีสิทธิ์ที่จะโอนข้อมูลของตนไปยังผู้ควบคุมข้อมูลรายอื่น ซึ่งเจ้าของข้อมูลมีสิทธิขอให้โอนโดยตรงได้หากสามารถกระทำได้ในทางปฏิบัติ[148]

สิทธิในการคัดค้าน (Right to object) เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล[149]

สิทธิในการคัดค้านการตัดสินใจแทนโดยวิธีการอัตโนมัติรวมถึงการทำโปรไฟล์ (Right on Automated Individual Decision-Making, including Profiling) เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะคัดค้านการตัดสินใจโดยอิงจากการประมวลผลโดยอัตโนมัติรวมถึง (Profiling) ซึ่งมีผลทางกฎหมาย หรือส่งผลกระทบอย่างยิ่งยวดต่อเจ้าของข้อมูล ยกเว้นในบางกรณี เช่น การตัดสินใจนั้นจำเป็นต่อการปฏิบัติตามข้อสัญญา การตัดสินใจนั้นได้รับอนุญาตจากกฎหมายของสหภาพยุโรปหรือรัฐสมาชิก หรือได้รับความยินยอมที่ชัดเจนจากเจ้าของข้อมูล[150]

ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคลผู้ควบคุมจะต้องแจ้งเตือนล่าช้าได้ไม่เกิน 72 ชั่วโมงหลังจากทราบว่ามีการการละเมิดข้อมูลส่วนบุคคลต่อเจ้าหน้าที่กำกับดูแล เว้นแต่ การละเมิด

---

[148] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 Reads:

Article 22 Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (d) of Article 5 (1) or point (a) of Article 10 (2) or on a contract pursuant to point (c) of Article 5 (1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another or to controllers other than Union institutions and bodies, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 19. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

[149] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 Reads:

Section 4 Right to object and automated individual decision-making. Article 23 Right to object

[150] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 Reads:

Article 24 Automated individual decision-making, including profiling

ไม่น่าจะส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลนั้น ในกรณีที่การแจ้งเตือนไปยังผู้ดูแลการป้องกันข้อมูลในสหภาพยุโรปไม่ได้ภายใน 72 ชั่วโมงจะต้องมีเหตุผลสำหรับความล่าช้านั้น[151] หากฝ่าฝืนมีบทลงโทษสำหรับองค์กรที่ฝ่าฝืนข้อกำหนด (GPPR) สูง โดยกำหนดให้ปรับสูงสุด 20 ล้านยูโร หรือร้อยละ 4 ของรายได้ทั้งหมดทั่วโลกของบริษัท ขึ้นอยู่กับว่าจำนวนใดจะสูงกว่ากันก็ให้ใช้จำนวนนั้น การฝ่าฝืนข้อกำหนด (GDPR) เช่น องค์กรไม่ได้รับความยินยอมจากลูกค้าในการประมวลผลข้อมูลส่วนบุคคล การไม่แจ้งเจ้าของข้อมูล หรือเจ้าหน้าที่เมื่อมีการรั่วไหลของข้อมูลส่วนบุคคล[152]

3.2.4 มาตรการข้อมูลไบโอเมตริกซ์ (Biometrics)

ประเด็นที่หนึ่ง คำจำกัดความของข้อมูลส่วนบุคคลที่ได้รับการคุ้มครองข้อมูลส่วนบุคคลภายใต้ (GDPR) ตามกฎหมายความเป็นส่วนตัวของข้อมูลในสหภาพยุโรป โดยกำหนดให้ข้อมูลไบโอเมตริกซ์เป็น “หมวดหมู่ข้อมูลส่วนบุคคลพิเศษ” และห้าม “การประมวลผล” องค์ประกอบหลักของคำนิยามหมายถึง “ข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุ หรือระบุตัวตนของบุคคลนั้น คำจำกัดความที่กำหนดโดยกฎระเบียบนั้นได้รวมถึง “ข้อมูลพันธุกรรม” (หมวดหมู่ของข้อมูลส่วนบุคคลพิเศษ) โดย (GDPR) จัดให้มีเงื่อนไขที่สอดคล้องกันสำหรับการประมวลผลข้อมูลส่วนบุคคลประเภทนี้ ในแง่ของความต้องการเฉพาะ เพื่อประโยชน์ของบุคคลนั้นและสังคมโดยรวม ซึ่ง Regulation (EU) 2018/1725 มาตรา 3 (1) ได้บัญญัติคำนิยามไว้เหมือนกัน แต่อยู่คนละมาตราของคำนิยาม โดยมีความแตกต่างของกฎข้อบังคับ (Regulation (EU) 2016/679) และ (Regulation (EU) 2018/1725) ดังนี้[153]

---

[151] Regulation (EU) 2016/679 Article 33 Reads:

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

[152] Regulation (EU) 2016/679 Article 83 Reads:

General conditions for imposing administrative fines reads: 5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20, 000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

[153] Regulation (EU) 2016/679 & Regulation (EU) 2018/1725: GDPR

“ข้อมูลพันธุกรรม” ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนโดยบัญญัติอยู่ในหมวดหมู่ทั่วไปด้วย แต่อย่างไรก็ตาม “ข้อมูลพันธุกรรม” ถูกบัญญัติไว้หมวดพิเศษอย่างชัดเจนของกฎข้อบังคับ (Regulation (EU) 2016/679) มาตรา 4 (13) (Regulation (EU) 2018/172) ตามมาตรา 3 (17)

“ข้อมูลไบโอเมตริกซ์” (Biometrics) ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนจัดให้จำแนกอยู่ในหมวดพิเศษของ (Regulation (EU) 2016/679) มาตรา 4 (14) และ (Regulation (EU) 2018/1725) ตามมาตรา 3 (18) ซึ่งเป็นหมวดหมู่ข้อมูลส่วนพิเศษถูกบัญญัติห้ามมิให้มีการประมวลผลไว้ในของ (Regulation (EU) 2016/679) มาตรา 9 (1) และ(Regulation (EU) 2018/1725) มาตรา 10 (1)

เมื่อพิจารณาจากขอบเขตการบังคับใช้กฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation) กฎระเบียบ (General Data Protection Regulation: GDPR) ของสหภาพยุโรป (European Union : EU) ซึ่งเป็นกฎระเบียบที่ออกมาเพื่อคุ้มครองประชาชนในกลุ่มประทศ (EU) มิให้ถูกล่วงละเมิดในความเป็นส่วนตัว เนื่องจากปัจจุบันมีการล่วงละเมิดในความเป็นส่วนตัว และนำข้อมูลส่วนบุคคลของประชาชน เพื่อไปแสวงหาผลประโยชน์ หรือเปิดเผยโดยไม่ได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลก่อน จนเป็นการสร้างความเสียหาย แก่เจ้าของข้อมูลเป็นอย่างมาก โดยเป็นกฎระเบียบที่ปรับปรุงใหม่ให้เหมาะสมกับสถานการณ์ที่แตกต่างไปจาก (EU) Directive 95/46/EC (EU Directive 95/46) โดยมีประการสำคัญดังนี้

ขอบเขตบังคับใช้กฎหมายในเชิงพื้นที่โดยบังคับใช้ทุกหน่วยงานที่มีการประมวลผลข้อมูลส่วนบุคคลของบุคคลที่อาศัยอยู่ใน (EU) โดยไม่คำนึงถึงว่าบริษัทนั้นจะตั้งอยู่ที่ใด ไม่ว่าการประมวลผลนั้นจะทำใน (EU) หรือไม่ก็ตาม และบังคับใช้กับทุกกิจกรรมที่เป็นการจำหน่ายสินค้าและบริการแก่พลเมืองของ (EU) และทุกกิจกรรมที่มีลักษณะเป็นการติดตามพฤติกรรมของพลเมืองที่เกิดขึ้นใน (EU)

บทลงโทษในกรณีที่ก่อให้เกิดความเสียหาย หรือการรั่วไหลของข้อมูล (Data Breach) ผู้ที่ไม่ปฏิบัติตามข้อกำหนดจะถูกปรับเป็นจำนวนเงินถึง 20 ล้านยูโร หรือในอัตราร้อยละ 4 ของรายได้ต่อปี แต่อย่างก็ตาม สหภาพยุโรปได้มีมาตรการเพื่อเสริมความแข็งแกร่งให้กับบทบาทการกำกับดูแลของ (European Data Protection Supervisor)[154] และการบังคับใช้กฎระเบียบดังกล่าวนี้แก่

---

[154] Regulation (EU) 2018/1725 raeds:

(81) In order to strengthen the supervisory role of the European Data Protection Supervisor and the effective enforcement of this Regulation, the European Data Protection Supervisor should, as a sanction of last resort, have the power to impose administrative fines. The fines should aim at sanctioning the Union institution or body — rather than

ผู้ควบคุมอย่างมีประสิทธิภาพในการปกป้องข้อมูลของสหภาพยุโรป จึงมีข้อบังคับให้มีอำนาจในการกำหนดค่าปรับทางปกครอง โดยค่าปรับมีเป้าหมายเพื่อลงโทษสถาบัน หรือองค์กรของสหภาพ ซึ่งไม่ใช่ตัวบุคคล สำหรับการไม่ปฏิบัติตามข้อบังคับนี้ เพื่อยับยั้งการละเมิดกฎระเบียบนี้ในอนาคตและเพื่อส่งเสริมวัฒนธรรมการปกป้องข้อมูลส่วนบุคคลภายในสถาบันและองค์กรของสหภาพ โดยคำนึงถึงสถานการณ์ที่เกี่ยวข้องทั้งหมดของสถานการณ์เฉพาะ ความลักษณะแรง และระยะเวลาของการละเมิด โดยไม่เน้นการลงโทษทางอาญา ซึ่งบทลงโทษทางอาญานั้น อาจอนุญาตให้ตัดผลกำไรที่ได้จากการฝ่าฝืนกฎระเบียบตามพระราชบัญญัตินี้ โดยเคารพหลักการทั่วไปของกฎหมายสหภาพซึ่งตีความโดยศาลยุติธรรม[155]

การให้ความยินยอม การเก็บรวบรวม การใช้การประมวลผล การเปิดเผยข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยในการขอความยินยอมต้องดำเนินการในรูปแบบที่เข้าใจได้ และสามารถเข้าถึงได้โดยสะดวกและต้องแจ้งวัตถุประสงค์ของการประมวลผลข้อมูลในการขอความยินยอม การขอความยินยอมต้องมีความชัดเจน ใช้ภาษาที่ง่ายต่อการเข้าใจ รวมถึงการยถอนให้ความยินยอมต้องดำเนินการได้โดยสะดวก

สิทธิของเจ้าของข้อมูลภายใต้กฎหมายฉบับนี้ สิทธิที่จะได้รับการแจ้งเมื่อเกิดความเสียหาย (Breach notification) การแจ้งเป็นหน้าที่ที่ต้องปฏิบัติเมื่อเกิดความเสียหาย หรือ การรั่วไหลของ

---

individuals — for non-compliance with this Regulation, to deter future violations of this Regulation and to foster a culture of personal data protection within the Union institutions and bodies. This Regulation should indicate the infringements subject to administrative fines and the upper limits and criteria for setting the associated fines. The European Data Protection Supervisor should determine the amount of the fine in each individual case, by taking into account all relevant circumstances of the specific situation, with due regard to the nature, gravity and duration of the infringement, its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. When imposing an administrative fine on a Union institution or body, the European Data Protection Supervisor should consider the proportionality of amount of the fine. The administrative procedure for the imposition of fines on Union institutions and bodies should respect the general principles of Union law as interpreted by the Court of Justice.

[155] Regulation (EU) 2016/679 raeds:

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice.

ข้อมูลซึ่งเกิดผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล โดยผู้ประมวลผลข้อมูลจะต้องแจ้งให้ลูกค้า และผู้ควบคุมข้อมูลโดยไม่ชักช้าหลังเกิดความเสียหายภายใน 72 ชั่วโมง

สิทธิที่จะรับรู้และเข้าถึงข้อมูลของตน (Right to access) เจ้าของข้อมูลมีสิทธิที่จะได้รับการแจ้งจากผู้ควบคุมข้อมูลว่ามีการประมวลผลข้อมูล หรือไม่ การประมวลผลนั้นดำเนินการที่ไหน อย่างไร มีวัตถุประสงค์เพื่ออะไร และเจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอผู้ควบคุมข้อมูลทำสำเนาข้อมูลดังกล่าวได้ รวมทั้งข้อมูลในรูปแบบอิเล็กทรอนิกส์โดยไม่คิดค่าใช้จ่าย

สิทธิในการขอลบข้อมูลที่เกี่ยวกับตนเอง (Right to erase หรือ Right to be forgotten) เจ้าของข้อมูลมีสิทธิแจ้งดังนี้[156] แจ้งให้ลบข้อมูล ระงับการเผยแพร่ หยุดการประมวลผลโดยบุคคลที่สามแจ้งให้ลบข้อมูลที่ไม่มีส่วนเกี่ยวข้องตามวัตถุประสงค์ในการจัดเก็บครั้งแรก แจ้งให้ลบข้อมูลที่เจ้าของข้อมูลได้ยกเลิกความยินยอมแล้ว

สิทธิที่จะได้รับข้อมูลเกี่ยวกับตัวเอง (Data portability) สิทธิที่จะได้รับข้อมูลเกี่ยวกับตนเองในรูปแบบที่สามารถใช้งานได้ตามปกติ ทั้งในรูปที่อ่านได้ด้วยเครื่องหรืออุปกรณ์

สิทธิที่จะได้รับการคุ้มครองตั้งแต่ครั้งแรก (Privacy by design หรือ Privacy by default) ได้กำหนดระบบความคุ้มครองตั้งแต่ครั้งแรกของระบบมากกว่าการเพิ่มมาตรการในภายหลัง ซึ่งเป็นการคุ้มครองสิทธิของเจ้าของข้อมูล และผู้ควบคุมข้อมูลจะเก็บ หรือประมวลผลข้อมูลได้เท่าที่มีความจำเป็นเพื่อวัตถุประสงค์ และจะต้องจำกัดการเข้าถึงข้อมูลกับผู้ที่ไม่มีส่วนเกี่ยวข้องใด ๆ

สิทธิที่จะได้รับการคุ้มครองโดยเจ้าหน้าที่รับผิดชอบ (Data protection officers: DPO) ในการแต่งตั้งเจ้าหน้าที่สำหรับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลและมีภารกิจในการติดตามและประมวลผลข้อมูล

ดังนั้น มาตรการในการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปจึงมีความเข้มงวดสูงดังที่ได้กล่าวมาแล้วข้างต้น โดยผู้วิจัยได้ทราบถึงแนวความคิด ทฤษฎี เกี่ยวกับกับมาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลไบโอเมตริกซ์ภายใต้กฎหมาย (EU) มีความหมายอย่างไร

ในประเด็นแรก “ข้อมูลทางพันธุกรรม” ซึ่งเป็นข้อมูลส่วนบุคคลในประเภทข้อมูลทั่วไป แต่ก็ถูกจัดให้อยู่ในหมวดหมู่ประเภทข้อมูลพิเศษ เนื่องจาก “ข้อมูลพันธุกรรม” แม้ว่าจะถูกรวบรวมไว้ในการระบุตัวตนของบุคคลทั่วไปด้วยก็ตาม แต่ก็ยังสามารถพิจารณาได้ว่าสิ่งนี้เป็นข้อมูลไบโอเมตริกซ์ และได้รับความคุ้มครองพิเศษตามมาตรา 10 (1) ในการใช้กับการระบุตัวตนทางพันธุกรรมเท่านั้น ซึ่งกฎระเบียบได้ให้การคุ้มครองเป็นพิเศษในข้อมูลส่วนบุคคลบางประเภทว่ามีความละเอียดอ่อนและสิ่งนี้จะต้องมีการป้องกันและเข้มงวดมากขึ้น สำหรับการประมวลผลข้อมูลไบโอ

---

[156] สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2562). ***รู้จัก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล.*** เอกสารทางวิชาการ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. หน้า 26-29.

เมตริกซ์ดังกล่าว จากข้อมูลส่วนบุคคลซึ่งเป็นไปตามธรรมชาติของแต่ละบุคคลนั้นมีความละเอียดอ่อนต่อความรู้สึก โดยเฉพาะอย่างยิ่งเกี่ยวกับสิทธิขั้นพื้นฐานและเสรีภาพได้รับการคุ้มครองที่เฉพาะเจาะจงเป็นพิเศษ เนื่องจากบริบทของการประมวลผลของแต่ละบุคคลสามารถสร้างความเสี่ยงที่สำคัญได้ และผู้เป็นเจ้าของข้อมูลไบโอเมตริกซ์ไม่อาจแก้ไขเปลี่ยนแปลงได้เมื่อข้อมูลดังกล่าวรั่วไหล

การคุ้มครองข้อมูลประเภทพิเศษนั้น โดยกฎระเบียบ (GDPR) ไม่เคยมีมาก่อนเนื่องจากคำสั่ง (Directive)[157] ได้ใช้แนวทางที่คล้ายกันในเรื่องทั่วไปนี้ตามมาตรา 9 ของคำสั่งมีข้อห้ามทั่วไปเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่เปิดเผยเชื้อชาติ หรือ ชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา หรือ ปรัชญา สมาชิกสหภาพแรงงานและการประมวลผลข้อมูลที่เกี่ยวข้องกับสุขภาพ หรือ ชีวิตทางเพศ ที่เกี่ยวกับหมวดหมู่พิเศษของข้อมูล (ข้อมูลที่ละเอียดอ่อน) ได้รับการคุ้มครองในหมวดหมู่พิเศษ คำจำกัดความไม่เพียงรวมแต่เฉพาะข้อมูลทั่วไปที่มีข้อมูลละเอียดอ่อน แต่ยังรวมถึงข้อมูลที่สามารถบ่งชี้ หรือ สรุปได้ว่าข้อมูลที่ละเอียดอ่อนนั้นสามารถระบุตัวตนเกี่ยวกับบุคคลนั้นได้ ต้องห้ามการประมวลผล เว้นแต่กฎหมายอนุญาตให้กระทำได้ตตาม 10 ของ (GDPR)[158]

ประเด็นที่สอง ความยินยอมและการถอนความยินยอมข้อมูลไบโอเมตริกซ์ (Biometrics) หลักในการแจ้งผลกระทบเนื่องจากการถอนความยินยอมของกฎข้อบังคับ (Regulation (EU) 2016/679) และ (Regulation (EU) 2018/1725) ตามมาตรา 7 ของข้อมูลไบโอเมตริกซ์ (Biometrics) เมื่อการประมวลผลข้อมูลส่วนบุคคลตกอยู่ภายใต้ขอบเขตการบังคับใช้กฎหมาย (GDPR) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักพื้นฐานในการประมวลผลข้อมูลส่วนบุคคล เช่น ต้องประมวลผลข้อมูล “โดยชอบด้วยกฎหมาย” เป็นธรรม และโปร่งใสต่อเจ้าของข้อมูล ซึ่งการประมวลผลข้อมูลจะชอบด้วยกฎหมายหรือไม่นั้น โดยเฉพาะการให้ความยินยอมตามสัญญาจ้างของลูกจ้าง ซึ่งมี “ผลประโยชน์ที่ถูกต้องตามกฎหมาย” ที่ไม่สามารถใช้เป็นพื้นฐานทางกฎหมายในการประมวลผลข้อมูลไบโอเมตริกซ์ได้ตาม มาตรา 29 ของ (GDPR)

---

[157] Paul De Hert, Vagelis Papakonstantinou. (2012). ***Article The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals***. International Hellenic University, Greece

[158] Regulation (EU) 2018/1725 Article 10 Processing of special categories of personal data reads:

1.“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.”

โดย (GDPR) เพิ่มหมวดเกี่ยวกับสัญญาจ้างงาน ซึ่งนายจ้างเป็นผู้ประมวลผลข้อมูลไบโอเมตริกซ์ของพนักงาน หากนายจ้างไม่สามารถโต้แย้งได้ว่ากำลังประมวลผลข้อมูลไบโอเมตริกซ์อยู่ภายใต้ข้อตกลงร่วม หรือทำเพื่อผลประโยชน์สาธารณะ หรือไม่มีทางเลือกอื่นใด จะต้องพิจารณาจาก “ความยินยอม” (Consent) ซึ่งเป็นหัวใจสำคัญของการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งความยินยอมในการใช้ (Cookies) โดยอิสะ ชัดเจนต้องรับแจ้งข้อมูลที่เพียงพอต่อการตัดสินใจไม่สร้างความสับสนหลงผิด และต้องมีการแสดงออกของการกระทำโดยชัดแจ้งว่ามีการให้ความยินยอม (Active consent)ตามอารัมภบทข้อ 32 หากเป็นกรณีที่ได้เลือกมาให้แล้วล่วงหน้า (Pre-select tick)

กรณีนี้จะถือไม่ได้ว่าได้มีการให้ความยินยอม (Silence pre-ticked boxes or inactivity should not therefore constitute consent.) การให้ความยินยอมประกอบด้วยดังต่อไปนี้[159]

เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมอย่างเสรี (Freely given) หมายถึง เจ้าของข้อมูลมีทางเลือกในการตัดสินใจว่าจะให้ หรือไม่ให้ข้อมูลส่วนใดบ้าง และการไม่ให้ความยินยอมในส่วนนั้นต้องไม่ทำให้เกิดผลเสียแก่เจ้าของข้อมูลส่วนบุคคลด้วย

การให้ความยินยอมมีวัตถุประสงค์ที่เฉพาะเจาะจงในการขอความยินยอม (Specific) หมายถึง การประมวลผลข้อมูลนต้องเป็นไป เพื่อวัตถุประสงค์ที่ได้แจ้งไว้กับเจ้าของข้อมูลส่วนบุคคลเท่านั้น

การแจ้งการประมวลผลข้อมูลให้เจ้าของข้อมูลส่วนบุคคลทราบ (Informed) หมายถึง เจ้าของข้อมูลส่วนบุคคลจะต้องทราบแล้วว่าจะมีการประมวลผลนั้น ๆ ก่อนที่จะให้ความยินยอม

การที่เจ้าของข้อมูลจะต้องแสดงความยินยอมอย่างไม่เครือบคุม หรือกำกวม (Unambiguous) หรือ เป็นการแสดงออกโดยชัดเจน ต้องปราศจากความลังเลสงสัยในการตีความว่าเป็นการกระทำของเจ้าของข้อมูลหรือไม่ เช่น การกดอัพโหลดภาพบัตรประจำตัวประชาชน การลงลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น

การจำแนก ในกรณีที่คำร้องขอความยินยอมเป็นส่วนหนึ่งของแบบฟอร์มที่เป็นลายลักษณ์อักษรจะต้องแยกความแตกต่างอย่างชัดเจนจากเรื่องอื่น ๆ

การถอน เจ้าของข้อมูลสามารถถอนความยินยอมได้ตลอดเวลาและง่ายในการถอนความยินยอมต้องแจ้งให้ทราบถึงสิทธินั้นก่อนที่จะให้ความยินยอม

---

[159] Regulation (EU) 2018/1725 Article 3 Definitions Reads:

(15) “consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”

ประเด็นที่สาม มาตรการในการบังคับใช้กฎหมายโดยเฉพาะอย่างยิ่งระยะเวลาในการเก็บรักษาข้อมูลไบโอเมตริกซ์ (Biometrics) ซึ่งจะเป็นไปตามหลัก (Right to be forgotten) การประเมินผลกระทบความเป็นส่วนตัวสำหรับการประมวลผลข้อมูลไบโอเมตริกซ์หลายรูปแบบ เหตุผลสำคัญ คือ เนื่องจากการประมวลผลข้อมูลไบโอเมตริกซ์หลายรูปแบบจำเป็นต้องเกี่ยวข้องกับการใช้เทคโนโลยีใหม่ ๆ

ปัจจัยที่ (GDPR) กำหนดเงื่อนไขที่ให้ความสำคัญของการดำเนินการประเมินผลกระทบความเป็นส่วนตัว ผู้ให้บริการจะต้องป้องกันมากกว่าแก้ไข กล่าวคือ คาดคะเนถึงเหตุการณ์ที่ไม่พึงประสงค์และสุ่มเสี่ยงต่อความเป็นส่วนตัวของผู้ใช้บริการ และดำเนินมาตรการการป้องกันไว้ก่อนที่จะเกิดขึ้นจริง เริ่มต้นจากการตระหนักถึงคุณประโยชน์ของการปฏิบัติตามนโยบายความเป็นส่วนตัวที่เข้มข้น โดยผู้ควบคุมจะอยู่ภายใต้ข้อผูกพันในแจ้งข้อมูล “ภายในระยะเวลาที่เหมาะสมหลังจากได้รับข้อมูลส่วนบุคคล แต่ไม่เกินภายใน 1 เดือน โดยคำนึงถึงสถานการณ์เฉพาะที่ข้อมูลส่วนบุคคลถูกประมวลผล” ไม่ว่าในกรณีใด ๆ หากข้อมูลส่วนบุคคลจะถูกใช้เพื่อจุดประสงค์ในการสื่อสารกับข้อมูลส่วนบุคคล หรือ หากมีการเปิดเผยข้อมูลดังกล่าวไปยังบุคคลที่สามข้อมูลนั้น ผู้ควบคุมจะต้องแจ้งการให้ข้อมูลกับเรื่องข้อมูลก่อนการติดต่อครั้งแรกกับบุคคลนั้น หรือบุคคลนั้นให้ไว้ก่อนที่จะมีการเปิดเผย ข้อมูลส่วนบุคคล แต่ไม่เกิน “ภายใน 1 เดือน” โดยคำนึงถึงสถานการณ์เฉพาะที่ข้อมูลส่วนบุคคลถูกประมวลผล ตามมาตรา 14 ข้อ 3 (a)[160]

ผู้ให้บริการจะต้องประกาศแจ้งไว้ก่อนให้ความยินยอมสำหรับการบันทึก แต่อาจถูกเก็บไว้ในโหมดเก็บถาวรหากกฎหมายกำหนดไว้ ซึ่งเป็นปัจจัยที่จะมีผลต่อการอนุญาตให้ใช้ “ข้อมูลพันธุกรรม และ ข้อมูลไบโอเมตริกซ์” ที่จะยืนยันว่าการเก็บข้อมูลดัง เป็นปัญหาภายในขอบเขตของสิทธิในความเป็นส่วนตัว การเก็บรักษา ใช้ เปิดเผย ลบ ซึ่งสามารถทำให้เกิดการรบกวนกับสิทธิความเป็นส่วนตัว รวมทั้ง สิทธิที่จะถูกลืม (Right to be forgotten) เพื่อให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลถูกลบเลือน หรือ ลืมไปเสียจากระบบโลกออนไลน์ โดยการแจ้งเป็นลายลักษณ์จึงเป็นแนวคิดที่สอดคล้องกับข้อเท็จจริงในการพัฒนาทางเทคโนโลยีในปัจจุบัน เนื่องจากสถานการทางสังคมได้เปลี่ยนแปลงไปสู่ยุคสังคมข้อมลข่าวสาร (Information society) ซึ่งข้อมูลจำนวนมหาศาลที่อยู่ในระบบออนไลน์ (Big data) มีแนวโน้มที่จะถูกรวบรวม (Collected) จัดเก็บ (Stored)

---

[160] Regulation (EU) 2016/679 Article 14 Information to be provided where personal data have not been obtained from the data subject raeds:

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

และประมวลผล (Processed) อย่างต่อเนื่อง และประมวลผลอัตโนมัติบนเครือข่ายอินเตอร์เน็ตที่สามารถสืบค้นได้ง่าย (Searchable)

ด้วยเหตุดังกล่าวนี้ ที่ความมีอยู่ของข้อมูลส่วนบุคคลดังกล่าว อาจก่อทั้งผลดีและผลเสียแก่เจ้าของข้อมูล โดยแนวโน้มข้อกังวลเกี่ยวกับการประมวลผลข้อมูลไบโอเมตริกซ์ในระบบออนไลน์จะกระทำอย่างไรให้ข้อมูลส่วนบุคคลถูกจดในระบบออนไลน์น้อยที่สุด และ สิ่งใดบ้างที่ควรจะถูกลบเลือนไป (How to remember less and what should be forgotten) เพื่อจุดประสงค์ในการโต้แย้งตามกฎหมายที่มีผลบังคับใช้ การใช้มาตรการสูงสุดในการคุ้มครองความเป็นส่วนตัวในการเก็บรักษาข้อมูลส่วนบุคคลได้ แต่ไม่เกินความจำเป็นตามกฎข้อบังคับ (Regulation (EU) 2016/679) และ (Regulation (EU) 2018/1725) ตามมาตรา 5 (1) (e)

สิทธิที่จะถูกลืม (Right to be forgotten) ภายใต้ (General Data Protection Regulation: GDPR) ภายใต้กฎหมายฉบับใหม่ของสหภาพยุโรป กล่าวคือ (GDPR) ที่จะมีผลใช้บังคับแทน (Directive 95/46/EC) ตั้งแต่วันที่ 25 พฤษภาคม คริสต์ศักราช 2018 นั้น (Right to be forgotten) ได้ถูกพัฒนาและยกระดับขึ้นเป็นสิทธิใหม่ที่ได้รับการรับรองโดยชัดแจ้งใน Article 17[161] (Right to erasure)

---

[161] General Data Protection Regulation (EU) 2016/679 Article 17 reads: Right to erasure (‘right to be forgotten’)

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6 (1), or point (a) of Article 9 (2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21 (1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21 (2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8 (1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

“(right to be forgotten)” โดยอาจพิจารณาสาระสำคัญโดยเปรียบเทียบในเชิงพัฒนาการกับสิทธิเดิมที่เคยได้รับการรับรองโดยคำวินิจฉัยของ (CJEU) ได้ดังต่อไปนี้

เนื้อหาแห่งสิทธิ ผู้มีหน้าที่ และข้อยกเว้น ภายใต้ Article 17 ของ (GDPR) สิทธิดังกล่าวได้ก้าวไปไกลกว่า (Right to de-listing) หรือการลบ (link) แสดงผลการค้นหาจากผู้ให้บริการ (Search engine) เนื่องจากมีการเน้นย้ำในเนื้อหาแห่งสิทธิใหม่ว่าเป็น (Right to erasure) หรือการลบซึ่งข้อมูลส่วนบุคคลที่เกี่ยวกับเจ้าของข้อมูลอย่างแท้จริง โดยไม่ชักช้า และสามารถใช้ยันได้ต่อผู้ประมวลผลข้อมูลทั้งหมด ทั้งเจ้าของ Webpage ว่าเป็นผู้ดำเนินการตัดสินใจว่าจะประมวลผลข้อมูลส่วนบุคคลหรือไม่ หรือผู้ให้บริการ (Search engine) จากแนวทางการตีความในคดี (Google Spain) ทั้งนี้ การคงถ้อยคำในวงเล็บว่า (Right to be forgotten) หลัง (Right to erasure) นั้น มีเจตนารมณ์เพื่อเน้นย้ำถึงความสำคัญในการพัฒนา (Right to erasure) เดิมตาม Directive 95/46/EC เข้าสู่การลบเลือนข้อมูลส่วนบุคคลในบริบททางดิจิทัล คดีตัวอย่างเช่น

คดี Google Spain[162]

ในปี 1998 ชายชาวสเปนคนหนึ่ง ชื่อ Mario Costeja González ซึ่งเป็นโจทก์ถูกบังคับให้ชำระหนี้ด้วยการนำเอาอสังหาริมทรัพย์ออกมาขายเพื่อชำระหนี้ การขายถูกบันทึกในไม่กี่บรรทัดในหนังสือพิมพ์ท้องถิ่นระบุถึงการนำบ้านและทรัพย์สินออกประมูลเพื่อแก้ไขปัญหาทางการเงิน และตามปกติประวัติจะต้องถูกลืมในไม่ช้า อย่างไรก็ตาม หนังสือพิมพ์ได้ทำการจัดเก็บระบบข้อมูลออนไลน์และหลังจากนั้นในทุกการค้นหาเมื่อใส่คำค้นหาเป็นชื่อขอโจทก์ลงใน Google Search

---

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9 (3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

[162] Homo Digitalis. (2018). ***The case Google Spain v AEPD and Mario Costeja Gonzalez of the Court of Justice of the European Union: A brief critical analysis***. (Online).Available: https://www.homodigitalis.gr/en/posts/2900. [2019, 21 December]

กลับปรากฏว่าลิงค์ที่เชื่อมโยงไปยังข้อมูลในหนังสือพิมพ์ฉบับหนึ่งถูกบันทึกเป็นเวลา 16 ปี และ Mario Costeja González ได้เป็นโจทก์ฟ้อง Google ต่อศาลยุติธรรมของสหภาพยุโรป โดยมีคำสั่งให้ Google ลบข้อมูลส่วนตัวของโจทก์ออกจากระบบการค้นหา โดยเมื่อปี 2010 โจทก์เรียกร้องให้ Google ลบลิงค์และข้อมูลของโจทก์ออกจากฐานข้อมูล ซึ่งภายหลังจากการตัดสิน ศาลได้ชี้แจงว่าผู้บริโภคสมควรได้รับสิทธิ์ที่เรียกว่า “สิทธิที่จะถูกลืม” กล่าวคือ จำเลยสามารถลบร่องรอย ดิจิทัล (Digital footprints) หรือ ลิงค์ข้อมูลของจำเลยออกจากอินเทอร์เน็ตได้ โดยทางด้านโฆษกของ Google ได้ออกมาแสดงความผิดหวังต่อการตัดสินใจของศาล และทำให้ Google จำเป็นต้องมาวิเคราะห์สถานการณ์เพื่อหาผลกระทบต่อไป[163]

จากข้อเท็จจริง (Google) โต้แย้งว่า (Google Spain) นั้น เป็นแต่เพียง สาขาหนึ่ง ของ (Google Inc) ในสหภาพยุโรปเพื่อทำหน้าที่เป็นตัวแทนทางธุรกิจสำหรับการโฆษณา แต่มิได้เป็นผู้ดำเนินการทางเทคนิคในส่วนของการสืบค้นข้อมูล หรือ อีกนัยหนึ่ง คือ ไม่ได้เป็นที่ตั้งของระบบ (Server) ทาง (Website) ของ (Google) ที่ในทางปฏิบัติที่จะดำเนินการโดย (Google Inc) ในประเทศสหรัฐอเมริกา ดังนั้น การประมวลผลข้อมูลจึงมิได้ดำเนินการในสหภาพยุโรป และไม่ตกอยู่ภายใต้บังคับของ Directive 95/46/EC เป็นเหตุให้ (CJEU) ต้องใช้หลักการตีความอย่างกว้างเพื่อประโยชน์ในการปรับใช้ Directive 95/46/EC โดยอาศัยหลักการตีความที่เรียกว่าเป็นการกระทำในเชิงบริบทของสาขา หรือ ตัวแทนที่ตั้งอยู่ในสหภาพยุโรป (Context of the activities of establishment) ของ (Google Inc) กล่าวคือ แม้ว่า (Google Spain) ในฐานะตัวแทนทางธุรกิจจะมิใช่ผู้ประมวลผลข้อมูล แต่ (Google Inc) ซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคลตัวจริงนั้น ท้ายที่สุดแล้วย่อมได้รับประโยชน์ที่ไม่อาจแบ่งแยกได้ (Inextricably linked) อันเป็นผลมาจากการประมวลผลนั้นจาก (Google Spain) ดังนั้น การกระทำของ (Google Inc) จึงย่อมตกอยู่ภายใต้บังคับของ Directive 95/46/EC ด้วย[164]

จากคำวินิจฉัยในประเด็นนี้ จึงเป็นการวางแนวทางให้สามารถปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลตัวจริงซึ่งอาจเป็นบริษัทข้ามชาติที่มีเพียงแต่สำนักงาน หรือสาขาในพื้นที่เพื่อติดต่อทางธุรกิจให้ตกอยู่ใต้บังคับของกฎหมายเพื่อประโยชน์ในการคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลที่ถูกประมวลผล มิให้เกิดช่องโหว่ในการบังคับใช้สิทธิเพียงเพราะเหตุตำแหน่งที่ตั้งของระบบ (Server) ของบริษัทเหล่านั้น

---

[163] Artemi Rallo Epig.org (2018). ***The Right to Be Forgotten (Google v. Spain).*** (Online). Available: https://epic.org/privacy/right-to-be-forgotten/. [2562, 22 December]

[164] Stefan Kulk & Frederik Zuiderveen Borgesius. (2017). ***Privacy, freedom of expression, and the right to be forgotten in Europe. Forthcoming in: Cambridge Handbook of Consumer Privacy***, eds. Jules Polonetsky, Omer Tene, and Evan Selinger (Cambridge University Press). p. 22

ข้อยกเว้น เพื่อประโยชน์สาธารณะเพื่อวัตถุประสงค์ทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ของ (GDPR) เท่านั้น ในกรณีดังต่อไปนี้[165]

หลักการปกป้องข้อมูลหลักใน (GDPR) ได้รับการแก้ไข แต่มีความคล้ายคลึงกับหลักการที่กำหนดไว้ใน (DPD) การรวบรวมข้อมูลส่วนบุคคลต้องมีวัตถุประสงค์ที่ชัดแจ้งชอบด้วยกฎหมายและความโปร่งใส Article 5 (1) (a) ถูกประมวลโดยชอบด้วยกฎหมาย เป็นธรรมและเป็นไปในลักษณะที่โปร่งใสต่อเจ้าของข้อมูล

ข้อจำกัดตามวัตถุประสงค์ตาม Article5 (1) (b) ถูกรวบรวมเพื่อวัตถุประสงค์เฉพาะ ชัดเจนและถูกต้องตามกฎหมายและมิได้ ประมวลต่อไปในลักษณะที่ขัดแย้งกับวัตถุประสงค์ดังกล่าว การประมวลเพิ่มเติมโดยวัตถุประสงค์การ จัดเก็บเพื่อประโยชน์สาธารณะ การวิจัยทางวิทยาศาสตร์ หรือประวัติศาสตร์ หรือเพื่อวัตถุประสงค์ ทางสถิติจะ ตามข้อ 89 (1) ไม่ถือว่าเป็นการขัดกับวัตถุประสงค์หลัก

การลดขนาดของข้อมูลตาม Article 5 (1) (c) เพื่อความเหมาะสมและเกี่ยวข้องเพียงเท่าที่จำเป็นตามวัตถุประสงค์ในการประมวลผลข้อมูลนั้นคือ “การลดจำนวนข้อมูล”

ความถูกต้อง Article 5 (1) (d) ในกรณีที่จำเป็นทำให้มีความทันสมัย มีขั้นตอนการจัดการที่เหมาะสมเพื่อทำให้แน่ใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องตามวัตถุประสงค์การประมวลข้อมูลได้มีการลบ หรือแก้ไขให้ถูกต้องโดยไม่ล่าช้า

ข้อจำกัดในการจัดเก็บตาม Article 5 (1) (e) ถูกจัดเก็บอยู่ในรูปแบบที่อนุญาตให้มีการระบุตัวเจ้าของข้อมูลภายในระยะเวลาไม่ เกินกว่าเท่าที่จำเป็นเพื่อวัตถุประสงค์ที่ข้อมูลส่วนบุคคลนั้นได้ถูกประมวลข้อมูลส่วนบุคคลอาจถูกจัดเก็บในระยะเวลาที่นานขึ้น ในกรณีที่การประมวลข้อมูลส่วนบุคคลนั้นเพื่อวัตถุประสงค์การจัดเก็บเพื่อประโยชน์สาธารณะ การวิจัยทางวิทยาศาสตร์ หรือประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติเพียงเท่านั้น ตามข้อ 89 (1) ซึ่งตกอยู่ภายใต้บังคับการดำเนินมาตรการทางเทคนิคและมาตรการที่ เกี่ยวข้องกับองค์กรที่เหมาะสมที่กำหนดโดยข้อบังคับนี้เพื่อการปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูล

ความสมบูรณ์และความลับตาม Article 5 (1) (f) ถูกประมวลในลักษณะที่ทำให้แน่ใจในความปลอดภัยที่เหมาะสมของข้อมูลส่วนบุคคล รวมทั้งการป้องกันการประมวลที่ไม่ได้รับอำนาจหรือไม่ชอบด้วยกฎหมาย และต่อการสูญหายโดยบังเอิญ การทำลาย หรือความเสียหาย ซึ่งใช้มาตรการทางเทคนิค หรือมาตรการที่เกี่ยวข้องกับองค์กรที่เหมาะสม

---

[165] Nils Gruschka†, Vasileios Mavroeidis†, Kamer Vishi†, Meiko Jensen. (2018). Research Group of Information and Cyber Security ***Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR***. Faculty of Computer Science and Electrical Engineering, Kiel University of Applied Science, German.

ความรับผิดชอบตาม Article 5 (2) ให้ผู้ควบคุมข้อมูลรับผิดชอบและสามารถที่จะแสดงให้เห็นการปฏิบัติตามวรรคหนึ่ง[166]

ประเด็นที่สี่ แนวทางในการแก้ไขปัญหาข้อมูลไบโอเมตริกซ์ (Biometrics) เพื่อให้เป็นไปตามบทบัญญัติ ในการลงโทษและความมั่นคงปลอดภัยของข้อมูลไบโอเมตริกซ์ (Biometrics) กฎเกณฑ์การควบคุมความปลอดภัยของข้อมูลและความเป็นส่วนตัวในสหภาพยุโรป ตาม (GDPR) บัญญัติไว้ในมาตรา 32 ว่า "ผู้ควบคุมและผู้ประมวลผลจะใช้มาตรการทางเทคนิคและองค์กรที่เหมาะสมเพื่อให้แน่ใจว่าระดับความปลอดภัยที่เหมาะสมกับความเสี่ยง" เป็นสิ่งที่สำคัญที่สุดเสมอ แต่การจัดเก็บข้อมูลที่มีความอ่อนไหวสูง จะเป็นเพิ่มภาระหน้าที่พิเศษให้องค์กร โดยจะต้องปฏิบัติ

---

[166] Regulation (EU) 2016/679 Chapter II Principles Article 5 Principles relating to processing of personal data reads:

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

ตามกฎระเบียบ (Regulation (EU) 2018/1725) หลักความรับผิดชอบ (GDPR) ให้ความสำคัญที่ “ตัวควบคุมในทางปฏิบัติ” ซึ่งเป็นเจ้าของธุรกิจ เนื่องจากเจ้าของธุรกิจมักจะเป็น “ไดรเวอร์หลัก (Main driver)” ในขณะที่ผู้บริหารระดับสูงมีหน้าที่รับผิดชอบในการสร้างบันทึกกิจกรรมการประมวลผล และการดำเนินการ กฎระเบียบข้อบังคับ(Regulation (EU) 2016/679)

มาตรการของการละเมิดข้อมูลส่วนบุคคลผู้ควบคุมจะต้องแจ้งเตือนล่าช้าได้ไม่เกิน 72 ชั่วโมง หลังจากทราบว่ามีการการละเมิดข้อมูลส่วนบุคคลต่อเจ้าหน้าที่กำกับดูแล เว้นแต่ การละเมิดนั้นไม่น่าจะส่งผลให้ทำเกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลนั้น ในกรณีที่การแจ้งเตือนไปยังผู้ดูแลการป้องกันข้อมูลในสหภาพยุโรปไม่ได้ภายใน 72 ชั่วโมงจะต้องมีเหตุผลสำหรับความล่าช้านั้น ตามมาตรา 33 หากฝ่าฝืนมีบทลงโทษสำหรับองค์กรที่ฝ่าฝืนข้อกำหนด (GPPR) สูง โดยกำหนดปรับสูงถึง 20 ล้านยูโร หรือร้อยละ 4 ของรายได้ทั้งหมดทั่วโลก มาตรการดังกล่าวนี้ ทำให้มีมาตรฐานที่สูงมากสำหรับการปกป้องข้อมูล สิ่งนี้ทำให้สามมารถดำเนินการเชิงรุกและดำเนินการ เพื่อนำมาตรการที่จำเป็นมาใช้เพื่อให้แน่ใจว่าสภาพแวดล้อมโดยรวมมีความปลอดภัยสำหรับการประมวลผลข้อมูลส่วนบุคคล[167]

ดังนั้น สหภาพยุโรปได้ให้การคุ้มครองข้อมูลส่วนบุคคลรวมถึงข้อมูลไบโอเมตริกซ์ (Biometric Data) ไว้อย่างชัดเจนภายใต้คำสั่งเรื่องความเป็นส่วนตัว โดยกฎหมายได้อธิบายการใช้เทคโนโลยี(Biometric) เพื่อได้ข้อมูลทั้งในเชิงกายภาพ พฤติกรรม รวมถึงคุณลักษณะต่าง ๆ ที่สามารถจำแนกลักษณะเฉพาะของแต่ละบุคคลได้ ดังจะเห็นได้ว่า ข้อมูลส่วนบุคคลแบบข้อมูลไบโอเมตรอกซ์ (Biometric Data) จึงได้รับความคุ้มครองภายใต้กฎหมายข้อมูลส่วนบุคคลของประเทศกลุ่มสหภาพยุโรป ในการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษ ไว้ในมาตรา 10 (Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018) รวมถึงให้การคุ้มครองข้อมูลที่มีความอ่อนไหว(Sensitive Data) ซึ่งสหภาพยุโรปได้บัญญัติข้อมูลที่มีความอ่อนไหวไว้ในข้อบังคับที่ (29) เช่น เชื้อชาติศาสนา เพศวิถี เนื่องด้วยบริบททางประวัติศาสตร์ของทวีปยุโรปเอง ที่เคยมีการนำข้อมูลเหล่านี้ไปใช้ในทางรุนแรงมากมาย โดยมีความสำคัญดังนี้ คือ

การกำหนดข้อมูลไบโอเมตริกซ์ไว้เฉพาะดังนี้ “ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิคเฉพาะที่เกี่ยวข้องกับลักษณะทางกายภาพสรีรวิทยา หรือพฤติกรรมของบุคคล

---

[167] Regulation (EU) 2018/1725 Article 83 reads:

General conditions for imposing administrative fines reads: 6 “Non-compliance with an order by the supervisory authority as referred to in Article 58 (2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.”

ธรรมดาซึ่งอนุญาต หรือยืนยันอัตลักษณ์เฉพาะของบุคคลธรรมดา เช่น ใบหน้า ภาพ หรือข้อมูล (Dactyloscopic) ตามคำนิยามมาตรา 3 (18) คำจำกัดความนี้ ค่อนข้างกว้าง ซึ่งข้อมูลไบโอเมตริกซ์ประกอบด้วยลักษณะทางกายภาพและพฤติกรรมของบุคคล ดังนั้น การระบุตัวตนของบุคคลอาจรวมถึงลายนิ้วมือ สแกนม่านตา การจดจำใบหน้าผ่านระบบการสแกน แต่ยังรมถึงลักษณะบุคลิกภาพของบุคคลทางกายภาพ เช่น ปฏิกิริยาและนิสัยที่อาจนำไปสู่การระบุเอกลักษณ์ของเรื่องข้อมูลได้ เช่น การตรวจสอบลายเซ็นที่เขียนด้วยมือ การวิเคราะห์การกดแป้น เป็นต้น

การระบุว่าข้อมูลไบโอเมตริกซ์เป็นหมวดหมู่ใหม่ของ “ข้อมูลพิเศษ” ไว้อย่างชัดเจน ซึ่งข้อมูลไบโอเมตริกซ์นั้นจะเกิดจากข้อมูลที่แท้จริงเพื่อจุดประสงค์ในการใช้ระบุตัวตนและการเปิดเผยข้อมูลไบโอเมตริกซ์โดยไม่ได้รับอนุญาต หรือโดยไม่ได้ตั้งใจ ความไวข้อมูลอาจก่อให้เกิดความเสี่ยงร้ายแรงต่อการที่จะขโมยข้อมูลประจำตัว

ข้อมูลไบโอเมตริกซ์มีความอ่อนไหวเป็นพิเศษ มีข้อยกเว้น เพื่อเปลี่ยนคุณสมบัติข้อมูลไบโอเมตริกซ์ ใช้ในทางเทคโนโลยีการแพทย์ทำให้สามารถใช้ข้อมูลไบโอเมตริกซ์เพื่อสรุปเกี่ยวกับสุขภาพของแต่ละบุคคลได้ จึงทำให้ข้อมูลดังกล่าวมีคุณสมบัติเป็นข้อมูลทางการแพทย์ ซึ่งถูกควบคุมภายใต้ (GDPR) เป็นข้อมูลที่ละเอียดอ่อน

ข้อมูลเกี่ยวกับลักษณะทางสรีรวิทยา หรือพฤติกรรมของบุคคลจึงมีคุณสมบัติเป็นข้อมูลไบโอเมตริกซ์ภายใต้ (GDPR) เมื่อข้อมูลนี้ถูกประมวลผลผ่านวิธีการทางเทคนิคเฉพาะที่อนุญาตให้มีการระบุ หรือการตรวจสอบอักลักษณ์ของบุคคลนั้น ก็หมายความว่ารูปภาพของใบหน้าของใครบางคนนั้นถือว่าเป็น “ไบโอเมตริกซ์”ในแง่ของกฎหมายความเป็นส่วนตัว เมื่อมีการใช้รูปภาพ เพื่อระบุตัวตน หรือยืนยันตัวตนของบุคคล ด้วยเทคโนโลยีที่ใช้เพื่อจุดประสงค์นี้มักจะประเมินความหลากหลายของปัจจัย เช่น ระยะห่างระหว่างตากับจมูกจมูกและปาก เป็นต้น เพื่อในการระบุตัวบุคคล ดังนั้น ภาพถ่ายสามัญของบุคคลจึงไม่อาจถือได้ว่าเป็นข้อมูลไบโอเมตริกซ์ในแง่ของการประมวลผลมาตรา 29 (WP29)[168] ของข้อมูลไบโอเมตริกซ์ มีความเห็นว่าระบบไบโอเมตริกซ์ที่เข้าเกี่ยวข้องกับลักษณะทางกายภาพจะไม่ควรทิ้งร่องรอย เช่น รูปร่างของมือ แต่ไม่ใช่ลายนิ้วมือ ที่เจ้าของข้อมูลไม่พึ่งประสงค์ให้จดจำข้อมูลเพื่อลดสร้างความเสี่ยงให้น้อยลง

นอกจากนี้ ข้อมูลหลายประเภทไม่ได้อยู่ในหมวดหมู่ของข้อมูลพิเศษตามกฎหมาย แต่ยังมีความอ่อนไหวอย่างปฏิเสธไม่ได้ เนื่องจากอาจมีผลกระทบต่อบุคคล หากข้อมูลสูญหายหรือถูกขโมยซึ่งรวมถึงรหัสผ่านสำหรับการเข้าถึงระบบ (IT) และเว็บไซต์ หรือ เครือข่ายการสื่อสารทางอิเล็กทรอนิกส์ตามมาตรา 3 (25) ที่ถูกบัญญัติเพิ่มเติม เพื่อคุ้มครองในด้านรายละเอียด

---

[168] WP29. (2003). ***Working Document on biometrics***. (Online). Available:http://www.greeklawdigest.gr/topics/data-protection/item/304-health-biometric-and-genetic-data-under-gdpr. [2562, 29 July].

ของบัตรเครดิตหมายเลขประกันสังคม หมายเลขหนังสือเดินทางและอื่น ๆ ซึ่งความไวของข้อมูลมักเหล่านี้ขึ้นอยู่กับชุดค่าผสมดังกล่าวด้วย เนื่องจากสามารถใช้ข้อมูลเพื่อสร้างอีเมลฟิชชิ่ง (Phishing emails) ที่น่าเชื่อถือได้ แต่ที่อยู่อีเมลไม่ได้อยู่ในข้อมูลที่มีความอ่อนไหว แต่ถ้ารวมกับรหัสผ่านก็จะกลายเป็นเรื่องละเอียดอ่อนมาก เนื่องจากหลาย ๆ คนจะใช้ชุดอีเมล หรือรหัสผ่านเดียวกันเพื่อเข้าถึงเว็บไซต์และระบบต่าง ๆ จากนั้นมีสถานการณ์ที่ข้อมูลปกติจะกลายเป็นข้อมูลอ่อนไหว เมื่อเชื่อมโยงกับข้อมูลที่อาจมีความอ่อนไหวทางอ้อม แต่ในทางกลับกันมีหลายตัวอย่างที่ข้อมูลหมวดหมู่พิเศษไม่อ่อนไหว เมื่อใช้เพื่อจุดประสงค์ในการรวบรวม ซึ่งหมายความว่า ไม่จำเป็นจะต้องมีระบอบการป้องกันที่เข้มงวดเสมอไป เช่น บันทึกเงินบำนาญ รวมถึงชื่อและเพศของหุ้นส่วนของพนักงาน ดังนั้น จึงเป็นการเปิดเผยข้อมูลพื้นฐานเพศของบุคคลนั้น สำหรับความต้องการควบคุมข้อมูลของระบบการป้องกันพิเศษ ด้วยข้อกำหนดด้านความปลอดภัยที่เข้มงวดสำหรับข้อมูลเหล่านี้อาจยังไม่ชัดเจนในตัวเองเสมอไป

ประเด็นสำคัญ คือ ความยินยอม สิทธิที่จะถูกลืม หรือ (Right to be forgotten) นั้น จากสิทธิอย่างแคบเฉพาะการลบ (link) แสดงผลการค้นหาของผู้ให้บริการ (Search engine) ที่ได้รับการรับรองผ่านคำวินิจฉัยของ (CJEU) เข้าสู่มิติใหม่ของสิทธิที่ได้รับการรับรองชัดแจ้งโดยกฎหมายที่จะเรียกร้องให้ผู้ประมวลผลข้อมูลลบข้อมูลส่วนบุคคลออกจากโลกดิจิทัลอย่างถาวรและเป็นรูปธรรม ข้อจำกัดและสภาพปัญหาในการตีความและบังคับใช้ Directive 95/46/EC ซึ่งขาดความเหมาะสมกับสภาวการณ์ทางสังคมและเทคโนโลยีที่เปลี่ยนแปลงไปอย่างมากมายในช่วง 20 ปีที่ผ่านมานั้น ดูเหมือนจะได้รับการพิจารณาปรับปรุงในหลายประเด็น[169] และมาตรการความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในการลงโทษของ (GDPR)

โดยกำหนดเฉพาะโทษทางปกครองและโทษปรับเท่านั้น เพื่อลงโทษสถาบัน หรือ องค์กรของสหภาพ ที่ไม่ใช่บุคคล ตาม Regulation (EU) 2018/1725 ข้อบังคับ 81 สำหรับการตั้งค่าปรับที่เกี่ยวข้องกับผู้ควบคุมดูแลการป้องกันข้อมูลของยุโรปค่าปรับแล้วแต่กรณี โดยคำนึงถึงประโยชน์สาธารณะทั่วไปของสหภาพยุโรป หรือของประเทศสมาชิกโดยเฉพาะอย่างยิ่งผลประโยชน์ทางเศรษฐกิจสำหรับการละเมิดกฎข้อบังคับนี้ บทบัญญัติดังกล่าวได้กำหนดข้อเฉพาะในการคุ้มครองบุคคลธรรมดาที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลที่มีโทษทางอาญานั้น อาจอนุญาตให้ตัดผลกำไรที่ได้จากการฝ่าฝืนกฎระเบียบตามพระราชบัญญัตินี้ ซึ่งมุ่งเน้นความรับผิดที่ผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้ตระหนักถึงมาตรการความมั่นคงปลอดภัยของผู้ให้บริการ

---

[169] อรรถกร สุขปุณพันธ์. (2560). “สิทธิที่จะถูกลืม (Right to be forgotten): จากคำวินิจฉัยสู่มิติใหม่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป”. ***ดุลพาห*** , 3(64). หน้า 18.

ในวันที่ 25 พฤษภาคม คริสต์ศักราช 2018 ประชาชนในสหภาพยุโรปจะได้รับสิทธิที่พัฒนาขึ้นมาใหม่ให้เกิดความชัดเจนขึ้นทั้งในส่วนของเนื้อหาแห่งสิทธิ ผู้มีหน้าที่ ข้อยกเว้นแห่งสิทธิ สภาพบังคับที่เหมาะสมกับการประมวลผลข้อมูลในโลกออนไลน์ ตลอดจนมาตรการบังคับทางกฎหมายที่สอดคล้องและมีประสิทธิภาพมากยิ่งขึ้น ซึ่งเวลาจะเป็นผู้ให้คำตอบถึงผลลัพธ์ในทางปฏิบัติของบทบัญญัติตามกฎหมายใหม่ของสหภาพยุโรปฉบับนี้ว่าจะมีประสิทธิภาพในการบังคับใช้จริงมากน้อยเพียงไร ทั้งนี้ ประสบการณ์และสภาพปัญหาของสหภาพยุโรปในการบังคับใช้ Directive 95/46/EC ผ่านคำวินิจฉัยในคดี (Google Spain) และการบังคับใช้สิทธิดังกล่าวที่ได้รับรองโดย (GDPR) ในอนาคตอันใกล้นี้ จะเป็นตัวอย่างที่สมควรให้ความสนใจสำหรับประเทศที่อยู่ระหว่างการพิจารณากำหนดให้มีหรือแก้ไขกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลว่าจะให้การรับรอง (Right to be forgotten) หรือไม่ ในขอบเขตแค่ไหนเพียงไร ตลอดจนมาตรการทางกฎหมายใดบ้างที่สำคัญและจำเป็นสมควรกำหนดเพื่อบังคับใช้สิทธิดังกล่าวให้เกิดประสิทธิภาพและสอดคล้องกับมาตรฐานสากลสำหรับโลกดิจิทัล ในการป้องกันการประมวลผลเกี่ยวข้องกับข้อมูลที่มีความละเอียดอ่อนประเภทพิเศษ หรือไม่นั้น เนื่องจากเป็นข้อมูลประเภทพิเศษภายใต้มาตรา 10 ของคำสั่ง หรือด้วยเหตุผลอื่นใด เช่น ในกรณีของข้อมูลไบโอเมตริกซ์ ข้อมูลพันธุกรรม ข้อมูลการสื่อสาร ข้อมูลสถานที่และข้อมูลส่วนบุคคลประเภทอื่น ๆ ที่ยังคงต้องการ “การป้องกันเป็นพิเศษ” นอกจากนี้ หลักความยินยอมข้อมูลหมวดหมู่พิเศษ

3.3 มาตรการทางกฎหมายสหรัฐอเมริกา Privacy Act 1974

เนื่องจากรัฐธรรมนูญของประเทศสหรัฐอเมริกา ได้มีบทบัญญัติคุ้มครองความเป็นส่วนตัวของประชาชน โดยเฉพาะอย่างยิ่งการแก้ไขครั้งที่สี่ (Fourth Amendment) ได้รับรองว่าบุคคลมีสิทธิที่จะได้รับความปลอดภัยในร่างกาย เคหสถาน เอกสาร และทรัพย์สิน จากการค้น ยึด และจับกุมโดยปราศจากเหตุอันสมควร ซึ่งเคหสถานและทรัพย์สินของบุคคลที่ได้รับความคุ้มครองนั้น ได้รวมไปถึงการสนทนาทางโทรศัพท์ด้วย ในขณะที่การเก็บรวบรวมข้อมูลใช้ และเปิดเผยส่วนบุคคลโดยองค์กรของรัฐกลับไม่มีข้อจำกัด โดยรัฐได้รวบรวมข้อมูลของประชาชนจำนวนมากทั้งข้อมูลทั่วไปและข้อมูลที่มีความอ่อนไหว เช่น ภาษีรายได้ ประกันสังคม หรือ ข้อมูลที่ได้จากการสำรวจเพื่อทำวิจัย เป็นต้น ซึ่งหากรัฐบาลมีข้อมูลเกี่ยวกับประชาชนมากเท่าไรก็ย่อมก่อให้เกิดผลเสียต่อประชาชนผู้เป็นเจ้าของข้อมูลส่วนบุคคลมากขึ้นเท่านั้น โดยเฉพาะอย่างยิ่งเทคโนโลยีทางคอมพิวเตอร์ที่ถูกนำมาใช้เพื่อการเก็บรวบรวมและเปิดเผยข้อมูลส่วนบุคคล ย่อมทำให้กระทำได้ง่ายมากขึ้น ดังนั้น (Privacy Act) จึงได้ถูกนำมาใช้บังคับเพื่อกำหนดกฎเกณฑ์ควบคุมการเก็บรวบรวม การ

เก็บรักษา การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐ ซึ่งในบางครั้งถูกเรียกว่า แนวปฏิบัติเกี่ยวกับสารสนเทศที่เป็นธรรม (Code of fair information practices)[170]

3.3.1 พระราชบัญญัติความเป็นส่วนตัว (Privacy Act 1974)

พระราชบัญญัติความเป็นส่วนตัว (Privacy Act 1974) กฎหมายฉบับนี้ ใช้บังคับเฉพาะข้อมูลของประชาชนที่ถูกจัดเก็บและรักษาในหน่วยงานภาครัฐ ซึ่งไม่รวมข้อมูลส่วนบุคคลที่อยู่ในภาคเอกชน โดยรายละเอียดสำคัญของกฎหมายฉบับนี้ (Privacy Act) บัญญัติให้สิทธิเฉพาะบุคคลผู้เป็นเจ้าของข้อมูล ได้ให้การคุ้มครองข้อมูลส่วนบุคคลแก่บุคคล ซึ่งมีสัญชาติอเมริกัน หรือบุคคลที่มีภูมิลำเนาถาวรถูกต้องตามกฎหมายในประเทศสหรัฐอเมริกาและข้อมูลส่วนบุคคลทีผู้เป็นเจ้าของข้อมูลจะใช้สิทธิเข้าถึงตาม(Privacy Act) นั้นจำกัดเฉพาะข้อมูลส่วนบุคคลทีถูกบันทึกไว้ใน “ระบบบันทึกข้อมูล” (System of Records) เท่านั้น บุคคลอื่นใดนอกจากนี้ ไม่สามารถอ้างความคุ้มครองตามพระราชบัญญัติฉบับนี้ได้ โดยเฉพาะ (Privacy Act) ได้กำหนดหลักเกณฑ์เกี่ยวกับการรักษา การเก็บรวบรวม การใช้ หรือ การเผยแพร่ข้อมูลส่วนบุคคล จึงถูกนำมาบังคับใช้แก่หน่วยงานของรัฐ ได้แก่ หน่วยงานด้านการบริหารหน่วยงานทางทหาร รัฐวิสาหกิจ บริษัทที่รัฐบาลมีอำนาจในควบคุม เช่น บริการไปรษณีย์ของสหรัฐอเมริกา (U.S. Postal Service)[171]

พระราชบัญญัติ (Privacy Act) ฉบับนี้ให้ความหมายของข้อมูลส่วนบุคคลไว้ใน 5 U.S.C.§ 552 a (a) (4) ว่า “บันทึก” หมายถึง สิ่งใด ๆ ชุด หรือกลุ่มของข้อมูลเกี่ยวกับบุคคลซึ่งการเก็บรวบรวม การเก็บรักษา ใช้ หรือเปิดเผยโดยหน่วยงานของรัฐ ซึ่งให้รวมไปถึงการศึกษา ธุรกรรมการเงิน ประวัติการรักษาพยาบาล ประวัติอาชญากรรม ประวัติการทำงาน ซึ่งมีชื่อของบุคคลนั้นหรือเลขบัตรประจำตัวประชาชน สัญลักษณ์ หรือบ่งชี้สิ่งอื่นใดที่สามารถระบุตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ หรือลายพิมพ์เสียง หรือรูปภาพ[172] และ 5 U.S.C.§ 552 a (a) (5) 2 “ระบบการ

---

[170] วรรณรัชชา ทรัพย์รดาพัดชา. (2558). ***ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศกับสหภาพยุโรป : ศึกษาผลกระทบของคดีค าพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดี C-362/14 ต่อโครงการเซฟฮาร์เบอร์ (Safe Harbour)***. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขากฎหมายมหาชน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. หน้า 19.

[171] สัญญา วิริยะอมรพันธุ์. (2554). ***มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล: ในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ***. สารนิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ. หน้า 54.

[172] 5 U.S.C. § 552 a (a) For purposes of this section reads:

(4) the term “record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history,

บันทึก” หมายถึง กลุ่มของการบันทึกซึ่งควบคุมโดยหน่วยงานของรัฐโดยข้อมูลนั้นเรียกคืนด้วยชื่อของบุคคลนั้น หรือด้วยเลขบัตรประชาชน สัญลักษณ์ หรือสิ่งอื่นที่สามารถระบุถึงตัวบุคคลนั้น[173]

การเก็บรวบรวมข้อมูลส่วนบุคคลภายใต้ (Privacy Act) หน่วยงานของรัฐจะต้องได้รับข้อมูลนั้นมาจากบุคคลผู้เกี่ยวข้องโดยตรง โดยต้องแจ้งกฎหมาย หรือคำสั่งที่ให้อำนาจแก่หน่วยงานรัฐในการเก็บรวบรวมข้อมูล แจ้งให้ทราบถึงลักษณะของข้อมูล ต้องระบุว่าข้อมูลนั้นจะถูกนำไปใช้เพื่อวัตถุประสงค์ใด[174] หน่วยงานของรัฐต้องเก็บข้อมูลเพียงเท่าที่จำเป็นและเกี่ยวข้องกับวัตถุประสงค์ และหากข้อมูลนั้นอาจก่อให้เกิดผลเสียแก่เจ้าของข้อมูลส่วนบุคคล เช่น กระทบต่อสิทธิ หรือประโยชน์ของเจ้าของข้อมูลส่วนบุคคล หน่วยงานของรัฐต้องพยายามเก็บรวบรวมข้อมูลนั้นจากเจ้าของข้อมูลโดยตรง

พระราชบัญญัติ (Privacy Act) กำหนดให้หน่วยงานของรัฐที่มีหน้าที่ดูแลระบบการบันทึกต้องยินยอมให้เจ้าของข้อมูลส่วนบุคคลเข้าถึงข้อมูลส่วนบุคคลของตน โดยเจ้าของข้อมูลส่วนบุคคลสามารถที่จะตรวจสอบความถูกต้องและขอสำเนาข้อมูลส่วนบุคคลของตนได้ หากพบว่าข้อมูลของตนไม่ถูกต้องสามารถที่จะขอแก้ไขข้อมูลนั้นได้ เมื่อมีคำขอแก้ไขข้อมูลส่วนบุคคลแล้วหน่วยงานของรัฐจะต้องพิจารณาและตอบรับคำขอของเจ้าของข้อมูลส่วนบุคคลภายใน 30 วันทำการ[175]

---

and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voiceprint or a photograph

[173] 5 U.S.C.§ 552 a (a) For purposes of this section reads:

(5) the term “system of records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

[174] 5 U.S.C.§ 552 a (a) For purposes of this section reads:

(e) Agency Requirements. Each agency that maintains a system of rec-ords shall

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

[175] 5 U.S.C.§ 552 a (a) For purposes of this section reads:

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the

หากหน่วยงานของรัฐปฏิเสธคำขอดังกล่าว หน่วยงานของรัฐต้องแจ้งเหตุผลในการปฏิเสธ และแจ้งหน่วยงานที่เจ้าของข้อมูลส่วนบุคคลสามารถอุทธรณ์คำสั่งได้

การเปิดเผยข้อมูลส่วนบุคคล (Privacy Act) ห้ามมิให้หน่วยงานของรัฐที่มีข้อมูลส่วนบุคคลเปิดเผยข้อมูลส่วนบุคคลนั้น เว้นแต่ จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นการเปิดเผยตามที่ พระราชบัญญัติ (Privacy Act) บัญญัติยกเว้นตาม 5 U.S.C § 552 a. (b) ไว้ซึ่งมีจำนวน 12 กรณี ดังนี้

กรณีความจำเป็นต้องรู้ภายในหน่วยงาน (Need to know within agency)

กรณีการเปิดเผยตามบทบัญญัติของ Freedom of Information Act (Required FOIL disclosure)

กรณีการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลนั้น (Routine uses)

กรณีการเปิดเผยต่อสำนักงานสำมะโนประชากร (Bureau of the Census)

กรณีการเปิดเผยเพื่อการวิจัยทางสถิติ (Statistical research)

กรณีการเปิดเผยต่อหอจดหมายเหตุแห่งชาติ (National Archives)

กรณีการเปิดเผยเพื่อการบังคับการให้เป็นไปตามกฎหมาย (Law enforcement request)

กรณีเป็นเรื่องอันตรายต่อสุขภาพ หรือความปลอดภัยของบุคคล (Health or safety of an individual)

กรณีการเปิดเผยต่อสภาคองเกรส (Congress)

กรณีการเปิดเผยต่ออธิบดีกรมบัญชีกลาง (General Accounting Office) หรือตัวแทนที่ได้รับอนุญาต

กรณีการเปิดเผยตามคำสั่งของศาล (Court order)

กรณีการเปิดเผยตามกฎหมาย Debt Collection Act

การเปิดเผยตาม (Freedom of Information Act) เป็นการเปิดเผยแก่บุคคล ซึ่งได้แจ้งแก่หน่วยงานของรัฐล่วงหน้าว่าบันทึกนั้น จะถูกใช้เพื่อการศึกษาทางสถิติ หรือรายงานและบันทึกนั้นจะถูกโอนถ่ายโดยปราศจากข้อมูลที่สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ เป็นการเปิดเผยแก่หน่วยงานของรัฐภายใต้อำนาจของรัฐบาลซึ่งอยู่ภายใต้การควบคุมของประเทศสหรัฐอเมริกา เพื่อการบังคับตามกฎหมายแพ่ง หรืออาญาและโดยมีคำขอเป็นหนังสือจากหัวหน้าของหน่วยงานนั้น หรือ

---

refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g) (1) (A) of this section;

เป็นการเปิดเผยภายใต้สถานการณ์จำเป็นที่กระทบต่อสุขภาพหรือความปลอดภัยของบุคคลใด และบุคคลซึ่งได้รับผลกระทบต่อสุขภาพหรือความปลอดภัย [176] เป็นต้น

เมื่อมีการเปิดเผยข้อมูลส่วนบุคคลแล้ว หน่วยงานของรัฐต้องทำรายงานข้อมูลเกี่ยวกับวันเวลา บุคคลที่ได้รับการเปิดเผยข้อมูล ข้อมูลเกี่ยวกับการติดต่อบุคคล หรือองค์กรที่ได้รับข้อมูลส่วนบุคคลนั้น โดยจะต้องเก็บรายงานดังกล่าวไว้เป็นเวลา 5 ปี หรือตลอดอายุของบันทึกระยะเวลาใดยาวกว่าให้ถือระยะเวลานั้น หากเจ้าของข้อมูลส่วนบุคคลร้องขอหน่วยงานของรัฐต้องเปิดเผยรายงานนี้แก่เจ้าของข้อมูลส่วนบุคคล เว้นแต่ เป็นการเปิดเผยเพื่อการบังคับตามกฎหมาย[177]เช่น

พระราชบัญญัติฉบับนี้ยังได้กำหนดข้อยกเว้นการเปิดเผยข้อมูลต่อบุคคลที่สามในกรณีดังนี้

ข้อยกเว้นกรณีพิเศษ (Special exemption) ตามมาตรา 5 U.S.C § 552 a. (d) (5) บทบัญญัติในกฎหมายที่จะอนุญาตให้บุคคลเข้าถึงข้อมูลใด ๆ ที่ถูกจัดเก็บรวบรวมไว้สำหรับการฟ้องร้อง หรือการดำเนินกระบวนพิจารณาคดีทางแพ่ง[178]

ข้อยกเว้นกรณีทั่วไป (General Exemption) ตามมาตรา 5 U.S.C § 552 a. (j) บัญญัติว่า “หัวหน้าของหน่วยราชการอาจจะประกาศกฎระเบียบ เพื่อยกเว้นการเข้าถึงบันทึกข้อมูลส่วนบุคคลได้ ถ้าระบบบันทึกข้อมูลนั้น”[179]

ข้อมูลถูกเก็บรักษาไว้โดยหน่วยสืบราชการลับของรัฐบาลกลาง (Central Intelligence Agency)

---

[176] หทัยชนก หร่ายวงศ์. (2559). ***ปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพ***. วิทยานิพนธ์นิติศาสตรมหาบัณฑิตสาขากฎหมายธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.หน้า 14-35.

[177] 5 U.S.C. § 552 a (c) Reads:

(2) “retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made”

[178] 5 U.S.C.§ 552 a (a) For purposes of this section reads:

(d) Access to Records. Each agency that maintains a system of rec-ords shall

(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

[179] 5 U.S. Code § 552 a. Records maintained on individuals reads:

(j) General Exemptions.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553 (b) (1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c) (1) and (2), (e) (4) (A) through (F), (e) (6), (7), (9), (10), and (11), and (i) if the system of rec-ords is

ข้อมูลถูกเก็บรักษาไว้โดยหน่วยงานซึ่งมีหน้าที่ปฏิบัติการให้เป็นไปตามกฎหมายอาญา ซึ่งรวมถึงงานรับผิดชอบของเจ้าหน้าทีตำรวจในการป้องกันควบคุม หรือลดอาชญากรรม และการปฏิบัติหน้าที่ของพนักงานอัยการ ศาล หรืออำนาจหน้าที่ในการแก้ไขผู้กระทำความผิด (Correctional) การคุมความประพฤติ (Probation) การอภัยโทษ (Pardon) หรือการทำประกันทัณฑ์บน (Parole) และตามข้อยกเว้น ดังต่อไปนี้[180]

(A) ข้อมูลที่รวบบรวมไว้ใช้เพื่อวัตถุประสงค์ในการแจ้งให้ทราบว่าบุคคลใดมีสถานภาพเป็นผู้กระทำความผิดอาญา (Criminal offenders) และผู้ถูกกล่าวหาว่าเป็นผู้กระทำความผิดทางอาญา (Alleged offenders) โดยต้องประกอบด้วยข้อมูลในการแสดงสถานภาพ และบันทึกการจับกุมสภาพของการกระทำความผิด และการถูกควบคุมตัวเนื่องจากถูกฟ้องในคดีอาญา การถูกพิพากษาลงโทษ การถูกจำคุก การพ้นจากการถูกจำคุก การทำทัณฑ์บน และการคุมประพฤติ

(B) ข้อมูลที่รวบรวมไว้เพื่อวัตถุประสงค์ในการสืบสวนคดีอาญา และรวมถึงรายงานของผู้ให้ข่าว สายสืบและทีมงานที่สามารถรู้ได้ถึงสถานภาพส่วนบุคคลของบุคคลเหล่านั้นได้

(C) รายงานที่สามารถระบุชีตัวบุคคลผู้ดำเนินการอยู่ในระดับต่าง ๆ ของกระบวนการบังคับใช้กฎหมายอาญาเกี่ยวกบการจับกุม หรือการฟ้องคดีอาญา ตลอดจนการปล่อยจากการควบคุม

ข้อยกเว้นกรณีเฉพาะ (Specific exemptions) ในกรณีที่หน่วยงานของรัฐบาลกลางทั่วไปภายใต้พฤติการณ์ที่ระบุไว้อยู่ 7 กรณี ตามที่บัญญัติไว้ใน 5 U.S.C § 552 a. (k) โดยมาตรานี้ได้กำหนดให้หัวหน้าหน่วยราชการสามารถกำหนดหลักเกณฑ์การเข้าถึงระบบบันทึกข้อมูลข้อภายในหน่วยราชการนั้นได้ในบางกรณีดังนี้

กรณีแรก ข้อมูลที่เกี่ยวข้องกับการป้องกันประเทศและนโยบายการต่างประเทศ 5 U.S.C § 552a. (k) (1)

---

[180] 5 U.S. Code § 552 a. (j) General exemptions. Reads:

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

กรณีที่สอง ข้อมูลที่เป็นข้อมูลในการสืบสวน (Investigatory Material) ซึ่งรวบรวมไว้เพื่อวัตถุประสงค์ในการบังคับการให้เป็นไปตามกฎหมายนอกเหนือจากที่กำหนดไว้ในมาตรา 552 a. (j)

กรณีที่สาม ข้อมูลที่จัดเก็บไว้ เพื่อใช้ในการให้ความคุ้มครองประธานาธิบดีแห่งสหรัฐอเมริกา หรือบุคคลอื่นใดภายใต้การคุ้มครองของหน่วยงาน Secret Service 5 U.S.C § 552 a. (k) (3)

กรณีที่สุดท้าย ข้อมูลที่กำหนดไว้โดยกฎหมายให้ใช้เพียงเพื่อวัตถุประสงค์ทางด้านสถิติเท่านั้น 5 U.S.C § 552 a. (k) (4)

มาตรการในการเยียวยาทางแห่งตามบทบัญญัติฉบับนี้ (The Privacy Act) ได้มีกำหนดให้บุคคลผู้ได้รับความเสียหายจากการเปิดเผยบันทึกข้อมูลได้รับการเยียวยาทางแพ่งไว้ โดยสามารถทำการฟ้องร้องได้ภายใน 2 ปีหลังจากที่พบการเปิดเผยบันทึกข้อมูลแต่ไม่อนุญาตให้มีการฟ้องเรียกค่าเสียหายทางแพ่งซึ่งเป็นความเสียหายที่เกิดขึ้นจากการเปิดเผยบันทึกข้อมูลก่อนวันที่ 27 กันยายน ค. ศ.1975[181]

มาตรการของบทกำหนดโทษเจ้าหน้าที่ของหน่วยงานของรัฐใด หรือผู้ซึ่งโดยอาศัยอำนาจตามตำแหน่งหน้าที่หรืออำนาจตามกฎหมายในการครอบครอง หรือเข้าถึงข้อมูลส่วนบุคคลของหน่วยงานของรัฐซึ่งได้เปิดเผยข้อมูลส่วนบุคคลที่ต้องห้ามเปิดเผยโดยทุจริต หรือไม่เหตุสมควรถือว่าเป็นการกระทำความผิดลหุโทษและมีโทษปรับถึง 5,000 ดอลลาร์สหรัฐอเมริกา เจ้าหน้าที่ของหน่วยงานของรัฐใดที่เจตนาที่จะเก็บรักษาระบบบันทึกข้อมูลโดยปราศจากข้อกำหนดที่ประกาศไว้ถือว่าเป็นการกระทำความผิดลหุโทษและมีโทษปรับถึง 5,000 ดอลลาร์สหรัฐอเมริกา

---

[181] The Privacy Act of 1974 reads: (5 U.S.C. § 552a) § 552a. Records maintained on individuals

(a) Definitions.

(g) (1) Civil remedies. Whenever any agency

(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

ผู้ขอข้อมูลบุคคลใดโดยทุจริตได้ร้องขอ หรือได้รับข้อมูลที่เกี่ยวกับบุคคลจากหน่วยงานของรัฐถือว่าเป็นการกระทำความผิดลหุโทษและมีโทษปรับไม่เกิน 5,000 ดอลลาร์สหรัฐอเมริกา[182]

ดังนั้น พระราชบัญญัติ (Privacy Act) มิได้กำหนดให้มีหน่วยงานใดมีหน้าที่ดูแลและกระทำการตามกฎหมายเป็นการเฉพาะ ดังนั้น การวินิจฉัยการเปิดเผยข้อมูลส่วนบุคคล ในเบื้องต้นจึงเป็นอำนาจหน้าที่ของเจ้าหน้าที่ที่มีอำนาจของหน่วยราชการนั้น ๆ แต่ถ้าเป็นกรณีกระบวนการทางคอมพิวเตอร์ในการเปรียบเทียบข้อมูลเพื่อวัตถุประสงค์ตามที่พระราชบัญญัติ (Privacy Act) กำหนโดยโปรแกรมจับคู่ (Matching Program) พระราชบัญญัติ (Privacy Act) ได้บัญญัติให้หน่วยราชการแต่ละแห่งทีมีส่วนร่วมในกระบวนการดังกล่าว ต้องจัดให้มีคณะกรรมการควบคุมการประมวลผลข้อมูลที่ถูกต้อง (Data Integrity Boards: DIB) เพื่อทำหน้าที่ตามที่พระราชบัญญัติ (Privacy Act) บัญญัติไว้ในเรื่องเกี่ยวกับโปรแกรมจับคู่ (Matching Program) หากเป็นกรณีการเปิดเผยข้อมูลตามกระบวนการ (Matching Programs) จึงอยู่ในอำนาจหน้าที่ของ (DIB) ของหน่วยราชการแต่ละแห่งที่มีอำนาจจะวินิจฉัยการเปิดเผยข้อมูลส่วนบุคคลในกรณีดังกล่าว[183]

เมื่อถ้ามีข้อพิพาทอันเกิดจากการขอเข้าถึง หรือขอให้เปิดเผยข้อมูลส่วนบุคคล (Privacy Act)ได้กำหนดให้นำกระบวนการเยียวยาในทางแพ่งมาใช้บังคับ โดยบุคคลนั้นมีสิทธินำคดีขึ้นสู่การพิจารณาของศาลได้ ซึ่งจะต้องฟ้องคดีต่อศาลแขวงแห่งสหรัฐ(Federal District Courts) ฉะนั้น

---

[182] The Privacy Act of 1974 reads: (5 U.S.C. § 552a) § 552a. Records maintained on individuals

(a) Definitions.

(i) (1) Criminal penalties.

Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $ 5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e) (4) of this section shall be guilty of a misdemeanor and fined not more than $ 5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $ 5,000.

[183] ปิยะบุตร บุญอร่ามเรือง, พีรพัฒ โชคสุวัฒนสกุล, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร และฐิติรัตน์ ทิพย์สัมฤทธิ์กุล. (2562). ***แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล***. เอกสารงานวิจัยทางวิชาการ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. หน้า 102.

ศาลจึงเป็นอีกองค์กรหนึ่งที่มีอำนาจหน้าที่ในการวินิจฉัยการเปิดเผยข้อมูลส่วนบุคคลตาม (Privacy Act) ซึ่งก็มีปัญหาว่า การดำเนินคดีตาม (Privacy Act) จะต้องผ่านการพิจารณาโดยลูกขุน (Jury trial) เหมือนอย่างกรณีทั่วไปหรือไม่ ในประเด็นนี้ (Privacy Act) มิได้บัญญัติไว้ แต่ทุก ๆ ศาลก็ได้พิจารณาวางหลักเกณฑ์ไว้ว่า โจทก์ไม่มีสิทธิได้รับการพิจารณาโดยลูกขุนภายใต้กฎหมายนี้ ฉะนั้น แม้มีกรณีที่ต้องดำเนินคดีในทางศาล แต่คณะลูกขุนก็มิได้มีบทบาทหน้าที่ในการวินิจฉัยการเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายฉบับนี้แต่อย่างใด ผู้วิจัยพิจารณาเห็นว่า ด้วยเหตุเพราะการพิจารณาวินิจฉัยการเปิดเผยข้อมูลส่วนบุคคลนั้น ต้องอาศัยบุคคลที่มีความรู้เชี่ยวชาญเฉพาะเรื่องข้อมูลส่วนบุคคลสูงกว่าบุคคลธรรมดาทั่วไปเป็นพิเศษ โดยพฤติการณ์แห่งการใช้ชีวิตและการงาน มีความชำนาญในการให้ความเห็นต่อปัญหาข้อพิพาทจึงอยู่ในอำนาจหน้าที่ของ DIB ดังนั้น คณะลูกขุนจึงไม่สามารถวินิจฉัยการเปิดเผยข้อมูลส่วนบุคคลในกรณีเช่นนี้ได้

3.3.2 พระราชบัญญัติความเป็นส่วนตัวการสื่อสารทางอิเล็กทรอนิกส์ (Electronic Communications Privacy Act 1986)

พระราชบัญญัติความเป็นส่วนตัวการสื่อสารทางอิเล็กทรอนิกส์ (ECPA) หรือที่รู้จักกันใน ชื่อพระราชบัญญัติการดักฟัง (Wiretap Act) ใช้บังคับในปี คริสต์ศักราช 1986 บัญญัติไว้ใน 18 U.S. Code §2510-2522 กฎหมายฉบับดังกล่า มีวัตถุประสงค์ในการห้ามการดักฟังทางโทรศัพท์รวมไปถึงการดักรับข้อมูลที่ส่งโดยทางอิเล็กทรอนิกส์ผ่านทางคอมพิวเตอร์ กฎหมายเกี่ยวกับการดักฟังของสหรัฐอเมริกาอาจแบ่งออกได้เป็น 2 ระดับ[184] คือ กฎหมายระดับสหรัฐ (Federal law)และกฎหมายระดับมลรัฐ (State law) และ (ECPA) ถูกนำมาใช้เพื่อเป็นการแก้ไขพระราชบัญญัติการควบคุมอาชญากรรมของรถโดยสารและความปลอดภัยบนถนนพระราชบัญญัติการขนส่งทางบก (Omnibus Crime Control and Safe Streets Act of 1986) โดยกฎหมายการดักฟัง (Wiretap) ฉบับแรกได้มีขึ้นเพื่อป้องกันการเปิดเผยความลับของรัฐบาลในระหว่างสงครามโลกครั้งที่ 1 ในปัจจุบัน (ECPA) มีบทบัญญัติเกี่ยวกับการเข้าถึงการเปิดเผย การดักจับ และคุ้มครองความเป็นส่วนตัวในการสื่อสารผ่านทางสื่ออิเล็กทรอนิกส์กฎหมายฉบับนี้ครอบคลุมบุคคลหลายประเภท เช่น หน่วยงานของรัฐ ลูกจ้าง บุคคลธรรมดา บริษัทหุ้นส่วน หรือทรัสต์ เป็นต้น

กฎหมายระดับสหรัฐ (Federal law) ก่อนปี คริสต์ศักราช 1934 สหรัฐอเมริกายังไม่มีกฎหมายลาลักษณ์อักษรในระดับสหรัฐที่เกี่ยวข้องกับการดักฟังไว้โดยเฉพาะกฎหมายที่นำมาปรับใช้ เช่น รัฐธรรมนูญฉบับแก้ไขครั้งที่ 4 (The Fourth Amendment) โดยให้การรับรองสิทธิในความ

---

[184] คณาธิป ทองรวีวงศ์. (2556). “มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของผู้ถูกดักฟังการสื่อสารข้อมูล”. ***วารสารกระบวนการยุติธรรม***, 6(1). หน้า 2.

เป็นส่วนตัว ในส่วนที่เกี่ยวกับตัวบุคคลจะไม่ถูกตรวจค้นทรัพย์สิน หรือยึดโดยมิชอบด้วยกฎหมาย จะต้องออกหมายค้นโดยชอบสำหรับการค้นดังกล่าว โดยต้องระบุสถานที่และบุคคลที่ต้องการตรวจค้นอย่างเฉพาะเจาะจง ดังนั้น จึงพิจารณาได้จากเจตนารมณ์ของรัฐธรรมนูญนั้น ต้องการให้หลักประกันแก่ประชาชนที่จะไม่ถูกสอดเข้าเกี่ยวข้องและรบกวนความเป็นส่วนตัวจากรัฐ รวมทั้งการดักฟัง หรือดักรับข้อมูลการสื่อสารของบุคคลนั้นด้วย[185]

กฎหมายระดับมลรัฐ (State law) ในปัจจุบันมลรัฐได้ตรากฎหมายลายลักษณ์อักษรเกี่ยวกับการดักฟัง Federal Wiretap Act โดยหลักสำคัญของกฎหมายระดับมลรัฐมีองค์ประกอบเช่นเดียวกับกฎหมายระดับสหรัฐ เช่น กฎหมายมลรัฐนิวยอร์ก ได้วางหลักไว้ว่า “บุคคลจะรับผิดฐานดักฟังได้ต่อเมื่อได้มีการดักฟังโดยปราศจากความยินยอมจากผู้ส่ง หรือผู้รับข้อมูลรวมทั้งได้บันทึกการสื่อสารดังกล่าวนั้น ไม่ว่าด้วยอุปกรณ์ใด ๆ ก็ตาม”[186] ดังนั้น การให้ความยินยอมต้องได้รับความยินยอมจากคู่กรณีฝ่ายหนึ่ง (One party consent) อันเป็นข้อยกเว้นความรับผิด[187] อย่างไรก็ตาม แม้ว่าบางมลรัฐกำหนดให้ความเข้มงวดมากกว่ากฎหมายในระดับสหรัฐ เช่น มลรัฐเพนซิลวาเนีย ได้ให้ความยินยอมในการดักรับข้อมูลการสื่อสาร (All-party consent rule)[188]ให้แก่กรณีที่คู่ของกรณีทุกฝ่ายที่เกี่ยวข้องกับการสื่อสารดังกล่าว โดยเป็นข้อยกเว้นในการดักฟัง

---

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

[186] N.Y. Penal Law §250.00 (1) reads:

S 250.00 Eavesdropping; definitions of terms.

1. “Wiretapping" means the intentional overhearing or recording of a telephonic or telegraphic communication by a person other than a sender or receiver thereof, without the consent of either the sender or receiver, by means of any instrument, device or equipment. The normal operation of a telephone or telegraph corporation and the normal use of the services and facilities furnished by such corporation pursuant to its tariffs or necessary to protect the rights or property of said corporation shall not be deemed "wiretapping.”

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

[188] Pennsylvania General Assembly reads: Title 18

§ 5704. Exceptions to prohibition of interception and disclosure of communications.

(4) A person, to intercept a wire, electronic or oral communication, where all parties to the communication have given prior consent to such interception.

โดย (ECPA) นิยามของคำต่าง ๆ ไว้ใน 18 U.S. Code § 2510 มีรายละเอียด ดังนี้

“การดักจับ” หมายถึง การฟังหรือการได้รับมาโดยวิธีอื่นซึ่งเนื้อหาของการสื่อสารผ่านทางสายอิเล็กทรอนิกส์ หรือการพูดคุย โดยใช้อุปกรณ์ทางอิเล็กทรอนิกส์ เครื่องมือหรืออุปกรณ์อื่นใด[189]

“บุคคล” หมายถึง ลูกจ้าง หรือหน่วยงานของรัฐ หรือหน่วยงานย่อยของรัฐหรือหน่วยงานย่อยทางการเมือง และรวมถึงบุคคลธรรมดา หุ้นส่วน สมาคม บริษัทร่วมทุน ทรัสต์ หรือบริษัท[190]

“เนื้อหา” เมื่อใช้ร่วมกับคำว่า สาย การพูดคุย หรือการสื่อสารทางอิเล็กทรอนิกส์ให้รวมถึงข้อมูลใด ๆเกี่ยวกับสาระสำคัญ ข้อความหรือความหมายของการสื่อสาร[191]

“การติดต่อสื่อสารทางอิเล็กทรอนิกส์” หมายถึง การส่งสัญลักษณ์ สัญญาหนังสือ รูปภาพ เสียง ข้อมูล หรือข่าวกรองที่ถูกส่งทั้งหมด หรือบางส่วนผ่านทางสาย วิทยุแม่เหล็กไฟฟ้า (Photo electronic)หรือระบบแสง (Photo optical) ซึ่งส่งผลต่อการค้าระหว่างประเทศ หรือระหว่างมลรัฐ แต่ไม่รวมถึงกรณีดังนี้[192]

กรณีแรก การสื่อสารใด ๆ ผ่านทางสาย หรือผ่านทางการพูดคุย

กรณีที่สอง การสื่อสารใด ๆ ซึ่งกระทำผ่านทางอุปกรณ์เสียงเพียงอย่างเดียว

กรณีที่สาม การสื่อสารใด ๆ จากอุปกรณ์ในการติดตาม

---

[189] 18 U.S. Code § 2510.Definitions reads:

(4) “intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

[190] 18 U.S. Code § 2510.Definitions reads:

(b)a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

[191] 18 U.S. Code § 2510.Definitions reads:

(8) “contents”, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

[192] 18 U.S. Code § 2510.Definitions reads:

(12) “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce, but does not include.

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

กรณีสุดท้าย ข้อมูลการโอนเงินผ่านระบบอิเล็กทรอนิกส์ซึ่งเก็บรวบรวมโดยสถาบันการเงินในระบบการสื่อสารซึ่งใช้เพื่อการเก็บรวบรวมทางอิเล็กทรอนิกส์และการโอนเงิน

"ระบบการสื่อสารทางอิเล็กทรอนิกส์" หมายถึง อุปกรณ์เกี่ยวกับสายเพื่ออำนวยความสะดวก วิทยุแม่เหล็กไฟฟ้า (Photo optical หรือ Photoelectronic) ซึ่งใช้เพื่อการส่งผ่านการสื่อสารทางสาย หรือสื่อสารทางอิเล็กทรอนิกส์ และอุปกรณ์เกี่ยวกับคอมพิวเตอร์ใด ๆ หรือเกี่ยวกับอุปกรณ์ทางอิเล็กทรอนิกส์ ซึ่งใช้เพื่อสำหรับการจัดการเก็บรวบรวมข้อมูลการสื่อสารทางอิเล็กทรอนิกส์ดังกล่าว[193]

"ผู้บุกรุกคอมพิวเตอร์"[194] หมายถึง บุคคลซึ่งเข้าถึงคอมพิวเตอร์ที่มีมาตรการป้องกันโดยมิได้รับอนุญาตและปราศจากเหตุอันสมควรที่จะคาด หมายถึง สิทธิในความเป็นส่วนตัวโดยชอบด้วยกฎหมายในการสื่อสารที่ส่งจาก หรือผ่านจากคอมพิวเตอร์ที่มีระบบป้องกันนั้น แต่ไม่รวมถึงบุคคลที่ผู้ให้บริการ หรือเจ้าของคอมพิวเตอร์ได้ทราบอยู่แล้วว่ามีสัญญากับผู้ให้บริการ หรือเจ้าของคอมพิวเตอร์สำหรับการเข้าถึงทั้งหมด หรือบางส่วนของคอมพิวเตอร์ที่มีมาตรการป้องกัน

ดังนั้น หากพิจารณา (ECPA) ได้มีการบทบัญญัติเกี่ยวกับการคุ้มครองการดักจับและการเปิดเผยการสื่อสารผ่านทางสาย การพูดคุย และอิเล็กทรอนิกส์ใน 18 U.S. Code §2511 ซึ่งกำหนดให้การกระทำดังต่อไปนี้เป็นความผิด[195]

---

[193] 18 U.S. Code § 2510.Definitions reads:

(14) "electronic communications system" means any wire, radio, electromagnetic, photo optical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

[194] 18 U.S. Code § 2510.Definitions reads:

(21) "computer trespasser"

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, though, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

[195] 18 U.S. Code § 2511.Interception and disclosure of wire, oral, or electronic communications prohibited reads:

(1) Except as otherwise specifically provided in this chapter any person who

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

บุคคลซึ่งเจตนาดักจับ หรือพยายามดักจับ หรือจัดหาบุคคลเพื่อการดักจับ หรือพยายามดักจับการสื่อสารผ่านทางสาย การพูดคุย หรือผ่านทางอิเล็กทรอนิกส์

บุคคลซึ่งเจตนาใช้ หรือพยายามใช้ หรือจัดหาบุคคลอื่นใด เพื่อใช้ หรือพยายามใช้อุปกรณ์ทางอิเล็กทรอนิกส์ เครื่องมือ หรืออุปกรณ์อื่นเพื่อดักจับการสื่อสาร

อุปกรณ์นั้นติดต่อ หรือส่งสัญญาผ่านทางสาย สายเคเบิล หรือการเชื่อมต่ออื่นซึ่งมีลักษณะเดียวกันซึ่งใช้ในการสื่อสารทางสาย หรือ

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(e) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2) (a) (ii), 2511(2) (b)–(c), 2511(2) (e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

อุปกรณ์นั้นส่งการสื่อสารผ่านทางวิทยุ หรือรบกวนการส่งการสื่อสารนั้น หรือบุคคลนั้นรู้ หรือมีเหตุผลอันควรรู้ได้ว่าอุปกรณ์นั้น หรือส่วนประกอบของอุปกรณ์นั้นถูกส่งโดยพัสดุ หรือถูกขนส่งในการค้าระหว่างประเทศ หรือระหว่างมลรัฐ

การใช้ หรือการพยายามใช้นั้นก่อให้เกิด โดยอาจส่งผลกระทบต่อการค้าระหว่างรัฐ หรือระหว่างมลรัฐ หรือได้รับ หรือมีวัตถุประสงค์เพื่อให้ได้รับข้อมูลเกี่ยวกับการดำเนินงานของธุรกิจ หรือห้างร้างอื่นซึ่งอาจส่งผลกระทบต่อการค้าระหว่างรัฐ หรือระหว่างมลรัฐ หรือตั้งใจเปิดเผย หรือพยายามเปิดเผยแก่บุคคลอื่นซึ่งเนื้อหาเกี่ยวกับการสื่อสารทางสาย ทางการพูดคุย หรือทางอิเล็กทรอนิกส์ โดยรู้ หรือมีเหตุอันควรรู้ว่าการสื่อสารนั้นได้มาจากการดักจับผ่านทางสาย การพูดคุย หรือทางอิเล็กทรอนิกส์

เจตนาใช้ หรือพยายามใช้เนื้อหาการสื่อสารทางสาย ทางการพูดคุย หรืออิเล็กทรอนิกส์ โดยรู้ หรือเหตุอันควรรู้ว่าการสื่อสารนั้นได้รับจากการดักจับผ่านทางสาย การพูดคุย หรือทางอิเล็กทรอนิกส์เจตนาเปิดเผย หรือพยายามเปิดเผยแก่บุคคลใด ๆ ซึ่งเนื้อหาของการสื่อสารทางสาย การพูดคุย หรืออิเล็กทรอนิกส์ ซึ่งได้มาโดยวิธีการที่ไม่ชอบ

บุคคลดังกล่าวรวมถึงบุคคลที่ได้กระทำในโคลอมเบีย เปอร์โตริโก หรือดินแดน หรือดินแดนซึ่งอยู่สมบัติของประเทศสหรัฐอเมริกา

ดังนั้น ประการสำคัญของกฎหมายความเป็นส่วนตัวในการสื่อสารทางอิเล็กทรอนิกส (Electronic Communications Privacy Act: ECPA) ซึ่งเกี่ยวกับความเป็นส่วนตัวของผู้บริโภคนั้น เป็นการวางหลักการห้ามการดักฟังการสื่อสารใด ๆ ก็ตาม ซึ่งข้อมูลที่ได้มานั้นอาจส่งผลทำให้เกิดการตัดสินใจที่เป็นปรปักษ์กับสิทธิส่วนบุคคลนั้น ทั้งนี้ เนื่องจากกฎหมายกำหนดว่า การดักฟัง (Interception) จะเกิดขึ้นเมื่อมีการได้ยิน หรือการได้มาซึ่งเนื้อหาข้อมูลทางการสื่อสารโดยใช้สายแอบฟัง (Wire) วาจา (Oral) ผ่านทางอิเล็กทรอนิกส์ หรืออุปกรณ์ใด ๆ[196] ดังนั้น จะเห็นได้ว่ากฎหมายฉบับนี้มิได้จำกัดเฉพาะการ “ดักฟัง” แต่ครอบคลุมการ “ดักรับการสื่อสารข้อมูล” ไม่ว่าจะกระทำด้วยวิธีการใด ๆ ก็ตาม ซึ่งสหรัฐอเมริกาก็ได้ให้ความสำคัญต่อการคุ้มครองสิทธิในความเป็นส่วนตัวรวมถึงการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างมาก เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่หน่วยงานของรัฐที่จัดเก็บที่อยู่ในความดูแล รวมถึงการส่งเสริมความเชื่อมั่นให้สำหรับประชาชนในการให้ข้อมูลที่เป็นจริงกับหน่วยงานของอีกประการหนึ่งด้วย ทั้งนี้ ปัญหาความเป็นส่วนตัวกลายเป็นประเด็นที่ทั่วยุโรปให้ความสำคัญเป็นอย่างมาก ซึ่งจากกรณีของเอ็ดเวิร์ด

---

[196] 18 U.S.C. §2510 (4) (2006) reads:

“interception occurs by the “aural or other acquisition of contents of any wire, electronic, or oral communicationthrough the use of any electronic, mechanical, or other device.”

สโนว์เดน ที่ออกมาเปิดเผยข้อมูลลับของหน่วยงานราชการของสหรัฐอเมริกาที่ลักลอบดักฟังการสนทนาในระบบสื่อสารทั่วโลก ทำให้ยุโรปจำเป็นต้องวางแผนการป้องกันข้อมูลอย่างรัดกุมต่อไป

3.3.3 พระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ (Biometric Information Privacy Act 2008: BIPA)

ประวัติโดยย่อของกฎหมายข้อมูลไบโอเมตริกซ์ ใช้บังคับเมื่อในปี ค.ศ 2008 อิลลินอยส์ (Illinois) (Biometric Information Privacy:BIPA) เป็นครั้งแรกที่ให้ความสำคัญเกี่ยวกับลายนิ้วมือของรัฐอิลลินอยส์ (BIPA) และการบังคับใช้เพิ่มอีกสองรัฐ เช่น รัฐเท็กซัส หรือการใช้กฎระเบียนการระบุตัวตนทางชีวมาตร (Texas Biometric Identifier Statute: BIS) กฎหมายการระบุตัวตนทางชีวมาตรของวอชิงตัน (Washington Biological Identification Law: BI) มีผลบังคับใช้มาจากกฎหมายข้อมูลไบโอเมตริกทั้งสามรัฐนี้ มีเพียงรัฐอิลลินอยส์ (BIPA) เท่านั้นที่ให้สิทธิในการดำเนินคดีด้วยตนเองได้ และควบคุมการเก็บรวบรวมชีวมาตรทั้งหมด ไบโอเมตริกซ์ (Biometrics) รวมถึงลายนิ้วมือ (DNA) ท่าทาง การเดิน จังหวะการพิมพ์ การพิมพ์เสียง รูปแบบหลอดเลือดดำและรูปทรงของใบหน้า หรือเพียงเพื่อชื่อไม่กี่ชื่อ สำหรับผู้ให้บริการด้านการดูแลสุขภาพรวบรวมข้อมูลที่ระบุตัวตนเกี่ยวกับผู้ป่วย ซึ่งโดยปกติจะรวมถึงข้อมูล (DNA)[197] (สำหรับการปรึกษาทางพันธุกรรม) รูปแบบการเดิน (สำหรับนักกายภาพบำบัด หรือศูนย์บำบัด) ข้อมูลเสียง (สำหรับนักบำบัดการพูด) รูปแบบหลอดเลือดดำปาล์ม (สำหรับแพทย์ผิวหนัง) และใบหน้า (สำหรับการปฏิบัติโดยใช้ภาพถ่ายผู้ป่วยเพื่อยืนยันตัวตนเมื่อทำการเข้ารักษา) หน่วยงานด้านการดูแลสุขภาพบางแห่งก็ใช้ระบบไบโอเมตริกซ์ เช่น ลายนิ้วมือของพนักงานเพื่อจัดการกับกระบวนการเข้า – ออกและการตอกบัตรแทนที่จะใช้บัตรประจำตัวของพนักงานแบบเดิม ๆ ที่ดูเหมือนจะโบราณไปแล้ว และในขณะที่วิธี (Biometrics) ดังกล่าวนี้ ได้รับการปรับปรุงในความแม่นยำของการตรวจสอบการปฏิบัติงานของพนักงานให้ง่ายและสะดวกขึ้นด้วย แต่ต้องดำเนินการภายในขอบเขตของ (BIPA) เท่านั้น

พระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ (BIPA) ได้ให้คำนิยามศัพท์ไว้ดังนี้

“ข้อมูลไบโอเมตริกซ์” หมายถึง ข้อมูลใด ๆ ก็ตาม โดยไม่คำนึงถึงวิธีการบันทึก แปลง จัดเก็บ หรือ แชร์โดยการอ้างอิงจากอัตลักษณ์ จากการระบุตัวตนด้วยระบบไบโอเมตริกซ์ของ

---

[197] Hannah Zimmerman. (2018). ***The Data of You: Regulating Private Industry's Collection of Biometric Information.*** Vol. 66. p. 5

บุคคลนั้น เพื่อใช้ระบุตัวตนบุคคล ด้วยข้อมูลไบโอเมตริกซ์ ไม่รวมถึงข้อมูลที่ได้มาจากการรวบรวม หรือ ขั้นตอน ที่ได้ยกเว้นภายใต้คำจำกัดความของระบบไบโอเมตริกซ์ฉบับนี้[198]

"การระบุตัวบุคคลทางชีวมาตร" (Biometric identifier) หมายถึง การสแกนม่านตา หรือพิมพ์ลายนิ้วมือเสียง หรือ การสแกนรูปทรงของฝ่ามือ หรือใบหน้า การระบุตนด้วย (Biometric) จะไม่รวมถึง การเขียนด้วยลายเซ็นที่เป็นลายลักษณ์อักษร ภาพถ่ายตัวอย่างทางชีวภาพของมนุษย์ที่ใช้สำหรับการทดสอบทางวิทยาศาสตร์หรือ ข้อมูลของประชากร รอยสัก หรือลักษณะทางกายภาพ เช่น ความสูง น้ำหนัก สีผม หรือ สีตา การระบุตนทางไบโอเมตริกซ์ ไม่รวมถึง การบริจาคอวัยวะ เนื้อเยื่อ หรือชิ้นส่วนตามที่กำหนดไว้ในพระราชบัญญัติกายวิภาคของรัฐอิลลินอยส์ หรือ เลือด หรือ เซรัมที่จัดเก็บในนามของผู้รับ หรือผู้รับที่อาจมีชีวิตที่รอการปลูกถ่ายอวัยวะ หรือ ผู้ที่เสียชีวิต ข้อมูลผู้ป่วย ข้อมูลสุขภาพ ข้อมูลทางพันธุกรรมที่มีการควบคุมภายใต้พระราชบัญญัติความเป็นส่วนตัว หรือข้อมูลที่รวบรวม ใช้ หรือเก็บไว้สำหรับการดูแลสุขภาพ การชำระเงิน หรือ การดำเนินงานภายใต้พระราชบัญญัติประกันสุขภาพของรัฐบาลกลางและพระราชบัญญัติความรับผิดชอบปี 1996 X- ray กระบวนการ (Roentgen) การตรวจเอกซเรย์คอมพิวเตอร์ (MRI) การสแกนด้วย (PET) การตรวจด้วยแมมโมแกรม หรือภาพ หรือภาพยนตร์อื่น ๆ ของกายวิภาคศาสตร์มนุษย์ที่ใช้ในการวินิจฉัยโรค หรือรักษาโรค หรือ อาการทางการแพทย์อื่น ๆ[199]

---

[198] 740 ILCS 14/1 reads: Section. 1. Short title. This Act may be cited as the Biometric Information Privacy Act. (740 ILCS 14/10) Section. 10. Definitions. In this Act. reads:

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

[199] (740 ILCS 14/10) Sec. 10. Definitions. In this Act: reads:

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography,

“ข้อมูลที่เป็นความลับและละเอียดอ่อน” (Biometric and sensitive information) หมายถึง ข้อมูลส่วนบุคคลที่สามารถใช้เพื่อระบุบัญชี หรือ ทรัพย์สินของบุคคล หรือ ระบุตัวตนบุคคลโดยเฉพาะ เช่น ข้อมูลที่เป็นความลับและละเอียดอ่อน แต่ไม่รวมถึงเครื่องหมายทางพันธุกรรม ข้อมูลการทดสอบทางพันธุกรรม หมายเลขตัวบ่งชี้เฉพาะเพื่อค้นหาบัญชี หรือทรัพย์สิน หมายเลขบัญชี หมายเลข PINรหัสผ่าน หมายเลขใบขับขี่ หรือหมายเลขประกันสังคม[200]

“ความยินยอม” (Written release) หมายถึง การยินยอมเป็นลายลักษณ์อักษร หรือ ตามสัญญาการจ้างงานการสมัครงานของพนักงานให้เป็นไปตามเงื่อนไขของการจ้างงาน[201]

“การถอน” ต้องแจ้งเจ้าของข้อมูลเป็นลายลักษณ์อักษรของข้อมูลไบโอเมตริกซ์ หรือตัวแทนผู้มีอำนาจตามกฎหมาย[202]

“การเก็บรักษา” หมายถึง การรวบรวม เปิดเผย การทำลาย หน่วยงานเอกชนที่ครอบครองข้อมูลไบโอเมตริกซ์จะต้องพัฒนานโยบายที่เป็นลายลักษณ์อักษรที่จะเปิดเผยต่อสาธารณชน กำหนดตารางการเก็บรักษาและแนวทางสำหรับการทำลายข้อมูลไบโอเมตริกซ์อย่างถาวรเมื่อไม่ประสงค์[203]

MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

[200] (740 ILCS 14/5) Section. 5. Legislative findings; intent. The General Assembly finds all of the following: reads:

“Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number”.

[201] (740 ILCS 14/5). Section. 5. Legislative findings; intent. The General Assembly finds all of the following: reads:

"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

[202] 740 ILCS 14/15 (3) reads:

“receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.”

[203] (740 ILCS 14/15) Section. 15. Retention; collection; disclosure; destruction. reads:

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has

“องค์กรเอกชน” หมายถึง ห้างหุ้นส่วนบุคคล บริษัท สมาคม หรือองค์กรกลุ่มอื่น ๆ หน่วยงานเอกชนไม่รวมถึงหน่วยงานรัฐ หรือหน่วยงานรัฐบาลท้องถิ่น หน่วยงานเอกชนไม่รวมศาลของรัฐอิลลินอยส์ เสมียนศาลหรือผู้พิพากษา หรือผู้พิพากษาดังกล่าว[204]

การสแกนนิ้วมือ หรือรูปทรงใบหน้าของบุคคลถูกกำหนดให้ “ข้อมูลไบโอเมตริกซ์” เป็น “ข้อมูลใด ๆ ... ตามตัวระบุไบโอเมตริกซ์ของบุคคลที่ใช้ เพื่อระบุตัวบุคคล” ตาม 740 ILCS 14/10 ซึ่งเป็นข้อมูลประเภทพิเศษและละเอียดอ่อนภายใต้ (BIPA) องค์กรเอกชนที่ครอบครองตัวระบุและข้อมูลดังกล่าว จะต้องกำหนดนโยบายเป็นลายลักษณ์อักษรเกี่ยวกับการเก็บ รักษา การลบ การทำลายและไม่สามารถรับข้อมูลดังกล่าวได้ เว้นแต่จะแจ้งเรื่องการรวบรวม

การแจ้งเรื่องข้อมูลที่ประสงค์เฉพาะสำหรับการรวบรวมและระยะเวลาที่ข้อมูลจะถูกเก็บไว้ และได้รับความยินยอมเป็นลายลักษณ์อักษรตาม 740 ILCS 10/15 (b) และการถอนความยินยอมตาม Section 740 ILCS 14/25[205] ที่สำคัญ (BIPA) กำหนดโทษปรับมาจากสาเหตุของการกระทำโดยการละเมิดความเป็นส่วนตัวทางชีวมาตร ตามกฎหมายปรับสูงถึง 1,000 ดอลลาร์ ในความเสียหายที่ต้องจ่าย หรือความเสียหายที่เกิดขึ้นจริงสำหรับค่าปรับสูงถึง 5,000 ดอลลาร์ ในความเสียหายที่ต้องจ่าย หรือความเสียหายที่แท้จริง สำหรับการละเมิดโดยเจตนา หรือโดยประมาทตาม 740 ILCS 14/20 (1) และ (2) กฎหมายยังให้สิทธิผู้เสียหายเรียกค่าธรรมเนียมและค่าใช้จ่ายทนายความได้เองตามความเหมาะสม 740 ILCS 14/20 (3)

พระราชบัญญัติ (Illinois BIPA) กำหนดให้ “การระบุตัวตนด้วยไบโอเมตริกซ์ โดยวิธีการสแกนม่านตา หรือม่านตาลายนิ้วมือ เสียง หรือการสแกนรูปฝ่ามือ หรือรูปทรงของใบหน้า โดยมีข้อยกเว้นอื่น ๆ อิลลินอยส์ (BIPA) จะไม่รวมการเขียนลายเซ็น ภาพถ่าย รูปถ่ายตัวอย่างชีวภาพมนุษย์ การทดสอบทางวิทยาศาสตร์ หรือการคัดกรองข้อมูลประชากร คำบรรยาย รอยสัก หรือลักษณะทางกายภาพ เช่น ความสูง น้ำหนัก สีผม และสีนัยน์ตา ข้อมูลที่บันทึกจากผู้ป่วยในการดูแลสุขภาพ และข้อมูลประเภทอื่นด้วย[206]

---

[204] (740 ILCS 14/10). Section. 10. Definitions. In this Act: reads:

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

[205] Section 740 ILCS 14/25 reads:

(a) Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.

[206] 740 ILCS 14/10.

3.3.3.1 พระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์รัฐเท็กซัส (Texas Biometric Privacy Act 2009)

พระราชบัญญัติ (Texas BIS) ได้ถูกบัญญัติไว้ในมาตรา 11.A.503[207] ของรหัสเท็กซัสธุรกิจและการพาณิชย์และมีผลบังคับใช้ในวันที่ 23 กรกฎาคม 2017 โดยใช้คำจำกัดความที่

---

[207] Business and commerce code. Title 11. Personal identity information

Subtitle A. identifying information Chapter 503. biometric identiffrs

Section. 503.001. Capture or use of biometric identifier. Reads:

(a) In this section,"biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.

(b) A person may not capture a biometric identifier of an individual for a commercial purpose unless the person:

(1) informs the individual before capturing the biometric identifier; and

(2) receives the individual's consent to capture the biometric identifier.

(c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose:

(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:

(A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death;

(B) the disclosure completes a financial transaction that the individual requested or authorized;

(C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code or

(D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant;

(2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses; and

(3) shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1).

(c-1) If a biometric identifier of an individual captured for a commercial purpose is used in connection with an instrument or document that is required by another law to be maintained for a period longer than the period prescribed by Subsection (c)(3), the person who possesses the biometric identifier shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the instrument or document is no longer required to be maintained by law.

แคบกว่า “ตัวระบุไบโอเมตริกซ์” หมายถึง การสแกนม่านตา หรือ ลายนิ้วมือ เสียง หรือ รูปทรงมือ หรือรูปทรงของใบหน้า[208] สำหรับบทลงโทษกฎหมายอนุญาตให้มีการลงโทษทางแพ่งสูงถึง 25,000

(c-2) If a biometric identifier captured for a commercial purpose has been collected for security purposes by an employer, the purpose for collecting the identifier under Subsection (c) (3) is presumed to expire on termination of the employment relationship.

(d) A person who violates this section is subject to a civil penalty of not more than $25,000 for each violation. The attorney general may bring an action to recover the civil penalty.

(e) This section does not apply to voiceprint data retained by a financial institution or an affiliate of a financial institution, as those terms are defined by 15 U.S.C. Section 6809.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

Amended by:

Acts 2009, 81st Leg., R.S., Ch. 1163 (H.B. 3186), Sec. 1, eff. September 1, 2009.

Acts 2017, 85th Leg., R.S., Ch. 913 (S.B. 1343), Sec. 1, eff. September 1, 2017.

[208] Sec. 503.001. Capture or use of biometric idenifer. reads:

(a) In this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.

(b) A person may not capture a biometric identifier of an individual for a commercial purpose unless the person:

(1) informs the individual before capturing the biometric identifier; and

(2) receives the individual's consent to capture the biometric identifier.

(c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose:

(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:

(A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death;

(B) the disclosure completes a financial transaction that the individual requested or authorized;

(C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or

(D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant;

(2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses; and

ดอลลาร์ แต่มีเพียงอัยการสูงสุดเท่านั้นที่สามารถฟ้องบริษัทได้ สำหรับการละเมิดความเป็นส่วนตัวทางชีวมาตร

3.3.3.2 ร่างพระราชบัญญัติฉบับที่ 1493 แห่งมลรัฐวอชิงตัน (Washington House Bill 1493 Act 2017)

พระราชบัญญัติ (Washington BI) ซึ่งต่อไปในวิทยานิพนธ์ฉบับนี้ เรียกว่า HB 1493 มีผลบังคับใช้ในวันที่ 23 กรกฎาคม 2017 วอชิงตันจึงเป็นรัฐที่สามที่ผ่านการออกกฎหมายควบคุมการใช้ตัวระบุไบโอเมตริกซ์เชิงพาณิชย์ โดยกำหนดให้ข้อมูลไบโอเมตริกซ์เป็น “ข้อมูลที่สร้างขึ้นโดยอัตโนมัติของลักษณะทางชีวภาพของแต่ละบุคคล” และข้อจำกัดเฉพาะข้อมูลไบโอเมตริกซ์ที่ได้รับการ “ลงทะเบียน” หรือลดรูปแบบในฐานข้อมูล โดยบัญญัติไว้ดังนี้ “ห้ามมิให้องค์เอกชนใดระบุตัวบุคคลในการลงทะเบียนด้วยการระบบไบโอเมตริกซ์ลงในฐานข้อมูล โดยไม่แจ้งให้ทราบล่วงหน้าและให้ความยินยอม ห้ามการขายให้เช่าซื้อ หรือเปิดเผยตัวระบุไบโอเมตริกซ์เพื่อวัตถุประสงค์ทางการค้า เว้นแต่จะมีคุณสมบัติตรงตามเกณฑ์ที่กำหนด โดยกำหนดนโยบายเกี่ยวกับการเก็บรักษาและการเข้าถึงตัวระบุไบโอเมตริกซ์”[209] เช่นเดียวกับ (Illinois BIPA)

---

(3) shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1).

(c-1) If a biometric identifier of an individual captured for a commercial purpose is used in connection with an instrument or document that is required by another law to be maintained for a period longer than the period prescribed by Subsection (c) (3), the person who possesses the biometric identifier shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the instrument or document is no longer required to be maintained by law.

(c-2) If a biometric identifier captured for a commercial purpose has been collected for security purposes by an employer, the purpose for collecting the identifier under Subsection (c) (3) is presumed to expire on termination of the employment relationship.

(d) A person who violates this section is subject to a civil penalty of not more than $ 25,000 for each violation. The attorney general may bring an action to recover the civil penalty.

(e) This section does not apply to voiceprint data retained by a financial institution or an affiliate of a financial institution, as those terms are defined by 15 U.S.C. Section 6809.

[209] 2017 House Bill 1493: Concerning biometric identifiers

Substitute offered in the House on February 14, 2017 reads:

“Prohibits a person from identifying an individual by enrolling a biometric identifier in a database without notice and consent. Prohibits selling, leasing, or disclosing a biometric identifier for a commercial

และ (Texas BIS) โดยไม่รวมภาพถ่ายและข้อมูลที่เก็บรวบรวมเกี่ยวกับการรักษาพยาบาลและยังไม่รวมถึงข้อมูลที่เกิดจากรูปถ่ายทั่วไปที่ไม่ชัดเจน[210] HB 1493 ได้มีข้อกำหนดเพิ่มเติม โดยเฉพาะอย่างยิ่งเกี่ยวกับรายละเอียดในการลงทะเบียนตัวระบุไบโอเมตริกซ์ เพื่อวัตถุประสงค์ทางการค้า รวมถึงการเปิดเผยข้อมูลดังกล่าวไว้ในภายหลัง เมื่อวันที่ 2 มีนาคม 2017 ซึ่งกฎหมายทั้งสามฉบับระบุบทในการลงโทษทางแพ่งสำหรับการละเมิด แต่รัฐอิลลินอยส์ (BIPA) เป็นกฎหมายเพียงฉบับเดียวในสามฉบับที่ให้สิทธิส่วนบุคคล ในการดำเนินการฟ้องร้องที่ได้รับอนุญาตให้โจทก์สามารถ

---

purpose unless certain criteria are met. Establishes requirements regarding biometric identifier retention and access."

[210] RCW 19.375.010. Definitions. reads:

The definitions in this section apply throughout this chapter, unless the context clearly requires otherwise.

(1) "Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric identifier" does not include a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996.

(2) "Biometric system" means an automated identification system capable of capturing, processing, and storing a biometric identifier, comparing the biometric identifier to one or more references, and matching the biometric identifier to a specific individual.

(3) "Capture" means the process of collecting a biometric identifier from an individual.

(4) "Commercial purpose" means a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier. "Commercial purpose" does not include a security or law enforcement purpose.

(5) "Enroll" means to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual.

(6) "Law enforcement officer" means a law enforcement officer as defined in RCW 9.41.010 or a federal peace officer as defined in RCW 10.93.020.

(7) "Person" means an individual, partnership, corporation, limited liability company, organization, association, or any other legal or commercial entity, but does not include a government agency.

(8) "Security purpose" means the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person.

เรียกร้องค่าเสียหายและค่าธรรมเนียมทนายความได้เองตามความเหมาะสม ส่วนในรัฐเท็กซัสและวอชิงตันมีเพียงอัยการสูงสุดของรัฐเท่านั้นที่สามารถฟ้องร้องดำเนินคดีได้

ตัวอย่างคดี เช่น

คดี Rosenbach v. Six Flags[211]

เมื่อวันที่ 25 มกราคม 2019 ศาลฎีกาแห่งรัฐอิลลินอยส์ได้กลับคำพิพากษาของศาลอุทธรณ์ของรัฐว่าเป็นการละเมิดกฎหมายความเป็นส่วนตัวด้านข้อมูลทางชีวมาตรของรัฐอิลลินอยส์ “BIPA” 740 ILL COMP. STAT 14 (2008) คดี Rosenbach v. Six Flags โดย Stacy Rosenbach[212] โจทก์ได้ทำการซื้อบัตรผ่านเข้าสู่ซีซันสวนสนุกให้สำหรับบุตรชายวัย 14 ปี ของโจทก์ ซึ่งเป็นส่วนหนึ่งของการทัศนศึกษาที่สวนสนุก Six Flags Amusement Park เมื่อมาถึงที่สวนสาธารณะบุตรชายของโจทก์จะต้องถูกส่งสแกนลายนิ้วมือเพื่อใช้บัตร ซึ่งก่อนหน้านี้บุตรชายของโจทก์พยายามเปิดใช้งานบัตรผ่านนั้น Rosenbach ได้รับการแจ้งเกี่ยวกับข้อกำหนดการพิมพ์ลายนิ้วมือ หรือวิธีการใช้ หรือจัดเก็บข้อมูลที่สำคัญ Rosenbach ไม่ได้ให้ข้อกล่าวอ้างว่าการละเมิดนั้น ก่อให้เกิดความเสียหายทางการเงินหรือ อื่น ๆ ใดจากการตรวจสอบข้อเท็จจริงเหล่านี้แล้ว ศาลฎีการัฐอิลลินอยส์ได้ยอมรับข้อโต้แย้งของโจทก์ว่านโยบาย Six Flags จำเลยเป็นการกระทำละเมิดและเป็นการละเมิดกฎหมาย (BIPA)

โดยการรวบรวมลายนิ้วมือของผู้เยาว์ “โดยไม่แจ้งล่วงหน้าเป็นลายลักษณ์อักษรและไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรล่วงหน้า” อันเป็นการเพียงพอที่จะนำคดีมาฟ้องต่อสู่ศาลโดยศาลระบุว่าบุคคลที่ “ได้รับอันตราย” อาจเรียกร้องให้ชำระความเสียหายและการบรรเทาทุกข์ตามพระราชบัญญัติฉบับนี้ได้ แม้ว่าพวกเขาจะไม่ได้รับอันตราย หรือ ผลกระทบที่ร้ายแรงจากการละเมิดก็ตาม ซึ่งเป็นสิทธิภายใต้บทบัญญัติของกฎหมาย (BIPA) เนื่องจากกฎหมายกำหนดให้รักษาสิทธิส่วนบุคคลไว้โดยชัดแจ้ง 740 ILCS 14/1 et seq. (BIPA) นับตั้งแต่นั้นเป็นมาก็มีการฟ้องร้องหลายคดีเกิดขึ้นภายใต้ (BIPA) ซึ่งรวมถึงการฟ้องร้องของลูกจ้างเป็นโจทก์ฟ้องเรียกร้องสำหรับการกระทำของนายจ้างได้ เช่น การรวบรวมและการใช้ลายนิ้วมือ เพื่อติดตามเวลาการทำงาน หรือการควบคุมความปลอดภัยที่มีลักษณะคล้ายบทบัญญัติของ (BIPA) ที่บ่งบอกถึงความเสี่ยงที่จะได้รับอันตรายเพิ่มขึ้น สำหรับองค์กรที่ได้รวบรวม ใช้และจัดเก็บข้อมูล

---

[211] Illinois Official Reports Supreme Court. (2019). ***Rosenbach v. Six Flags Entertainment Corp***., 2019 IL 123186 (Online). Available: https://courts.illinois.gov/Opinions/SupremeCourt/2019/123186.pdf. [2562, 29 July]

[212] Skadden. (2019). ***Illinois Supreme Court Holds That Biometric Privacy Law Does Not Require Actual Harm for Private Suits***. (Online). Available: https://www.skadden.com/insights/publications/2019/01/illinois-supreme-court. [2562, 29 July]

ไบโอเมตริกซ์ของพนักงาน หรือลูกค้าเพื่อวัตถุประสงค์ ในการรวบรวมข้อมูลนั้นจะหมดอายุลงเมื่อมีการยกเลิกตามสัญญาในการจ้างงาน[213]

คดี Facebook[214]

คดีเฟซบุ๊ก (Facebook) ในการละเมิดข้อมูลส่วนบุคคลครั้งประวัติศาสตร์ เมื่อถูกปรับ 150,000 ล้าน ซึ่งเป็นบทเรียนสำคัญต่อบริษัทเทคโนโลยียักษ์ใหญ่ และโซเชียลมีเดียทั่วโลกต้องมีมาตรการปกป้องผู้ใช้บริการระหว่าง Patel v. Facebook, Inc. หมายเลข 18-15982 (8 สิงหาคม 2019) ทำให้ศาลยุติธรรมแห่งสหภาพยุโรปมีคำพิพากษาในคดีระหว่าง FashionID GmbH & Co. KGและ Verbraucherzentrale NRW (สมาคมคุ้มครองผู้บริโภคแห่งรัฐนอร์ทไรน์-เว็สท์ฟาเลิน) โดยมี Facebook Ireland Limited ซึ่งเป็นบริษัทลูกของ (Facebook Inc) ที่ให้บริการนอกประเทศสหรัฐอเมริกา โดยได้ขอเข้ามาเป็นคู่ความในคดีนี้ด้วย เนื่องจากพฤติกรรมของคดี รวมทั้งผลของคำพิพากษาจะต้องส่งผลกระทบโดยตรงต่อการประกอบธุรกิจของ (Facebook)

คดีนี้ได้ฟ้องเมื่อปี 2015โดยฟ้องตาม (Data Protection Directive 95/46/EC) ซึ่งเป็นกฎหมายฉบับเก่าที่สหภาพยุโรปถูกยกเลิกก่อนที่จะบังคับได้ใช้ GDPR ฉบับใหม่ โดยเริ่มต้นการฟ้องในศาลแห่งเมืองดีสเซิลดอร์ฟ (Düsseldorf) ประเทศสหพันธ์รัฐสาธารณรัฐเยอรมนี โดย Verbraucherzentrale NRW เห็นว่า FashionID ได้กระทำผิดกฎหมาย (Data Protection Directive 95/46/EC) เนื่องจากไม่ได้มีการแจ้งให้ผู้เข้าใช้เว็บไซต์ของตนเองทราบว่าได้มีการประมวลผลข้อมูลส่วนบุคคลโดย Facebook และไม่มีการขอความยินยอมจากผู้บริโภคในการส่งข้อมูลส่วนบุคคลให้แก่ (Facebook) แต่อย่างใด

---

[213] Robert fallah, (FEB. 6, 2019), Illinois Supreme Court Ruling: Biometric Privacy Law Only Requires Violation, Not Actual Harm.reads: In the class action at issue, Rosenbach v. Six Flags Entertain. Corp., plaintiff Stacy Rosenbach purchased a season pass for her 14-year-old son as part of a school field trip to Six Flags Amusement Park. Upon arrival at the park, her son was required to submit to a fingerprint scan in order to use the pass. At no point before her son attempted to activate the pass was Rosenbach informed about the fingerprinting requirement or how the information would be used or stored. Importantly, Rosenbach did not claim that the violation caused financial or other harm. Upon reviewing these facts, The Illinois Supreme Court accepted her argument that the Six Flags policy violated the act, and that the violation of BIPA alone was sufficient to bring suit. Specifically, the court stated that an "aggrieved" person "may seek liquidated damages and injunctive relief pursuant to the Act even if he or she has not alleged some actual injury or adverse effect, beyond violation of his or her rights under the statute. (Online). Available:https://www.fisherphillips.com/Employment-Privacy-Blog/illinois-supreme-court-ruling-biometric-rivacy-law. [2562, 9 September]

[214] Justia Opinion Summary.Patel v. Facebook, Inc., No. 18-15982 (9th Cir. 2019). (Online). Available: https://law.justia.com/cases/federal/appellate-courts/ca9/18-15982/18-15982-2019-08-08.html. [2562, 9 September].

จากข้อเท็จจริง (FashionID) ซึ่งเป็นผู้ประกอบการค้าปลีกออนไลน์จำหน่ายสินค้าประเภทเสื้อผ้าและเครื่องแต่งกายผ่านเว็บไซต์ของตนเอง (https: / / www. fashionid.de) โดยเว็บไซต์ดังกล่าวนี้ ได้มีการนำฟังก์ชั่นปุ่ม “Like” ของ Facebook มาใช้กับการทำการตลาดสินค้าของตนเพื่อให้ผู้เข้ามาซื้อสินค้าสามารถแสดงความเห็นต่อสินค้าและแชร์สินค้าดังกล่าวไปยัง (Facebook) ของตนเองได้โดยฟังก์ชั่นของปุ่ม “Like” ดังกล่าวจะส่งข้อมูลของผู้เข้าใช้ (www. Fashionid.de) ทั้งหมดไปยัง (Facebook) โดยอัตโนมัติไม่ว่าผู้เข้าใช้รายดังกล่าวจะได้กดปุ่ม “Like” หรือไม่ก็ตาม หรือแม้แต่ไม่ได้เข้าสู่ระบบของ (Facebook) ด้วยก็ตาม นั้นย่อมหมายความว่าการประมวลผลและการส่งข้อมูลส่วนบุคคลจะเกิดขึ้นทันทีที่เข้าได้ไปหน้าเว็บที่มีการใช้ฟังก์ชั่นปุ่ม “Like” เมื่อพิจารณาถึงการกระทำของประกอบการดังกล่าว ได้แสดงให้เห็นว่าผู้ประกอบการมิได้มีการขอความยินยอมจากเจ้าของข้อมูลก่อนที่จะกดปุ่ม “Like” ดังกล่าว[215]

3.3.4 มาตรการข้อมูลไบโอเมตริกซ์ (Biometrics)

กฎหมาย (Illinois: BIPA) ได้มีประกาศที่เข้มงวดมากที่สุดและข้อกำหนดการยินยอมขององค์กรเอกชนที่จะสามารถรวบรวมข้อมูลไบโอเมตริกซ์ได้จะต้องแจ้งเรื่องเป็นลายลักษณ์อักษรว่ามีการรวบรวม หรือจัดเก็บข้อมูลไบโอเมตริกซ์และระบุวัตถุประสงค์และระยะเวลาในการรวบรวมจัดเก็บและใช้ข้อมูล ซึ่งจะต้องได้รับการเซ็นสัญญาเป็นลายลักษณ์อักษรตาม 740 ILCS 14/5 (b) (1) - (3) (West) แต่รัฐเท็กซัส BIS ก็ยังคงต้องประกาศและได้การยินยอม แต่ไม่จำเป็นต้องได้รับความยินยอมเป็นลายลักษณ์อักษรก่อนรวบรวมข้อมูลไบโอเมตริกซ์ตาม Wash. Rev. Code Ann. §19.375.020 (1) (West) แต่กฎหมาย Washington BI นั้น ค่อนข้างเข้าใจยากในการแจ้งเตือนและการยินยอม โดยเฉพาะอย่างยิ่งจะต้องพิจารณาความเหมาะสมของการแจ้งเตือนก่อนใน “การลงทะเบียน” ของข้อมูลไบโอเมตริกซ์ เพื่อป้องกันการใช้ข้อมูลไบโอเมตริกซ์เพื่อวัตถุประสงค์เชิงพาณิชย์ในภายหลัง ซึ่งกฎหมาย (Illinois: BIPA Texas: BIS และ Washington: BI) โดยมีลักษณะทั่วไปคล้ายคลึงกันในลักษณ์ 6 ประการดังนี้[216]

ประการแรก การใช้กับหน่วยงานเอกชน แต่ไม่ใช่หน่วยงานของรัฐ หรือหน่วยงานท้องถิ่น

ประการที่สอง ต้องมีการแจ้งให้ทราบก่อนที่จะมีการรวบรวมข้อมูลไบโอเมตริกซ์

ประการที่สาม ห้าม การขาย และการเปิดเผยข้อมูลไบโอเมตริกซ์

---

[215] Makena Kelly. (Jul 24, 2019). ***FTC hits Facebook with $5 billion fine and new privacy checks***. (Online). Available: https://www.theverge.com/2019/7/24/20707013/ftc-facebook-settlement-data-cambridge-analytica-penalty-privacy-punishment-5-billion. [2562, 9 September]

[216] jacksonlewis. (2017). ***Article Illinois Biometric Information Privacy Act: FAQs***. Vol. 2

ประการท่สี่ ต้องมรมาตรการดูแลที่เหมาะสมเพื่อปกป้องข้อมูลไบโอเมตริกซ์

ประการที่ห้า ห้ามการเก็บรักษาข้อมูลไบโอเมตริกซ์ไว้เพื่อวัตถุประสงค์ในการรวบรวม

ประการสุดท้าย ต้องทำลายข้อมูลไบโอเมตริกซ์เมื่อหมดวัตถุประสงค์

ประเด็นที่หนึ่ง จำกัดความของข้อมูลส่วนบุคคลตามพระราชบัญญัติ (Privacy Act) ให้คำนิยามไว้ใน 5 U.S.C.§ 552 a (a) (4)[217] ว่า “บันทึก” หมายถึง สิ่งใด ๆ ที่ข้อมูลนั้นเกี่ยวกับบุคคลโดยการเก็บ รวบรวม การเก็บรักษา ใช้ หรือเปิดเผย รวมไปถึงการศึกษา ธุรกรรมการเงิน ประวัติการรักษาพยาบาล ประวัติอาชญากรรม ประวัติการทำงาน ชื่อของบุคคล หรือเลขบัตรประจำตัวประชาชน สัญลักษณ์ หรือบ่งชี้สิ่งอื่นใดที่สามารถระบุตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ หรือลายพิมพ์เสียง หรือรูปภาพ ซึ่งคำจำกัดความนี้ บ่งชี้ว่าสิ่งอื่นใดสามารถระบุตัวบุคคลนั้นได้

อันเป็นการแสดงให้เห็นได้ว่ารวมถึงการใช้เทคโนโลยีไบโอเมตริกซ์นั้นด้วย ซึ่งมิได้มีการแยกข้อมูลที่อ่อนไหวออกจากข้อมูลทั่วไป แต่อย่างไรก็ตาม พระราชบัญญัติข้อมูลความเป็นส่วนตัวทางชีวมาตร (BIPA) ของรัฐอิลลินอยส์ ได้บัญญัติคำนิยามศัพท์ “ข้อมูลไบโอเมตริกซ์” โดยจำแนกต่างหากจาก ข้อมูลส่วนบุคคลทั่วไป โดยระบุไว้ในหมวดหมู่ “ข้อมูลที่มีความอ่อนไหว” เป็นข้อมูลใด ๆ ก็ตามโดยไม่คำนึกวิธีการใดที่อ้างอิงจากลักษณ์ของบุคคลนั้นได้ เว้นแต่ ข้อมูลที่ได้จากการรวบรวม หรือ ขั้นตอนที่ได้ยกเว้นภายใต้คำจำกัดความ โดยมิได้บัญญัติ “ข้อมูลพันธุกรรม” ไว้ในหมวดหมู่ข้อมูลที่มีความอ่อนไหว แต่ได้บัญญัติไว้ในหมวด “การระบุตัวบุคคลทางชีวมาตร” (Biometrics identifier) ซึ่งเกิดจากผลทางเทคนิคตามพระราชบัญญัติทางกายวิภาคของรัฐอิลลินอยส์ อันแสดงให้เห็นว่าเป็นข้อมูลที่อ่อนไหวที่ได้รับการคุ้มครองไว้กรณีพิเศษตามพระราชบัญญัติของรัฐอิลลินอยส์

ประเด็นที่สอง หลักการความยินยอม (Consent) และการถอนความยินยอมของข้อมูลไบโอเมตริกซ์ (Biometrics) ในการเปิดเผยข้อมูลส่วนบุคคล (Privacy Act) ห้ามมิให้หน่วยงานของรัฐที่มีข้อมูลส่วนบุคคลเปิดเผยข้อมูลส่วนบุคคลนั้น เว้นแต่ จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือ เว้นแต่บทบัญญัติยกเว้นให้กระทำได้ โดย (Privacy Act) กำหนดให้หน่วยงานของรัฐที่มีหน้าที่ดูแลระบบการบันทึกต้องยินยอมให้เจ้าของข้อมูลส่วนบุคคลเข้าถึงข้อมูลส่วนบุคคลของตน โดยเจ้าของข้อมูลส่วนบุคคลสามารถที่จะตรวจสอบความถูกต้องและขอสำเนาข้อมูลส่วนบุคคลของตนได้ และหน่วยงานของรัฐจะต้องพิจารณาและตอบรับคำขอของเจ้าของข้อมูลส่วนบุคคลภายใน 30 วันทำการ หากหน่วยงานของรัฐปฏิเสธคำขอดังกล่าว หน่วยงานของรัฐต้องแจ้งเหตุผลในการปฏิเสธ และแจ้งหน่วยงานที่เจ้าของข้อมูลส่วนบุคคลสามารถอุทธรณ์คำสั่งได้

---

[217] Privacy Act 1974.

พระราชบัญญัติข้อมูลความเป็นส่วนตัวทางชีวมาตร (BIPA) ได้บัญญัติให้ความยินยอมต้องแจ้งตั้งแต่ครั้งแรกเป็นลายลักษณ์อักษรเกี่ยวกับการเก็บ รักษา เปิดเผย ใช้ การลบ การทำลายข้อมูลไบโอเมตริกซ์อย่างถาวรเมื่อไม่ประสงค์และไม่สามารถรับข้อมูลดังกล่าวได้[218] เว้นแต่จะมีการแจ้งดังนี้

แจ้งเรื่องการรวบรวม แจ้งเรื่องข้อมูลที่ประสงค์เฉพาะสำหรับการรวบรวมและระยะเวลาที่ข้อมูลจะถูกเก็บไว้ และได้รับความยินยอมเป็นลายลักษณ์อักษร ตั้งแต่ครั้งได้รับข้อมูลแจ้งการถอนเป็นลายลักษณ์อักษรก่อนให้ความยินยอม

การยินยอมโดยมิได้แจ้งล่วงหน้าเป็นลายลักษณ์อักษณและมิได้รับความยินยอมเป็นลายลักษณ์อักษรล่วงหน้า หากมีการละเมิดอันเป็นการเพียงพอที่จะนำคดีขึ้นสู่ศาล แม้ว่าเจ้าของข้อมูลจะไม่ได้รับอันตรายจากการที่ไม่แจ้งความยินยอมดังกล่าวนั้น

ประเด็นที่สาม มาตรการในการบังคับใช้กฎหมายโดยเฉพาะอย่างยิ่งระยะเวลาในการเก็บรักษาข้อมูลซึ่งจะเป็นไปตามหลัก (Right to be forgotten) การแจ้งระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล โดย (Privacy Act 1994) กำหนดให้หน่วยงานของรัฐต้องทำรายงานข้อมูลส่วนบุคคลเกี่ยวกับวัน เวลา ของข้อมูลบุคคลที่ได้รับการเปิดเผยข้อมูลเกี่ยวกับการติดต่อของบุคคล หรือที่องค์กรได้รับข้อมูลส่วนบุคคลนั้น โดยจะต้องเก็บรายงานดังกล่าวไว้เป็นเวลา 5 ปี หรือตลอดอายุของบันทึก และกฎหมาย (BIPA) ของรัฐอิลลินอยส์ยังได้กำหนดให้ผู้ประกอบธุรกิจที่มีข้อมูลไบโอเมตริกซ์อยู่ในความครอบครองมีนโยบายเป็นลายลักษณ์อักษรต้องเปิดเผยต่อสาธารณชน โดยกำหนดตารางเวลาการเก็บรักษาและแนวทางสำหรับการทำลายข้อมูลไบโอเมตริกซ์ นโยบายจะต้องกำหนดให้มีการทำลายข้อมูลไบโอเมตริกซ์มีนโยบายเป็นตารางทำเป็นลายลักษณ์อักษรภายใน 3 ปี Section 740 ILCS 14/15 หากระยะเวลาใดยาวกว่าให้ถือเอาระยะเวลานั้นก่อน (Texas: BIS) มีระยะเวลาทำลายหนึ่งปีแทนที่จะเป็นสามปี แต่ไม่จำเป็นต้องมีนโยบายเป็นลายลักษณ์อักษรที่เปิดเผยต่อสาธารณะ

พระราชบัญญัติข้อมูลความเป็นส่วนตัวทางชีวมาตร (Biometric Information Privacy Act 2008: BIPA) โดยกำหนดให้องค์กรเอกชนที่ครอบครองข้อมูลไบโอเมตริกซ์ ในการเก็บรักษา รวบรวม เปิดเผย การทำลาย จะต้องมีนโยบายเป็นลายลักษณ์อักษรโดยทำตารางการเก็บรักษาและแนวทางสำหรับทำลายข้อมูลอย่างถาวรเมื่อไม่ประสงค์ ดังนั้น จึงเห็นได้ว่า การเก็บรักษาข้อมูลไบโอเมตริกซ์จะต้องประกาศนโยบายและแจ้งตั้งแต่ครั้งแรกเป็นตารางสำหรับองค์กรเอกชน

---

[218] 740 ILCS 14/15 reads:

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

ประเด็นที่สี่ บทลงโทษเพื่อความมั่นคงปลอดภัยของข้อมูลไบโอเมตริกซ์ (Biometrics) โดยกำหนดให้ข้อมูลไบโอเมตริกซ์ เป็นข้อมูลที่ถูกสร้างขึ้นโดยวิธีการอัตโนมัติของลักษณะทางชีวมาตรของแต่ละบุคคล และข้อจำกัดเฉพาะข้อมูลไบโอเมตริกซ์ที่ได้รับการลงทะเบียน หรือลดรูปแบบในฐานข้อมูล ซึ่งถูกบัญญัติ ห้ามมิให้องค์กรเอกชนระบุตัวบุคคลในการลงทะเบียนด้วยระบบไบโอเมตริกซ์ในฐานข้อมูล โดยไม่มีการแจ้งล่วงหน้าให้ทราบก่อนและให้ความยินยอม ห้ามขาย ให้เช่าซื้อ หรือเปิดเผยข้อมูลไบโอเมตริกซ์เพื่อวัตถุประสงค์ทางการค้า เว้นแต่จะมีคุณสมบัติตรงตามเกณฑ์ที่กำหนด โดยมีมาตรการกำหนดให้ประกาศนโยบายเกี่ยวกับการเก็บรักษาและการเข้าถึงข้อมูลไบโอเมตริกซ์เป็นตารางแก่เจ้าของข้อมูล (BIPA) ได้มีมาตรการในกำหนดโทษปรับมาจากสาเหตุของการกระทำโดยการละเมิดความเป็นส่วนตัวทางชีวมาตร ตามกฎหมายปรับมากกว่า 1,000 ดอลลาร์ ในความเสียหายที่ต้องจ่าย หรือความเสียหายที่เกิดขึ้นจริงสำหรับการละเมิดโดยประมาทตาม Section 5-202 โดยมุ่งเน้นโทษปรับมากกว่า 5,000 ดอลลาร์ สำหรับความเสียหาย หรือความเสียหายที่แท้จริง สำหรับการละเมิดโดยเจตนา หรือโดยประมาท และกฎหมายยังให้มีสิทธิผู้เสียหายเรียกค่าธรรมเนียมและค่าใช้จ่ายทนายความได้เองตามความเหมาะสมด้วย

ดังนั้น จะเห็นได้ว่า (BIPA) ได้กำหนดข้อมูลไบโอเมตริกซ์เป็น “ข้อมูลใด ๆ โดยไม่คำนึงถึงวิธีการที่ถูกบันทึก แปลง จัดเก็บ หรือแบ่งปันโดยอ้างอิงจากการระบุข้อมูลไบโอเมตริกซ์ของแต่ละบุคคลที่ใช้เพื่อระบุตัวบุคคลนั้นได้ ยกเว้นภายใต้คำจำกัดความของการระบุตัวบุคคลด้วยเทคโนโลยีไบโอเมตริกซ์”[219] โดยกฎหมายข้อมูลไบโอเมตริกซ์ของมลรัฐสหรัฐอเมริกา ได้มีการบทบัญญัติห้ามมิให้เอกชนกระทำการลงทะเบียนระบุตัวบุคคลด้วยระบบไบโอเมตริกซ์ไว้ในฐานข้อมูล โดยมิได้การแจ้งให้ทราบตั้งแต่แรกและให้ความยินยอมรวมทั้งการแจ้งผลกระทบของการถอนความยินยอม และห้ามขาย ให้เช่าซื้อ หรือเปิดเผยข้อมูลไบโอเมตริกซ์ เพื่อวัตถุประสงค์ทางการค้า เว้นแต่จะมีคุณสมบัติตรงตามที่บทบัญญัติได้กำหนดไว้ในกฎหมาย อันเกี่ยวกับข้อกำหนดในการเก็บรักษาและการเข้าถึงการระบุอัตลักษณ์ของบุคคลด้วยระบบไบโอเมตริกซ์ แต่อย่างไรก็ตาม การเก็บรวบรวมข้อมูลไบโอเมตริกซ์จากผู้ป่วย หรือการดูแลสุขภาพต้องอยู่ภายใต้พระราชบัญญัติการประกันสุขภาพและความรับผิดชอบของรัฐบาลกลาง (The Health Insurance Portability and Accountability Act of 1996: HIPAA) ซึ่งได้รับการยกเว้นจากกฎระเบียบกฎหมายของรัฐอิลลินอยส์และวอชิงตัน สาระสำคัญของพระราชบัญญัติฉบับนี้จะกำหนดให้ “องค์กรเอกชน” ใด ๆ ก็ตามต้องกระทำตามบทบัญญัติ (BIPA) ฉบับนี้ เช่น

---

[219] Ron Hedges. (2018). ***How Collecting Biometric Information Can Lead to Litigation***. (Online). Available: https://journal.ahima.org/2018/06/27/how-collecting-biometric-information-can-lead-to-litigation/. [2562, 9 September].

การแจ้งให้บุคคลผู้เป็นเจ้าของข้อมูลทราบก่อนรวบรวมข้อมูลไบโอเมตริกซ์ของบุคคลนั้น ว่าข้อมูลชีวมาตรดังกล่าวจะถูกรวบรวมและการแจ้งให้บุคคลนั้นทราบถึงวัตถุประสงค์เฉพาะ และการแจ้งระยะเวลาที่ข้อมูลชีวมาตรได้ถูกรวบรวม ใช้ จัดเก็บและการลบ

การขอความยินยอมเป็นลายลักษณ์อักษรจากบุคคลนั้น ก่อนการรวบรวมข้อมูลไบโอเมตริกซ์ของบุคคลดังกล่าว และการถอนคำยินยอมอย่างอิสระโดยต้องแจ้งผลกระทบของการถอนคำยินยอมนั้น

การจัดทำนโยบายการเก็บรักษาข้อมูลให้เป็นลายลักษณ์อักษรไว้โดยเฉพาะสำหรับข้อมูลไบโอเมตริกซ์จะต้องกำหนดตารางการเก็บข้อมูลและแนวทางสำหรับการลบข้อมูลไบโอเมตริกซ์อย่างถาวร เมื่อไม่วัตถุประสงค์ในการรวบรวมข้อมูลไบโอเมตริกซ์ให้เป็นที่พึงพอใจ หรือภายในสามปี หรือแล้วแต่จำนวนใดจะถึงก่อนตามพระราชบัญญัติฉบับนี้ แต่กรณี (Texas: BIS) มีระยะเวลาในการลบข้อมูลภายใน 1 ปี แทนที่จะเป็นระยะเวลา 3 ปี และไม่จำเป็นต้องมีนโยบายเป็นลายลักษณ์อักษรในการเปิดเผยต่อสาธารณะ ซึ่ง (BIPA) กำหนดให้องค์กรเอกชนห้ามบันทึกข้อมูลไบโอเมตริกซ์ไว้ในฐานข้อมูล ได้แก่ บริษัท หุ้นส่วน บริษัทรับผิดจำกัด สมาคม หรือกลุ่มองค์กรอื่น ๆ แต่ไม่รวมถึงหน่วยงานของรัฐ หรือหน่วยงานท้องถิ่นใด ๆ

ประเด็นปัญหา จากพระราชบัญญัติ (BIPA) เนื่องจากประเด็นในการตีความไว้หลายประการเกี่ยวกับพระราชบัญญัติ (BIPA) จากกรณีคดี Rosenbach v. Six Flags Entertainment Corp. โดยยังคงไม่มีความชัดเจนของคำจำกัดความ คำว่า “การประมาท” หรือ “เจตนา” ขององค์กรเอกชนที่ถูกกล่าวหาว่าเป็นการเปิดเผยข้อมูลส่วนบุคคลเป็นการเพียงพอหรือไม่อย่างไร[220] ในทางปฏิบัติจริงได้กระทำการละเมิดตามข้อกำหนดของพระราชบัญญัติ (BIPA) หรือไม่ว่าจะเป็นการยินยอมโดยพฤตินัยหรือไม่ อันเป็นการป้องกันข้อมูลไบโอเมตริกซ์ที่ถูกต้อง (โดยเฉพาะอย่างยิ่งตามสัญญาการจ้างงาน) ซึ่งเป็นสิ่งที่ถือว่าข้อมูลส่วนบุคคลอยู่ในความ “ครอบครอง” ว่าเป็นข้อมูลไบโอเมตริกซ์และสิ่งที่ถือว่าเป็น “ข้อมูลไบโอเมตริกซ์” ว่าอะไรบ้างเป็นการกระทำโดย “ประมาท หรือเจตนา” หากข้อมูลไบโอเมตริกซ์ของลูกจ้าง ก็ยังมิได้มีการบัญญัติคำจำกัดความดังกล่าวไว้เช่นเดียวกัน เพียงบัญญัติไว้กว้าง ๆ เท่านั้นเอง

โดยบทบัญญัติในการดำเนินคดีที่เกิดขึ้นในรัฐอิลลินอยส์และรัฐอื่น ๆในการรวบรวมจัดเก็บข้อมูลไบโอเมตริกซ์ หรือใช้ในการละเมิด (BIPA) ดูเหมือนจะอยู่ในช่วงเริ่มต้นและศาลจะแบ่งการละเมิด (BIPA) เพียงแค่จะให้ทราบถึงการรับรู้ว่าจะได้รับอันตรายจากการรวบรวม

---

[220] Tae Kim – Edited by Anita Liu. (2019).***Rosenbach v. Six Flags: Illinois Supreme Court Interprets Illinois Biometric Privacy Law***. (Online). Available: https://jolt.law.harvard.edu/digest/rosenbach-v-six-flags-illinois-supreme-court-interprets-illinois-biometric-privacy-law. [2562, 28 November]

การจัดเก็บข้อมูลไบโอเมตริกซ์ หรือใช้ และการดำเนินคดีที่เกิดขึ้น โดยมาตรการในการลงโทษสำหรับผู้ที่กระทำละเมิดตามความรุนแรงซึ่งการมุ่งแน้นโทษปรับมากกว่า อันเป็นเรื่องเตือนสำหรับผู้ให้บริการและผู้ให้บริการในหลาย ๆ ด้าน รวมทั้งการดูแลสุขภาพด้วย ซึ่งได้มีการเก็บรวบรวม การจัดเก็บและการใช้ข้อมูลไบโอเมตริกซ์ใด ๆ ซึ่งข้อมูลไบโอเมตริกซ์อาจมีประโยชน์อย่างยิ่ง แต่อย่างไรก็ตาม การพึ่งพาข้อมูลไบโอเมตริกซ์จึงจะต้องคำนึงถึงข้อกำหนดของกฎหมายและการควบคุมของรัฐสหรัฐอเมริกาด้วย

3.4 มาตรการทางกฎหมายไบโอเมตริกซ์ (Biometrics) สหพันธ์สาธารณรัฐเยอรมนี

กฎหมายของประเทศสหพันธ์สาธารณรัฐเยอรมนีจะต้องอยู่ภายใต้การใช้บังคับตามหลักการของกฎระเบียบแห่งสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลโดยทั่วไป คริสตศักราช 2016 ซึ่งเป็นกฎเกณฑ์ระหว่างประเทศเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ใช้บังคับในกลุ่มประเทศสมาชิกสหภาพยุโรปแล้ว ในระดับกฎหมายภายในประเทศสหพันธ์สาธารณรัฐเยอรมนีมีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในลักษณะของกฎหมายกลาง หรือกฎหมายทั่วไป (Comprehensive Law) สำหรับข้อมูลส่วนบุคคลได้รับการรับรองและให้การคุ้มครองตามกฎหมายเป็นการทั่วไป หมายถึง กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล คริสตศักราช 2009 (Bundesdatenschutzgesetz: BDSG)[221] ซึ่งมีวัตถุประสงค์เพื่อคุ้มครองการประมวลผล หรือใช้ข้อมูลส่วนบุคคลสำหรับหน่วยงานของรัฐในระดับสหพันธรัฐและองค์กรของเอกชนและบทบัญญัติใหม่กำหนดข้อจำกัดเพิ่มเติมเกี่ยวกับนายจ้างในการละเมิด หรือการใช้ข้อมูลโดยไม่ได้ตั้งใจจะต้องรายงานให้พนักงานทราบ โดยเฉพาะกฎพิเศษสำหรับการเฝ้าระวังข้อมูลวิดีโอ ข้อมูลไบโอเมตริกซ์และข้อมูลการสื่อสารโทรคมนาคม

นอกจากนี้ เมื่อวันที่ 5 กรกฎาคม 2017 พระราชบัญญัติคุ้มครองข้อมูลของประเทศสหพันธ์สาธารณรัฐเยอรมนี (Bundesdatenschutzgesetz : BDSG)[222] ได้รับการเผยแพร่อย่างเป็นทางการใน (Federal Gazette: BDSG) แทนที่พระราชบัญญัติคุ้มครองข้อมูลของรัฐบาลกลางเยอรมนี (BDSG) และได้ยกเลิกการใช้ (BDSG) ฉบับก่อนหน้าในวันเดียวกัน โดยมีวัตถุประสงค์เพื่อปรับกรอบกฎหมายเยอรมนีให้เป็นกฎระเบียบว่าด้วยการป้องกันข้อมูลทั่วไปของยุโรป (GDPR) ใหม่ทั้งสองฉบับ (BDSG) ใหม่และ (GDPR) ให้เป็นกฎหมายที่มีประสิทธิภาพมากขึ้น ในวันที่

---

[221] Loin n° 78-17 ***du 6 Janvier 1978 relative à l 'in formatique, aux fichiersetaux liberties Article 8 (ii) Article 68***.

[222] Viola Bensinger Carsten Kociok. (2017). ***New German Federal Data Protection Act Officially Published***. (Online). Available: https://www.gtlaw.com/en/insights/2017/7/new-german-federal-data-protection-act-officially-published. [2562, 9 September].

25 พฤษภาคม 2018 บทบัญญัติใหม่ที่สำคัญของ (BDSG) มีวัตถุประสงค์เพิ่มขึ้นเพื่อการป้องกันข้อมูลส่วนบุคคล สำหรับในการประมวลผลข้อมูล การเก็บรวบรวม การใช้ข้อมูลและการประเมินข้อมูลโดยองค์กรสาธารณะและหน่วยงานราชการ (BDSG) นั้นได้รับการรับรองโดยกฎหมายของรัฐ เพื่อวัตถุประสงค์ในทางธุรกิจ การใช้ประโยชน์จากข้อมูลส่วนบุคคลดังกล่าวทำได้เฉพาะเมื่อกฎหมายกำหนด หรือบทบัญญัติของกฎหมายอื่นอนุญาตให้กระทำได้ หรือเท่าที่บุคคลผู้เป็นเจ้าของข้อมูลนั้นได้ให้ความยินยอม ในกรณีได้มีการขอยินยอมแล้วจะต้องแจ้งถึงวัตถุประสงค์ของการจัดเก็บข้อมูลนั้นด้วยตาม มาตรา 51 (2)[223]

3.4.1 พระราชบัญญัติการคุ้มครองข้อมูลของรัฐบาลกลาง (Federal Data Protection Act 2018: BDSG)

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (BDSG) ได้ให้คำจำกัดความไว้ดังนี้

“ข้อมูลส่วนบุคคล” (Personal Data) ตามมาตรา 46 (1)[224] หมายถึง ข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัว หรืออาจระบุตัวตนได้ กล่าวคือ บุคคลที่สามารถระบุตัวตนได้ทั้งทางตรงและทางอ้อมโดยเฉพาะอย่างยิ่งการอ้างอิงถึงสิ่งบ่งชี้ตัวตนของบุคคลนั้นได้ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลสถานที่ตั้ง ระบบออนไลน์ หรืออย่างหนึ่งอย่างใด หรือหลายอย่างที่เฉพาะเจาะจง ในลักษณะทางกายสรีรวิทยา อัตลักษณ์ทางพันธุกรรม เศรษฐกิจ ความคิดวัฒนธรรม หรือสังคมของบุคคลนั้น

“การประมวลผล” (Processing)[225] หมายถึง การดำเนินการใด ๆ ของข้อมูลส่วนบุคคลไม่ว่าจะด้วยวิธีอัตโนมัติ เช่น การเก็บ การรวบรวม การบันทึกการปรับ การเปลี่ยนแปลง ขององค์กร

---

[223] Federal Data Protection Act (BDSG) Section 51Consent reads:

(2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

[224] Federal Data Protection Act (BDSG) Section 46 Definitions reads:

1.‘personal data’ means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

[225] Federal Data Protection Act (BDSG) Section 46 Definitions reads:

2. ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization,

การปรับ การให้คำปรึกษา การใช้ การเปิดเผย โดยการส่ง การเผยแพร่ หรือการทำให้พร้อมใช้งาน การจัดตำแหน่ง การรวบรวม การจำกัด การลบ หรือทำลาย

“ระบบการจัดเก็บข้อมูล” (Filing System)[226] หมายถึง ชุดข้อมูลส่วนบุคคลที่สามารถเข้าถึงได้ในการเก็บ รวบรวม หรือเปิดเผยตามอำนาจหน้าที่ตามกฎหมาย

“ผู้ควบคุม” (Controller) หมายถึง บุคคลธรรมดา หรือหน่วนงานรัฐ หรือหน่วยงานอื่นใด หรือวิธีการตามวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย [227]

“การละเมิดข้อมูลส่วนบุคคล” (Personal data breach) หมายถึง การเข้าถึงข้อมูลส่วนบุคคลในการเก็บ รวบรวม ใช้ เปิดเผย การทำลาย การแก้ไข โดยไม่ได้รับอนุญาต หรือการเข้าถึงข้อมูลส่วนบุคคลโดยผิดกฎหมาย[228]

“ข้อมูลทางพันธุกรรม” (Genetic data)หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับลักษณะทางพันธุกรรมที่สืบทอดมาของบุคคล ซึ่งข้อมูลเฉพาะเกี่ยวกับสรีรวิทยา หรือสุขภาพของบุคคลนั้น โดยเฉพาะอย่างยิ่งการวิเคราะห์ตัวชีวมาตร[229]

---

structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction;

[226] Federal Data Protection Act (BDSG) Section 46 Definitions reads:

6.‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

[227] Federal Data Protection Act (BDSG) Section 46 Definitions reads:

7.‘controller’ means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;

[228] Federal Data Protection Act (BDSG) Section 46 Definitions reads:

10.‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data processed;

[229] Federal Data Protection Act (BDSG) Section 46 Definitions reads:

11. ‘genetic data’ means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

“ข้อมูลไบโอเมตริกซ์” (Biometric data) หมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิคเฉพาะที่เกี่ยวข้องกับลักษณะทางกายภาพ สรีรวิทยา หรือพฤติกรรมของบุคคลในการระบุเอกลักษณ์ของบุคคลนั้นโดยเฉพาะภาพใบหน้า หรือข้อมูลลายนิ้วมือ (Dactyloscopic)[230]

“ข้อมูลสุขภาพ”(Data concerning)[231] หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการเปิดเผยข้อมูลสุขภาพทางร่างกาย หรือจิตใจของบุคคลรวมถึงการให้บริการด้านการดูแลสุขภาพของบุคคล

“ข้อมูลส่วนบุคคลประเภทพิเศษ” (Special categories of personal data)[232] หมายถึง ข้อมูลที่เปิดเผยถึงเชื้อชาติ หรือเผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา หรือ ปรัชญา หรือการเป็นสมาชิกสหภาพแรงงาน ข้อมูลทางพันธุกรรม ข้อมูลไบโอเมตริกซ์ในการระบุถึงเอกลักษณ์ข้อมูลเกี่ยวกับสุขภาพ และข้อมูลเกี่ยวกับชีวิต หรือรสนิยมทางเพศของบุคคล

“ความยินยอม” (Consent)[233] หมายถึง สิ่งบ่งชี้ใด ๆ ที่ได้รับแจ้งโดยเฉพาะเจาะจงและชัดเจนไม่คลุมเครือตามวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับผู้ให้ความยินยอมนั้น

---

[230] Federal Data Protection Act (BDSG) Section 46 Definitions reads:

12.‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, in particular facial images or dactyloscopic data;

[231] Federal Data Protection Act (BDSG) Section 46 Definitions reads:

13.‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

[232] Federal Data Protection Act (BDSG) Section 46 Definitions reads:

14. ‘special categories of personal data’

a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;

b) genetic data;

c) biometric data for the purpose of uniquely identifying a natural person;

d) data concerning health; and

e) data concerning a natural person’s sex life or sexual orientation;

[233] Federal Data Protection Act (BDSG) Section 46 Definitions reads:

17. ‘consent’ means any freely given, specific, informed and unambiguous indication of the data subject's wishes in a particular case by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

โดยกฎหมายของ (BDSG) ในการประมวลผลข้อมูลส่วนบุคคลทั้งหมด หรือบางส่วนด้วยวิธีการอัตโนมัติและการประมวลผลอื่น ๆ นอกเหนือจากวิธีการอัตโนมัติของข้อมูลส่วนบุคคลที่เป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูล หรือมีวัตถุประสงค์เพื่อความเป็นส่วนตัวในการจัดเก็บข้อมูลของบุคคลนั้น หรือภายในประเทศ ตามหมวดส่วนที่ 1 (1) ของ (BDSG)[234]

การคุ้มครองข้อมูลไบโอเมตริกซ์ของ (BDSG) สำหรับการเก็บ รวบรวมข้อมูลที่ละเอียดอ่อนเป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคลรวมถึงข้อมูลของพนักงานที่มีความสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ ตาม Section 46 ถือว่า “การประมวลผลข้อมูลพันธุกรรมข้อมูลไบโอเมตริกซ์ เพื่อจุดประสงค์ในการระบุตัวตนของบุคคลที่เป็นเอกลักษณ์” ซึ่งเป็นสิ่งจะต้องได้รับอนุญาต เมื่อมีความจำเป็นอย่างยิ่งสำหรับการปฏิบัติงานของผู้ควบคุมเท่านั้น เว้นแต่จะเป็นข้อยกเว้นตามกฎหมายที่กำหนดไว้เฉพาะตามมาตรา Section 22 ต้องเป็นไปตามกฎของ (EU) 2016/679 ดังต่อไปนี้

การประมวลผลของข้อมูลส่วนบุคคลชนิดพิเศษก่อให้เกิดความเสียหายเกิดขึ้นตาม มาตรา 9 (1) ของกฎระเบียบ (EU) 2016/679 จะได้รับอนุญาตก่อน[235]

---

[234] Federal Data Protection Act (BDSG) Section 46 Definitions reads:

Section 1 Scope of the Act

(1) This Act shall apply to the processing of personal data by

1. public bodies of the Federation,

2. public bodies of the Länder, where data protection is not governed by Land law and where they

a) carry out federal law or

b) act in the capacity of judicial bodies in matters other than administrative matters.

For private bodies, this Act shall apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system unless such processing is conducted by natural persons in the course of a purely personal or domestic activity.

[235] Federal Data Protection Act (BDSG) Section 22 reads:

Processing of special categories of personal data

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted

1. by public and private bodies if

a) processing is necessary to exercise the rights derived from the right of social security and social protection and to meet the related obligations;

โดยหน่วยงานภาครัฐและเอกชน

a. ความจำเป็นในการใช้สิทธิที่ได้รับจากประกันสังคมและการคุ้มครองทางสังคมเกี่ยวข้องกับสัญญาการจ้างงาน

b. เพื่อความจำเป็นของวัตถุประสงค์ในการใช้ยาป้องกันเพื่อการวินิจฉัยทางการแพทย์ การให้บริการด้านสุขภาพ หรือการดูแลสังคม หรือการรักษา หรือการจัดการระบบและบริการด้านสุขภาพ หรือเรื่องของข้อมูลกับผู้เชี่ยวชาญด้านสุขภาพและหากข้อมูลเหล่านี้ถูกประมวลผลโดยผู้เชี่ยวชาญด้านสุขภาพ หรือบุคคลอื่นที่อยู่ภายใต้ภาระหน้าที่ของการรักษาความลับ หรือภายใต้การดูแลขององค์กรนั้น ๆ

c. ความจำเป็นเพื่อประโยชน์สาธารณะในด้านสาธารณสุข เช่น การป้องกันภัยคุกคามข้ามพรมแดนที่รุนแรงต่อสุขภาพ หรือการสร้างมาตรฐานคุณภาพและความปลอดภัยสูงของการดูแลสุขภาพและผลิตภัณฑ์ยาหรืออุปกรณ์ทางการแพทย์ นอกเหนือจากมาตรการที่อ้างถึงในส่วนที่ 2 ไว้โดยเฉพาะในการประกอบอาชีพที่เป็นความผิดทางอาญา เพื่อให้มั่นใจว่ามีการปฏิบัติตามหน้าที่อันเป็นความลับทางวิชาชีพ

---

b) processing is necessary for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to the data subject's contract with a health professional and if these data are processed by health professionals or other persons subject to the obligation of professional secrecy or under their supervision; or

c) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; in addition to the measures referred to in subsection 2, in particular occupational and criminal law provisions to ensure professional secrecy shall be complied with;

2. by public bodies if

a) processing is urgently necessary for reasons of substantial public interest;

b) processing is necessary to prevent a substantial threat to public security;

c) processing is urgently necessary to prevent substantial harm to the common good or to safeguard substantial concerns of the common good; or

d) processing is necessary for urgent reasons of de fence or to fulfil supra- or intergovernmental obligations of a public body of the Federation in the field of crisis management or conflict prevention or for humanitarian measures; and as far as the interests of the controller in data processing in the cases of no. 2 outweigh the interests of the data subject.

โดยองค์กรสาธารณะ

a. การประมวลผลมีความจำเป็นเร่งด่วนเพื่อเหตุผลที่เป็นประโยชน์สาธารณะ

b. การประมวลผลเป็นสิ่งจำเป็นเพื่อป้องกันภัยคุกคามต่อความมั่นคงสาธารณะ

c. การประมวลผลมีความจำเป็นเร่งด่วนในการป้องกันอันตรายที่อาจเกิดขึ้นกับสินค้าทั่วไป หรือ เพื่อป้องกันสินค้าที่สำคัญ หรือ

d. ความจำเป็นเร่งด่วนในการป้องกัน หรือเพื่อปฏิบัติตามข้อผูกพันระหว่างรัฐบาล หรือประชาชนของสหพันธรัฐที่เกิดวิกฤตการณ์ หรือการป้องกันความขัดแย้ง หรือการประมวลผลข้อมูลส่วนบุคคลด้านมนุษยธรรม

ในกรณีเพื่อมาตรการที่เหมาะสมโดยเฉพาะเจาะจงเพื่อปกป้องผลประโยชน์เรื่องของข้อมูลจะต้องคำนึงถึงวิธีการดำเนินการและลักษณะสิ่งแวดล้อมเพื่อวัตถุประสงค์ของการประมวลผลตลอดจนโอกาสเกิดความเสี่ยงและความรุนแรงที่แตกต่างเพื่อสิทธิและเสรีภาพของบุคคลนั้น โดยคำนึงถึงมาตรการดังต่อไปนี้[236]

---

[236] Federal Data Protection Act (BDSG) Section 22 reads:

Processing of special categories of personal data

(2) In the cases of subsection 1, appropriate and specific measures shall be taken to safeguard the interests of the data subject. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:

1. technical organizational measures to ensure that processing complies with Regulation (EU) 2016/679;

2. measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;

3. measures to increase awareness of staff involved in processing operations;

4. designation of a data protection officer;

5. restrictions on access to personal data within the controller and by processors;

6. the pseudonymization of personal data;

7. the encryption of personal data;

8. measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;

9. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;

มาตรการทางเทคนิคขององค์กรเพื่อให้แน่ใจว่าการประมวลผลเป็นไปตามกฎระเบียบของ (EU) 2016/679

มาตรการในการกำหนดความถูกต้องของข้อมูลส่วนบุคคล หรือแก้ไข หรือลบออกและสามารถเข้าตรวจสอบได้ในภายหลัง

มาตรการที่เกี่ยวข้องกับข้อมูลของพนักงานเพื่อเพิ่มความตระหนักในการดำเนินการ การกำหนดเจ้าหน้าที่คุ้มครองข้อมูล ข้อจำกัดในการเข้าถึงข้อมูลส่วนบุคคลของผู้ควบคุมและระบบประมวลผล การปลอมแปลงข้อมูลส่วนบุคคล การเข้ารหัสข้อมูลส่วนบุคคล

มาตรการของระบบการประมวลผลข้อมูลส่วนบุคคลและการบริการ ในกรณีที่เกิดเหตุการณ์ทางเทคนิค หรือทางกายภาพ เพื่อให้มั่นใจว่าสามารถการเข้าถึงและพร้อมใช้งานอย่างรวดเร็วและความยืดหยุ่นรวมถึงความลับของข้อมูลและความสามารถในการกู้คืนข้อมูล

มาตรการสำหรับการทดสอบการประเมินประสิทธิภาพของทางเทคนิคและองค์กรอย่างสม่ำเสมอเพื่อรับรองความปลอดภัยของการประมวลผล

กฎระเบียบเฉพาะเพื่อให้สอดคล้องกับพระราชบัญญัติฉบับนี้และตามกฎระเบียบของ (EU) 2016/679 ในกรณีที่มีการถ่ายโอน หรือประมวลผลเพื่อวัตถุประสงค์อื่น

ดังนั้น การคุ้มครองข้อมูลส่วนบุคคลในการจัดเก็บ หรือการประมวลผลข้อมูลส่วนบุคคลหรือผู้ใช้อุปกรณ์เพื่อการประมวลผลอัตโนมัติจะต้องมีมาตรการในการเข้าถึง ข้อจำกัด วิธีการทำงานของอุปกรณ์ ประเภทของข้อมูลส่วนบุคคลที่ถูกประมวลผลและในกรณีที่ต้องกระทำที่เกิดการสูญหาย หรือถูกทำลายข้อมูลส่วนบุคคล รวมถึงต้องแจ้งให้ทราบถึงสิทธิที่จะเข้าข้อมูลแก่เจ้าของข้อมูลทราบ อันเป็นมาตรการป้องกันตาม (BDSG)

สิทธิเจ้าของข้อมูลส่วนบุคคลตามคำนิยามไว้ใน (BDSG) และสิทธิในการควบคุมผู้ประมวลข้อข้อมูลดังต่อไปนี้

---

10. specific rules of procedure to ensure compliance with this Act and with Regulation (EU) 2016/679 in the event of transfer or processing for other purposes.

การประมวลผลข้อมูลส่วนบุคคลของพนักงานตาม Section 26 (BDSG) ใหม่ ในการรักษากฎตามพระราชบัญญัติคุ้มครองข้อมูลของรัฐบาลกลางเยอรมันฉบับนี้[237]

[237] Federal Data Protection Act (BDSG) Section 26 reads: Data processing for employment-related purposes

(1) Personal data of employees may be processed for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise or satisfy rights and obligations of employees' representation laid down by law or by collective agreements or other agreements between the employer and staff council. Employees' personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason.

(2) If personal data of employees are processed on the basis of consent, then the employee's level of dependence in the employment relationship and the circumstances under which consent was given shall be taken into account in assessing whether such consent was freely given. Consent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests. Consent shall be given in written form, unless a different form is appropriate because of special circumstances. The employer shall inform the employee in text form of the purpose of data processing and of the employee's right to withdraw consent pursuant to Article 7 (3) of Regulation (EU) 2016/679.

(3) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 for employment-related purposes shall be permitted if it is necessary to exercise rights or comply with legal obligations derived from lab our law, social security and social protection law, and there is no reason to believe that the data subject has an overriding legitimate interest in not processing the data. Subsection 2 shall also apply to consent to the processing of special categories of personal data; consent must explicitly refer to these data. Section 22 (2) shall apply accordingly.

(4) The processing of personal data, including special categories of personal data of employees for employment-related purposes, shall be permitted on the basis of collective agreements. The negotiating partners shall comply with Article 88 (2) of Regulation (EU) 2016/679.

(5) The controller must take appropriate measures to ensure compliance in particular with the principles for processing personal data described in Article 5 of Regulation (EU) 2016/679.

(6) The rights of participation of staff councils shall remain unaffected.

(7) Subsections 1 to 6 shall also apply when personal data, including special categories of personal data, of employees are processed without forming or being intended to form part of a filing system.

ข้อมูลส่วนบุคคลของพนักงานสามารถถูกประมวลผลเพื่อวัตถุประสงค์ในดำเนินการการจัดตั้ง หรือยกเลิกสัญญาในการจ้างงาน หรือเพื่อวัตถุประสงค์ในการใช้สิทธิและปฏิบัติตามข้อผูกพันที่เกิดจากข้อตกลงของสหภาพในการทำงาน หรือตามกฎหมาย

การยินยอมและการถอนความยินยอมจะต้องทำเป็นลายลักษณ์อักษรต้องแจ้งผลกระทบการถอนก่อนให้ความยินยอมตาม Section 51(3)[238] เว้นแต่ความเหมาะสมนั้น เนื่องจากสถานการณ์

---

(8) For the purposes of this Act, employees are

1. dependently employed workers, including temporary workers contracted to the borrowing employer;

2. persons employed for occupational training purposes;

3. participants in benefits to take part in working life, in assessments of occupational aptitude or work trials (persons undergoing rehabilitation);

4. persons employed in accredited workshops for persons with disabilities;

5. volunteers working pursuant to the Youth Volunteer Service Act or the Federal Volunteer Service Act;

6. persons who should be regarded as equivalent to dependently employed workers because of their economic dependence; these include persons working at home and their equivalents;

7. federal civil servants, federal judges, military personnel and persons in the alternative civilian service.

Applicants for employment and persons whose employment has been terminated shall be regarded as employees.

[238] Federal Data Protection Act (BDSG) Section 51 reads:

Consent (1) If personal data may be processed by law on the basis of consent, the controller must be able to present evidence of the data subject's consent.

(2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

(3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The data subject shall be informed of this before giving consent.

(4) Consent shall be effective only when based on the data subject's free decision. When assessing whether consent was freely given, the circumstances in which it was given must be taken into account. The data subject shall be informed of the intended purpose of the processing. If necessary, in the individual case or on request, the data subject shall also be informed of the consequences of withholding consent.

(5) If special categories of personal data are to be processed, the consent must explicitly refer to these data.

พิเศษ นายจ้างจะต้องแจ้งให้พนักงานทราบตามรูปแบบ เพื่อวัตถุประสงค์ในการประมวลผลข้อมูลและสิทธิ์ของพนักงานในการเพิกถอนความยินยอมตามมาตรา 7 (3) ของระเบียบ (EU) 2016/679

การประมวลผลของข้อมูลส่วนบุคคลชนิดพิเศษตาม มาตรา 9 (1) ของกฎระเบียบ (EU) 2016/679 สำหรับวัตถุประสงค์ที่เกี่ยวข้องกับสัญญาการจ้างงานลักษณะความยินยอมจะต้องคำนึงถึงความถูกต้องและความสมัครใจ โดยพิจารณาจากความสัมพันธ์ในการจ้างงานตามกฎหมายแรงงาน หรือ กฎหมายประกันสังคม เช่น หากพนักงานได้รับผลประโยชน์จากการให้ความยินยอม หรือ ผลประโยชน์ฝ่ายเดียว เพื่อนำไปใช้กับความยินยอมในการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษ ความยินยอมจะต้องอ้างถึงข้อมูลที่ชัดเจนตามข้อบังคับไว้ในมาตรา 22 (2)

กรณีการประมวลผลข้อมูลส่วนบุคคลของพนักงานให้รวมถึงข้อมูลที่ “ละเอียดอ่อน” อาจได้รับอนุญาตอยู่บนพื้นฐานของข้อตกลงของการเจรจาต่อรองจะต้องปฏิบัติตามข้อบังคับตามมาตรา 88 (2) ของกฎระเบียบ (EU) 2016/679

การประมวลผลข้อมูลส่วนบุคคลที่ละเอียดอ่อนของ (BDSG) ใหม่ ซึ่งเป็นกฎหมายพื้นฐานสำหรับการประมวลผลของข้อมูลที่ “อ่อนไหว”

เพื่อวัตถุประสงค์ในการวิจัยทางวิทยาศาสตร์ หรือประวัติศาสตร์หรือเพื่อวัตถุประสงค์ทางสถิติ หากการประมวลผลมีความจำเป็นและมากกว่าผลประโยชน์ของผู้ควบคุมการประมวลผลข้อมูลนั้นมีความสำคัญมากกว่าเรื่องที่ไม่ใช่การประมวลผลข้อมูล

การประมวลผลข้อมูลของข้อมูลที่ “ละเอียดอ่อน” ซึ่งจำเป็นต่อการใช้สิทธิที่เกิดขึ้นจากการใช้สิทธิในการประกันสังคมและการคุ้มครองทางสังคม

การตรวจสอบ (Monitoring) การเฝ้าระวังวิดีโอ (Surveillance) BDSG ใหม่ ซึ่งมีกฎเกณฑ์เฉพาะเกี่ยวกับการเฝ้าระวังวิดีโอในพื้นที่ที่สาธารณชนเข้าถึงได้ตาม Section 4[239]

---

[239] Federal Data Protection Act (BDSG) Section 4 Video surveillance of publicly accessible spaces reads:

(1) Monitoring publicly accessible areas with optical-electronic devices (video surveillance) shall be permitted only as far as it is necessary

1. for public bodies to perform their tasks,

2. to exercise the right to determine who shall be allowed or denied access or

3. to safeguard legitimate interests for specifically defined purposes and if there is nothing to indicate legitimate overriding interests of the data subjects. For video surveillance of

1. large publicly accessible facilities, such as sport facilities, places of gathering and entertainment, shopping centres and car parks, or

2. vehicles and large publicly accessible facilities of public rail, ship or bus transport,

protecting the lives, health and freedom of persons present shall be regarded as a very important interest.

ขอบเขต (Scope) การใช้งานที่กว้างขึ้นของข้อผูกพันในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer: DPO) ตาม Sec. 38 (BDSG) บริษัททุกแห่งที่จ้างพนักงานมากกว่า 10 คน ในการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติจะต้องแต่งตั้งจาก (DPO)[240]

สถานะ (Status) การละเมิดข้อมูลส่วนบุคคล (BDSG) มีมาตรการเยียวยาความเสียหาย ให้แก่เจ้าของข้อมูลส่วนบุคคลสามารถเรียกร้องค่าเสียหายทางแพ่งโดยตรง ส่วนโทษทางปกครอง ได้บัญญัติให้พิจารณาตามสัดส่วนของการกระทำผิดโดยกำหนดโทษมากกว่าผลประโยชน์ที่ได้รับ และโทษทางอาญาในการดำเนินคดีเพื่อตามมาตรา 83 (4) ถึง (6) ของกฎระเบียบ (EU) 2016/679 มาตรา 17 มาตรา 35 และมาตรา 36 ที่ระบุไว้ใน (GDPR) ใหม่และ(BDSG) ใหม่ รวมถึงค่าปรับสูง ถึง 100,000 ยูโรสำหรับการละเมิดข้อมูลส่วนบุคคลในด้านเครดิตของผู้บริโภคตามมาตรา 41

โทษทางอาญาที่มีโทษจำคุกไม่เกิน 3 ปี หรือค่าปรับทางอาญาในกรณีที่มีการประมวลผล ข้อมูลส่วนบุคคลที่ผิดกฎหมายโดยเจตนาตาม Sec. 42 (BDSG)[241]

---

(2) Appropriate measures shall be taken to make the surveillance and the controller's name and contact details identifiable as early as possible.

(3) Storing or using data collected pursuant to subsection 1 shall be permitted if necessary, to achieve the intended purpose and if there is nothing to indicate legitimate overriding interests of the data subjects. Subsection 1, second sentence, shall apply accordingly. The data may be further processed for another purpose only if necessary, to prevent threats to state and public security and to prosecute crimes.

(4) If data collected from video surveillance are attributed to a particular person, that person shall be informed of the processing in accordance with Articles 13 and 14 of Regulation (EU) 2016/679. Section 32 shall apply accordingly.

(5) The data shall be deleted without delay, if they are no longer needed for the intended purpose or if the data subject's legitimate interests stand in the way of any further storage.

[240] Federal Data Protection Act (BDSG) Section 39 Accreditation reads:

The power to act as a certification body in accordance with Article 43 (1), first sentence of Regulation (EU) 2016/679 shall be granted by the supervisory authority of the Federation or the Länder responsible for data protection supervision of the certification body on the basis of accreditation by the German accreditation body. Section 2 (3), second sentence, Section 4 (3) and Section 10 (1), first sentence, no. 3 of the Accreditation Body Act shall apply on the condition that data protection falls within the scope of Section 1 (2), second sentence.

[241] Federal Data Protection Act (BDSG) Section 42 Penal provisions reads:

(1) The following actions done deliberately and without authorization with regard to the personal data of a large number of people which are not publicly accessible shall be punishable with imprisonment of up to three years or a fine:

การจำกัดสิทธิ์ของผู้ควบคุมข้อมูลส่วนบุคคลให้เป็นไปตามกฎเกณฑ์ในการประกอบธุรกิจ มาตรา 32 ถึง มาตรา 35

สิทธิเจ้าของข้อมูลจะต้องได้รับการแจ้งจากผู้ควบคุม หากผู้ควบคุมต้องการประมวลผลข้อมูลส่วนบุคคลเพิ่มเติมเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่เก็บข้อมูลส่วนบุคคล (มาตรา 13 GDPR) ซึ่งอาจถูกจำกัด หากข้อมูลถูกจัดเก็บเป็นการเปรียบเทียบ หรือการประมวลผลเพิ่มเติมเข้ากับวัตถุประสงค์เดิมและการสื่อสารเกี่ยวกับเรื่องข้อมูลไม่ได้เกิดขึ้นแบบดิจิทัล

ภาระหน้าที่ในการให้ข้อมูลในส่วนของผู้ควบคุมข้อมูลอาจถูกจำกัด ในกรณีของภาระหน้าที่ต้องการรักษาความลับ เช่น ความลับในวิชาชีพ

สิทธิการเข้าถึงข้อมูลของผู้ควบคุมตามมา ตรา 15 GDPR) อาจถูกจำกัด หากข้อมูลส่วนบุคคลถูกเก็บไว้ตามระยะเวลา หรือการเก็บรักษาตามกำหนดของกฎหมายเท่านั้น

สิทธิในการร้องขอให้ทำการลบและแก้ไข เนื่องจากการจัดเก็บบางประเภทที่ไม่เป็นข้อมูลปัจจุบัน หรือหมดวัตถุประสงค์ต้องทำการลบทันทีตาม (Sec. 35 BDSG)[242]

---

1. transferring the data to a third party or

2. otherwise making them accessible

for commercial purposes.

(2) The following actions done with regard to personal data which are not publicly accessible shall be punishable with imprisonment of up to two years or a fine:

1. processing without authorization, or

2. fraudulently acquiring

and doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

(3) Such offences shall be prosecuted only if a complaint is filed. The data subject, the controller, the Federal Commissioner and the supervisory authority shall be entitled to file complaints.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in criminal proceedings against the person required to provide a notification or a communication or relatives as referred to in Section 52 (1) of the Code of Criminal Procedure only with the consent of the person required to provide a notification or a communication.

[242] Federal Data Protection Act (BDSG) Section 35 Right to erasure reads:

(1) If in the case of non-automated data processing erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage and if the data subject's interest in erasure can be regarded as minimal, the data subject shall not have the right to erasure and the controller shall not be obligated to erase personal data in accordance with Article 17 (1) of Regulation (EU) 2016/679 in addition to the

กฎหมาย (BDSG) กำหนดให้บริษัทส่วนใหญ่เปลี่ยนโปรแกรม และการปฏิบัติตามนโยบายความเป็นส่วนตัวของข้อมูลส่วนบุคคลที่มีอยู่ ตัวอย่างเช่น การออกกฎหมายจำกัดผลประโยชน์ของข้อตกลงของสหภาพแรงงานของลูกจ้างเป็นเหตุผลสำหรับการใช้ข้อมูลและมีแนวโน้มที่บริษัทจะต้องทบทวนและอาจเจรจาใหม่ ข้อตกลงใหม่ในการสร้างเกณฑ์สำหรับการใช้ข้อมูลส่วนบุคคลเป็นเรื่องการละเมิด หรือการใช้ข้อมูลโดยไม่ได้ตั้งใจจะต้องรายงานให้พนักงานทราบโดยไม่คำนึงถึงความเสียหาย นายจ้างที่ละเมิดข้อกำหนดของ (BDSG)

สำหรับค่าปรับทางปกครองในการกระทำความผิดทางปกครองอาจถูกปรับได้มากถึงห้าหมื่นยูโร ตาม Section 43 (2) ต่อการละเมิดข้อมูลส่วนบุคคล และพนักงานจะสามารถเรียกร้องค่าเสียหายจากการละเมิดที่ถูกกล่าวหาได้และสหภาพแรงงานสามารถยื่นคำร้องเพื่อขอคำสั่งศาลได้ และเพื่อให้สอดคล้องกับของรัฐสภายุโรปเกี่ยวกับการคุ้มครองบุคคลธรรมดาที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล โดยบทบัญญัติความผิดทางปกครองจะใช้บังคับต่อการละเมิดตามมาตรา 83 (4) ถึง (6) กฎ (EU) 2016/679 มาตรา 17 มาตรา 35 และ มาตรา 36[243] สำหรับโทษทางอาญาที่เป็นการกระทำโดยจงใจและไม่ได้รับอนุญาตเกี่ยวกับข้อมูลส่วนบุคคลที่ไม่สามารถเข้าถึงได้จะถูกลงโทษจำคุกไม่เกินสามปี หรือปรับตาม Section 42[244] จะต้องมีการแจ้งเตือนเมื่อเกิดเหตุข้อมูล

---

exceptions given in Article 17 (3) of Regulation (EU) 2016/679. In this case, restriction of processing in accordance with Article 18 of Regulation (EU) 2016/679 shall apply in place of erasure. The first and second sentences shall not apply if the personal data were processed unlawfully.

(2) In addition to Article 18 (1) (b) and (c) of Regulation (EU) 2016/679, subsection 1, first and second sentences shall apply accordingly in the case of Article 17 (1) (a) and (d) of Regulation (EU) 2016/679 as long and as far as the controller has reason to believe that erasure would adversely affect legitimate interests of the data subject. The controller shall inform the data subject of the restriction of processing if doing so is not impossible or would not involve a disproportionate effort.

(3) In addition to Article 17 (3) (b) of Regulation (EU) 2016/679, subsection 1 shall apply accordingly in the case of Article 17 (1) (a) of Regulation (EU) 2016/679 if erasure would conflict with retention periods set by statute or contract.

[243] Section 41 reads:

(1) Unless this Act provides otherwise, the provisions of the Administrative Offences Act shall apply accordingly to violations pursuant to Article 83 (4) to (6) of Regulation (EU) 2016/679. Sections 17, 35 and 36 of the Administrative Offences Act shall not apply. Section 68 of the Administrative Offences Act shall apply on the condition that the regional court shall decide if the administrative fine exceeds the amount of one hundred thousand euros.

[244] Section 42 Penal provisions reads:

รั่วหากพบว่าข้อมูลรั่วไหล หน่วยงานควบคุมข้อมูล และผู้ประมวลผลข้อมูลต้องแจ้งให้หน่วยงานกำกับดูแล และประชาชนทราบภายใน 72 ชั่วโมงตาม Section 65(1)[245]

3.4.2 มาตรการข้อมูลไบโอเมตริกซ์ (Biometrics)

พระราชบัญญัติการปกป้องข้อมูลของรัฐบาลกลางใหม่ (BDSG) ซึ่งเป็นการบังคับใช้กฎเกณฑ์ของระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป[246] อันมีประเด็นสำคัญซึ่งผู้วิจัยศึกษาดังนี้

---

(1) The following actions done deliberately and without authorization with regard to the personal data of a large number of people which are not publicly accessible shall be punishable with imprisonment of up to three years or a fine:

1. transferring the data to a third party or

2. otherwise making them accessible

for commercial purposes.

(2) The following actions done with regard to personal data which are not publicly accessible shall be punishable with imprisonment of up to two years or a fine:

1. processing without authorization, or

2. fraudulently acquiring

and doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

(3) Such offences shall be prosecuted only if a complaint is filed. The data subject, the controller, the Federal Commissioner and the supervisory authority shall be entitled to file complaints.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in criminal proceedings against the person required to provide a notification or a communication or relatives as referred to in Section 52 (1) of the Code of Criminal Procedure only with the consent of the person required to provide a notification or a communication.

[245] Federal Data Protection Act (BDSG) Section 65 reads:

(1) In the case of a personal data breach, the controller shall notify the Federal Commissioner without delay and, if possible, not later than 72 hours after having become aware of it, of the personal data breach, unless the personal data breach is unlikely to result in a risk to the legally protected interests of natural persons. If the Federal Commissioner is not notified within 72 hours, the notification shall be accompanied by reasons for the delay.

[246] Jur. Christian L. Geminn. (JUNE 2018). The New Federal Data Protection Act – Implementation of the GDPR in Germany. Senior researcher at Kassel University and Managing Director of the Project Group Constitutionally Compatible Technology Design (provet) at the Research Center for Information System Design (ITeG)

ประเด็นที่หนึ่ง คำจำกัดความข้อมูลส่วนบุคคลของ (BDSG) ตาม Sec. 46 (1) บัญญัติคำนิยาม คำว่า ข้อมูลใด ๆ ที่เกี่ยวกับบุคคลที่ระบุ หรือ สามารถระบุตัวตนของบุคคลได้ทั้งทางตรงและทางอ้อม โดยเฉพาะการอ้างอิงถึงสิ่งบ่งชี้ตัวตนของบุคคลนั้นได้ รวมทั้งลักษณ์ทางพันธุกรรมของบุคคลที่ถูกบัญญัติให้อยู่ในหมวดข้อมูลประเภททั่วไป แต่อย่างไรก็ตาม (BDSG) ได้มีการบัญญัติข้อมูลทางพันธุกรรม และข้อมูลไบโอเมตริกซ์ที่เป็นข้อมูลที่มีความอ่อนไหวง่าย อันเป็นข้อมูลที่เป็นเรื่องส่วนตัวโดยเฉพาะแท้จริง จึงได้ถูกบัญญัติให้แยกต่างหากจากข้อมูลส่วนบุคคลทั่วไป ตาม Sec. 46 (12) ของ (BDSG) ที่เกิดจากการประมวลผลทางเทคนิคในการยืนยันตัวตนของบุคคลที่เกี่ยวข้องกับลักษณ์ทางกายภาพที่สามารถบ่งชี้ถึงอัตลักษณ์ของแต่ละบุคคลออกจากบุคคลอื่น ซึ่งมีความสุ่มเสี่ยงสูงที่จะถูกละเมิด จึงถูกบัญญัติแยกให้การคุ้มครองในหมวดหมู่ประเภทข้อมูลพิเศษตาม Sec. 46 (14) ของ (BDSG) โดยการให้คำนิยามได้จำแนกประเภทของข้อมูลชัดเจนทำให้ง่ายต่อการจัดเก็บรวบรวมข้อมูลในแต่ละประเภท เพื่อปกป้องผลกระทบจากการจัดการข้อมูลส่วนบุคคลจากข้อเท็จจริงในทางปฏิบัติ

ประเด็นที่สอง หลักการความยินยอม (Consent) และการถอนความยินยอมของข้อมูลไบโอเมตริกซ์ ตาม Section 51 (3) ของ (BDSG) บัญญัติหลักการให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลจะต้องได้รับการแจ้งก่อนให้ความยินยอมไว้โดยเฉพาะเจาะจงชัดเจนและไม่คลุมเครือเป็นลายลักษณ์อักษรต้องเป็นไปตามวัตถุประสงค์ของเจ้าข้อมูลที่เกี่ยวข้องกับผู้ให้ความยินยอมนั้น ความยินยอมต้องเป็นอิสระ และสามารถเพิกถอนความยินยอมนั้นได้ ซึ่งจะต้องแจ้งผลกระทบในการถอนคำยินยอม “ก่อน” ล่วงหน้าที่จะให้ความยินยอมแก่เจ้าของข้อมูลทราบก่อน เว้นแต่ความยินยอมนั้น ได้ยกเว้นตามกฎหมายที่ได้กำหนไว้เช่นเดียวกับกฎระเบียบของ (EU)

ประเด็นที่สาม มาตรการในการบังคับใช้กฎหมายโดยเฉพาะอย่างยิ่งระยะเวลาในการเก็บ รักษาข้อมูลซึ่งจะเป็นไปตามหลัก (Right to be forgotten) การแจ้งระยะเวลาการเก็บรักษาข้อมูลไบโอเมตริกซ์ ซึ่งผู้ให้บริการในการประมวลผลข้อมูลส่วนบุคคลไม่ว่าทั้งหมด หรือบางส่วนด้วยวิธีการอัตโนมัติ ซึ่งเป็นข้อมูลพิเศษ หรือวิธีการประมวลผลแบบอื่น ๆ ของข้อมูลส่วนบุคคลก็เป็นส่วนหนึ่งของการจัดเก็บข้อมูลจะต้องได้รับอนุญาตจากเจ้าของข้อมูลทราบก่อน หากไม่มีการแจ้งระยะเวลาเก็บข้อมูลผู้ควบคุมต้องคำนึงถึงภายในระยะเวลาที่เหมาะสมแต่ไม่เกิน 2 สัปดาห์ ตาม Section 32 (3) หากมีการประมวลผลข้อมูลส่วนบุคคลเพิ่มเติม นอกเหนือจากที่เก็บข้อมูลไว้หรือข้อมูลถูกเปรียบเทียบเข้ากับวัตถุประสงค์เดิมผู้ควบคุมจะถูกกำจัดสิทธิ์ตาม (GDPR) โดยข้อมูลส่วนบุคคลจะถูกเก็บไว้ตามระยะเวลาของข้อตกลงที่เป็นไปตามวัตถุประสงค์ หรือสัญญา หรือการเก็บรักษาตามระยะของกฎหมายกำหนดไว้เท่านั้น

ประเด็นที่สี่ แนวทางในการแก้ไขปัญหาข้อมูลไบโอเมตริกซ์ (Biometrics) เพื่อให้เป็นไปตามบทบัญญัติของมาตรการลงโทษและความมั่นคงปลอดภัยของข้อมูลไบโอเมตริกซ์ที่มีความละเอียดอ่อนพิเศษของ (BDSG) จึงได้ดำเนินการด้วยความระมัดระวังเป็นกรณีพิเศษตามกฎหมาย (BDSG) ในการประมวลผลข้อมูลส่วนบุคคลที่จะต้องได้รับอนุญาตก่อนจากเจ้าของข้อมูล ผู้ควบคุมจะต้องใช้มาตรการทางเทคนิคและองค์กรที่จำเป็นเพื่อให้มั่นใจในระดับความปลอดภัยที่เหมาะสมกับความเสี่ยง เมื่อมีการประมวลผลข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษ เช่น ตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลที่รวบรวมเพื่อวัตถุประสงค์ที่แตกต่างกันสามารถประมวลผลแยกกันได้ ตาม Section 64

กรณีหากมีการละเมิดข้อมูลส่วนบุคคลได้กำหนดบทลงโทษสูงทั้งโทษทางอาญาและโทษทางปกครอง สำหรับการดำเนินคดีเพื่อกำหนดบทลงโทษปรับสูงถึง 100,000 ยูโร ตาม Section 41(1)[247] และโทษทางอาญาจำคุกไม่เกิน 2 ปี และสำหรับนายจ้างที่มีการละเมิดข้อมูลส่วนบุคคลของพนักงาน (BDSG) โทษปรับสูงถึง 500,000 ยูโร Section 43 (2) ต่อการละเมิดข้อมูลส่วนบุคคลและพนักงานจะสามารถเรียกร้องค่าเสียหายจากการละเมิดที่ถูกกล่าวหาได้และสหภาพแรงงานสามารถยื่นคำร้องเพื่อขอคำสั่งศาลได้ การแจ้งเตือนเมื่อพบว่าข้อมูลรั่วไหล หน่วยงานที่ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องแจ้งให้หน่วยงานกำกับดูแล และเจ้าของข้อมูลทราบภายใน 72 ชั่วโมงตาม Section 65 (1) ซึ่งมาตรการดังกล่าวอาจทำให้ผู้ควบคุม หรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องตระหนักในการที่จะต้องรับโทษและระมัดระวังในการประมวลผลข้อมูลส่วนบุคคลดังกล่าว

ดังนั้น สหพันธ์รัฐสาธารณรัฐเยอรมนี โดยมีการจำแนกประเภทของข้อมูลส่วนบุคคลและบัญญัติคำนิยามศัพท์ไว้อย่างชัดเจน โดยข้อมูลส่วนบุคคลประเภททั่วไป หมายความว่า “ข้อมูลส่วนบุคคล (Personal data)” ซึ่งเป็นข้อมูลที่เกี่ยวข้องกับบุคคล หรือรายละเอียดใด ๆ ที่สามารถระบุถึงตัวบุคคล (เจ้าของข้อมูล)ได้ ในส่วนคำว่า “ข้อมูลทางพันธุกรรม” แม้ว่าจะเป็นข้อมูลทั่วไป แต่ก็ยังได้จำแนกจากข้อมูลทั่วไปตาม Section 46 (11) รวมทั้ง ข้อมูลไบโอเมตริกซ์ที่เป็น“ข้อมูลส่วนบุคคลที่มีความอ่อนไหวง่าย (Sensitive data)” ซึ่งกฎหมายสหพันธ์รัฐสาธารณรัฐเยอรมนีบัญญัติคำนิยามศัพท์ไว้อย่างชัดเจนว่า “ข้อมูลส่วนบุคคลที่มีความอ่อนไหวง่ายต่อความรู้สึก (Special categories of personal data)” และถูกคุ้มครองในหมวดหมู่ข้อมูลประเภทพิเศษตาม Section 46 (14) นอกจากนี้ ยังได้มีการจำแนกประเภทของคำนิยามศัพท์ข้อมูลส่วนบุคคลดังกล่าวแล้ว ยังมีมาตรการทางกฎหมายที่ได้ให้รับการคุ้มครองข้อมูลส่วนบุคคลทั้งสองประเภทเกี่ยวกับข้อมูลส่วนบุคคลที่มี

---

[247] Federal Data Protection Act 2018: BDSG

ความอ่อนไหวอย่างเข้มงวดเป็นอย่างมาก เพื่อความแตกต่างกันให้ชัดเจนในการจำแนกประเภทไว้อย่างละเอียด

โดยพบว่า จากการให้ความยินยอมเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลประเภทที่ส่งผลกระทบต่อความรู้สึกตาม Section 46 ของ (Federal Data Protection Act 2018) โดยวางหลักมาตรการเกี่ยวกับข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนไว้ว่า “กรณีผู้ควบคุม หรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องขอความยินยอมจากผู้เป็นเจ้าของข้อมูลและต้องแจ้งให้ชัดเจนเป็นลายลักษณ์อักษรที่เกี่ยวข้องกับข้อมูลที่มีความละเอียดอ่อนก่อนให้ความยินยอม” เนื่องจากข้อมูลส่วนบุคคลอาจมีทั้งข้อมูลส่วนบุคคลทั่วไปและข้อมูลส่วนบุคคลที่มีความอ่อนไหวง่ายรวมอยู่ด้วยกันก็ได้โดยกฎหมายของสหพันธ์สาธารณรัฐเยอรมนีกำหนดให้ การขอความยินยอมเกี่ยวกับข้อมูลที่มีความละเอียดอ่อนดังกล่าวนี้ จะต้องได้รับการชี้แจงเป็นลายลักษณ์อักษรและแสดงให้เห็นชัดแจ้งถึงการขอความยินยอมในเรื่องนั้น ๆ แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อน

กฎหมายของ (BDSG) ใหม่นั้น ผู้วิจัยเห็นว่า มีความซับซ้อนและยากที่จะเข้าใจ เนื่องจากปัญหาสำคัญผลสืบเนื่องจากแนวโน้มการประมวลผลข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและข้อมูลของพนักงานซึ่งอาจมีทั้งข้อมูลทั่วไปและข้อมูลไบโอเมตริกซ์ที่มีความอ่อนไหวรวมกันอยู่ ในการกระทำเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลดังกล่าวจะมีสักกี่คนที่เข้าใจและนำไปใช้ถูกอย่างถูกต้อง หรือถึงแม้กระทั่งว่าการตรากฎหมายของสหพันธ์สาธารณรัฐเยอรมนีมีความสมบูรณ์แบบแล้ว แต่ในทางปฏิบัติรัฐบาลเยอรมนีก็ต้องการใช้ประโยชน์จากขอบเขตของการกระทำที่ได้รับจากข้อแตกต่างของข้อกฎหมายประเทศตนนั้นเท่าที่จะกระทำได้ในหน่วยงานคุ้มครองข้อมูลของสหพันธ์สาธารณรัฐเยอรมนีเอง อย่างไรก็ตาม (BDSG) ใหม่บัญญัติกฎหมายเกินขอบเขตที่ (GDPR) กำหนดไว้ ดังนั้นคณะกรรมาธิการสหภาพยุโรป อาจมีการเริ่มละเมิดต่อข้อมูลของสหพันธ์สาธารณรัฐเยอรมนีก็ได้ ยิ่งไปกว่านั้น กล่าวคือศาลและหน่วยงานของสหพันธ์สาธารณรัฐเยอรมนีจะต้องไม่ใช้บทบัญญัติของ (BDSG) หากเห็นว่าขัดกับกฎหมายของยุโรป สิ่งนี้อาจนำไปสู่ความไม่แน่นอนของกฎหมายภายในที่สำคัญตามมาก็ได้

3.5 มาตรการทางกฎหมายไบโอเมตริกซ์ (Biometrics) สาธารณรัฐสิงคโปร์

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ฉบับนี้ผ่านการพิจารณาจากรัฐสภาสิงคโปร์ตั้งแต่เมื่อวันที่ 15 ตุลาคม 2012 และประธานาธิบดีได้ลงนามเมื่อวันที่ 20 พฤศจิกายน ค. ศ. 2012 โดยได้มีการตีพิมพ์ประกาศทั่วไปเมื่อวันที่ 7 ธันวาคม 2012 ซึ่งกฎหมายฉบับนี้ชื่อ (Personal Data Protection Act 2012 No. 26 of 2012) มีทั้งหมด 68 มาตราและมีรายการท้ายกฎหมายอีก 9 เรื่อง ซึ่งกำหนดรายละเอียดเพิ่มเติมของเนื้อหาที่เกี่ยวข้องกับบางมาตราในกฎหมายรัฐบาลสิงคโปร์

ประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนตัว โดยมีเป้าหมายเพื่อคุ้มครองข้อมูลส่วนตัวของชาวสิงคโปร์ที่อาจถูกองค์กรต่าง ๆ นำไปใช้แสวงหาผลประโยชน์โดยไม่ได้รับอนุญาต กฎหมายดังกล่าวกำหนดให้องค์กรใด ๆ ก็ตาม ในสิงคโปร์ที่ต้องการเก็บรวบรวมข้อมูลส่วนตัวของประชาชนต้องได้รับการอนุมัติจากเจ้าของข้อมูลทราบเสียก่อน โดยหน่วยงานของรัฐมีวัตถุประสงค์เพื่อให้เกิดความน่าเชื่อถือระหว่างผู้บริโภคและภาคธุรกิจ อีกทั้งประชาชนยังมีสิทธิที่จะรับรู้ว่าองค์กรเหล่านั้นจะนำข้อมูลใดของข้อมูลส่วนบุคคลไปใช้เพื่อวัตถุประสงค์อะไร ข้อมูลใดจะได้รับการเปิดเผยและข้อมูลใดจะปิดไว้เป็นความลับ[248] นอกจากนี้ ยังมีวัตถุประสงค์เพื่อเสริมศักยภาพในการแข่งขันทางการค้าของประเทศสิงคโปร์และเพื่อให้ประเทศสิงคโปร์เป็นศูนย์กลางธุรกิจที่ได้รับความเชื่อถือระดับโลก

3.5.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act 2012: PDPA)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ซึ่งเป็นกฎหมายที่ใช้บังคับสำหรับการคุ้มครองข้อมูลส่วนบุคคลในประเทศสิงคโปร์ รวมถึงในขณะที่ข้อมูลส่วนบุคคลได้รับการถ่ายโอนระหว่างประเทศเพื่อการประมวลผล (PDPA) กำกับดูแลการรวบรวม การใช้งาน การเปิดเผยและการปกป้องข้อมูลส่วนบุคคล (PDPA) จะใช้กับข้อมูลส่วนบุคคลของบุคคลที่ให้ไว้สำหรับส่วนบุคคลเท่านั้นและไม่ใช้กับ “ข้อมูลติดต่อทางธุรกิจ” ที่กำหนดไว้ใน (PDPA) ในกรณี “ชื่อบุคคล ชื่อตำแหน่ง หรือหมายเลขโทรศัพท์ธุรกิจธุรกิจ ที่อยู่ ที่อยู่อีเมลธุรกิจหรือหมายเลขแฟกซ์ธุรกิจและข้อมูลอื่น ๆ ที่คล้ายคลึงกันเกี่ยวกับบุคคลนั้น ที่ไม่ได้กระทำเพื่อจุดประสงค์ส่วนบุคคล” องค์กรไม่จำเป็นต้องได้รับความยินยอม หรือปฏิบัติตาม (PDPA) ในการรวบรวมใช้ หรือเปิดเผยข้อมูลการติดต่อทางธุรกิจใด ๆ ที่เปิดเผยในการทำธุรกรรมเชิงพาณิชย์

โดยคณะกรรมการคุ้มครองข้อมูลส่วนตัวของประเทศสิงคโปร์ (The Personal Data Protection Commission) กฎหมายดังกล่าว ซึ่งช่วยให้องค์กรต่าง ๆ สามารถเก็บข้อมูลส่วนบุคคลจากประชาชนอย่างถูกกฎหมายและขณะเดียวกันประชาชนในสิงคโปร์ก็จะได้รับการคุ้มครองให้พ้นจากการละเมิดข้อมูลส่วนตัวใด ๆ ได้ด้วย อย่างไรก็ตาม กฎหมายดังกล่าวไม่ได้ครอบคลุมไปถึงภาคเอกชนในสิงคโปร์ เพราะมีกฎหมายเฉพาะในการควบคุมอยู่แล้วก่อนที่จะออกพระราชบัญญัติฉบับนี้ โดยกฎหมายฉบับนี้แบ่งเนื้อหาออกเป็นทั้งหมด 10 ส่วน[249]

---

[248] ศูนย์ข้อมูลข่าวสารอาเซียน กรมประชาสัมพันธ์. (2014). ***สิงคโปร์ประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนตัว***. (ออนไลน์). เข้าถึงได้จาก : http://www.aseanthai.net/ewt_news.php?nid=4145&filename=index_2. [2562, 12 กรกฎาคม]

[249] Personal data protection act 2012 (No. 26 of 2012)

กฎหมายฉบับนี้จะไม่ส่งผลกระทบต่อสิทธิพิเศษใด ๆ ที่บุคคลเคยได้รับอยู่แล้วรวมถึงกฎหมายอื่น ๆ หากขัดกับหลักการของกฎหมายฉบับนี้กฎหมายนั้นให้ถือว่ามีผลบังคับเหนือกว่ากฎหมายฉบับนี้

ข้อมูลส่วนบุคคลถูกกำหนดไว้ในพระราชบัญญัติ เพื่อให้การคุ้มครองข้อมูลไม่ว่าจะเป็นจริงหรือไม่เกี่ยวข้องกับบุคคล (ไม่ว่าจะมีชีวิตอยู่ หรือกรณีเพิ่งตาย)[250] ซึ่งสามารถระบุข้อมูลส่วนบุคคลได้ ข้อจำกัดเฉพาะการเปิดเผย และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งข้อมูลดังกล่าวเป็นเรื่องเกี่ยวกับบุคคลที่ถึงแก่กรรมสิบปี หรือน้อยกว่าและการปกป้องข้อมูลภายใต้พระราชบัญญัตินี้ ไม่บังคับใช้กับข้อมูลติดต่อทางธุรกิจ เช่น ชื่อ ชื่อตำแหน่ง หมายเลขโทรศัพท์ธุรกิจ ที่อยู่สถานที่ทำงาน ที่อยู่อีเมลธุรกิจ หมายเลขแฟกซ์ สถานที่ประกอบธุรกิจ อีกทั้ง ยังไม่บังคับใช้กับข้อมูลติดต่อเชิงธุรกิจ เว้นแต่ระบุไว้อย่างชัดแจ้ง

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลไม่ว่าจะเป็นจริง หรือไม่เกี่ยวกับบุคคลที่สามารถระบุได้มาจากข้อมูลที่ระบุตัวตนของบุคคลนั้น หรือจากข้อมูลบุคคลธรรมดาและข้อมูลอื่น ๆ ที่องค์กรมีหรือน่าจะเข้าถึงได้[251]

“การประมวลผล” หมายถึง ส่วนที่เกี่ยวกับข้อมูลส่วนบุคคลในการดำเนินการใด ๆ หรือชุดการดำเนินงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและรวมถึงการบันทึก หรือหน่วยงานที่แก้ไขเปลี่ยนแปลง มีไว้ในความครอบครอง ส่ง ลบ หรือทำลาย[252]

---

[250] Personal data protection act 2012 (No. 26 of 2012) reads:

Interpretation2. (1) In this Act, unless the context otherwise requires “individual” means a natural person, whether living or deceased;

[251] Personal data protection act 2012 (No. 26 of 2012) reads: Interpretation

2.(1) In this Act, unless the context otherwise requires

personal data” means data, whether true or not, about an individual who can be identified.

(a) from that data; or

(b) from that data and other information to which the organisation has or is likely to have access;

[252] Personal data protection act 2012 (No. 26 of 2012) reads: Interpretation

2.(1) In this Act, unless the context otherwise requires

processing”, in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:

(a) recording;

(b) holding;

(c) organisation, adaptation or alteration;

(d) retrieval;

“ธุรกิจ” รวมถึงกิจกรรมขององค์กรใด ๆ ไม่ว่าจะดำเนินการเพื่อวัตถุประสงค์ในการแสวงหาผลประโยชน์ หรือดำเนินการตามปกติซ้ำ ๆ หรือต่อเนื่อง แต่ไม่รวมถึงการกระทำของบุคคลธรรมดาที่กระทำโดยอาศัยความสามารถส่วนตัว[253]

“ข้อมูลติดต่อทางธุรกิจ” หมายถึง ชื่อบุคคล ตำแหน่ง หรือหมายเลขโทรศัพท์ที่ใช้ในทางธุรกิจที่อยู่ธุรกิจ หรือที่อยู่ในทางธุรกิจ หรืออีเมลธุรกิจ หรือหมายเลขแฟกซ์ใช้ในธุรกิจและข้อมูลอื่น ๆ ที่มีลักษณ์เช่นเดียวกันเกี่ยวกับบุคคล แต่ไม่ใช่เพื่อวัตถุประสงค์เป็นการส่วนตัว[254]

“รายงานเครดิต” หมายถึง การสื่อสารไม่ว่าจะเป็นลายลักษณ์อักษรวาจา หรือรูปแบบอื่นให้แก่องค์กรเพื่อประเมินความน่าเชื่อถือของบุคคลที่เกี่ยวข้องกับธุรกรรมระหว่างองค์กรและบุคคล[255]

“ตัวกลางข้อมูล” หมายถึง องค์กรที่ประมวลผลข้อมูลส่วนบุคคลในนามขององค์กรอื่นแต่ไม่รวมถึงพนักงานขององค์กรอื่นนั้น[256]

“เอกสาร” รวมถึงข้อมูลที่บันทึกในรูปแบบใด ๆ[257]

(e) combination;

(f) transmission;

(g) erasure or destruction;

[253] Personal data protection act 2012 (No. 26 of 2012) reads: Interpretation

2.(1) In this Act, unless the context otherwise requires

“Business” includes the activity of any organisation, whether or not carried on for purposes of gain, or conducted on a regular, repetitive or continuous basis, but does not include an individual acting in his personal or domestic capacity;

[254] Personal data protection act 2012 (No. 26 of 2012) Interpretation

2.(1) In this Act, unless the context otherwise requires

“business” contact information” means an individual’s name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes;

[255] Personal data protection act 2012 (No. 26 of 2012) reads: Interpretation

2.(1) In this Act, unless the context otherwise requires

credit report” means a communication, whether in written, oral or other form, provided to an organisation to assess the creditworthiness of an individual in relation to a transaction between the organisation and the individual

[256] Personal data protection act 2012 (No. 26 of 2012) reads: Interpretation

2.(1) In this Act, unless the context otherwise requires

data intermediary” means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation;

“การให้ความยินยอม” หมายถึง บุคคลไม่ได้รับความยินยอมภายใต้พระราชบัญญัตินี้สำหรับการรวบรวมใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับบุคคลโดยองค์กรเพื่อวัตถุประสงค์เว้นแต่ บุคคลให้ความยินยอม โดยบุคคลได้รับข้อมูลที่จำเป็นตาม มาตรา 20 หรือ เพื่อจุดประสงค์ทางธุรกิจตามพระราชบัญญัตินี้[258]

“การละเมิดข้อตกลง”[259] หรือการฝ่าฝืนกฎหมายที่เป็นลายลักษณ์อักษรใด ๆ หรือกฎของการประกอบวิชาชีพ หรือ ข้อกำหนดอื่น ๆ ที่ได้กำหนดโดยหน่วยงานกำกับดูแลใด ๆ ในการใช้อำนาจของตนภายใต้กฎหมายใด ๆ ที่เป็นลายลักษณ์อักษร หรือสถานการณ์ หรือความประพฤติที่อาจส่งผลให้มีการเยียวยา หรือบรรเทาทุกข์ภายใต้กฎหมายใด ๆ

“คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” หมายถึง หน่วยงานพัฒนาสื่อการสื่อสารข้อมูลได้รับมอบหมายให้เป็นคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่มีหน้าที่รับผิดชอบในการบริหารงานของพระราชบัญญัตินี้ องค์กรมีข้อจำกัดในการรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

---

[257] Personal data protection act 2012 (No. 26 of 2012) reads: Interpretation

2.(1) In this Act, unless the context otherwise requires

document” includes information recorded in any form;

[258] Personal data protection act 2012 (No. 26 of 2012) reads:

Part IV

Collection, use and disclosure of

Personal data

Provision of consent

14.(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless

(a) the individual has been provided with the information required under section 20; and

(b) the individual provided his consent for that purpose in accordance with this Act.

[259] Personal data protection act 2012 (No. 26 of 2012) reads: Interpretation

2.(1) In this Act, unless the context otherwise requires

“investigation” means an investigation relating to

(a) a breach of an agreement;

(b) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

(c) a circumstance or conduct that may result in a remedy or relief being available under any law;

เพื่อจุดประสงค์ที่บุคคลที่เหมาะสมจะพิจารณาความเหมาะสมในสถานการณ์และเพื่อวัตถุประสงค์ที่บุคคลนั้นยินยอม[260]

ในการเก็บรักษาข้อมูลส่วนบุคคลองค์กรต้องป้องกันข้อมูลส่วนบุคคลซึ่งอยู่ในความครอบครอง หรือความควบคุมขององค์กร โดยจัดให้มีการรักษาความปลอดภัยตามสมควร เพื่อป้องกันมิให้ข้อมูลส่วนบุคคลนั้นถูกเข้าถึงโดยไม่ได้รับอนุญาต แก้ไข ใช้ เปิดเผย คัดลอก เปลี่ยนแปลง ทำลายหรือความเสี่ยงอื่นที่มีลักษณะเช่นเดียวกันและในการเก็บรักษาข้อมูลส่วนบุคคลนั้น (PDPA) กำหนดให้องค์กรต้องไม่เก็บรักษาเอกสารซึ่งมีข้อมูลส่วนบุคคล หรือต้องลบวิธีการซึ่งข้อมูลส่วนบุคคลนั้นสามารถเชื่อมโยงไปยังตัวบุคคลนั้นได้ เมื่อมีกรณีดังต่อไปนี้[261]

กรณีแรก การเก็บรักษาข้อมูลส่วนบุคคลนั้น ไม่สามารถใช้เพื่อวัตถุประสงค์ซึ่งข้อมูลส่วนบุคคลนั้น ถูกเก็บรวบรวมอีกต่อไป

กรณีที่สอง การเก็บรักษาข้อมูลส่วนบุคคลนั้นไม่จำเป็นเพื่อวัตถุประสงค์ทางกฎหมาย หรือทางธุรกิจอีกต่อไปหลักการในบทบัญญัติของกฎหมาย (Personal Data Protection ACT 2012)

เพื่อให้การปฏิบัติตามกฎหมายฉบับนี้เกิดขึ้นได้อย่างเป็นรูปธรรมมาตรา 11 กำหนดให้แต่ละองค์กรจะต้องแต่งตั้งบุคคลขึ้นรับผิดชอบการปฏิบัติตามกฎหมายฉบับนี้และเปิดเผยข้อมูลติดต่อทางธุรกิจของบุคคลนั้น ๆ ให้สาธารณชนรับทราบมาตรา 12[262] กำหนดให้แต่ละองค์กรกำหนด

---

[260] Personal data protection act 2012 (No. 26 of 2012) Part II reads:

Personal data protection commission and administration

Personal Data Protection Commission

5. (1) The Info－ communications Media Development Authority is designated as the Personal Data Protection Commission.

(2) The Personal Data Protection Commission is responsible for the administration of this Act.

[261] Personal data protection act 2012 (No. 26 of 2012) reads: Retention of personal data

25. Part V

Care of Personal data

An organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that

(a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and

(b) retention is no longer necessary for legal or business purposes.

[262] Personal data protection act 2012 (No. 26 of 2012) reads: Policies and practices

12. An organisation shall

นโยบายและแนวปฏิบัติที่จำเป็นสำหรับการปฏิบัติตามกฎหมายฉบับนี้ สร้างช่องทางในการร้องเรียนที่เกี่ยวข้องรวมถึงประกาศให้สาธารณชนรับทราบทั้งนโยบายและช่องทางร้องเรียนและซักซ้อมความเข้าใจกับบุคลากรภายในองค์กร กฎหมายฉบับนี้ยังกำหนดหลักการอื่น ๆ ที่องค์กรจะต้องปฏิบัติตามเมื่อพิจารณารายละเอียดของข้อกฎหมายแล้วพบว่า ค่อนข้างกำหนดหน้าที่ของผู้ที่เกี่ยวข้องมีความชัดเจนและประนีประนอมต่อความจำเป็นในการใช้ข้อมูลโดยเฉพาะในเชิงธุรกิจค่อนข้างมาก โดยมีข้อยกเว้นของกฎต่าง ๆ อยู่หลายประการซึ่งอาจสร้างภาระให้กับองค์กรในการคุ้มครองข้อมูลส่วนบุคคลเฉพาะในส่วนที่จะส่งผลกระทบโดยตรงต่อเจ้าของข้อมูลหรือสิทธิของผู้ที่เกี่ยวข้องเท่านั้น

หลักความยินยอม (Consent) มาตรา 13[263] และ มาตรา 14[264] กำหนดให้แต่ละองค์กรเก็บใช้เปิดเผยข้อมูลส่วนบุคคลได้ ในกรณีที่มีการให้ความยินยอมโดยเจ้าของข้อมูลก่อนดำเนินการใด ๆ

(a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

(b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act;

(c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and

(d) make information available on request about

(i) the policies and practices referred to in paragraph (a); and

(ii) the complaint process referred to in paragraph (b).

[263] Personal data protection act 2012 (No. 26 of 2012) reads:

Collection, use and disclosure of person data

Division 1 Consent Consent required

13. An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless

(a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or

(b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law.

[264] Personal data protection act 2012 (No. 26 of 2012) Provision of consent reads:

14. (1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless

(a) the individual has been provided with the information required under section 20; and

และเจ้าของข้อมูลสามารถปฏิเสธ หรือยกเลิกความยินยอมได้ ซึ่งองค์กรไม่อาจกำหนดให้การให้ความยินยอมเป็นเงื่อนไข ในการขายสินค้าและบริการในระดับที่เกินกว่าความสมเหตุสมผลต่อการให้บริการนั้น (Beyond what is reasonable) องค์กรไม่สามารถขอความยินยอมโดยการปลอมแปลงข้อเท็จจริงความยินยอมที่ได้มาด้วยวิธีการดังกล่าวข้างต้นนั้น ไม่ถือเป็นความยินยอมที่มีผลใช้ได้ตามกฎหมายฉบับนี้ ความยินยอมนั้น อาจเป็นความยินยอมแบบโดยปริยายได้ แต่ต้องอยู่ในขอบเขตของมาตรา 15[265]

การถอนความยินเมื่อไม่มีความประสงค์ให้เก็บใช้และเปิดเผยข้อมูลส่วนบุคคล หรือดำเนินการใด ๆ อีกต่อไปต้องแจ้งให้ทราบแก่เจ้าของข้อมูลอาจถึงผลที่จะเกิดขึ้นจากการเพิกถอนความยินยอมใด ๆ[266]

(b) the individual provided his consent for that purpose in accordance with this Act.

(2) An organisation shall not

(a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual; or

(b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices.

(3) Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act.

(4) In this Act, references to consent given, or deemed to have been given, by an individual for the collection, use or disclosure of personal data about the individual shall include consent given, or deemed to have been given, by any person validly acting on behalf of that individual for the collection, use or disclosure of such personal data.

[265] Personal data protection act 2012 (No. 26 of 2012) reads: Deemed consent

15. (1) An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation for a purpose if

(a) the individual, without actually giving consent referred to in section 14, voluntarily provides the personal data to the organisation for that purpose; and

(b) it is reasonable that the individual would voluntarily provide the data.

(2) If an individual give, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation.

[266] Personal data protection act 2012 (No. 26 of 2012) reads: Withdrawal of consent

หลักวัตถุประสงค์ (Purpose) กำหนดให้เก็บใช้และเปิดเผยข้อมูลส่วนบุคคลได้ต่อเมื่อวัตถุประสงค์นั้นเหมาะสมกับสถานการณ์และเจ้าของข้อมูลได้รับแจ้งถึงวัตถุประสงค์ไว้ตามมาตรา 20[267]

การเข้าถึงและแก้ไขข้อมูล (Access and correction) มาตรา 21[268] กำหนดสิทธิของบุคคลในการเข้าถึงข้อมูลและวิธีการที่ข้อมูลถูกใช้และเปิดเผยออกไปภายในหนึ่งปีตั้งแต่ถูกร้องขอ เว้นแต่

---

16 (1) On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose.

(2) On receipt of the notice referred to in subsection (1), the organisation concerned shall inform the individual of the likely consequences of withdrawing his consent.

(3) An organisation shall not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section shall not affect any legal consequences arising from such withdrawal.

(4) Subject to section 25, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation shall cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless such collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or other written law.

[267] Personal data protection act 2012 (No. 26 of 2012) reads: Division 2 Purpose Notification of purpose

20. (1) For the purposes of sections 14(1) (a) and 18(b), an organisation shall inform the individual of

(a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data;

(b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and

(c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data.

[268] Personal data protection act 2012 (No. 26 of 2012) Part V access to and correction of Access to personal data reads:

21 (1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation shall, as soon as reasonably possible, provide the individual with

(a) personal data about the individual that is in the possession or under the control of the organisation; and

การเข้าถึงนั้นจะเป็นอันตรายต่อตัวเจ้าของข้อมูลเอง หรือกระทบสิทธิของผู้อื่นและมาตรา 22 กำหนดสิทธิของบุคคลในการร้องขอให้องค์กรแก้ไขข้อมูลของตนเองได้เว้นแต่จะมีเหตุผลอันสมควร

ความถูกต้องของข้อมูล (Accuracy) มาตรา 23[269] กำหนดให้องค์กรมีหน้าที่จัดการให้ข้อมูลส่วนบุคคลที่เก็บรักษาไว้มีความถูกต้องครบถ้วนถ้าหากข้อมูลนั้นอาจถูกใช้โดยหน่วยงานที่

(b) information about the ways in which the personal data referred to in paragraph (a) has been or may have been used or disclosed by the organisation within a year before the date of the request.

(2) An organisation is not required to provide an individual with the individual's personal data or other information under subsection (1) in respect of the matters specified in the Fifth Schedule.

(3) An organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information, as the case may be, could reasonably be expected to —

(a) threaten the safety or physical or mental health of an individual other than the individual who made the request;

(b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;

(c) reveal personal data about another individual;

(d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or

(e) be contrary to the national interest.

(4) An organisation shall not inform any individual under subsection (1) that it has disclosed personal data to a prescribed law enforcement agency if the disclosure was made without the consent of the individual pursuant to paragraph 1(f) or (n) of the Fourth Schedule or under any other written law.

(5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation shall provide the individual with access to the personal data and other information without the personal data or other information excluded under subsections (2), (3) and (4).

[269] Personal data protection act 2012 (No. 26 of 2012) Accuracy of personal data reads:

23. An organisation shall make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data

(a) is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or

(b) is likely to be disclosed by the organisation to another organisation.

จะตัดสินใจในประเด็นที่ส่งผลกระทบต่อตัวเจ้าของข้อมูลหรือผู้เกี่ยวข้องหรือในกรณีที่อาจต้องเปิดเผยข้อมูลของบุคคลนั้นให้องค์กรอื่น

การรักษาความปลอดภัยของข้อมูล (Security) มาตรา 24[270] กำหนดให้องค์กรมีหน้าที่ในการรักษาความปลอดภัยของข้อมูลที่อยู่ในความครอบครองแต่ไม่ได้มีการกำหนดมาตรการด้านความปลอดภัยไว้เป็นพิเศษจึงเป็นหน้าที่ขององค์กรเองที่ต้องจัดให้มีมาตรการในการรักษาความปลอดภัยที่เหมาะสมกับลักษณะและการใช้ข้อมูลนั้น ๆ มาตรา 25[271] กำหนดให้ทำลายข้อมูลเมื่อหมดความจำเป็นตามวัตถุประสงค์แล้วและการเก็บข้อมูล (Retention) นั้นไม่จำเป็นต่อวัตถุประสงค์เชิงกฎหมาย หรือธุรกิจอื่น ๆ อีก

การส่งข้อมูลไปต่างประเทศ (Transfer) มาตรา 26[272] ห้ามการส่งข้อมูลออกไปยังประเทศอื่นยกเว้นกรณีที่องค์กรผู้ดูแลข้อมูลสามารถพิสูจน์ได้ว่าประเทศอื่นที่มีการส่งออกข้อมูลนั้น

---

[270] Personal data protection act 2012 (No. 26 of 2012) Protection of personal data reads:

24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

[271] Personal data protection act 2012 (No. 26 of 2012) Retention of personal data reads:

25. An organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that

(a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and

(b) retention is no longer necessary for legal or business purposes.

[272] Personal data protection act 2012 (No. 26 of 2012) Transfer of personal data outside Singapore reads:

26. (1) An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act.

(2) The Commission may, on the application of any organisation, by notice in writing exempt the organisation from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organisation.

(3) An exemption under subsection (2)

(a) may be granted subject to such conditions as the Commission may specify in writing; and

(b) need not be published in the Gazette and may be revoked at any time by the Commission.

(4) The Commission may at any time add to, vary or revoke any condition imposed under this section.

มีมาตรฐานด้านความปลอดภัยเทียบเท่า หรือสูงกว่ากฎหมายของสิงคโปร์ (Commissioner) อาจออกข้อยกเว้นให้กับบางองค์กรที่เห็นว่าเหมาะสมได้

การแจ้งว่ามีการกระทำผิด (Breach notification) ไม่มีการกำหนดไว้ แต่หน่วยงานย่อยของรัฐอาจจะสามารถออกข้อบังคับเป็นพิเศษเกี่ยวกับหน้าที่นี้ได้

การบังคับใช้และบทลงโทษการบังคับใช้กฎหมายเป็นหน้าที่ของคณะกรรมการ โดยที่คณะกรรมการมีอำนาจดังต่อไปนี้สั่งให้หยุดการเก็บการใช้การเปิดเผยข้อมูลส่วนบุคคล หากพบการกระทำที่ฝ่าฝืนต่อบทบัญญัติของกฎหมายทำลายข้อมูลส่วนบุคคลที่มีการเก็บไว้ โดยฝ่าฝืนต่อกฎหมายการฝ่าฝืนกฎหมายอาจต้องรับโทษถึง 100, 000 ดอลลาร์สิงคโปร์ หรือต้องโทษจำคุกไม่เกิน 12 เดือน หรือทั้งจำทั้งปรับ ทั้งนี้ ผู้อำนวยการและเจ้าหน้าที่ของหน่วยงานสามารถถูกฟ้องร้องความรับผิดชอบจากความผิดที่หน่วยงานเป็นผู้กระทำได้ด้วย[273] ซึ่งหน่วยงานในสาธารณรัฐสิงคโปร์ถูกสั่งปรับค่าเสียหายเนื่องจากทำข้อมูลลูกค้ารั่วไหลออกไป แต่อย่างไรก็ตาม แม้ว่าสาธารณรัฐสิงคโปร์จะมีโทษทางอาญาแต่ก็มุ่งเน้นให้ผู้ประกอบการธุรกิจตระหนักถึงตัวบุคคลที่อยู่ในองค์กรของตนคำนึงความมั่นคงปลอดภัยตาม (Offences by bodies corporate, etc.51)[274]

---

[273] Personal data protection act 2012 (No. 26 of 2012) reads: Offences and penalties

51 (4) An organisation or person that commits an offence under subsection (3)(a) is liable

(a) in the case of an individual, to a fine not exceeding $5,000; and

(b) in any other case, to a fine not exceeding $50,000.

(5) An organisation or person that commits an offence under subsection (3)(b) or (c) is liable

(a) in the case of an individual, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both; and

(b) in any other case, to a fine not exceeding $100,000.

[274] Personal data protection act 2012 (No. 26 of 2012) reads:

Reads: Offences by bodies corporate, etc. 52. (1) Where an offence under this Act committed by a body corporate is proved

(a) to have been committed with the consent or connivance of an officer; or

(b) to be attributable to any neglect on his part, the officer as well as the body corporate shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members, subsection (1) shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

(3) Where an offence under this Act committed by a partnership is proved —

(a) to have been committed with the consent or connivance of a partner; or

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือ (Personal Data Protection Commission: PDPC)ของประเทศสิงคโปร์ ประกาศว่ามีการสั่งปรับค่าเสียหายจากหน่วยงาน 4 แห่งที่ไม่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ดีพอจนทำให้ข้อมูลส่วนตัวของลูกค้าต้องรั่วไหลออกไป

ตัวอย่างเช่น K Box Entertainment Group

ศาลสั่งมีคำปรับค่าเสียหายหน่วยงาน (K Box Entertainment Group) ซึ่งข้อมูลส่วนตัวของลูกค้าที่รั่วไหลออกไป โดยถูกสั่งปรับ 50,000 ดอลลาร์สิงคโปร์ เนื่องจากถูกโจมตีในระบบฐานข้อมูลเมื่อปี 2014 และฐานข้อมูลลูกค้ามีการรั่วไหล นอกจากนี้ทาง (PDPC) ยังได้มีการแจ้งเตือนไปยังหน่วยงานและบริษัทอื่น ๆ อีก 7 แห่ง เพื่อให้เพิ่มมาตรการรักษาข้อมูลของลูกค้า เนื่องจากพบว่าหลายหน่วยงานดังกล่าวนั้นมีการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่ยังไม่ดีพอ[275]

3.5.2 มาตรการในการคุ้มครองข้อมูลไบโอเมตริกซ์ (Biometrics)

ประเด็นที่หนึ่ง คำนิยามของ “ข้อมูลส่วนบุคคล” (Personal Data Protection) บัญญัติไว้ว่า “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใด ๆ ไม่ว่าจะเป็นข้อมูลจริง หรือไม่เกี่ยวกับบุคคล แต่สามารถระบุตัวตนของบุคคลนั้นได้ โดยให้ความคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับผู้ที่ถึงแก่กรรมแล้วภายใน 10 ปี แต่ไม่คุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการติดต่อทางธุรกิจ แม้ว่าจะเป็นข้อมูลเกี่ยวกับบุคคล ซึ่งมิใช่เพื่อวัตถุประสงค์เป็นการส่วนตัว เว้นแต่ จะได้ระบุไว้อย่างชัดเจน (Personal Data Protection) โดยบัญญัติคำนิยามไว้กว้าง ๆ แต่มิได้บัญญัติคำนิยาม “ข้อมูลพันธุกรรม”และ “ข้อมูลไบโอเมตริกซ์” ซึ่งเป็นข้อมูลที่มีความละเอียดอ่อนไว้ในพระราชบัญญัติฉบับนี้แต่อย่างใด อย่างไรก็ตาม ข้อมูลไบโอเมตริกซ์ซึ่งเป็นข้อมูลส่วนบุคคลที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

(b) to be attributable to any neglect on his part,

the partner as well as the partnership shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(4) Where an offence under this Act committed by an unincorporated association (other than a partnership) is proved —

(a) to have been committed with the consent or connivance of an officer of the unincorporated association or a member of its governing body; or

(b) to be attributable to any neglect on the part of such an officer or member, the officer or member as well as the unincorporated association shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

[275] ETDA สพธอ. (2016). ***ข่าวสั้นกฎหมายคุ้มครองข้อมูลส่วนบุคคล***. (ออนไลน์). เข้าถึงได้จาก: https://www.thaicert.or.th/newsbite/2016-04-22-03.html. [2562, 2 กันยายน]

ที่ถูกใช้ในระบบของธนาคาร ก็ย่อมได้รับการคุ้มครองข้อมูลส่วนบุคคลดังกล่าว ไม่แตกต่างไปจากมาตรฐานของข้อมูลส่วนบุคคลประเภทอื่น ๆ

ประเด็นที่สอง หลักการความยินยอม (Consent) และการถอนความยินยอมของข้อมูลส่วนบุคคล ในการประมวลผลข้อมูลส่วนบุคคล หรือ เก็บ รวบรวม ใช้ เปิดเผย ลบ หรือทำลาย จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนดำเนินการใด ๆ และเจ้าของข้อมูลสามารถปฏิเสธ หรือยกเลิกความยินยอมได้ตาม (Withdrawal of consent Section 16) โดยแจ้งวัตถุประสงค์ในขณะ หรือก่อนการรวบรวมข้อมูลส่วนบุคคลตาม (Notification of purpose Section 20) ซึ่งองค์กรไม่อาจกำหนดให้การให้ความยินยอมเป็นเงื่อนไข ในการขายสินค้าและบริการในระดับที่เกินกว่าความสมเหตุสมผลต่อการให้บริการนั้น ๆได้ (Beyond what is reasonable) โดยองค์กรไม่สามารถขอความยินยอมโดยปลอมแปลงข้อเท็จจริงของความยินยอมที่ได้มาด้วยวิธีการดังกล่าวได้และไม่ถือว่าเป็นความยินยอมที่มีผลใช้ได้ตามกฎหมายฉบับนี้ ความยินยอมนั้น อาจเป็นความยินยอมแบบโดยปริยายได้

ประเด็นที่สาม มาตรการในการบังคับใช้กฎหมายโดยเฉพาะอย่างยิ่งระยะเวลาในการเก็บรักษาข้อมูลซึ่งจะเป็นไปตามหลัก (Right to be forgotten) การแจ้งระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล โดย (PDPA) กำหนดให้องค์กรต้องไม่เก็บรักษาเอกสารซึ่งเป็นข้อมูลส่วนบุคคลที่ได้รับการประมวลผล หรือวิธีการที่ข้อมูลส่วนบุคคลนั้นสามารถเชื่อมโยงไปยังตัวบุคคลบุคคลใดบุคคลหนึ่งได้และถูกเข้าถึงโดยไม่ได้รับอนุญาต ไม่ให้เก็บรักษาข้อมูลส่วนบุคคล หรือต้องลบข้อมูลโดยทันทีที่มีเหตุผลอันสมควรที่สันนิษฐานได้ว่าไม่จำเป็นสำหรับธุรกิจ หรือตามวัตถุประสงค์ทางกฎหมายอีกต่อไปตามข้อบังคับ (Retention of personal data Section 25)

ประเด็นที่สี่ แนวทางในการแก้ไขปัญหาข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามบทบัญญัติเพื่อบทลงโทษความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (PDPA) องค์กรเป็นหน่วยงานป้องกันข้อมูลส่วนบุคคล ซึ่งอยู่ในความครอบครอง หรืออยู่ในการความควบคุมขององค์กร โดยมีมาตรการเพื่อป้องกันมิให้ข้อมูลส่วนบุคคลนั้น ถูกเข้าถึงโดยไม่ได้รับอนุญาต แก้ไข ใช้ เปิดเผย คัดลอก เปลี่ยนแปลง ทำลาย หรือความเสี่ยงอื่นที่มีลักษณะเช่นเดียวกันและในการเก็บรักษาข้อมูลส่วนบุคคลนั้น ข้อมูลส่วนบุคคลจะถูกเก็บไว้ในเซิร์ฟเวอร์ส่วนกลางเพื่อปกป้องความลับ และความปลอดภัยของข้อมูลส่วนบุคคลภายใต้การบริการผ่านเทคโนโลยีการป้องกันความปลอดภัยทางกายภาพและการบริหารในการรักษาความปลอดภัย หากมีการละเมิดโดยฝ่าฝืนต่อกฎหมายต้องรับโทษปรับถึง 100,000 ดอลลาร์สิงคโปร์ หรือต้องโทษจำคุกไม่เกิน 12 เดือน หรือทั้งจำทั้งปรับตาม (Offences by bodies corporate, etc.51) โดยมุ่งเน้นให้ผู้ประการธุรกิจตระหนักควบคุมดูแลบุคคลในองค์ของตนให้คำนึงความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งนี้ ผู้อำนวยการและ

เจ้าหน้าที่ของหน่วยงานสามารถถูกฟ้องร้องความรับผิดชอบจากความผิดที่หน่วยงานเป็นผู้กระทำได้ด้วยตาม (Offences and penalties Section 51)

ดังนั้น หากพิจารณาตามกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act 2012) คำว่า "ข้อมูลส่วนบุคคล" ที่ปรากฏอยู่ใน (PDPA) ของสาธารณรัฐสิงคโปร์ บัญญัติคำว่า ข้อมูลทั้งหลายที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคล โดยมีชื่อ หรือเลขหมาย หรือรหัส หรือสิ่งบอกลักษณะอื่นใดที่ทำให้รู้ตัวบุคคลนั้นได้ และการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act)[276] กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลส่วนบุคคลทราบเสียก่อน และกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตนเองและสิทธิในการถอนคำยินยอมต้องมีการแจ้งผลกระทบในการถอนคำยินยอนนั้นตาม (Withdrawal of consent Section 16)) เป็นลายลักษณ์อักษร หากเห็นว่าข้อมูลส่วนบุคคลของตนดังกล่าวไม่ถูกต้องครบถ้วน หรือไม่เป็นปัจจุบัน เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคลแก้ไขได้ ในกรณีเช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแก้ไขข้อมูลส่วนบุคคลโดยเร็วเท่าที่จะสามารถกระทำได้ และส่งการแก้ไขข้อมูลส่วนบุคคลนั้นให้แก่องค์กรอื่นซึ่งได้รับการเปิดเผยข้อมูลส่วนบุคคลนั้น ๆ และในด้านข้อมูล (IP Address) จะถือว่าเป็นข้อมูลส่วนบุคคลได้ก็ต่อเมื่อข้อมูลนั้น สามารถเชื่อมโยงไปยังเจ้าของข้อมูลได้และข้อมูล (Biometric)ไม่ปรากฏว่าได้รับความคุ้มครองตาม (Personal Data Protection Act 2012) แต่อย่างไรก็ดี ในแง่ของกฎหมาย (PDPA) เอง ซึ่งการที่ข้อมูลส่วนบุคคลของลูกค้า หรือผู้รับบริการในรูปแบบ (Biometric data) ถือว่าเป็นข้อมูลส่วนบุคคลของผู้รับบริการ โดยเฉพาะอย่างยิ่งธุรกิจการธนาคารที่ได้นำระบบเทคโนโลยี (Biometrics) มาประยุกต์ใช้เพื่อป้องกันการทุจริตทางการเงินและสร้างความปลอดภัยในการเข้าถึงบริการทางการเงินในรูปแบบต่าง ๆ ที่เป็นข้อมูลติดต่อทางธุรกิจ

ดังนั้น เมื่อพิจารณาตามถ้อยคำของกฎหมาย จะเห็นได้ว่าข้อมูลของลูกค้า หรือผู้รับบริการที่ได้จากการใช้ (Biometrics) แม้จะอยู่ในรูปของรหัสชุด หรือรูปแบบอิเล็กทรอนิกส์ ย่อมเป็นข้อมูลส่วนบุคคลของลูกค้า หรือผู้รับบริการทั้งสิ้น เพราะเป็นสิ่งที่ทำให้ธนาคาร หรือผู้ให้บริการสามารถระบุการยืนยัน และทราบถึงตัวตนของลูกค้าแต่ละรายได้อย่างถูกต้องก่อนให้บริการ หรืออาจกล่าวได้ว่า (Biometric data)คือ ข้อมูลส่วนบุคคลที่ธนาคารต้องดูแลตามมาตรฐานที่กฎหมายกำหนดในทางปฏิบัติของข้อมูลไบโอเมตริกซ์ (Biometric data) ของลูกค้า หรือผู้รับบริการจะถูกเก็บไว้ในอุปกรณ์อิเล็กทรอนิกส์ในหลายรูปแบบ เช่น อาจเก็บไว้ใน (Smart mobile devices :SMDs) โดยผู้ให้บริการบาง

---

[276] อธิพร สิทธิธีรรัตน์. (2558). ***ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขาการค้าระหว่างประเทศ, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. หน้า 48.

รายอาจเก็บข้อมูลทั้งหมดไว้บนฐานข้อมูลประเภทคลาวด์ (Cloud) ด้วยอีกชั้นหนึ่ง และต้องลบข้อมูลทันทีที่มีเหตุผลอันสมควรที่สันนิษฐานได้ว่าไม่จำเป็นสำหรับธุรกิจ หรือตามวัตถุประสงค์ทางกฎหมาย แสดงได้ว่า (Biometric data) อันเป็นข้อมูลส่วนบุคคลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ซึ่งมาตรฐานในการให้ความคุ้มครองย่อมไม่แตกต่างไปจากข้อมูลส่วนบุคคลประเภทอื่น ๆ ของ (Personal Data Protection Act 2012) นั้นเอง

บทสรุป

จากการศึกษามาตราทางกฎหมายในการให้ความคุ้มครองข้อมูลไบโอเมตริกซ์ สำหรับปัญหาของประเทศไทยแม้ว่าจะมีบทบัญญัติให้ความคุ้มครองข้อมูลข่าวสาร พุทธศักราช 2540 แต่อย่างไรก็ตาม การให้ความคุ้มครองข้อมูลข่าวดังกล่าว ซึ่งเป็นการคุ้มครองข้อมูลข่าวสารที่อยู่ในความครอบครองของหน่วยรัฐ แต่มิได้ให้ความคุ้มครองข้อมูลข่าวสารที่อยู่ในความครอบครองของหน่วนงานเอกชน หรือ บุคคลแต่อย่างไร เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 บทบัญญัติให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป โดยพบว่าข้อมูลไบโอเมตริกซ์ตามมาตรา 26 นั้น ยังไม่สอดคล้องกับคำนิยามศัพท์ โดยมิได้บัญญัติประเภท “ข้อมูลไบโอเมตริกซ์” ซึ่งเป็นข้อมูลละเอียดอ่อนบ่งชี้ถึงเอกลักษณ์ของบุคคลโดยแท้จริง แต่พบว่าหน่วยงานรัฐบางหน่วยงานได้เก็บข้อมูลชีวมาตรส่วนบุคคล หรือข้อมูลไบโอเมตริกซ์ (Biometrics) และใช้ในการพิสูจน์ยืนยันตัวบุคคล โดยรัฐ หรือหน่วยงานที่รัฐให้อำนาจในการจัดเก็บ รวบรวม ใช้ เปิดเผย เช่น ลายนิ้วมือ ใบหน้า ม่านตา ในการใช้ข้อมูลชีวมาตรในการระบุตัวบุคคล และการพิสูจน์ยืนยันตัวบุคคลล้วนแต่ใช้ข้อมูลเหล่านี้

อันเป็นข้อมูลลับเฉพาะตัวที่สามารถเชื่อโยงถึงตัวบุคคลได้ ซึ่งหน่วยงานรัฐยังขาดการกำกับดูแล ธรรมาภิบาล กล่าวคือ การตรากฎหมาย กฎ ระเบียบข้อบังคับและกติกาต่าง ๆ ให้ทันสมัยและเป็นธรรม ตลอดจนเป็นที่ยอมรับของสังคมโลก โดยมีการยินยอมพร้อมใจและถือปฏิบัติร่วมกันอย่างเสมอภาคให้โปร่งใส ซึ่งรัฐต้องมีมาตรการในการเยียวยาข้อมูลรั่วไหลและเสี่ยงที่จะถูกนำข้อมูลส่วนบุคคลไปใช้งานโดยมิชอบ เพราะผู้เป็นเจ้าของข้อมูลชีวมาตรจะไม่สามารถที่จะเปลี่ยนแปลงแก้ไขข้อมูลชีวมาตรของตนเองได้เลย เมื่อมีการรั่วไหลของข้อมูลไบโอเมตริกซ์ เช่น หน่วยงานของกระทรวงการต่างประเทศ โดยกระทรวงมหาดไทยได้ให้บริษัทเอกชนเก็บข้อมูลเหล่านี้

ทั้งนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 บัญญัติว่า หากมีการละเมิดเจ้าของข้อมูลส่วนบุคคลนั้นไม่สามารถฟ้องการละเมิดสิทธิดังกล่าวนี้ได้ตามมาตรา 24 บัญญัติว่า การเก็บและใช้ข้อมูลส่วนบุคคลต้องได้รับความยินยอม เว้นแต่ เพื่อประโยชน์สาธารณะและการใช้อำนาจรัฐ กรณีมาตรา 27 ห้ามมิให้ทำการเปิดเผยข้อมูลที่เก็บ เว้นแต่ในกรณีตามมาตรา 24 และมาตรา 27 ดังนั้น ประเทศไทยควรมีมาตรการทางกฎหมายในการควบคุม การจัดการและการใช้

ข้อมูลไบโอเมตริกซ์ของหน่วยรัฐและเอกชน ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนโดยชัดแจ้งไม่คลุมเคลือ รวมทั้งการถอนคำยินยอมนั้นต้องแจ้งผลกระทบ “ก่อน” ให้ความยินยอม ในการจัดเก็บและการใช้ข้อมูลไบโอเมตริกซ์ควรมีการกำหนดระยะเวลาในการจัดเก็บ รวบรวม เปิดเผย ใช้ การทำลายข้อมูลไบโอเมตริกซ์และในกรณีหน่วยงานรัฐ หรือบริษัทเอกชนโดยใช้อำนาจของกฎหมาย หากมีการละเมิด เจ้าของข้อมูลควรมีสิทธิฟ้องเรียกค่าเสียหายตามที่คาดว่าจะได้รับผลกระทบจากการละเมิด เพื่อให้ข้อมูลไบโอเมตริกซ์ตามมาตรา 26 เพื่อให้มีความสอดคล้องในการให้การคุ้มครองในหมวดหมู่ข้อมูลประเภทพิเศษเฉพาะ

ด้วยเหตุนี้ ในงานวิจัยฉบับนี้ผู้วิจัยได้ทำการศึกษากฎหมายคุ้มครองข้อมูลไบโอเมตริกซ์ของสหภาพยุโรป สหรัฐอเมริกา สาธารณรัฐเยอรมนี และสาธารณรัฐสิงคโปร์ ซึ่งเป็นแนวทางในการคุ้มครองส่วนบุคคล กรณีข้อมูลไบโอเมตริกซ์ (Biometrics) หรือข้อมูลชีวมาตร ในการใช้ข้อมูลชีวมาตรนี้อาจส่งผลกระทบต่อบุคคลผู้เป็นเจ้าของข้อมูลในการละเมิดความเป็นส่วนตัวอย่างมากนั้น แม้ว่าผู้วิจัยจะได้ทำศึกษาและการเปรียบเทียบกับสหรัฐอเมริกา ซึ่งเป็นกฎหมายในระดับมลรัฐก็ตาม เนื่องจากสหรัฐอเมริกาเป็นประเทศมีฐานเศรษฐกิจอยู่ทั่วโลก จึงเป็นที่น่าสนในอย่างยิ่ง ผู้วิจัยจึงได้ทำการศึกษาเกี่ยวกับการคุ้มครองข้อมูลไบโอเมตริกซ์กับต่างประเทศโดยพบเหตุดังนี้

กฎระเบียบข้อบังคับ (Regulation (EU) 2018/1725: GDPR) ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของ (EU) จัดให้ข้อมูลไบโอเมตริกซ์ หรือข้อมูลชีวมาตรเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนโดยให้ความสำคัญเป็นกรณีพิเศษ (Special Categories of Personal Data) ห้ามการเก็บบันทึก หรือประมวลผลตาม Article 10 เนื่องจากการประมวลผลข้อมูลส่วนตัวประเภทพิเศษครอบคลุมถึงข้อมูลไบโอเมตริกซ์ เมื่อประมวลผลด้วยวิธีการทางเทคนิคเฉพาะที่อนุญาตให้มีการระบุตัวตน หรือการพิสูจน์ตัวตนของบุคคลได้ รวมถึงข้อมูลทางพันธุกรรมก็จะอยู่ในหมวดหมู่ประเภทข้อมูลส่วนบุคคลพิเศษ โดยได้รับอนุญาตภายใต้เงื่อนไขเฉพาะ หรือการประมวลผลที่ทำให้เกิดมาตรการที่มีผลกระทบต่อการตัดสินใจ ยกเว้น มีความจำเป็นอย่างหลีกเลี่ยงไม่ได้ตามกฎหมาย หรือได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลทราบก่อนเสมอ

พระราชบัญญัติข้อมูลส่วนบุคคล (Privacy Act 1974) การเก็บรวบรวมข้อมูลส่วนบุคคลต้องอยู่ภายใต้ (Privacy Act) ซึ่งหน่วยงานของรัฐจะต้องได้รับข้อมูลส่วนบุคคลนั้นมาจากบุคคลผู้เกี่ยวข้องโดยตรงและต้องแจ้งกฎหมาย หรือคำสั่งที่ให้อำนาจแก่หน่วยงานรัฐ ในการเก็บ รวบรวมข้อมูลส่วนบุคคล โดยแจ้งให้ทราบถึงลักษณะของข้อมูลส่วนบุคคลและต้องระบุว่าข้อมูลนั้นจะถูกนำไปใช้เพื่อวัตถุประสงค์ใด เว้นแต่ กรณีพิเศษ (Special Exemption) ตามมาตรา 5 U.S.C § 552 a. (d) (5) หน่วยงานของรัฐต้องเก็บข้อมูลเพียงเท่าที่จำเป็นและเกี่ยวข้องกับวัตถุประสงค์ เมื่อมีการเปิดเผยข้อมูลส่วนบุคคลแล้ว หน่วยงานของรัฐจะต้องทำรายงานข้อมูลเกี่ยวกับวันเวลา

ของข้อมูลส่วนบุคคลที่ได้รับการเปิดเผยข้อมูลเกี่ยวกับการติดต่อบุคคล หรือองค์กรที่ได้รับข้อมูลส่วนบุคคลนั้น โดยจะต้องเก็บรายงานดังกล่าวไว้ภายใน 5 ปี หรือตลอดอายุของบันทึก แล้วแต่ระยะเวลาใดยาวกว่าให้ถือระยะเวลานั้น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในการสื่อสารทางอิเล็กทรอนิกส์ (Electronic Communications Privacy Act 1986) ซึ่งบทบัญญัติไว้ใน18 U.S. Code §2510-2522 มีวัตถุประสงค์ในการห้ามการดักฟังทางโทรศัพท์รวมไปถึงการดักรับข้อมูลที่ส่งโดยทางอิเล็กทรอนิกส์ผ่านทางคอมพิวเตอร์และมิได้จำกัดเฉพาะการ “ดักฟัง” แต่ยังได้ครอบคลุมถึงการ “ดักรับการสื่อสารข้อมูล” ไม่ว่าจะกระทำด้วยวิธีการใด ๆ ก็ตาม ซึ่งสหรัฐอเมริกาก็ได้ให้ความสำคัญต่อการคุ้มครองสิทธิในความเป็นส่วนตัวรวมถึงการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างมาก แต่ยังมิได้ให้การคุ้มครองถึงประเภทของข้อมูลไบโอเมตริกซ์

พระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ (Biometric Information Privacy Act: BIPA) มีเพียงสามรัฐที่ได้ผ่านนิติบัญญัติโดยรัฐอิลลินอยส์ (Illinois Biometric Information Privacy Act: BIPA) เป็นรัฐแรกที่ให้ความสำคัญเกี่ยวกับลายนิ้วมือของรัฐอิลลินอยส์ (BIPA) หรือการใช้กฎระเบียนการระบุตัวตนทางชีวมาตรรัฐเท็กซัส (Texas Biometric Identifier Statute: BIS) และกฎหมายการระบุตัวตนทางชีวมาตรของวอชิงตัน (Washington Biological Identification Law : BI) ที่มีผลบังคับใช้กฎหมายข้อมูลไบโอเมตริกทั้งสามรัฐนี้ มีเพียงรัฐอิลลินอยส์ (BIPA) เท่านั้นที่ให้สิทธิในความเป็นส่วนตัว และควบคุมการเก็บ รวบรวมชีวมาตรไม่ว่าทั้งหมด หรือบางส่วนโดยกฎหมายไบโอเมตริกซ์ของมลรัฐสหรัฐอเมริกา บัญญัติห้ามมิให้เอกชนกระทำการลงทะเบียนระบุตัวบุคคลด้วยระบบไบโอเมตริกซ์ไว้ในฐานข้อมูล โดยมิได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบล่วงหน้าและให้ความยินยอม ห้ามการขาย ให้เช่าซื้อ หรือเปิดเผยข้อมูลไบโอเมตริกซ์เพื่อวัตถุประสงค์ทางการค้า เว้นแต่จะมีคุณสมบัติตรงตามที่บทบัญญัติได้กำหนดไว้ในกฎหมายอันเกี่ยวกับข้อกำหนดในการเก็บรักษาและการเข้าถึงการระบุอัตลักษณ์ของบุคคลด้วยระบบไบโอเมตริกซ์ การเก็บรักษาข้อมูลส่วนบุคคลต้องเป็นลายลักษณ์อักษรไว้ โดยเฉพาะสำหรับข้อมูลไบโอเมตริกซ์จะต้องกำหนดเป็นตารางการเก็บข้อมูล และ แนวทางสำหรับการลบข้อมูลไบโอเมตริกซ์อย่างถาวร เมื่อไม่วัตถุประสงค์ในการรวบรวมข้อมูลไบโอเมตริกซ์ให้เป็นที่พึงพอใจแก่ผู้เจ้าของข้อมูลส่วนบุคคล หรือภายใน 3 ปี หรือแล้วแต่จำนวนใดจะถึงก่อนตามพระราชบัญญัติฉบับนี้

พระราชบัญญัติคุ้มครองข้อมูลของรัฐบาลกลาง (Federal Data Protection Act: BDSG 2018) สหพันธ์รัฐสาธารณรัฐเยอรมนี บัญญัติให้มีการจำแนกประเภทของข้อมูลส่วนบุคคลทั่วไปที่เกี่ยวข้องกับบุคคล หรือรายละเอียดใด ๆ ที่สามารถเชื่อมโยงถึงตัวบุคคลที่มีความอ่อนไหวง่ายต่อความรู้สึก (Special categories of personal data) ซึ่งเกี่ยวกับพฤติกรรมทางเพศ สุขภาพ การแสดง

ความคิดเห็นทางการเมือง ความเชื่อทางศาสนาลัทธิปรัชญา ความเป็นสมาชิกสหภาพแรงงาน เชื้อชาติ เผ่าพันธ์และ รวมถึงข้อมูลไบโอเมตริกซ์ โดยจะให้การคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลที่มีความอ่อนไหวเข้มงวดมาก โดยจะเห็นได้ชัดเจน จากการขอความยินยอมเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลประเภทที่เป็นข้อมูลที่ละเอียดอ่อนและกระทบต่อความรู้สึกตาม Section 46 ของ (Federal Data Protection Act 2018) ซึ่งมีการกำหนดมาตรการเกี่ยวกับข้อมูลที่มีความละเอียดอ่อนและอ่อนไหวง่าย โดยผู้ควบคุม หรือผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องขอความยินยอมจากเจ้าของข้อมูลก่อน และจะต้องแสดงการขอความยินยอมเป็นลายลักษณ์อักษรให้ชัดเจนเป็นตารางว่าเป็นการขอความยินยอมเกี่ยวกับการประมวลผลข้อมูลที่มีความอ่อนไหว ซึ่งข้อมูลประเภททางพันธุกรรมที่เป็นข้อมูลทั่วไปนั้น

หากเกิดจากเทคนิคไบโอเมตริกซ์ ก็ถือว่าเป็นข้อมูลส่วนบุคคลประเภทพิเศษได้ และข้อมูลส่วนบุคคลที่มีความอ่อนไหวรวมอยู่ด้วย โดยกฎหมายสหพันธ์สาธารณรัฐเยอรมนีกำหนดว่าการขอความยินยอมเกี่ยวกับเรื่องข้อมูลส่วนบุคคลที่มีความอ่อนไหวดังกล่าว จะต้องได้รับการชี้แจงเป็นลายลักษณ์อักษณ์ และแสดงตารางรายละเอียดให้ชัดเจนก่อนจะให้ความยินยอม และแจ้งผลกระทบในการถอนความยินยอมให้แก้เจ้าของข้อมูลทราบก่อน รวมทั้งระยะเวลาในการเก็บรวบรวม ทำลายตาม New Section 51 (3) ซึ่งต้องสอดคล้องกับกฎระเบียบของ (GDPR) กล่าวคือในส่วนที่มีความเกี่ยวข้องกับการคุ้มครองข้อมูลทั่วไป และข้อบังคับของ (BDSG) จะใช้บังคับได้เฉพาะในกรณีที่ (GDPR) ไม่ได้ใช้บังคับโดยตรงเท่านั้น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act 2012: PDPA) สาธารณรัฐสิงคโปร์ ได้บัญญัติให้ข้อมูลใด ๆ ที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคล หรือสิ่งบอกเอกลักษณ์อื่นใดที่ทำให้รู้ตัวบุคคลได้และการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอม และรวมทั้งต้องแจ้งผลกระทบในการถอนคำยินยอมจากผู้เป็นเจ้าของข้อมูลส่วนบุคคลเสียก่อน หรือในขณะอย่างอิสระตาม Withdrawal of consent Section 16 โดยกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตนเอง หากเห็นว่าข้อมูลส่วนบุคคลของตนดังกล่าวไม่เป็นปัจจุบัน หรือไม่ถูกต้องครบถ้วนที่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลได้ และต้องลบข้อมูลทันทีที่มีเหตุผลอันสมควรที่สันนิษฐานได้ว่าไม่จำเป็นสำหรับธุรกิจ หรือตามวัตถุประสงค์ของกฎหมายที่ได้บัญญัติไว้ แต่ปรากฏว่ามิได้จำแนกการคุ้มครองข้อมูลไบโอเมตริกซ์ไว้ใน (PDPA) แต่อย่างไรก็ตามหากพิจารณาถึงข้อมูล (Biometrics data) ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวง่ายที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ก็ย่อมคุ้มครองไม่แตกต่างไปจากข้อมูลส่วนบุคคลประเภทอื่น

จากการศึกษากฎหมายต่างประเทศดังกล่าวข้างต้น อันเกี่ยวกับมาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลไบโอเมตริกซ์ภายใต้กฎหมายไทยควรจะมีความหมายอย่างไร อีกทั้งแนวทางในการแก้ไขปัญหาข้อมูลไบโอเมตริกซ์ (Biometrics) เพื่อมาตรการให้ความยินและการถอนความยินยอมข้อมูลไบโอเมตริกซ์ (Biometrics) ในการบังคับใช้กฎหมายตามพระราชบัญญัติฉบับนี้ โดยเฉพาะอย่างยิ่งระยะเวลาในการจัดเก็บรักษาข้อมูลส่วนบุคคลซึ่งจะต้องเป็นไปตามหลัก (Right to be forgotten) อันจะนำไปสู่การวิเคราะห์ปัญหาเกี่ยวกับข้อมูลไบโอเมตริกซ์ของประเทศไทยในบทต่อไป