บทที่ 4

บทวิเคราะห์ปัญหาทางกฎหมายเกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย

4.1 ปัญหาเรื่องการสร้างความมั่นใจให้ผู้บริโภคในการใช้บริการและการทำธุรกรรมที่เกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์

ในปัจจุบันลูกค้าของธนาคารจะมีทางเลือกมากมายที่จะใช้บริการหรือทำธุรกรรมของธนาคารพาณิชย์จากที่ใดก็ได้ในโลกนี้ โดยไม่จำเป็นต้องเดินทางไปที่ธนาคารหรือสาขาของธนาคารเหมือนในอดีต อีกทั้งสามารถใช้บริการหรือธุรกรรมในเวลาใด ๆ ก็ได้ โดยไม่จำเป็นต้องคำนึงว่าเป็นวันหยุด หรือเป็นเวลาทำการของธนาคารหรือไม่ โดยลูกค้าสามารถใช้บริการธนาคารพาณิชย์อิเล็กทรอนิกส์ต่าง ๆ ของธนาคาร เช่น การเบิกถอนเงินหรือโอนเงินจากตู้กดเงินสดอัตโนมัติ (ATMs) ของธนาคาร, การทำธุรกรรมชำระค่าสินค้าและบริการจากโทรศัพท์มือถือ (Mobile Phone Banking) เป็นต้น

ทั้งนี้ รูปแบบของธนาคารพาณิชย์อิเล็กทรอนิกส์ที่ได้รับความนิยมมากที่สุดในปัจจุบัน ก็คือ ธนาคารทางอินเตอร์เน็ท (Internet Banking) ซึ่งในปัจจุบันธนาคารพาณิชย์หลักในประเทศไทยต่างก็มีการให้บริการต่าง ๆ ของธนาคารแก่ลูกค้าครบถ้วนเสมือนว่าลูกค้าได้ไปใช้บริการหรือทำธุรกรรมต่าง ๆ เหล่านั้นที่ทำการของธนาคารเลยทีเดียว ไม่ว่าจะเป็นการเช็คยอดบัญชี, การโอนเงิน, การชำระค่าสินค้าหรือบริการ ฯลฯ

แต่ถึงอย่างไรก็ตาม การใช้บริการหรือการทำธุรกรรมกับธนาคารพาณิชย์อิเล็กทรอนิกส์ในประเทศไทยนั้น ก็ยังคงมีอัตราส่วนที่น้อยอยู่ดี เมื่อเทียบกับปริมาณการใช้บริการและการทำธุรกรรมทั้งหมดของลูกค้ากับธนาคาร ซึ่งก็เป็นไปในทิศทางเดียวกันกับธุรกรรมทางพาณิชย์อิเล็กทรอนิกส์อื่น ๆ ที่ยังไม่สามารถสร้างความเชื่อมั่นได้มากพอที่จะทำให้ผู้บริโภคหันมาใช้บริการหรือทำธุรกรรมต่าง ๆ ทางอิเล็กทรอนิกส์แทน

4.1.1 ปัจจัยที่มีผลต่อความมั่นใจของผู้บริโภคในการใช้บริการและการทำธุรกรรมที่เกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์

สำหรับปัจจัยที่มีผลต่อความมั่นใจของผู้บริโภคในการใช้บริการหรือทำธุรกรรมที่เกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์ และเป็นอุปสรรคที่ทำให้ธุรกรรมทางพาณิชย์

อิเล็กทรอนิกส์ยังไม่สามารถเติบโตได้เท่าที่ควรนั้นอาจจะมีอยู่หลายปัจจัยด้วยกัน เช่น พฤติกรรมการซื้อสินค้าของประชาชนชาวไทยยังต้องการที่จะเห็นและจับต้องสินค้าก่อนที่จะจ่ายเงินมากกว่าที่จะเห็นในภาพแล้วตัดสินใจซื้อ, ปัญหาด้านโครงสร้างพื้นฐานของเทคโนโลยีการเข้าถึงเทคโนโลยีของประชาชนยังไม่เพียงพอ, ปัญหาเรื่องการชำระเงินที่ส่วนใหญ่จะต้องใช้บัตรเครดิต แต่จำนวนประชากรที่มีบัตรเครดิตในประเทศไทยยังนับว่าน้อยอยู่ทำให้การแข่งขันและการลงทุนในด้านพาณิชย์ยังไม่คึกคักเท่าที่ควร เป็นต้น

แต่ปัจจัยหลักที่มีผลกระทบและเป็นอุปสรรคต่อการใช้บริการหรือทำธุรกรรมพาณิชย์อิเล็กทรอนิกส์ คือ

(1) ความปลอดภัยของข้อมูลส่วนบุคคล

ปัจจัยสำคัญอย่างหนึ่งที่มีผลกระทบต่อความเชื่อมั่นของผู้บริโภคในการใช้บริการและทำธุรกรรมทางอิเล็กทรอนิกส์กับธนาคารพาณิชย์อิเล็กทรอนิกส์ ก็คือ ความไม่มั่นใจในความปลอดภัยในการทำธุรกรรมผ่านระบบอิเล็กทรอนิกส์ ซึ่งจะเห็นได้จากข่าวต่าง ๆ เกี่ยวกับการกระทำผิดในการละเมิดสิทธิและอาชญากรรมอื่น ๆ บนอินเตอร์เน็ท เช่น เวลาสั่งซื้อสินค้าจะต้องใช้หมายเลขบัตรเครดิตและการบันทึกข้อมูลส่วนตัวไว้ แต่หากเจ้าของไม่ได้สั่งซื้อสินค้าหรือสั่งซื้อไปเพียงรายการเดียวแต่มีการโจรกรรมข้อมูลบัตรไปซื้อของ แล้วมีใบเรียกชำระเงินมาจำนวนมากหรือชำระเงินแล้วจะได้สินค้าหรือไม่ เป็นต้น

นอกจากนี้ การหลอกลวงอีกวิธีที่ลูกค้าของธนาคารมักตกเป็นเหยื่อของคนร้ายก็คือ Phishing Mail ซึ่งกระบวนการ Phishing Mail นั้น คนร้ายจะทำการส่งอีเมล์หรือข้อความที่อ้างว่ามาจากธนาคารที่เราเป็นลูกค้าอยู่ โดยการส่งข้อความนั้นเป็นการขอให้ลูกค้า "อัพเดท" หรือ "ยืนยัน" ข้อมูลบัญชีของตัวเอง ซึ่งคนร้ายมักจะเขียนขู่ลูกค้าเอาไว้ว่า หากลูกค้าไม่ตอบกลับอีเมล์ดังกล่าว อาจก่อให้เกิดผลเสียตามมาได้ และเพื่อให้อีเมล์ปลอมที่ส่งมานั้นดูสมจริง ผู้ส่งอีเมล์ลวงนี้จะใส่ hyperlink ที่อีเมล์ เพื่อให้เหมือนกับ URL ขององค์กรนั้น ๆ จริง ซึ่งแท้ที่จริงแล้วมันคือเว็บไซต์ปลอม หรือหน้าต่างที่สร้างขึ้น หรือที่เราเรียกว่า "เว็บไซต์ปลอมแปลง" (Spoofed Website) เมื่อลูกค้าที่ถูกหลอกได้เข้าสู่เว็บไซต์ปลอมเหล่านี้ ก็อาจจะถูกล่อลวงให้กรอกข้อมูลส่วนตัวที่จะถูกส่งไปยังผู้ผลิตเว็บไซต์ลวงเหล่านี้ เพื่อนำข้อมูลของท่านไปใช้ประโยชน์ เช่น ซื้อสินค้า สมัครบัตรเครดิต หรือแม้แต่ทำสิ่งผิดกฎหมายอื่น ๆ ในนามของลูกค้านั่นเอง

(2) ผลทางกฎหมายของการทำธุรกรรมทางอิเล็กทรอนิกส์

อีกปัจจัยหนึ่งที่มีผลอย่างมากต่อความมั่นใจของผู้บริโภคในการตัดสินใจใช้บริการหรือเข้าทำธุรกรรมกับธนาคารพาณิชย์อิเล็กทรอนิกส์ ก็คือ การที่ผู้บริโภคยังไม่มีความมั่นใจการทำธุรกรรมทางอิเล็กทรอนิกส์นั้น กฎหมายรับรองผลของการทำมากน้อยเพียงใด เช่น ในกรณีของการ

ลงลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) ที่แม้ในพระราชบัญญัติว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์จะรับรองผลก็ตาม แต่ลายมือชื่ออิเล็กทรอนิกส์ที่ได้รับการยอมรับในระบบสากลนั้นก็คือลายมือชื่ออิเล็กทรอนิกส์ที่มีการออกใบรับรอง (Digital Certificate) ซึ่งในประเทศไทยก็เริ่มมีหน่วยงานหรือองค์กรที่เปิดให้บริการแล้ว แต่กฎหมายที่จะควบคุมหรือกำกับดูแลธุรกิจการให้บริการออกใบรับรองดังกล่าวก็ยังไม่เกิดขึ้น

4.1.2 บทวิเคราะห์ปัญหาทางกฎหมายที่มีผลต่อความมั่นใจของผู้บริโภคในการใช้บริการและการธุรกรรมที่เกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์

ในปัจจุบันจำนวนผู้ใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์กับธนาคารพาณิชย์ในประเทศไทยนั้นถึงแม้จะมีปริมาณเพิ่มมากขึ้น แต่ก็ยังถือว่าน้อยมากเมื่อเทียบกับประเทศที่เป็นศูนย์กลางทางการเงินอื่น ๆ เช่น สหรัฐอเมริกา, อังกฤษ, ฮ่องกง, สิงคโปร์ ฯลฯ ซึ่งปัญหาที่เป็นอุปสรรคนั้นอาจจะเกิดได้จากหลายสาเหตุด้วยกัน เช่น ปัญหาด้านโครงสร้างพื้นฐาน ซึ่งมีความไม่เท่าเทียมกันของการเข้าถึงบริการโครงสร้างโทรคมนาคมพื้นฐานของภาครัฐระหว่างคนในกรุงเทพและต่างจังหวัด, ปัญหาด้านการใช้อินเตอร์เน็ท ที่แม้ว่าการใช้อินเตอร์เน็ทของไทยจะขยายตัวมากขึ้นแต่การพัฒนาอินเตอร์เน็ทเชิงการค้าของไทยยังคงอยู่ในระดับต่ำกว่าที่ควรจะเป็น, ปัญหาด้านบุคลากร ที่ไม่สามารถพัฒนาบุคลากรไอทีของสถาบันการศึกษาต่าง ๆ ในประเทศไม่เพียงพอกับความต้องการของตลาดที่ขยายตัวอย่างรวดเร็ว เป็นต้น

แต่ทั้งนี้ ปัญหาที่เป็นปัญหาสำคัญอีกประการหนึ่งก็คือ ความไม่มั่นใจในเรื่องความปลอดภัยของข้อมูลส่วนบุคคลที่ส่วนหนึ่งอาจจะถูกกลุ่มคนผู้ไม่หวังดีโจรกรรมหรือหลอกลวงเอาไปและอีกส่วนหนึ่งอาจจะถูกธนาคารพาณิชย์ที่ใช้บริการหรือทำธุรกรรมนั้นเอาไปใช้ประโยชน์อย่างอื่นนอกจากที่ได้แจ้งให้ทราบในครั้งแรกก็เป็นได้ ซึ่งในส่วนของกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลนั้นในปัจจุบันมีกฎหมาย 3 ฉบับที่เกี่ยวข้อง ได้แก่

1) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

2) พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

3) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ในส่วนของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 นั้น ได้ให้นิยามของคำว่า "ข้อมูลข่าวสารส่วนบุคคล" ในมาตรา 4 ว่าหมายถึง “ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติ อาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่น ที่ทำให้รู้ตัวผู้นั้นได้ เช่น

ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับ สิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย” ซึ่งในหมวด 3 ตั้งแต่มาตรา 21 ถึง 25 ได้กำหนดหน้าที่ในการจัดเก็บข้อมูล และสิทธิในการเปิดเผยข้อมูลส่วนบุคคล เฉพาะของหน่วยงานรัฐเท่านั้น โดยไม่ได้รวมถึงข้อมูลส่วนบุคคลที่อยู่ภาคชน

สำหรับพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 มีจุดกำเนิดมาจากการที่สถาบันการเงินต่าง ๆ รวมถึงธนาคารพาณิชย์ด้วยนั้น ไม่มีข้อมูลเกี่ยวกับฐานะทางการเงินและประวัติการชำระหนี้ของลูกค้าอย่างเพียงพอ จึงมีการผลักดันให้เกิดแนวคิดที่จะให้มีการแลกเปลี่ยนข้อมูลของลูกค้ากันระหว่างสถาบันการเงินด้วยกันเอง เพื่อช่วยในการพิจารณาทางฐานะการเงินและประวัติการชำระหนี้ของลูกค้า ดังนั้นรัฐบาลจึงได้ผลักดันให้มีการร่างพระราชบัญญัติฉบับนี้ขึ้นเพื่อสนับสนุนให้มีการประกอบธุรกิจข้อมูลเครดิต โดยมีการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการทำธุรกรรมข้อมูลเครดิตเอาไว้ด้วย เพื่อเป็นการคุ้มครองประชาชนผู้เป็นเจ้าของข้อมูล

ทั้งนี้ ในมาตรา 3 ของพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิตฉบับดังกล่าวได้ให้นิยามของคำว่า “ข้อมูลเครดิต” ว่า หมายถึง ข้อเท็จจริงเกี่ยวกับลูกค้าที่ขอสินเชื่อ ดังต่อไปนี้

1) ข้อเท็จจริงที่บ่งชี้ถึงตัวลูกค้า และคุณสมบัติของลูกค้าที่ขอสินเชื่อ

(ก) กรณีบุคคลธรรมดา หมายถึง ชื่อ ที่อยู่ วันเดือนปีเกิด สถานภาพ การสมรส อาชีพ เลขที่บัตรประจำตัวประชาชน หรือบัตรประจำตัวเจ้าหน้าที่ของรัฐ หรือหนังสือเดินทาง และเลขประจำตัวผู้เสียภาษีอากร (ถ้ามี)

(ข) กรณีนิติบุคคล หมายถึง ชื่อ สถานที่ตั้ง เลขที่ทะเบียนการจัดตั้งนิติบุคคลหรือเลขประจำตัวผู้เสียภาษีอากร

2) ประวัติการขอ และการได้รับอนุมัติสินเชื่อ และการชำระสินเชื่อของลูกค้าที่ขอสินเชื่อรวมทั้งประวัติการชำระราคาสินค้าหรือบริการโดยบัตรเครดิต

และยังให้นิยาม “ข้อมูลห้ามจัดเก็บ” หมายความว่า ข้อมูลของบุคคลธรรมดาที่ไม่เกี่ยวกับการรับบริการ การขอสินเชื่อ หรือที่มีผลกระทบต่อความรู้สึกหรืออาจก่อให้เกิดความเสียหายหรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน ดังต่อไปนี้

1) ลักษณะพิการทางร่างกาย

2) ลักษณะทางพันธุกรรม

3) ข้อมูลของบุคคลที่อยู่ในกระบวนการสอบสวนหรือพิจารณาคดีอาญา

4) ข้อมูลอื่นใดตามที่คณะกรรมการประกาศกำหนด

ซึ่งจากคำนิยามของพระราชบัญญัติฉบับนี้จะเห็นได้ว่า แม้ว่าพระราชบัญญัติฉบับนี้จะให้ความคุ้มครองข้อมูลที่บ่งชี้ถึงตัวลูกค้าและข้อมูลเครดิตของลูกค้าที่ให้ไว้กับขอธนาคารหรือสถาบันการเงินก็ตาม แต่ก็เป็นการให้ความคุ้มครองเฉพาะในส่วนของลูกค้าที่ใช้บริการขอสินเชื่อจากธนาคารหรือสถาบันการเงินเท่านั้น ไม่ได้หมายความรวมถึงข้อมูลของลูกค้าที่ใช้บริการอื่น ๆ ของธนาคารแต่อย่างใด

และสำหรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มีผลบังคับใช้ตั้งแต่วันที่ 18 กรกฎาคม 2550 เป็นต้นมานั้น ก็เพื่อเป็นมาตรการที่ใช้ในการป้องกันและปราบปรามผู้ที่กระทำความผิดเกี่ยวกับเกี่ยวกับคอมพิวเตอร์ ไม่ว่าจะเป็นการกระทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ซึ่งทำให้รัฐสามารถลงโทษผู้ที่กระทำความผิดต่าง ๆ เช่น ผู้ที่ใช้ Phishing Mail เพื่อหลอกลวงเอาข้อมูลส่วนบุคคลของผู้อื่น หรือผู้ที่เจาะเข้าระบบคอมพิวเตอร์เพื่อเอาข้อมูลของบุคคลอื่นไปก็ตาม

ทั้งนี้ จะเห็นได้ว่าพระราชบัญญัติฉบับนี้มุ่งที่จะปราบปรามผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นการเฉพาะ โดยกำหนดหน้าที่ให้ผู้ให้ต้องมีหน้าที่ในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ด้วย เพื่อช่วยให้เจ้าหน้าที่ของรัฐสามารถดำเนินการกับผู้ที่กระทำความผิดได้เท่านั้น แต่พระราชบัญญัติฉบับดังกล่าวก็มิได้กล่าวถึงกรณีที่ผู้เข้าถึงข้อมูลในระบบคอมพิวเตอร์ได้โดยชอบ แต่ได้มีการนำข้อมูลของบุคคลไปใช้เพื่อประโยชน์ของตน แต่ไม่ได้ทำให้บุคคลผู้ถูกเอาข้อมูลไปต้องเสียหายแต่อาจจะทำให้เกิดความรำคาญได้ เช่น ในปัจจุบันที่ลูกค้าของธนาคาร หรือผู้ให้บริการหลาย ๆ ราย อาจจะเคยได้รับโทรศัพท์เข้ามาขายประกัน หรือเสนอสินเชื่อให้เป็นจำนวนมาก เป็นต้น

จะเห็นได้ว่า แม้ในปัจจุบันประเทศไทยจะมีกฎหมายที่สามารถนำมาปรับใช้กับการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์กับธนาคารพาณิชย์อยู่แล้วถึง 3 ฉบับก็ตาม **แต่ผู้เขียนมีความเห็นว่า กฎหมายทั้ง 3 ฉบับดังกล่าว ยังไม่เพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าธนาคารได้ในทุกกรณี เช่น กรณีที่เป็นลูกค้าที่ไม่ได้ขอสินเชื่อกับธนาคาร และธนาคารได้ให้ข้อมูลของลูกค้าดังกล่าวกับบริษัทขายประกัน หรือบริษัทผู้ให้บริการสินเชื่อส่วนบุคคล และบริษัทดังกล่าวได้ใช้ข้อมูลส่วนบุคคลดังกล่าว โทรศัพท์ หรือส่งอีเมล์เข้ามาขายประกัน หรือเสนอสินเชื่อให้แก่ลูกค้า ซึ่งอาจทำให้เกิดความรำคาญแก่ลูกค้าได้ ดังนั้นผู้เขียนเห็นว่า “รัฐควรจะมีการตรากฎหมาย**

“คุ้มครองข้อมูลส่วนบุคคล (Data Protection Law)” **เพื่อกำหนดหลักเกณฑ์ในการเก็บรวบรวม การใช้ การเปิดเผย การเก็บรักษา การแก้ไข และการโอนข้อมูลใช้ส่วนบุคคล ที่อยู่ในความครอบครองของหน่วยงานเอกชน โดยอาจมีการกำหนดให้มีการจัดตั้ง “คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” และ “สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” รวมทั้งกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลด้วย”**

ในส่วนของผลทางกฎหมายของการทำธุรกรรมทางอิเล็กทรอนิกส์กับธนาคารนั้น เราสามารถนำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาปรับใช้ได้เช่นเดียวกันกับทำธุรกรรมทางพาณิชย์อิเล็กทรอนิกส์อื่น ๆ โดยในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 7 – 8 [58] ได้กำหนดว่า ห้ามมิให้ปฏิเสธความผูกพันและผลทางกฎหมายด้วยเหตุเพราะการใช้ข้อมูลอิเล็กทรอนิกส์ รวมถึงรับรองการทำหลักฐาน หรือมีหลักฐานเป็นหนังสือที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ด้วย ซึ่งหลักดังกล่าวก็เป็นไปในทิศทางเดียวกันกับกฎหมายแม่แบบของคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติว่าด้วยพาณิชย์อิเล็กทรอนิกส์ (UNCITRAL Model Law on Electronic Commerce) มาตรา 6 ซึ่งได้บัญญัติไว้ว่า

“Article 6 Writing

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing

(3) The provisions of the article do not apply to the following : [...].”

---

[58] มาตรา 7 ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

มาตรา 8 ภายใต้บังคับบทบัญญัติแห่งมาตรา 9 ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว

นอกจากนี้ในส่วนของการลงลายมือชื่อนั้น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ มาตรา 9[59] ก็ได้รับรองให้การลงลายมือชื่อทางอิเล็กทรอนิกส์นั้นให้มีผลทางกฎหมายเช่นเดียวกับการลงลายมือชื่อตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 9 ที่ได้บัญญัติไว้ว่า “เมื่อมีกิจการอันใดซึ่งกฎหมายบังคับให้ทำเป็นหนังสือ บุคคลผู้จะต้องทำหนังสือไม่จำเป็นต้องเขียนเองแต่หนังสือนั้นจะต้องลงลายมือชื่อของบุคคลนั้น” ซึ่งก็เป็นไปในทิศทางเดียวกันกับกฎหมายแม่แบบ (UNCITRAL Model Law) เช่นกัน โดยมาตรา 7 ได้บัญญัติไว้ว่า

“Article 7 Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if :

(a) a method is used to identify that person and to indicate that person’s approval of the information contained in the data message ; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation of whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following : [...].”

โดยในส่วนของการลงลายมือชื่อทางอิเล็กทรอนิกส์ หมวดที่ 2 มาตรา 26 – 31 ยังได้บัญญัติเกี่ยวกับหลักเกณฑ์ของการลงลายมือชื่ออิเล็กทรอนิกส์เอาไว้อีกด้วย ซึ่งเป็นร่างตามแนวของกฎหมายแม่แบบของคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติว่า

---

[59] มาตรา 9 ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(2) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

ด้วยลายมือชื่ออิเล็กทรอนิกส์ (UNCITRAL Model Law on Electronic Signatures) ซึ่งได้กำหนดหลักเกณฑ์ของการลงลายมือชื่ออิเล็กทรอนิกส์ อีกทั้งยังได้พูดถึงการให้รับรองลายมือชื่ออิเล็กทรอนิกส์โดย ผู้ให้บริการออกใบรองอิเล็กทรอนิกส์ (Certification Authority) ซึ่งจะช่วยให้การการลงลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวได้รับความมั่นใจจากคู่สัญญาทั้งสองฝ่าย

อย่างไรก็ตาม แม้ในปัจจุบันพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 จะมีผลบังคับใช้มาตั้งแต่วันที่ 3 เมษายน 2545 แต่กลับไม่มีคดีที่เกี่ยวข้องกับธนาคารพาณิชย์อิเล็กทรอนิกส์ รวมทั้งการพาณิชย์อิเล็กทรอนิกส์ฟ้องร้องขึ้นสู่ศาลเลยแม้แต่คดีเดียว ซึ่งส่วนหนึ่งก็เกิดจากความไม่มั่นใจในการพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ ทั้ง ๆ ที่กฎหมายจะระบุให้การธุรกรรมทางอิเล็กทรอนิกส์นั้นมีผลผูกพันทางกฎหมาย โดยการทำเป็นหนังสือหรือลงลายมือชื่อในรูปข้อมูลอิเล็กทรอนิกส์นั้นก็มีผลทางกฎหมายเหมือนกับการทำเป็นหนังสือและลงลายมือชื่อตามประมวลกฎหมายแพ่งและพาณิชย์ทุกประการก็ตาม

ทั้งสาเหตุของความไม่มั่นใจในการพิสูจน์พยานหลักฐานของการทำธุรกรรมทางอิเล็กทรอนิกส์ส่วนหนึ่งนั้น อาจจะเกิดมาจากการความยากในการพิสูจน์ลายมือชื่ออิเล็กทรอนิกส์ตามมาตรา 26[60] ที่ได้บัญญัติเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ที่สามารถเชื่อถือได้เอาไว้ เพราะการ

---

[60] มาตรา 26 ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(1) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(2) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(3) การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้ และ

(4) ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

บทบัญญัติในวรรคหนึ่งไม่เป็นการจำกัดว่าไม่มีวิธีการอื่นใดที่แสดงได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หรือการแสดงพยานหลักฐานใดเกี่ยวกับความไม่น่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

ลงลายมือชื่อทางอิเล็กทรอนิกส์จะมีผลเหมือนกันกับลงลายมือชื่อตามปกตินั้น จะต้องแสดงให้เห็นถึงหน้าที่สำคัญ 5 ประการของการลงลายมือชื่อ คือ

(1) บ่งชี้ตัวผู้ลงลายมือชื่อ หรือ ชี้ว่าใครคือเจ้าของลายมือชื่อ

(2) แสดงความแท้จริงของเนื้อหาในเอกสาร

(3) เป็นพยานหลักฐาน

(4) เป็นการยืนยันว่าเอกสารดังกล่าวเป็นข้อตกลงขั้นสุดท้าย

(5) เป็นสิ่งที่ย้ำเตือนผู้ลงลายมือชื่อ หรือ คู่สัญญาว่า ตนมีหน้าที่ตามกฎหมายต้องปฏิบัติตามเนื้อหาที่ตกลงไว้ในเอกสาร

โดยเฉพาะในการบ่งชี้ตัวผู้ลงลายมือชื่อด้วยอุปกรณ์อิเล็กทรอนิกส์นั้นทำได้ยาก และอาจถูกลอกเลียน ปลอมแปลงได้ง่ายมาก ทำให้ในมาตรา 28 – 30 จึงได้วางหลักเกณฑ์ และเงื่อนไขของการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์เอาไว้ รวมทั้งยังได้มีการมีพูดถึงบริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์เอาไว้ด้วย ซึ่งหากพิจารณาตามบทบัญญัติแห่งกฎหมายนี้แล้วก็ดูเหมือนว่าไม่น่าจะมีปัญหาใด ๆ แต่เหมือนพิจารณาอย่างละเอียดแล้วจะพบว่าในมาตรา 29[61] ได้บัญญัติถึงการพิจารณาความเชื่อถือของระบบ วิธีการ และบุคคลากรของธุรกิจการให้บริการออกใบรับรองลายมือชื่ออิเล็กทรอนิกส์เอาไว้ โดยเฉพาะใน

---

[61] มาตรา 29 ในการพิจารณาความเชื่อถือได้ของระบบ วิธีการ และบุคลากรตามมาตรา 28 (6) ให้คำนึงถึงกรณีดังต่อไปนี้

(1) สถานภาพทางการเงิน บุคลากร และสินทรัพย์ที่มีอยู่

(2) คุณภาพของระบบฮาร์ดแวร์และซอฟต์แวร์

(3) วิธีการออกใบรับรอง การขอใบรับรอง และการเก็บรักษาข้อมูลการให้บริการนั้น

(4) การจัดให้มีข้อมูลข่าวสารเกี่ยวกับเจ้าของลายมือชื่อ ที่ระบุในใบรับรองและผู้ที่อาจคาดหมายได้ว่าจะเป็นคู่กรณีที่เกี่ยวข้อง

(5) ความสม่ำเสมอและขอบเขตในการตรวจสอบโดยผู้ตรวจสอบอิสระ

(6) องค์กรที่ให้การรับรองหรือให้บริการออกใบรับรองเกี่ยวกับการปฏิบัติหรือการมีอยู่ของสิ่งที่กล่าวมาใน (1) ถึง (5)

(7) กรณีใด ๆ ที่คณะกรรมการประกาศกำหนด

มาตรา 29 (6) ได้กล่าวถึงองค์กรที่ให้รับรองหรือให้บริการออกใบรับรองดังกล่าวเอาไว้ ซึ่งปัญหาที่พบในปัจจุบันก็คือ องค์กรที่ได้รับการรองหรือน่าเชื่อถือนั้น คือ องค์กรใด ใครจะเป็นผู้พิจารณา

ดังนั้น ในปัญหาการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์นี้ **ผู้เขียนเห็นว่า ประเทศไทยควรจะมีกฎหมายที่มีความชัดเจนเกี่ยวกับการองค์กรที่จะมากำกับดูแลธุรกิจบริการการให้บริการออกใบรับรองอิเล็กทรอนิกส์** (Certification Authority: CA) **โดยรัฐควรจะตรากฎหมายที่บัญญัติเกี่ยวกับ หลักเกณฑ์ ข้อกำหนด หรือเงื่อนไข ของผู้ที่ประสงค์จะให้ประกอบธุรกิจให้บริการออกใบรับรองลายมือชื่ออิเล็กทรอนิกส์ รวมทั้งรัฐควรมีส่วนในการจัดตั้งองค์กรหรือหน่วยงานที่มีความน่าเชื่อถือจะเข้ามากำกับดูแลธุรกิจประเภทดังกล่าวด้วย**

4.2 ปัญหาเรื่องมาตรฐานความมั่นคงปลอดภัยในการประกอบธุรกรรมที่เกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์

4.2.1 มาตรฐานความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

(1) **มาตรฐานขั้นต่ำของระบบ** ITMX – Interbank Transaction Management and Exchange

สำหรับประเทศไทย ธนาคารแห่งประเทศไทยได้กำหนดนโยบายทิศทางการชำระเงินของประเทศและกำหนดมาตรฐานเทคโนโลยีที่เหมาะสม โดยได้กำหนดให้มีการพัฒนาและดำเนินการระบบ ITMX (Interbank Transaction Management and Exchange) ขึ้น เพื่อเป็นโครงสร้างพื้นฐานของระบบการชำระเงินและโอนเงินระหว่างธนาคาร เพื่อรองรับธุรกรรมทางพาณิชย์อิเล็กทรอนิกส์ที่มีเพิ่มขึ้นในปัจจุบัน

ทั้งนี้ ธนาคารแห่งประเทศไทยได้ออกประกาศธนาคารแห่งประเทศไทย เรื่อง ข้อกำหนดและเงื่อนไขของระบบ ITMX (Interbank Transaction Management and Exchange) ขึ้น โดยในส่วนของมาตรฐานการรักษาความปลอดภัยและความน่าเชื่อถือของระบบงานและระบบเครือข่ายที่ให้บริการของ ITMX นั้น ธนาคารแห่งประเทศไทยได้กำหนดหลักเกณฑ์ขั้นต่ำไว้ เช่น ด้านความปลอดภัยด้านเครือข่าย (Network Interconnection Security) ได้กำหนดว่า เครือข่ายที่ใช้สำหรับรองรับการเชื่อมโยงกับสมาชิก ITMX เท่านั้น ต้องไม่มีการเชื่อมโยงโดยตรงเข้าสู่ระบบอินเตอร์เน็ททั้งด้าน ITMX และด้านสมาชิก รวมทั้งมีระบบหรืออุปกรณ์ในการป้องกันความปลอดภัยบนเครือข่ายการรับส่งข้อมูล และการเข้าใช้ระบบที่เชื่อถือได้

หรือในส่วนของความปลอดภัยของระบบคอมพิวเตอร์ (System Security) ในประกาศฉบับนี้ก็ได้กำหนดหลักเกณฑ์และเงื่อนไขไว้ ดังนี้

1) ควรมีกระบวนการเสริมความแข็งแกร่งของระบบ (System Hardening) และมีการตรวจสอบโดยทีมงานที่ไม่มีส่วนเกี่ยวข้องกับการติดตั้ง ซึ่งได้รับการยอมรับจากผู้บริหารระบบ ITMX เพื่อให้การรับรองความปลอดภัยของระบบก่อนนำไปติดตั้ง และใช้งานในสภาวะแวดล้อมสำหรับการปฏิบัติงานจริง (Production Environment)

2) ควรกำหนดระยะเวลาตรวจสอบสิทธิของผู้ใช้งานและบริการต่าง ๆ ที่จำเป็น พร้อมทั้งมีการทดสอบความปลอดภัยของระบบอย่างสม่ำเสมอ

3) ควรมีการจัดหาเครื่องมือที่ใช้ตรวจจับผู้บุกรุกระบบ (Intrusion Detection System: IDS) และควรมีการกำหนดให้มีการตรวจสอบความปลอดภัยของระบบอย่างอัตโนมัติ

4) ควรติดตามเหตุการณ์เกี่ยวกับความปลอดภัย เพื่อ Upgrade Patch ที่ปิดช่องโหว่ของซอฟต์แวร์ที่ใช้งาน

นอกจากนี้ประกาศฉบับนี้ยังได้กำหนดมาตรฐานการควบคุมความปลอดภัยของระบบ ITMX ที่ให้บริการชำระเงินและโอนเงินข้ามธนาคารต้องคำนึงถึงมาตรฐานการควบคุมความปลอดภัยที่ครอบคลุมประเด็นต่าง ๆ ได้แก่

1) นโยบายในการรักษาความปลอดภัยของระบบ (Security Policy)

ผู้ดำเนินการระบบ ITMX จัดทำและดำเนินการตามนโยบายในการรักษาความปลอดภัยของระบบ เพื่อให้มีการเตรียมการการปฏิบัติงาน การตรวจสอบ การควบคุม รวมถึงการเชื่อมโยงกับระบบที่เกี่ยวข้องได้อย่างปลอดภัยทั้งภายในและภายนอกองค์กร

2) การควบคุมการเข้าถึงระบบให้บริการและข้อมูล (Access Control)

กระบวนการและเทคโนโลยีที่ใช้ควบคุมการเข้าถึงระบบให้บริการต้องสามารถป้องกันการลักลอบเข้าถึงโดยผู้ที่ไม่มีสิทธิทั้งจากภายในและภายนอกองค์กร โดยมีการควบคุมการเข้าถึงสถานที่ตั้งของระบบให้บริการและอุปกรณ์สำคัญ (Physical Access Control) และมีการควบคุมการเข้าถึงระบบให้บริการและข้อมูลด้วยวิธีการทางคอมพิวเตอร์ (Logical Access Control)

3) การตรวจสอบตัวตนลูกค้าและการป้องกันการปฏิเสธความรับผิด (Authentication & Non-repudiation)

กระบวนการและเทคโนโลยีที่ใช้ในการตรวจสอบตัวตนและป้องกันการปฏิเสธความรับผิด (Authentication & Non-repudiation) นอกจากจะเป็นประโยชน์กับสมาชิกในการพิสูจน์ตัวตนของลูกค้าก่อนอนุญาตให้ใช้บริการ และยังเป็นประโยชน์ในกรณีมีข้อพิพาท

4) การรักษาความถูกต้องของระบบและข้อมูล (System & Data Integrity)

กระบวนการที่ใช้ในการรักษาความถูกต้องของระบบและข้อมูลที่อยู่ระหว่างการรับส่ง การประมวลผล และการจัดเก็บ รวมทั้งการดำเนินการให้ระบบสามารถทำงานได้อย่างถูกต้องและตอบสนองความต้องการของลูกค้าได้อย่างมีประสิทธิภาพ

5) การรักษาความลับของข้อมูล (Data Confidentiality)

กระบวนการและเทคโนโลยีที่ใช้ในการรักษาความลับของข้อมูล (Data Confidentiality) โดยเฉพาะข้อมูลลูกค้าที่อยู่ระหว่างการรับส่ง การประมวลผลและการจัดเก็บ

6) ความพร้อมในการให้บริการของระบบและการรองรับการขยายตัวในอนาคต (System Availability and Scalability)

กระบวนการที่ใช้รักษาความพร้อมในการให้บริการของระบบ หมายถึงการดำเนินการให้ระบบมีประสิทธิภาพและพร้อมให้บริการได้ตลอดเวลา โดยอย่างน้อยสามารถให้บริการได้ตามช่วงเวลาที่ได้ตกลงไว้กับสมาชิก สามารถรองรับการทำธุรกรรมตามความต้องการของสมาชิกได้อย่างพอเพียง ตอบสนองการทำธุรกรรมได้อย่างรวดเร็วทั้งในช่วงเวลาปกติและช่วงเวลาที่มีการใช้บริการอย่างหนาแน่น รวมทั้งมีการสำรองข้อมูลอย่างเหมาะสมเพื่อให้สามารถกู้ระบบให้กลับมาทำงานได้ตามปกติทันท่วงทีในกรณีที่เกิดความเสียหาย ในการเตรียมการรองรับเหตุการณ์ความเสียหายที่อาจเกิดขึ้นโดยไม่ได้คาดหมาย ควรจัดให้มีแผนฉุกเฉินในการรักษาความพร้อมใช้ของระบบโดยคำนึงถึงปัญหาขัดข้องที่เกิดจากระบบขององค์กรภายนอกที่ระบบ ITMX พึ่งพาหรือเชื่อมต่อด้วย ทั้งนี้ระบบที่ให้บริการสามารถรองรับและตอบสนองต่อการขยายตัวของภาคธุรกิจและความเปลี่ยนแปลงทางด้านเทคโนโลยีสารสนเทศด้วย

7) การติดตามตรวจสอบความผิดปกติของระบบ (System Detection)

กระบวนการและเทคโนโลยีที่ใช้ในการติดตามตรวจสอบความผิดปกติของระบบควรคลอบคลุมถึง การจัดให้มีหลักฐานการตรวจสอบสำหรับกิจกรรมที่สำคัญ, การติดตามตรวจสอบรายละเอียดการทำธุรกรรมกับลูกค้า (Transaction Log), การตรวจสอบและแก้ไขความล่อแหลม (Vulnerabilities) ของระบบอย่างต่อเนื่อง และการทดสอบเจาะระบบ (Penetration Test)

8) การแก้ไขปัญหาและการรายงานในกรณีระบบได้รับความเสียหายจากภัยคุกคาม (Incident Response & Report)

กระบวนการแก้ไขปัญหาและการรายงานในกรณีระบบได้รับความเสียหายจากภัยคุกคามหรือการลักลอบเข้าถึง (Hacking Incidents) ควรครอบคลุมถึง การประเมินความเสี่ยงจากภัยคุกคามและการลักลอบเข้าถึง, ขั้นตอนในการรับรู้และแก้ไขปัญหาที่เกิดขึ้นอย่างทันท่วงที, การสื่อสารและประชาสัมพันธ์เพื่อชี้แจงและทำความเข้าใจกับสมาชิก, การรวบรวมหลักฐานต่าง ๆ ที่เป็นประโยชน์ในการดำเนินคดีกับผู้บุกรุก

(2) แนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ของธนาคารแห่งประเทศไทย

ในส่วนของการให้บริการเงินอิเล็กทรอนิกส์ (Electronic Money) นั้น ธนาคารแห่งประเทศไทยได้ออกประกาศธนาคารแห่งประเทศไทย เรื่อง แนวนโยบายการกำกับดูแลการให้บริการเงินอิเล็กทรอนิกส์ (Electronic Money) เพื่อให้ผู้ใช้บริการสามารถนำเงินอิเล็กทรอนิกส์หรือที่อาจเรียกเป็นอย่างอื่น เช่น Multipurpose Stored Value Card, E-purse, E-Wallet หรือ Smart Card เป็นต้น ไปใช้ซื้อสินค้าหรือบริการต่าง ๆ ได้ โดยธนาคารแห่งประเทศไทยได้วางแนวทางกำกับการให้บริการเงินอิเล็กทรอนิกส์ในเบื้องต้น ซึ่งรวมถึงแนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ และแนวปฏิบัติในการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น เป็นต้น

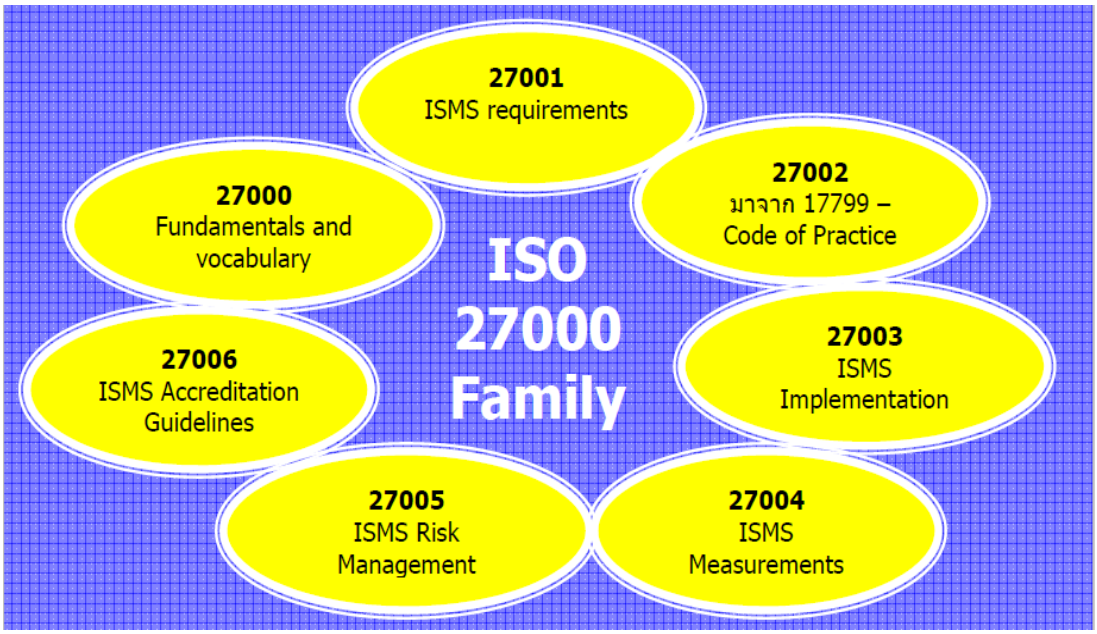
(3) มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์โดยองค์การนานาชาติเพื่อระบบมาตรฐาน (ISO)

หากจะกล่าวถึงระดับมาตรฐานในวงการอุตสาหกรรมที่ได้รับความยอมรับจากคนทั่วโลกรวมถึงคนไทยด้วยนั้น หนึ่งในนั้นจะต้องมีระบบมาตรฐานที่กำหนดและควบคุมโดยองค์การนานาชาติเพื่อระบบมาตรฐาน (International Organization for standardization) หรือที่รู้จักกันดีว่า ISO โดยมีการกำหนดตัวเลขรหัสต่าง ๆ ต่อชื่อท้าย ISO เพื่อแยกความแตกต่างว่าเป็นมาตรฐานที่เกี่ยวข้องกับด้านใด ยกตัวอย่างเช่น ISO 14001 คือ มาตรฐานด้านสิ่งแวดล้อมของอุตสาหกรรมการผลิต, ISO 9400 คือ มาตรฐานด้านการพัฒนาผลิตภาพ หรือ Productivity Improvement, ISO 14750 คือ มาตรฐานด้านเทคโนโลยีสารสนเทศเพื่อการประมวลผลแบบกระจายตัวมาตรฐานเปิด หรือ Open Distributed Processing เป็นต้น

ในส่วนของมาตรฐานด้านการบริหารความปลอดภัยสำหรับสารสนเทศ (Information Security and Management – ISMS) นั้น องค์การนานาชาติเพื่อระบบมาตรฐาน หรือ ISO ได้ร่วมกับคณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอนิกส์หรือ IEC (The

International Electrotechnical Commission) ซึ่งเป็นองค์กรอิสระที่เริ่มก่อตั้งขึ้นเมื่อ พ.ศ.2449 โดยมีวัตถุประสงค์เพื่อจัดทำมาตรฐานระหว่างประเทศทางด้านไฟฟ้าอิเล็กทรอนิกส์และกิจกรรมที่เกี่ยวข้อง[62] ร่วมกันจัดทำมาตรฐานสากลเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ ซึ่งจะกำหนดความต้องการเกี่ยวกับการจัดทำระบบให้มีความมั่นคงปลอดภัย โดยเน้นความสำคัญที่ “ระบบบริหารจัดการ” (Management System) โดยมีวัตถุประสงค์เพื่อช่วยให้องค์กรสามารถสร้างระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศขึ้นมาได้อย่างมีประสิทธิภาพ โดยในปัจจุบัน มาตรฐานเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยของข้อมูลสารสนเทศนั้นถูกจัดอยู่ในตระกูล ISO 27000

แผนภาพแสดง ชื่อของมาตรฐานความมั่นคงปลอดภัย ISO ตระกูล 27000



ที่มา: http://thaicert.nectec.or.th/

สำหรับปัจจุบัน ISO/IEC 27001:2005 ถือว่าเป็นมาตรฐานสากลที่หน่วยงานหรือองค์กรชั้นนำของโลกนำมาใช้ในการบริหารความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ซึ่งหัวใจสำคัญของระบบบริหารความปลอดภัยสารสนเทศนั้นมีอยู่ด้วยกัน 3 ประการด้วยกัน คือ

1) ข้อมูลส่วนตัว ข้อมูลสำคัญขององค์กร

การรักษาความปลอดภัยด้านข้อมูลไม่ให้ถูกขโมย ลักลอบนำไปใช้ ดัดแปลง หรือทำให้เกิดข้อผิดพลาดอื่นใด ซึ่งสำหรับหลายหน่วยงานอาจเป็นอันตรายระดับวิกฤติได้ ซึ่งข้อมูลนี้ไม่

[62] สืบค้นจาก http://app.tisi.go.th/iso_iec/iec_t.html.

เพียงเฉพาะข้อมูลสำคัญขององค์กรแต่ยังรวมถึงข้อมูลส่วนตัวของลูกค้าหรือบุคคลที่สามที่เกี่ยวข้องอื่น ๆ ด้วย

2) การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่างๆ

การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่างๆ ซึ่งปัจจุบันมีการคำนึงถึงการตั้งเว็บไซต์สำรอง ในลักษณะของศูนย์สำรองข้อมูลและดำเนินการกู้คืนระบบภายหลังภัยพิบัติหรือ Disaster Recovery Center (DRC) ซึ่งมีความสำคัญมากในหลายธุรกิจ เช่น ธุรกิจการเงิน หรือบริการด้านสุขภาพ เพราะข้อมูลเหล่านั้นมีความสำคัญยิ่งยวดต่อความสามารถในการดำเนินธุรกิจให้ต่อเนื่องต่อไปได้ (Business continuity)

3) บริหารระบบเพื่อป้องกันความปลอดภัยของข้อมูล

รายละเอียดการบริหารระบบเพื่อป้องกันความปลอดภัยของข้อมูล ซึ่งหัวข้อนี้นับเป็นหนึ่งในรายละเอียดหลักของเนื้อหาในร่างมาตรฐาน ISO 27000 ทั้งหมดก็ว่าได้ โดยครอบคลุมตั้งแต่นโยบาย แผน กลยุทธ์ การตรวจวัด การบริหาร และการควบคุมการปฏิบัติการ

ทั้งนี้ นอกจากมาตรฐาน ISO 27000 แล้วในวงการคอมพิวเตอร์และสารสนเทศก็มีระบบมาตรฐานอื่น ๆ อีกเช่น

- ISO 20000: เน้นเรื่องการบริหารบริการไอที

- ITIL: เน้นเรื่องเฟรมเวิร์กระดับล่างลงไปสำหรับการบริหารบริการไอที (ITSM – IT Service Management)

- Six Sigma: มีเนื้อหาในส่วนที่เกี่ยวข้องกับผลิตภาพการปฏิบัติการและการบ่งชี้ข้อบกพร่องในการทำงาน

- COBIT: เน้นเรื่องเฟรมเวิร์กสำหรับความเสี่ยงด้านการบริหารข้อมูลสารสนเทศไอที

- Balanced Scorecard: เน้นเรื่องเฟรมเวิร์กสำหรับตรวจวัดกิจกรรมของบริษัทในเรื่องวิสัยทัศน์และกลยุทธ์

- Prince 2: เป็นวิธีการบริหารโครงการไอที[63]

[63] สืบค้นจาก http://www.uih.co.th/article/ISO_27001/iso_27001.html.

4.2.2 บทวิเคราะห์ปัญหาเรื่องมาตรฐานความมั่นคงปลอดภัยในการประกอบธุรกรรมที่เกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์ในด้านกฎหมาย

ในโลกของเทคโนโลยีสารสนเทศปัจจุบันนี้ ที่การพาณิชย์อิเล็กทรอนิกส์กำลังเติบโตขึ้นอย่างรวดเร็ว รวมถึงธนาคารพาณิชย์ต่าง ๆ ที่หันมาให้บริการทางอิเล็กทรอนิกส์มากยิ่งขึ้น เนื่องจากเป็นการลงทุนที่คุ้มค่าสามารถลดค่าใช้จ่ายในการดำเนินงานได้มาก แต่ในทางกลับกันการให้บริการทางอิเล็กทรอนิกส์ดังกล่าวก็มีปัจจัยความเสี่ยงในด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศมากยิ่งขึ้นจากหลายสาเหตุ เช่น ภัยธรรมชาติ, ไวรัสคอมพิวเตอร์, มิจฉาชีพที่หลอกลวง หรือเจาะเข้าสู่ระบบฐานข้อมูลของธนาคาร เป็นต้น ซึ่งความไม่มั่นคงปลอดภัยของข้อมูลสารสนเทศนั้นจะส่งผลกระทบต่อความเชื่อมั่นของลูกค้าผู้ใช้บริการ และนับว่าเป็นอุปสรรคสำคัญที่ขัดขวางการเติบโตของการธนาคารพาณิชย์อิเล็กทรอนิกส์อย่างแท้จริง

ทั้งนี้ จุดประสงค์หลักของความปลอดภัยทางข้อมูลสารสนเทศ (ICT Security) คือ ความลับ (Confidentiality) ความสมบูรณ์ (Integrity) ความพร้อมใช้ (Availability) และการห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) ของข้อมูลต่าง ๆ ภายในองค์กร (CIA-N) โดยมีรายละเอียดโดยสรุป ดังนี้

1) การรักษาความลับ (Confidentiality) คือการรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ และผู้มีสิทธิเท่านั้นจึงจะเข้าถึงข้อมูลนั้นได้

2) การรักษาความสมบูรณ์ (Integrity) คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา

3) ความพร้อมใช้ (Availability) คือการรับรองว่าข้อมูลและบริการการสื่อสารต่าง ๆ พร้อมที่จะใช้ได้ในเวลาที่ต้องการใช้งาน

4) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) คือวิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

และในทางปฏิบัตินั้นสามารถกำหนดลักษณะของการควบคุมความมั่นคงปลอดภัย (Security Controls) ได้ 5 ระดับตามรูป

รูปที่ แสดง Security Pyramid

ที่มา: Doug Graham, "It's all about authentication", SANS Reading Room, 15 March 2003

ดังที่กล่าวมาแล้วนั้น จะเห็นได้ว่าการจัดการด้านมั่นคงปลอดภัยของข้อมูลสารสนเทศนั้นเป็นเรื่องที่สำคัญมาก และผู้ประกอบพาณิชย์ธุรกรรมทางอิเล็กทรอนิกส์จะต้องใส่ใจและมีมาตรการเตรียมพร้อมที่จะรับมือกับสถานการณ์ต่าง ๆ ที่เป็นภัยต่อข้อมูลที่อยู่ในรูปเทคโนโลยีสารสนเทศของตน ซึ่งในส่วนนี้เองการประกอบกิจการธนาคารพาณิชย์อิเล็กทรอนิกส์ก็ได้ตระหนักถึงความสำคัญดังกล่าวด้วย ซึ่งเห็นได้จากการที่ธนาคารแห่งประเทศไทยได้ออกประกาศต่าง ๆ มาเพื่อให้รองรับและสอดคล้องกับการให้บริการของธนาคารพาณิชย์ในปัจจุบัน เช่น ประกาศเรื่องมาตรฐานขั้นต่ำของระบบ ITMX – Interbank Transaction Management and Exchange ที่กำหนดเรื่องมาตรฐานความปลอดภัยของระบบชำระเงินอิเล็กทรอนิกส์ของระบบการชำระเงินทั้งหมดในปัจจุบัน, ประกาศเรื่องแนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ของธนาคารแห่งประเทศไทย ที่กำหนดแนวทางในการให้บริการเงินอิเล็กทรอนิกส์ (e-Money) ของผู้ให้บริการต่าง ๆ เป็นต้น

แต่จะเห็นได้ว่า การกำหนดต่าง ๆ ของธนาคารแห่งประเทศไทยนั้นเป็นเพียงมาตรฐานขั้นต่ำ หรือแนวทางที่จะให้ธนาคารนำไปปฏิบัติเท่านั้น ยกตัวอย่างเช่น ในการให้บริการธนาคารทางอินเตอร์เน็ทของ 5 ธนาคารพาณิชย์ใหญ่ของไทย คือ ธนาคารกรุงเทพ, ธนาคารกสิกรไทย, ธนาคารไทยพาณิชย์, ธนาคารกรุงศรีอยุธยา และธนาคารกรุงไทย เพียงแค่การระบุตัวตน (Identification) และการพิสูจน์ตัวตน (Authentication)[64] ของธนาคารแต่ละแห่งก็ใช้ระบบที่แตกต่างกันออกไป เช่น

---

[64] การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

- ธนาคารกรุงเทพ (Bualuang i-banking) ใช้การรักษาความปลอดภัยของข้อมูลมีการใช้ระบบความปลอดภัยขั้นสูง และเคารพสิทธิในการเป็นส่วนตัวของลูกค้า ส่วนบริการนั้นทางธนาคารได้ใช้เทคโนโลยีเข้ารหัสข้อมูลที่ระดับ 128 บิท ซึ่งเป็นการเข้ารหัสระดับสูงสุดใช้สำหรับการทำธุรกรรมผ่านบริการธนาคารทางอินเตอร์เน็ท

ภาพแสดงหน้าเว็บไซต์ของบริการธนาคารทางอินเตอร์เน็ทของธนาคารกรุงเทพ

ที่มา: https://ibanking.bangkokbank.com/SignOn.aspx

- ธนาคารกสิกรไทย (K-Cyber Banking) ใช้การใส่รหัสรักษาความปลอดภัย แบ่งออกเป็น 2 รูปแบบคือ รหัสรักษาความปลอดภัยแบบ PIN2 ซึ่งเป็นรหัสที่ใช้ยืนยันการทำธุรกรรมทางการเงินที่สำคัญ และรหัสรักษาความปลอดภัยแบบ OTP (One Time Password) ซึ่งเป็นรหัสที่ใช้ยืนยันการทำธุรกรรมทางการเงินในแต่ละครั้ง โดยเมื่อมีการทำรายการทางบัญชีหรือมีการเปลี่ยนแปลงข้อมูลส่วนตัว ระบบจะส่งรหัสผ่าน OTP 6 หลัก พร้อมรหัสอ้างอิง 4 หลัก ผ่านทาง

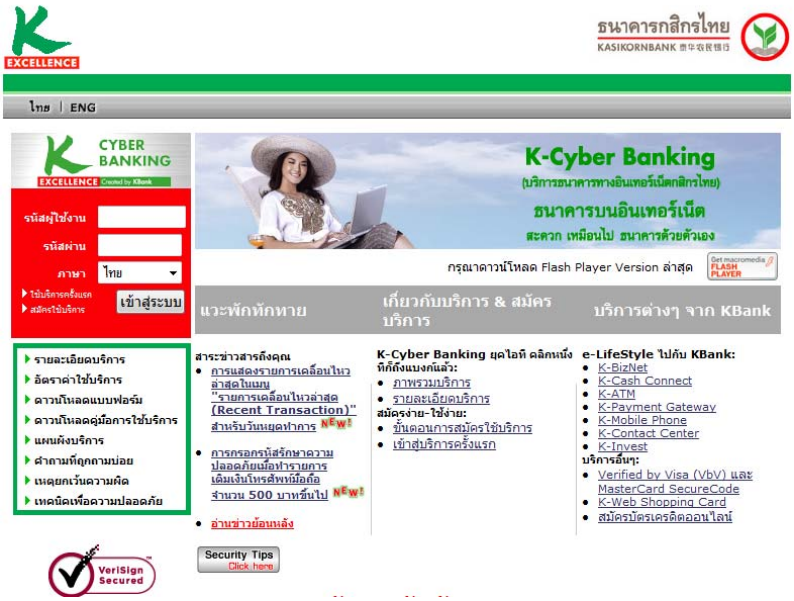
---

1) การระบุตัวตน คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (username)

2) การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

โทรศัพท์มือถือ (SMS) ทั้งนี้คุณจะต้องกรอกรหัสผ่าน OTP เพื่อยืนยันการทำรายการภายใน 6 นาที ในกรณีที่ไม่ได้รหัสผ่าน OTP ภายในเวลาที่กำหนด ระบบจะส่งผ่าน OTP ผ่านทางโทรศัพท์มือถือ (SMS) อีกครั้ง

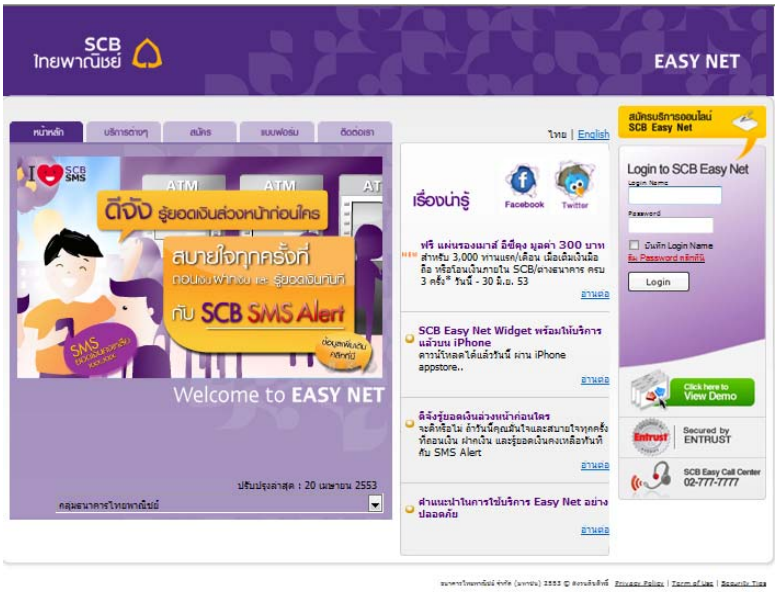
ภาพแสดงหน้าเว็บไซต์ของบริการธนาคารทางอินเตอร์เน็ทของธนาคารกสิกรไทย



ที่มา: https://ebank.kasikornbank.com/kcyber/login_th.html

ธนาคารไทยพาณิชย์ (SCB Easy Net) ในด้านระบบความปลอดภัย ธนาคารจะใช้การเข้ารหัสที่มีความปลอดภัยสูง 128-bit (SSL 128 bit) ซึ่งเป็นระบบความปลอดภัยที่สถาบันการเงินชั้นนำได้นำมาใช้และมีระบบ Double Firewall Protection ที่จะช่วยให้คุณมั่นใจได้ว่าข้อมูลทางการเงินจะถูกเก็บรักษาเป็นอย่างดี

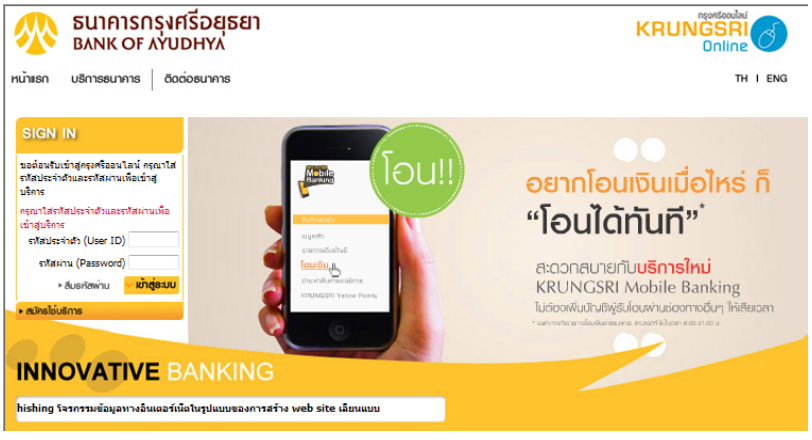
ภาพแสดงหน้าเว็บไซต์ของบริการธนาคารทางอินเตอร์เน็ทของธนาคารไทยพาณิชย์



ที่มา: https://www.scbeasy.com/v1.4/site/presignon/index.asp

- ธนาคารกรุงศรีอยุธยา (Krungsri Online) ใช้การรักษาความปลอดภัยด้วยการติดตั้งระบบ Firewall 2 ชั้น ซึ่งเป็นระบบที่ป้องกันไม่ให้บุคคล หรือเครือข่ายอื่นทุกระบบที่ไม่ได้รับอนุญาตเข้ามาติดต่อ ในส่วนของการเข้ารหัสข้อมูลธนาคารได้ใช้การเข้ารหัสแบบ Secured Socket Layer (SSL) ที่ 128 บิท เพื่อป้องกันและรักษาความลับข้อมูลของคุณ

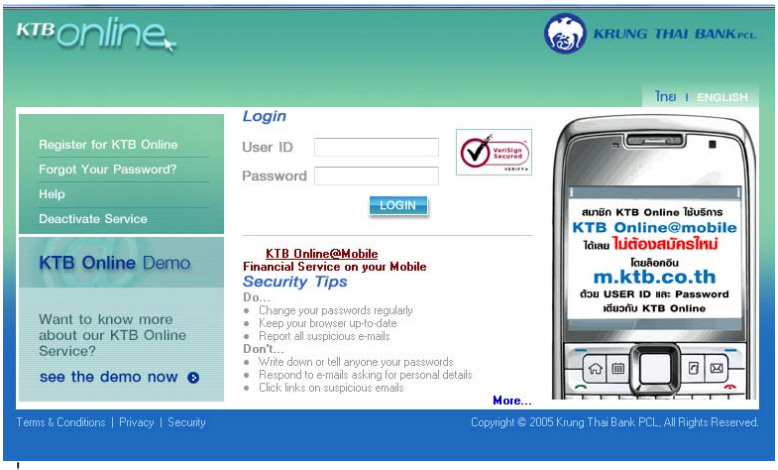
ภาพแสดงหน้าเว็บไซต์ของบริการธนาคารทางอินเตอร์เน็ทของธนาคารกรุงศรีอยุธยา



ที่มา: https://www.krungsrionline.com/cgi-bin/bvisapi.dll/krungsri_ib/login/login.jsp

- ธนาคารกรุงไทย KTB Online ในส่วนของระบบความปลอดภัยนั้น ทางธนาคารกรุงไทยให้ความสำคัญต่อข้อมูลส่วนบุคคล ไม่เปิดเผยข้อมูลของคุณให้บุคคลอื่นทราบ โดยทางธนาคารมีมาตรการรักษาความปลอดภัยข้อมูลอย่างเข้มงวดเช่นธนาคารอื่น เพื่อป้องกันความเสียหาย

ภาพแสดงหน้าเว็บไซต์ของบริการธนาคารทางอินเตอร์เน็ทของธนาคารกรุงไทย



ที่มา: https://www.ktbonline.ktb.co.th

จากตัวอย่างดังกล่าวจะเห็นได้ว่าธนาคารแต่ละแห่งได้ใช้เทคโนโลยีในการรักษาความปลอดภัยในการพิสูจน์ตัวบุคคลแตกต่างกันออกไป อันเนื่องมาจากการที่ธนาคารแห่งประเทศไทยไม่ได้กำหนดนโยบายที่ชัดเจน รวมถึงหน่วยงานที่ทำหน้าที่เกี่ยวข้องโดยตรงกับเรื่องเทคโนโลยีสารสนเทศ เช่น กระทรวงกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ไม่มีการจัดตั้งหรือมอบหมายให้หน่วยงานออกมารับผิดชอบในเรื่องของมาตรฐานความปลอดภัยของข้อมูลสารสนเทศของประเทศอย่างเป็นระบบ คงมีแต่เพียงคณะกรรมการทางอิเล็กทรอนิกส์ที่ตั้งขึ้นตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ที่มีหน้าที่ในการเสนอแนะนโยบายและมาตรการด้านความมั่นคงให้เกิดความเชื่อมั่นและปลอดภัยในระบบคอมพิวเตอร์หรือเครือข่ายของประเทศไทยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

โดยทางคณะกรรมการทางอิเล็กทรอนิกส์ดังกล่าว ได้มอบหมายให้ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) ในฐานะที่เป็นหน่วยงานวิจัยและพัฒนาด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายข้อมูลสารสนเทศ ซึ่งมีหน้าที่ในการศึกษาวิจัยและพัฒนาทางด้านมาตรฐานทางด้านมาตรฐานความมั่นคงปลอดภัยด้วย โดยได้จัดทำ “มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทาง

อิเลคทรอนิกส์" ซึ่งปัจจุบันเวอร์ชั่นล่าสุด คือ เวอร์ชั่น 2.5 ออกมาเมื่อเดือนธันวาคมปี 2550 ที่ผ่านโดยเสนอให้หน่วยงานและองค์กรภายในประเทศที่มีความเกี่ยวข้องกับการใช้ข้อมูลสารสนเทศควรจะต้องผ่านการรับรองจากมาตรฐาน ISO/IEC 27001:2005 (ปรับปรุงจากเวอร์ชั่นเดิมที่เสนอมาตรฐานตาม ISO/IEC 17799:2005)[65] ซึ่งในปัจจุบันก็มีหน่วยงานหลายแห่งที่ผ่านการรับรองมาตรฐานดังกล่าวแล้ว เช่น สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ (สบทร. หรือ GITS), บริการ Co-Location ของบริษัท UIH, บริษัทข้อมูลเครดิตแห่งชาติจำกัด (NCB), การไฟฟ้านครหลวง, สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) เป็นต้น

ในส่วนของรายละเอียดในภาพรวมของ ISO/IEC 27001:2005 ประกอบด้วยกระบวนการ 6 ขั้นตอนด้วยกัน ได้แก่

1) กำหนดนโยบายด้านความปลอดภัย

2) กำหนดขอบเขตของระบบบริหารความปลอดภัยสารสนเทศ (ISMS)

3) รายละเอียดการประเมินความเสี่ยง

4) การบริหารความเสี่ยง

5) เลือกวัตถุประสงค์ในการควบคุมและวิธีการควบคุมที่จะนำไปใช้งานจริง

6) จัดเตรียมคำอธิบายสำหรับการปฏิบัติงานจริง

ซึ่งในส่วนนี้ของมาตรฐานการบริหารความมั่นคงของข้อมูลสารสนเทศนี้เองที่ **ผู้เขียนมีความเห็นว่า ธนาคารแห่งประเทศไทยควรจะออกประกาศให้ธนาคารพาณิชย์ที่อยู่ภายใต้กำกับและประสงค์จะใช้ให้บริการทางอิเล็กทรอนิกส์ทั้งหมด ต้องได้รับการรับรองมาตรฐานด้านการบริหารความปลอดภัยสำหรับสารสนเทศที่เป็นสากล เช่น ผ่านการรับรองมาตรฐาน** ISO/IEC 27001:2005 **หรือ มาตรฐานอื่นที่สามารถเทียบเคียงได้จาก**

---

[65] ข้อแตกต่างระหว่าง ISO/IEC 17799:2005 กับ ISO/IEC 27001:2005 คือ

1) ISO/IEC 27001:2005 เน้นเรื่องรายละเอียดเชิงเทคนิคมาตรฐานสำหรับการบริหารความปลอดภัยด้านสารสนเทศ ISMS (Information Security Management System) โดยเป็นรายละเอียดแบบมุ่งเน้นกระบวนการตามหลักการ PDCA (Plan-Do-Check-Act Process focused) สามารถใช้เป็นเกณฑ์เพื่อนำไปใช้งานจริง (Implement) และขอการรับรองได้

2) ISO/IEC 17799:2005 เป็นรายละเอียดการดำเนินการ (code of practice) เพื่อการควบคุมด้านความปลอดภัย (Security control) ต่อมาได้ถูกนำไปโยงความสัมพันธ์กับ ISO 27000 ซึ่งครอบคลุมเรื่องความปลอดภัยสารสนเทศทั้งหมดและถูกเรียกรหัสใหม่เป็น ISO 27002

หน่วยงานที่รับผิดชอบด้านความมั่นคงของข้อมูลสารสนเทศทั้งระบบของประเทศ เพื่อให้เกิดความเชื่อมั่นจากลูกค้าและผู้ใช้บริการของธนาคารพาณิชย์เองด้วย

นอกจากนี้รัฐก็ควรตรากฎหมายเพื่อกำหนดวิธีการแบบ (มั่นคง) ปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้มีการกำหนดหน่วยงานที่มีหน้ารับผิดชอบและเป็นกำหนดนโยบายในด้านการบริหารความปลอดภัยของข้อมูลสารสนเทศอย่างเป็นเอกภาพ และเป็นไปในทิศทางเดียวกันทั้งระบบ

4.3 ปัญหาเรื่องการจัดสรรความเสี่ยง (Allocation of Risk) ระหว่าง ผู้บริโภค กับ ผู้ประกอบการ ในการประกอบธุรกรรมที่เกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์

ขณะที่ลูกค้าเข้าใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์ต่าง ๆ ในครั้งแรกกับธนาคารพาณิชย์ สิ่งหนึ่งที่ลูกค้าทุกคนจะต้องพบแต่อาจจะไม่ใส่ใจ คือ ข้อความที่เป็นข้อกำหนดหรือเงื่อนไข (Terms and Conditions) ในการเข้าใช้บริการนั้น ๆ โดยธนาคารจะเป็นผู้กำหนดเงื่อนไขต่าง ๆ ซึ่งอาจจะมีความยาวหลายบรรทัดและมีขนาดตัวอักษรที่ไม่ใหญ่นัก จนทำให้ลูกค้าส่วนใหญ่หรือเกือบจะทุกคนไม่เคยอ่าน หรือสนใจข้อความดังกล่าวเลย ทั้ง ๆ ที่ข้อกำหนดและเงื่อนไขดังกล่าวมีความสำคัญอย่างยิ่ง เพราะเป็นการกำหนดสิทธิและหน้าที่ของธนาคารพาณิชย์ผู้ให้บริการกับลูกค้าผู้เข้าใช้บริการ ซึ่งรวมถึงการจำกัดความรับผิดของคู่สัญญาด้วย และโดยส่วนใหญ่ธนาคารก็มักจะเขียนในลักษณะที่เป็นการสงวนสิทธิหรือจำกัดความรับผิดของตนเองไว้แทบทั้งสิ้น

แม้ว่าลูกค้าส่วนหนึ่งอาจจะพยายามลองอ่านและทำความเข้าใจในข้อกำหนดและเงื่อนไขเหล่านั้นก็ตาม และอาจจะมีข้อสงสัยในถ้อยคำบางอย่างก็ดี หรือมีความรู้สึกว่าตนเป็นฝ่ายเสียเปรียบในสัญญาดังกล่าวก็ดี แต่ทั้งหมดที่กล่าวมานั้นลูกค้าก็ได้แต่ตั้งไว้เป็นคำถามหรือข้อสงสัยที่อยู่ในใจของตนเท่านั้น เพราะทราบดีว่าถึงอย่างไรก็ไม่สามารถที่จะไปเรียกร้องให้ธนาคารพาณิชย์ทั้งหลายให้หันมาเปลี่ยนแปลงถ้อยคำหรือข้อความใด ๆ เหล่านั้นได้เลย ด้วยความที่อำนาจต่อรองทางเศรษฐกิจระหว่างลูกค้าที่เป็นพียงผู้บริโภคธรรมดากับธนาคารพาณิชย์นั้น มีความแตกต่างกันอยู่มากพอสมควร

ทั้งนี้ แม้ว่าข้อกำหนดและเงื่อนไขในการเข้าใช้บริการเหล่านั้นจะไม่สามารถแก้ไขได้โดยผู้บริโภคก็ตาม แต่ในปัจจุบันนี้นอกจากธนาคารแห่งประเทศไทยที่เป็นผู้ควบคุมและกำกับดูแลธนาคารพาณิชย์ที่ให้บริการทั้งหมดในประเทศไทยแล้ว ในเรื่องของสิทธิของผู้บริโภคก็เริ่มเป็นที่แพร่หลาย โดยเฉพาะสำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) ที่เปรียบเสมือนเป็นที่พึ่ง

ของผู้บริโภคทุกคน ที่จะช่วยในการต่อรองกับผู้ประกอบการต่าง ๆ ได้อย่างมีประสิทธิภาพ เพราะมีเป็นองค์กรที่มีกฎหมายให้อำนาจไว้โดยเฉพาะ

4.3.1 **ความเสี่ยงภัยขณะใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์กับธนาคารพาณิชย์**

ในการเข้าใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์กับธนาคารพาณิชย์แต่ละครั้งนั้น เทียบได้กับการที่ลูกค้าได้เข้าทำสัญญาอย่างหนึ่งอย่างได้กับธนาคาร โดยผ่านการแสดงเจตนาของคู่สัญญาทั้งสองฝ่าย ที่ฝ่ายหนึ่งเป็นผู้ทำคำเสนอและอีกฝ่ายเป็นผู้ทำคำสนอง และเมื่อการเสนอสนองนั้นต้องตรงกันสัญญาจึงเกิดขึ้น แต่ในกรณีที่เป็นการทำสัญญากันทางอิเล็กทรอนิกส์นั้นไม่เหมือนกับการทำสัญญากันตามปกติ เพราะการแสดงเจตนาต่าง ๆ นั้นจะต้องผ่านอุปกรณ์อิเล็กทรอนิกส์เสียก่อนถึงจะไปถึงคู่สัญญาอีกฝ่ายหนึ่งได้ ซึ่งทำให้มีกรณีปัญหาที่จะต้องพิจาณา คือ สัญญาจะเกิดขึ้นเมื่อใด เวลาใด และ ณ สถานที่ใดด้วย

1) การแสดงเจตนาทำสัญญาทางอิเล็กทรอนิกส์

สำหรับกฎหมายไทยในปัจจุบันนั้น การแสดงเจตนานี้กฎหมายมิได้บัญญัติไว้ว่าจะต้องมีการแสดงเจตนาออกมาในรูปใด จึงอาจมีการแสดงเจตนาออกมาได้หลายทาง ซึ่งสิ่งที่เป็นสาระสำคัญก็คือผู้ให้ผู้รับ การแสดงเจตนานั้นเข้าใจถึงการแสดงเจตนานั้นก็เป็นอันใช้ได้ ซึ่งการกระทำด้วยการแสดงเจตนานั้น อาจจะมีลักษณะเป็นการทำด้วยวาจา ลายลักษณ์อักษร หรือกิริยาท่าทางหรือการกระทำอย่างหนึ่งอย่างใด มีผลเป็นการแสดงเจตนา ซึ่งเมื่อพิจารณาถึงวิธีแสดงเจตนาโดยลักษณะต่าง ๆ แล้วนั้นอาจแบ่งออกได้เป็น 3 ประการ คือ

1. การแสดงเจตนาโดยชัดแจ้ง ได้แก่ การแสดงเจตนาด้วยการกระทำโดยวาจา ลายลักษณ์อักษร หรือการแสดงกิริยาอาการอย่างใดอย่างหนึ่งหรือการกระทำอย่างอื่นซึ่งแสดงออกโดยแจ้งชัดซึ่งเจตนาของผู้กระทำว่ามุ่งประสงค์จะผูกนิติสัมพันธ์

2. การแสดงเจตนาโดยปริยาย ได้แก่ การกระทำอย่างใดอย่างหนึ่ง ซึ่งเห็นได้โดยปริยายว่าผู้กระทำได้แสดงเจตนาเพื่อทำนิติกรรมโดยตรงแก่พฤติกรรม ย่อมเป็นที่สามารถคาดหมายได้ว่ามีเจตนาที่จะทำนิติกรรมนั้น

3. การแสดงเจตนาโดยการนิ่ง โดยปกติแล้วการแสดงเจตนาถ้ามิใช่โดยการแสดงเจตนาโดยชัดแจ้ง หรือโดยปริยายให้ปรากฏแล้ว ตามหลักทั่วไปแล้วการนิ่งหรือการงดเว้นไม่กระทำการนั้น โดยปกติไม่ถือว่าเป็นการแสดงเจตนาทำนิติกรรม เพราะมิได้มีการแสดงกิริยาอาการอย่างใดออกมาอันจะถือได้ว่าเป็นการแสดงเจตนา อย่างไรก็ตาม มีข้อยกเว้นให้ถือว่าการนิ่งเป็นการแสดงเจตนาได้หาก

ก. การนิ่งที่มีกฎหมายบัญญัติรับรองได้ว่าการนิ่งในเหตุการณ์บางอย่างถือว่าเป็นการแสดงเจตนา

ข. การนิ่งอันมีธรรมเนียมประเพณีถือว่าเป็นการแสดงเจตนา

สำหรับการแสดงเจตนาทางอิเล็กทรอนิกส์นั้น ก็จะต้องพิจารณาคล้ายกับกรณีการแสดงเจตนาในการทำสัญญาทั่วไป คือ เริ่มตั้งแต่การทำคำเสนอ และการทำคำสนองตอบกลับมาตามปกติด้วย

1.1) คำเสนอทางอิเล็กทรอนิกส์

คำเสนอที่กระทำโดยใช้สื่ออิเล็กทรอนิกส์นั้น จะต้องเป็นการแสดงเจตนาของคนต่อบุคคลใดบุคคลหนึ่งหรือหลายบุคคลโดยเฉพาะเจาะจง หรืออาจแสดงต่อสาธารณชนทั่วไปเพื่อขอทำสัญญา โดยคำเสนอนั้นต้องเป็นการแสดงเจตนาที่ชัดแจ้งและต้องมีข้อความที่ชัดเจนแน่นอนพอที่จะทำให้สัญญาเกิดขึ้นได้หากผู้รับทำคำเสนอตอบรับกลับมา เพียงแต่การทำคำเสนอทางอิเล็กทรอนิกส์อาจมีวิธีการแสดงเจตนาที่ต่างออกไปจากเดิมที่อาจเป็นการแสดงเจตนาด้วยวาจาหรือลายลักษณ์อักษรหรือกิริยาอาการอย่างใดอย่างหนึ่ง ในขณะที่การทำคำเสนอทางอิเล็กทรอนิกส์ อาจทำโดยส่งทางไปรษณีย์อิเล็กทรอนิกส์ (E-mail) หรือบนหน้าเว็บไซต์ (Web page) เป็นต้น

1.2) คำสนองทางอิเล็กทรอนิกส์

คำสนองที่กระทำโดยใช้สื่ออิเล็กทรอนิกส์ก็เช่นเดียวกัน ต้องมีลักษณะเหมือนกันกับคำสนองตามหลักทั่วไป คือ จะต้องเป็นการแสดงเจตนาตอบรับไปยังผู้ทำคำเสนอหรือตามที่ผู้เสนอได้กำหนดไว้ การแสดงเจตนาทำคำสนองนั้น อาจเป็นการแสดงเจตนาโดยชัดแจ้ง เป็นการทำด้วยวาจา หรือโดยลายลักษณ์อักษร หรือด้วยอาการกิริยาต่าง ๆ ที่ชัดแจ้ง เช่น การผงกศีรษะรับ ส่วนการทำคำสนองทางอิเล็กทรอนิกส์อาจกระทำโดยการใช้กดปุ่มเมาส์ (Click mouse) ที่ปรากฏบนหน้าจอคอมพิวเตอร์ หรือกดแป้นพิมพ์ (Key board) เป็นต้น

นอกจากนี้ การแสดงเจตนาทำคำสนองยังอาจเกิดขึ้นได้โดยปริยาย ต่างกับคำเสนอที่ต้องเป็นการแสดงเจตนาโดยชัดแจ้งเท่านั้น และในประการสำคัญ คำสนองนั้นต้องมีข้อความชัดเจนแน่นอน ไม่มีเงื่อนไข และไม่มีการแก้ไข จำกัดตัดทอนหรือเปลี่ยนแปลงคำเสนอ

2) เวลาและสถานที่เกิดของสัญญาทางอิเล็กทรอนิกส์

สัญญาจะเกิดขึ้นเมื่อมีการทำคำสนองตอบรับคำเสนอ โดยที่มิได้มีการเปลี่ยนแปลงหรือแก้ไขเนื้อหาในคำเสนอแต่อย่างใด และได้มีการทำคำสนองส่งไปยังผู้ทำคำเสนอ เวลาที่คำ

สนองมีผลจึงมีความสำคัญต่อการเกิดของสัญญาและจะส่งผลต่อการเลือกใช้กฎหมายและเขตอำนาจในการบังคับตามสัญญาด้วย

ในการทำคำสนองของการทำสัญญาพาณิชย์อิเล็กทรอนิกส์จะมีวิธีการ เช่น การแสดงเจตนาผ่านทางไปรษณีย์อิเล็กทรอนิกส์ (E-mail) หรือวิธีการใช้เมาส์ (Mouse) กดปุ่มบนหน้าจอคอมพิวเตอร์ในตำแหน่งที่ผู้ขายได้กำหนดไว้ เพื่อแสดงเจตนาตกลงทำสัญญาพาณิชย์อิเล็กทรอนิกส์ ผ่านทางเว็บไซต์ซึ่งทำให้เกิดปัญหาขึ้นว่า สัญญาเกิดขึ้นเมื่อใด

สำหรับทฤษฎีการเกิดของสัญญาในปัจจุบันมีอยู่ด้วยกัน 4 ทฤษฎี คือ

1. สัญญาเกิดเมื่อมีการแสดงเจตนาสนองรับปรากฏแก่ผู้เสนอ (Theory of Acception)

2. สัญญาเกิดเมื่อผู้สนองส่งเจตนาสนองคำเสนอ (Theory of Dispatch)

3. สัญญาเกิดเมื่อเจตนาสนองรับคำเสนอไปถึงผู้เสนอ (Theory of Reception)

4. สัญญาเกิดเมื่อผู้เสนอรับรู้การแสดงเจตนาสนองคำเสนอแล้ว (Theory of Perception)

ซึ่งตามประมวลกฎหมายแพ่งและพาณิชย์ในปัจจุบันสัญญาเกิด ณ เวลา และสถานที่ ดังนี้

1. สัญญาระหว่างบุคคลผู้ห่างกันโดยระยะทางย่อมเกิดเป็นสัญญานั้นแต่เวลาเมื่อคำบอกกล่าวสนองไปถึงผู้เสนอ (มาตรา 361 วรรคแรก, 169 วรรคแรก) หรืออีกนัยหนึ่งสัญญาเกิดขึ้น ณ ที่ผู้เสนอได้รับคำสนองนั้น

2. สัญญาระหว่างบุคคลซึ่งอยู่เฉพาะหน้า ไม่ว่าจะมีการบ่งระยะเวลาให้ทำคำสนอง (มาตรา 354) หรือไม่มีการบ่งระยะเวลาให้ทำคำสนอง (มาตรา 356) เมื่อสนองรับต่อหน้าก็เกิดสัญญา ณ ที่สนองรับนั้น แต่ถ้าเป็นคำเสนอคำสนองโดยทางโทรศัพท์ต้องถือว่าสัญญาเกิด ณ ที่ผู้เสนอได้รับทราบคำสนองนั้นทางโทรศัพท์ เพราะถือว่าเป็นการสนองรับต่อหน้าผู้เสนอ ผู้เสนออยู่ ณ ที่ใด สัญญาย่อมเกิดขึ้น ณ ที่นั่น กล่าวคือ นำหลักมาตรา 169 มาใช้บังคับ สัญญาเกิดขึ้น ณ สถานที่ที่การแสดงเจตนาสนองรับไปถึงผู้เสนอ

3. สัญญาระหว่างบุคคลซึ่งเกิดจากการแสดงเจตนาสนองรับโดยปริยายโดยการกระทำอย่างหนึ่งซึ่งตามเจตนาอันผู้เสนอหรือตามปกติประเพณี ไม่จำเป็นจะต้องมีการบอกกล่าวสนองรับมาโดยชัดแจ้งก็สันนิษฐานได้เช่นนั้น สัญญาย่อมเกิด ณ ที่ซึ่งมีการอันใดอันหนึ่ง อันสันนิษฐานได้ว่าเป็นการแสดงเจตนาสนองรับ (มาตรา 361 วรรค 2) กล่าวคือ สนองรับ ณ ที่ใด สัญญาย่อมเกิดขึ้น ณ ที่นั่น

จะเห็นได้ว่า กฎหมายไทยในปัจจุบันยึดถือทฤษฎีที่ว่า สัญญาจะเกิดเมื่อเจตนาสนองรับคำเสนอกลับไปถึงผู้เสนอ (Theory of Reception) และเมื่อพิจารณาถึงการเกิดสัญญาทางอิเล็กทรอนิกส์แล้ว จะเห็นได้ว่ามาตรา 21 – 23[66] แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 นั้น เป็นไปในทิศทางเดียวกันกับการเกิดสัญญาตามกฎหมายแม่แบบของคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติว่าด้วยพาณิชย์อิเล็กทรอนิกส์ (UNCITRAL Model Law on Electronic Commerce)[67] ซึ่งมิได้ระบุไว้โดยตรงว่า

---

[66] มาตรา 21 เว้นแต่ผู้ส่งข้อมูลและผู้รับข้อมูลจะได้ตกลงกันไว้เป็นอย่างอื่น ให้ถือว่าได้มีการส่งข้อมูลอิเล็กทรอนิกส์เมื่อเวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่อยู่นอกเหนือการควบคุมของผู้ส่งข้อมูล

มาตรา 22 เว้นแต่ผู้ส่งข้อมูลและผู้รับข้อมูลจะได้ตกลงกันไว้เป็นอย่างอื่น ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลของผู้รับข้อมูล หากผู้รับข้อมูลได้กำหนดระบบข้อมูลที่ประสงค์จะใช้ในการรับข้อมูลอิเล็กทรอนิกส์ไว้โดยเฉพาะ ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่ผู้รับข้อมูลได้กำหนดไว้นั้น แต่ถ้าข้อมูลอิเล็กทรอนิกส์ดังกล่าวได้ส่งไปยังระบบข้อมูลอื่นของผู้รับข้อมูลซึ่งมิใช่ระบบข้อมูลที่ผู้รับข้อมูลกำหนดไว้ ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ได้เรียกข้อมูลอิเล็กทรอนิกส์จากระบบข้อมูลนั้น ความในมาตรานี้ให้ใช้บังคับแม้ระบบข้อมูลของผู้รับข้อมูลตั้งอยู่ในสถานที่อีกแห่งหนึ่งต่างหากจากสถานที่ที่ถือว่าผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์ตามมาตรา 23

มาตรา 23 เว้นแต่ผู้ส่งข้อมูลและผู้รับข้อมูลจะได้ตกลงกันไว้เป็นอย่างอื่น การส่งหรือการรับข้อมูลอิเล็กทรอนิกส์ให้ถือว่าได้ส่ง ณ ที่ทำการงานของผู้ส่งข้อมูล หรือได้รับ ณ ที่ทำการงานของผู้รับข้อมูล แล้วแต่กรณี ในกรณีที่ผู้ส่งข้อมูลหรือผู้รับข้อมูลมีที่ทำการงานหลายแห่ง ให้ถือเอาที่ทำการงานที่เกี่ยวข้องมากที่สุดกับธุรกรรมนั้นเป็นที่ทำการงานเพื่อประโยชน์ตามวรรคหนึ่ง แต่ถ้าไม่สามารถกำหนดได้ว่าธุรกรรมนั้นเกี่ยวข้องกับที่ทำการงานแห่งใดมากที่สุด ให้ถือเอาสำนักงานใหญ่เป็นสถานที่ที่ได้รับหรือส่งข้อมูลอิเล็กทรอนิกส์นั้น ในกรณีที่ไม่ปรากฏที่ทำการงานของผู้ส่งข้อมูลหรือผู้รับข้อมูล ให้ถือเอาถิ่นที่อยู่ปกติเป็นสถานที่ที่ส่งหรือได้รับข้อมูลอิเล็กทรอนิกส์ ความในมาตรานี้มิให้ใช้บังคับกับการส่งและการรับข้อมูลอิเล็กทรอนิกส์โดยวิธีการทางโทรเลข และโทร-พิมพ์ หรือวิธีการสื่อสารอื่นตามที่กำหนดในพระราชกฤษฎีกา

[67] Article 15 Time and place of dispatch and receipt of data message

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows :

-if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs :

(i) at the time when the data message enters the designated information system ; or

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee ;

-if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Paragraph applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph.

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph :

-if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business ;

-if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

(5) The provisions of this article do not apply to the following : [...],

สัญญาจะเกิดขึ้นเมื่อใด และที่ไหน กฎหมายดังกล่าวคงบัญญัติไว้แต่เพียงเวลา และสถานที่รับส่งข้อมูลทางอิเล็กทรอนิกส์เท่านั้น แต่เมื่อพิจารณาว่าสัญญาย่อมเกิดเมื่อคำเสนอคำสนองถูกต้องตรงกัน ดังนั้น เมื่อพิจารณาจากตัวบทกฎหมายแล้วสัญญาจะเกิดเมื่อเวลาคำบอกกล่าวสนองไปถึงผู้เสนอ คือเข้าไปสู่ระบบข้อมูลของผู้รับและสถานที่เกิดของสัญญาก็คือที่ซึ่งเป็นสถานที่ประกอบธุรกิจของผู้รับคำสนองนั่นเอง ซึ่งจะเห็นได้ว่าการเกิดของสัญญานี้เป็นไปตามทฤษฎี Theory of Reception เช่นเดียวกันนั่นเอง

4.3.2 การคุ้มครองผู้บริโภคในการใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์กับธนาคารพาณิชย์

ในการคุ้มครองผู้บริโภคในการใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์นั้น องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา หรือ OECD (Organization for Economic Co-operation and Development - OECD) ซึ่งเป็นองค์การระหว่างประเทศของกลุ่มประเทศพัฒนาแล้วที่ยอมรับระบอบประชาธิปไตยและเศรษฐกิจการค้าเสรี OECD ก่อตั้งขึ้นเมื่อ พ.ศ. 2491 ในฐานะที่เป็นองค์กรความร่วมมือทางเศรษฐกิจของภูมิภาคยุโรปและอเมริกา เป็นหน่วยงานกลางในการสร้างแบบแผนระเบียบปฏิบัติในเรื่องต่าง ๆ เพื่อให้ประเทศต่าง ๆ ได้นำหลักการนี้ไปใช้โดยอาจมีการนำไปเป็นต้นแบบในการร่างกฎหมายของแต่ละประเทศ และในประเด็นเรื่องการคุ้มครองครองผู้บริโภคนี้ OECD ได้วางแนวทางคุ้มครองการคุ้มครองผู้บริโภคไว้เป็นการเฉพาะสำหรับการทำพาณิชย์อิเล็กทรอนิกส์ ใน Guidelines for Consumer Protection in the Context of Electronic Commerce (1999) ซึ่งในการคุ้มครองผู้บริโภคที่เกี่ยวข้องกับพาณิชย์อิเล็กทรอนิกส์ควรที่จะได้รับการคุ้มครองไม่น้อยกว่าการคุ้มครองผู้บริโภคในกรณีทั่วไป

สำหรับแนวทางที่กำหนดขึ้นนี้ใช้กับพาณิชย์อิเล็กทรอนิกส์สำหรับผู้ประกอบธุรกิจกับผู้บริโภค แต่ไม่รวมถึงพาณิชย์อิเล็กทรอนิกส์ระหว่างผู้ประกอบธุรกิจด้วยกัน ซึ่งการซื้อขายสินค้าทางอินเตอร์เน็ท ก็อยู่ในบังคับของแบบแผนดังกล่าว โดยแบบแผนดังกล่าวแบ่งออกเป็นมาตรการในด้านต่างๆ ดังนี้

1) หลักการคุ้มครอง (ผู้บริโภค) ต้องชัดเจนและมีประสิทธิภาพ (Transparent and effective protection) โดยกำหนดให้ผู้ที่เกี่ยวข้องกับพาณิชย์อิเล็กทรอนิกส์ควรได้รับการคุ้มครองไม่น้อยไปกว่าการคุ้มครองผู้บริโภคในกรณีทั่วไป

2) แนวทางปฏิบัติว่าด้วยการดำเนินธุรกิจ การโฆษณา และวิธีการทางการตลาดที่เป็นธรรม (Fair business, advertising and marketing practices)

3) การเปิดเผยข้อมูลผ่านระบบออนไลน์ (Online disclosures)

4) ขั้นตอนการยืนยัน (Confirmation process)

5) การชำระเงิน (Payment)

6) การระงับข้อพิพาทและการเยียวยาความเสียหาย (Dispute resolution and redress)

7) ความเป็นส่วนตัว (Privacy)

8) การเผยแพร่ความรู้ และการประชาสัมพันธ์ (Education and awareness)

9) ความร่วมมือระหว่างประเทศ

4.3.3 บทวิเคราะห์ปัญหาทางกฎหมายในการจัดสรรความเสี่ยงระหว่างผู้บริโภคกับผู้ประกอบการ ในการประกอบธุรกรรมที่เกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์

ในปัจจุบันนี้ ลูกค้าของธนาคารพาณิชย์ส่วนใหญ่ไม่ค่อยมีความตระหนักถึงความสำคัญของข้อกำหนดและเงื่อนไขในการเข้าใช้บริการทางอิเล็กทรอนิกส์ต่าง ๆ ของธนาคาร ซึ่งอาจเกิดได้จากหลายสาเหตุ ซึ่งทำให้ลูกค้าที่ไม่ได้สนใจเหล่านั้น ไม่ทราบถึงสิทธิและหน้าที่ของตนขณะที่เข้าใช้บริการ และเมื่อเกิดปัญหาขึ้นก็อาจจะไม่มีสิทธิเรียกร้องค่าเสียหายใด ๆ จากธนาคารได้อย่างเต็มเม็ดเต็มหน่วยสักเท่าใดนัก

อย่างไรก็ตาม แม้ลูกค้าหรือผู้ใช้บริการจะไม่ค่อยมีอำนาจในการต่อรองในการแก้ไขหรือกำหนดเงื่อนไขในสัญญาก็ตาม แต่ธนาคารพาณิชย์ทุกแห่งในประเทศก็อยู่ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย และต้องปฏิบัติตามระเบียบ หรือข้อบังคับของธนาคารแห่งประเทศไทยอยู่แล้ว จึงทำให้ธนาคารต่าง ๆ ไม่สามารถร่างข้อกำหนดหรือเงื่อนไขต่าง ๆ ได้ตามใจชอบสักเท่าใดนัก

นอกจากนี้ สำนักคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) ก็เริ่มมีบทบาทมากขึ้นในการที่จะเข้ามาคุ้มครองดูแลสิทธิของผู้บริโภค 5 ประการ ดังนี้

1. สิทธิที่จะได้รับข่าวสารรวมทั้งคำพรรณนาคุณภาพที่ถูกต้องและเพียงพอเกี่ยวกับสินค้าหรือบริการ ได้แก่ สิทธิที่จะได้รับการโฆษณาหรือการแสดงฉลากตามความเป็นจริงและปราศจากพิษภัยแก่ผู้บริโภค รวมตลอดถึงสิทธิที่จะได้รับทราบข้อมูลเกี่ยวกับสินค้าหรือบริการอย่างถูกต้องและเพียงพอที่จะไม่หลงผิด ในการซื้อสินค้าหรือรับบริการโดยไม่เป็นธรรม

2. สิทธิที่จะมีอิสระในการเลือกหาสินค้าหรือบริการ ได้แก่ สิทธิที่จะเลือกซื้อสินค้าหรือรับบริการโดยความสมัครใจของผู้บริโภค และปราศจากการชักจูงใจอันไม่เป็นธรรม

3. สิทธิที่จะได้รับความปลอดภัยจากการใช้สินค้าหรือบริการ ได้แก่ สิทธิที่จะได้รับสินค้าหรือบริการที่ปลอดภัย มีสภาพและคุณภาพได้มาตรฐานเหมาะสมแก่การใช้ ไม่ก่อให้เกิดอันตรายต่อชีวิต ร่างกายหรือทรัพย์สิน ในกรณีใช้ตามคำแนะนำหรือระมัดระวังตามสภาพของสินค้าหรือบริการนั้นแล้ว

4. สิทธิที่จะได้รับความเป็นธรรมในการทำสัญญา ได้แก่ สิทธิที่จะได้รับข้อสัญญาโดยไม่ถูกเอารัดเอาเปรียบจากผู้ประกอบธุรกิจ

5. สิทธิที่จะได้รับการพิจารณาและชดเชยความเสียหาย ได้แก่ สิทธิที่จะได้รับการคุ้มครองและชดใช้ค่าเสียหาย เมื่อมีการละเมิดสิทธิของผู้บริโภคตามข้อ 1, 2, 3 และ 4 ดังกล่าว

ทั้งนี้ การจะคุ้มครองสิทธิต่าง ๆ ของผู้บริโภคนั้น สำนักงานคุ้มครองผู้บริโภคจะต้องออกประกาศในเรื่องที่จะควบคุม เช่น ประกาศระเบียบคณะกรรมการว่าด้วยสัญญา เรื่อง ให้ธุรกิจบัตรเครดิตเป็นธุรกิจที่ควบคุมสัญญา, ประกาศระเบียบคณะกรรมการว่าด้วยสัญญา เรื่อง ให้ธุรกิจให้กู้ยืมเงินเพื่อผู้บริโภคของสถาบันการเงินเป็นธุรกิจที่ควบคุมสัญญา, ประกาศระเบียบคณะกรรมการว่าด้วยสัญญา เรื่อง ให้ธุรกิจให้เช่าซื้อรถยนต์และรถจักรยานยนต์เป็นธุรกิจที่ควบคุมสัญญา เป็นต้น

แต่จะเห็นได้ว่าในปัจจุบันยังไม่มีประกาศใด ๆ ของสำนักงานคุ้มครองผู้บริโภคที่จะเข้ามาควบคุมสัญญาทางอิเล็กทรอนิกส์ของธนาคารหรือบริการต่าง ๆ เลย ซึ่งทำให้ในปัจจุบันหากมีคดีที่จะต้องฟ้องร้องขึ้นสู่ศาลโดยลูกค้าเป็นผู้ฟ้องร้องตามประมวลกฎหมายวิธีพิจารณาความแพ่งมาตรา 84 [68]นั้น ได้กำหนดให้ผู้ที่กล่าวอ้างนั้นมีหน้าที่ในการนำสืบต่อศาล ซึ่งในความเป็นจริงแล้วนั้นเป็นเรื่องที่ยากมากโดยเฉพาะในการทำสัญญาทางอิเล็กทรอนิกส์ ถ้าลูกค้าจะต้องมีหน้าที่นำสืบให้ศาลเห็นถึงความเสียหายที่เกิดขึ้น

---

[68] มาตรา 84 ว่า “ถ้าคู่ความฝ่ายใดฝ่ายหนึ่งกล่าวอ้างข้อเท็จจริงอย่างใด ๆ เพื่อสนับสนุนคำฟ้องหรือคำให้การของตน ให้หน้าที่นำสืบข้อเท็จจริงนั้นตกอยู่แก่คู่ความฝ่ายกล่าวที่อ้าง

แต่ว่า (1) คู่ความไม่ต้องพิสูจน์ข้อเท็จจริง ซึ่งเป็นที่รู้กันอยู่ทั่วไป หรือซึ่งมิอาจโต้แย้งได้ หรือซึ่งศาลเห็นว่าคู่ความอีกฝ่ายหนึ่งได้รับแล้ว

(2) ถ้ามีข้อสันนิษฐานไว้ในกฎหมายเป็นคุณแก่คู่ความฝ่ายใด คู่ความฝ่ายนั้นต้องพิสูจน์แต่เพียงว่า ตนได้ปฏิบัติตามเงื่อนไขแห่งการที่ตนจะได้รับประโยชน์จากข้อสันนิษฐานนั้นครบถ้วนแล้ว”

ดังนี้ในส่วนของการจัดสรรความเสี่ยงระหว่างลูกค้ากับธนาคารพาณิชย์ในการเข้าใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์นั้น **ผู้เขียนมีความเห็นว่า ธนาคารแห่งประเทศไทยควรจะนำแนวทางคุ้มครองผู้บริโภคในธุรกิจพาณิชย์อิเล็กทรอนิกส์** (OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999)) **ซึ่งเป็นแนวทางสากลในการคุ้มครองผู้บริโภคมาปรับใช้ โดยอาจออกเป็นประกาศเพื่อให้ธนาคารพาณิชย์ภายใต้กำกับปฏิบัติตาม และนอกจากนี้สำนักงานคณะกรรมการผู้บริโภค (สคบ.) ก็ควรจะมีการออกประกาศของคณะกรรมการว่าด้วยสัญญา ในเรื่องเกี่ยวกับการคุ้มครองการให้บริการทางอิเล็กทรอนิกส์ของสถาบันการเงิน เพื่อช่วยคุ้มครองผู้บริโภคและผลักภาระการนำสืบให้ไปอยู่กับธนาคารพาณิชย์แทน**

4.4 ปัญหาทางกฎหมายในแง่ของการสนับสนุนหรือขัดขวางการให้บริการและการทำธุรกรรมเกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์

ย้อนกลับไปเมื่อปี พ.ศ. 2541 กระทรวงการต่างประเทศได้เสนอต่อคณะรัฐมนตรีในกระทรวงและหน่วยงานต่าง ๆ แบ่งกันรับผิดชอบพิจารณาปรับปรุงและพัฒนากฎหมายการค้าระหว่างประเทศของไทยให้ สอดคล้องกับอนุสัญญาต่าง ๆ ที่ประเทศไทยได้มีพันธะลงนามกับต่างประเทศ รวมทั้งกฎหมายแม่แบบต่าง ๆ ซึ่งคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติ (UNCITRAL) ได้ยกร่างขึ้น กระทรวงยุติธรรมได้รับผิดชอบในการปรับปรุงแก้ไขกฎหมายเกี่ยวกับการพาณิชย์ทางอิเล็กทรอนิกส์ และต่อมาคณะรัฐมนตรีได้เห็นชอบอนุมัติให้แต่งตั้งคณะกรรมการเพื่อศึกษาและพิจารณาปรับปรุงกฎหมายเกี่ยวกับการค้าระหว่างประเทศของไทยขึ้น โดยมีวัตถุประสงค์ให้คณะกรรมการชุดนี้มีอำนาจหน้าที่ในการพิจารณาปรับปรุงกฎหมายเกี่ยวกับการค้าระหว่างประเทศของไทยรวมทั้งเรื่องการพาณิชย์ทางอิเล็กทรอนิกส์ให้สอดคล้องกับประเพณีปฏิบัติทางการค้าระหว่างประเทศ และให้เป็นไปในแนวทางเดียวกันกับกฎหมายแม่แบบของคณะกรรมาธิการการค้าระหว่างประเทศแห่งสหประชาชาติ (UNCITRAL Model Law) รวมทั้งให้ยกร่างกฎหมายที่เกี่ยวข้องเพื่อให้เกิดความชัดเจนและสามารถนำไปใช้ให้เกิดความเป็นธรรมแก่คู่ค้าและผู้เกี่ยวข้องในวงการธุรกิจการค้าทั้งในและระหว่างประเทศ ซึ่งคณะกรรมการดังกล่าวได้ยกร่างพระราชบัญญัติการพาณิชย์ทางอิเล็กทรอนิกส์ พ.ศ. .... แล้วเสร็จเมื่อปลายปี พ.ศ. 2542

ต่อมา ในปี พ.ศ. 2541 คณะรัฐมนตรีได้มีมติให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติเป็นผู้ดำเนินการโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศขึ้น โครงการดังกล่าวประกอบด้วยการศึกษาและยกร่างกฎหมาย 6 ฉบับ[69] ได้แก่

1) กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Law) ซึ่งเป็นกฎหมายที่รับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อันเป็นการรองรับนิติสัมพันธ์ต่าง ๆ ซึ่งแต่เดิมอาจจะจัดทำขึ้นในรูปแบบของหนังสือให้เท่าเทียมกับนิติสัมพันธ์รูปแบบใหม่ที่จัดทำขึ้นให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ รวมตลอดทั้งการลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ และการรับฟังพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ (มีผลใช้บังคับเมื่อวันที่ 3 เมษายน 2545)

2) กฎหมายลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signatures Law) ซึ่งเป็นกฎหมายที่รับรองการใช้ลายมือชื่ออิเล็กทรอนิกส์ด้วยกระบวนการใด ๆ ทางเทคโนโลยีให้เสมอด้วยการลงลายมือชื่อธรรมดา อันส่งผลต่อความเชื่อมั่นมากขึ้นในการทำธุรกรรมทางอิเล็กทรอนิกส์ และกำหนดให้มีการกำกับดูแลการให้บริการเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ตลอดจนการให้บริการอื่นที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ ทั้งนี้ กฎหมายฉบับนี้ไม่ได้มีการจัดทำแยกเป็นอีกหนึ่งฉบับ เพราะได้มีการรวมหลักการไว้กับกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (มีผลใช้บังคับแล้วเมื่อวันที่ 3 เมษายน 2545)

3) กฎหมายการโอนเงินทางอิเล็กทรอนิกส์ (Electronic Funds Transfer Law) ซึ่งเป็นกฎหมายที่กำหนดกลไกสำคัญทางกฎหมายในการรองรับระบบการโอนเงินทางอิเล็กทรอนิกส์ทั้งที่เป็นการโอนเงินระหว่างสถาบันการเงิน และระบบการชำระเงินรูปแบบใหม่ในรูปของเงินอิเล็กทรอนิกส์ก่อให้เกิดความเชื่อมั่นต่อระบบการทำธุรกรรมทางการเงินและการทำธุรกรรมทางอิเล็กทรอนิกส์มากยิ่งขึ้น (มีผลใช้บังคับแล้วเมื่อวันที่ 14 มกราคม 2552)

4) กฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Computer Crime Law) ซึ่งเป็นกฎหมายที่กำหนดมาตรการทางอาญาในการลงโทษผู้กระทำผิดต่อระบบการทำงานของคอมพิวเตอร์ ระบบข้อมูล และระบบเครือข่าย ซึ่งในปัจจุบันยังไม่มีบทบัญญัติของกฎหมายฉบับใด

---

[69]สืบค้นจาก http://www.nectec.or.th/index.php?option=com_content&view=article&id=79:-2550&catid=40:technology-news&Itemid=165.

กำหนดว่าเป็นความผิด ทั้งนี้ เพื่อเป็นหลักประกันสิทธิเสรีภาพและการคุ้มครองการอยู่ร่วมกันของสังคม (มีผลใช้บังคับแล้วเมื่อวันที่ 19 กรกฎาคม 2550)

5) กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Law) ซึ่งเป็นกฎหมายที่ก่อให้เกิดการรับรองสิทธิและให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจถูกประมวลผล เปิดเผยหรือเผยแพร่ถึงบุคคลจำนวนมากได้ในระยะเวลาอันรวดเร็วโดยอาศัยพัฒนาการทางเทคโนโลยี จนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ในทางมิชอบอันเป็นการละเมิดต่อเจ้าของข้อมูล ทั้งนี้ โดยคำนึงถึงการรักษาดุลยภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัว เสรีภาพในการติดต่อสื่อสารและความมั่นคงของรัฐ (ปัจจุบันอยู่ระหว่างการดำเนินการปรับร่าง)

6) กฎหมายเกี่ยวกับการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน (กฎหมายลำดับรองของรัฐธรรมนูญมาตรา 78) (National Information Infrastructure Law) เพื่อเป็นกฎหมายที่ก่อให้เกิดการส่งเสริม สนับสนุน และพัฒนาโครงสร้างพื้นฐานสารสนเทศ อันได้แก่ โครงข่ายโทรคมนาคมเทคโนโลยีสารสนเทศ ทรัพยากรมนุษย์ และโครงสร้างพื้นฐานสารสนเทศสำคัญอื่น ๆ อันเป็นปัจจัยพื้นฐานสำคัญในการพัฒนาสังคมและชุมชนโดยอาศัยกลไกของรัฐ ซึ่งรองรับเจตนารมณ์สำคัญประการหนึ่งของแนวนโยบายพื้นฐานแห่งรัฐตามรัฐธรรมนูญมาตรา 78 ในการกระจายสารสนเทศให้ทั่วถึงและเท่าเทียมกัน และนับเป็นกลไกสำคัญในการช่วยลดความเหลื่อมล้ำของสังคมอย่างค่อยเป็นค่อยไป เพื่อสนับสนุนให้ท้องถิ่นมีศักยภาพในการปกครองตนเอง พัฒนาเศรษฐกิจภายในชุมชน และนำไปสู่สังคมแห่งปัญญาและการเรียนรู้ (ปัจจุบันอยู่ระหว่างการดำเนินการปรับร่าง)

ทั้งนี้ เมื่อพิจารณาถึงหลักการและลายละเอียดของกฎหมาย 3 ฉบับแรก แล้วพบว่าเป็นกฎหมายที่ส่งเสริมการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารในเชิงสร้างสรรค์ อันเอื้อต่อการทำธุรกรรมทางอิเล็กทรอนิกส์หรือพาณิชย์อิเล็กทรอนิกส์ หรือการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ส่วนกฎหมายในลำดับที่ 4 และลำดับ 5 นั้นเป็นกฎหมายที่จะใช้เป็นมาตรการในการคุ้มครองหรือปกป้องสังคมจากการประยุกต์ ใช้เทคโนโลยีสารสนเทศและการสื่อสารในเชิงไม่สร้างสรรค์ และฉบับสุดท้ายเป็นกฎหมายฉบับที่จะสร้างกลไกเพื่อลดความเหลื่อมล้ำของสังคม สารสนเทศของประเทศไทยต่อไป

สำหรับปัญหาทางกฎหมายในแง่ของการสนับสนุนหรือขัดขวางการให้บริการและการทำธุรกรรมเกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์นั้น พบว่านับตั้งแต่ปี พ.ศ. 2544 ที่ประเทศไทยได้มี พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ออกมาบังคับใช้ แต่จำนวนการทำธุรกรรมทางอิเล็กทรอนิกส์ในประเทศกลับไม่ค่อยเติบโตอย่างที่ควรจะเป็น ซึ่งก็อาจจะมีหลาย

เหตุปัจจัยที่เป็นอุปสรรคต่อการเติบโตของการทำธุรกรรมอิเล็กทรอนิกส์ในประเทศ โดยสาเหตุสำคัญประการหนึ่งก็น่าจะเกิดจากผู้ประกอบการธุรกิจ และผู้บริโภคยังไม่เกิดความมั่นใจในการบังคับใช้กฎหมายในเรื่องการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยเห็นได้จากนับตั้งแต่พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มีผลบังคับใช้มาจนกระทั่งถึงปัจจุบันนี้ ยังไม่เคยมีข้อพิพาทที่มีการฟ้องร้องกันตามพระราชบัญญัติดังกล่าวเลยแม้แต่คดีเดียว

ในส่วนของการทำธุรกรรมหรือให้บริการที่เกี่ยวกับธนาคารพาณิชย์อิเล็กทรอนิกส์นั้น ถึงแม้หลายธนาคารจะนำมาให้บริการแก่ลูกค้าของธนาคารหลายปีแล้ว แต่การให้บริการดังกล่าวนั้นก็มิได้มีกฎหมายที่กำกับดูแลโดยตรง มีเพียงธนาคารแห่งประเทศไทยที่อาศัยอำนาจของตนในการออกประกาศเกี่ยวกับหลักเกณฑ์ ข้อปฏิบัติ ในเบื้องต้นเพื่อให้ธนาคารพาณิชย์ต่าง ๆ ที่อยู่ภายใต้การกำกับดูแลนำไปใช้ จนกระทั่งเกิดความพยายามของหลายองค์กร และหน่วยงานที่ต้องการผลักดันให้พาณิชย์อิเล็กทรอนิกส์ในประเทศไทยมีการเติบโตมากยิ่งขึ้น ได้ร่วมกันผลักดันให้มีตราพระราชกฤษฎีกาที่เกี่ยวข้องกับการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ขึ้น โดยธนาคารแห่งประเทศไทยซึ่งมีความศักยภาพและความพร้อมในด้านต่าง ๆ มากที่สุดได้ผลักดันจนสามารถตราพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 ออกมามีผลบังคับใช้ได้ในปี 2552 ที่ผ่านมานี้เอง

ซึ่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 ฉบับดังกล่าวนี้ ธนาคารแห่งประเทศไทยได้มุ่งหวังให้เป็นกฎหมายที่สนับสนุนให้เกิดการทำธุรกรรม และให้บริการทางพาณิชย์อิเล็กทรอนิกส์มากยิ่งขึ้น โดยเปิดโอกาสให้บริษัทอื่น ๆ นอกจากธนาคารพาณิชย์สามารถเข้ามาเป็นผู้ให้บริการบางประเภทตามพระราชกฤษฎีกาดังกล่าวได้ แต่จะต้องมีคุณสมบัติครบถ้วนตามหลักเกณฑ์ที่ธนาคารแห่งประเทศไทยกำหนดไว้ แต่อย่างไรก็ตาม การให้บริการชำระเงินทางอิเล็กทรอนิกส์นี้ก็จัดเป็นเพียงส่วนหนึ่งของกิจการธนาคารพาณิชย์อิเล็กทรอนิกส์เท่านั้น กฎหมายที่มีอยู่ในปัจจุบันยังไม่สามารถครอบคลุมถึงการให้บริการของธนาคารพาณิชย์อิเล็กทรอนิกส์ได้ทุกประเภท ซึ่งทำให้ธนาคารพาณิชย์หลายแห่ง และผู้บริโภคจำนวนมากยังมั่นใจในการให้บริการทางอิเล็กทรอนิกส์ของธนาคารอย่างที่ควรจะเป็น

นอกจากในส่วนของการตรากฎหมายแล้ว สิ่งที่เป็นอุปสรรคสำคัญอีกประการหนึ่งก็คือ การบังคับใช้กฎหมายนั่นเอง ซึ่งในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 นั้นก็ประสบปัญหาดังกล่าวด้วยเช่นกัน โดยในพระราชบัญญัติดังกล่าวได้กำหนดให้มีการจัดตั้งหน่วยงานที่มีหน้าที่ในการรับรองลายมือชื่ออิเล็กทรอนิกส์ขึ้น แต่ในปัจจุบันก็การจัดตั้ง

หน่วยงานดังกล่าวก็ยังไม่สามารถเกิดขึ้นได้ นอกจากนี้ในการทำหน้าที่กำกับดูแลและช่วยส่งเสริมให้พาณิชย์ธุรกรรมอิเล็กทรอนิกส์ในประเทศเติบโตก็เกิดความทับซ้อนในเรื่องของหน้าที่และความรับผิดชอบระหว่างหน่วยงานขึ้น โดยพระราชบัญญัติฉบับนี้ได้มีการตราขึ้นตั้งแต่ปี พ.ศ. 2544 โดยให้กำหนดให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ทำหน้าที่เป็นหน่วยงานธุรการของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ แต่พอในปี พ.ศ. 2545 ก็ได้มีการจัดตั้งกระทรวงเทคโนโลยีสารสนเทศ และการสื่อสารขึ้น ซึ่งทำให้หน้าที่ความรับผิดชอบบางประการอยู่ในความดูแลของหน่วยงานที่แตกต่างกันออกไป ทำให้การผลักดันและสนับสนุนให้มีธุรกรรมทางอิเล็กทรอนิกส์นั้นเป็นไปในทิศทางที่ไม่ชัดเจน และขาดความเป็นเอกเทศ ซึ่งส่งผลให้ธนาคารพาณิชย์อิเล็กทรอนิกส์ซึ่งเป็นส่วนหนึ่งของพาณิชย์อิเล็กทรอนิกส์นั้น ไม่สามารถพัฒนาและเติบโตได้อย่างเต็มที่เช่นเดียวกัน