

มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลที่เป็นข้อมูลชีวภาพของ ผู้ใช้บริการในสถาบันการเงิน¹

ศศิกันต์ ศรีอินทร์²

จากการศึกษาเกี่ยวกับมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลที่เป็นข้อมูลชีวภาพของผู้ใช้บริการในสถาบันการเงิน มีวัตถุประสงค์เพื่อศึกษาถึงความเป็นมา แนวคิด ทฤษฎีเกี่ยวกับสิทธิความเป็นส่วนตัว หลักการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและข้อมูลชีวภาพที่ถูกนำไปประมวลผลเพื่อใช้ในการกิจการของสถาบันการเงิน ศึกษามุมมองที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เป็นข้อมูลชีวภาพตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของกฎหมายไทย กฎหมายระหว่างต่างประเทศ และกฎหมายต่างประเทศจากการศึกษานี้การคุ้มครองข้อมูลส่วนบุคคลมีแนวความคิดพื้นฐานมาจากสิทธิในความเป็นส่วนตัวซึ่งเป็นหลักการพื้นฐานของสิทธิมนุษยชนที่ถูกบัญญัติอยู่ในกฎบัตรของสหประชาชาติ ซึ่งทำให้ผู้ศึกษาได้รับความรู้ความเข้าใจเกี่ยวกับสิทธิความเป็นส่วนตัวที่ต้องได้รับการคุ้มครองจากรัฐ และความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลที่มีอำนาจตัดสินใจให้ผู้ใดสามารถนำข้อมูลส่วนบุคคลที่สามารถระบุถึงตัวตนของเจ้าของข้อมูลส่วนบุคคลไปใช้ในกิจกรรมใด ๆ ได้โดยอาศัยหลักความยินยอมมาโดยผู้ใดจะเข้ามาแทรกแซงมิได้ สำหรับประเทศไทยการคุ้มครองข้อมูลส่วนบุคคลก็ถูกรับรองอยู่ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ในมาตรา 32 ด้วย นอกจากนี้ยังให้ผู้ศึกษาได้ทำความเข้าใจเกี่ยวกับข้อมูลชีวภาพ ซึ่งถือได้ว่าเป็นเรื่องใหม่สำหรับกฎหมายของไทย ซึ่งข้อมูลชีวภาพนี้เป็นข้อมูลส่วนบุคคลที่เป็นข้อมูลที่มีความละเอียดอ่อนเป็นพิเศษกว่าข้อมูลส่วนบุคคลทั่วไป เพราะเป็นข้อมูลนำเอาอัตลักษณ์หรือลักษณะเด่นทางร่างกายหรือพฤติกรรมของบุคคลมาใช้ในการยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนคนอื่น และเป็นข้อมูลถาวรที่ไม่สามารถเปลี่ยนแปลงได้ ทำให้มีความเสี่ยงในการกระทบต่อสิทธิเสรีภาพทางร่างกายของเจ้าของข้อมูลชีวภาพได้ โดยเฉพาะขณะนี้หลายสถาบันการเงินของไทยเองก็มีการนำข้อมูลชีวภาพมาใช้ในการยืนยันตัวตนของผู้ใช้บริการอย่างแพร่หลายเพิ่มขึ้นมากขึ้น มาตรฐานการเก็บ ใช้เปิดเผยข้อมูลก็ต้องสูงขึ้นไป เพราะถ้ามันเกิดข้อผิดพลาดข้อมูลมันจะกระจายไปอย่างรวดเร็วและยากที่จะควบคุมได้ ผู้ควบคุมมีหน้าที่ในการจัดให้มีมาตรการการรักษาความมั่นคงความปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

¹ บทความนี้เรียบเรียงจากการค้นคว้าอิสระ เรื่อง มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลที่เป็นข้อมูลชีวภาพของผู้ใช้บริการในสถาบันการเงิน โดยมีอาจารย์ที่ปรึกษา คือ ผู้ช่วยศาสตราจารย์ ดร.มณฑิลา ภักดีคง และคณะกรรมการสอบคือ รองศาสตราจารย์ ดร.พันธ์เทพ วิฑิตอนันต์ และ ผู้ช่วยศาสตราจารย์ ดร.คนพร จิตต์จริงเกียรติ

² นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต (ส่วนกลาง) คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

หลักการสำคัญของการคุ้มครองข้อมูลทุกประเทศนั้นคือหลักความยินยอมที่เจ้าของต้องมีอำนาจและอิสระตามใจชอบที่จะให้ความยินยอมในการประมวลหรือไม่ ซึ่งต้องไม่เกิดจากการขู่เข็ญ หลอกลวง ทำให้สับสน มีการแจ้งรายละเอียดของข้อมูลที่เพียงพอให้แก่เจ้าของข้อมูลส่วนบุคคล โดยเฉพาะการแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลที่ได้ขอความยินยอม นอกจากนี้ ในการประมวลข้อมูลส่วนบุคคลต้องมีการประมวลอย่างจำกัด ไม่กระทำการใดๆนอกจุดประสงค์ที่แจ้งไว้ในข้อมูลชีวภาพนั้นเป็นข้อมูลที่เป็นข้อมูลถาวรไม่สามารถมีการเปลี่ยนแปลงได้ ทำให้ระดับการคุ้มครองนั้นต้องมากและเข้มงวดกว่าข้อมูลส่วนบุคคลระดับทั่วไป สำหรับการมาตรการรักษาความปลอดภัยผู้ควบคุมและผู้ประมวลข้อมูลต้องมีหน้าที่ในการจัดการการการดูแลรักษาความปลอดภัยให้เหมาะสมกับข้อมูลที่ได้เก็บรวบรวมไป โดยเฉพาะอย่างยิ่งสถาบันการเงินที่ได้มีการเก็บรวบรวมข้อมูลบุคคลจำนวนมากเป็นหน่วยงานที่ถือได้ว่าเป็น Big Data ขนาดใหญ่ของข้อมูลชีวภาพจากผู้ให้บริการของสถาบันการเงิน ส่งผลให้สถาบันการเงินต้องต้องมีมาตรฐานในการดูแลข้อมูลส่วนบุคคลในระดับที่สูงและต้องมีหน้าที่ในการรักษาไม่ให้มีการใช้หรือเปิดเผยข้อมูลโดยมิชอบหรือแสวงหาผลประโยชน์ทางการค้าจากข้อมูลชีวภาพโดยที่มิได้มีกฎหมายให้อำนาจกระทำได้

จากการศึกษาทำให้ทราบว่ามาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลที่เป็นข้อมูลชีวภาพของผู้ให้บริการในสถาบันการเงินยังคุ้มครองข้อมูลชีวภาพไม่เพียงพอและไม่ชัดเจนหลายประการซึ่งสามารถสรุปได้ดังต่อไปนี้

จากการศึกษาประเด็นปัญหาความยินยอมในการเก็บรวบรวมข้อมูลชีวภาพนั้นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในมาตรา 19 วรรค 3 การขอความยินยอมต้องมีการแจ้งวัตถุประสงค์ที่จะเก็บรวบรวมข้อมูลส่วนบุคคลแต่ไม่ได้มีการบัญญัติให้การขอความยินยอมและการแจ้งวัตถุประสงค์มีรายละเอียดที่มีลักษณะเป็นการเฉพาะเจาะจง ทำให้ขาดความแน่นอนชัดเจนในการขอความยินยอมและขอบเขตของวัตถุประสงค์ที่ผู้ควบคุมข้อมูลนั้นจะกว้างไม่จำกัด ทำให้ขัดกับหลักการเก็บข้อมูลส่วนบุคคลอย่างจำกัด ปัญหาอีกประการหนึ่งในเรื่องการขอความยินยอมในข้อมูลชีวภาพนั้นมาตรา 26 บัญญัติเพียงให้การมีการขอความยินยอมโดยชัดแจ้ง แต่ไม่ได้ระบุถึงรายละเอียดที่ต้องมีการแจ้งวัตถุประสงค์เป็นการเฉพาะเจาะจงเช่นเดียวกัน โดยเฉพาะการที่ข้อมูลชีวภาพนั้นมีหลายประเภทหลายชนิด พระราชบัญญัติฉบับนี้ไม่ได้มีการให้ผู้ควบคุมข้อมูลระบุประเภทหรือลักษณะของข้อมูลชีวภาพที่จะทำการเก็บรวบรวม อาจจะส่งผลให้ผู้ควบคุมข้อมูลขอความยินยอมแบบกลุ่มเกินความจำเป็น ทำให้เจ้าของข้อมูลได้รับข้อมูลที่ไม่เพียงพอเป็นผลต่อการตัดสินใจในการให้ความยินยอม

ประเด็นปัญหาที่สองการนำข้อมูลชีวภาพที่ถูกเก็บรวบรวมอยู่ในสถาบันการเงินไปเปิดเผยเพื่อวัตถุประสงค์ทางการค้านั้น โดยหลักการคุ้มครองข้อมูลส่วนบุคคลจะนำเปิดเผยโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลมิได้ แต่ข้อมูลชีวภาพนั้นเป็นข้อมูลส่งผลกระทบต่อสิทธิเสรีภาพของประชาชนถือเป็นข้อมูลที่มีความละเอียดอ่อน ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมิได้มีการบัญญัติห้ามให้มีการซื้อขาย เช่า ทำการค้า หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์ทางการค้าไว้โดยตรงเช่นเดียวกับ

รัฐบัญญัติคุ้มครองข้อมูล ไบโอเมตริกส์ของรัฐบาลลินคอล์นส์ ประเทศสหรัฐอเมริกา (BIPA) หรือกฎหมายการคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐประชาชนจีน (PIPL) แต่มีการบัญญัติเฉพาะเรื่องการเปิดเผยข้อมูลส่วนบุคคลไว้ใน มาตรา 27 ห้ามผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยข้อมูลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ซึ่งการบัญญัติเพียงเท่านี้ทำให้ข้อมูลชีวภาพไม่ได้รับการคุ้มครองในเรื่องการเปิดเผยข้อมูลที่เข้มงวดรัดกุมมากกว่าข้อมูลบุคคลทั่วไป โดยการที่มีได้มีการบัญญัติห้ามให้มีการขาย เช่า ส่งต่อ หรือเปิดเผยข้อมูลชีวภาพเพื่อการค้าหรือการแสวงหากำไรอาจทำให้ผู้ควบคุมข้อมูลอาศัยหลักการยินยอมของเจ้าของข้อมูลนำข้อมูลชีวภาพที่อยู่ในการเก็บครอบครองหรือการเก็บรักษานำไปเปิดเผยต่อบุคคลที่สามเพื่อวัตถุประสงค์ทางการค้า ทำให้เกิดผลกระทบต่อสิทธิเสรีภาพ เกิดความเสียหาย และขัดกับหลักความสงบและศีลธรรมอันดีของประชาชนได้ ซึ่งถือเป็นภัยคุกคามต่อความปลอดภัยในการคุ้มครองข้อมูลส่วนบุคคลด้วย พร้อมทั้งขัดกับหลักการประมวลผลต้องมีความโปร่งใสและชอบด้วยกฎหมาย อย่างไรก็ดีแม้ในประกาศธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market conduct) จะมีหลักเกณฑ์ในเรื่องการเปิดเผยข้อมูลลูกค้าให้แก่บุคคลอื่น แต่ก็มิได้มีการห้ามการซื้อขายหรือการเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการหรือลูกค้าไว้โดยตรง มีเพียงกำหนดว่าจะมีการดูแลรักษาความปลอดภัยเพื่อป้องกันเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบเท่านั้น ซึ่งจะทำให้ถ้ามีการกระทำใดเป็นการเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการค้าหรือแสวงหาผลประโยชน์อื่น โดยจากความยินยอมของเจ้าของข้อมูลก็จะสามารถกระทำได้ ทำให้สถาบันทางการเงินต่าง ๆ ใช้ช่องทางตรงนี้หาผลประโยชน์ทางการค้าจากข้อมูลส่วนบุคคลได้

ปัญหาที่สามในการคุ้มครองข้อมูลชีวภาพคือ มาตรการรักษาความมั่นคงปลอดภัยในข้อมูลชีวภาพของสถาบันการเงิน ประเด็นแรกของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนดหน้าที่ในการจัดการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นหน้าที่ผู้ควบคุมข้อมูลส่วนบุคคล อยู่ในมาตรา 37 (1) และเป็นหน้าที่ของผู้ประมวลข้อมูลส่วนบุคคลในมาตรา 40 (2) ที่ทั้งสองต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ปัญหาประการแรกของมาตรการรักษาความมั่นคงปลอดภัย คือยังไม่มีมาตรการหรือกฎหมายทั้งในพระราชบัญญัติฉบับนี้หรือกฎหมายลำดับรองที่กำหนดถึงมาตรฐานขั้นต่ำในการรักษาความมั่นคงปลอดภัยควรมีหลักเกณฑ์เช่นไรที่ถือว่าเหมาะสมที่ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องดำเนินการในการจัดการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่อยู่ในการเก็บรักษาไว้

ต่อมาประเด็นที่สองในเรื่องมาตรการรักษาความมั่นคงปลอดภัยในข้อมูลชีวภาพของสถาบันการเงินคือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 นั้น ไม่มีการกำหนดถึงมาตรการทั้งด้านเทคนิคและทางด้านองค์กรเพื่อช่วยในการออกแบบความปลอดภัยในการคุ้มครองข้อมูลส่วนบุคคลให้มีความเหมาะสมกับแต่ละองค์กรหรือแต่ละหน่วยงานที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล อาจจะทำให้มีการปฏิบัติตามหน้าที่การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทั้งทางกายภาพและการบริหารจัดการ

ความปลอดภัยของข้อมูลส่วนบุคคล ไม่มีความครบถ้วนสมบูรณ์มีประสิทธิภาพเทียบเท่ามาตรฐานของประเทศอื่น ซึ่งจะส่งผลในปัญหาด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลประการต่อไป

ประเด็นสุดท้ายในเรื่องมาตรการรักษาความมั่นคงปลอดภัยในข้อมูลชีวภาพคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนี้มีการบัญญัติถึงข้อมูลชีวภาพแต่ก็ยังคุ้มครองในด้านความปลอดภัยที่ไม่เพียงพอเหมาะสมกับระดับความเสี่ยงของข้อมูลชีวภาพ โดยเมื่อเปรียบเทียบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ ไม่ว่าจะเป็น GDPR, BIPA, PIPL มีการบัญญัติให้ผู้ควบคุมข้อมูลต้องมีการประเมินความเสี่ยงและผลกระทบในข้อมูลที่มีความละเอียดอ่อนอย่างข้อมูลชีวภาพเป็นประจำ เพื่อประเมินถึงผลกระทบหรือการถูกละเมิดความเป็นส่วนตัวที่จะเกิดกับเจ้าของข้อมูลได้ การที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยไม่ได้กำหนดหน้าที่ในการประเมินความเสี่ยงในผลกระทบของข้อมูลชีวภาพให้แก่ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคล การคุ้มครองความมั่นคงปลอดภัยของข้อมูลชีวภาพจึงอาจอยู่ในเกณฑ์ที่ไม่ได้มาตรฐานเทียบเท่าสากลส่งผลต่อการคุ้มครองข้อมูลชีวภาพที่มีการประมวลจากลักษณะทางกายภาพของร่างกายและพฤติกรรมของเจ้าของข้อมูลส่วนบุคคล ทำให้มีความเสี่ยงในเรื่องความปลอดภัยมากกว่าข้อมูลส่วนบุคคลทั่วไป เพราะอาจจะก่อให้เกิดการกระทบต่อสิทธิทางร่างกายและเสรีภาพต่อเจ้าของข้อมูลโดยตรงได้มากกว่า ดังนั้น กฎหมายไม่มีมาตรการที่ชัดเจนและเหมาะสมกับความเสี่ยงนั้นทำให้กำหนดแนวทางป้องกันความเสี่ยงไม่มีความรัดกุมปลอดภัยไม่มีความเหมาะสมและมีประสิทธิภาพ

จากการศึกษาค้นคว้ามาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลที่เป็นข้อมูลชีวภาพของผู้ใช้บริการในสถาบันการเงิน ข้อเสนอแนะ คือ

1. ปัญหาความยินยอมในการเก็บรวบรวมข้อมูลชีวภาพ

สำหรับปัญหาในการเก็บรวบรวมข้อมูลชีวภาพจากเจ้าของข้อมูลส่วนบุคคล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ยังมีข้อที่ต้องปรับปรุงในหลายองค์ประกอบเพื่อให้หลักเกณฑ์ในการขอความยินยอมข้อมูลชีวภาพมีความชัดเจนและเจ้าของข้อมูลได้รับข้อมูลที่ถูกต้องและแน่นอนอยู่ในขอบเขต จึงขอเสนอแนวทางแก้ไขและปรับปรุง ดังนี้

1.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรค 3

กำหนดให้การขอความยินยอมมีการแจ้งวัตถุประสงค์การเก็บรวบรวมข้อมูลส่วนบุคคล ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเท่านั้นยังขาดองค์ประกอบเรื่องความเฉพาะเจาะจงของการขอความยินยอมและการแจ้งวัตถุประสงค์ ซึ่งเป็นองค์ประกอบที่สำคัญประการหนึ่งของความยินยอม เนื่องจากการแจ้งวัตถุประสงค์ถ้าไม่มีการบัญญัติกฎหมายไว้อย่างชัดเจน อาจทำให้ผู้ควบคุมข้อมูลแจ้งวัตถุประสงค์อย่างกว้าง และมีลักษณะไม่เฉพาะเจาะจงว่าการเก็บ รวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้นไปเกิดขอบเขตที่ไม่แน่นอนชัดเจน ทำให้เจ้าของข้อมูลส่วนบุคคลเกิดความสับสน เข้าใจผิด หรือได้ข้อมูลที่ไม่เพียงพอมิผลต่อการตัดสินใจให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคลได้ ดังนั้น เพื่อเจ้าของข้อมูลส่วนบุคคลที่ต้องให้ความยินยอมมี

ความเข้าใจถึงวัตถุประสงค์ในการเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลได้อย่างถูกต้อง มีความชัดเจนเฉพาะเจาะจง จึงขอเสนอแก้ไข มาตรา 19 วรรค 3 ดังนี้

ก่อนการแก้ไข

มาตรา 19 วรรค 3 ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้ง วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้น ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้ง ใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

แก้ไขเป็น

มาตรา 19 วรรค 3 ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์เป็นการเฉพาะเจาะจงในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อเป็นการกำหนดขอบเขตที่แน่นอนในการกระทำที่กระทำต่อข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ขอความยินยอมไป และการขอความยินยอมนั้น ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้ง ใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

แก้ไขเพิ่มเติมในรายละเอียดให้มีการแจ้งวัตถุประสงค์ที่มีลักษณะเฉพาะเจาะจงในการประมวลข้อมูล

1.2 ความยินยอมในการเก็บรวบรวมข้อมูลชีวภาพนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมาตรา 26 บัญญัติห้ามมิให้มีการเก็บรวบรวมห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลที่เกี่ยวกับข้อมูลชีวภาพโดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลเท่านั้นยังขาดความชัดเจนในเรื่องลักษณะของการขอความยินยอม การแจ้งวัตถุประสงค์และลักษณะของข้อมูลชีวภาพที่ต้องการเก็บรวบรวม ทำให้การขอความยินยอมในการเก็บรวบรวมข้อมูลชีวภาพตามมาตรา 26 วรรค 2 ไม่ได้มีหลักเกณฑ์ในเรื่องข้อมูลที่ควรระบุในการการขอความยินยอมในการเก็บรวบรวมข้อมูลชีวภาพ รวมทั้งไม่มีการให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งถึงวัตถุประสงค์หรือการขอความยินยอมที่เป็นการเฉพาะเจาะจงถึงประเภทและลักษณะของข้อมูลชีวภาพที่จะขอความยินยอม เพราะ ดังที่กล่าวมาแล้วว่าข้อมูลชีวภาพนั้นมีหลากหลายประเภทชนิด และเป็นข้อมูลที่มีความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลไม่ใช้วัตถุประสงค์ในการเก็บรวบรวมข้อมูลชีวภาพแบบกว้าง หรือเป็นการขอความยินยอมแบบเหมารวมในข้อมูลชีวภาพทุกประเภท และนำข้อมูลชีวภาพไปประมวลผลเท่าที่จำเป็นและมีความโปร่งใสในการใช้ข้อมูลชีวภาพ ดังนั้น เพื่อเป็นการคุ้มครองเจ้าของข้อมูลชีวภาพให้มีประสิทธิภาพมากขึ้น ในการขอความ

ยินยอมในการเก็บรวบรวมข้อมูลชีวภาพควรกำหนดถึงให้มีการแจ้งวัตถุประสงค์เป็นการเฉพาะในการเก็บรวบรวมข้อมูลชีวภาพ โดยมีการระบุถึงประเภทหรือลักษณะของข้อมูลชีวภาพที่ต้องการเก็บรวบรวมและควรแยกออกจากการขอความยินยอมข้อมูลละเอียดอ่อนอื่น ๆ ด้วยเพื่อความชัดเจนให้เจ้าของข้อมูลมีอิสระในการตัดสินใจเลือกมากขึ้นพร้อมทั้งได้รับข้อมูลที่มีถูกต้อง โปร่งใส และมีขอบเขตแน่นอนเฉพาะเจาะจงมากขึ้น ด้วย ผู้วิจัยจึงเห็นว่าควรมีการปรับปรุงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยการเพิ่ม มาตรา 26/1 ดังนี้

มาตรา 26/1 ความยินยอมในการเก็บรวบรวมข้อมูลชีวภาพตามมาตรา 26 นั้น ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์เป็นการเฉพาะเจาะจง พร้อมทั้งระบุถึงประเภทหรือชนิดของข้อมูลชีวภาพที่ต้องการเก็บรวบรวมตามวัตถุประสงค์โดยคำนึงถึงเทคโนโลยีใหม่ ๆ ที่เกี่ยวกับข้อมูลชีวภาพด้วย และการขอความยินยอมเก็บรวบรวมข้อมูลชีวภาพนี้ต้องแยกส่วนออกจากความยินยอมอื่น ๆ อย่างชัดเจน

2. ปัญหาการนำข้อมูลชีวภาพที่ถูกเก็บรวบรวมอยู่ในสถาบันการเงินไปเปิดเผยเพื่อวัตถุประสงค์ทางการค้า

การที่ข้อมูลส่วนบุคคลที่เป็นข้อมูลชีวภาพนั้นไปเปิดเผยไม่ว่าด้วยวัตถุประสงค์ใดก็ตาม โดยหลักจะกระทำมิได้ เว้นแต่กฎหมายให้อำนาจไว้ ซึ่งถือเป็นการละเมิดที่เป็นภัยคุกคามต่อความปลอดภัยของข้อมูลส่วนบุคคล ทั้งนี้ ถ้าการเปิดเผยนั้นเป็นไปเพื่อวัตถุประสงค์ทางการค้า เช่น การซื้อขาย เช่าซื้อ หรือเปิดเผยเพื่อนำไปแสวงหาประโยชน์อันมิชอบโดยเฉพาะอย่างยิ่ง สถาบันการเงินของไทยนั้นถือได้ว่าเป็น Big Data ขนาดใหญ่ที่มีการเก็บรวบรวมข้อมูลชีวภาพไปใช้ในการยืนยันตัวตนของผู้ใช้บริการ ทำให้มีความเสี่ยงสูงที่ข้อมูลชีวภาพจะถูกนำไปเปิดเผยต่อบุคคลที่สามได้ สถาบันทางการเงินของไทยควรมีข้อกำหนดที่เข้มงวดมากขึ้นห้ามนำข้อมูลชีวภาพไปเปิดเผยเพื่อวัตถุประสงค์ทางการค้าหรือเพื่อแสวงหาผลประโยชน์ใด ๆ จึงเสนอแนวทางแก้ไข ดังนี้

2.1 สำหรับการเปิดเผยข้อมูลส่วนบุคคลนั้นตามมาตรา 27 ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 นั้นวางหลักว่าห้ามมิให้มีการใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม เว้นแต่เหตุหรือฐานอื่นซึ่งกฎหมายกำหนดให้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ซึ่งในมาตรา 27 เป็นการบัญญัติถึงการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลที่เป็นมาตรฐานขั้นต่ำของหลักการคุ้มครองข้อมูลส่วนบุคคล แต่สำหรับข้อมูลชีวภาพนั้นเป็นข้อมูลที่มีความละเอียดอ่อน โดยมีความเสี่ยงสูงที่กระทบต่อสิทธิเสรีภาพต่อเจ้าของข้อมูลส่วนบุคคล ดังนั้น การข้อมูลส่วนบุคคลควรที่จะมีมาตรการทางกฎหมายที่เคร่งครัด รัดกุม และมีความโปร่งใสมากกว่าข้อมูลส่วนบุคคลทั่วไป เฉพาะอย่างยิ่ง การเปิดเผย ส่งต่อ ขาย หรือเช่าซื้อให้บุคคลที่สามเพื่อใช้ในวัตถุประสงค์ทางการค้า ควรมีการบัญญัติห้ามให้กระทำไว้อย่างชัดเจนว่าเป็นการกระทำที่มิชอบด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคล ผู้ศึกษาจึงขอเสนอแก้ไขมาตรา 27 วรรค 1 ดังนี้

ก่อนแก้ไข

มาตรา 27 วรรค 1 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้น ไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

แก้ไขเป็น

มาตรา 27 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้น ไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

สำหรับข้อมูลชีวภาพตามมาตรา 26 ห้ามมิให้มีการขาย เช่า ส่งต่อหรือเปิดเผยข้อมูลชีวภาพเพื่อวัตถุประสงค์ทางการค้ากับบุคคลที่สาม เว้นแต่จะมีกฎหมายบัญญัติให้กระทำได้

2.2 สำหรับสถาบันการเงินนั้นแม้จะมีประกาศของธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม หรือ Market Conduct ที่แม้มีการกำหนดให้มีการดูแลข้อมูลส่วนบุคคลของลูกค้าให้เป็นความลับ มีความมั่นคงปลอดภัยอย่างรัดกุม ให้มีการเก็บข้อมูลลูกค้าเท่าที่จำเป็นและใช้ข้อมูลตามวัตถุประสงค์ที่ได้แจ้ง แต่อย่างไรควรมีการเพิ่มเติมในการห้ามมิให้สถาบันการเงินต่าง ๆ ที่อยู่ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย มีการขาย ให้เช่า ส่งต่อ หรือเปิดเผยข้อมูลชีวภาพของลูกค้าเพื่อวัตถุประสงค์ทางการค้า โดยเป็นการป้องกันการแสวงหาผลประโยชน์จากข้อมูลชีวภาพที่สถาบันการเงินเก็บรวบรวมจากลูกค้าผู้ใช้บริการ และเป็นการสร้างความเชื่อมั่นไว้วางใจให้แก่ลูกค้าที่ได้ให้ความยินยอมในการเก็บรวบรวมข้อมูลชีวภาพของตนเองแก่ทางสถาบันการเงินด้วย

3. ปัญหาการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลชีวภาพของสถาบันการเงิน

การรักษาความมั่นคงปลอดภัยของข้อมูลเป็นหนึ่งในหลักการพื้นฐานที่สำคัญของการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลมีหน้าที่ในการดูแลรักษาความปลอดภัยให้เหมาะสม เพื่อป้องกันมิให้ข้อมูลส่วนบุคคลถูกละเมิดหรือมีภัยคุกคามที่ทำให้ข้อมูลส่วนบุคคลสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ ในการที่ผู้ควบคุมข้อมูลเป็นสถาบันการเงินการรักษาความปลอดภัยของข้อมูลของผู้ใช้บริการก็ต้องมีความเข้มงวดและรัดกุมมากยิ่งขึ้นด้วย สำหรับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ ได้กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมอยู่ในมาตรา 37 (1) และมาตรา 40 (2) จากการศึกษาปัญหานี้ ผู้ศึกษาเสนอการแก้ไขและปรับปรุงดังนี้

3.1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลควรในการกำหนดมาตรฐานขั้นต่ำของมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมนั้น มิควรใช้มาตรฐานเดียวกันในทุกองค์กรหรือทุกหน่วยงาน แต่ละองค์กรก็มีขนาดของการเก็บรักษาข้อมูลที่แตกต่างกันหรือเก็บข้อมูลส่วนบุคคลคนละ

ประเภท ดังนั้น มาตรการนั้นควรมีมาตรฐานที่แตกต่างกันในข้อมูลส่วนบุคคลแต่ละประเภทให้สอดคล้องกับความเสี่ยงด้านความปลอดภัย สิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลทุกกลุ่ม ปริมาณของข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม ค่าใช้จ่าย และเทคโนโลยีที่เปลี่ยนแปลงตลอดเวลา โดยเฉพาะข้อมูลชีวภาพที่ปัจจุบันในเป็นที่นิยมมาใช้อย่างแพร่หลายควรมีการกำหนดมาตรการที่เข้มงวดมากกว่าข้อมูลทั่วไป เนื่องจากมีความเสี่ยงสูงที่จะกระทบต่อสิทธิเสรีภาพของข้อมูลส่วนบุคคลเนื่องจากเป็นข้อมูลที่ระบุตัวตนและพฤติกรรมของเจ้าของข้อมูลได้อย่างแม่นยำและไม่สามารถเปลี่ยนแปลงได้

3.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) และมาตรา 40 (2) กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ควรมีการระบุเพิ่มดังนี้ ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่จัดให้มีมาตรการมีทางเทคนิคและทางองค์กรที่เหมาะสมสอดคล้องกับมาตรการความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล คือ การเข้ารหัสไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

3.3 กำหนดหน้าที่ของผู้ควบคุมในการที่ต้องประเมินผลกระทบของข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคลเป็นประจำ โดยเฉพาะข้อมูลชีวภาพนั้นกฎหมายต้องกำหนดอย่างชัดเจนว่าต้องมีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลโดยไม่มีข้อยกเว้น เพื่อจัดการในความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลและกำหนดมาตรฐานได้อย่างเหมาะสม

3.4 ธนาคารแห่งประเทศไทยควรมีการจัดทำแนวนโยบายด้านการรักษาความปลอดภัยของข้อมูลชีวภาพให้สอดคล้องกับมาตรฐานสากลโดยมีมาตรฐานที่สูงกว่าที่ระบุไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อใช้เป็นแนวทางของสถาบันการเงินภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทยให้มีมาตรการการรักษาความปลอดภัยของข้อมูลชีวภาพและเหมาะสมกับกิจการของสถาบันการเงิน เพราะแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometrics) ในการให้บริการทางการเงินที่ออกมาก่อนหน้านั้นนั้นอาจจะไม่เพียงพอสำหรับการป้องกันหรือรักษาความปลอดภัยของข้อมูลชีวภาพที่ถูกเก็บรักษาอยู่ในสถาบันการเงิน

เอกสารอ้างอิง

คณะรป ทอกรวิวงศ์.คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล.

กรุงเทพมหานคร.นิติธรรม, 2564.

นคร เสรีรักษ์ ,ความเป็นส่วนตัว,กรุงเทพมหานคร: พี.เพรส, 2557.

ปิยะบุตร บุญอร่ามเรือง, พัฒนาพร โกวิทพัฒนกิจ, พีรพัฒน์ โชคสุวัฒน์สกุล,เสกศิริ นิวัติชัยวงศ์,

ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร, จุติรัตน์ ทิพย์สัมฤทธิ์กุล, ภูมิศิริ คำรงวุฒิ,
โมกซ์พิศุทธิ์ รัตนารุณ. **Thailand Data Protection Guidelines 3.0: แนวปฏิบัติเกี่ยวกับการ**
คุ้มครองข้อมูลส่วนบุคคล Final Version 3.0, พิมพ์ครั้งที่ 1. กรุงเทพฯ:จุฬาลงกรณ์มหาวิทยาลัย,

2563.