คำนำ

สืบเนื่องจากพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งตราขึ้นเพื่อรับรองผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์และจะมีผลใช้บังคับในวันที่ 3 เมษายน 2545 นี้นั้น นับเป็นกฎหมายเทคโนโลยีสารสนเทศฉบับแรกที่ตราขึ้นใช้บังคับ โดยกำหนดขอบเขตการใช้บังคับกับ "ธุรกรรมทางอิเล็กทรอนิกส์" หรือที่นิยมเรียกว่า "พาณิชย์อิเล็กทรอนิกส์" ซึ่งครอบคลุมทั้งกิจกรรมในทางแพ่งและพาณิชย์ รวมถึงการดำเนินงานของรัฐที่ใช้วิธีการทางอิเล็กทรอนิกส์ และอาจมีลักษณะเฉพาะที่ต่างไปจากระบบกระดาษ ดังนั้น พระราชบัญญัติฉบับนี้จึงตราขึ้นเสริมหรือใช้ประกอบกับกฎหมายทุกฉบับที่ใช้บังคับอยู่ในปัจจุบันเพื่อรองรับนิติสัมพันธ์ที่เกิดขึ้นในรูปของข้อมูลอิเล็กทรอนิกส์

อย่างไรก็ตาม สาระสำคัญของพระราชบัญญัติบางส่วนได้มีการเพิ่มเติมในชั้นการพิจารณาของวุฒิสภาเพื่อให้เหมาะสมขึ้นและเพื่อให้เป็นไปตามหลักการสำคัญของกฎหมายแม่แบบว่าด้วยพาณิชย์อิเล็กทรอนิกส์ และกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ ของคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติ ดังนั้น คำอธิบายพระราชบัญญัติฉบับนี้จึงได้จัดทำขึ้นโดยปรับสาระสำคัญในส่วนที่เกี่ยวกับกฎหมายแม่แบบจากคำอธิบายร่างพระราชบัญญัติซึ่งเคยจัดทำขึ้นเผยแพร่ พร้อมทั้งคำอธิบายถึงเจตนารมณ์และการบังคับใช้สำหรับบทบัญญัติที่เพิ่มเติมในภายหลัง

ทั้งนี้ คำอธิบายฉบับนี้จัดทำขึ้นและปรับปรุงโดยความอนุเคราะห์ของศาสตราจารย์พิเศษ ชัยวัฒน์ วงศ์วัฒนศานต์ ซึ่งมีบทบาทสำคัญยิ่งต่อการพิจารณาพระราชบัญญัติฉบับนี้ในกระบวนการนิติบัญญัติ และสำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และ

คอมพิวเตอร์แห่งชาติ จึงหวังว่าคำอธิบายพระราชบัญญัติฉบับนี้คงก่อให้เกิดประโยชน์อย่างยิ่งต่อการทำความเข้าใจเบื้องต้นเมื่อกฎหมายมีผลใช้บังคับ

ศาสตราจารย์ ไพรัช ธัชยพงษ์
ผู้อำนวยการ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม

บทสรุป

เนื่องด้วยปัจจุบันเมื่อเทคโนโลยีเริ่มเข้ามามีบทบาทต่อการดำเนินกิจกรรมหรือประกอบธุรกรรมต่าง ๆ ของมนุษย์มากขึ้น เป็นเหตุให้ต้องมีการปรับปรุงและพัฒนากฎหมายซึ่งเป็นกฎเกณฑ์ที่กำหนดขึ้นเพื่อรองรับการดำเนินกิจกรรมต่าง ๆ ของมนุษย์ให้สอดคล้องกับพัฒนาและความก้าวหน้าทางเทคโนโลยีดังกล่าว ดังนั้น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 จึงถูกตราขึ้นเพื่อใช้เสริมหรือใช้ประกอบกับกฎหมายที่ใช้บังคับอยู่ในปัจจุบันทุกฉบับ ในกรณีที่ธุรกรรมหรือกิจกรรมที่กระทำภายใต้กฎหมายที่ใช้บังคับอยู่ในปัจจุบันในระบบกระดาษเปลี่ยนไปกระทำด้วยวิธีการทางอิเล็กทรอนิกส์

พระราชบัญญัติฉบับนี้วางอยู่บนหลักการพื้นฐานที่สำคัญ 2 ประการ คือ หลักความเท่าเทียมกัน (Functional Equivalent Approach) ซึ่งหมายความถึงความเท่าเทียมกันระหว่างการใช้ข้อความที่อยู่ในรูปของกระดาษกับข้อความที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ และหลักความเป็นกลางทางเทคโนโลยีและความเป็นกลางของสื่อ (Technology Neutrality / Media Neutrality) ซึ่งหมายความว่ากฎหมายจะต้องเปิดกว้างเพื่อรองรับการติดต่อสื่อสารด้วยวิธีการทางอิเล็กทรอนิกส์ในทุกรูปแบบ ทั้งที่มีอยู่ในปัจจุบันและที่จะมีการพัฒนาขึ้นในอนาคต

อย่างไรก็ตาม พระราชบัญญัติฉบับนี้นับเป็นกฎหมายพื้นฐานฉบับหนึ่ง ซึ่งตราขึ้นเพื่อรองรับความก้าวหน้าทางเทคโนโลยี และจำเป็นต้องตรากฎหมายลำดับพระราชกฤษฎีกาหรือกำหนดหลักเกณฑ์ต่าง ๆ ออกมารองรับรายละเอียดของกฎหมาย อันมีผลต่อการดำเนินธุรกิจหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ทั้งภาครัฐ

และภาคเอกชน ซึ่งนับวันจะยิ่งมีบทบาทและความสำคัญต่อชีวิตประจำวันมากขึ้นทุกขณะ จึงอาจเป็นกฎหมายอีกฉบับหนึ่งที่จำเป็นต้องติดตามความคืบหน้าอย่างใกล้ชิด

นายทวีศักดิ์ กออนันตกูล
ผู้อำนวยการ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ผู้แต่ง

1. ศาสตราจารย์พิเศษ ชัยวัฒน์ วงศ์วัฒนศานต์
เลขาธิการคณะกรรมการกฤษฎีกา
สำนักงานคณะกรรมการกฤษฎีกา

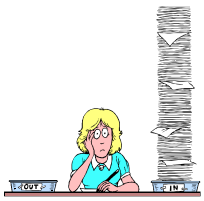
2. นายทวีศักดิ์ กออนันตกูล
ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

3. นางสุรางคณา แก้วจำนงค์
หัวหน้าโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ

สารบัญ

บทที่ 2 ลายมือชื่ออิเล็กทรอนิกส์

บทนำ



1. ความเป็นมาของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

สืบเนื่องจากเมื่อวันที่ 28 กุมภาพันธ์ 2539 คณะรัฐมนตรีได้มีมติเห็นชอบต่อนโยบายเทคโนโลยีสารสนเทศแห่งชาติ (ไอที ๒๐๐๐) เพื่อพัฒนาสังคมและเสริมสร้างความแข็งแกร่งทางด้านธุรกิจอุตสาหกรรมและการค้าระหว่างประเทศ ในการก้าวเข้าสู่ยุคเศรษฐกิจใหม่แห่งศตวรรษที่ ๒๑ โดยหนึ่งในมาตรการสำคัญของนโยบายดังกล่าว คือ การปฏิรูปกฎหมายเทคโนโลยีสารสนเทศ

ต่อมาเมื่อวันที่ ๑๕ ธันวาคม ๒๕๔๑ คณะรัฐมนตรีได้มีมติเห็นชอบให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ดำเนินโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ ที่เสนอโดยกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม และให้คณะกรรมการฯ เป็นศูนย์กลางดำเนินการและประสานงานระหว่างหน่วยงานต่างๆ ที่กำลังดำเนินการจัดทำกฎหมายเทคโนโลยีสารสนเทศและกฎหมายอื่นๆ ที่เกี่ยวข้องโดยมีศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ทำหน้าที่เป็นเลขานุการคณะกรรมการฯ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค) ในฐานะสำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ได้ดำเนินโครงการพัฒนากฎหมาย

เทคโนโลยีสารสนเทศ ซึ่งประกอบด้วยกฎหมาย 6 ฉบับ ได้แก่ กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ (เดิมเรียกว่า "กฎหมายแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์") กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ (ต่อมาได้มีการรวมหลักการเข้ากับกฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ และรวมเรียกชื่อเดียวว่า "กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์") กฎหมายเกี่ยวกับการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน (เดิมเรียกว่า "กฎหมายลำดับรองของรัฐธรรมนูญ มาตรา 78") กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ และกฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์

อนึ่ง เพื่อให้บรรลุวัตถุประสงค์หลักในการดำเนินงานของโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศในการยกร่างกฎหมายเทคโนโลยีสารสนเทศทั้ง 6 ฉบับข้างต้น คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ จึงได้แต่งตั้งคณะอนุกรรมการเฉพาะกิจขึ้นมา 6 คณะ ประกอบด้วยผู้แทนจากหน่วยงานต่างๆ ที่เกี่ยวข้องทั้งภาครัฐและภาคเอกชน และผู้ทรงคุณวุฒิทั้งจากสาขานิติศาสตร์ รัฐศาสตร์ วิศวกรรมศาสตร์ วิทยาการคอมพิวเตอร์ การเงินการธนาคาร และอื่นๆ ที่เกี่ยวข้อง เพื่อทำหน้าที่ในการพิจารณายกร่างกฎหมายโดยมีศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติเป็นเลขานุการในการยกร่างกฎหมายดังกล่าว

สำหรับการยกร่างกฎหมายเทคโนโลยีสารสนเทศในส่วนที่เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ นั้น แต่เดิมได้แยกออกเป็น 2 ฉบับ เนื่องจากหลักการของกฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ นั้น ตราขึ้นเพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ เพื่อให้ข้อความที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์มีสถานะเท่าเทียมกับข้อความที่ปรากฏอยู่บนกระดาษ หลักการดังกล่าวมีลักษณะเป็นกฎหมายกลางที่เสริมประมวลกฎหมายแพ่งและพาณิชย์ เพียงแต่อาจจะมีขอบเขตการบังคับใช้กว้างขวางมากเนื่องจากใช้ครอบคลุมธุรกรรมทุกประเภทที่ใช้วิธีการทางอิเล็กทรอนิกส์ ทั้งกิจกรรมทางแพ่ง ทางพาณิชย์ และการดำเนินงานของรัฐ และยังรับรองสถานะทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์ซึ่ง

ใช้ในการยืนยันตัวบุคคลเอาไว้ด้วย เพื่อให้ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นมีสถานะเช่นเดียวกับลายมือชื่อธรรมดาของมนุษย์ ทั้งนี้ เพื่อเอื้อประโยชน์และก่อให้เกิดความมั่นใจอย่างเต็มที่ในการทำธุรกรรมทางอิเล็กทรอนิกส์

แม้มีการรับรองสถานะทางกฎหมายทั้งของข้อมูลอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ไว้ในฉบับเดียวกัน ซึ่งเป็นกฎหมายฉบับแรกที่มีการยกร่างแล้วเสร็จ คือ กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ แต่หลักการสำคัญ ๆ เกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์นั้น ได้แยกไว้ในกฎหมายฉบับที่ 2 ที่ได้ยกร่างขึ้น ได้แก่ กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ เพื่อให้กฎหมายทั้งสองฉบับมีความเป็นอิสระจากกัน เพราะแม้ว่ากฎหมายฉบับแรกจะรองรับสถานะทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์ไว้ด้วยก็ตาม แต่ก็เป็นการบัญญัติรองรับไว้เพื่อเอื้อให้เกิดความสะดวกต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ในกรณีที่กฎหมายกำหนดให้มีการลงลายมือชื่อเท่านั้น ส่วนหลักการสำคัญของลายมือชื่ออิเล็กทรอนิกส์นั้นจะไปกำหนดไว้ในกฎหมายฉบับที่ 2 ซึ่งจะครอบคลุมหลักการสำคัญในการยืนยันตัวบุคคลและตรวจสอบตัวบุคคลทั้งโดยวิธีการที่ไม่ซับซ้อนและวิธีการซับซ้อน ซึ่งคณะอนุกรรมการเฉพาะกิจเพื่อพิจารณายกร่างกฎหมายฯ เห็นว่าน่าจะมีการกำหนดหลักการสำคัญเพื่อรองรับหลักการสำคัญของการใช้เทคโนโลยีที่นิยมใช้ทั้งในปัจจุบันและคาดการณ์ว่าจะยังคงนิยมใช้ในอนาคตไปอีกนานมากเอาไว้ด้วย เพื่อให้เกิดความมั่นใจในการใช้บังคับกฎหมายซึ่งผ่านการพิจารณาของฝ่ายนิติบัญญัติเพราะมีการตราหลักการสำคัญไว้ในกฎหมายอย่างครบถ้วน

อนึ่ง กฎหมายทั้งสองฉบับเป็นกฎหมายที่รัฐบาลต้องการเร่งรัดผลักดันเพื่อให้มีผลใช้บังคับโดยเร็ว เพราะนับเป็นโครงสร้างพื้นฐานที่สำคัญในการเอื้อประโยชน์และส่งเสริมสนับสนุนต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ และด้วยเนื้อหาของกฎหมายซึ่งอาจค่อนข้างยากต่อการทำความเข้าใจในเบื้องต้นเนื่องจากอิงอยู่กับพื้นฐานของความก้าวหน้าทางเทคโนโลยี ประกอบกับข้อจำกัดในการใช้คำศัพท์ต่าง ๆ ซึ่งมักเป็นคำศัพท์ใหม่ ๆ โดยเฉพาะอย่างยิ่งคำที่มีความหมายในทางเทคโนโลยี แม้บางคำจะมีการแปลไว้ในศัพท์บัญญัติของราชบัณฑิตยสถานแล้วก็ตาม แต่ก็ไม่ได้มีการอธิบายความหมายไว้แต่อย่างใด จึงมีส่วนทำให้การพิจารณายกร่างกฎหมายนั้น

จำเป็นต้องใช้ระยะเวลาพอสมควร ดังนั้นการพิจารณาแยกร่างกฎหมายทั้งสองฉบับออกจากกัน จึงอาจส่งผลให้การพิจารณายกร่างกฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ซึ่งมีหลักการสำคัญอยู่เพียงไม่กี่มาตรานั้นสามารถกระทำได้ค่อนข้างเร็ว และการพิจารณาอาจกระทำได้ทันภายในสมัยประชุมของรัฐสภาประจำปี 2543 ต่างกับกฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ที่มีการกำหนดหลักการสำคัญทางเทคโนโลยีไว้ด้วย จึงอาจต้องใช้ระยะเวลาในการพิจารณาร่างกฎหมายนานกว่า และอาจทำให้การพิจารณายกร่างกฎหมายไม่สามารถกระทำได้ทันในปี 2543

หลังจากคณะอนุกรรมการเฉพาะกิจเพื่อพิจารณายกร่างกฎหมายฯ ได้พิจารณายกร่างกฎหมายแล้วเสร็จ จึงได้เสนอร่างกฎหมายทั้งสองฉบับให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติได้พิจารณาให้ความเห็นชอบ 2 ครั้ง โดยครั้งแรกเป็นการพิจารณาเพื่อให้ความเห็นชอบในหลักการของร่างพระราชบัญญัติฯ และครั้งที่สองเพื่อพิจารณาอนุมัติร่างพระราชบัญญัติเสนอต่อคณะรัฐมนตรี ทั้งนี้โดยได้ขอความเห็นไปยังกระทรวงต่าง ๆ และหน่วยงานภาครัฐที่เกี่ยวข้อง และได้เผยแพร่ร่างพระราชบัญญัติไปยังหน่วยงานต่าง ๆ อย่างเปิดกว้างทั้งภาครัฐและภาคเอกชน และจัดสัมมนาเพื่อระดมความเห็นและข้อเสนอแนะจากสาธารณชนหลายครั้ง รวมทั้งเผยแพร่ร่างพระราชบัญญัติทั้งสองฉบับผ่านทางเว็บไซต์ของหน่วยงาน กล่าวคือ เว็บไซต์ http://www.nitc.go.th และ http://www.ecomerce.co.th

ในการยกร่างพระราชบัญญัตินั้น นอกจากกระทรวงวิทยาศาสตร์ฯ จะได้รับมอบหมายจากคณะรัฐมนตรีให้รับผิดชอบในการยกร่างกฎหมายเทคโนโลยีสารสนเทศแล้ว ก็ยังได้มีมติเห็นชอบในหลักการโครงการปรับปรุงและพัฒนากฎหมายเกี่ยวกับการค้าระหว่างประเทศของไทย เมื่อวันที่ 30 ธันวาคม 2540 และอนุมัติให้กระทรวงยุติธรรมตั้งคณะกรรมการเพื่อศึกษาและพิจารณาปรับปรุงกฎหมายดังกล่าว โดยกระทรวงยุติธรรมได้แต่งตั้งคณะอนุกรรมการเพื่อศึกษาและพิจารณาปรับปรุงกฎหมายเกี่ยวกับการค้าระหว่างประเทศของไทยในเรื่องพาณิชย์อิเล็กทรอนิกส์ โดยได้ดำเนินการยกร่างพระราชบัญญัติการพาณิชย์อิเล็กทรอนิกส์

พ.ศ. .... ขึ้น ซึ่งมีหลักการกฎหมายอย่างเดียวกับร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. . . . .

ดังนั้น ก่อนจะมีการเสนอร่างพระราชบัญญัติต่อคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติครั้งที่ 2 นั้น ประธานคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ (ฯพณฯ รองนายกรัฐมนตรี นายไตรรงค์ สุวรรณคีรี) จึงได้มีคำสั่งที่ 18/2542 แต่งตั้งคณะทำงานเพื่อรวมร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... และร่างพระราชบัญญัติการพาณิชย์อิเล็กทรอนิกส์ พ.ศ..... ให้เป็นร่างพระราชบัญญัติฉบับเดียว ซึ่งที่ประชุมคณะทำงานเพื่อรวมร่างพระราชบัญญัติได้บรรลุข้อตกลงร่วมกันในทุกมาตรา และให้ใช้ชื่อร่างพระราชบัญญัติดังกล่าวว่า “ร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ....” และเป็นฉบับที่ได้เสนอให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติได้ให้ความเห็นชอบในครั้งที่ 2

จากนั้นกระทรวงยุติธรรมจึงได้เสนอร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... และกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ในฐานะสำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ได้เสนอร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... และร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. .... ให้คณะรัฐมนตรีได้พิจารณา ทั้งนี้ คณะรัฐมนตรีได้พิจารณาและมีมติเห็นชอบในหลักการของร่างพระราชบัญญัติทั้งที่เสนอโดยกระทรวงยุติธรรมและกระทรวงวิทยาศาสตร์ฯ เมื่อวันที่ 14 มีนาคม 2543 และมอบหมายให้สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาร่างพระราชบัญญัติทั้งสองฉบับดังกล่าวต่อไป

สำนักงานคณะกรรมการกฤษฎีกาจึงได้แต่งตั้งคณะกรรมการกฤษฎีกา (คณะพิเศษ) ขึ้นพิจารณาร่างพระราชบัญญัติทั้งสองฉบับข้างต้น โดยมีผู้แทนกระทรวงยุติธรรมและผู้แทนกระทรวงวิทยาศาสตร์ฯ (เนคเทค สวทช.) เป็นผู้ชี้แจง

รายละเอียดกฎหมาย ในการนี้ คณะกรรมการกฤษฎีกา (คณะพิเศษ) ได้พิจารณาร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ไปทั้งสิ้นรวม 2 วาระ โดยให้คงหลักการเดิมไว้เกือบทุกมาตรา เพียงแต่มีการปรับแก้ถ้อยคำบ้างเท่านั้น และให้มีการตัดแต่เพียงมาตรา 3 เดิมออก ซึ่งกำหนดว่า "เมื่อใดไม่มีบทบัญญัติในพระราชบัญญัตินี้หรือกฎหมายอื่นใดที่จะยกมาปรับแก่กรณีได้ ให้วินิจฉัยตามหลักกฎหมายทั่วไป รวมทั้งหลักกฎหมายว่าด้วยข้อมูลอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ที่นานาประเทศถือปฏิบัติ" เนื่องจากพิจารณาเห็นว่าบทบัญญัติดังกล่าวบัญญัติขึ้นเพื่ออุดช่องว่างในกฎหมายนั้น สามารถใช้หลักเกณฑ์ตามมาตรา 4 แห่งประมวลกฎหมายแพ่งและพาณิชย์ได้อยู่แล้ว

ส่วนร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์นั้น คณะกรรมการกฤษฎีกา (คณะพิเศษ) ได้พิจารณาไปในวาระที่ 1 ได้เพียงบางมาตราเท่านั้น แต่เนื่องจากร่างพระราชบัญญัติทั้งสองฉบับดังกล่าวจำเป็นต้องปรับปรุงให้แล้วเสร็จเพื่อเสนอต่อสภาผู้แทนราษฎรโดยด่วนตามมติคณะรัฐมนตรี ซึ่งสำนักงานคณะกรรมการกฤษฎีกาได้พิจารณาแล้วเห็นว่า คณะกรรมการกฤษฎีกา (คณะพิเศษ) คงไม่สามารถตรวจพิจารณาปรับปรุงร่างพระราชบัญญัติทั้งสองฉบับโดยละเอียดได้ทัน สำนักงานฯ จึงได้นำร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ... ตามที่คณะกรรมการกฤษฎีกา (คณะพิเศษ) ได้ตรวจพิจารณาแก้ไขไว้แล้วมาพิจารณาในรายละเอียดอีกครั้งหนึ่งและได้แก้ไขถ้อยคำในบางมาตราอีกเล็กน้อย แล้วจึงเสนอต่อคณะรัฐมนตรีเป็นแบบที่ 1

อย่างไรก็ตาม สำนักงานคณะกรรมการกฤษฎีกามีข้อสังเกตเกี่ยวกับร่างพระราชบัญญัติทั้งสองฉบับว่าเป็นกฎหมายที่มีเนื้อหาสาระที่เกี่ยวข้องกัน เพราะวิธีการรับรองลายมือชื่ออิเล็กทรอนิกส์นั้นก็เพื่อให้การทำธุรกรรมมีความน่าเชื่อถือ ดังนั้น จึงควรแยกกำหนดรายละเอียดเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์เป็นพระราชกฤษฎีกา เพื่อให้สามารถระบุรายละเอียดต่าง ๆ ได้อย่างชัดเจนในการนำไปปฏิบัติและสามารถปรับเปลี่ยนได้ทันตามเทคโนโลยีที่มีการเปลี่ยนแปลงไปเสมอ จึงได้จัดทำ

ร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... เสนอต่อคณะรัฐมนตรี เป็นแบบที่ 2 ซึ่งรวมหลักการของร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... และร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. .... เข้าด้วยกัน โดยคงหลักการส่วนแรกที่เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ไว้ และเพิ่มบทบัญญัติเกี่ยวกับการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ และให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ด้วย ซึ่งสำนักงานคณะกรรมการกฤษฎีกา ได้เสนอร่างพระราชบัญญัติทั้ง 2 แบบ ให้คณะรัฐมนตรีได้พิจารณาพร้อมกัน

คณะรัฐมนตรีได้พิจารณาร่างพระราชบัญญัติอีกครั้งเมื่อวันที่ 25 กรกฎาคม 2543 และได้ให้ความเห็นชอบกับร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... (แบบที่ 2) ซึ่งมีการรวมร่างกฎหมายทั้งสองฉบับเข้าด้วยกัน และได้เสนอให้คณะกรรมการประสานงานสภาผู้แทนราษฎรพิจารณาเมื่อวันที่ 26 กรกฎาคม 2543 เพื่อเสนอต่อสภาผู้แทนราษฎรต่อไป

ในการประชุมสภาผู้แทนราษฎร ชุดที่ 20 ปีที่ 4 ครั้งที่ 17 (สมัยนิติบัญญัติ) เมื่อวันที่ 23 สิงหาคม 2543 ที่ประชุมได้พิจารณาและลงมติรับหลักการแห่งร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... รวมทั้งได้รับหลักการของร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... (นายบุญมาก ศิริเนาวกุล กับคณะเป็นผู้เสนอ) ซึ่งเป็นร่างพระราชบัญญัติฉบับที่มีแต่เพียงหลักการของธุรกรรมทางอิเล็กทรอนิกส์เท่านั้น ทั้งนี้ โดยได้มีการตั้งคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... โดยให้ถือเอาร่างพระราชบัญญัติของคณะรัฐมนตรีเป็นหลัก

หลังจากคณะกรรมาธิการวิสามัญได้พิจารณาแล้วเสร็จ จึงได้เสนอให้สภาผู้แทนราษฎรพิจารณาอีกครั้ง ที่ประชุมสภาผู้แทนราษฎร ชุดที่ 20 ปีที่ 4 ครั้งที่ 27 (สมัยนิติบัญญัติ) วันที่ 27 กันยายน 2543 ได้ลงมติเห็นชอบด้วยกับร่าง

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... ซึ่งคณะรัฐมนตรีและสมาชิกสภาผู้แทนราษฎรเป็นผู้เสนอ และให้เสนอต่อวุฒิสภาเพื่อพิจารณาต่อไป

หลังจากนั้น คณะกรรมาธิการวิสามัญกิจการวุฒิสภา จึงได้พิจารณาร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... เมื่อวันที่ 3 ตุลาคม 2543 และได้มีการบรรจุร่างพระราชบัญญัติในระเบียบวาระการประชุมของวุฒิสภา (สมัยสามัญนิติบัญญัติ) อย่างไรก็ตาม ได้มีพระราชกฤษฎีกาปิดสมัยประชุมรัฐสภา สมัยประชุมสามัญนิติบัญญัติ พ.ศ. 2543 ตั้งแต่วันที่ 22 ตุลาคม 2543 โดยที่ประชุมวุฒิสภายังไม่ได้พิจารณารับหลักการของร่างพระราชบัญญัติแต่อย่างใด และต่อมาได้มีการประกาศใช้พระราชกฤษฎีกายุบสภาผู้แทนราษฎรเมื่อวันที่ 9 พฤศจิกายน 2543

รัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 178 วรรคสอง ได้กำหนดไว้ว่า กรณีที่มีการยุบสภาผู้แทนราษฎร วุฒิสภาจะพิจารณาร่างพระราชบัญญัติที่รัฐสภายังไม่ได้ให้ความเห็นชอบต่อไปได้ ก็ต่อเมื่อคณะรัฐมนตรีที่ตั้งขึ้นใหม่ภายหลังการเลือกตั้งทั่วไปร้องขอภายในหกสิบวันนับแต่วันเรียกประชุมรัฐสภาครั้งแรกหลังการเลือกตั้งทั่วไป และรัฐสภามีมติเห็นชอบด้วย แต่ถ้าคณะรัฐมนตรีมิได้ร้องขอภายในกำหนดเวลาดังกล่าว ให้ร่างพระราชบัญญัติเป็นอันตกไป

คณะรัฐมนตรีได้มีมติเมื่อวันที่ 21 พฤศจิกายน 2543 และวันที่ 19 กุมภาพันธ์ 2544 อนุมัติให้สำนักเลขาธิการคณะรัฐมนตรีส่งคืนร่างพระราชบัญญัติของคณะรัฐมนตรีและร่างพระราชบัญญัติของสมาชิกสภาผู้แทนราษฎรที่ค้างการพิจารณาอยู่ตามขั้นตอนต่าง ๆ ของสภาผู้แทนราษฎรและวุฒิสภาให้กระทรวง ทบวง กรม หรือหน่วยงานที่เกี่ยวข้องพิจารณาว่ามีฉบับใดที่สมควรหรือไม่สมควรดำเนินการต่อไป โดยให้กระทรวง ทบวง กรม และหน่วยงานที่เกี่ยวข้องเร่งรัดพิจารณา และรวบรวมส่งสำนักเลขาธิการคณะรัฐมนตรีภายในวันที่ 15 มีนาคม 2544

ในการนี้ กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม ในฐานะหน่วยงานที่นำเสนอร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... ซึ่ง

ค้างการพิจารณาของวุฒิสภา วาระที่ 1 นั้น พิจารณาแล้วเห็นสมควรให้ดำเนินการพิจารณาร่างพระราชบัญญัติดังกล่าวต่อไป โดยได้มีหนังสือแจ้งไปยังสำนักเลขาธิการคณะรัฐมนตรีเมื่อวันที่ 14 มีนาคม 2544 ต่อมาเมื่อวันที่ 27 มีนาคม 2544 คณะรัฐมนตรีมีมติให้ดำเนินการนำส่งร่างพระราชบัญญัติที่ค้างการพิจารณาของวุฒิสภาและกระทรวงยืนยันมายังสำนักเลขาธิการคณะรัฐมนตรีภายในกำหนด ไปยังคณะกรรมการประสานงานสภาผู้แทนราษฎรเพื่อดำเนินการต่อไป

จากนั้น ในการประชุมสภาผู้แทนราษฎร เมื่อวันที่ 23 พฤษภาคม 2544 ที่ประชุมได้มีมติให้นำร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... เสนอให้วุฒิสภาดำเนินการพิจารณาต่อไป

ในการประชุมวุฒิสภาสมัยสามัญ ครั้งที่ 17 เมื่อวันที่ 25 พฤษภาคม 2544 ที่ประชุมได้พิจารณาและลงมติรับหลักการแห่งร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... ทั้งนี้ โดยตั้งคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติ ซึ่งมีพลเอกวิชา ศิริธรรม เป็นประธานคณะกรรมาธิการวิสามัญ

ที่ประชุมคณะกรรมาธิการวิสามัญ วุฒิสภา ได้พิจารณาปรับแก้ร่างพระราชบัญญัติฯ โดยยังคงหลักการของร่างพระราชบัญญัติฯ เดิมไว้เกือบทั้งสิ้น อาจปรับเปลี่ยนแต่เพียงถ้อยคำเพื่อให้ความหมายชัดเจนขึ้น อย่างไรก็ตาม เพื่อให้ร่างพระราชบัญญัติฯ กำหนดหลักการสำคัญ ๆ ไว้อย่างครบถ้วนสมบูรณ์ตามแนวทางกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ที่นานาประเทศใช้เป็นแนวในการตรากฎหมายตามกฎหมายแม่แบบสหประชาชาติ ที่ประชุมจึงได้พิจารณาเพิ่มหลักการสำคัญบางประการไว้ด้วย อาทิ หน้าที่เจ้าของลายมือชื่อ หน้าที่ของผู้ประกอบธุรกิจการรับรอง หน้าที่ของคู่กรณีที่เกี่ยวข้อง รวมทั้งระบบที่น่าเชื่อถือในการให้บริการ และมีการปรับเปลี่ยนลำดับหมวดเพื่อความเหมาะสม

ภายหลังที่คณะกรรมาธิการวิสามัญได้พิจารณาร่างพระราชบัญญัติฯ ดังกล่าวแล้วเสร็จ จึงได้เสนอให้วุฒิสภาพิจารณาอีกครั้งในการประชุมวุฒิสภา ครั้งที่ 23 (สมัย

สามัญนิติบัญญัติ) วันที่ 9 ตุลาคม 2544 ซึ่งที่ประชุมได้ลงมติเห็นชอบด้วยกับร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... ตามที่คณะกรรมาธิการวิสามัญฯ ได้ตรวจพิจารณาแก้ไขเพิ่มเติม

แต่เนื่องจากร่างพระราชบัญญัติฯ ที่ผ่านการพิจารณาของวุฒิสภามีการแก้ไขเพิ่มเติมแตกต่างไปจากร่างพระราชบัญญัติฯ ที่ผ่านการพิจารณาของสภาผู้แทนราษฎร ซึ่งตามบทบัญญัติมาตรา 175 อนุมาตรา 3 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 กำหนดให้วุฒิสภาต้องส่งร่างพระราชบัญญัติฯ ที่มีการแก้ไขเพิ่มเติมนั้นไปยังสภาผู้แทนราษฎรอีกครั้งหนึ่ง หากสภาผู้แทนราษฎรเห็นชอบด้วยกับการแก้ไขเพิ่มเติมก็ให้ดำเนินการต่อไป แต่หากเห็นเป็นกรณีอื่น ให้แต่ละสภาพิจารณาตั้งบุคคลซึ่งเป็นหรือมิได้เป็นสมาชิกแห่งสภานั้น ๆ ในจำนวนที่เท่ากันตามที่สภาผู้แทนราษฎรกำหนดประกอบเป็นคณะกรรมาธิการร่วมกันเพื่อพิจารณาร่างพระราชบัญญัติฯ ดังกล่าว

ต่อมา ในการประชุมสภาผู้แทนราษฎร ชุดที่ 21 ปีที่ 1 ครั้งที่ 28 (สมัยสามัญนิติบัญญัติ) เมื่อวันที่ 18 ตุลาคม 2544 สภาผู้แทนราษฎร ได้ลงมติเห็นชอบด้วยกับการแก้ไขร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... ของวุฒิสภา และให้นายกรัฐมนตรีนำขึ้นทูลเกล้าทูลกระหม่อมถวายพระมหากษัตริย์ เพื่อลงทรงพระปรมาภิไธย

ในการนี้ พระมหากษัตริย์ได้ทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ขึ้นไว้โดยคำแนะนำและยินยอมของรัฐสภา เมื่อวันที่ 2 ธันวาคม 2544 โดยพระราชบัญญัติฉบับนี้ได้นำลงประกาศในราชกิจจานุเบกษา เมื่อวันที่ 4 ธันวาคม 2544 ในฉบับกฤษฎีกา เล่ม 118 ตอนที่ 112ก และมีผลใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษา ซึ่งมีผลใช้บังคับตั้งแต่วันที่ 3 เมษายน 2545 เป็นต้นไป

2. ความจำเป็นในการตราพระราชบัญญัติฯ

การทำธุรกรรมทางอิเล็กทรอนิกส์นับเป็นอีกทางเลือกหนึ่งในการติดต่อสื่อสารยุคโลกาภิวัฒน์โดยอาศัยพัฒนาการทางเทคโนโลยีซึ่งมีความสะดวก รวดเร็ว และมีประสิทธิภาพ เอื้ออำนวยในการติดต่อสื่อสารระหว่างกัน แต่เนื่องจากรูปแบบใหม่ในการทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวจะมีความแตกต่างไปจากเดิมโดยสิ้นเชิง ไม่ว่าจะเป็นการติดต่อสื่อสารกันบนเครือข่ายโดยใช้วิธีการทางอิเล็กทรอนิกส์ การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic Data Interchange: EDI) ไปรษณีย์อิเล็กทรอนิกส์ (Electronic mail) หรือวิธีการทางอิเล็กทรอนิกส์อื่นๆ ล้วนแต่ทำอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ (Data message) มิได้ทำลงบนกระดาษดังเช่นเดิม (Traditional paper-based documents) อีกต่อไป

ดังนั้น การนำวิธีการดังกล่าวมาใช้จึงส่งผลให้ต้องมีการรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ (Legal recognition of data message) ให้เสมอกับหนังสือ หรือหลักฐานเป็นหนังสือ (Writing) รับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ (Attribution of data messages) รวมตลอดทั้งการรับฟังพยานหลักฐานและการชั่งน้ำหนักพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ (Admissibility and evidential weight of data messages) ดังนั้น เพื่อส่งเสริมการติดต่อสื่อสารโดยวิธีการทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ (Reliability) และก่อให้เกิดความเชื่อมั่น (Confidence) ซึ่งเอื้อต่อการทำธุรกรรมทางอิเล็กทรอนิกส์พร้อมทั้งก่อให้เกิดกฎหมาย ข้อบังคับ หรือระเบียบที่เป็นเอกรูป (Uniformity of Law, Rules, and Regulations) ที่สอดคล้องตามมาตรฐานที่นานาประเทศยอมรับจึงจำเป็นต้องตราพระราชบัญญัตินี้

3. หลักการทั่วไปของพระราชบัญญัติฯ

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้ยกร่างขึ้นตามแนวทางกฎหมายแม่แบบว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ (Model Law on Electronic Commerce 1996) และกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ (Model Law on Electronic Signatures 2001) ของคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติ (United Nations Commission on International Trade Law : UNCITRAL) อันเป็นกฎหมายที่หลายประเทศยอมรับและใช้เป็นแนวทางในการยกร่างกฎหมาย ทั้งนี้ โดยมีหลักการพื้นฐานที่สำคัญ คือ

3.1 หลักความเท่าเทียมกัน (Functional Equivalent Approach)

หลักความเท่าเทียมกันในที่นี้หมายถึงความเท่าเทียมระหว่างการใช้เอกสารที่อยู่ในรูปของกระดาษ (Paper-Based Documentation) และการใช้ข้อมูลคอมพิวเตอร์ (Computer-Based Information)[1] กล่าวคือ การติดต่อสื่อสารหรือการผูกนิติสัมพันธ์ผ่านสื่อที่อยู่ในรูปของกระดาษ หรือ การทำธุรกรรมผ่านสื่ออิเล็กทรอนิกส์จะต้องให้ผลทางกฎหมายที่เท่าเทียมกัน

[1] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, p. 17

3.2 หลักความเป็นกลางทางเทคโนโลยีรวมทั้งหลักการความเป็นกลางของสื่อ (Technology Neutrality / Media Neutrality)

โดยในการติดต่อสื่อสารจะต้องไม่มีการเลือกปฏิบัติเทคโนโลยีใดเทคโนโลยีหนึ่งโดยเฉพาะ ทั้งนี้ กฎหมายฉบับนี้ได้เปิดกว้างเพื่อรองรับการติดต่อสื่อสารด้วยวิธีการทางอิเล็กทรอนิกส์ในทุกรูปแบบ กล่าวคือ บางช่วงอาจมีการจัดทำให้ข้อความอยู่ในรูปของดิจิทัล (Digitized Information) บางช่วงติดต่อกันทางโทรพิมพ์ โทรสาร หรือการติดต่อกันผ่านทางคอมพิวเตอร์ซึ่งกำหนดให้โปรแกรมอัตโนมัติกระทำการแทน และวางหลักการเพื่อรองรับเทคโนโลยีทั้งที่มีอยู่ในปัจจุบันและที่จะมีการพัฒนาขึ้นในอนาคต [2]

4. โครงสร้างของพระราชบัญญัติฯ

พระราชบัญญัติฉบับนี้แบ่งออกเป็น 6 หมวดหลัก ดังต่อไปนี้

หมวด 1 ธุรกรรมทางอิเล็กทรอนิกส์ (มาตรา 7 – มาตรา 25)

หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์ (มาตรา 26 – มาตรา 31)

หมวด 3 ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ (มาตรา 32 – มาตรา 34)

หมวด 4 ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ (มาตรา 35)

หมวด 5 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (มาตรา 36 – 43)

---

[2] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, p.18 para.8

หมวด 6 บทกำหนดโทษ (มาตรา 44 – มาตรา 46)

โดยหมวด 1 จะเป็นบทบัญญัติเกี่ยวกับหลักเกณฑ์ต่าง ๆ ที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ หมวด2 เป็นบทบัญญัติเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ รวมทั้งหน้าที่ของบุคคลต่าง ๆ ที่เกี่ยวข้องกับการลงลายมือชื่ออิเล็กทรอนิกส์ หมวด 3 เป็นบทบัญญัติเกี่ยวกับการกำหนดหลักเกณฑ์การกำกับธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ หมวด 4 เป็นบทบัญญัติเกี่ยวกับการทำธุรกรรมทางอิเล็กทรอนิกส์กับหน่วยงานภาครัฐหรือโดยหน่วยงานภาครัฐ หมวด 5 เป็นบทบัญญัติเกี่ยวกับการจัดตั้งและบทบาทของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และหมวด 6 เป็นบทกำหนดโทษ ซึ่งเนื้อหาโดยละเอียดของแต่ละหมวดจะได้กล่าวถึงในบทต่อไป

อย่างไรก็ตาม แม้ว่ากฎหมายจะกำหนดกฎเกณฑ์และกระบวนการต่าง ๆ เพื่อรองรับวิธีการบันทึกและติดต่อสื่อสารที่ทันสมัยในรูปแบบหลากหลาย แต่ก็ได้คำนึงถึงความยืดหยุ่นของกฎหมายซึ่งควรปรับให้ใช้หรือรองรับเทคโนโลยีในอนาคตได้โดยการวางกลไกทางกฎหมายให้สามารถกำหนดบทบัญญัติในรายละเอียดต่าง ๆ ของเทคโนโลยีที่จะนำมาใช้โดยสามารถออกเป็นพระราชกฤษฎีกา ดังจะเห็นได้จากบทบัญญัติในหลายมาตราซึ่งได้ให้อำนาจในการตราพระราชกฤษฎีกาเพื่อกำหนดรายละเอียดเพิ่มเติมได้ อย่างไรก็ตาม แม้กฎหมายบัญญัติขึ้นเพื่อรองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ แต่ปัญหาข้อกฎหมายที่เกิดขึ้นอาจต้องพิจารณาโดยนำกฎหมายอื่นที่เกี่ยวข้องโดยตรงมาปรับใช้ด้วย เช่น กฎหมายว่าด้วยสัญญา [3] เป็นต้น

4.1 ขอบเขตของพระราชบัญญัติฯ (มาตรา 3)

[3] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, p.19 paras.13-14

พระราชบัญญัติฉบับนี้กำหนดขอบเขตไว้ให้ใช้ได้เป็นการทั่วไป กล่าวคือให้ใช้บังคับแก่ธุรกรรมในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ เว้นแต่ธุรกรรมที่มีพระราชกฤษฎีกากำหนดมิให้นำพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับ [4] และให้ใช้บังคับแก่การดำเนินงานของรัฐด้วย

โดยเหตุที่กฎหมายให้อำนาจในการตราพระราชกฤษฎีกากำหนดธุรกรรมที่ยกเว้นมิให้นำพระราชบัญญัตินี้มาใช้บังคับ ก็ด้วยเหตุผลที่ว่าลักษณะของธุรกรรมบางประเภทโดยสภาพไม่อาจทำด้วยวิธีการทางอิเล็กทรอนิกส์ หรือการพัฒนาทางเทคโนโลยียังไม่เอื้ออำนวยให้สามารถดำเนินการในรูปข้อมูลอิเล็กทรอนิกส์ รวมทั้งบางกรณีอาจเป็นนโยบายของกฎหมายที่ต้องการยกเว้นเพราะธุรกรรมบางประเภทมีความละเอียดอ่อนที่ต้องการการพิจารณาอย่างรอบคอบก่อนดำเนินการ ดังนั้นเพื่อให้กฎหมายสามารถปรับใช้ได้อย่างเหมาะสมกับสภาพการณ์ต่าง ๆ ที่เกิดขึ้นจึงได้บัญญัติให้การยกเว้นธุรกรรมที่มิให้ทำในรูปของข้อมูลอิเล็กทรอนิกส์สามารถตราเป็นพระราชกฤษฎีกา

ในการกำหนดข้อยกเว้นของธุรกรรมบางประเภทที่มิให้ดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์นี้ มีบัญญัติในกฎหมายของหลายประเทศ อาทิ Singapore Electronic Transactions Act 1998, Hong Kong Electronic Transaction Ordinance 2000 หรือ USA Electronic Signatures in Global and National

---

[4] ลักษณะการบัญญัติข้อยกเว้นในกฎหมายของแต่ละประเทศจะมีความแตกต่างกัน บางประเทศบัญญัติยกเว้นประเภทของธุรกรรมที่มิให้นำกฎหมายมาใช้บังคับไว้ในกฎหมาย อาทิ

กฎหมายสิงคโปร์ Electronic Transactions Act 1998

กฎหมายฮ่องกง Electronic Transaction Ordinance

กฎหมายอินเดีย The Information Technology Act,2000

ในขณะที่กฎหมายของบางประเทศก็มิได้บัญญัติข้อยกเว้นการบังคับใช้ไว้ในกฎหมาย อาทิ กฎหมายฟิลิปปินส์ Electronic Commerce Act หรือ กฎหมายของกาหลีใต้ Basic Law on Electronic Commerce เป็นต้น

Commerce Act 2000 เป็นต้น ทั้งนี้ ประเภทของธุรกรรมที่ยกเว้นดำเนินการในรูปของข้อมูลอิเล็กทรอนิกส์นั้น โดยส่วนใหญ่จะคล้ายกัน ตัวอย่างเช่น พินัยกรรม การดำเนินการใดๆ อันเกี่ยวกับการโอนสิทธิในอสังหาริมทรัพย์ หรือตราสารเปลี่ยนมือได้ เป็นต้น

สำหรับในส่วนของการดำเนินงานของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ ก็อยู่ภายใต้บังคับของกฎหมายนี้เช่นกัน แต่ในการดำเนินการจะต้องเป็นไปตามบทบัญญัติในหมวดที่ 4 ซึ่งจะเป็นการบัญญัติเกี่ยวกับหลักเกณฑ์ของหน่วยงานภาครัฐที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ว่าจะต้องดำเนินการอย่างไร โดยจะได้กล่าวในรายละเอียดในบทที่ 4

4.2 คำนิยาม (มาตรา 4)

พระราชบัญญัติได้บัญญัติคำนิยามของคำหลายๆ คำซึ่งมีความสำคัญเพื่อความชัดเจนในการบังคับใช้กฎหมาย และเพื่อมิให้เกิดปัญหาในการตีความเนื่องจากคำศัพท์บางคำเป็นคำศัพท์ใหม่ หรือแม้จะเป็นคำศัพท์ที่ใช้กันเป็นการทั่วไปแล้วก็ตามแต่ก็เป็นคำซึ่งมีความหมายในทางเทคโนโลยีซึ่งยังไม่ปรากฏว่ามีการให้คำนิยามอย่างเป็นทางการอันต้องตรงตามวัตถุประสงค์ในการใช้คำดังกล่าวแต่อย่างใด เช่น คำว่า “อิเล็กทรอนิกส์” “ข้อมูลอิเล็กทรอนิกส์” “ลายมือชื่ออิเล็กทรอนิกส์” “ระบบข้อมูล” “บุคคลที่เป็นสื่อกลาง” หรือคำธรรมดาซึ่งประสงค์จะให้มีความหมายพิเศษ เช่น “ข้อความ” “ธุรกรรม” “ธุรกรรมทางอิเล็กทรอนิกส์” “ผู้ส่งข้อมูล” “ผู้รับข้อมูล” “ใบรับรอง” “เจ้าของลายมือชื่อ” “คู่กรณีที่เกี่ยวข้อง”หรือ “หน่วยงานของรัฐ” เป็นต้น ทั้งนี้ โดยมีคำสำคัญดังต่อไปนี้

(ก) ข้อมูลอิเล็กทรอนิกส์ [5]

[5] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติคำนิยามคำนี้ ได้แก่ UNICTRAL Model Law on Electronic Commerce 1996, Singapore Electronic Transactions Act 1998,

คำว่า “ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่งรับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ และโทรสาร อนึ่ง คำว่า “ข้อมูลอิเล็กทรอนิกส์” ตามกฎหมายฉบับนี้ไม่ได้จำกัดอยู่เฉพาะข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการติดต่อสื่อสาร เท่านั้น แต่มุ่งประสงค์ให้ครอบคลุมถึงข้อมูลหรือบันทึกที่สร้างขึ้นโดยคอมพิวเตอร์ แม้จะไม่ได้ใช้เป็นสื่อในการติดต่อสื่อสารกับบุคคลอื่นก็ตาม และวิธีการทางอิเล็กทรอนิกส์ในที่นี้ให้รวมถึงพัฒนาการทางเทคโนโลยีในลักษณะอื่นที่คล้ายคลึงกันในอนาคต

(ข) ลายมือชื่ออิเล็กทรอนิกส์ [6]

ความหมายของคำว่า “ลายมือชื่ออิเล็กทรอนิกส์” ตามกฎหมายนี้ มีความหมายทำนองเดียวกับกฎหมายหลายๆ ประเทศ กล่าวคือ “ลายมือชื่ออิเล็กทรอนิกส์” หมายความว่า “อักษร อักขระ ตัวเลข เสียง หรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น” ซึ่งคำนิยามดังกล่าวเป็นคำนิยามที่มีความหมายกว้าง ไม่ได้เจาะจงเทคโนโลยีใดเทคโนโลยี

Philippines Electronic Commerce Act 2000 , Japan Law concerning Electronic Signatures and Certification Service หรือ Hong Kong Electronic Transaction Ordinaceเป็นต้น

[6] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติคำนิยามคำนี้ ได้แก่ UNICTRAL Model Law on Electronic Commerce 1996, Singapore Electronic Transactions Act 1998, Philippines Electronic Commerce Act 2000 , India Information Technology Act 2000 หรือ South Korea Basic Law on Electronic Commerce and Digital Signature Act เป็นต้น

หนึ่งโดยเฉพาะ ทั้งนี้เพื่อให้กฎหมายมีความยืดหยุ่นสามารถปรับใช้ได้กับทุกเทคโนโลยีทั้งที่มีอยู่ในปัจจุบัน และที่อาจเกิดขึ้นในอนาคต

(ค) การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ [7]

คำว่า "การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์" มาจากภาษาอังกฤษคำว่า Electronic Data Interchange หรือ EDI หมายความว่า "การส่งหรือรับข้อความโดยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า" สำหรับคำว่า "การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์" ในกฎหมายแม่แบบว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ ได้นำมาจากคำนิยามของ Working Party on Facilitation of International Trade Procedures (WP.4) ของคณะกรรมการเศรษฐกิจแห่งสหภาพยุโรป (The Economic Commission of Europe) ในส่วนที่องค์การสหประชาชาติ (UN) รับผิดชอบในการพัฒนามาตรฐานทางเทคโนโลยีที่เรียกว่า UN/EDIFACT[8] อันเป็นการติดต่อสื่อสารทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์ในรูปมาตรฐานที่ตกลงกันและนิยมใช้ในพิธีการศุลกากร [9]

---

[7] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติคำนิยามคำนี้ ได้แก่ UNICTRAL Model Law on Electronic Commerce 1996, Philippines Electronic Commerce Act 2000 , India Information Technology Act 2000 , South Korea Basic Law on Electronic Commerce and Digital Signature Act หรือ Hong Kong Electronic Transaction Ordinance เป็นต้น

[8] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, p.24 para.33

[9] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, p. 24 para. 34

(ง) ผู้ส่งข้อมูล และผู้รับข้อมูล [10]

คำว่า "ผู้ส่งข้อมูล" และ "ผู้รับข้อมูล" นั้น หากพิจารณาที่มาและวัตถุประสงค์ในการใช้คำแล้ว คำทั้งสองคำดังกล่าวมีความหมายค่อนข้างกว้าง เพราะไม่ได้มุ่งแต่เพียง "ผู้ส่ง" หรือ "ผู้รับ" เท่านั้น แต่หมายถึง "ผู้สร้าง" ด้วย และ "ผู้สร้าง" นั้น ในบางกรณีก็อาจไม่ใช่ผู้ส่งก็เป็นได้ แต่เนื่องจากวิธีการใช้ถ้อยคำในกฎหมายมักจะกำหนดให้สั้นและสื่อความหมายให้กระชับและรัดกุมที่สุด ดังนั้น ในการกำหนดคำนิยามจึงกำหนดใช้แต่เพียงคำว่า "ผู้ส่งข้อมูล" และ "ผู้รับข้อมูล" แต่มีการอธิบายความหมายของคำนิยามให้ครอบคลุมถึง "ผู้สร้าง" ไว้ด้วย และหมายความรวมถึง บุคคลซึ่งเป็นหรือถือว่าเป็นผู้ส่งหรือผู้รับหรือสร้างข้อมูลอิเล็กทรอนิกส์ก่อนที่จะมีการเก็บรักษาข้อมูลนั้น โดยบุคคลนั้นอาจจะส่งหรือสร้างหรือรับข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งหรือสร้างหรือรับข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ ทั้งนี้ ไม่รวมถึงบุคคลที่ทำหน้าที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้นแต่อย่างใด

อนึ่ง คำว่า "ผู้ส่งข้อมูล" และ "ผู้รับข้อมูล" นั้น ครอบคลุมทั้งบุคคลธรรมดาและนิติบุคคล อย่างไรก็ตามในคำอธิบายประกอบกฎหมายแม่แบบนั้นกำหนดให้ครอบคลุมถึงกรณีที่ได้มีการสร้างข้อมูลอิเล็กทรอนิกส์ขึ้นด้วยวิธีการอัตโนมัติโดยเครื่องคอมพิวเตอร์ (Automatically by Computer) ด้วย และจะถือได้ว่า "เริ่มมีการส่งหรือรับ" เมื่อข้อมูลอิเล็กทรอนิกส์นั้นออกจากหรือเข้าสู่ระบบ

---

[10] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติคำนิยามคำนี้ ได้แก่ UNICTRAL Model Law on Electronic Commerce 1996 , India Information Technology Act 2000 ,South Korea Basic Law on Electronic Commerce and Digital Signature Act, Hong Kong Electronic Transaction Ordinance เป็นต้น

ข้อมูลคอมพิวเตอร์เช่นเดียวกับกรณีที่ส่งโดยบุคคลธรรมดาหรือนิติบุคคล[11] อย่างไรก็ตาม สำหรับความสัมพันธ์ของผู้แทนซึ่งกระทำการแทนผู้ส่งหรือผู้รับหรือผู้สร้างก็จะเป็นไปตามกฎหมายที่เกี่ยวกับเรื่องตัวแทน [12]

(จ) ใบรับรอง [13]

คำว่า "ใบรับรอง" หมายความว่า "ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใดซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อ กับข้อมูลสำหรับสร้างลายมือชื่อ" สำหรับคำว่า "ข้อมูลที่ใช้ในการสร้างลายมือชื่อ" นั้น ตามกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ หมายความถึง กุญแจลับ (Secret keys) รหัสลับ (Codes) หรือองค์ประกอบอื่น อันเป็นส่วนสำคัญที่ใช้ในขั้นตอนของการสร้างลายมือชื่อ ซึ่งให้ความเชื่อมโยงที่ปลอดภัยระหว่างผู้สร้างลายมือชื่อและลายมือชื่ออิเล็กทรอนิกส์นั้น[14] ตัวอย่างเช่น การสร้างและใช้ลายมือชื่อดิจิทัลที่วางอยู่บนพื้นฐานของวิทยาการเข้ารหัสแบบอสมมาตร (Asymetric cryptography) นั้น จะมีความเชื่อมโยงระหว่างผู้ลงลายมือชื่อกับกุญแจคู่ที่สร้างขึ้นเท่านั้น เพราะหากใช้กุญแจคู่ที่ไม่ใช่คู่ที่ผู้ลงลายมือชื่อสร้างขึ้นก็จะไม่สามารถยืนยันตัวบุคคลที่สร้างกุญแจคู่นั้นได้

---

[11] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, p. 24 para. 35

[12] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, p. 24 para. 35

[13] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติคำนิยามคำนี้ ได้แก่ UNICTRAL Model Law on Electronic Signatures 2001, Singapore Electronic Transactions Act 1998, Malaysia Digital Signature Act , South Korea Digital Signature Act หรือ Hong Kong Electronic Transaction Ordinance เป็นต้น

[14] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations., A/CN.9/WG.IV/WP.88, p.34 para.94 และ A/CN.9/483, paras.65 and 67.

ความเชื่อมโยงระหว่างผู้ลงลายมือชื่อและลายมือชื่ออิเล็กทรอนิกส์ที่ชัดเจนอีกตัวอย่างก็คือการใช้เทคโนโลยีชีวภาพ (Biometric devices) ในการระบุตัวบุคคล เช่น การใช้ลายพิมพ์นิ้วมือ หรือฝ่ามือ เป็นต้น ก็ต้องอาศัยลักษณะทางชีวภาพของผู้ลงลายมือชื่อในการตรวจสอบเพื่อยืนยันตัวบุคคลนั้น

(ฉ) เจ้าของลายมือชื่อ [15]

คำว่า "เจ้าของลายมือชื่อ" หมายความว่า "ผู้ซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ และสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นในนามตนเองหรือแทนบุคคลอื่น" ซึ่งคำว่า "ผู้ซึ่ง" ในที่นี้หมายความถึงทั้งกรณี บุคคลธรรมดา และนิติบุคคล ซึ่งสามารถใช้ลายมือชื่ออิเล็กทรอนิกส์ในนามตนเองหรือในนามของบุคคลอื่นโดยเฉพาะอย่างยิ่งในกรณีของนิติบุคคลซึ่งต้องมีผู้กระทำการแทนนิติบุคคลนั้นโดยบุคคลธรรมดาเสมอ

ปัจจุบันได้มีการพัฒนาให้มีการใช้ประโยชน์จากลายมือชื่ออิเล็กทรอนิกส์ในกิจกรรมอื่น ๆ เพิ่มขึ้น เช่น การจัดเก็บภาษีและกิจกรรมทางปกครอง ซึ่งมีวัตถุประสงค์ในการนำไปใช้กว้างกว่าเพียงแค่ใช้ในการระบุตัวบุคคล และมักใช้กับนิติบุคคลมากกว่า [16]

(ช) หน่วยงานของรัฐ

เนื่องจากพระราชบัญญัติฉบับนี้ได้กำหนดให้ใช้บังคับกับหน่วยงานของรัฐด้วย ดังนั้น จึงได้มีการบัญญัติคำนิยามของคำนี้ไว้ดังต่อไปนี้ "หน่วยงานของรัฐ" หมายความว่า "กระทรวง ทบวง กรม ส่วนราชการที่เรียกชื่ออย่างอื่นและมีฐานะเป็นกรม ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจที่ตั้งขึ้นโดย

---

[15] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติคำนิยามคำนี้ ได้แก่ UNICTRAL Model Law on Electronic Signatures 2001.

[16] References to UNCITRAL documents: A/CN.9/WG.IV/WP.88, p.35 para.101 และ A/CN.9/483, paras.85 and 86

พระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใด ๆ"

ตามเจตนารมณ์ในการบัญญัติคำนิยามคำนี้ในขั้นตอนการผ่านความเห็นชอบของรัฐสภา ต้องการให้หมายความถึงหน่วยงานของรัฐทั้งหมดไม่ว่าจะเป็นฝ่ายนิติบัญญัติ บริการหรือตุลาการ โดยเห็นว่าคำว่า "...ให้หมายความรวมถึงนิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใด ๆ" เป็นคำที่มีความหมายกว้างสามารถครอบคลุมถึงทุกหน่วยงานได้อยู่แล้ว อย่างไรก็ตามเนื่องจากคำนิยามคำนี้เป็นการให้คำนิยามตามรูปแบบของกฎหมายเดิมที่มีอยู่ ดังนั้นจึงอาจมีปัญหาในการตีความว่าครอบคลุมถึงฝ่ายนิติบัญญัติและตุลาการหรือไม่ แม้ว่าตามเจตนารมย์ต้องการให้ครอบคลุมถึงก็ตาม

4.3 หลักเกณฑ์ที่คู่กรณีสามารถตกลงเปลี่ยนแปลงเป็นอย่างอื่นได้ (มาตรา 5)

หลักการสำคัญอีกประการหนึ่งในกฎหมายฉบับนี้ คือ การกำหนดบทบัญญัติโดยคำนึงถึง "หลักความศักดิ์สิทธิ์ในการแสดงเจตนาหรือเสรีภาพในการแสดงเจตนา (Principle of Party Autonomy)" ตามที่บัญญัติไว้ในมาตรา 5 ซึ่งได้กำหนดหลักเกณฑ์ให้บทบัญญัติของหมวด 1 ในมาตรา 13 – มาตรา 24 และ หมวด 2 ในมาตรา 26 – มาตรา 3 1 เป็นบทบัญญัติที่จะตกลงเป็นอย่างอื่นก็ได้ ซึ่งโดยส่วนใหญ่จะเป็นการกำหนดรายละเอียดเกี่ยวกับวิธีการติดต่อสื่อสาร การส่งหรือการรับข้อมูลอิเล็กทรอนิกส์ เป็นต้น

สำหรับบทบัญญัติอื่นที่กฎหมายไม่ได้บัญญัติยกเว้นให้ตกลงเปลี่ยนแปลงเป็นอย่างอื่นได้นั้น ส่วนใหญ่เป็นบทบัญญัติเกี่ยวกับข้อกำหนดทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ซึ่งกำหนดขึ้นเพื่อรองรับและส่งเสริมการติดต่อสื่อสารด้วยวิธีการที่ทันสมัยและเพื่อให้เกิดความแน่นอน (Certainty) ในกรณีที่มีการใช้วิธีการดังกล่าว ดังนั้น เพื่อลดอุปสรรคหรือความไม่แน่นอนจากบทบัญญัติของกฎหมาย จึงกำหนด

ไว้ไม่ให้คู่กรณีสามารถตกลงเปลี่ยนแปลงเป็นอย่างอื่น กล่าวได้ว่าเป็น "หลักเกณฑ์ที่คู่กรณีไม่สามารถตกลงเปลี่ยนแปลงเป็นอย่างอื่นได้ (Mandatory Rules)" [17]

4.4 ผู้รักษาการตามกฎหมาย (มาตรา 6)

เนื่องจากนวัตกรรมใหม่เกี่ยวกับเทคโนโลยีสารสนเทศมีประสิทธิภาพสะดวก และรวดเร็วโดยเฉพาะอย่างยิ่งในการทำธุรกรรมทางอิเล็กทรอนิกส์จะทวีบทบาทและความสำคัญยิ่งขึ้นในการติดต่อสื่อสารหรือทำการค้าขายทั้งในระดับภายในประเทศและระดับระหว่างประเทศ อันมีความเกี่ยวข้องกับหลายหน่วยงานอาทิ

(ก) คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ที่ได้รับความเห็นชอบในหลักการจากคณะรัฐมนตรีให้เป็นศูนย์กลางดำเนินการและประสานงานหน่วยงานต่าง ๆ ที่กำลังดำเนินการจัดทำกฎหมายเทคโนโลยีสารสนเทศและกฎหมายอื่นที่เกี่ยวข้อง

(ข) กระทรวงยุติธรรมซึ่งเป็นผู้รักษากฎหมายและได้รับความเห็นชอบจากคณะรัฐมนตรีเช่นกันในการพัฒนาและปรับปรุงกฎหมายว่าด้วยการพาณิชย์ทางอิเล็กทรอนิกส์ ตามกฎหมายแม่แบบของ UNCITRAL Model Law on Electronic Commerce

(ค) กระทรวงพาณิชย์ในฐานะที่รับผิดชอบด้านการค้าขายทั้งภายในประเทศและระหว่างประเทศและมีบทบาทสำคัญอย่างยิ่งในการเจรจาต่อรองบนเวทีการค้าโลก

---

[17] References to UNCITRAL documents: A/CN.9/WG.IV/WP.88, p.22 para.21

(ง) กระทรวงการคลังซึ่งรับผิดชอบในการจัดเก็บรายได้ให้กับรัฐในรูปของภาษีต่าง ๆ

(จ) ธนาคารแห่งประเทศไทยในฐานะที่รับผิดชอบในการกำกับดูแลธนาคารพาณิชย์และสถาบันการเงินเพื่อควบคุมเสถียรภาพทางการเงินของประเทศ

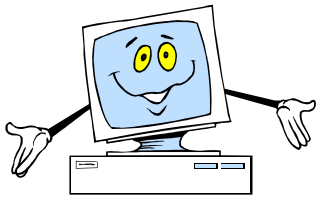
(ฉ) กระทรวงการต่างประเทศในฐานะที่มีส่วนสำคัญในการร่วมเจรจาต่อรองบนเวทีการค้าโลก

(ช) กระทรวงคมนาคมในฐานะที่รับผิดชอบการพัฒนาระบบสื่อสารโทรคมนาคมของประเทศ

(ซ) กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม ในฐานะที่ช่วยส่งเสริมการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงตามที่กำหนดไว้ในรัฐธรรมนูญฉบับปัจจุบันว่า "รัฐต้องเร่งพัฒนาโครงสร้างพื้นฐานสารสนเทศในท้องถิ่นให้ทั่วถึงและเท่าเทียมกันทั่วประเทศ"

ซึ่งหน่วยงานต่าง ๆ ดังที่ได้กล่าวมา หรือหน่วยงานอื่น ๆ ที่มิได้กล่าวถึงในที่นี้ ต่างก็เป็นหน่วยงานที่ปัจจุบันได้มีบทบาทสำคัญในการนำเทคโนโลยีสารสนเทศมาใช้ทั้งในด้านการให้บริการประชาชน หรือในด้านของการทำธุรกรรมทางอิเล็กทรอนิกส์อื่น ๆ ดังนั้น เมื่อเกี่ยวข้องกับงานของหลายกระทรวง และกฎหมายนี้มีสภาพเป็นกฎหมายกลางที่ทุกหน่วยงานต้องได้ใช้หรืออาจใช้ พระราชบัญญัตินี้จึงได้กำหนดให้นายกรัฐมนตรีเป็นผู้รักษาการ

บทที่ 1
ธุรกรรมทางอิเล็กทรอนิกส์



1.1 เทคโนโลยีสารสนเทศกับวิวัฒนาการในการติดต่อสื่อสาร

จากพฤติกรรมการติดต่อสื่อสารของมนุษย์ นับแต่อดีตกาลที่การติดต่อสื่อสารของมนุษย์จะต้องอาศัยการติดต่อสื่อสารเฉพาะหน้าเท่านั้น ไม่ว่าจะแสดงโดยใช้กริยาท่าทางหรือการพูด และต่อมาพัฒนาเป็นการติดต่อสื่อสารระหว่างบุคคลที่อยู่ห่างโดยระยะทาง เช่น การใช้คนหรือสัตว์เป็นพาหนะในการติดต่อสื่อสารระหว่างที่หนึ่งไปยังอีกที่หนึ่ง แต่เนื่องจากการติดต่อสื่อสารด้วยวิธีการดังกล่าวต้องเสียเวลามาก และอาจเกิดอุปสรรคนานัปการกว่าที่สารหรือข้อความจะถึงผู้รับปลายทาง หรือข้อความของผู้ส่งอาจไปไม่ถึงผู้รับปลายทางโดยที่ผู้ส่งอาจไม่ทราบ

ดังนั้น มนุษย์จึงได้พยายามคิดค้นวิธีการติดต่อสื่อสารรูปแบบใหม่ เพื่อให้การติดต่อสื่อสารมีความปลอดภัย สะดวกและรวดเร็วประหยัดเวลามากยิ่งขึ้น โดยการกำหนดรูปแบบหรือจัดระบบการติดต่อสื่อสาร หรือระบบต่างๆ ที่เกี่ยวข้องกับข้อความให้มีความปลอดภัยมากขึ้น ทั้งนี้เกิดจากการผสมผสานระหว่างแนวความคิดริเริ่มแบบใหม่ ประกอบกับการพัฒนาของเทคโนโลยี เช่น การส่งไปรษณีย์ โทรเลข หรือโดยการใช้อุปกรณ์อิเล็กทรอนิกส์ เช่น โทรศัพท์ หรือโทรสาร เป็นต้น

จวบจนปัจจุบันที่เทคโนโลยีสารสนเทศ [18] เป็นตัวแปรสำคัญต่อการที่สังคมก้าวเข้าสู่ยุค "สังคมสารสนเทศ (The Information Society)" หรือที่เรียกกันว่าเป็นยุคของสังคมแห่งข้อมูลข่าวสาร เป็นสังคมที่มีการใช้เทคโนโลยีสารสนเทศ (Information Technology) หรือที่เรียกว่า IT เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการ และการประกอบการด้านต่าง ๆ ให้เกิดประสิทธิภาพมากขึ้น และปัจจัยสำคัญที่พัฒนาสังคมไปสู่ "สังคมสารสนเทศ" อย่างรวดเร็ว เริ่มต้นจากพัฒนาการทางวิทยาการคอมพิวเตอร์ สู่ระบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ (Computer Networks) เข้าด้วยกัน หรือที่นิยมเรียกกันว่า "อินเทอร์เน็ต (Internet)" อันเป็นที่มาของคำว่า "โลกไร้พรมแดน"

ดังนั้น คำว่า "โลกไร้พรมแดน" จึงมีที่มาจากพัฒนาการในการติดต่อสื่อสารด้วยวิธีการทางเทคโนโลยีที่ทันสมัยเสมือนหนึ่งโลกถูกย่อให้มีขนาดเล็กลง เพราะบุคคลสามารถติดต่อสื่อสารถึงกันได้ง่าย สะดวก และรวดเร็ว และสามารถรับทราบข้อมูลหรือสารสนเทศได้อย่างรวดเร็วด้วยวิธีการทางอิเล็กทรอนิกส์ และทำให้เกิดรูปแบบกิจกรรมค้าขายแบบใหม่เกิดขึ้น กล่าวคือ พาณิชย์อิเล็กทรอนิกส์ หรือการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งต่อมาได้กลายเป็นกลไกสำคัญในการแข่งขันในเวทีการค้าโลก ปัจจัยพื้นฐานสำคัญทางเทคโนโลยีสารสนเทศหลายประการที่ส่งเสริมและสนับสนุนต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ ดังนี้

---

[18] ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศ พ.ศ.2535 ข้อ 5 และร่างพระราชบัญญัติว่าด้วยการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน พ.ศ. .... มาตรา 3 ได้ให้ความหมายคำว่า "เทคโนโลยีสารสนเทศ" ไวดังนี้

"เทคโนโลยีสารสนเทศ" หมายความว่า ความรู้ในผลิตภัณฑ์หรือในกระบวนการดำเนินการใด ๆ ที่อาศัยเทคโนโลยีซอฟต์แวร์ (Software) ฮาร์ดแวร์ (Hardware) การติดต่อสื่อสาร การรวบรวมและการนำข้อมูลมาใช้ทันการ เพื่อก่อให้เกิดประสิทธิภาพทั้งทางด้านการผลิต การบริการ การบริหาร และการดำเนินงาน รวมทั้งเพื่อการศึกษาและการเรียนรู้ ซึ่งจะส่งผลต่อความได้เปรียบทางด้านเศรษฐกิจ การค้า และการพัฒนาด้านคุณภาพของประชาชนในสังคม"

1.1.1 คอมพิวเตอร์

ปัจจุบัน “คอมพิวเตอร์” เป็นคำที่คุ้นหูมาก อาจจะถือว่าเป็น “ปัจจัย” อย่างหนึ่งในการดำเนินชีวิตของคนเราก็ว่าได้ ไม่ว่าจะเป็น นักเรียน นักศึกษา นักธุรกิจ ข้าราชการ แม้แต่พระภิกษุสงฆ์ ก็มีโอกาสได้สัมผัสกับเทคโนโลยีนี้ทั้งทางตรง และทางอ้อม ดังนั้นการศึกษาถึงเทคโนโลยีนี้ ย่อมเป็นการสร้าง “โอกาส” ให้กับตนเองได้อย่างแน่นอน เนื้อหาเกี่ยวกับเทคโนโลยีนี้มีกว้างมาก แต่ก็ไม่ยากเกินกว่าจะทำความเข้าใจ สำหรับมือใหม่ มือสมัครเล่น และทุกๆ ท่าน การทำความรู้จักกับ “คอมพิวเตอร์” และการใช้งาน “คอมพิวเตอร์” ในระดับพื้นฐาน เป็นสิ่งจำเป็นที่ควรทำก่อนเป็นอันดับแรก ดังนั้น ลองมาทำความรู้จักกับ “คอมพิวเตอร์” กันก่อนเลย

คอมพิวเตอร์มีหลากหลายลักษณะ หลากหลายรูปแบบ ทั้งคอมพิวเตอร์ขนาดพกพา คอมพิวเตอร์แบบตั้งโต๊ะ คอมพิวเตอร์แบบกระเป๋าหิ้ว คอมพิวเตอร์ขนาดใหญ่ เช่น คอมพิวเตอร์เมนเฟรม หรือซุปเปอร์คอมพิวเตอร์

แต่ไม่ว่าจะเป็นรูปแบบใดก็ตาม คอมพิวเตอร์ก็มีความหมายที่ชัดเจนในตัวของมันเอง คือ เครื่องคำนวณ ในรูปของอุปกรณ์อิเล็กทรอนิกส์ ที่สามารถรับข้อมูลและคำสั่ง ผ่านอุปกรณ์รับข้อมูล แล้วนำข้อมูลและคำสั่งนั้น ไปประมวลผลด้วยหน่วยประมวลผลเพื่อให้ได้ผลลัพธ์ที่ต้องการ และแสดงผลผ่านอุปกรณ์แสดงผล ตลอดจนสามารถบันทึกรายการต่างๆ ไว้เพื่อใช้งานได้ด้วยอุปกรณ์บันทึกข้อมูลสำรอง

(ก) ประเภทของเครื่องคอมพิวเตอร์

การจัดแบ่งประเภทของเครื่องคอมพิวเตอร์ อาศัยความเร็วของการประมวลผล และขนาดความจำของหน่วยบันทึกข้อมูล ซึ่งสามารถแบ่งได้เป็น 4 ประเภท ได้แก่

- Supercomputers
  เป็นคอมพิวเตอร์ที่มีประสิทธิภาพสูง มีความเร็วในการประมวลผลที่สูงประมาณ 100 ล้านคำสั่งต่อวินาที และมีขนาดความจำปริมาณมาก ต้องการห้องที่สามารถปรับอุณหภูมิได้ และมักจะใช้ในงานวิจัยต่าง ๆ เช่น การวิจัยเกี่ยวกับดินฟ้าอากาศ (อุตุนิยมวิทยา) การวิเคราะห์ภาพถ่ายดาวเทียม การวิเคราะห์ด้านโมเลกุลของสสารต่าง ๆ

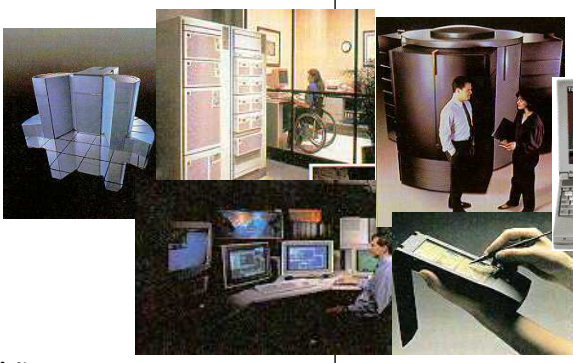
- Mainframe Computers
  เป็นคอมพิวเตอร์ที่มีประสิทธิภาพรองมาจาก Supercomputers มีความต้องการการบำรุงรักษาคล้าย ๆ กับ Supercompters แต่มักจะพบในองค์กรขนาดใหญ่ เช่น ธนาคาร ธุรกิจการบิน บริษัท และมหาวิทยาลัยต่าง ๆ เพราะเป็นเครื่องคอมพิวเตอร์ที่สามารถเชื่อมโยงกับเครื่องปลายทางได้จำนวนมาก ทำให้สามารถตอบสนองการใช้งานของผู้ใช้ได้พร้อมกันหลายคน

- Minicomputers
  เป็นคอมพิวเตอร์ขนาดกลาง ที่มักจะพบในหน่วยงานบริษัทที่ใช้งานเฉพาะด้าน เช่น ประมวลผลงานบัญชี โดยสามารถนำไปเชื่อมต่อกับเครื่องปลายทางได้หลายเครื่อง มีลักษณะการทำงานแบบ Centralized

- Microcomputers เป็นคอมพิวเตอร์ใช้งานที่พบได้อย่างแพร่หลาย โดยอาจจะพบได้ทั้งในรูปของเครื่องคอมพิวเตอร์ส่วนบุคคลแบบตั้งโต๊ะ (Personal Computer) หรือแบบพกพา (Portable Computer) ลักษณะต่าง ๆ

(ข) ระบบคอมพิวเตอร์

คอมพิวเตอร์ไม่ว่าอยู่ในรูปแบบใดก็ตาม จะมีการทำงานเป็นระบบเดียวกัน เรียกว่า "ระบบคอมพิวเตอร์ (Computer System)" ซึ่งประกอบด้วยหน่วยการทำงาน 3 ระบบร่วมกัน ได้แก่



- **ฮาร์ดแวร์** (Hardware) เป็นอุปกรณ์ที่ประกอบเป็นคอมพิวเตอร์และอุปกรณ์เสริมอื่น ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ ซึ่งสามารถมองเห็น และจับต้องได้

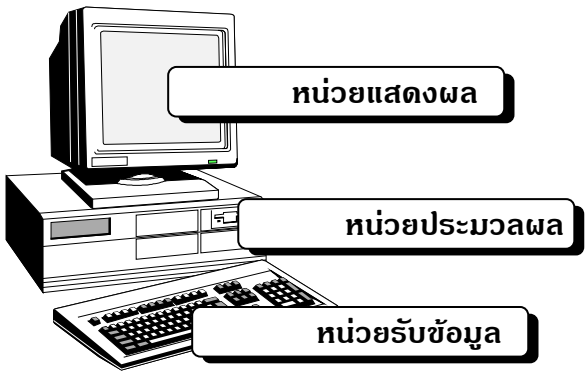
- **ซอฟต์แวร์** (Software)

เป็นชุดคำสั่ง หรือโปรแกรมที่สั่งการให้คอมพิวเตอร์ทำงานตามที่ต้องการ

- **บุคลากรทางคอมพิวเตอร์** (Peopleware) ได้แก่ บุคคลที่ทำงานเกี่ยวข้องกับคอมพิวเตอร์

ฮาร์ดแวร์ (Hardware)

ฮาร์ดแวร์ เป็นอุปกรณ์ที่ประกอบเป็นคอมพิวเตอร์ และอุปกรณ์เสริมอื่น ๆ ที่สามารถมองเห็น และจับต้องได้ และจากความหมายของ “คอมพิวเตอร์” ก็คงจะมองออกว่า คอมพิวเตอร์จะทำงานได้ ต้องประกอบด้วยส่วนรับข้อมูลและคำสั่ง ส่วนประมวลผล และส่วนที่ใช้แสดงผลลัพธ์จากการประมวลผล ซึ่งเรียกรวมกันว่า “องค์ประกอบของคอมพิวเตอร์” อันเป็นส่วนประกอบหนึ่งของฮาร์ดแวร์นั่นเอง

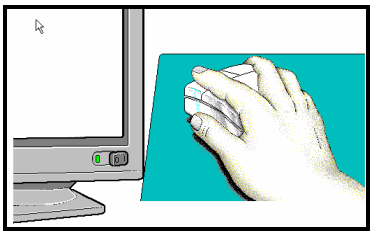


แผนภาพแสดงองค์ประกอบของคอมพิวเตอร์

หน่วยรับข้อมูล (Input Unit) เป็นหน่วยที่ทำหน้ารับข้อมูล หรือคำสั่งเข้าสู่คอมพิวเตอร์ เพื่อให้คอมพิวเตอร์ดำเนินการประมวลผลต่อไป โดยอาศัยอุปกรณ์รับข้อมูลหลากรูปแบบ เช่น

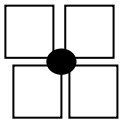
1. **แผงแป้นอักขระ** (Keyboard) แผงแป้นอักขระ หรือที่รู้จักกันว่า “แป้นพิมพ์” เป็นอุปกรณ์รับข้อมูลเบื้องต้น มีลักษณะการทำงานคล้ายแป้นพิมพ์ของเครื่องพิมพ์ดีด แต่ได้เพิ่มปุ่มควบคุมเฉพาะสำหรับคอมพิวเตอร์ หน้าที่หลักของคีย์บอร์ด ได้แก่ การเปลี่ยนกลไลการกดปุ่ม ให้เป็นสัญญาณทางไฟฟ้า เพื่อส่งให้คอมพิวเตอร์ โดยสัญญาณดังกล่าวจะบอกให้คอมพิวเตอร์ทราบว่ามีการกดคีย์อะไร

2. **เมาส์** (Mouse) อุปกรณ์รับข้อมูลที่นิยมรองจากคีย์บอร์ด ได้แก่ อุปกรณ์ชี้ตำแหน่งที่เรียกว่า เมาส์ (Mouse) หรือ “หนูอิเล็กทรอนิกส์” เนื่องจากเป็นอุปกรณ์ที่มีลักษณะคล้ายหนู มีสายต่ออยู่ที่ปลายลักษณะเดียวกับหางหนู หน้าที่ของเมาส์จะช่วยในการบ่งชี้ตำแหน่งว่าขณะนี้กำลังอยู่ณ จุดใดบนจอภาพ เรียกว่า “ตัวชี้ตำแหน่ง (Pointer)” ซึ่งอาศัยการเลื่อนเมาส์ แทนการกดปุ่มบังคับทิศทางบนคีย์บอร์ด



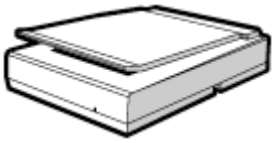
3. **แทร็กบอล** (Track Ball) อุปกรณ์รับข้อมูลที่มีลักษณะคล้ายเมาส์ แต่เอาลูกบอลมาวางอยู่ด้านบน เพื่อลดพื้นที่การใช้งาน เมื่อต้องการเลื่อนตำแหน่ง ก็ใช้นิ้วมือกลิ้งลูกบอลไปมา และปุ่มกดก็มีจำนวนเท่ากับปุ่มกดของเมาส์ เพียงแต่วางไว้ด้านข้าง มักจะพบ Track Ball กับ Notebook Computer

4. **ปุ่มเลื่อนตำแหน่ง** (AccuPoint) อุปกรณ์บ่งชี้ของเครื่อง Portage/Note Book ตระกูล Toshiba โดยจะติดตั้งไว้ระหว่างปุ่มตัวอักษร G, H และ B ส่วนปุ่มกดจะอยู่บริเวณด้านล่างของ Space Bar

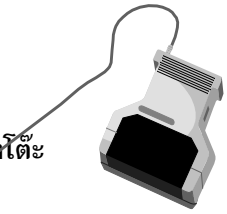


5. **สแกนเนอร์** (Scanner) สแกนเนอร์ คือ อุปกรณ์ต่อเชื่อมคอมพิวเตอร์แบบกราฟิก ที่มีหน้าที่ในการเปลี่ยนแปลงภาพต้นฉบับ (รูปถ่าย ตัวอักษรบนหน้ากระดาษ ภาพวาด) ให้เป็นข้อมูล เพื่อให้คอมพิวเตอร์สามารถนำ

ข้อมูลดังกล่าวมาใช้ประโยชน์ในการแสดงผลที่หน้าจอ ทำให้สามารถแก้ไข ตกแต่งเพิ่มเติม และจัดเก็บข้อมูลได้

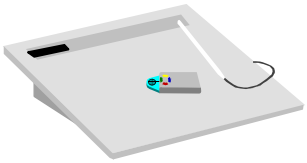


สแกนเนอร์แบบตั้งโต๊ะ



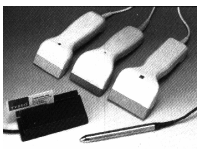
สแกนเนอร์แบบพกพา

6. **ดิจิไทเซอร์** (Digitizer)
ดิจิไทเซอร์ หรือ แท็ปเลต (Tablet) เป็นอุปกรณ์รับข้อมูลที่มักจะใช้ในคอมพิวเตอร์กราฟิกสำหรับงานเขียนแบบ (Computer Aided Design/ Computer Aided Manufactory: CAD/CAM) มีลักษณะเป็นแผ่นสี่เหลี่ยมขนาดเท่ากับจอภาพ และมีอุปกรณ์ชี้ตำแหน่ง คล้ายเมาส์วางบนแผ่นสี่เหลี่ยม เรียกว่า ทรานซดิวเซอร์ เมื่อเลื่อนตัวชี้ตำแหน่งไปบนกระดาน จะมีการส่งสัญญาณจากตะแกรงใต้แผ่นกระดานไปให้คอมพิวเตอร์



7. **ก้านควบคุม** (Joy Stick)
เป็นอุปกรณ์การทำงานลักษณะเดียวกับเมาส์ มีลักษณะเป็นกล่อง หรือรูปทรงแปลกตาที่มีก้านควบคุมอยู่ด้านบน โดยก้านควบคุมนี้ สามารถเคลื่อนที่ได้เหมือนคันโยก ทำให้สามารถควบคุมการเลื่อนตำแหน่งได้สะดวก นิยมใช้กับเกมส์คอมพิวเตอร์

8. **เครื่องอ่านแถบรหัสแท่ง** (Bar-code Reader)



เครื่องอ่านแถบรหัสแท่ง เป็นเครื่องอ่านรหัสแถบขาว ดำ ที่เรียกว่า Bar Code ที่ใช้เป็นสัญลักษณ์แทนข้อมูล โดยเครื่องอ่านรหัสแถบนี้ มีหลายรูปแบบด้วยกัน Bar Code หรือ รหัสแท่ง มีลักษณะเป็นลายเส้นดำขาว ที่มีขนาดของแต่ละแท่งในแผ่นป้ายที่แตกต่างกัน พร้อมทั้งบรรจุตัวเลขหรือตัวอักษร

อุปกรณ์รับข้อมูล ยังมีอีกหลายอย่างซึ่งไม่สามารถนำเสนอได้ครบ หากท่านมีความสนใจคงต้องศึกษาเพิ่มเติมจากคู่มือคอมพิวเตอร์ต่าง ๆ ที่มีการพิมพ์เผยแพร่ออกมาหลาย ๆ เล่ม

หน่วยประมวลผลกลาง (Central Processing Unit; CPU)

หน่วยประมวลผลกลาง เปรียบได้กับสมองของคอมพิวเตอร์ เป็นส่วนที่สำคัญที่สุด มีหน้าที่ประมวลผลและควบคุมระบบต่าง ๆ ของคอมพิวเตอร์ ให้ทุกหน่วยทำงานสอดคล้องสัมพันธ์กัน

หน่วยประมวลผลกลาง ประกอบด้วยหน่วยย่อย ดังนี้

(1) **หน่วยความจำหลัก** (Main Memory Unit)

(2) **หน่วยคำนวณและตรรกะ** (Arithmetic and Logic Unit; ALU)

(3) **หน่วยควบคุม** (Control Unit)

หน่วยความจำหลัก (Main Memory)

เป็นหน่วยที่ใช้เก็บข้อมูล และคำสั่ง แบ่งได้เป็น 2 ประเภท คือ

หน่วยความจำสำหรับเก็บคำสั่ง (Program Memory)

ใช้เก็บคำสั่งที่มักใช้บ่อย ๆ เช่น คำสั่งเริ่มต้นการทำงานของคอมพิวเตอร์ โดยคำสั่งนี้จะอยู่ภายในคอมพิวเตอร์ตลอดไป แม้ว่าจะทำการปิดเครื่องไปแล้ว สามารถแยกประเภทย่อยได้เป็น

- ROM (Read Only Memory) เป็นหน่วยความจำที่บริษัทผู้ผลิตได้บรรจุคำสั่งเอาไว้แล้วอย่างถาวร ไม่สามารถแก้ไขเปลี่ยนแปลงได้ โดยปกติหน่วยความจำนี้ติดตั้งมาจากบริษัทผู้ผลิต โดยผู้ใช้ไม่มีโอกาสเลือก
- PROM (Programmable ROM) เป็นหน่วยความจำรอมประเภทที่ผู้ใช้สามารถเขียนคำสั่ง แล้วบันทึกเอาไว้อย่างถาวร โดยอาศัยเครื่องมือเฉพาะ แต่คำสั่งที่บันทึกนั้นไม่สามารถแก้ไขได้อีก
- EPROM (Erasable PROM) เป็นหน่วยความจำรอมประเภทที่สามารถเขียนคำสั่ง บันทึกและแก้ไขด้วยเครื่องมือเฉพาะได้หลาย ๆ ครั้ง

หน่วยความจำสำหรับเก็บข้อมูลและคำสั่ง
(Data & Programming Memory)

หน่วยความจำสำหรับเก็บข้อมูลและคำสั่ง หรือที่เรียกว่า "แรม (RAM; Random Access Memory)" เป็นหน่วยความจำที่สามารถเก็บข้อมูลและคำสั่งจากหน่วยรับข้อมูล แต่ข้อมูลและคำสั่งเหล่านั้นสามารถหายไปได้ เมื่อมีการรับข้อมูลหรือคำสั่งใหม่ หรือปิดเครื่อง หรือกระแสไฟฟ้าขัดข้อง หน่วยความจำแรมเป็นหน่วยความจำที่สำคัญที่สุดของคอมพิวเตอร์ จำเป็นจะต้องเลือกซื้อให้มีขนาดใหญ่พอสมควร มิฉะนั้นจะทำงานไม่สะดวก

โดยเหตุที่หน่วยความจำแรม เป็นส่วนสำคัญของคอมพิวเตอร์นี่เอง เมื่อกล่าวถึงขนาดความจุของหน่วยความจำ เราจึงหมายความถึงขนาดของหน่วยความจำแรม เช่น บอกว่าคอมพิวเตอร์เครื่องนี้ มีขนาดความจุของหน่วยความจำ 4 MB หมายความว่า คอมพิวเตอร์มีขนาดหน่วยความจำแรม เท่ากับ 4 MB นั่นเอง การวัดขนาดหน่วยความจำ นิยมใช้หน่วยเป็นไบต์ (Byte) ซึ่งอาจเทียบได้เท่ากับตัวอักษร 1 ตัว โดยที่คอมพิวเตอร์ต้องใช้หน่วยความจำที่ใหญ่มาก เพื่อให้สะดวกจึงต้องคิดหน่วยที่ใหญ่ขึ้นไปอีกมาเรียก นั่นคือ หน่วย KB เท่ากับ 1024 ไบต์

(แต่อาจถือเอาคร่าวๆ ว่าเป็นพันไบต์ได้) และ MB ซึ่งเท่ากับประมาณ หนึ่งล้านไบต์ ดังนี้

1 Byte (ไบต์) = 1 ตัวอักษร

1 KB (กิโลไบต์) = 1024 ตัวอักษร

1 MB (เมกกะไบต์) = 1024 KB

1 GB (กิกะไบต์) = 1024 MB

หน่วยคำนวณและตรรกะ (ALU; Arithmetic and Logic Unit)

หน่วยนี้ทำหน้าที่คำนวณทางคณิตศาสตร์ เช่น บวก ลบ คูณ หาร และทางตรรกศาสตร์ เช่น การเปรียบเทียบค่าจริง หรือเท็จ โดย ALU จะใช้หน่วยความจำขนาดเล็กที่เรียกว่า Register ในการเก็บค่าของข้อมูลที่ต้องการนำมาคำนวณจากหน่วยความจำ และเมื่อทำการคำนวณแล้ว ก็จะส่งผลลัพธ์ใน Register ที่ได้กลับไปสู่หน่วยความจำอีกครั้ง

หน่วยควบคุม (Control Unit)

หน่วยที่ทำหน้าที่ควบคุมการทำงานของหน่วยทุกๆ หน่วย ใน CPU และอุปกรณ์อื่นที่ต่อพ่วง เปรียบเสมือนสมองที่ควบคุมการทำงานส่วนประกอบต่าง ๆ ของร่างกายมนุษย์ เช่น แปลคำสั่งที่ป้อน ควบคุมให้หน่วยรับข้อมูลรับข้อมูลเข้ามาเพื่อทำการประมวลผล ตัดสินใจว่าจะให้เก็บข้อมูลไว้ที่ไหน ถูกต้องหรือไม่ ควบคุมให้ ALU ทำการคำนวณข้อมูลที่รับเข้ามา ตลอดจนควบคุมการแสดงผลลัพธ์ เป็นต้น

หน่วยแสดงผล (Output Unit)

หน่วยแสดงผล ทำหน้าที่รับข้อมูลจากหน่วยความจำ ซึ่งผ่านการประมวลผลแล้วมาแสดง โดยอาศัยอุปกรณ์แสดงผล ได้แก่ จอภาพ, เครื่องพิมพ์, เครื่องวาด

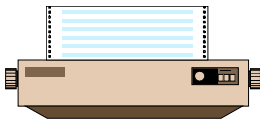
1. **จอภาพ** (Monitor)

จอภาพเป็นอุปกรณ์แสดงผลพื้นฐานที่สุดของคอมพิวเตอร์ มีลักษณะคล้ายกับจอภาพของโทรทัศน์ ปกติแล้วจอภาพสามารถแบ่งได้ 2 ประเภท คือ จอภาพสีเดียว (Monochrome Monitor) และจอภาพหลายสี (Color Monitor) ซึ่งปัจจุบันได้รับความนิยมเป็นอย่างมาก และแสดงสีได้มากกว่า 16.7 ล้านสี

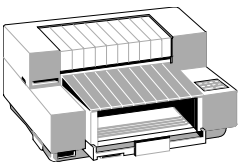
2. **เครื่องพิมพ์** (Printer)

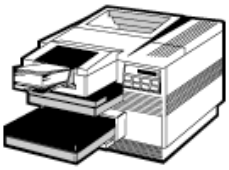
เครื่องพิมพ์เป็นอุปกรณ์แสดงผลลัพธ์ โดยอาศัยการพิมพ์ข้อมูลลงในแผ่นกระดาษ หรือแผ่นใส หรืออื่นๆ ตามแต่ชนิดของเครื่องพิมพ์ สามารถแบ่งเครื่องพิมพ์ได้ 2 กลุ่มตามลักษณะการพิมพ์ ได้แก่

- **เครื่องพิมพ์แบบกระทบ** (Impact Printers) เป็นเครื่องพิมพ์ที่อาศัยการกดหัวพิมพ์กับแถบผ้าหมึกเพื่อให้เกิดตัวอักษร ได้แก่ *เครื่องพิมพ์แบบเรียงจุด (Dot Matrix Printer)* เป็นเครื่องพิมพ์ ที่ได้รับความนิยม โดยองค์ประกอบสำคัญได้แก่ หัวพิมพ์ (Print Head) ที่ประกอบไปด้วยเข็มพิมพ์ 9 เข็ม หรือ 24 เข็ม (ทำให้เรียกเครื่องพิมพ์ชนิดนี้ได้อีกว่า เครื่องพิมพ์ 9 เข็ม และเครื่องพิมพ์ 24 เข็ม) ชุดของเข็มพิมพ์แบบ 9 เข็มจะเรียงตรงกันในแนวตั้งคอลัมน์เดียว ส่วนชุดของเข็มพิมพ์แบบ 24 เข็ม จะเรียงกันในแนวตั้งโดยแบ่งเป็น 3 คอลัมน์ๆ ละ 8 เข็ม วางเหลื่อมกันระหว่างคอลัมน์



- **เครื่องพิมพ์แบบไม่กระทบ** (Non - Impact Printers) เป็นเครื่องพิมพ์ที่ไม่ต้องอาศัยหัวพิมพ์กดลงบนกระดาษ แต่อาศัยเทคนิคอื่น เช่น การพ่นหมึก การใช้ความร้อน หรือการใช้แสงเลเซอร์





- **เครื่องพิมพ์แบบพ่นหมึก**
(Ink Jet Printer)
- **เครื่องพิมพ์เลเซอร์**
(Laser Printer)

3. Plotter

เป็นอุปกรณ์แสดงข้อมูลที่มักจะใช้กับงานออกแบบเขียนแบบ (CAD) โดยจะแปลงสัญญาณข้อมูล เป็นเส้นตรงหรือเส้นโค้งก่อนพิมพ์ลงบนกระดาษ ทำให้แสดงผลเป็นกราฟแผนที่ แผนภาพต่างๆ ได้ โดยตัวพล็อตเตอร์จะมีปากกามากกว่า 1 ด้าม เคลื่อนไปมาด้วยการควบคุมของคอมพิวเตอร์ โดยปากกาแต่ละด้ามจะมีสี และขนาดเส้นที่ต่างกันทำให้ได้ภาพที่สวยงาม มีคุณภาพสูงและขนาดตามขนาดของเครื่องพล็อตเตอร์

หน่วยเก็บข้อมูลรอง (Secondary Storage Unit)

นอกจากองค์ประกอบที่ได้กล่าวไปแล้ว ยังมีส่วนการทำงานอีกส่วนหนึ่งที่จำเป็น และสำคัญมากในการใช้คอมพิวเตอร์ ได้แก่ ***"หน่วยเก็บข้อมูลรอง"*** เนื่องจากข้อมูลต่างๆ ที่ส่งเข้ามาประมวลผล และผลลัพธ์จากการประมวลผล จะถูกเก็บไว้ในหน่วยความจำแรม ซึ่งเมื่อปิดเครื่อง หรือมีปัญหาทางไฟฟ้า อาจจะทำให้ข้อมูลเหล่านั้นสูญหาย จึงจำเป็นต้องมีหน่วยเก็บข้อมูลรอง เพื่อนำข้อมูลจากหน่วยความจำแรมมาเก็บไว้เพื่อเรียกใช้ต่อไป

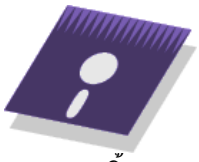
หน่วยเก็บข้อมูลรองที่นิยมใช้กันอย่างแพร่หลายในปัจจุบัน ได้แก่แผ่นบันทึกแม่เหล็ก (Floppy Disk หรือ Diskette), ฮาร์ดดิสก์ (Hard Disk) และซีดี-รอม (CD-ROM)

- **แผ่นบันทึกแม่เหล็ก** (Floppy Disk หรือ Diskette)

เป็นแผ่นบันทึกข้อมูลที่มีลักษณะกลมบาง ทำจากสารไมล่าร์ (Mylar) ที่ฉาบด้วยสารแม่เหล็ก บรรจุในซอง PVC หรือพลาสติกแข็ง เพื่อป้องกันฝุ่นละอองและการขูดขีด

Floppy Disk ที่ใช้กันในปัจจุบันมี 2 ขนาด คือ

- ขนาด 5.25 นิ้ว ($5\ ^1/_4$ นิ้ว) เรียกว่า Mini Floppy Disk
- ขนาด 3.50 นิ้ว ($3\ ^1/_2$ นิ้ว) เรียกว่า Micro Floppy Disk



5.25 นิ้ว

3.50 นิ้ว

และแต่ละขนาดยังแบ่งได้อีก 2 ประเภท ตามความจุข้อมูล ดังนี้

- ความจุธรรมดา หรือ แผ่นความจุ 2 เท่า (Double Density)
- ความจุสูง เรียกว่า High Density

ซึ่งสามารถแบ่งกลุ่มได้ดังนี้

- Floppy Disk ขนาด $5\ ^1/_4$ นิ้ว ความจุธรรมดา (DSDD) เก็บข้อมูลได้ 360 KB ส่วนความจุสูง (DSHD) เก็บข้อมูลได้ 1.2 MB
- Floppy Disk ขนาด $3\ ^1/_2$ นิ้ว ความจุธรรมดา (DSDD) เก็บข้อมูลได้ 720 KB ส่วนความจุสูง (DSHD) เก็บข้อมูลได้ 1.44 MB

- **ฮาร์ดดิสก์** (Hard Disk)

ฮาร์ดดิสก์ เป็นอุปกรณ์บันทึกข้อมูลที่มีลักษณะเป็นจานหลายแผ่นซ้อนกันบนแกนเดียว ติดตรึงอยู่ในกล่องโลหะมิดชิด กันฝุ่นละอองเข้า สามารถบันทึก

ข้อมูลได้เป็นจำนวนมาก เมื่อเริ่มผลิตนั้นบันทึกข้อมูลได้เพียง 10 MByte ต่อมาจึงได้รับการปรับปรุงจนบันทึกได้เป็นพันล้านไบต์ (GByte)

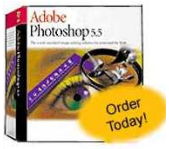
- CD-ROM

CD-ROM หรือ Compact Disk Read Only Memory เป็นอุปกรณ์บันทึกข้อมูลประเภทอ่านได้อย่างเดียว ปัจจุบันกำลังได้รับความนิยมเนื่องจากมีความจุในการเก็บบันทึกข้อมูล 600 MB ต่อ 1 แผ่น แผ่นซีดีรอม มีลักษณะเหมือนแผ่นซีดีที่ใช้บันทึกเพลงวางขายทั่วไปนั่นเอง ที่เติมคำว่า “รอม” ลงไปด้วย ก็เพื่อแยกให้ชัดเจนว่าเก็บบันทึกข้อมูลมาให้อ่านไปใช้เท่านั้น บันทึกทับไม่ได้

ซอฟต์แวร์ (Software)

ซอฟต์แวร์หรือ โปรแกรมคำสั่งเครื่อง แบ่งได้เป็น 2 ประเภทใหญ่ ๆ คือ

- โปรแกรมระบบ (System Software)
- โปรแกรมประยุกต์ (Application Software)



1. **โปรแกรมระบบ** (System Software) เป็นตัวกลางสำคัญที่ผู้ใช้สามารถใช้เครื่องคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ แบ่งออกเป็น

- Language Software
- Operating System Software
- Utilities Software

Language Software

เป็นซอฟต์แวร์ที่เขียนเพื่อใช้ในการแปลความหมายของคำสั่งในภาษาคอมพิวเตอร์ เพื่อให้เครื่องคอมพิวเตอร์ทำงานตามที่ต้องการ เช่น Assembly, Pascal, BASIC, COBOL เป็นต้น

Operating System Software

เป็นซอฟต์แวร์ที่เขียนขึ้นเพื่อช่วยให้การสั่งงานเครื่องคอมพิวเตอร์กระทำได้รวดเร็ว ง่าย และมีประสิทธิภาพ มักใช้ชื่อเรียกทั่วไปว่า “ระบบปฏิบัติการ” เช่น DOS, Windows, OS/2, UNIX

ระบบปฏิบัติการทำหน้าที่จัดการเกี่ยวกับอุปกรณ์ต่างๆ ของระบบไมโครคอมพิวเตอร์ เช่น หน่วยประมวลผลกลาง อุปกรณ์รับ-ส่งข้อมูล รวมทั้งโปรแกรมต่างๆ ในชุดนี้ยังช่วยเพิ่มประสิทธิภาพในการทำงานของคอมพิวเตอร์ให้เกิดความสะดวก รวดเร็วด้วย ถือได้ว่าระบบปฏิบัติการ เป็นตัวเชื่อมระหว่างฮาร์ดแวร์กับผู้ใช้เพื่อจัดการเกี่ยวกับสิ่งต่อไปนี้ คือ

- การจัดการเกี่ยวกับไฟล์และ Software ต่างๆ
- การจัดการเกี่ยวกับอุปกรณ์รับข้อมูลและแสดงผล
- การจัดการเกี่ยวกับหน่วยความจำ
- การจัดการเวลาในหน่วยประมวลผลกลาง

Utility Software

เป็นซอฟต์แวร์ทำหน้าที่ช่วยเสริมให้การใช้คอมพิวเตอร์ กระทำได้สะดวกขึ้น โดยเฉพาะในการจัดการกับตัวเครื่อง หน่วยความจำ จานแม่เหล็ก แฟ้มข้อมูล โดยหน้าที่เสริมได้แก่

- การกู้แฟ้มข้อมูลทั้งหมด หรือบางส่วน
- การรักษาความปลอดภัยของข้อมูล
- การจัดการข้อมูลของดิสก์
  - การบำรุงรักษาฮาร์ดดิสก์
  - การสร้างแฟ้มย่อย
  - การจัดการบัญชีชื่อแฟ้มข้อมูล

2. **โปรแกรมประยุกต์** (Application Software)

โปรแกรมที่ผู้ใช้จัดทำขึ้นมาเพื่องานโดยเฉพาะหรืองานที่ผู้ใช้ต้องการ โดยที่ผู้ใช้จะใช้โปรแกรมภาษาจัดทำขึ้นมา แล้วให้โปรแกรมควบคุมเครื่องนำไปประมวลเพื่อให้เครื่องปฏิบัติตาม โดยผู้ใช้สามารถใช้ภาษาคอมพิวเตอร์ต่างๆ ในการทำโปรแกรมนี้ก็ได้ เช่น FORTRAN, COBOL, BASIC, C, Pascal เป็นต้น

โปรแกรมที่เน้นการประยุกต์ใช้งานตามสภาพลักษณะงานของผู้ใช้คอมพิวเตอร์ สามารถแบ่งได้เป็น

ก. ซอฟต์แวร์จัดระบบฐานข้อมูล (Data Base Management Software)

เป็นซอฟต์แวร์ในด้านการประมวลผล และจัดการกับข้อมูล กลุ่มข้อมูลจำนวนมาก เช่น FoxPro for Windows, Paradox, Microsoft Access, Instant Database, Mini/Micro CDS/ISIS

ข. ซอฟต์แวร์จัดพิมพ์รายงาน หรือซอฟต์แวร์ประมวลผลคำ (Word Processing Software)

ซอฟต์แวร์ที่ทำหน้าที่จัดการเกี่ยวกับการสร้างเอกสารหรือรายงาน การแก้ไข ดัดแปลง และการพิมพ์เอกสารหรือรายงาน เช่น CU-WORD, Word Perfect For DOS/For Windows, Microsoft Word, Ami Pro

ค. ซอฟต์แวร์การคำนวณ (Calculation Software)

เป็นซอฟต์แวร์ที่ช่วยอำนวยความสะดวกในการคำนวณ โดยเฉพาะการคำนวณที่ต้องการเห็นผลการเปลี่ยนแปลงของค่าต่างๆ เมื่อข้อมูลเปลี่ยนแปลง และโปรแกรมบางตัวยังรวมเอาความสามารถทาง Data Base Management และ Word Processor มารวมอยู่ด้วย เช่น LOTUS 1-2-3 For DOS/For Windows, Microsoft Excel

ง. ซอฟต์แวร์สำหรับงานกราฟฟิก (Graphic Software)

ซอฟต์แวร์ที่ใช้วาดรูป สร้างรูป หรือการทำงานนำเสนอต่างๆ ซึ่งบางโปรแกรมสามารถสร้างภาพเคลื่อนไหวได้ด้วย เช่น Adobe PhotoShop, Macromedia Firework, CorelDraw

จ. ซอฟต์แวร์สำหรับนำเสนอผลงาน (Presentation Software)

ซอฟต์แวร์สำหรับสร้างงาน เพื่อใช้ในการนำเสนอ (Present) โดยอาจจะเป็นภาพนิ่ง หรือภาพเคลื่อนไหว เช่น Microsoft PowerPoint, Freelance Graphics

ช. ซอฟต์แวร์สำหรับงานธุรกิจ (Business Software)

ซอฟต์แวร์ที่เขียนขึ้นมาเฉพาะงาน เช่น งานระบบสินค้าคงคลัง งานธนาคาร

บุคลากรทางคอมพิวเตอร์ (Peopleware)

หมายถึง บุคคลที่มีส่วนเกี่ยวข้องในการทำงานด้านคอมพิวเตอร์ ได้แก่

ก. ผู้บริหารงานคอมพิวเตอร์

มีหน้าที่ในการจัดการและบริหารงานต่าง ๆ

ข.นักออกแบบระบบ (System Designer)
มีหน้าที่กำหนดการปฏิบัติการของเครื่องคอมพิวเตอร์ให้เป็นไปตามความต้องการด้านข่าวสารที่นักวิเคราะห์ข่าวสารวางไว้

ค.นักโปรแกรมระบบ (System Programmer)
มีหน้าที่เขียนโปรแกรมปฏิบัติการ (Operating System) และโปรแกรมจัดการเกี่ยวกับข้อมูล (Data Management)

ง.นักโปรแกรมประยุกต์ (Application Programmer)
มีหน้าที่เขียน ทดสอบและแก้ไขปรับปรุงโปรแกรมที่ใช้เฉพาะงาน เช่น งานธุรกิจ งานการรักษา เป็นต้น

จ.นักบำรุงรักษาโปรแกรม (Maintenance Programmer)
มีหน้าที่บำรุงรักษาโปรแกรม ที่นักโปรแกรมระบบและนักโปรแกรมประยุกต์เขียนไว้ โดยเมื่อนำเอาโปรแกรมไปใช้แล้ว เกิดข้อผิดพลาดนักบำรุงรักษาโปรแกรมจะต้องจัดหาสาเหตุ และทำการแก้ไขโปรแกรมนั้น ๆ

ฉ.พนักงานเตรียมข้อมูล (Data Preparation Clerk)
มีหน้าที่ในการเตรียมข้อมูลให้อยู่ในรูปแบบที่คอมพิวเตอร์อ่านได้ เช่น เจาะบัตร พิมพ์เข้าจานแม่เหล็ก เป็นต้น

ช.ผู้ใช้โปรแกรม (Uses)
เป็นผู้นำเอาโปรแกรมที่เขียนเสร็จแล้วมาใช้งาน

ข้อมูลในคอมพิวเตอร์

การใช้โปรกรรมต่างๆ ในคอมพิวเตอร์ จะเกี่ยวข้องกับข้อมูลอย่างแน่นอน โดยที่ข้อมูลซึ่งป้อนเข้าไปในคอมพิวเตอร์จะถูกแปลงให้อยู่ในระบบเลขฐานสอง อันประกอบด้วยตัวเลขเพียงสองตัว คือ 0 กับ 1 เท่านั้น ในทางคอมพิวเตอร์จะเรียกตัวเลข 0 หรือ 1 นั้นๆ ว่า "บิต (bit)" และเรียกตัวเลข 0 หรือ 1 ที่เรียงกัน 8 ตัวเลขว่า "ไบต์ (byte)" หรือจะกล่าวได้ว่า 1 byte เท่ากับ 8 bit นั่นเอง

0 หรือ 1	=	1 บิต (bit)
11011100	=	1 ไบต์ (byte)

ทั้งนี้ จะมีการกำหนดค่าหรือรหัสมาตรฐานสำหรับการใช้เลขฐานสอง คือ 0 และ 1 เพื่อกำหนดแทนค่าพยัญชนะ สระ และวรรณยุกต์ไว้ เช่น คำว่า "ธุรกรรม"[19] ซึ่งแยกได้ ดังนี้

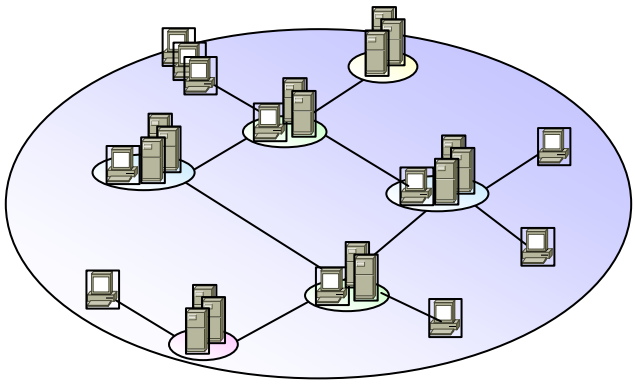
- อักษร "ธ" จะแทนด้วย " 1 0 1 1 1 0 0 0 "
- สระ "ุ" จะแทนด้วย " 1 1 0 1 1 0 0 0 "
- อักษร "ก" จะแทนด้วย " 1 0 1 0 0 0 0 1 "
- อักษร "ร" จะแทนด้วย " 1 1 0 0 0 0 1 1 "
- อักษร "ม" จะแทนด้วย " 1 1 0 0 0 0 0 1 "

ดังนั้น คำว่า "ธุรกรรม" จึงประกอบด้วยกลุ่มเลข 0 และ 1 มากมาย

[19] รหัสภาษาไทยที่ใช้ใน Microsoft Windows 95 Thai Edition.

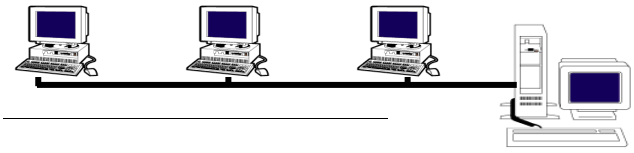
1.1.2 ระบบเครือข่ายคอมพิวเตอร์ (Computer Networks)

เครือข่ายคอมพิวเตอร์เกิดจากการนำเครื่องคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไป มาต่อพ่วงกันเพื่อประโยชน์ในการส่ง หรือรับข้อมูลอิเล็กทรอนิกส์



ระบบเครือข่ายคอมพิวเตอร์หากจำแนกตามระยะทางของการเชื่อมต่อระหว่างอุปกรณ์สื่อสารสามารถแบ่งได้เป็น 3 ประเภทดังนี้ [20]

Local Area Network (LAN) ระบบเครือข่ายแบบนี้จะเป็นเครือข่ายคอมพิวเตอร์ที่มีการเชื่อมต่ออุปกรณ์สื่อสารในระยะทางที่จำกัดซึ่งมีความเร็วในการแลกเปลี่ยนข้อมูลสูง เป็นเครือข่ายที่ใช้ในหน่วยงานต่าง ๆ เฉพาะกลุ่มจึงเป็นระบบเครือข่ายแบบปิด (Close Network) เช่น ระบบอินทราเน็ต (Intranet) เป็นต้น



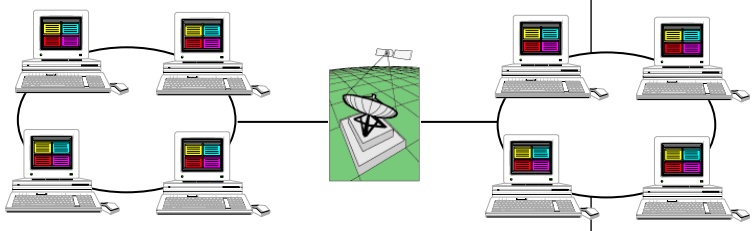
[20] ศรีไพร ศักดิ์รุ่งพงศากุล, เทคโนโลยีคอมพิวเตอร์ และสารสนเทศ, (กรุงเทพฯ: ซีเอ็ดยูเคชั่น, 2544), หน้า 165.

Metropolitan Area Network (MAN)

เป็นระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ครอบคลุมพื้นที่มากกว่าระบบเครือข่ายแบบ LAN เครือข่ายนี้เกิดจากการเชื่อมต่อของเครือข่ายคอมพิวเตอร์แบบ LAN ตั้งแต่ 2 เครือข่ายเข้าด้วยกัน

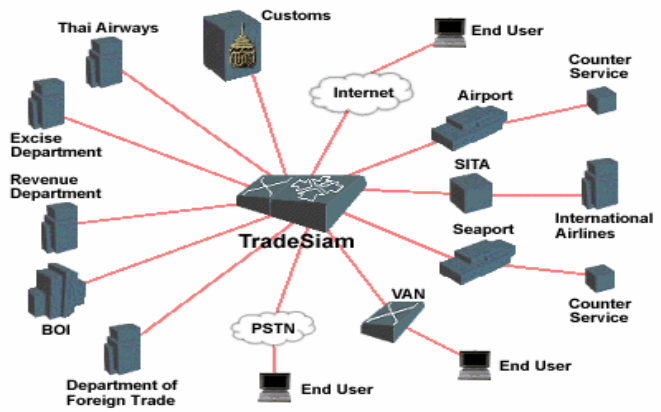
Wide Area Network (WAN)

เป็นระบบเครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่ ประกอบด้วยระบบเครือข่ายคอมพิวเตอร์ทั้งแบบ LAN และเครือข่ายคอมพิวเตอร์แบบ MAN พื้นที่ของเครือข่ายสามารถครอบคลุมพื้นที่ได้ในระดับประเทศ หรือระดับโลก และเป็นระบบเครือข่ายแบบเปิด (Open Network) ระบบเครือข่ายอินเทอร์เน็ต (Internet) ก็เป็นระบบเครือข่ายแบบ WAN เช่นกัน



1.1.3 **การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์** (Electronic Data Interchange)

การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ หรือ EDI เป็นการติดต่อทางเครือข่ายรูปแบบหนึ่ง เกิดขึ้นในปี ค.ศ.1960 โดยบริษัทในประเทศสหรัฐอเมริกาได้นำระบบส่งเอกสารที่เป็นข้อมูลอิเล็กทรอนิกส์มาใช้ในการซื้อขายสินค้าของบริษัท ต่อมาได้มีการร่วมมือกันระหว่างกลุ่มผู้ประกอบการอุตสาหกรรมขึ้นเพื่อกำหนดรูปแบบมาตรฐานของข้อมูลอิเล็กทรอนิกส์ที่จะใช้ติดต่อสื่อสารกัน มักนิยมใช้กับการส่ง-รับเอกสารจำพวกใบสั่งซื้อ ใบเสนอราคา ใบกำกับสินค้า และเอกสารอื่น ๆ โดยเฉพาะอย่างยิ่งในการผ่านพิธีการทางศุลกากรเพื่อนำเข้าและส่งออกสินค้า



ปัจจุบันได้มีมาตรฐานในการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ ที่เป็นที่ยอมรับกันในนานาประเทศอยู่ 2 รูปแบบ คือ

1. EDIFACT (Electronic Data Interchange For Administration, Commerce, and Transport) อันเป็นมาตรฐานที่กำหนดขึ้นโดยสหประชาชาติ United Nation Economic Commission for Europe ประมาณปี ค.ศ. 1985 เป็นมาตรฐานในการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ที่ได้รับความนิยมและใช้กันอย่างแพร่หลายในทวีปเอเชีย และยุโรป

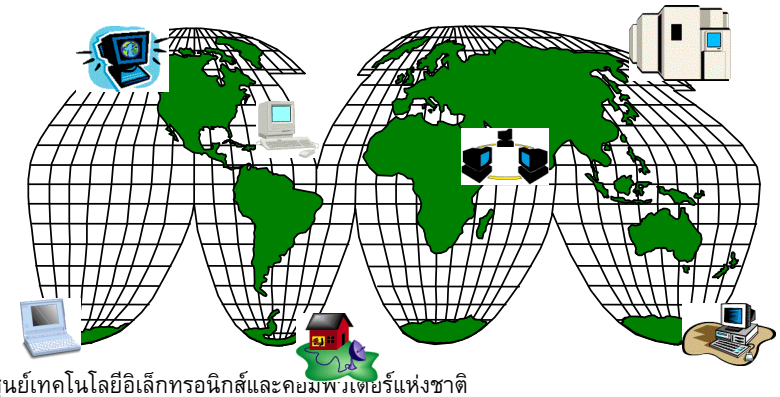
2. ANSI X.12 เป็นการกำหนดมาตรฐานการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ที่กำหนดขึ้นโดย ANSI หรือ American National Standards Institute เป็นมาตรฐานในประเทศแถบอเมริกาเหนือ และนิวซีแลนด์

ประโยชน์ที่ได้รับกรณีที่มีการนำ EDI มาใช้ เช่น ลดค่าใช้จ่ายในการคีย์ข้อมูลและได้ข้อมูลที่ถูกต้องมากขึ้น ทำให้การติดต่อสื่อสารในกลุ่มที่มีการตกลงกันให้ใช้ EDI สามารถทำได้รวดเร็วขึ้น และช่วยลดงานทางด้านเอกสารอันจะช่วยให้การตัดสินใจมีประสิทธิภาพมากยิ่งขึ้น

1.1.4 ระบบเครือข่ายอินเทอร์เน็ต (Internet Network)

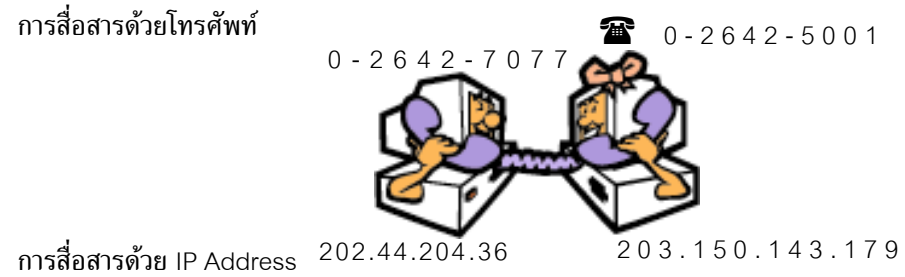
(ก) ความรู้ทั่วไป

ระบบเครือข่ายอินเทอร์เน็ตนับเป็นระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เกิดขึ้นจากการเชื่อมต่อเครือข่ายต่างๆ ไม่ว่าจะเป็นแบบ LAN หรือ WAN หลายเครือข่ายเข้าด้วยกัน ทำให้เครื่องคอมพิวเตอร์นับล้านๆ เครื่องทั่วโลกสามารถติดต่อสื่อสารกันได้



โดยเครื่องคอมพิวเตอร์แต่ละเครื่องที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตจะใช้มาตรฐานของการสื่อสารแบบเดียวกัน เรียกว่า TCP/IP หรือ Transmission Control Protocol/Internet Protocol และเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่ายอินเทอร์เน็ตจะต้องมีหมายเลขประจำตัวของเครื่องนั้น หรือที่เรียกว่า IP address ที่ประกอบด้วยเลขฐานสอง 4 ชุด ชุดละ 8 บิต ดังนั้น เลขหมายของ IP address จึงมีขนาด 32 บิต ต่อมาเพื่อความสะดวกในการใช้งานได้มีการแปลง IP address ที่อยู่ในระบบตัวเลขฐานสองเป็นระบบเลขฐานสิบ 4 ชุดเช่นเดิม

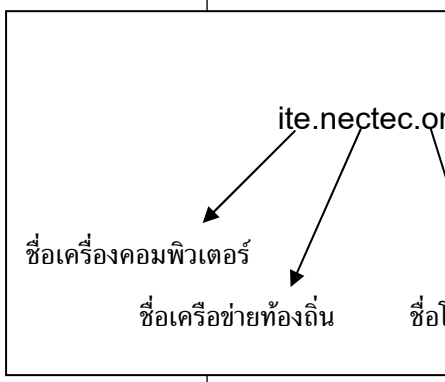
IP address = **เลขฐานสอง 4 ชุด ๆ ละ 8 บิต = ตัวเลขฐานสิบ 4 ชุด**
11001011. 10010110. 11110011. 10110011 = 203.150.243.179



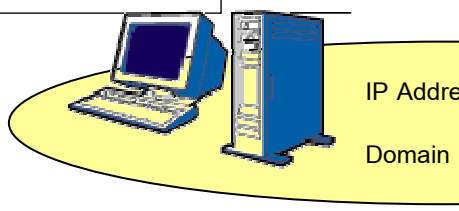
สืบเนื่องจากเลขหมาย IP address มีจำนวนมากขึ้น ทำให้ไม่สะดวกต่อการจำเลขหมาย ดังนั้น จึงได้มีการกำหนดชื่อที่เป็นตัวอักษรเพื่อใช้แทนหมายเลข IP address โดยเรียกชื่อที่ใช้แทนว่า “โดเมนเนม (Domain Name)” ดังนั้นโดเมนเนม ก็คือชื่อที่เป็นตัวอักษรของเลขหมาย IP address ของเครื่องคอมพิวเตอร์นั่นเอง

โดเมนเนมจะประกอบด้วยชื่อเครื่องคอมพิวเตอร์ ชื่อเครือข่ายท้องถิ่น ชื่อโดเมนย่อย และชื่อโดเมน ตัวอย่างเช่น

การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตจำเป็นต้องอาศัยอุปกรณ์พื้นฐานสำคัญ ๆ ได้แก่ เครื่องคอมพิวเตอร์ โมเด็ม สายโทรศัพท์ โดยเชื่อมต่อระบบอินเทอร์เน็ตผ่านการให้บริการของผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider หรือ ISP)



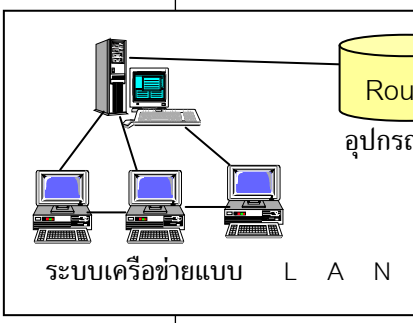
ทั้งนี้ ในการเชื่อมต่อเครือข่ายอินเทอร์เน็ตจะมีอุปกรณ์สำคัญอีกชนิดหนึ่งซึ่งนับเป็นคอมพิวเตอร์ประเภทหนึ่งใช้ในการจัดหาเส้นทางที่จะเชื่อมระหว่าง



คอมพิวเตอร์เครื่องหนึ่งกับคอมพิวเตอร์อีกเครื่องหนึ่ง นั่นคือ อุปกรณ์จัดเส้นทาง (Router)

อย่างไรก็ตาม การเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตมักเป็นการเชื่อมต่อโดยผ่านการให้บริการของผู้ให้บริการอินเทอร์เน็ตหรือ ISP แต่ในบางกรณีก็อาจเป็นการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตโดยตรง (Direct Internet Access) โดยไม่ผ่านการให้บริการของผู้ให้บริการอินเทอร์เน็ต มักเป็นการเชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ตโดยหน่วยงานของรัฐ หรือสถาบันการศึกษา เป็นต้น

นอกจากการเชื่อมต่อกับอินเทอร์เน็ตที่กล่าวมาข้างต้นซึ่งมักเป็นการติดต่อระหว่างเครื่องคอมพิวเตอร์เท่านั้น ก็เริ่มมีการประยุกต์ให้มีการใช้บริการอินเทอร์เน็ตผ่านระบบโทรศัพท์มือถือได้ด้วย โดยเรียกเทคโนโลยีนี้ว่า WAP หรือ Wireless Application Protocol ที่สามารถใช้โทรศัพท์มือถือเชื่อมต่อกับเครือข่ายอินเตอร์เน็ตได้โดยไม่ต้องอาศัยโมเด็ม (MODEM) และสายโทรศัพท์เช่นเดิม



(ข) ประโยชน์ของเครือข่ายอินเทอร์เน็ต

เนื่องจากเครือข่ายอินเทอร์เน็ตเป็นเครือข่ายการสื่อสารที่ครอบคลุมถึงบุคคลจำนวนมากไม่ว่าในประเทศหรือในโลก และเป็นเครือข่ายที่มีราคาถูกแต่มีประสิทธิภาพมากมาย และเนื่องจากประโยชน์นานัปการของเครือข่ายอินเทอร์เน็ตทำให้จำนวนผู้ใช้อินเทอร์เน็ตเพิ่มขึ้นอย่างรวดเร็วในระยะเวลาอันสั้น

ประโยชน์ของเครือข่ายอินเทอร์เน็ตมีหลายประการ เช่น ใช้ในการส่งจดหมายอิเล็กทรอนิกส์หรือข้อความอิเล็กทรอนิกส์ ศึกษาค้นคว้าข้อมูลจากแหล่งข้อมูลต่าง ๆ ที่มีอยู่เป็นจำนวนมาก ใช้ในการสนทนาผ่านเครือข่าย หรือใช้ในกิจการอื่น ๆ เพื่อความบันเทิง

และเมื่อมีการพัฒนาประสิทธิภาพของเครือข่ายอินเทอร์เน็ตมากขึ้น จนในปัจจุบันสามารถใช้เครือข่ายนี้อำนวยความสะดวกในการประกอบธุรกิจการค้าผ่านเครือข่ายอินเทอร์เน็ต หรือที่เรียกว่า "การทำพาณิชย์อิเล็กทรอนิกส์" (Electronic Commerce) ได้ด้วย

1.1.5 จดหมายอิเล็กทรอนิกส์ (Electronic Mail)

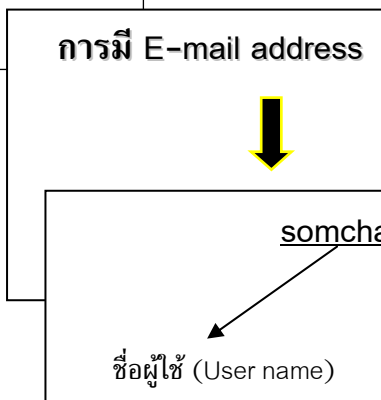
จดหมายอิเล็กทรอนิกส์ หรือที่เรียกว่า e-mail นั้นเป็นรูปแบบการติดต่อสื่อสารอีกประเภทหนึ่งที่ใช้เครือข่ายอินเทอร์เน็ตเพื่อช่วยให้การติดต่อสื่อสารระหว่างบุคคลสะดวก และรวดเร็วยิ่งขึ้น

หากจะเปรียบเทียบระหว่างการส่งจดหมายธรรมดา และจดหมายอิเล็กทรอนิกส์แล้ว โดยปกติในการส่งจดหมายธรรมดานั้น ผู้ส่งจะต้องมีการระบุชื่อ

และที่อยู่ของผู้รับ ในการส่งจดหมายอิเล็กทรอนิกส์ก็เช่นเดียวกัน ที่ผู้ส่งจะต้องระบุที่อยู่ของผู้รับจดหมายอิเล็กทรอนิกส์นั้น

ที่อยู่ของผู้ส่งและผู้รับในระบบเครือข่ายอินเตอร์เน็ตนั้นเราเรียกว่า e-mail address เช่น somchai@hotmail.com

e-mail address เปรียบเสมือนชื่อบุคคล เลขที่บ้าน และที่อยู่ในการส่งจดหมายธรรมดา e-mail address จะประกอบด้วย ชื่อผู้ใช้ (User Name) และชื่อโดเมนเนม (Domain Name)

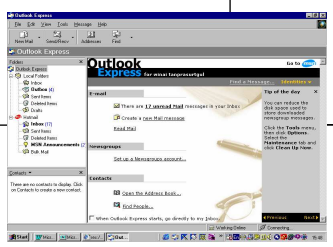


การส่งจดหมายอิเล็กทรอนิกส์นั้นผู้ส่งอาจใช้โปรแกรมในการรับส่ง ซึ่งปัจจุบันมีโปรแกรมหลายชนิดที่ทำหน้าที่ในการส่งและรับจดหมายอิเล็กทรอนิกส์ เช่น Netscape Mail, Microsoft Outlook Express หรือ Lotus Notes เป็นต้น

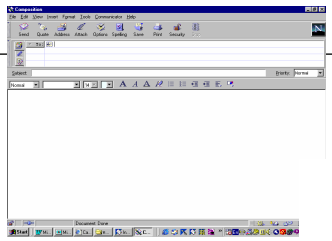
(1) ปัญหาการใช้ E-mail address

เนื่องจากวิวัฒนาการของเทคโนโลยีการติดต่อสื่อสารที่ก้าวหน้าอย่างไม่หยุดยั้ง จนปัจจุบันการติดต่อสื่อสารไม่จำเป็นที่จะต้องมีการพบหน้ากัน หรือจำเป็นที่จะต้องรู้จักกันมาก่อน สามารถกระทำได้ผ่านเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) การสนทนาผ่านระบบเครือข่ายอินเทอร์เน็ตแบบออนไลน์ เป็นต้น

ปัญหาประการหนึ่งที่สำคัญเมื่อมีการใช้เทคโนโลยีการสื่อสารที่ต้องอาศัยเครือข่ายคอมพิวเตอร์ คือการระบุสถานที่ของบุคคลที่มีการติดต่อสื่อสาร ยกตัวอย่างเช่นการรับการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) จะทราบได้อย่างไรว่าบุคคลดังกล่าวได้ทำการส่งจดหมายมาจากมุมใดของโลก เพราะเนื่องจากระบบเครือข่าย อินเทอร์เน็ตเป็นระบบเปิดบุคคลสามารถเข้าถึงเวลาใด ณ ที่ใดของโลกก็ได้



Microsoft Outlook Express



Netscape Mail

ก. ปัญหาการระบุตัวบุคคลผู้ส่ง และรับข้อมูลอิเล็กทรอนิกส์หรือจดหมายอิเล็กทรอนิกส์

ปัญหาที่ตามมาก็คือในกรณีที่เป็น e-mail address ของผู้ให้บริการ free e-mail address ในการสมัครขอใช้บุคคลทุกคนสามารถสมัคร และได้รับ e-mail address และที่สำคัญที่สุดการให้ข้อมูลต่าง ๆ นั้นบุคคลสามารถกรอกข้อความที่ไม่ต้องตรงกับความเป็นจริงได้ เนื่องจากว่าผู้ให้บริการ Free e-mail ไม่มีการตรวจสอบข้อมูลที่ผู้สมัครกรอกลงในใบลงทะเบียนหรือที่เรียกว่า Register แต่อย่างใด

ดังนั้น บุคคลคนเดียวสามารถขอ e-mail address ได้หลายชื่อในผู้ให้บริการเดียวกัน เพราะการให้ข้อมูลกับผู้ให้บริการ Free e-mail address อาจจะมีการปกปิด หรือให้ข้อเท็จจริงที่คลาดเคลื่อนด้วยเหตุผลบางประการ

เมื่อบุคคลสามารถที่จะมี e-mail address ได้หลายชื่อในเวลาเดียวกัน ทำให้เกิดปัญหาในการระบุตัวบุคคลว่า เจ้าของ e-mail address นั้นแท้จริงแล้วเป็นบุคคลใดกันแน่ ยิ่งในกรณีที่การติดต่อสื่อสารกันด้วยจดหมายอิเล็กทรอนิกส์นั้นเป็นการติดต่อสื่อสารระหว่างบุคคลที่ไม่เคยพบหน้ากันมาก่อน

ดังนั้น ในการทำธุรกรรมทางอิเล็กทรอนิกส์ จึงจำเป็นที่จะต้องมีหลักการของบุคคลที่สาม (Third Parties) เข้ามารับรองความมีตัวตนของคู่กรณีที่มีการทำ
ธุรกรรมทางอิเล็กทรอนิกส์ หรือการใช้เทคโนโลยีเข้ามาพิสูจน์เพื่อระบุตัวบุคคลที่เป็นคู่กรณีดังกล่าว เช่น ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) ลายมือชื่อดิจิทัล (Digital Signature) หรือเทคโนโลยีชีวภาพ เป็นต้น

ข. ปัญหาการระบุสถานที่ในการส่งหรือการได้รับข้อมูลอิเล็กทรอนิกส์หรือจดหมายอิเล็กทรอนิกส์

ปัญหาที่สำคัญอีกประการหนึ่งของการใช้เครือข่ายอินเทอร์เน็ตในการทำธุรกรรมทางอิเล็กทรอนิกส์ คือการระบุว่าสถานที่ใดคือสถานที่มีการส่ง การรับข้อมูลอิเล็กทรอนิกส์ เนื่องจากกว่าเทคโนโลยีสารสนเทศที่เกี่ยวกับเรื่องของการส่งการรับข้อมูลอิเล็กทรอนิกส์ที่มักจะกระทำผ่านระบบเครือข่าย ซึ่งในปัจจุบันได้พัฒนาให้

สามารถเชื่อมต่อกับระบบเครือข่ายที่ใช้ในการติดต่อสื่อสารได้แม้ว่าได้เดินทางไปนอกประเทศ ก็สามารถใช้บริการเชื่อมต่อระบบเครือข่ายได้เสมือนกับอยู่ในประเทศ

ยกตัวอย่างเช่น ในกรณีที่ผู้ประกอบการค้าในประเทศไทยทำการติดต่อทำธุรกรรมโดยใช้ข้อมูลอิเล็กทรอนิกส์เสนอทำสัญญากับผู้ประกอบการค้าในประเทศจีน และในกรณีที่ผู้ประกอบการค้าในประเทศไทยใช้เครื่องคอมพิวเตอร์กระเป๋าหิ้วของตนส่งข้อมูลอิเล็กทรอนิกส์ให้กับผู้ประกอบการค้าในประเทศจีนในขณะที่ตนเองไปเข้าร่วมการประชุมที่ประเทศจีน ทั้งสองกรณีนี้จะถือว่ามีการส่ง การรับข้อมูลอิเล็กทรอนิกส์เกิดขึ้นในประเทศใด และผลของการส่ง หรือการได้รับข้อมูลอิเล็กทรอนิกส์เหมือนกับกรณีแรกหรือไม่

ดังนั้น เพื่อขจัดปัญหาในเรื่องของการระบุสถานที่ในการส่ง การรับข้อมูลอิเล็กทรอนิกส์ที่เกิดขึ้นในการทำธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายจึงจำเป็นต้องกำหนดหลักการเกี่ยวกับสถานที่ที่ถือว่าการส่ง การรับข้อมูลอิเล็กทรอนิกส์มีผล โดยวางหลักไว้ในกรณีที่ผู้ส่งและผู้รับข้อมูลอิเล็กทรอนิกส์ไม่มีการตกลงกันว่าจะเลือกสถานที่ใดเป็นที่ที่มีการส่ง หรือการรับข้อมูลอิเล็กทรอนิกส์ ให้ถือว่าได้ทำการส่งหรือได้รับข้อมูลอิเล็กทรอนิกส์ ณ ที่ทำการงานของผู้นั้น หากคู่กรณีมีสถานที่ทำการงานหลายแห่งให้ถือเอาแห่งที่มีความสัมพันธ์กับธุรกรรมนั้นมากที่สุด หากไม่สามารถระบุได้ว่าสถานที่ทำการงานใดมีความสัมพันธ์ใกล้ชิดมากที่สุดให้ถือว่ามีการส่ง และได้รับข้อมูลอิเล็กทรอนิกส์นั้นที่สำนักงานใหญ่ และในกรณีที่ไม่มีสถานที่ทำการงาน ก็ให้ถือเอาถิ่นที่อยู่เป็นสถานที่ทำการส่ง หรือการได้รับข้อมูลอิเล็กทรอนิกส์นั้น [21]

---

[21] หลักการของร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ....

"มาตรา 23 เว้นแต่ผู้ส่งข้อมูลและผู้รับข้อมูลจะได้ตกลงกันไว้เป็นอย่างอื่น การส่งหรือการรับข้อมูลอิเล็กทรอนิกส์ ให้ถือว่าได้ส่ง ณ ที่ทำการงานของผู้ส่งข้อมูล หรือได้รับ ณ ที่ทำการงานของผู้รับข้อมูล แล้วแต่กรณี

ในกรณีที่ผู้ส่งข้อมูลหรือผู้รับข้อมูลมีที่ทำการงานหลายแห่ง ให้ถือเอาที่ทำการงานที่เกี่ยวข้องมากที่สุดกับธุรกรรมนั้นเป็นที่ทำการงานเพื่อประโยชน์ตามวรรคหนึ่ง แต่ถ้าไม่สามารถกำหนดไว้ว่าธุรกรรมนั้นเกี่ยวข้องกับที่ทำการงานแห่งใดมากที่สุด ให้ถือเอาสำนักงานใหญ่เป็นสถานที่ที่ได้รับหรือส่งข้อมูลอิเล็กทรอนิกส์นั้น

ในกรณีดังกล่าวข้างต้น ไม่ว่าผู้ประกอบการค้าของไทยจะทำการส่งหรือได้รับข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่ายในขณะที่ตนพักอยู่ที่ประเทศใด ก็จะถือว่าผู้ประกอบการค้าของไทยนั้นทำการส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์ในสถานที่ที่ทำการงานของผู้ประกอบการนั้นเอง โดยไม่คำนึงถึงสถานที่ที่ข้อมูลอิเล็กทรอนิกส์นั้นจะได้มีการส่ง หรือได้รับกันจริง ๆ

แต่ในกรณีที่มีการส่ง หรือการรับข้อมูลอิเล็กทรอนิกส์โดยผ่านอุปกรณ์อิเล็กทรอนิกส์อย่างอื่นนอกเหนือจากการใช้ระบบคอมพิวเตอร์ เช่น การส่ง หรือรับข้อมูลผ่านทางโทรเลข โทรพิมพ์ โทรสาร นั้นจะไม่ใช้บังคับกับหลักการที่ให้ถือว่าการส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์เกิดขึ้น ณ สถานที่ทำการงานของผู้ส่งข้อมูล หรือของผู้รับข้อมูล เพราะเนื่องจากเห็นได้ชัดว่าการส่งข้อมูล หรือการได้รับข้อมูลอิเล็กทรอนิกส์นั้นเกิดขึ้นที่ใด

(2) **การส่งและการรับข้อมูลอิเล็กทรอนิกส์**

ในการส่งหรือการรับข้อมูลข้อมูลอิเล็กทรอนิกส์โดยการติดต่อทางคอมพิวเตอร์ผ่านระบบเครือข่ายนั้น สามารถกระทำได้หลายวิธี เช่น

- การแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ หรือระบบอีดีไอ (Electronic Data Interchange: EDI)
- จดหมายอิเล็กทรอนิกส์ หรืออีเมล์(Electronic Mail: e-mail)
- การสนทนาโต้ตอบระหว่างบุคคล เช่น ICQ

ในกรณีที่ไม่ปรากฏที่ทำการงานของผู้ส่งข้อมูลหรือผู้รับข้อมูล ให้ถือเอาถิ่นที่อยู่ปกติเป็นสถานที่ที่ส่งหรือรับข้อมูลอิเล็กทรอนิกส์

ความในมาตรานี้มิให้ใช้บังคับกับการส่งและการรับข้อมูลอิเล็กทรอนิกส์โดยวิธีการทางโทรเลข และโทรพิมพ์ หรือวิธีการสื่อสารอื่นตามที่กำหนดในพระราชกฤษฎีกา"

- การสนทนาโต้ตอบระหว่างกลุ่มบุคคลบนเครือข่าย เช่น Chat/IRC

และเนื่องจากวิธีการส่งและการรับข้อมูลอิเล็กทรอนิกส์ที่กล่าวมาข้างต้นนั้นมีกระบวนการทางเทคโนโลยีที่สลับซับซ้อน กว่าที่ข้อมูลอิเล็กทรอนิกส์จะไปถึงผู้รับปลายทาง เพราะอาจต้องใช้อุปกรณ์อิเล็กทรอนิกส์อื่นประกอบด้วย เช่น MODEM หรือต้องผ่านสื่อกลางหรือผู้ให้บริการอีกหลายแห่ง ดังตัวอย่างกระบวนการรับและส่งข้อมูลอิเล็กทรอนิกส์โดยใช้จดหมายอิเล็กทรอนิกส์ หรือ e-mail มีขั้นตอนดังนี้

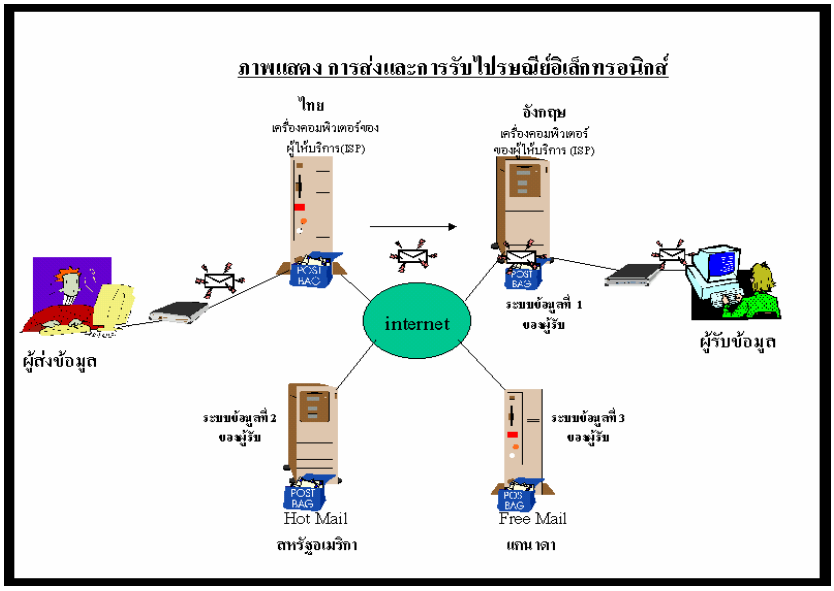
1. ผู้ส่งข้อมูลคลิกปุ่ม send เพื่อทำการส่งข้อมูลอิเล็กทรอนิกส์ไปยังผู้รับข้อมูล
2. ข้อมูลอิเล็กทรอนิกส์ดังกล่าวจะถูกส่งไปยังเครื่องคอมพิวเตอร์ของ ISP ของผู้ส่ง โดยผ่าน MODEM
3. เครื่องคอมพิวเตอร์ของ ISP ดังกล่าวจะส่งข้อมูลอิเล็กทรอนิกส์ไปยังเครื่องคอมพิวเตอร์ของ ISP ของผู้รับ โดยผ่านเครือข่ายอินเทอร์เน็ต
4. ข้อมูลอิเล็กทรอนิกส์ดังกล่าวจะถูกเก็บไว้ที่เครื่องคอมพิวเตอร์ของ ISP ของผู้รับจนกว่าผู้รับข้อมูลจะเรียกดูหรือเปิดอ่าน

ตัวอย่างดังกล่าวเป็นเพียงกระบวนการส่งและรับข้อมูลอิเล็กทรอนิกส์อย่างง่ายที่ไม่มีความสลับซับซ้อนมากนัก เพราะผู้รับข้อมูลมี e-mail address หรือ Mail box เพียงแห่งเดียว หรือเทียบได้กับบุคคลที่มีที่อยู่ซึ่งเป็นภูมิลำเนาเพียงแห่งเดียว

ทั้งนี้ การส่งข้อมูลอิเล็กทรอนิกส์ทาง e-mail ไปยังผู้รับปลายทางนั้นอาจมีความสลับซับซ้อนมากกว่าตัวอย่างข้างต้น เพราะนอกจากจะต้องผ่านเครื่องคอมพิวเตอร์ของผู้ให้บริการอินเทอร์เน็ต (ISP) แล้ว อาจจะต้องผ่านระบบข้อมูลของผู้ให้บริการ e-mail อื่นๆ ด้วย ดังนั้น เพื่อป้องกันกรณีที่ผู้รับข้อมูลมี e-mail

address หรือ Mail box หลายแห่ง หรือกรณีที่ e-mail ไม่ถึงผู้รับปลายทางโดยที่ผู้ส่งข้อมูลไม่ทราบ จึงได้มีการแก้ไขปัญหาดังกล่าวโดยอาจมีการตกลงกันระหว่างผู้รับข้อมูลกับผู้ส่งข้อมูลว่าจะให้ผู้ส่งข้อมูลส่งข้อมูลไปยังระบบข้อมูลใดของผู้รับข้อมูล หรือให้ผู้รับข้อมูลตอบแจ้งการรับไปยังผู้ส่งข้อมูลเมื่อตนได้รับข้อมูลแล้ว ซึ่งได้มีการกำหนดหลักเกณฑ์ดังกล่าวไว้ในกฎหมายด้วย

อนึ่ง หากเปรียบเทียบกับการส่งจดหมายตามปกติแล้วก็เป็นกรณีผู้รับข้อมูลมีบ้านหรือที่อยู่หลายแห่ง ซึ่งอาจมีการตกลงไว้ล่วงหน้าว่าให้ผู้ส่งจะส่งจดหมายมาที่บ้านหลังไหน หรือตกลงกันว่าหากผู้รับได้รับจดหมายแล้วให้ตอบแจ้งการรับกลับมายังผู้ส่งด้วย



1.2 ความหมายของธุรกรรมทางอิเล็กทรอนิกส์

การทำธุรกรรมทางอิเล็กทรอนิกส์ หมายถึง ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมด หรือแต่บางส่วน โดยอาจจะกระทำผ่านทางเครือข่าย

อินเทอร์เน็ต หรือด้วยวิธีการทางอิเล็กทรอนิกส์อื่น ๆ อาทิ โทรเลข โทรพิมพ์ หรือโทรสารก็ได้

ตัวอย่างของ การทำธุรกรรมทางอิเล็กทรอนิกส์ เช่น การสั่งซื้อหรือขายสินค้าทางเครือข่ายอินเทอร์เน็ต การชำระเงินผ่านทางเครือข่าย เช่น การสั่งซื้อผ่านเว็บไซต์ โดยการใช้เลขที่บัตรเครดิตในการชำระราคาสินค้าเหล่านั้น

ภาพแสดงตัวอย่างการให้บริการในรูปแบบต่าง ๆ บนเครือข่ายอินเทอร์เน็ต

ด้วยความสะดวก และรวดเร็วของการติดต่อสื่อสารด้วยวิธีการทางอิเล็กทรอนิกส์ ประกอบกับราคาอุปกรณ์ต่าง ๆ ที่เริ่มมีราคาถูกลงกว่าเดิมทำให้ปัจจุบันเริ่มมีการใช้เครือข่ายอินเทอร์เน็ต หรือเครือข่ายอื่น ๆ กันอย่างแพร่หลาย รวมทั้งมีการทำธุรกรรมทางอิเล็กทรอนิกส์มากขึ้น ทั้งนี้คำว่า “ธุรกรรมทางอิเล็กทรอนิกส์” ตามพระราชบัญญัติฉบับนี้ เป็นคำที่มีความหมายกว้าง กล่าวคือนอกจากหมายถึง กิจกรรมในทางแพ่งและพาณิชย์แล้ว ยังรวมถึงการดำเนินงานของรัฐด้วย โดยอาจแบ่งประเภทของธุรกรรมทางอิเล็กทรอนิกส์ได้ดังต่อไปนี้

1.3 การทำธุรกรรมทางอิเล็กทรอนิกส์ในเชิงพาณิชย์

การทำธุรกรรมทางอิเล็กทรอนิกส์ในส่วนของการกระทำที่เป็นการพาณิชย์ หรือที่เรียกว่าเป็นการพาณิชย์อิเล็กทรอนิกส์นั้น หมายความถึงการทำการพาณิชย์ที่อาศัยระบบอิเล็กทรอนิกส์เป็นสื่อกลางในการดำเนินการ

การพาณิชย์อิเล็กทรอนิกส์ หรือ E-Commerce มีรูปแบบตามลักษณะของคู่กรณีในธุรกรรมที่เกิดขึ้นดังนี้ [22]

ระหว่างธุรกิจกับธุรกิจ (Business to Business: B2B)

เป็นการดำเนินการพาณิชย์อิเล็กทรอนิกส์ ระหว่างองค์กรที่ทำการค้าร่วมกัน อาจจะเป็นการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลทางการค้าระหว่างกัน เช่นการแลกเปลี่ยนข้อมูลทางการค้าระหว่างสถาบันการเงิน หรือระหว่างธนาคาร หรืออาจจะเป็นการค้าขายสินค้าในปริมาณมาก ๆ เป็นต้น

ระหว่างธุรกิจกับผู้บริโภค (Business to Consumer: B2C)

เป็นรูปแบบการดำเนินการพาณิชย์อิเล็กทรอนิกส์ ระหว่างผู้ประกอบการทางธุรกิจกับบุคคลที่เป็นผู้บริโภครายย่อย อย่างเช่นการสั่งซื้อหนังสือ เทปเพลง หรือสินค้าที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ (Digitized Goods) ผ่านทางระบบเครือข่ายอินเทอร์เน็ต เป็นต้น

ระหว่างธุรกิจกับภาครัฐบาล (Business to Government: B2

เป็นรูปแบบการดำเนินการพาณิชย์อิเล็กทรอนิกส์ระหว่างเอกชนที่ประกอบธุรกิจ กับหน่วยงานภาครัฐบาล

---

[22] ยืน ภู่สุวรรณ, บนเส้นทางพาณิชย์อิเล็กทรอนิกส์, (กรุงเทพฯ : ซีเอ็ดยูเคชั่น,2543), หน้า 33

1.4 การทำธุรกรรมทางอิเล็กทรอนิกส์เกี่ยวกับการบริการของภาครัฐ[23]

ในปัจจุบันหน่วยงานภาครัฐได้นำเทคโนโลยีสารสนเทศเข้ามาช่วยพัฒนาการดำเนินการ และเพิ่มความสะดวกสบายในการบริการทางด้านต่าง ๆ แก่ประชาชน โดยเฉพาะอย่างยิ่งการให้บริการทางอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ เพื่อนำไปสู่เป้าหมายสำคัญของการเป็นรัฐบาลอิเล็กทรอนิกส์ หรือ e-government ในอนาคตต่อไป ซึ่งการให้บริการของหน่วยงานของรัฐผ่านสื่ออิเล็กทรอนิกส์ในรูปแบบต่าง ๆ ที่มีอยู่ในปัจจุบัน หาอ่านรายละเอียดได้จากภาคผนวก

1.5 หลักการสำคัญของพระราชบัญญัติฯ ที่รองรับการทำธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้วางหลักการสำคัญเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ไว้ในหมวดที่ 1 ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ โดยในหมวดนี้ได้บัญญัติขึ้นตามแนวทางของกฎหมายแม่แบบว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ (Model Law on Electronic Commerce 1996) ของคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติ (United Nations Commission on International Trade Law : UNCITRAL)

---

[23] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, แบบสำรวจแนวทางการจัดทำแผนปฏิบัติการ e-Government, และเอกสารแนะนำโครงการที่ได้รับรางวัล "โครงการเทคโนโลยีสารสนเทศภาครัฐดีเด่น" ครั้งที่ 1 พ.ศ. 2543,

ทั้งนี้ สาระสำคัญของบทบัญญัติในหมวดนี้ คือ การรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ เพื่อให้การดำเนินการใด ๆ ตามที่กฎหมายบัญญัติสามารถทำในรูปของข้อมูลอิเล็กทรอนิกส์ได้และมีผลผูกพันตามกฎหมาย โดยมีรายละเอียดที่สำคัญ ดังนี้

1.5.1 การรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ (มาตรา 7)[24]

พระราชบัญญัติฉบับนี้ได้รับรองสถานะหรือผลทางกฎหมายของข้อความที่ทำให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้มีการปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายไว้ใน มาตรา 7 ซึ่งมาตรานี้นับเป็นมาตราที่สำคัญที่สุดของพระราชบัญญัติ โดยเป็นการกำหนดหลักการพื้นฐานมิให้มีการเลือกปฏิบัติระหว่างสิ่งที่จัดทำขึ้นในรูปของกระดาษทั้งในรูปของหนังสือ หลักฐานเป็นหนังสือ หรือต้นฉบับ (Original) กับสิ่งที่จัดทำขึ้นในรูปของข้อมูลอิเล็กทรอนิกส์

อย่างไรก็ตาม แม้บทบัญญัติตามมาตรา 7 จะกำหนดเป็นหลักพื้นฐานในการรับรองผลหรือสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ แต่ความสมบูรณ์ทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ตามมาตรานี้ บัญญัติขึ้นเพื่อมิให้มีการปฏิเสธผลทางกฎหมายเท่านั้น ไม่ได้หมายความว่าจะเป็นการรับรองความถูกต้องสมบูรณ์ของข้อความที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้นแต่อย่างใด

ทั้งนี้ โดยบทบัญญัติตามมาตรา 7 เป็นเพียงมาตราหลักทั่วไปซึ่งปรับใช้ได้กับข้อความทุกชนิดที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ แต่หากต้องการทำข้อมูล

---

[24] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Commerce 1996, Singapore Electronic Transactions Act 1998, Philippines Electronic Commerce Act 2000 , India Information Technology Act 2000 หรือ South Korea Basic Law on Electronic Commerce เป็นต้น

อิเล็กทรอนิกส์ให้อยู่ในรูปของหนังสือ หลักฐานเป็นหนังสือ ลงลายมือชื่อ การเก็บรักษาเอกสาร หรือเพื่อประโยชน์อื่นใดตามที่กฎหมายกำหนด จะต้องเป็นไปตามข้อกำหนดตามที่กฎหมายบัญญัติไว้ในมาตราต่าง ๆ ดังจะได้กล่าวในรายละเอียดต่อไป

1.5.2 การทำเป็นหนังสือ (มาตรา 8)[25]

หลักเกณฑ์ในมาตรานี้บัญญัติขึ้นเพื่อขยายหลักการทั่วไปของมาตรา 7 โดยเน้นในรายละเอียดถึงเงื่อนไขในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือหรือมีเอกสารมาแสดง เช่น ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 653 ซึ่งกำหนดว่าการกู้ยืมเงินเกินกว่า 50 บาทขึ้นไปจะฟ้องร้องบังคับคดีได้ต้องมีหลักฐานเป็นหนังสือ ดังนั้นคำว่า “หลักฐานเป็นหนังสือ” ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 653 ก็สามารถทำในรูปของข้อมูลอิเล็กทรอนิกส์ได้เมื่อกฎหมายฉบับนี้มีผลใช้บังคับ

อย่างไรก็ตาม แม้จะมีบทบัญญัติในมาตรา 7 รับรองสถานะของข้อมูลอิเล็กทรอนิกส์ไว้อยู่แล้วก็ตาม แต่หากในกรณีที่ต้องมีการจัดทำหนังสือ หลักฐานเป็นหนังสือ หรือเอกสารให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ดังเช่นกรณีของประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 653 ที่ยกมาข้างต้นนั้น การจะทำให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์จะต้องอยู่ภายใต้เงื่อนไขของมาตรา 8 ด้วยว่า เมื่อได้มีการจัดทำหนังสือ หลักฐานเป็นหนังสือ หรือเอกสารให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ข้อมูลอิเล็กทรอนิกส์นั้นจะต้องสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง

---

[25] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Commerce 1996, Singapore Electronic Transactions Act 1998 หรือ Hong Kong Electronic Transaction Ordinance เป็นต้น

อย่างไรก็ตาม หลักการของบทบัญญัติข้างต้นที่กำหนดให้ต้องสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลงนั้น คำว่า "สามารถเข้าถึงได้" หมายความรวมถึงข้อความ (Information) ที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ที่สามารถอ่านออกและอธิบายได้ (Readable and interpretable) โดยการใช้โปรแกรมหรือซอฟต์แวร์ (Software) และรวมถึงข้อมูลอิเล็กทรอนิกส์ที่จำเป็นต้องแปลงข้อมูลนั้นให้สามารถอ่านเข้าใจได้ด้วย (Such information readable)[26]

นอกจากนั้น คำว่า "นำกลับมาใช้ได้" (Usable) นั้น มิได้ครอบคลุมเฉพาะมนุษย์เท่านั้นที่ใช้ได้ แต่ยังหมายความรวมถึงการใช้โดยการประมวลผลด้วยเครื่องคอมพิวเตอร์ด้วย (Computer Processing) ส่วนความหมายของคำว่า "ความหมายไม่เปลี่ยนแปลง" นั้นต้องมีลักษณะถาวร ไม่มีการแก้ไขเปลี่ยนแปลง กล่าวคือข้อมูลนั้นต้องไม่ได้สร้างขึ้นโดยใช้มาตรฐานที่ต่ำเกินไป และข้อมูลอิเล็กทรอนิกส์นั้นต้องสามารถอ่านและเข้าใจได้ (Readability or intelligibility)

ทั้งนี้ เหตุที่ต้องกำหนดเงื่อนไขในการเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง เนื่องจากอาจมีการใช้เทคโนโลยีที่สร้างข้อมูลอิเล็กทรอนิกส์นั้น แตกต่างไปจากเทคโนโลยีที่ใช้เมื่อมีการอ่านหรือใช้ข้อมูลอิเล็กทรอนิกส์ในภายหลัง และกรณีอาจมีความเป็นไปได้ว่าเมื่อมีการใช้เทคโนโลยีที่แตกต่างกัน ก็อาจทำให้ไม่สามารถอ่านหรือแปลงข้อความที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ที่สร้างขึ้นโดยเทคโนโลยีแตกต่างกันนั้นได้

---

[26] UNCITRAL Model Law on Electronic Commerce 1996, paras.47-52 และ 62-69 และ 72 - 75 ตามลำดับ

1.5.3 ลายมือชื่อ (มาตรา 9)[27]

มาตรานี้บัญญัติขึ้นเพื่อรับรองสถานะทางกฎหมายของลายมือชื่อในข้อมูลอิเล็กทรอนิกส์เพื่อระบุหรือยืนยันตัวบุคคล เป็นอีกมาตราที่ขยายเงื่อนไขในรายละเอียดเพิ่มเติมจากการรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ตามที่บัญญัติไว้ในมาตรา 7 โดยมาตรา 8 นี้ วางหลักการในการรับรองการใช้ลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ให้มีผลเช่นเดียวกับที่กำหนดไว้ในระบบกระดาษ กล่าวคือ โดยส่วนใหญ่เมื่อมีการใช้ “ลายมือชื่อ” จะใช้เพื่อวัตถุประสงค์ในการยืนยันตัวบุคคล และกำหนดความผูกพันของบุคคลผู้ลงลายมือชื่อนั้น โดยอาจแตกต่างกันไปขึ้นอยู่กับเอกสารที่จะลงลายมือชื่อนั้น เช่น การลงลายมือชื่อในฐานะคู่สัญญา หรือการลงลายมือชื่อสลักหลังตราสารทางการเงิน เป็นต้น

อย่างไรก็ตาม บทบัญญัติในมาตรา 9 นี้เป็นบทบัญญัติที่กำหนดขึ้นบนพื้นฐานของหลักความเท่าเทียมกันระหว่าง “ลายมือชื่อหรือลายเซ็นบนกระดาษ” กับ “ลายมือชื่อที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์” และเนื่องจากวิธีการทางเทคโนโลยีที่นำมาใช้ในการลงลายมือชื่อข้อความที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์อาจมีความแตกต่างกันไป ขึ้นอยู่กับความประสงค์ของคู่กรณีที่ใช้ลายมือชื่อนั้นว่าประสงค์จะใช้ลายมือชื่อที่สร้างหรือกำหนดขึ้นมาแบบง่าย ๆ หรือต้องการใช้ลายมือชื่อที่สร้างขึ้นด้วยวิธีการทางเทคโนโลยีที่สลับซับซ้อนดังนั้น บทบัญญัติในมาตรานี้จึงมิได้บัญญัติรองรับเทคโนโลยีใดเทคโนโลยีหนึ่งโดยเฉพาะ แต่เปิดกว้างให้สามารถรองรับลายมือชื่อที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ได้ทุกรูปแบบ ทั้งนี้ โดยกำหนดหลักการไว้ดังนี้

“ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

---

[27] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Commerce 1996, Singapore Electronic Transactions Act 1998 หรือ Australia Electronic Transaction Act 1999 เป็นต้น

(1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(2) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี"

บทบัญญัติดังกล่าวมิได้มีการบัญญัติถึงเทคโนโลยีที่สามารถนำมาใช้ในการลงลายมือชื่อไว้ว่าหมายถึงเทคโนโลยีใดบ้าง ซึ่งหมายความว่าผู้ลงลายมือชื่อสามารถใช้วิธีการใดก็ได้เพียงแต่วิธีการดังกล่าวควรเป็นวิธีการที่เชื่อถือได้ ทั้งนี้ เหตุที่กฎหมายได้มีการกำหนดเกี่ยวกับวิธีการที่น่าเชื่อถือไว้ ก็เพื่อความปลอดภัยหรือความน่าเชื่อถือในการใช้วิธีการระบุหรือยืนยันตัวบุคคล ซึ่งตัวอย่างพฤติการณ์ที่อาจใช้เป็นแนวทางในการพิจารณาความน่าเชื่อถือไว้ อาทิ ประสิทธิภาพหรือความซับซ้อนของเครื่องมือหรืออุปกรณ์ที่ใช้ ลักษณะของกิจกรรมทางการค้า ความสม่ำเสมอในการทำการค้าของคู่กรณี ประเภทและขนาดของธุรกรรม กฎเกณฑ์ทางกฎหมายที่กำหนดให้มีการลงลายมือชื่อ ศักยภาพของระบบการติดต่อสื่อสาร การปฏิบัติตามขั้นตอนในการสร้างลายมือชื่อ จารีตประเพณีทางการค้า ความสำคัญและประโยชน์ในเชิงเศรษฐกิจของข้อมูลอิเล็กทรอนิกส์ ทางเลือกอื่นในการสร้างหรือลงลายมือชื่อ และต้นทุนที่เกิดขึ้น ความเป็นไปได้ในการยอมรับหรือไม่ยอมรับวิธีการในการระบุตัวบุคคล ณ ขณะที่มีการตกลงให้ใช้วิธีการนั้น หรือ ณ ขณะที่มีการติดต่อสื่อสารกัน รวมทั้งปัจจัยอื่นที่เกี่ยวข้อง [28]

1.5.4 ต้นฉบับ (มาตรา 10) [29]

---

[28] UNCITRAL Model Law on Electronic Commerce 1996, para.58

[29] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Commerce 1996, Philippines Electronic Commerce Act 2000 หรือ Hong Kong Electronic Transaction Ordinance เป็นต้น

บทบัญญัติตามมาตรานี้ เป็นการเพิ่มเติมรายละเอียดเกี่ยวกับกรณีที่กฎหมายกำหนดให้เสนอหรือเก็บรักษาเอกสารหรือข้อความในรูปของเอกสารต้นฉบับ ซึ่งหากได้มีการจัดเก็บเอกสารต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ โดยมีการดำเนินการตามเงื่อนไขที่กำหนดในกฎหมาย คือ ได้มีการใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ สามารถแสดงข้อความนั้นได้ในภายหลัง กฎหมายจึงบัญญัติรับรองให้สามารถจัดเก็บต้นฉบับดังกล่าวให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ได้

ทั้งนี้ ในการพิจารณาถึงความถูกต้องของข้อความตามที่กฎหมายกำหนดนั้น ให้พิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงใดของข้อความ เว้นแต่การรับรองหรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใดๆ ที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร โดยปกติในการติดต่อสื่อสารด้วยวิธีทางอิเล็กทรอนิกส์นั้นมักมีการเพิ่มเติมข้อมูลในส่วนต้นหรือส่วนท้ายของต้นฉบับแต่ละหน้าซึ่งอยู่ในรูปข้อมูลอิเล็กทรอนิกส์ เช่น หากเปรียบเทียบกับระบบกระดาษข้อความนั้นอาจจะอยู่ในส่วนหัวกระดาษหรือท้ายกระดาษ (Header or Footer) โดยมักเป็นข้อมูลเกี่ยวกับเวลาที่เริ่มมีการสร้าง ส่ง หรือเวลาที่ได้รับข้อมูลอิเล็กทรอนิกส์นั้น ซึ่งไม่มีผลกระทบต่อความสมบูรณ์ของต้นฉบับที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์แต่อย่างใด

อย่างไรก็ตาม สำหรับการนำเสนอหรือการจัดเก็บเอกสารต้นฉบับที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ บทบัญญัติตามมาตรานี้กำหนดให้ต้องใช้วิธีการที่เชื่อถือได้โดยพิเคราะห์จากพฤติการณ์ทั้งปวง รวมทั้งวัตถุประสงค์ของการสร้างข้อมูลอิเล็กทรอนิกส์นั้นด้วย

1.5.5 การรับฟังพยานหลักฐานและชั่งน้ำหนักพยานหลักฐาน (มาตรา 1 1)[30]

บทบัญญัติตามมาตรา 1 1 ได้กำหนดห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุที่ข้อมูลนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ทั้งนี้เพราะปัจจุบันหลักเกณฑ์การรับฟังพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้น นอกเหนือจากศาลชำนัญพิเศษต่าง ๆ ที่มีข้อกำหนดของตนเองแล้ว ศาลอื่น ๆ เป็นดุลพินิจของศาลที่จะรับฟังหรือไม่ก็ได้ เพราะมิได้มีหลักเกณฑ์บัญญัติไว้โดยชัดแจ้งว่าต้องรับฟัง แต่เมื่อบัญญัติให้ต้องรับฟังแล้วมิได้หมายความว่าพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ทุกชิ้นจะต้องมีน้ำหนักน่าเชื่อเสมอไป ดังนั้นมาตรานี้จึงได้กำหนดหลักเกณฑ์เกี่ยวกับการชั่งน้ำหนักพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ว่าจะเชื่อถือได้หรือไม่ เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษาหรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการที่ใช้ในการระบุตัวผู้ส่ง รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง ซึ่งหลักเกณฑ์ในมาตรานี้กำหนดไว้กว้าง ๆ ให้รับฟังพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ได้ แต่ไม่ได้กำหนดว่าให้รับฟังได้ในรูปพยานหลักฐานประเภทใด[31] หรือวิธีการใด ดังนั้นจึงอาจจำเป็นที่จะต้องกำหนดเป็นรายละเอียดเพิ่มเติมในภายหลัง

ปัจจุบันในการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์นั้น ศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศกลาง และศาลล้มละลายกลางได้ออกข้อกำหนดเกี่ยวกับการรับฟังพยานหลักฐานที่เป็นข้อมูล

---

[30] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Commerce 1996, South Korea Basic Law on Electronic Commerce หรือ Hong Kong Electronic Transaction Ordinance เป็นต้น

[31] UNCITRAL Model Law on Electronic Commerce 1996 , paras.70-71

อิเล็กทรอนิกส์เพื่อใช้การพิจารณารับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ของศาล โดยกำหนดไว้ดังนี้

- **ข้อกำหนดคดีทรัพย์สินทางปัญญา และการค้าระหว่างประเทศ พ.ศ. 2540 ของศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ**[32]

ข้อ 33 ศาลอาจรับฟังข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์เป็นพยานหลักฐานในคดีได้ หาก

(1) การบันทึกข้อมูลโดยเครื่องคอมพิวเตอร์ หรือการประมวลโดยเครื่องคอมพิวเตอร์เป็นการกระทำตามปกติในการประกอบกิจการของผู้ใช้เครื่องคอมพิวเตอร์ และ

(2) การบันทึกและการประมวลผลข้อมูลเกิดจากการใช้เครื่องคอมพิวเตอร์ปฏิบัติงานตามขั้นตอนการทำงานของเครื่องคอมพิวเตอร์อย่างถูกต้อง และหากมีกรณีการทำงานของเครื่องคอมพิวเตอร์ขัดข้องก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

การกระทำตามปกติของผู้ใช้ตาม (1) และความถูกต้องของการบันทึกและการประมวลผลข้อมูลตาม (2) ต้องมีการรับรองของบุคคลที่เกี่ยวข้องหรือดำเนินการนั้น

- **ข้อกำหนดศาลล้มละลาย พ.ศ. 2542**[33]

ข้อ 18 ศาลอาจรับฟังข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์เป็นพยานหลักฐานในคดีได้ หาก

---

[32] โปรดดูข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ. 2540

[33] โปรดดูข้อกำหนดคดีล้มละลาย พ.ศ. 2542 ออกตามความมาตรา 19 แห่งพระราชบัญญัติจัดตั้งศาลล้มละลายและวิธีพิจารณาคดีล้มละลาย พ.ศ. 2542

(1) การบันทึกข้อมูลโดยเครื่องคอมพิวเตอร์ หรือการประมวลโดยเครื่องคอมพิวเตอร์เป็นการกระทำตามปกติในการประกอบกิจการของผู้ใช้เครื่องคอมพิวเตอร์ และ

(2) การบันทึกและการประมวลผลข้อมูลเกิดจากการใช้เครื่องคอมพิวเตอร์ปฏิบัติงานตามขั้นตอนการทำงานของเครื่องคอมพิวเตอร์อย่างถูกต้อง และหากมีกรณีการทำงานของเครื่องคอมพิวเตอร์ขัดข้องก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

การกระทำตามปกติของผู้ใช้ตาม (1) และความถูกต้องของการบันทึกและการประมวลผลข้อมูลตาม (2) ต้องมีการรับรองของบุคคลที่เกี่ยวข้องหรือดำเนินการนั้น

1.5.6 การเก็บรักษาเอกสารหรือข้อความ (มาตรา 12)[34]

มาตรานี้กำหนดให้สามารถเก็บรักษาเอกสารหรือข้อความในรูปของข้อมูลอิเล็กทรอนิกส์ได้ โดยกำหนดเงื่อนไขในทำนองเดียวกันกล่าวคือ ต้องสามารถเข้าถึงข้อมูลอิเล็กทรอนิกส์นั้น และนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง รวมทั้งได้เก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้น ให้อยู่ในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์นั้น หรืออยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับให้ปรากฏอย่างถูกต้องได้

---

[34] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Commerce 1996, Singapore Electronic Transactions Act 1998, India Information Technology Act 2000 หรือ South Korea Basic Law on Electronic Commerce หรือ Hong Kong Electronic Transaction Ordinance เป็นต้น

หลักเกณฑ์เกี่ยวกับการเก็บรักษาข้อมูลอิเล็กทรอนิกส์ตามมาตรานี้ กำหนดให้ข้อความหรือเนื้อหาที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้น ต้องตรงกับข้อความหรือเนื้อหาของเอกสารก่อนการจัดเก็บให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ แม้ว่าในการแปลงข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ จะทำให้ข้อความหรือรูปแบบของเนื้อหาที่ปรากฏในภายหลังจะแตกต่างกันไปบ้าง เช่น ระยะหรือย่อหน้าบรรทัดคลาดเคลื่อนไปจากเดิมบ้างก็ตาม เนื่องจากการเข้ารหัสและถอดรหัส (Encode and Decode) เพื่อแปลงเป็นภาษามาตรฐานด้วยวิธีการทางอิเล็กทรอนิกส์ การถูกบีบอัด (Compressed) ให้มีขนาดเล็กลงเพื่อให้ง่ายและสะดวกในการจัดเก็บและการเพิ่มเนื้อที่ในการจัดเก็บ หรือแปลง (Converted) ข้อมูลอิเล็กทรอนิกส์นั้น [35]

อย่างไรก็ตาม หลักเกณฑ์ตามมาตรานี้จะเอื้อประโยชน์ต่อการเก็บรักษาเอกสาร เช่น ประมวลรัษฎากร มาตรา 87/3 กำหนดให้สถานประกอบการจัดเก็บเอกสารเกี่ยวกับใบกำกับภาษีและเอกสารที่เกี่ยวข้องไว้เป็นเวลาไม่น้อยกว่า 5 ปี หรือการกำหนดให้กระทรวงการคลังเก็บรักษาเอกสารเกี่ยวกับบัญชีและอื่นๆ ที่เกี่ยวข้องของสถาบันการเงินที่ยกเลิกเป็นเวลา 10 ปี ทั้งนี้ ตามมาตรา 43 ของพระราชกำหนดการปฏิรูประบบสถาบันการเงิน พ.ศ. 2540 ดังนั้น จากการเก็บรักษาเอกสารในรูปแบบเดิมซึ่งมักจัดเก็บอยู่ในรูปของกระดาษ ก็อาจจัดเก็บอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ได้ด้วยโดยมีกฎหมายนี้รองรับ

---

[35] UNCITRAL Model Law on Electronic Commerce 1996, paras.47-52 และ 62-69 และ 72-75 ตามลำดับ

1.5.7 สัญญาและเจตนาในรูปของข้อมูลอิเล็กทรอนิกส์ (มาตรา 13 และมาตรา 14)[36]

มาตรา 13 และมาตรา 14 ของพระราชบัญญัตินี้ ได้บัญญัติหลักเกณฑ์เกี่ยวกับการแสดงเจตนา และการทำสัญญาว่าจะไม่ถูกปฏิเสธผลทางกฎหมายแม้กระทำขึ้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ โดยบทบัญญัติตามมาตรานี้ได้คำนึงถึงหลักความศักดิ์สิทธิ์ในการแสดงเจตนา ดังนั้นคู่สัญญาจึงสามารถตกลงเป็นอย่างอื่นได้ กล่าวคือคู่สัญญาอาจตกลงกันว่าในกรณีที่สัญญาซื้อขายมีมูลค่าสูง จะต้องทำสัญญากันในรูปของกระดาษเท่านั้นก็ได้

ทั้งนี้ แม้บทบัญญัติตามมาตรา 7 ของกฎหมายฉบับนี้จะได้รับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ไว้แล้วก็ตาม แต่บทบัญญัติมาตรา 13 ก็ได้กำหนดขึ้นเพื่อสร้างความแน่นอนของผลทางกฎหมาย โดยเฉพาะอย่างยิ่งในกรณีที่มีการตั้งโปรแกรมให้เครื่องคอมพิวเตอร์ทำงานโดยอัตโนมัติในการทำคำเสนอและคำสนอง โดยไม่มีการแทรกแซงของมนุษย์เลย ส่วนบทบัญญัติมาตรา 14 เพิ่มเติมในภายหลังเพื่อให้ครอบคลุมการแสดงเจตนาฝ่ายเดียว เช่น การแจ้งความชำรุดบกพร่องของสินค้า การขอเสนอชำระราคา หรือการยอมรับสภาพหนี้ เป็นต้น

อย่างไรก็ตาม นอกจากมาตรา 13 จะใช้ได้กับการทำคำเสนอและคำสนองที่สร้าง ส่ง หรือรับทางอิเล็กทรอนิกส์แล้ว ยังใช้ได้กับกรณีที่มีการทำแต่เพียงคำเสนอหรือคำสนองอย่างหนึ่งอย่างใดทางอิเล็กทรอนิกส์เท่านั้นด้วย และแม้ว่ากฎหมายจะกำหนดเกี่ยวกับการทำคำเสนอ และคำสนองเอาไว้แต่ก็ไม่ได้กำหนดเกี่ยวกับเวลาและ

---

[36] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Commerce 1996, Singapore Electronic Transactions Act 1998, Philippines Electronic Commerce Act 2000 , Hong Kong Electronic Transaction Ordinance หรือ Brunei Electronic Transaction Order 2000 เป็นต้น

สถานที่ในการเกิดขึ้นของสัญญาเอาไว้ เนื่องจากไม่ต้องการไปแทรกแซงกฎหมายภายในว่าด้วยสัญญา อย่างไรก็ตาม เพื่อขจัดความไม่แน่นอนของการเกิดขึ้นของสัญญา ในกรณีที่มีการทำคำเสนอ คำสนอง ทางอิเล็กทรอนิกส์ จึงต้องพิจารณากฎหมายที่ใช้บังคับในปัจจุบันประกอบกับบทบัญญัติในมาตรา 22 – มาตรา 24 ว่าด้วยเวลาและสถานที่ในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์ [37]

1.5.8 บทสันนิษฐานเจ้าของข้อมูลอิเล็กทรอนิกส์ (มาตรา 15 – มาตรา 18)[38]

มาตรา 15 – มาตรา 18 ตามพระราชบัญญัติฉบับนี้ เป็นบทบัญญัติที่เป็นบทสันนิษฐานเกี่ยวกับเจ้าของข้อมูลอิเล็กทรอนิกส์ ซึ่งเมื่อพิจารณาโดยรวมแล้ว สามารถแบ่งออกได้เป็นกรณีต่าง ๆ ดังนี้

(ก) ข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูล หากผู้ส่งข้อมูลได้ส่งข้อมูลอิเล็กทรอนิกส์นั้นด้วยตนเอง (มาตรา 15 วรรคหนึ่ง)

(ข) ให้ถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูล หากข้อมูลอิเล็กทรอนิกส์นั้นได้ส่งโดยบุคคลผู้มีอำนาจกระทำแทนผู้ส่งข้อมูลเกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น (มาตรา 15 (1))

(ค) ให้ถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูล หากข้อมูลอิเล็กทรอนิกส์นั้นส่งโดยระบบข้อมูลที่ผู้ส่งข้อมูลหรือบุคคลผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูลได้กำหนดไว้ล่วงหน้าให้สามารถทำงานได้โดยอัตโนมัติ (มาตรา 15 (2)

---

[37] UNCITRAL Model Law on Electronic Commerce 1996, para.78

[38] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Commerce 1996, Singapore Electronic Transactions Act 1998, Philippines Electronic Commerce Act 2000 , India Information Technology Act 2000 , South Korea Basic Law on Electronic Commerce , Hong Kong Electronic Transaction Ordinance หรือ Brunei Electronic Transaction Order 2000 เป็นต้น

(ง) ในกรณีที่ผู้รับข้อมูลและผู้ส่งข้อมูลได้ตกลงวิธีการดำเนินการใดในการตรวจสอบตัวบุคคลไว้ด้วย เช่น การพิสูจน์ลายมือชื่อ และผู้รับข้อมูลได้ดำเนินการตามขั้นตอนดังกล่าวแล้ว ให้สันนิษฐานว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นของผู้ส่งข้อมูล (มาตรา 16 (1)) และ

(จ) ข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นเกิดจากการกระทำของบุคคลซึ่งใช้วิธีการที่ผู้ส่งข้อมูลใช้ในการแสดงว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นของผู้ส่งข้อมูลซึ่งบุคคลนั้นได้ล่วงรู้โดยอาศัยความสัมพันธ์ระหว่างบุคคลนั้นกับผู้ส่งข้อมูลหรือตัวแทนของผู้ส่งข้อมูล ให้สันนิษฐานว่าข้อมูลอิเล็กทรอนิกส์ที่ส่งนั้นเป็นของผู้ส่งข้อมูลเช่นกัน (มาตรา 16 (2))

อย่างไรก็ตาม สำหรับบทบัญญัติเกี่ยวกับบทสันนิษฐานเกี่ยวกับเจ้าของข้อมูลอันหมายถึงผู้ส่งข้อมูล ซึ่งกำหนดให้ผู้รับข้อมูลต้องดำเนินการพิสูจน์ตัวบุคคลเสียก่อน นั้น กฎหมายได้เปิดโอกาสให้ผู้ส่งข้อมูลอิเล็กทรอนิกส์บอกกล่าวแก่ผู้รับข้อมูลว่าข้อมูลอิเล็กทรอนิกส์นั้นมิใช่ของตน ทั้งนี้ โดยผู้รับข้อมูลต้องมีเวลาพอสมควรที่จะดำเนินการแก้ไขตามที่จำเป็นเกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้นได้ เว้นแต่ผู้รับข้อมูลไม่มีเวลาเพียงพอที่จะดำเนินการแก้ไขเกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้นก็ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นของผู้ส่งข้อมูลแม้ว่าผู้ส่งข้อมูลจะไม่ได้ส่งข้อมูลนั้นก็ตาม ทั้งนี้ บทสันนิษฐานเกี่ยวกับผู้ส่งข้อมูลซึ่งกำหนดให้ผู้รับข้อมูลต้องดำเนินการพิสูจน์ตัวบุคคลเสียก่อน นั้น มิให้ใช้บังคับกับกรณีที่ผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์นั้นไม่ใช่ของผู้ส่งข้อมูล หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควรหรือดำเนินการตามขั้นตอนที่ได้ตกลงไว้

อย่างไรก็ตาม บทบัญญัตินี้ไม่ได้กำหนดขึ้นเพื่อกำหนดความรับผิดให้กับฝ่ายใดฝ่ายหนึ่ง แต่กำหนดเพื่อให้เกิดความแน่นอนในการพิจารณาว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ใดเท่านั้น ส่วนความรับผิดจะเป็นของผู้ส่งข้อมูลหรือผู้รับ

ข้อมูลนั้น ต้องพิจารณาการดำเนินการตามขั้นตอนที่กฎหมายกำหนด เช่น การพิสูจน์ตัวบุคคล ประกอบกับความประมาทเลินเล่อของฝ่ายใดฝ่ายหนึ่ง [39]

นอกจากนี้ บทบัญญัติในมาตรา 18 ยังได้กำหนดเกี่ยวกับความผิดพลาดซึ่งอาจเกิดขึ้นในขั้นตอนของการส่งข้อมูลอิเล็กทรอนิกส์ด้วย โดยกำหนดให้ผู้รับข้อมูลมีสิทธิถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับแต่ละชุดเป็นข้อมูลที่แยกจากกัน เว้นแต่ ข้อมูลอิเล็กทรอนิกส์นั้นจะซ้ำกับข้อมูลอิเล็กทรอนิกส์อีกชุดหนึ่งและผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นข้อมูลอิเล็กทรอนิกส์ซ้ำ หากผู้รับได้ใช้ความระมัดระวังตามสมควรหรือดำเนินการตามขั้นตอนที่ได้ตกลงไว้ [40]

1.5.9 การตอบแจ้งการรับ (มาตรา 19 – มาตรา 21) [41]

บทบัญญัติตามมาตรา 19 – มาตรา 21 เป็นบทบัญญัติที่เชื่อมโยงกันโดยเป็นบทบัญญัติเกี่ยวกับการตอบแจ้งการรับ ซึ่งได้กำหนดให้ใช้กับกรณีที่ผู้ส่งได้ร้องขอหรือตกลงกับผู้รับให้มีการตอบแจ้งการรับเพื่อแสดงว่าผู้รับได้รับข้อมูลอิเล็กทรอนิกส์นั้นแล้ว ทั้งนี้ โดยอาจกำหนดเงื่อนไขหรือระยะเวลาที่กำหนดให้มีการตอบแจ้งการรับว่าได้มีการรับข้อมูลอิเล็กทรอนิกส์ไว้ด้วย และหากไม่มีการดำเนินการใด ๆ ตามเงื่อนไขที่ตกลงกันไว้หรือไม่ตอบแจ้งการรับในระยะเวลาที่กำหนด ก็ให้ถือว่าไม่ได้มีการส่งข้อมูลอิเล็กทรอนิกส์นั้นเลย แต่แม้มีการตอบแจ้งการรับว่าได้รับข้อมูลอิเล็กทรอนิกส์แล้ว ก็มิได้หมายความว่าเนื้อหาของข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูล

---

[39] UNCITRAL Model Law on Electronic Commerce 1996, paras.83-92

[40] UNCITRAL Model Law on Electronic Commerce 1996, paras.83-92

[41] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Commerce 1996, Singapore Electronic Transactions Act 1998, Philippines Electronic Commerce Act 2000 , India Information Technology Act 2000 , South Korea Basic Law on Electronic Commerce หรือ Brunei Electronic Transaction Order 2000 เป็นต้น

ได้รับนั้น ถูกต้องตรงกันกับเนื้อหาของข้อมูลอิเล็กทรอนิกส์ที่ผู้ส่งข้อมูลได้ส่งแต่อย่างใดไม่

อย่างไรก็ตามบทบัญญัติเกี่ยวกับการตอบแจ้งการรับนี้คล้าย ๆ กับระบบไปรษณีย์ตอบรับ (Return receipt request) โดยการกำหนดให้ตอบแจ้งการรับอาจกำหนดไว้ในเนื้อความของข้อมูลอิเล็กทรอนิกส์นั้นเอง หรืออาจกำหนดให้เป็นการแสดงเจตนาฝ่ายเดียวหรือกำหนดเป็นสัญญาซึ่งต้องกระทำสองฝ่าย หรือกำหนดไว้ในระบบที่ใช้ในการติดต่อสื่อสารนั้น

อนึ่ง ในการทำคำเสนอในรูปของข้อมูลอิเล็กทรอนิกส์ และได้มีการกำหนดให้มีระบบการตอบแจ้งการรับเมื่อมีการส่งข้อมูลอิเล็กทรอนิกส์นั้น ก็มิได้หมายความว่าการตอบแจ้งการรับนั้น เป็นการทำคำสนองอันมีผลทำให้เกิดสัญญาขึ้นแต่อย่างใด แต่การตอบแจ้งการรับดังกล่าวเป็นแต่เพียงพยานหลักฐานว่าผู้รับข้อมูลได้รับคำเสนอแล้วเท่านั้น

กรณีที่ได้มีการกำหนดให้มีการตอบแจ้งการรับเป็นเงื่อนไขว่าให้ถือว่ามีการส่งข้อมูลอิเล็กทรอนิกส์ต่อเมื่อมีการตอบแจ้งการรับ ก็ให้ถือว่าไม่มีการส่งข้อมูลอิเล็กทรอนิกส์เลยหากไม่มีการตอบแจ้งการรับกลับไป และในกรณีที่ไม่ได้มีการกำหนดเงื่อนไขให้มีการตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ แต่มีการกำหนดระยะเวลาให้ตอบแจ้งการรับและไม่ได้มีการตอบรับในระยะเวลาที่กำหนด หรือไม่มีการกำหนดระยะเวลาในการตอบแจ้งการรับและผู้ส่งข้อมูลได้แจ้งให้ผู้รับข้อมูลตอบแจ้งการรับในระยะเวลาที่กำหนด และผู้รับข้อมูลไม่ได้ตอบแจ้งการรับในระยะเวลาที่ได้รับแจ้งให้ถือว่าไม่ได้มีการส่งข้อมูลอิเล็กทรอนิกส์เลย และมีผลให้ผู้ส่งหลุดพ้นจากความผูกพันที่เกิดขึ้นจากการส่งข้อมูลอิเล็กทรอนิกส์นั้น

นอกจากนั้น มาตรา 21 ยังได้กำหนดบทสันนิษฐานในกรณีที่การตอบแจ้งการรับอันแสดงว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้น เป็นไปตามข้อกำหนดทางเทคนิคที่ผู้ส่งข้อมูลและผู้รับข้อมูลได้ตกลงหรือที่ระบุไว้ในมาตรฐานซึ่งใช้บังคับแล้ว เช่น การแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ (EDI) ซึ่งกำหนดให้ใช้ข้อความตาม

มาตรฐานของ EDIFACT และให้ถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับถูกต้องตามกฎไวยากรณ์หรือวากยสัมพันธ์ที่เป็นไปตามมาตรฐาน EDIFACT กำหนดแล้ว [42]

1.5.10 เวลาและสถานที่ส่งและรับข้อมูลอิเล็กทรอนิกส์ (มาตรา 22 – มาตรา 24)

สืบเนื่องจากการติดต่อสื่อสารด้วยวิธีการทางอิเล็กทรอนิกส์โดยเฉพาะอย่างยิ่งในการติดต่อทางเครือข่ายสาธารณะ เช่น เครือข่ายอินเทอร์เน็ตนั้น ค่อนข้างมีความซับซ้อนและต่างไปจากเดิมมาก เพราะต้องติดต่อผ่านระบบคอมพิวเตอร์ที่เชื่อมต่อกันเป็นทอดๆ กลายเป็นเครือข่ายขนาดใหญ่ ผ่านคอมพิวเตอร์จำนวนมากมาย อาทิ การส่งข้อมูลนั้นต้องผ่านเครื่องบริการ (Server) หรืออุปกรณ์จัดหาเส้นทาง (Router) จำนวนมาก แต่ระยะเวลาที่ส่งหรือได้รับข้อมูลอิเล็กทรอนิกส์นั้นรวดเร็วมาก ในขณะเดียวกัน ก็มีความซับซ้อนในการกำหนดเกี่ยวกับสถานที่มีการส่งหรือรับข้อมูลอิเล็กทรอนิกส์ เพราะมีความเป็นไปได้ที่ที่อยู่ของผู้ส่งข้อมูลอิเล็กทรอนิกส์จะปรากฏหรือถูกระบุเป็นสถานที่หนึ่ง แต่มีการส่งข้อมูลอิเล็กทรอนิกส์จริงจากอีกสถานที่หนึ่ง นอกจากนี้ การส่งและรับข้อมูลอิเล็กทรอนิกส์โดยเฉพาะอย่างยิ่ง ในการติดต่อทางเครือข่าย อาจมีวิธีการส่งและรับที่อาจระบุตัวบุคคล ระบุเวลาสถานที่ส่งและรับข้อมูลอิเล็กทรอนิกส์ได้ยากและแตกต่างไปจากวิธีการส่งและรับแบบเดิมๆ เช่น การส่งจดหมายโดยทางไปรษณีย์ ดังนั้น พระราชบัญญัติฉบับนี้จึงต้องกำหนดหลักการกว้างๆ เพื่อรองรับวิทยาการสมัยใหม่นี้ไว้ด้วย

[42] UNCITRAL Model Law on Electronic Commerce 1996, paras.93-99

พระราชบัญญัติฉบับนี้ ได้กำหนดวิธีการส่งและการรับข้อมูลอิเล็กทรอนิกส์ไว้เพื่อแก้ปัญหาที่อาจจะเกิดขึ้นในทางปฏิบัติอันเกิดจากการติดต่อทางอิเล็กทรอนิกส์โดยเฉพาะอย่างยิ่งในการติดต่อทางเครือข่ายหรือทางอินเทอร์เน็ต ซึ่งวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์อาจจะแตกต่างไปจากการติดต่อกันด้วยวิธีการทางอิเล็กทรอนิกส์อื่น เช่น การติดต่อกันทางโทรเลข หรือโทรพิมพ์ ซึ่งสามารถที่จะระบุตัวบุคคล ระบุเวลา รวมทั้งระบุสถานที่ส่งและรับข้อมูลอิเล็กทรอนิกส์ได้ง่ายและค่อนข้างแน่นอน แตกต่างไปจากวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ผ่านทางเครือข่าย

ปัญหาในการส่งและรับข้อมูลอิเล็กทรอนิกส์ผ่านทางระบบเครือข่าย ซึ่งเป็นสาเหตุให้ต้องมีการกำหนดวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ขึ้นโดยเฉพาะนั้น อาจเกิดขึ้นจากปัญหาในการระบุหรือยืนยันตัวบุคคลผู้ส่งข้อมูลหรือผู้รับข้อมูล กล่าวคือในการส่งข้อมูลหรือรับข้อมูลทางเครือข่ายนั้น ผู้ใช้บริการอาจจะจดทะเบียนกับผู้เป็นสื่อกลางซึ่งให้บริการอินเทอร์เน็ตหลายบัญชี (account) โดยมีชื่อบัญชีแตกต่างกัน ดังนั้น หากคู่สัญญาหรือบุคคลที่ทำการติดต่อกันไม่กำหนดบัญชีที่ประสงค์จะติดต่อให้ชัดเจนก็อาจทำให้เกิดปัญหาในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์ได้เช่นกัน เพราะกรณีอาจเป็นได้ว่ามีการส่งหรือรับแล้วแต่ผู้ส่งหรือผู้รับไม่ทราบว่าอีกฝ่ายยังไม่ได้รับเนื่องจากผู้ส่งหรือผู้รับไม่ได้เปิดดูบัญชีที่มีการส่งข้อมูลอิเล็กทรอนิกส์นั้นดังนั้น พระราชบัญญัติฉบับนี้จึงต้องกำหนดหลักการ กว้างๆ เพื่อรองรับวิทยาการสมัยใหม่นี้ไว้

- **เวลาที่ถือว่ามีการส่งและรับข้อมูลอิเล็กทรอนิกส์ (มาตรา 22 – มาตรา 23)**[43]

---

[43] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Commerce 1996, Singapore Electronic Transactions Act 1998, Philippines Electronic Commerce Act 2000 , India Information Technology Act 2000 , South

มาตรา 22 – มาตรา 23 ได้กำหนดเกี่ยวกับเวลาที่มีการส่งและรับข้อมูลอิเล็กทรอนิกส์ โดยให้ถือว่ามีการส่งข้อมูลอิเล็กทรอนิกส์เมื่อข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่อยู่นอกเหนือการควบคุมของผู้ส่งข้อมูลหรือบุคคลซึ่งได้ส่งข้อมูลนั้นในนามของผู้ส่งข้อมูล ซึ่งอาจจะเป็นระบบข้อมูลของบุคคลผู้เป็นสื่อกลาง (Intermediary) หรือระบบข้อมูลของผู้รับข้อมูลก็ได้ ทั้งนี้ คำว่า "ระบบข้อมูล" นั้นหมายถึง กระบวนการประมวลผลด้วยเครื่องมืออิเล็กทรอนิกส์สำหรับสร้าง ส่ง รับ เก็บรักษา หรือประมวลผลข้อมูลอิเล็กทรอนิกส์" นั่นเอง อย่างไรก็ตาม "การส่งและการรับข้อมูลอิเล็กทรอนิกส์" ไม่ได้บัญญัติขึ้นเพื่อแทนที่หลักเกณฑ์ทั่วไปในการส่งและรับตามหลักกฎหมายเกี่ยวกับนิติกรรมสัญญาแต่อย่างใด

นอกจากนั้น ในการกำหนดบทบัญญัติเกี่ยวกับการรับข้อมูลอิเล็กทรอนิกส์ก็ได้มีการกำหนดให้ถือว่ามีการรับข้อมูลอิเล็กทรอนิกส์ต่อเมื่อข้อมูลอิเล็กทรอนิกส์นั้นเข้าสู่ระบบข้อมูลที่ได้กำหนดไว้ ทั้งนี้ การเข้าสู่ระบบข้อมูลนั้นไม่ต้องคำนึงถึงว่าข้อมูลนั้นจะสามารถอ่านออกหรือเข้าใจได้หรือไม่ก็ตาม ทั้งนี้ เพราะมีความเป็นไปได้ว่าข้อมูลอิเล็กทรอนิกส์นั้นอาจมีการเข้ารหัสลับไว้ อย่างไรก็ตาม หากมีการกำหนดระบบข้อมูลที่รับข้อมูลอิเล็กทรอนิกส์ไว้แล้ว แต่หากมีการส่งข้อมูลไปยังระบบข้อมูลอื่นที่ผู้รับมิได้กำหนดเอาไว้ ก็ให้ถือว่าเวลาที่มีการรับข้อมูลอิเล็กทรอนิกส์นั้น มีผลนับแต่เวลาที่ได้มีการเรียกข้อมูลอิเล็กทรอนิกส์นั้นจากระบบข้อมูลนั้น

- **สถานที่ซึ่งถือว่ามีการส่งและรับข้อมูลอิเล็กทรอนิกส์ (มาตรา 24)**[44]

Korea Basic Law on Electronic Commerce หรือ Brunei Electronic Transaction Order 2000 เป็นต้น

[44] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Commerce 1996, Singapore Electronic Transactions Act 1998, Philippines Electronic Commerce Act 2000 , India Information Technology Act 2000 , South Korea Basic Law on Electronic Commerce, Hong Kong Electronic Transactions Ordinance หรือ Brunei Electronic Transaction Order 2000 เป็นต้น

เนื่องจากในการกำหนดเกี่ยวกับสถานที่ในการติดต่อสื่อสารทางระบบเครือข่ายอินเทอร์เน็ตนั้น ค่อนข้างยากที่จะกำหนดหรือรู้สถานที่ที่มีการส่งและรับข้อมูลอิเล็กทรอนิกส์จริง ทั้งนี้ เนื่องจากในการติดต่อทางอินเทอร์เน็ตนั้น แม้มีการลงทะเบียนสถานที่หรือที่อยู่ของผู้ส่งหรือรับข้อมูลอิเล็กทรอนิกส์ไว้ แต่บุคคลซึ่งส่งหรือรับข้อมูลอิเล็กทรอนิกส์ก็อาจส่งหรือรับข้อมูลอิเล็กทรอนิกส์จากอีกที่หนึ่งก็ได้ ดังนั้น ในกรณีที่คู่กรณีมิได้ตกลงเป็นอย่างอื่น กฎหมายจึงได้กำหนดให้สถานที่ที่มีการส่งหรือรับ คือ ที่ทำการงานของผู้ส่งข้อมูลหรือผู้รับข้อมูล และในกรณีที่มีที่ทำการงานหลายแห่งให้ถือเอาที่ทำการงานที่เกี่ยวข้องมากที่สุดกับการทำธุรกรรมนั้น และหากไม่สามารถกำหนดสถานที่ทำการงานที่เกี่ยวข้องที่สุดได้ ก็ให้ “สำนักงานใหญ่” เป็นที่ส่งหรือรับ และในกรณีที่ไม่มีที่ทำการงานให้ถือ “ถิ่นที่อยู่ปกติ” เป็นสถานที่ส่งหรือรับข้อมูลอิเล็กทรอนิกส์

1.5.11 วิธีการแบบปลอดภัย (มาตรา 25)

บทบัญญัติตามมาตรา 25 ของพระราชบัญญัตินี้ บัญญัติขึ้นเพื่อให้กฎหมายมีความยืดหยุ่นในการปรับใช้กับเทคโนโลยีต่างๆ ที่มีอยู่ในปัจจุบัน และที่อาจเกิดขึ้นในอนาคต กล่าวคือ เมื่อพิจารณาจากมาตราต่างๆ ตามที่ปรากฏในหมวดหนึ่ง จะพบว่ามีหลายมาตราที่ได้มีการระบุถึงการใช้วิธีการที่เชื่อถือได้ในการนำข้อมูลอิเล็กทรอนิกส์มาใช้ในรูปแบบต่างๆ อาทิ

- การใช้วิธีการที่เชื่อถือได้ในการลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ตามมาตรา 9 (2)
- การใช้วิธีการที่เชื่อถือได้ในการนำเสนอหรือเก็บรักษาข้อความในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ตามมาตรา 10 (1)

อย่างไรก็ตาม กฎหมายมิได้มีการกำหนดในรายละเอียดว่าวิธีการอย่างไรจึงจะเป็นวิธีการที่เชื่อถือได้ โดยปล่อยให้ผู้ที่ใช้เทคโนโลยีต้องพิจารณากันเองว่าอย่างไรจึงจะเป็นวิธีการที่เชื่อถือได้

ด้วยเหตุนี้ เพื่อช่วยให้การปฏิบัติตามกฎหมายมีหลักเกณฑ์ และวิธีการในรายละเอียด ประกอบกับเพื่อให้กฎหมายมีความยืดหยุ่นในการรองรับกับเทคโนโลยีต่างๆ ดังนั้นจึงได้มีการบัญญัติ มาตรา 25 ขึ้น โดยกำหนดให้มีการตราพระราชกฤษฎีกาเพื่อกำหนดว่าวิธีการใดบ้างเป็นวิธีการที่เชื่อถือได้ตามกฎหมาย เพราะวิธีการที่เชื่อถือได้อาจมีหลายรูปแบบแตกต่างกันไปตามเทคโนโลยีที่นำมาใช้

ทั้งนี้ กฎหมายมิได้มีบทบัญญัติห้ามผู้ประกอบธุรกรรมที่ต้องการจะใช้วิธีการอย่างอื่นนอกเหนือไปจากที่พระราชกฤษฎีกากำหนด เพียงแต่การนำมาใช้นั้น ผู้ใช้อาจต้องมีภาระในการพิสูจน์ว่าเพราะเหตุใดวิธีการดังกล่าวจึงเป็นวิธีการที่น่าเชื่อถือตามกฎหมาย

บทที่ 2
ลายมือชื่ออิเล็กทรอนิกส์

2.1 ความนำ

ดังที่ได้กล่าวมาแล้วในบทนำว่าพระราชบัญญัติฉบับนี้ได้มีการรวมหลักการของกฎหมายสองฉบับไว้ด้วยกันคือร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... และร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. .... ซึ่งในการพิจารณายกร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. .... ก่อนที่จะมีการรวมหลักการเข้ากับร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... และกลายเป็นส่วนหนึ่งของร่างพระราชบัญญัติดังกล่าวนั้น ได้มีการศึกษากฎหมายหลายๆ ประเทศประกอบการพิจารณา อาทิ สิงคโปร์ มาเลเซีย เกาหลีใต้ เยอรมัน และกฎหมายหลายมลรัฐของสหรัฐอเมริกา เช่น Utah Illinois และ Virginia เป็นต้น ควบคู่ไปกับการศึกษาการพิจารณายกร่างกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ที่อยู่ภายใต้ความรับผิดชอบของคณะทำงานของ UNCITRAL โดยใช้ชื่อเดิมในขณะที่มีการยกร่างว่า “Draft Uniform Rules on Electronic Signatures” ซึ่งในขณะนั้นยังพิจารณายกร่างไม่แล้วเสร็จ

ผลจากการศึกษากฎหมายของประเทศต่างๆ ข้างต้น พบว่ากฎหมายเกี่ยวกับการระบุตัวบุคคลทางอิเล็กทรอนิกส์นั้นแยกออกได้เป็น 2 แบบ กล่าวคือ

กฎหมายลายมือชื่อดิจิทัลและกฎหมายลายมือชื่ออิเล็กทรอนิกส์[45] โดยในประเทศที่มีการยกร่างกฎหมายหรือตรากฎหมายลายมือชื่อดิจิทัลขึ้นใช้บังคับนั้น ก็เนื่องจากการเพิ่มขึ้นอย่างรวดเร็วของการใช้ลายมือชื่อดิจิทัลซึ่งเทคโนโลยีชนิดนี้นอกจากจะให้ความมั่นใจในการระบุตัวบุคคลและตรวจสอบตัวบุคคลแล้ว ยังให้ความปลอดภัยในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์เพราะจะทำให้ผู้รับข้อมูลอิเล็กทรอนิกส์ทราบได้ทันทีว่าข้อมูลอิเล็กทรอนิกส์ที่ส่งมานั้นมีการแก้ไขเปลี่ยนแปลงหรือไม่ รวมทั้งยังรักษาความลับของข้อมูลอิเล็กทรอนิกส์ได้ด้วยหากใช้กุญแจสาธารณะในการเข้ารหัส (Public key cryptography) กับข้อมูลอิเล็กทรอนิกส์ ดังนั้นจึงแทบจะอาจกล่าวได้ว่าปัจจุบันเทคโนโลยี PKI เป็นระบบเดียวที่สามารถสร้างวิธีการในการระบุตัวบุคคลและมีกลไกในการตรวจสอบตัวบุคคลได้แน่นอน ประกอบกับแม้เทคโนโลยีจะมีการเปลี่ยนแปลงค่อนข้างรวดเร็วแต่หลักการพื้นฐานของวิทยาการการเข้ารหัสก็ยังประยุกต์ใช้ได้อยู่ตลอดเวลาและมีการพัฒนาก้าวตามเทคโนโลยีเพื่อรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์โดยเพียงเพิ่มความยาวของ “กุญแจ” ที่ใช้ให้ยาวขึ้นเท่านั้น ดังนั้น เพื่อสร้างความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์หลายประเทศจึงได้กำหนดรองรับลายมือชื่อดิจิทัลไว้อย่างชัดเจนในกฎหมาย

ส่วนประเทศที่ยกร่างหรือตรากฎหมายลายมือชื่ออิเล็กทรอนิกส์ขึ้นใช้บังคับส่วนหนึ่งก็เพื่อให้กฎหมายสามารถรองรับความเปลี่ยนแปลงของเทคโนโลยีและรองรับเทคโนโลยีใหม่นั้นได้ แต่แม้กระนั้นก็ตาม หากพิจารณากฎหมายเหล่านั้น รวมทั้งกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ของ UNCITRAL ซึ่งแต่เดิมก็มีพัฒนาการมาจากลายมือชื่อดิจิทัล[46] ก็ยังคงหลักการซึ่งสามารถรองรับกลไกของลายมือชื่อดิจิทัลไว้ในกฎหมายนั่นเอง อาทิ บทบัญญัติเกี่ยวกับใบรับรอง ผู้ประกอบการรับรอง เป็นต้น เพียงแต่กฎหมายแม่แบบดังกล่าว ได้มีการเขียนคำอธิบายไว้ชัดเจนถึงเจตนารมณ์ในการกำหนดกรอบกฎหมายไว้กว้าง ๆ โดยการ

---

[45] โปรดดูเอกสารในภาคผนวก ค.

[46] References to UNCITRAL documents: A/CN.9/WG.IV/WP.71

เลือกใช้คำกลางๆ ในกฎหมายเพื่อสื่อถึงเจตนารมณ์ของกฎหมาย เช่น คำว่า “การสร้างลายมือชื่อ” “การรับรอง” “ความเชื่อถือในลายมือชื่ออิเล็กทรอนิกส์”[47] เป็นต้น เพื่อให้เกิดความยืดหยุ่นในการปรับใช้กฎหมายได้กับลายมือชื่ออิเล็กทรอนิกส์ทุกประเภทไม่ใช่แต่เพียงกับลายมือชื่อดิจิทัลเท่านั้น

สำหรับการพิจารณายกร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ ในขณะนั้น แม้จะยกร่างกฎหมายเพื่อรองรับ “ลายมือชื่ออิเล็กทรอนิกส์” ทุกประเภทแต่ก็ได้กำหนดหลักการสำคัญตามกลไกของ “ลายมือชื่อดิจิทัล” ไว้ในกฎหมายด้วย อาทิ หน้าที่ของผู้ถือใบรับรอง ผู้ประกอบการรับรอง หน้าที่ของผู้ประกอบการรับรองรับอนุญาต การพักใช้และการเพิกถอนใบรับรอง และความรับผิดของผู้ประกอบการรับรอง เป็นต้น ทั้งนี้ เพื่อให้เป็นอำนาจของรัฐสภาในการกำหนดหลักการสำคัญดังกล่าวข้างต้นไว้ในกฎหมายเพื่อให้เกิดความแน่นอนในการบังคับใช้กฎหมาย ทั้งนี้ เป็นไปตามความเห็นส่วนใหญ่ซึ่งสำรวจได้จากภาคประชาชนและภาคธุรกิจในการจัดสัมมนาเผยแพร่ความรู้ความเข้าใจเกี่ยวกับร่างพระราชบัญญัติดังกล่าวจำนวนหลายครั้ง ซึ่งเชื่อมั่นว่าหากกำหนดหลักการสำคัญข้างต้นไว้ในกฎหมายชั้นพระราชบัญญัติน่าจะดีกว่ากำหนดในกฎหมายที่ตราขึ้นโดยฝ่ายบริหาร

อย่างไรก็ตาม เมื่อมีการรวมหลักการกฎหมายของร่างพระราชบัญญัติสองฉบับเข้าด้วยกันตามข้อเสนอของสำนักงานคณะกรรมการกฤษฎีกา ด้วยเห็นว่ากฎหมายทั้งสองฉบับมีความเกี่ยวข้องกัน โดยให้มีการกำหนดหลักการสำคัญของร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ให้เป็นอำนาจของฝ่ายบริหาร เพื่อให้กฎหมายมีความยืดหยุ่นเหมาะสมสำหรับการเปลี่ยนแปลงทางเทคโนโลยีในอนาคต ซึ่งคณะรัฐมนตรีก็ได้เห็นชอบตามนั้น จนผ่านการพิจารณาของสภาผู้แทนราษฎรและในขณะที่อยู่ระหว่างการเสนอให้วุฒิสภาพิจารณานั้น การพิจารณายกร่างกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ของ UNCITRAL ซึ่งแต่เดิมอยู่ในรูป Uniform

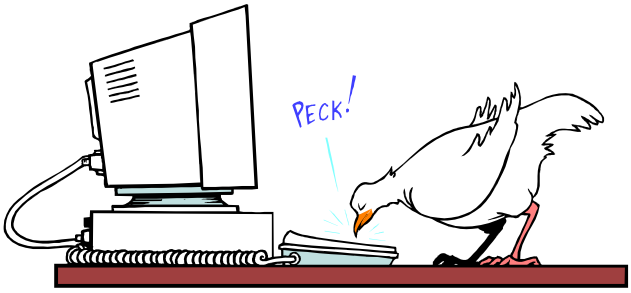
[47] References to UNCITRAL documents: A/CN.9/WG.IV/WP.88, p.16 paras.28

Rules ก็ได้แล้วเสร็จและกลายเป็นกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ ซึ่งกำหนดเป็นกรอบหรือแนวทางให้กับประเทศต่างๆ ในการตรากฎหมายภายในประเทศของตน ดังนั้น ในชั้นการพิจารณาของวุฒิสภาจึงได้มีการเพิ่มเติมบทบัญญัติในส่วนที่เกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ หมวดที่ 2 ขึ้น ทั้งนี้ เพื่อให้สอดคล้องกับกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ และเพื่อให้กฎหมายมีความยืดหยุ่น สามารถรองรับกับเทคโนโลยีได้ทุกชนิด

2.2 พัฒนาการทางเทคโนโลยีที่ใช้ในการสร้างลายมือชื่อ

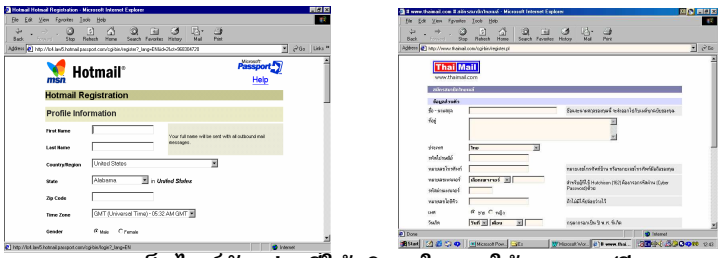
ปัจจุบันแม้ว่าการติดต่อสื่อสารผ่านทางเครือข่ายโดยเฉพาะอย่างยิ่งทางเครือข่ายอินเทอร์เน็ตจะได้รับความนิยมอย่างมากเพราะปัจจัยหลายๆ ประการ อาทิ การติดต่อผ่านทางอินเทอร์เน็ตสามารถทำให้บุคคลติดต่อถึงกันได้โดยสะดวก รวดเร็ว ถึงบุคคลจำนวนมากได้ในเวลาพร้อมๆ กันหรือใกล้เคียงกัน และเป็นแหล่งข้อมูลข่าวสาร ความรู้ หรือสารสนเทศ เปรียบเสมือนห้องสมุดขนาดมหึมาที่เปิดทำการตลอด 24 ชั่วโมง เป็นประโยชน์มหาศาลต่อมนุษยชาติทั้งด้านการศึกษา การสาธารณสุข การพาณิชย์และอื่นๆ อีกมากมาย แต่ปัญหาหรืออุปสรรคสำคัญประการหนึ่งที่สร้างความไม่มั่นใจอย่างมากให้กับบุคคลที่ประสงค์จะติดต่อสื่อสารถึงกันผ่านทางอินเทอร์เน็ต คือ ความไม่แน่ใจในตัวบุคคลที่ตนทำการติดต่อด้วยว่าเป็นบุคคลที่ตนประสงค์จะติดต่อจริงหรือไม่ โดยเฉพาะอย่างยิ่งเมื่อมีการติดต่อค้าขายระหว่างกันทางอิเล็กทรอนิกส์หรือการพาณิชย์อิเล็กทรอนิกส์ เพราะบุคคลที่ติดต่อกันอาจไม่เคยรู้จักหน้าค่าตากันมาก่อน และเนื่องจากการติดต่อสื่อสารกันผ่านทางอินเทอร์เน็ตนั้นอาจเป็นการติดต่อกันโดยบุคคลใดก็ได้ จนกลายเป็นที่มาของภาพล้อเลียนชื่อดังว่า

"วันหนึ่ง...อาจพบว่า บุคคลที่มนุษย์ทำการติดต่อด้วยนั้นอาจจะไม่ใช่มนุษย์อย่างที่เข้าใจก็ได้" เช่นภาพที่ปรากฏดังต่อไปนี้



Because on the Internet, no one knows you're a chicken!

การระบุตัวบุคคลมีความสำคัญอย่างยิ่งต่อความผูกพันหรือความรับผิดอันเกิดขึ้นจากการก่อนิติสัมพันธ์ระหว่างบุคคล ตัวอย่างปัญหาในการระบุตัวหรือยืนยันตัวบุคคลซึ่งเกิดขึ้นบ่อย ๆ มักเกิดขึ้นในการติดต่อสื่อสารทางอินเทอร์เน็ตโดยใช้จดหมายอิเล็กทรอนิกส์ (e-mail) ซึ่งจะขอใช้บริการได้โดยง่ายจากเว็บไซต์ที่เปิดให้ใช้บริการได้ฟรีทั้งหลาย อย่างไรก็ตาม การขอใช้บริการนั้นแม้ว่าในขั้นการสมัครขอใช้หรือขอมี e-mail address เพื่อให้ตนมีชื่อและที่อยู่ซึ่งสามารถทำการติดต่อสื่อสารกับบุคคลอื่นได้ทางอินเทอร์เน็ตนั้น จะกำหนดให้มีการลงทะเบียนโดยผู้สมัครขอใช้บริการต้องให้รายละเอียดเกี่ยวกับตนเองในแบบฟอร์มที่ผู้ให้บริการจัดไว้ก็ตาม แต่ก็ไม่มีการตรวจสอบตัวบุคคลหรือตรวจสอบรายละเอียดความถูกต้องของข้อมูลของผู้สมัครแต่อย่างใด ดังนั้น จึงอาจมีความเป็นไปได้ว่าผู้สมัครขอใช้บริการอาจให้ข้อมูลที่ไม่ตรงตามความเป็นจริงหรือไม่ถูกต้องก็เป็นได้ ทั้งนี้ อาจเพราะไม่เชื่อมั่นเกี่ยวกับระบบความปลอดภัยในการติดต่อทางอิเล็กทรอนิกส์หรือเพราะไม่ประสงค์ให้ข้อมูลส่วนบุคคลของตนถูกเปิดเผยโดยไม่ได้รับอนุญาต เช่น ในกรณีที่มีการแอบหรือดักเอาข้อมูลไปใช้โดยมิชอบ เป็นต้น



ภาพเว็บไซต์ตัวอย่างที่ให้บริการในการใช้ e-mail ฟรี
ซึ่งจะทำให้เราใช้งานได้แม้ข้อมูลที่เราป้อนเขาไปจะไม่ตรงกับสภาพความเป็นจริง

ดังนั้น การระบุตัวบุคคลเพื่อให้เกิดความเชื่อมั่นว่าบุคคลที่ตนประสงค์จะติดต่อด้วยนั้นเป็นบุคคลคนนั้นจริง มีตัวตนจริง จึงสำคัญอย่างยิ่งต่อการพัฒนาพาณิชย์อิเล็กทรอนิกส์ เพื่อแก้ปัญหาดังกล่าวจึงได้มีการพัฒนาวิธีการที่จะใช้ในการระบุหรือยืนยันตัวบุคคล และการระบุตัวบุคคลได้ดีที่สุดวิธีหนึ่งก็คือ การลงลายมือชื่อหรือเซ็นชื่อนั่นเอง แต่เมื่อพัฒนาการทางเทคโนโลยีก้าวหน้าไปไกล ก็เริ่มมีการพัฒนาลายมือชื่ออิเล็กทรอนิกส์ซึ่งสามารถใช้ในการระบุตัวบุคคลได้แม่นยำเช่นเดียวกับการลงลายมือชื่อหรือเซ็นชื่อธรรมดาของแต่ละบุคคลมีลายเซ็นที่แตกต่างกัน ดังนั้น การรับรองสถานะทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์ที่มนุษย์สร้างขึ้นให้เท่าเทียมกับลายมือชื่อหรือลายเซ็นของบุคคลจึงเกิดขึ้นดังได้มีการกล่าวไว้แล้วในส่วนที่หนึ่ง

2.2.1 หลักพื้นฐานในการพัฒนาเทคโนโลยีเพื่อระบุตัวบุคคล

พัฒนาการทางเทคโนโลยีในการระบุตัวบุคคลนั้นพัฒนามาจากหลักพื้นฐาน 3 หลัก [48] ได้แก่

[48] Benjamin Wright and Jane K. Winn, The Law of Electronic Commerce 3rd ed. (New York: Asen Law & Business, 1998), p.3-10.

ก) สิ่งที่รู้ (something you know) หมายถึง วิธีการยืนยันตัวบุคคลซึ่งเฉพาะบุคคลที่ตรวจสอบและบุคคลที่ถูกตรวจสอบเท่านั้นที่รู้เกี่ยวกับสิ่งที่ใช้ตรวจสอบ เช่น การใช้รหัสผ่าน (password) รหัสประจำตัว (personal certification number: PIN)

ข) สิ่งที่มี (something you have) หมายถึง การที่บุคคลซึ่งถูกตรวจสอบมีสิ่งซึ่งใช้ยืนยันตัวบุคคล เช่น บัตรประจำตัวพนักงานในการบันทึกเวลาเข้า-ออกในการทำงานแต่ละวัน บัตรสมาร์ทการ์ด (smart card) หรือบัตรแถบแม่เหล็ก (magnetic card) เป็นต้น

ค) สิ่งที่เป็น (something you are) หมายถึงการใช้ลักษณะเฉพาะของตัวบุคคลในการตรวจสอบและพิสูจน์ตัวบุคคล สิ่งที่ใช้ตรวจสอบมักเป็นเทคโนโลยีชีวภาพ เช่น ลายนิ้วมือ (fingerprints) ม่านตา (iris) เสียง (voice prints) หรือลักษณะของ DNA เป็นต้น

2.2.2 การรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์

นอกเหนือจากหลักพื้นฐานตามข้อ 2.2.1 ข้างต้นซึ่งใช้ในการระบุตัวบุคคลแล้ว ความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ในรูปของข้อมูลอิเล็กทรอนิกส์ ก็เป็นอีกประเด็นหนึ่งที่สำคัญอย่างยิ่งในการสร้างความมั่นใจให้กับผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ และมีส่วนสำคัญอย่างยิ่งต่อการพัฒนาเทคโนโลยีในการระบุตัวบุคคล การรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ แบ่งออกได้เป็น 5 ประการ[49] ดังนี้

---

[49] ในตำราทางวิชาการบางครั้งก็แบ่งออกเป็น 4 ประการเท่านั้น ทั้งนี้ โดยไม่รวม "การควบคุมการเข้าถึง" ไว้ด้วยแต่อย่างใด โปรดดู Bert-Jaap Koops, The Crypto Controversy : A Key Conflict in the Information Society, (Netherlands: Kluwer Law International, 1999),

ก) การระบุตัวบุคคล (Authentication) เพื่อยืนยันตัวบุคคลผู้ส่งหรือผู้สร้างข้อมูลอิเล็กทรอนิกส์

ข) การควบคุมการเข้าถึง (Access Control) ซึ่งอนุญาตให้เฉพาะบุคคลซึ่งมีสิทธิหรือได้รับอนุญาตเท่านั้นในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ และป้องกันมิให้บุคคลซึ่งไม่มีสิทธิหรือไม่ได้รับอนุญาตเข้าถึงข้อมูลอิเล็กทรอนิกส์

ค) การรักษาความลับ (Confidentiality) เพื่อป้องกันมิให้บุคคลซึ่งไม่ได้รับอนุญาตหรือไม่มีสิทธิอ่านข้อมูลอิเล็กทรอนิกส์ได้

ง) ความถูกต้องครบถ้วนของข้อมูลอิเล็กทรอนิกส์ (Integrity) เพื่อป้องกันมิให้มีการเปลี่ยนแปลง แก้ไข ทำลาย หรือสร้างข้อมูลอิเล็กทรอนิกส์ขึ้นโดยไม่ได้รับอนุญาต

จ) การป้องกันการปฏิเสธความรับผิด (Non-repudiation) เพื่อป้องกันมิให้ผู้ส่งข้อมูลหรือผู้รับข้อมูลปฏิเสธว่าตนไม่ได้ส่งหรือไม่ได้รับข้อมูลอิเล็กทรอนิกส์

2.2.3 พัฒนาการทางเทคโนโลยีสมัยใหม่ในการระบุตัวบุคคล

จากหลักพื้นฐานและความคิดเกี่ยวกับหลักความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ที่กล่าวมาในข้อ 2.2.1 และ 2.2.2 ข้างต้น ส่งผลต่อการพัฒนาเทคโนโลยีที่ใช้ในการระบุตัวบุคคล ซึ่งอาจลำดับพัฒนาการของเทคโนโลยีสมัยใหม่ได้ 3 รูปแบบ ดังนี้

---

p.38; Benjamin Wright and Jane K. Winn, The Law of Electronic Commerce, p. 3-12 to 9-13.

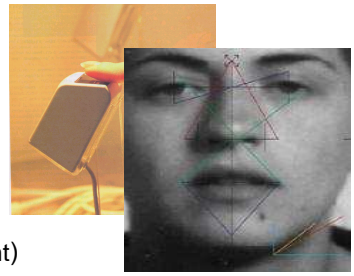
(1) **เทคโนโลยีบัตรแถบแม่เหล็ก** (Magnetic card) **หรือสมาร์ทการ์ด** (smart card)[50]

บัตรสมาร์ทการ์ดพัฒนาขึ้นมาโดยแถบแม่เหล็กที่ฝังชิป (chip) หรือหน่วยบันทึกความจำเกี่ยวกับชื่อผู้ใช้บัตร รหัสผ่าน และวันหมดอายุ บัตรประเภทนี้มักใช้เพื่อประโยชน์ในการผ่านทาง หรือเข้าไปยังระบบฐานข้อมูลของคอมพิวเตอร์ และประโยชน์ในทางกลับกันในการรักษาความปลอดภัยของระบบข้อมูลเพราะจะมีแต่เพียงบุคคลที่ได้รับอนุญาตเท่านั้นที่เข้าไปได้

ข้อดีของบัตรสมาร์ทการ์ดคือ สามารถใช้งานได้สะดวก และง่ายต่อการจดจำ และไม่ต้องใช้อุปกรณ์อย่างอื่นเข้าช่วย แต่มีข้อเสียตรงที่มีโอกาสที่บุคคลอื่นจะสามารถล่วงรู้และนำรหัสผ่านไปใช้ได้ ในการใช้งานจึงต้องระมัดระวังมิให้รหัสผ่านนั้นเปิดเผย หรือทำบัตรสมาร์ทการ์ดสูญหาย

(2) **เทคโนโลยีชีวภาพ** (Biometrics)

"เทคโนโลยีชีวภาพ" เป็นเทคโนโลยีชนิดหนึ่งที่ใช้ในการระบุตัวบุคคลโดยอาศัยหลักการพื้นฐานของลักษณะเฉพาะทางกายภาพของแต่ละบุคคล เช่น

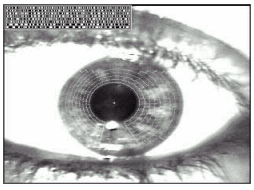


การใช้ลายพิมพ์นิ้วมือ (Finger Print)

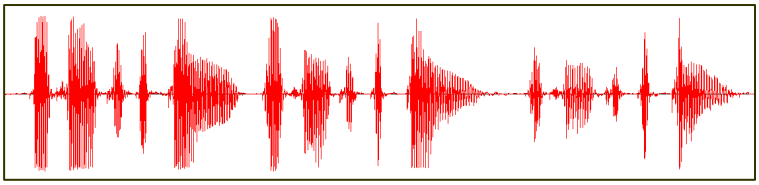
การบันทึกลักษณะโครงหน้าของมนุษย์

---

[50] ศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน ใช้คำแปลว่า "บัตรเก่ง", ราชบัณฑิตยสถาน, ศัพท์คอมพิวเตอร์, พิมพ์ครั้งที่ 4 (กรุงเทพฯ: โรงพิมพ์จุฬาลงกรณราชวิทยาลัย: 2540), หน้า 127



การบันทึกม่านตา (Iris)



การบันทึกความจำของเสียง (Voice Print)
ภาพตัวอย่างกราฟของคลื่นเสียงที่ถูกแปลงเป็นตัวเลข

ทั้งนี้ เทคโนโลยีชีวภาพนั้นจะแปลงลักษณะทางชีวภาพของบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ให้อยู่ในรูปของดิจิทัลและคำนวณออกมาโดยให้ค่าบันทึกความจำในลักษณะที่บ่งชี้ตัวบุคคลเจ้าของลักษณะทางชีวภาพนั้น

(3) **เทคโนโลยีการเข้ารหัสลับหรือวิทยาการการเข้ารหัสลับ** (Cryptography)

เทคโนโลยีการเข้ารหัสลับหรือวิทยาการการเข้ารหัสลับนั้นเริ่มเป็นที่รู้จักกันมาตั้งแต่สมัยโรมัน พัฒนาจากแนวคิดเกี่ยวกับพื้นฐานในการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์และพัฒนาเรื่อยมาจนถึงปัจจุบัน ซึ่งกลายเป็นกระบวนการทางคณิตศาสตร์ในการเข้ารหัสลับ (Cryptographic Algorithms) โดยการสร้างสิ่งที่อยู่ในรูปตัวอักษร อักขระ ตัวเลข หรือสัญลักษณ์ใด ๆ

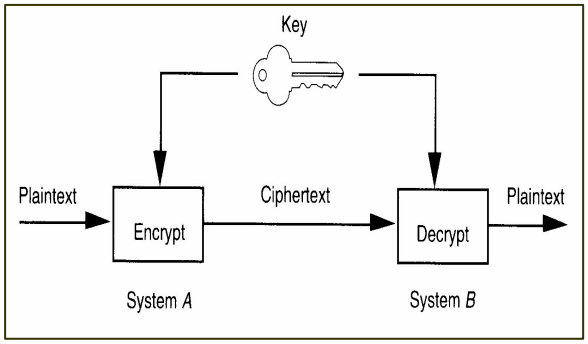
ขึ้นมา และเรียกสิ่งนั้นว่า “กุญแจ (key)” และใช้ “กุญแจ (key)” นั้นเอง เป็นกลไกสำคัญในการ “เข้ารหัส” และ “ถอดรหัส”

- **คำศัพท์สำคัญพื้นฐานในการทำความเข้าใจวิทยาการการเข้ารหัส**

ในการทำความเข้าใจพื้นฐานของวิทยาการในการเข้ารหัสนั้น จำเป็นต้องทำความเข้าใจคำศัพท์หลายคำเช่นกันซึ่งมีความสำคัญต่อขั้นตอนวิธีในการเข้าและถอดรหัส อันได้แก่

“การเข้ารหัส (encryption)” และ “การถอดรหัส (decryption)”

“การเข้ารหัส” หมายถึง การแปลงข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปหนึ่งที่อ่านได้ (plaintext) ให้อยู่ในอีกรูปแบบหนึ่งที่เปลี่ยนแปลงไปจากเดิมซึ่งอ่านไม่ได้ (ciphertext) ส่วน “การถอดรหัส” หมายถึงการแปลงข้อมูลอิเล็กทรอนิกส์จากรูปแบบที่เปลี่ยนแปลงไปจากเดิม (ciphertext) นั้น ให้กลับไปอยู่ในรูปของข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปแบบเดิมก่อนการเปลี่ยนแปลง (plaintext)



Source: Secure Electronic Commerce,
Warwick Ford and Michael S. Baum, Prentice Hall PTR, **1997**

สำหรับกระบวนการข้างต้นในการแปลงข้อมูลอิเล็กทรอนิกส์ที่อ่านได้เป็นข้อมูลอิเล็กทรอนิกส์ที่อ่านไม่ได้จะนี้เรียกว่า “การเข้ารหัส (Encryption) และการแปลงข้อมูลอิเล็กทรอนิกส์กลับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ที่อ่านได้เรียกว่า “การถอดรหัส (Decryption)”

“กุญแจ (key)”

คำว่า “กุญแจ (key)” ซึ่งเป็นกลไกสำคัญในการเข้ารหัสหรือถอดรหัสนั้น จะสร้างขึ้นด้วยกระบวนการทางคณิตศาสตร์ที่คำนวณโดยอัตโนมัติ และได้ผลลัพธ์ซึ่งอาจจะอยู่ในรูปของ อักษร อักขระ ตัวเลข หรือสัญลักษณ์ใดๆ ก็ได้ เช่น

D3K7EF8C9FE98A4B58CB2A57FD814BF78BC3D98B15FE8A
4FA8EB33C2F5D569FFB4A0012CF16EDA45CEF79AA5F1D3
AF7D9B46CF711CE84DEA011BF8A2D75F9CA701AD4B8A9F

คำว่า “กุญแจ” ในที่นี้จึงต่างไปจาก “กุญแจ” เป็นดอกๆ สำหรับใช้ไขแม่กุญแจทั่วไป แต่เหตุที่เรียกว่า “กุญแจ” อาจจะด้วยวัตถุประสงค์ในการสร้างขึ้นมาในการใช้เข้ารหัสโดยแปลงข้อความหรือตัวหนังสือที่อ่านเข้าใจได้ (plaintext) ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ซึ่งอ่านไม่ได้หรืออ่านไม่เข้าใจ (ciphertext) และในการใช้เพื่อถอดรหัสโดยทำหน้าที่ในการแปลงข้อความที่อ่านไม่ได้หรืออ่านไม่เข้าใจวัตถุประสงค์ของสิ่งๆนั้นให้อยู่ในรูปของข้อความที่อ่านได้หรือสามารถเข้าใจได้ถึงวัตถุประสงค์ของสิ่งๆ นั้น การทำงานของ “กุญแจ” โดยทำให้ข้อความนั้นเป็นความลับจึงคล้ายกับการปิดไม่ให้บุคคลอื่นได้รับรู้หรือเข้าถึงหรือเข้าใจ และสามารถใช้ไขความลับของข้อความนั้นได้คล้ายกับการเปิดออกอ่านได้ จึงน่าจะเป็นที่มาของการใช้คำว่า “กุญแจ”

“กุญแจคู่ (key pairs)”

“กุญแจคู่” จะประกอบด้วยกุญแจสองข้างที่สร้างขึ้นมาพร้อมกันด้วยกระบวนการทางคณิตศาสตร์ที่เรียกว่า “ระบบรหัสแบบอสมมาตร” โดยกุญแจข้างหนึ่งเรียกว่า “กุญแจส่วนตัว (private key)” ส่วนอีกข้างเรียกว่า “กุญแจสาธารณะ

(public key)" เหตุที่เรียกต่างกันเพราะลักษณะการทำงานของกุญแจทั้งสองข้างที่ต่างกัน กล่าวคือ "กุญแจส่วนตัว" นั้น ใช้ในการสร้างลายมือชื่อดิจิทัลเพื่อระบุหรือยืนยันตัวบุคคล ส่วน "กุญแจสาธารณะ" นั้นใช้ในการตรวจสอบลายมือชื่อ ดิจิทัล กุญแจทั้งสองข้างซึ่งสร้างขึ้นมาพร้อมกันนี้จึงเป็นกุญแจที่มีความสัมพันธ์กันในเชิงตรรกะซึ่งต้องใช้ควบคู่กันเสมอ [51]

"**กุญแจส่วนตัว** (private key)"
หมายความถึง กุญแจที่ใช้ในการสร้างลายมือชื่อดิจิทัล

"**กุญแจสาธารณะ** (public key)"
หมายความถึง กุญแจที่ใช้ในการตรวจสอบลายมือชื่อดิจิทัล

- **ประเภทระบบการเข้ารหัส**

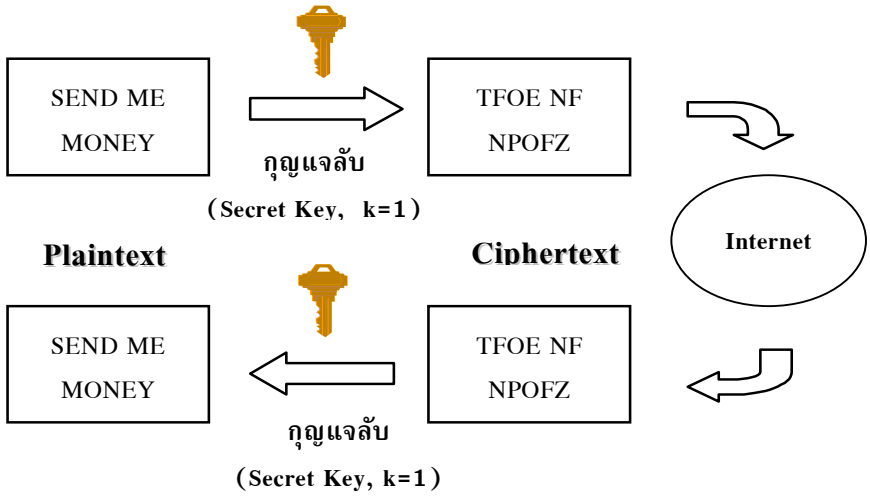
---

[51] แต่เดิมในร่างพระราชบัญญัติว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. ....ฉบับรับหลักการโดยคณะรัฐมนตรี เมื่อวันที่ 14 มีนาคม 2543 ก่อนจะมีการรวมหลักการให้เข้ากับร่างพระราชบัญญัติฯ เช่นในฉบับปัจจุบันนั้น ได้เคยมีการให้คำนิยามว่า "กุญแจคู่ หมายความว่า กุญแจส่วนตัวและกุญแจสาธารณะในระบบรหัสแบบอสมมาตร ที่ได้สร้างขึ้นโดยวิธีการที่ทำให้กุญแจส่วนตัวมีความสัมพันธ์ในทางคณิตศาสตร์กับกุญแจสาธารณะในลักษณะที่สามารถใช้กุญแจสาธารณะตรวจสอบได้ว่าลายมือชื่อดิจิทัลได้สร้างขึ้นโดยใช้กุญแจส่วนตัวนั้นหรือไม่" ซึ่งกฎหมายหลายประเทศก็กำหนดไว้ในกฎหมายเช่น Electronic Transactions Act ประเทศสิงคโปร์ ใน Article 2 ได้ให้นิยามว่า "key pair,in an asymmetric cryptosystem, means a private key and its mathematically related public key, having the property that the public key can verify a digital signature that the private key creates;" หรือ Digital Signature Act ของประเทศมาเลเซีย ใน Article 2 ซึ่งได้ให้ความหมายไว้ว่า "key pair means a private key and its corresponding public key in an asymmetric cryptosystem, where the public key can verify a digital signature that the private key creates;"

อย่างไรก็ตาม วิทยาการการเข้ารหัสนั้นสัมพันธ์อย่างยิ่งกับกลไกการทำงานของ “กุญแจ” ที่สร้างขึ้นให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ เพราะในการเข้ารหัสแต่ละครั้งอาจใช้กุญแจเพียงแค่ข้างเดียวหรือหลายข้างต่างวัตถุประสงค์กันไป จึงทำให้สามารถแยกประเภทของการเข้ารหัสตามจำนวนกุญแจที่นำมาใช้ได้ ดังนี้

ระบบการเข้ารหัสแบบกุญแจสมมาตร (Symmetric Key Cryptosystem)

ระบบการเข้ารหัสแบบสมมาตรเป็นการเข้ารหัสโดยใช้กุญแจข้างเดียวกันทั้งในการเข้ารหัสและถอดรหัส



ภาพแสดงระบบการเข้ารหัสแบบกุญแจสมมาตร โดยใช้สูตรการเข้ารหัสอย่างง่าย โดยกำหนดให้เลื่อนพยัญชนะภาษาอังกฤษตามปกติไปทางขวา 1 ตำแหน่ง ซึ่งจะได้ข้อความที่อ่านไม่ออก หรือไม่สามารถเข้าใจความหมายได้

การเข้ารหัสแบบสมมาตรนี้อาจจะเป็นการเข้ารหัสอย่างง่าย เช่น กำหนดเพียงให้เลื่อนพยัญชนะออกไปอีก 1 ตำแหน่ง กล่าวคือ คำว่า “กฎหมาย” หากเลื่อนตำแหน่งพยัญชนะไป 1 ตัว ก็จะปรากฏเป็นดังนี้ “ขฏฬาย” แทนคำว่า “กฎหมาย” จะเป็นการนำข้อมูลอิเล็กทรอนิกส์แบบธรรมดา เข้ารหัสโดยการแปลงข้อมูลนั้นให้อยู่ในรูปที่ไม่สามารถอ่านได้ด้วยการใช้กุญแจดอกเดียวกันหรือสูตรเดียวกันผ่านกระบวนการทางคณิตศาสตร์ทั้งในการเข้ารหัสและถอดรหัสเพื่อแปลงข้อมูลอิเล็กทรอนิกส์ที่อ่านไม่ได้ให้เป็นข้อมูลอิเล็กทรอนิกส์ที่อ่านได้ ดังนั้น เมื่อใช้กุญแจในการเข้ารหัสแล้วก็ต้องส่งมอบกุญแจนั้นให้กับผู้รับอีกฝ่ายซึ่งต้องใช้กุญแจดอกเดียวกันในการถอดรหัส และต้องมีการเก็บรายละเอียดเกี่ยวกับกุญแจไว้เป็นความลับเพื่อความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ กรณีที่ไม่ประสงค์ให้บุคคลที่สามหรือบุคคลอื่นได้ล่วงรู้อันอาจนำกุญแจไปใช้ในทางมิชอบโดยการเปิดเผยข้อมูลให้สาธารณะชนได้รับรู้

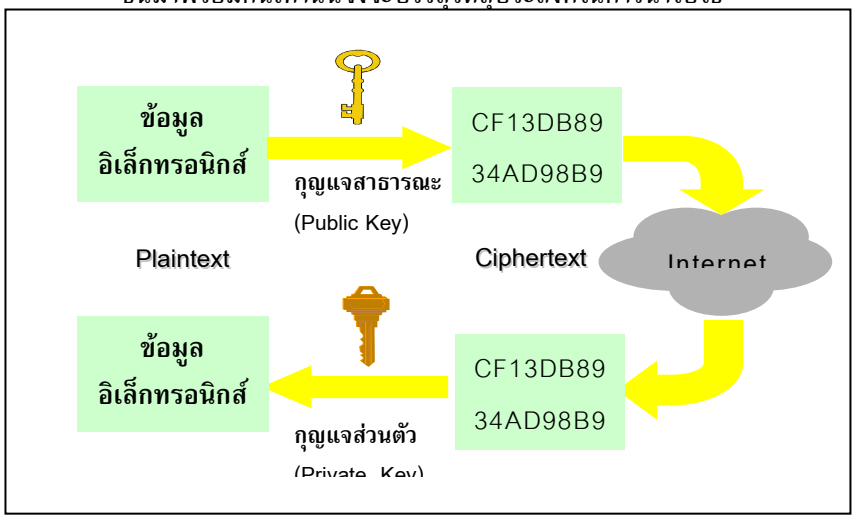
อย่างไรก็ตาม ระบบการเข้ารหัสแบบสมมาตรมีข้อดี คือ อาจตกลงให้มีการเข้ารหัสแบบง่าย ๆ เช่น การเลื่อนพยัญชนะ หรือกรณีที่มีการใช้เทคโนโลยีซับซ้อนขึ้น การเข้ารหัสแบบนี้ก็จะช่วยให้สามารถเข้ารหัสและถอดรหัสได้รวดเร็ว แต่ก็มีข้อเสียเพราะข้อตกลงให้มีการเข้ารหัสแบบง่าย ๆ อาจทำให้บุคคลอื่นล่วงรู้ได้ง่าย และในกรณีที่มีการใช้ระบบกุญแจก็จะประสบปัญหาในด้านการบริหารจัดการกุญแจ เพราะในการใช้กุญแจเพื่อเข้ารหัสและถอดรหัสนั้นจะต้องใช้กุญแจอันเดียวกัน ผู้สร้างกุญแจจึงต้องแจ้งให้บุคคลอื่นทราบเพื่อใช้ในการถอดรหัส ซึ่งการจะทำสำเนาให้บุคคลหลายคนเพื่อใช้ร่วมกันก็อาจจะก่อให้เกิดปัญหาในการระบุตัวบุคคล การแสดงความผูกพันหรือความรับผิดที่เกิดขึ้นจากการทำธุรกรรมในครั้งนั้น ดังนั้น โดยทั่วไปในการใช้กุญแจในระบบสมมาตรจึงมักมีการสร้างกุญแจขึ้นแบบสำหรับคนสองคนใช้ร่วมกัน ดังนั้นหากมีหลายคน ถ้าไม่ต้องการให้กุญแจซ้ำกันก็ต้องให้กุญแจหลายดอกเป็นจำนวนมากเพื่อความคล่องตัวและสะดวกในการใช้งานสำหรับกรณีที่ต้องติดต่อสื่อสารกับคนเป็นจำนวนมาก เช่น คนสี่คนติดต่อกันจะต้องใช้กุญแจคนละ 3 แบบ รวมทั้งสิ้นมีคู่กรณีได้ 6 คู่ รวมกุญแจทั้งสิ้น 6 แบบ ถ้าคน 100 คนจะต้องใช้

กุญแจจำนวนมาก ซึ่งก็จะเกิดปัญหามากมายติดตามมาเช่นกันในการบริหารจัดการกุญแจซึ่งมีเป็นจำนวนมาก

ระบบการเข้ารหัสแบบกุญแจอสมมาตร (Asymmetric KeyCryptosystem)

ระบบการเข้ารหัสแบบอสมมาตรเป็นการเข้าและถอดรหัสโดยใช้กุญแจสองดอก กุญแจข้างหนึ่งใช้เข้ารหัส อีกข้างหนึ่งหรืออีกดอกหนึ่งใช้ในการถอดรหัส ข้างที่ใช้ในการเข้ารหัสต้องเก็บไว้เป็นความลับ ส่วนข้างที่ใช้ในการถอดรหัสไม่จำต้องเก็บไว้เป็นความลับแต่อย่างใด (หรือจะใช้กลับกันก็ได้แล้วแต่วัตถุประสงค์)

กุญแจที่สร้างขึ้นจะสร้างขึ้นพร้อมกันเรียกว่า “กุญแจคู่ (Key Pair)” ข้างที่ใช้ในการเข้ารหัสเรียกว่า “กุญแจส่วนตัว (Private Key)” ส่วนอีกข้างใช้ในการถอดรหัสเรียกว่า “กุญแจสาธารณะ (Public Key)” และโดยทั่วไปกุญแจทั้งสองข้างแม้สร้างขึ้นมาพร้อมกันแต่ก็จะมีลักษณะไม่เหมือนกัน ยิ่งไปกว่านั้น การเข้ารหัสและถอดรหัส หากใช้กุญแจข้างเดียวกัน จะไม่ได้ผลต้องใช้อีกข้างหนึ่งซึ่งสร้างขึ้นมาพร้อมกันเท่านั้นจึงจะบรรลุวัตถุประสงค์ในการนำไปใช้



ภาพแสดงระบบการเข้ารหัสแบบกุญแจอสมมาตร

ข้อดีของการใช้ระบบกุญแจคู่ คือ ผู้สร้างอาจสร้างกุญแจขึ้นมาเพียงคู่เดียวและเก็บแต่เพียงกุญแจส่วนตัวของตนไว้เป็นความลับ ส่วนกุญแจสาธารณะนั้นก็สามารถนำไปแจกจ่ายหรือเปิดเผยไว้ได้โดยเปิดเผยในฐานข้อมูลของผู้ประกอบการรับรอง หรือในระบบเครือข่ายสาธารณะเพื่อให้บุคคลอื่นซึ่งเป็นใครก็ได้ติดต่อกับตน อันเป็นการขจัดข้อขัดข้องที่เกิดขึ้นในระบบสมมาตรเกี่ยวกับระบบการจัดการและบริหารกุญแจ หรือหากต้องการส่งเอกสารพร้อมกับลงลายมือชื่อ ก็สามารถทำได้โดยใช้กุญแจส่วนตัวในการเข้ารหัสกับข้อความที่ต้องการส่งซึ่งผ่านกระบวนการย่อย (Hash Function) แล้ว เป็นลายมือชื่อดิจิทัลส่งไปพร้อมกับข้อความที่ต้องการส่ง ซึ่งทำให้ผู้รับซึ่งสามารถนำกุญแจสาธารณะที่เผยแพร่ไว้โดยเปิดเผยสามารถตรวจสอบได้ว่า ลายมือชื่อดิจิทัลนี้เป็นของใคร และข้อความที่ส่งมาถูกเปลี่ยนแปลงแก้ไขหรือไม่

2.2.4 ลายมือชื่อดิจิทัลและเทคโนโลยี PKI (Public Key Infrastructure)

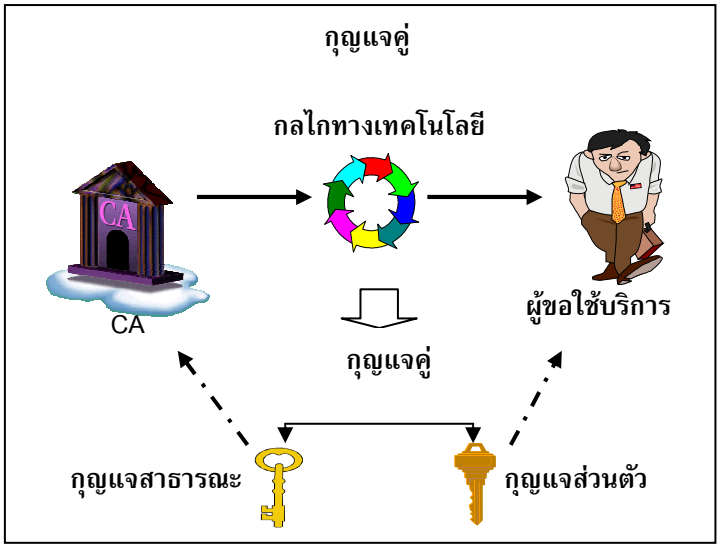
จากพื้นฐานของการเข้ารหัสแบบอสมมาตรโดยอาศัยกุญแจคู่ที่ไม่เหมือนกันในการเข้ารหัสและถอดรหัส และการใช้ “กุญแจส่วนตัว” ในการเข้ารหัสนี้เองจะเป็นส่วนสำคัญในการสร้างลายมือชื่ออิเล็กทรอนิกส์ประเภทหนึ่งที่นิยมใช้กันทั่วไปเรียกว่า “ลายมือชื่อดิจิทัล (Digital Signature)” เพื่อยืนยันตัวบุคคล และใช้กุญแจอีกข้างหนึ่งที่เรียกว่า “กุญแจสาธารณะ” ในการถอดรหัสซึ่งทำหน้าที่สำคัญในการตรวจสอบตัวบุคคล จนกลายเป็นที่มาของการเรียกเทคโนโลยีนี้ว่า “เทคโนโลยี PKI” ทั้งนี้ กลไกการทำงานของ “เทคโนโลยี PKI” ในระบบรหัสแบบอสมมาตรประกอบด้วยขั้นตอนดังนี้

(1) การสร้างลายมือชื่อดิจิทัล

(ก) การสร้างกุญแจคู่ (Key Pairs)

ก่อนการสร้างลายมือชื่อดิจิทัลนั้นต้องมีการสร้างกุญแจคู่ขึ้นมาเสียก่อนด้วยกระบวนการทางคณิตศาสตร์ โดยเจ้าของกุญแจคู่จะต้องเก็บกุญแจ

แรกที่เรียกว่า “กุญแจส่วนตัว” ไว้เป็นความลับเพื่อให้ตนเองเท่านั้นสามารถใช้กุญแจส่วนตัวได้แต่ผู้เดียว ยกเว้นในกรณีของการมอบอำนาจให้บุคคลอื่นใช้หรือในกรณีของนิติบุคคลซึ่งต้องกระทำการผ่านบุคคลผู้มีอำนาจกระทำการแทน และโดยปกติการเก็บรักษา “กุญแจส่วนตัว” นั้นก็มักจะบันทึกและเก็บไว้ในสมาร์ทการ์ด [52] ส่วน “กุญแจสาธารณะ” ก็จะเปิดเผยไว้ในระบบฐานข้อมูลของผู้ประกอบการรับรอง (Certificaton Authority) เพื่อให้สามารถตรวจสอบตัวบุคคลได้โดยง่าย

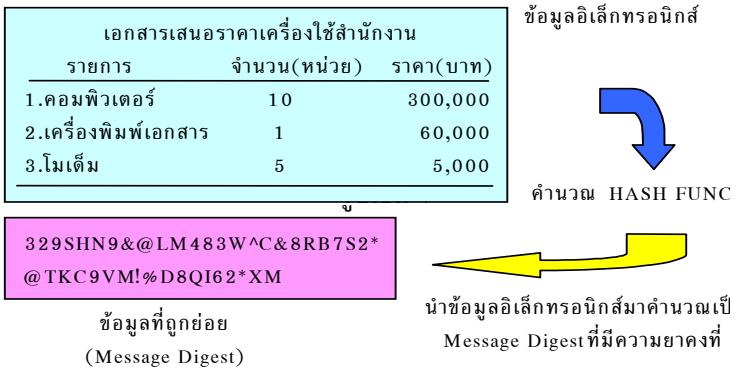


ภาพแสดงการเก็บกุญแจคู่โดยข้างที่เรียกว่า “กุญแจส่วนตัว”เก็บไว้กับผู้ขอใช้บริการและข้างที่เรียกว่า “กุญแจสาธารณะ” เปิดเผยโดยผู้ประกอบการรับรอง

[52] เช่น สิงคโปร์ เกาหลีใต้ และมาเลเซีย ก็จัดให้มีระบบการจัดเก็บกุญแจส่วนตัวในสมาร์ทการ์ด

(ข) ขั้นตอนการแฮชหรือย่อย (Hash Function)[53]

ในการสร้างลายมือชื่อดิจิทัลนั้น นอกจากจะต้องมีกุญแจคู่แล้ว ก่อนสร้างลายมือชื่อดิจิทัลก็มีขั้นตอนสำคัญในการนำข้อมูลอิเล็กทรอนิกส์ที่ผู้ส่งข้อมูลประสงค์จะส่งให้แก่ผู้รับข้อมูลนำมาคำนวณด้วยกระบวนการทางคณิตศาสตร์ (Algorithm) ที่เรียกว่า "ขั้นตอนการแฮช (Hash Function)"[54] หรือ One-way cryptography หรือ One-way hash function[55] เพื่อย่อยหรือทำให้ข้อมูลอิเล็กทรอนิกส์นั้นมีขนาดเล็กลงอันจะทำให้ง่ายต่อการคำนวณทางคณิตศาสตร์และการจัดส่งให้ผู้รับข้อมูลในขั้นตอนต่อไป ผลลัพธ์ที่ได้จากขั้นตอนการแฮช จะทำให้ได้ข้อมูลที่ย่อย (Message Digest) ซึ่งมีขนาดเล็กลงและคงที่ (Fixed Length)



ภาพแสดงขั้นตอนการแฮชหรือย่อยข้อมูลอิเล็กทรอนิกส์

---

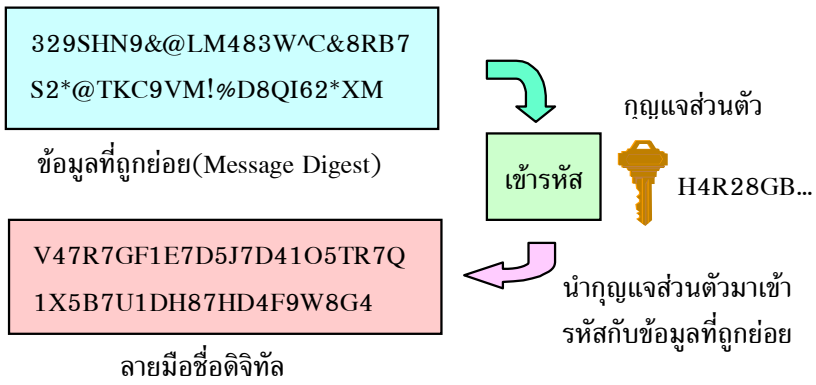
[53] ศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน ใช้คำแปลว่า "ฟังก์ชันแบบแฮช", หน้า 67

[54] เพิ่งอ้างหน้า 6 7

[55] United Nations Commission on International Trade Law Working Group on Electronic Commerce, Thirty- eighth session New York, 12-23 March 2001, A/CN.9/WG.IV/WP.88, p.19 para.40

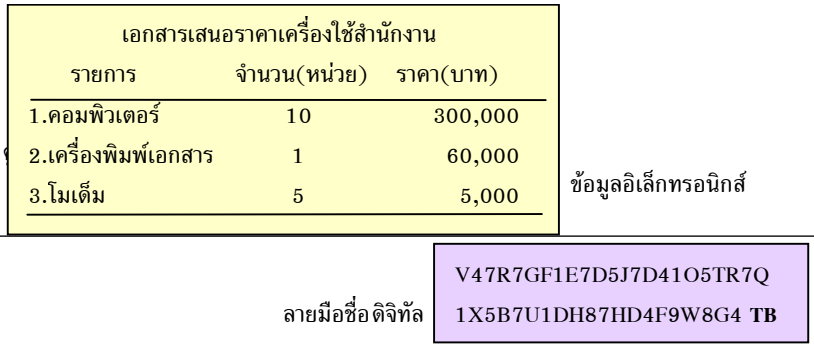
(ค) การสร้างลายมือชื่อดิจิทัล

หลังจากนั้นก็นำกุญแจส่วนตัวมาทำการเข้ารหัสกับข้อมูลที่แฮชหรือย่อย (Message Digest) ซอฟต์แวร์ก็จะทำการแปลงข้อมูลอิเล็กทรอนิกส์เหล่านั้น ให้เป็นลายมือชื่อดิจิทัล (Digital Signature) และลายมือชื่อดิจิทัลนั้นก็จะมีลักษณะเฉพาะที่สัมพันธ์กับข้อมูลแฮช และกุญแจส่วนตัว กล่าวคือ ทุกครั้งที่ข้อมูลแฮชหรือกุญแจส่วนตัวเปลี่ยนแปลงไปจากเดิม ลายมือชื่อดิจิทัลที่ได้ก็จะเปลี่ยนแปลงตามไปด้วย ลายมือชื่อดิจิทัลจึงไม่มีโอกาสซ้ำกันเลย



ภาพแสดงขั้นตอนการสร้างลายมือชื่อดิจิทัล

หลังจากสร้างลายมือชื่อดิจิทัลแล้ว ซอฟต์แวร์ก็จะทำการนำลายมือชื่อดิจิทัลที่ได้นั้นไปแนบไว้ท้ายข้อความที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์เพื่อใช้ส่งให้กับผู้รับข้อมูลต่อไป และเพื่อประโยชน์ในการตรวจสอบตัวบุคคลโดยปกติซอฟต์แวร์ก็จะถูกตั้งโปรแกรมให้แนบกุญแจสาธารณะและใบรับรองกุญแจสาธารณะของผู้ส่งข้อมูลไปกับข้อมูลอิเล็กทรอนิกส์พร้อมด้วยลายมือดิจิทัลด้วย เพื่อความสะดวกของผู้รับข้อมูลในการตรวจสอบลายมือชื่อดิจิทัลนั้น

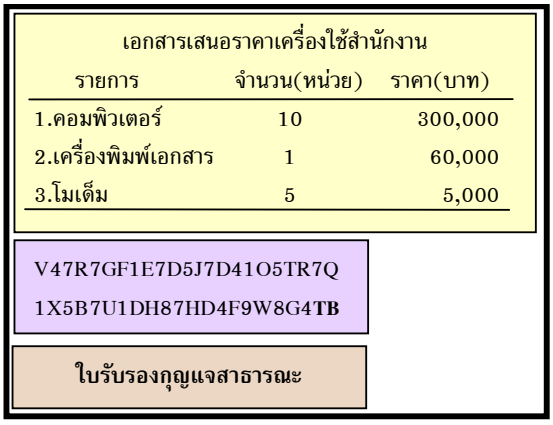


ดังนั้น ในการส่งข้อมูลอิเล็กทรอนิกส์โดยแนบลายมือชื่อดิจิทัลไปด้วยนั้น ก็จะประกอบด้วยข้อมูลอิเล็กทรอนิกส์ถึง 3 ส่วนได้แก่

(1) ส่วนแรก คือข้อมูลอิเล็กทรอนิกส์ที่มีข้อความเดิมซึ่งใช้ในการติดต่อสื่อสารระหว่างบุคคลอันเป็นข้อความที่อ่านออกและเข้าใจได้

(2) ส่วนที่สองเป็นลายมือชื่อดิจิทัล และ

(3) ส่วนสุดท้ายจะเป็นกุญแจสาธารณะพร้อมใบรับรองกุญแจสาธารณะของผู้ลงลายมือชื่อดิจิทัล

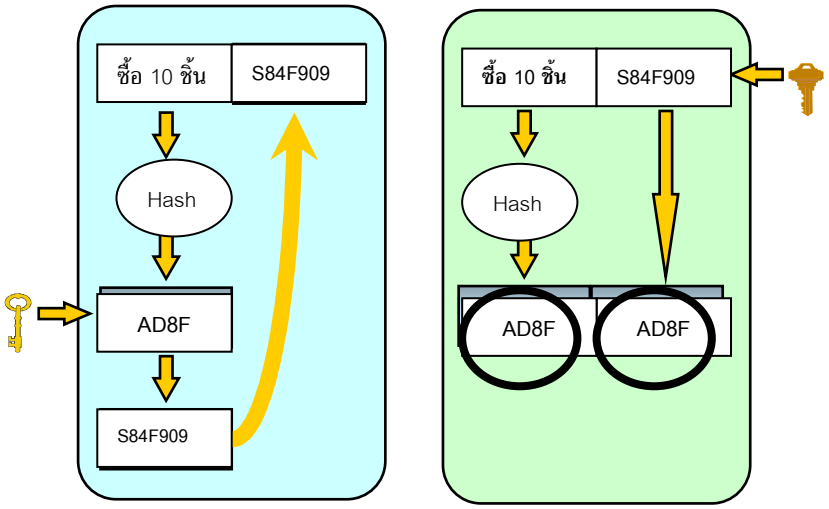


ภาพแสดงข้อมูลอิเล็กทรอนิกส์ที่มีการลงลายมือชื่อดิจิทัล

(2) การตรวจสอบลายมือชื่อดิจิทัล

เมื่อผู้รับข้อมูลได้ข้อมูลอิเล็กทรอนิกส์ที่มีการใช้ลายมือชื่อดิจิทัลเพื่อยืนยันตัวผู้ส่งข้อมูลมาด้วย หากผู้รับข้อมูลประสงค์จะตรวจสอบข้อมูลก็ทำได้โดยนำกุญแจสาธารณะของผู้ส่งข้อมูลมาเข้ารหัสกับลายมือชื่อดิจิทัล และเนื่องจากกุญแจสาธารณะนั้นมีความสัมพันธ์กับกุญแจส่วนตัว เมื่อดำเนินการตามกระบวนการทางคณิตศาสตร์ก็จะถอดรหัสออกมาและได้ผลลัพธ์ในรูปของ “ข้อมูลแฮช” หรือ “ข้อมูลที่

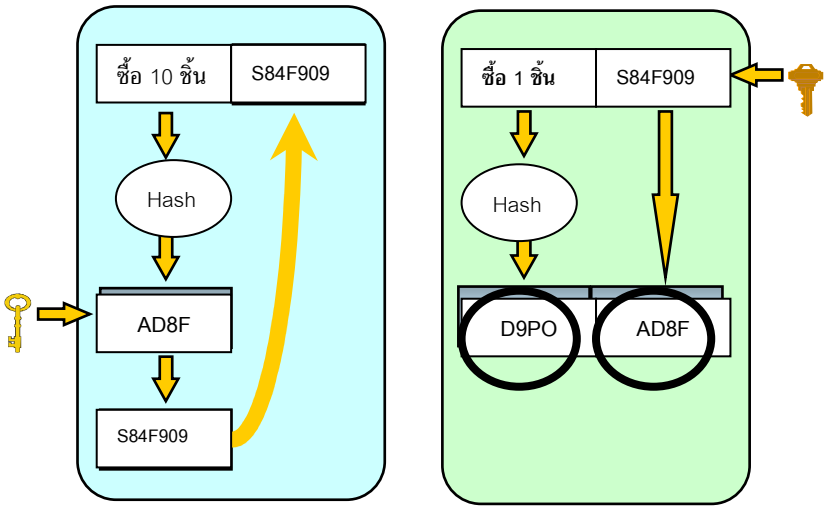
ย่อย” ในขณะเดียวกันข้อความที่ส่งมาในรูปของข้อมูลอิเล็กทรอนิกส์นั้นก็จะถูกย่อยด้วยกระบวนการทางคณิตศาสตร์เช่นกันซึ่งจะได้ผลลัพธ์เช่นกัน คือ “ข้อมูลแฮช” หรือ “ข้อมูลที่ย่อย” และหากว่า “ข้อมูลแฮช” หรือ “ข้อมูลที่ย่อย” ออกมาตรงกัน ก็เป็นบทพิสูจน์ว่าบุคคลที่ส่งมาเป็นเจ้าของกุญแจส่วนตัวซึ่งตรวจสอบได้ว่าเป็นผู้นั้นจริง



ภาพแสดงขั้นตอนการสร้างและตรวจสอบลายมือชื่อดิจิทัล
ในกรณีที่ไม่มีการแก้ไขเปลี่ยนแปลงข้อความที่ส่ง

นอกจากประโยชน์ในการระบุตัวบุคคลและตรวจสอบตัวบุคคลข้างต้นแล้ว ประโยชน์อีกประการในการใช้เทคโนโลยีชนิดนี้ ก็คือ การตรวจสอบได้ว่ามีการแก้ไขเปลี่ยนแปลงข้อมูลอิเล็กทรอนิกส์ที่ส่งมาเนื่องจากการทำงานของกุญแจคู่นั้นจะมีความสัมพันธ์กันในเชิงตรรกะ ดังนั้น เมื่อใช้กุญแจส่วนตัวเข้ารหัสกับข้อมูลที่ย่อยก็จะได้ลายมือชื่อดิจิทัลที่มีค่าออกมาคงที่ ในการตรวจสอบตัวบุคคลด้วยกุญแจสาธารณะซึ่งมีความสัมพันธ์กันในเชิงตรรกะก็จะได้ผลลัพธ์เป็นข้อมูลที่ย่อยซึ่งใช้ในการสร้างลายมือชื่อดิจิทัลเดิมนั้น ดังนั้น ในขั้นตอนของการตรวจสอบซึ่งจะต้องมีขั้นตอนในการ

ย่อยข้อความที่อ่านออกและเข้าใจได้เพื่อให้ได้ข้อมูลที่ย่อยและนำมาเปรียบเทียบกับข้อมูลที่ย่อยซึ่งเกิดจากการใช้กุญแจสาธารณะเข้ารหัสกับลายมือชื่อดิจิทัลนั้นต้องได้ข้อมูลที่ย่อยเหมือนกันเสมอ หากได้ค่าไม่เหมือนกันแสดงว่ามีการเปลี่ยนแปลงแก้ไขข้อความนั้น



ภาพแสดงขั้นตอนการสร้างและตรวจสอบลายมือชื่อดิจิทัล ในกรณีที่มีการแก้ไขเปลี่ยนแปลงข้อความที่ส่ง

ดังนั้น การใช้ระบบกุญแจคู่เพื่อสร้างลายมือชื่อดิจิทัลและตรวจสอบลายมือชื่อดิจิทัลจึงมีประโยชน์อีกประการหนึ่งในการตรวจสอบได้ว่ามีการแก้ไขเปลี่ยนแปลงข้อความที่ส่งมาให้แก่ผู้รับข้อมูลหรือไม่

(3) สรุปกระบวนการสร้างและตรวจสอบลายมือชื่อดิจิทัล

ก. สร้างกุญแจคู่

ข. เตรียมข้อมูลอิเล็กทรอนิกส์ที่ต้องการส่ง เช่น อาจอยู่ในรูปของ e-mail

ค. เตรียมข้อมูลอิเล็กทรอนิกส์ที่ต้องการส่งให้อยู่ในรูปของข้อมูลที่ถูกย่อย (message digest) โดยผ่านกระบวนการแฮช (hash function)

ง. ผู้ส่งเข้ารหัสข้อมูลที่ถูกย่อยด้วยกุญแจส่วนตัวโดยผ่านกระบวนการทางคณิตศาสตร์ ออกมาเป็นลายมือชื่อดิจิทัล ดังนั้น ลายมือชื่อดิจิทัลจึงประกอบด้วยข้อมูลที่ถูกย่อยที่นำมาเข้ารหัสกับกุญแจส่วนตัว

จ. นำลายมือชื่อดิจิทัลมาแนบท้าย หรือแนบติดกับข้อมูลอิเล็กทรอนิกส์ที่ต้องการส่ง

ฉ. ผู้ส่งทำการส่งลายมือชื่อดิจิทัล และข้อมูลอิเล็กทรอนิกส์ ไม่ว่าข้อมูลอิเล็กทรอนิกส์นั้นจะมีการเข้ารหัสลับหรือไม่ก็ตาม ไปให้กับผู้รับโดยทางสื่ออิเล็กทรอนิกส์

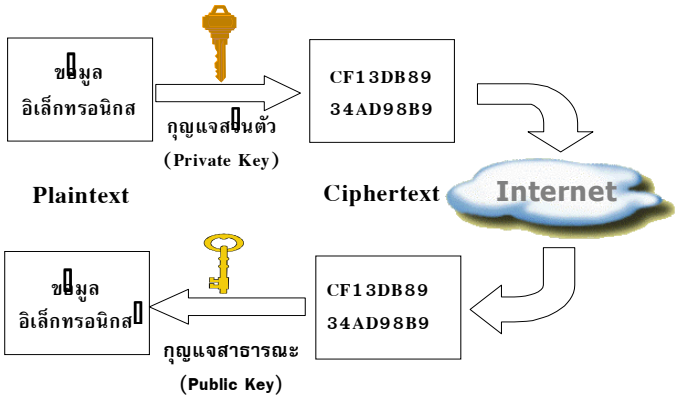
ช. ผู้รับใช้กุญแจสาธารณะของผู้ส่งในการตรวจสอบลายมือชื่อดิจิทัลของผู้ส่ง ซึ่งการตรวจสอบโดยการใช้กุญแจสาธารณะของผู้ส่งนั้นเป็นการรับรองในทางเทคนิคในระดับหนึ่งว่าข้อมูลอิเล็กทรอนิกส์มาจากผู้ส่งจริง

ซ. ผู้รับนำข้อมูลอิเล็กทรอนิกส์ที่ได้รับมาผ่านกระบวนการย่อยเพื่อให้ออกมาเป็นข้อมูลที่ถูกย่อย (message digest)

ฌ. ผู้รับนำข้อมูลที่ถูกย่อยทั้ง 2 ข้อมูลมาเปรียบเทียบกัน ถ้าข้อมูลที่ถูกย่อยทั้งสองข้อมูลเหมือนกันแสดงว่าข้อมูลอิเล็กทรอนิกส์ตั้งแต่ต้นไม่มีการเปลี่ยนแปลงนับแต่เวลาที่ลงลายมือชื่อแล้ว แต่หากที่การเปลี่ยนแปลงข้อมูลอิเล็กทรอนิกส์ดังกล่าวแม้เพียง 1 บิต (bit) นับแต่เวลาที่ลงลายมือชื่อแล้ว ข้อมูลย่อยที่ผู้รับสร้างขึ้นจะแตกต่างจากข้อมูลที่ถูกย่อยที่ผู้ส่งสร้างขึ้น

ญ. ในกรณีที่มีการใช้กระบวนการการรับรอง (certification process) ผู้รับได้รับใบรับรองจากผู้ประกอบการรับรอง (CA) (หรือจากผู้ส่งหรือจากที่อื่น) ซึ่งใช้ยืนยันลายมือชื่อดิจิทัลในข้อมูลอิเล็กทรอนิกส์ของผู้ส่ง

(4) **การเข้ารหัสลับข้อมูล** (Encryption) ในกรณีต้องการส่งข้อมูลไปยังผู้รับ โดยไม่ต้องการให้ผู้อื่นสามารถเปิดอ่านข้อความได้ ก็สามารถใช้เทคโนโลยีการเข้ารหัสลับ (Encryption Technology) เพื่อรักษาความลับของข้อมูลอิเล็กทรอนิกส์โดยการนำกุญแจสาธารณะของผู้รับข้อมูลมาเข้ารหัสกับข้อมูลอิเล็กทรอนิกส์ที่ต้องการส่งไป เมื่อผู้รับได้รับข้อมูลนั้นแล้วก็สามารถถอดรหัสได้แต่เพียงผู้เดียวโดยใช้กุญแจส่วนตัวที่ตนเก็บไว้เป็นความลับ แม้จะมีผู้อื่นในระบบได้รับข้อความนั้นด้วยก็ตามเนื่องจากกุญแจส่วนตัวจะถูกเก็บไว้เป็นความลับไม่เปิดเผยให้ผู้อื่นทราบ เรียกวิธีการเช่นนี้ว่า การเข้ารหัสลับข้อมูล (Data Message encryption)



ภาพแสดงขั้นตอนการเข้ารหัสเพื่อรักษาความลับของข้อมูล

2.2.5 คุณสมบัติของเทคโนโลยีแต่ละชนิด

จากที่ได้อธิบายมาแล้วในตอนต้นจะเห็นได้ว่า ปัจจุบันได้มีการพัฒนาด้านเทคโนโลยีเกี่ยวกับการรักษาความปลอดภัยของข้อมูลหลายรูปแบบเพื่อประโยชน์ในการติดต่อสื่อสารบนเครือข่าย โดยเทคโนโลยีแต่ละชนิดอาจมีคุณสมบัติแตกต่างกัน ไม่ว่าจะเป็นคุณสมบัติในการระบุตัวบุคคล (Authentication) การรักษาความถูกต้องสมบูรณ์ของข้อมูล (Integrity) การป้องกันการปฏิเสธความรับผิด (Non-repudiation) หรือการรักษาความปลอดภัยของข้อมูล (Confidentiality) อย่างไรก็ตาม จะเห็นได้ว่า เทคโนโลยีระบบการเข้ารหัสแบบอสมมาตรโดยใช้โครงสร้างพื้นฐานของกุญแจสาธารณะหรือ PKI ในการสร้างลายมือชื่อดิจิทัลนั้น มีคุณสมบัติทั้งในด้านการระบุตัวบุคคล (Authentication) และป้องกันการปฏิเสธความรับผิดชอบ (Non-repudiation) รักษาความแท้จริงของข้อมูล (Integrity) หากใช้วิธีการเข้ารหัสแบบลายมือชื่อดิจิทัล รวมทั้งใช้ในการรักษาความลับของข้อมูล (Confidentiality) หากใช้วิธีการเข้ารหัสลับข้อมูล ในขณะที่เทคโนโลยีอื่นอาจไม่มีคุณสมบัติที่เท่าเทียมกับเทคโนโลยีระบบการเข้ารหัสแบบอสมมาตร ซึ่งคุณสมบัติของเทคโนโลยีแต่ละชนิดปรากฏตามตารางต่อไปนี้

คุณสมบัติ / เทคโนโลยี	การระบุตัวบุคคล	การรักษาความลับของข้อมูล	ความครบถ้วนสมบูรณ์	การป้องกันการปฏิเสธความรับผิด	การพิสูจน์ร่วมกับปัจจัยอื่น
ID Password	✔				✔
E-Mail Address	✔				✔
Biometrics	✔			✔	✔
Encryption		✔			
Digital Signature	✔		✔	✔	

ภาพแสดงคุณสมบัติของเทคโนโลยีแต่ละชนิด

2.2.6 เทคโนโลยี P K I และผู้ประกอบการรับรอง

ในการตรวจสอบลายมือชื่อดิจิทัลนั้น ผู้ตรวจสอบจะต้องสามารถเข้าถึงกุญแจสาธารณะของผู้ลงลายมือชื่อ และจะต้องมั่นใจได้ว่ากุญแจสาธารณะนั้นสัมพันธ์กับกุญแจส่วนตัวของผู้ลงลายมือชื่อ อย่างไรก็ตามเป็นที่ทราบกันดีอยู่แล้วว่ากุญแจส่วนตัวและกุญแจสาธารณะนั้นไม่ได้มีความสัมพันธ์ใด ๆ กับบุคคลเพราะกุญแจส่วนตัวและกุญแจสาธารณะเป็นเพียงตัวเลขที่ถูกสร้างขึ้นมาเท่านั้น ด้วยเหตุนี้กลไกการทำงานจึงต้องสร้างความน่าเชื่อถือระหว่างบุคคลกับกุญแจคู่ และเพื่อให้กุญแจสาธารณะบรรลุวัตถุประสงค์ของการใช้งานจึงจำเป็นที่จะต้องทำให้บุคคลอื่น ๆ สามารถหาหรือเข้าถึงกุญแจสาธารณะได้โดยง่าย แม้ว่าบุคคลเหล่านั้นจะไม่เคยรู้จักผู้สร้างลายมือชื่อหรือไม่เคยมีความสัมพันธ์ใด ๆ กันมาก่อน ด้วยเหตุดังกล่าวคู่สัญญาจึงจำเป็นที่จะต้องให้ความเชื่อถือในกุญแจคู่ที่ถูกสร้างขึ้นมานั้น

ความน่าเชื่อถือระหว่างคู่สัญญาอาจเกิดขึ้นจากการที่คู่สัญญาเชื่อถือซึ่งกันและกัน เช่น เคยติดต่อกันมาก่อน เคยสื่อสารกันในระบบปิด (closed-system) หรืออื่น ๆ ซึ่งในการทำธุรกรรมระหว่างบุคคล 2 ฝ่ายที่มีความเชื่อถือระหว่างกันนั้นการติดต่อสื่อสารเพื่อให้อีกฝ่ายทราบกุญแจสาธารณะของตนสามารถทำได้โดยง่าย อย่างไรก็ตาม วิธีเดียวกันอาจทำไม่ได้หรือทำได้ยากหากบุคคล 2 ฝ่ายไม่ได้ติดต่อกันบ่อยครั้ง ติดต่อสื่อสารกันในระบบเปิด (เช่น อินเทอร์เน็ต) ไม่เคยมีข้อตกลงใด ๆ กันมาก่อน หรือไม่เคยมีกฎหมายใดที่กำหนดความสัมพันธ์ระหว่างบุคคล 2 ฝ่ายนั้นไว้

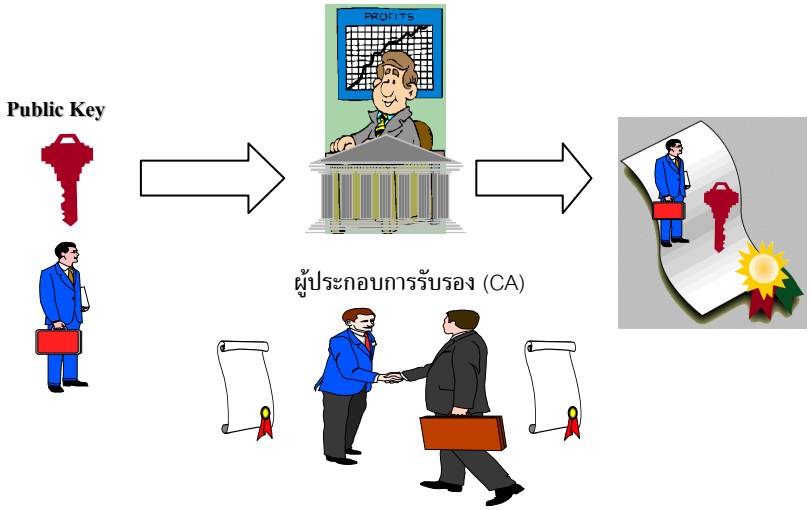
นอกจากนี้ ด้วยเหตุที่ระบบกุญแจคู่เป็นเทคโนโลยีที่ใช้กระบวนการทางคณิตศาสตร์ขั้นสูง ดังนั้น ผู้ใช้จะต้องเชื่อถือในทักษะ ความรู้ และการจัดการระบบกุญแจคู่ของคู่สัญญาที่สร้างกุญแจส่วนตัวและกุญแจสาธารณะนั้นขึ้น

การแก้ปัญหาต่าง ๆดังที่กล่าวมาข้างต้นวิธีหนึ่งคือการใช้บุคคลที่สามในการกำหนดความเกี่ยวเนื่องระหว่างผู้ลงลายมือชื่อกับกุญแจสาธารณะ โดยบุคคลที่สามนี้

โดยทั่วไปเรียกกันว่า “ผู้ประกอบการรับรอง” (Certification Authority หรือ Certification service provider หรือ Supplier of certification services)

(1) ผู้ประกอบการรับรอง (Certification Authority)

เป็นบุคคลฝ่ายที่สามทำหน้าที่สร้างกุญแจคู่ตามคำขอของผู้ขอใช้บริการออกใบรับรองยืนยันตัวบุคคลผู้ขอใช้บริการ จัดเก็บกุญแจสาธารณะในฐานข้อมูล เปิดเผยกุญแจสาธารณะต่อสาธารณชนที่ติดต่อทางเครือข่าย ยืนยันตัวบุคคลที่เป็นเจ้าของกุญแจสาธารณะตามคำขอของบุคคลทั่ว ๆ ไปและให้บริการอื่น ๆ ที่เกี่ยวข้อง

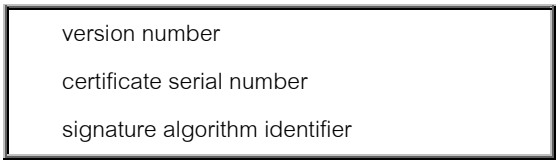


(ก)ใบรับรอง (Certificates)

ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างจากเทคโนโลยีการเข้ารหัสแบบอสมมาตรโดยอาศัยโครงสร้างพื้นฐานของกุญแจสาธารณะที่เรียกว่าลายมือชื่อดิจิทัลนั้น เมื่อส่งข้อความที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์พร้อมลายมือชื่อดิจิทัลไปยัง

ผู้รับจะสามารถตรวจสอบความถูกต้อง โดยใช้กุญแจสาธารณะของผู้ส่งซึ่งแสดงอยู่ในใบรับรอง (Certificate) ซึ่งส่วนใหญ่จะเก็บไว้ในฐานข้อมูลของผู้ประกอบการรับรอง (Repository) และเปิดเผยเพื่อให้ประชาชนทั่วไปสามารถนำกุญแจสาธารณะนั้นไปตรวจสอบได้

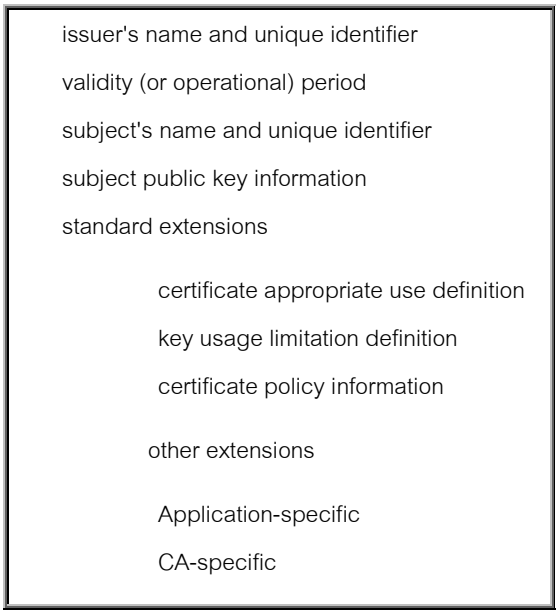
รูปแบบใบรับรองซึ่งเป็นที่ยอมรับโดยทั่วไปในปัจจุบัน ได้แก่ รูปแบบใบรับรองที่กำหนดมาตรฐานไว้โดย ITU (International Telecommunication Union) คือ มาตรฐาน X.509[56] ทั้งนี้ เนื่องจากกำหนดรายละเอียดต่าง ๆ ที่นิยมใช้กันอย่างแพร่หลาย[57] และสามารถประยุกต์ใช้กับโปรแกรมหรือสามารถนำมาประยุกต์ใช้ในการแลกเปลี่ยนใบรับรอง ปัจจุบันมาตรฐานที่ได้รับความนิยมอย่างแพร่หลายคือ มาตรฐาน X.509 Version 3[58] ซึ่งมีรายละเอียดต่าง ๆ อาทิ หมายเลขของใบรับรอง ชื่อและนามสกุลของผู้ถือใบรับรอง กุญแจสาธารณะของผู้ถือใบรับรอง อายุของใบรับรอง วิธีการตรวจสอบลายมือชื่อดิจิทัล ชื่อผู้ประกอบการรับรอง ลายมือชื่อดิจิทัลของผู้ประกอบการรับรอง ดังปรากฏรายการตามภาพต่อไปนี้



[56] Gary C.Kessler, An Overview of Cryptography, รายละเอียดเพิ่มเติม สืบค้นได้ที่ http://www.garykessler.net/library/crypto.html หรือ Diffie, W. and Hellman, M. E., "New directions in cryptography." *IEEE Transactions on Information Theory*, 22(1976), pp. 644-654.

[57] ตัวอย่างกฎหมายบางประเทศที่กำหนดเกี่ยวกับมาตรฐานใบรับรองได้แก่ Section 7 ของ Information Technology (Certifying Authorities) Rules, 2000. ประเทศอินเดีย, Section 24 ของ Electronic Transactions (Certification Authority) Regulations 1999 Singapore เป็นต้น

[58] ITU-T Recommendation X.509, June 1997, Adopted August 1997.



ที่มา : An Overview of Cryptography **โดย** Gary C. Kessler

ผู้ประกอบการรับรองสามารถออกใบรับรองได้หลายประเภท โดยจะขึ้นอยู่กับปัจจัยหลายประการ เช่น การนำใบรับรองไปใช้ ขนาดของกุญแจ วิธีการสร้างและตรวจสอบลายมือชื่อ และขอบเขตความรับผิดของผู้ประกอบการรับรอง เป็นต้น กล่าวคือ สำหรับผู้ประกอบการรายหนึ่ง ผู้นั้นอาจจะกำหนดระดับของใบรับรองเป็นสามประเภท คือ สำหรับธุรกรรมที่มีมูลค่าไม่เกิน 500 **บาท** 5,000 **บาท และ** 100,000 **บาท ตามลำดับ**

ในกฎหมายหลายประเทศมักจะกำหนดรายละเอียดต่างๆ ที่เกี่ยวข้องกับใบรับรองไว้ในกฎหมาย เช่น ประเทศมาเลเซีย ได้กำหนดรายละเอียดต่างๆ ของใบรับรองไว้ใน Digital Signature Regulation 1998[59] **ซึ่งออกตามความใน** Digital Signature Act 1997 **หรือ** Information Technology (Certifying

[59] Section 37 ,38

Authorities) Rules 2000[60] ของประเทศอินเดีย ซึ่งออกตามความใน Information Technology Act 2000

(ข) ประเภทของบริการใบรับรองอิเล็กทรอนิกส์ [61]

การแบ่งประเภทหรือระดับของใบรับรองนั้น โดยทั่วไปเป็นกรณีที่ผู้ประกอบการรับรอง (C A) แต่ละรายจะเป็นผู้กำหนดเอง

ใบรับรองอิเล็กทรอนิกส์สำหรับบุคคล

เหมาะสำหรับบุคคลทั่วไปที่ต้องการติดต่อสื่อสารผ่านเครือข่ายคอมพิวเตอร์แบบปลอดภัย โดยแบ่งระดับความปลอดภัยออกเป็น 2 ระดับ กล่าวคือ แบบธรรมดา ซึ่งกุญแจส่วนตัวถูกเก็บในระบบคอมพิวเตอร์ของผู้ใช้ และแบบพิเศษ ซึ่งกุญแจส่วนตัวถูกเก็บบนสมาร์ทการ์ด

ใบรับรองอิเล็กทรอนิกส์สำหรับเว็บไซต์

เหมาะสำหรับหน่วยงานที่ต้องการสร้างความเชื่อมั่นในการเผยแพร่ข้อมูลแก่บุคคลทั่วไปผ่านเครือข่ายคอมพิวเตอร์ ว่าข้อมูลดังกล่าวมาจากเว็บไซต์ของหน่วยงานนั้นจริง นอกจากนี้ยังสามารถใช้ในการสร้างช่องทางสื่อสารแบบปลอดภัยระหว่างเว็บไซต์กับบุคคลทั่วไปได้อีกด้วย

ใบรับรองอิเล็กทรอนิกส์สำหรับบุคคลในองค์กร

เหมาะสำหรับองค์กรที่ต้องการใช้เทคโนโลยีกุญแจสาธารณะในการรักษาความปลอดภัยของข้อมูลที่สื่อสารผ่านเครือข่ายคอมพิวเตอร์ เช่น อินเทอร์เน็ต (Internet) อินทราเน็ต (Intranet) หรือ เอ็กซ์ทราเน็ต (Extranet) โดยที่องค์กรสามารถออกใบรับรองอิเล็กทรอนิกส์ส่วนตัวเองโดยใช้ระบบของผู้ประกอบการรับรอง

---

[60] Section 7

[61] **ที่มา** http://www.nectec.or.th , http://gits.net.th

2.3 ความหมายของลายมือชื่ออิเล็กทรอนิกส์

ดังที่ได้กล่าวมาแล้วว่าคำว่า "ลายมือชื่ออิเล็กทรอนิกส์" ตามพระราชบัญญัตินี้เป็นคำที่มีความหมายกว้าง เพื่อให้สามารถรองรับลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นด้วยวิธีการทางอิเล็กทรอนิกส์ทุกประเภท ทั้งแบบที่สร้างขึ้นด้วยวิธีการง่ายๆ หรือสร้างขึ้นด้วยวิธีการที่ซับซ้อน กล่าวคือ เจ้าของลายมือชื่ออาจจะกำหนดเพียงแค่ตัวอักษรเพียงไม่กี่ตัวต่อท้ายข้อความในจดหมายอิเล็กทรอนิกส์ที่ตนเขียนขึ้นและส่งให้แก่ผู้รับข้อความเพื่อแสดงตัวตนว่าเป็นผู้ส่งข้อความนั้น หรืออาจจะใช้ "ลายมือชื่อดิจิทัล" ซึ่งเป็นลายมือชื่ออิเล็กทรอนิกส์ประเภทหนึ่งที่สร้างขึ้นโดยอาศัยวิธีการซับซ้อนทางเทคโนโลยีเพื่อระบุตัวผู้ส่งข้อมูลให้ผู้รับข้อมูลทราบก็ได้

นอกจากรูปแบบในการสร้างลายมือชื่ออิเล็กทรอนิกส์ที่อาจจะแตกต่างกันแล้ว สิ่งซึ่งใช้แทนลายมือชื่ออิเล็กทรอนิกส์ก็เปิดกว้างรองรับสิ่งใดก็ได้ที่สร้างขึ้นด้วยวิธีการทางอิเล็กทรอนิกส์ ทั้งนี้ โดยอาจเป็น "ตัวอักษร[62] อักขระ[63] ตัวเลข เสียง หรือสัญลักษณ์อื่นใด" ซึ่งใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ในการทำหน้าที่ยืนยันตัวบุคคล

---

[62] พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2525 ใช้คำแปลว่า "ตัวหนังสือ ,วิชาหนังสือ" ราชบัณฑิตยสถาน. พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2525, พิมพ์ครั้งที่ 6 (กรุงเทพฯ : อักษรเจริญทัศน์) ,หน้า 929

[63] หนังสือคอมพิวเตอร์กับภาษาไทย : การพัฒนามาตรฐานเบื้องต้นสำหรับเทคโนโลยีสารสนเทศของไทย ใช้คำแปลว่า "ตัวอักษร ตัวเลข เครื่องหมายพิเศษ และเครื่องหมายอื่นใดรวมทั้งอักขระควบคุมที่สามารถป้อนบันทึกลงสื่อและแสดงผลทางเครื่องคอมพิวเตอร์ได้" ,ทวีศักดิ์ กออนันตกูล และคณะทำงานร่างข้อกำหนดร่วมเพื่อการเขียนโปรแกรมซึ่งแสดงผลเป็นภาษาไทย (Thai API Comsortium),คอมพิวเตอร์กับภาษาไทย : การพัฒนามาตรฐานเบื้องต้นสำหรับเทคโนโลยีสารสนเทศของไทย,พิมพ์ครั้งที่ 1 (กรุงเทพฯ : โรงพิมพ์สารมวลชน) , หน้า 41

ตัวอย่างของลายมือชื่ออิเล็กทรอนิกส์อาจจะหมายความรวมถึง [64]

(1) ชื่อหรือสัญลักษณ์ของบุคคลซึ่งพิมพ์ไว้ท้ายเนื้อความของจดหมายอิเล็กทรอนิกส์

(2) รูปภาพดิจิทัลของลายเซ็นซึ่งแนบไปกับเอกสารอิเล็กทรอนิกส์ ที่อาจจะสร้างขึ้นโดยเทคโนโลยี Biometrics ซึ่งเรียกว่า Signature Dynamics รหัสลับหรือ PIN (เลขที่บัตร ATM และบัตรเครดิต) ทั้งนี้ เพื่อที่จะระบุตัวผู้ส่งข้อมูลอิเล็กทรอนิกส์ต่อผู้รับ

(3) รหัสที่ผู้ส่งข้อมูลอิเล็กทรอนิกส์ใช้ในการระบุตัวเอง

(4) การสแกนลายพิมพ์นิ้วมือหรือม่านตา

(5) ลายมือชื่อดิจิทัล

ทั้งนี้ เหตุที่พระราชบัญญัติฉบับนี้ให้ความหมายของคำว่า "ลายมือชื่ออิเล็กทรอนิกส์" ไว้กว้างก็เพื่อให้เป็นไปตาม "หลักความเป็นกลางทางเทคโนโลยี (Technology neutrality)" รวมทั้งเพื่อให้ทันกับพัฒนาการทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็วและมีความซับซ้อนเพิ่มขึ้นเรื่อย ๆ รวมทั้งเปิดกว้างสำหรับการใช้เทคโนโลยีทุกรูปแบบในการสร้างลายมือชื่ออิเล็กทรอนิกส์ อาทิ เทคโนโลยีชีวภาพ เทคโนโลยี P K I [65] เป็นต้น

อย่างไรก็ตาม กฎหมายหลาย ๆ ประเทศก็ได้ให้ความหมายของ "ลายมือชื่ออิเล็กทรอนิกส์" แตกต่างกันไป อาทิ

---

[64] Thomas J. Smedinghoff and Ruth Hill Bro, Moving With Change: Electronic Signature Legislation as a Vehicle for Advance e-Commerce.

[65] โปรดดูรายละเอียดเกี่ยวกับเทคโนโลยี P K I ในข้อ 2 . 2 . 4

(ก) **กฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ของสหประชาชาติ** Article 2 **ได้ให้ความหมายไว้ว่า** "Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message;[66]

(ข) Electronic Transactions Act **1998 ของประเทศสิงคโปร์ได้ให้ความหมายไว้ใน** Section **2 ว่า** "electronic signature means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record"

(ค) Electronic Commerce Act of **2000 ของประเทศฟิลิปปินส์ได้ให้ความหมายไว้ใน** Section **5 ว่า** "Electronic signature" refers to any distinctive mark, characteristic and/or sound in electronic form, representating the identity of a person and attached to or logically associated with the electronic data message or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic document.

(ง) กฎหมายสหรัฐอเมริกา กล่าวคือ Electronic Signatures in Global and National Commerce Act **ได้ให้ความหมายไว้ใน** Section **106 ว่า** "The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

---

[66] **โปรดดู** http://www.uncitral.org/...

หากพิจารณาการให้ความหมายคำนิยามของประเทศต่าง ๆ ข้างต้นจะพบว่า แม้จะมีการให้ความหมายแตกต่างกันบ้าง แต่ก็ครอบคลุมถึงองค์ประกอบสำคัญ 2 ประการ ของลายมือชื่ออิเล็กทรอนิกส์ กล่าวคือ ลายมือชื่ออิเล็กทรอนิกส์นั้นต้องสร้างขึ้นมาเพื่อใช้ในการระบุตัวบุคคล และแสดงว่าบุคคลนั้นยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์

2.4 ประเภทของลายมือชื่ออิเล็กทรอนิกส์

ตามพระราชบัญญัติฉบับนี้ อาจแบ่งลายมือชื่ออิเล็กทรอนิกส์ออกได้เป็น 2 ประเภท กล่าวคือ

2.4.1 ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป

ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป คือ ลายมือชื่อที่เป็นไปตามมาตรา 9 ของพระราชบัญญัติ อันเป็นหลักการที่เปิดกว้างรองรับวิธีการทุกประเภทที่อาจนำมาใช้ในลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ได้ โดยมาตรา 9 ได้วางหลักการสำคัญไว้ดังนี้

"ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(2) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี"

หลักเกณฑ์ตามมาตรา 9 บัญญัติขึ้นรับรองความเท่าเทียมกันระหว่างลายมือชื่ออิเล็กทรอนิกส์และลายมือชื่อที่ลงนามหรือเซ็นโดยบุคคลธรรมดา ซึ่งแบ่งออกเป็น

2 ส่วน ส่วนแรกเพื่อระบุตัวบุคคลผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ ส่วนที่สองได้กล่าวถึงความเห็นชอบของบุคคลในการรับรองข้อความที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ทั้งนี้ วิธีการดังกล่าวต้องเป็นวิธีการที่เชื่อถือได้ โดยคำว่า "วิธีการที่เชื่อถือได้" นี้ให้คำนึงถึงพฤติการณ์ที่เหมาะสมในการกำหนดวิธีการที่น่าเชื่อถือในการระบุตัวเจ้าของลายมือชื่อด้วย อาทิ ความเหมาะสมและความชอบด้วยกฎหมาย ความมีประสิทธิภาพหรือความซับซ้อนของเครื่องมือหรืออุปกรณ์ที่นำมาใช้ ลักษณะของกิจกรรมทางการค้า ความสม่ำเสมอในการทำธุรกรรมของคู่กรณี ประเภทและขนาดของธุรกรรม กฎหมายที่กำหนดให้มีการลงลายมือชื่อ ศักยภาพของของระบบการติดต่อสื่อสาร การปฏิบัติตามขั้นตอนในการใช้ลายมือชื่อเพื่อระบุตัวบุคคล การปฏิบัติตามประเพณีและทางปฏิบัติในทางการค้า ความสำคัญและประโยชน์เชิงเศรษฐกิจของข้อมูลอิเล็กทรอนิกส์ การจัดให้มีทางเลือกอื่นสำหรับวิธีการที่ใช้ในการใช้ลายมือชื่ออิเล็กทรอนิกส์เพื่อระบุตัวบุคคลและต้นทุนที่เกิดขึ้น ความเป็นไปได้ในการยอมรับหรือไม่ยอมรับวิธีการในการระบุตัวบุคคล ณ ขณะที่มีการตกลงให้ใช้วิธีนั้น หรือ ณ ขณะที่มีการติดต่อสื่อสารกัน และปัจจัยที่เกี่ยวข้องอื่น ๆ [67]

จากเจตนารมย์ของมาตรา 9 นี้เอง ซึ่งกำหนดให้การลงลายมือชื่อจะต้องใช้วิธีการที่เชื่อถือได้ ดังนั้น จึงทำให้มีการกำหนดหลักการเกี่ยวกับวิธีการที่น่าเชื่อถือไว้ใน Article 6 และ 7 ของกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ และการรับรองโดยหน่วยงานของรัฐ (state authority) หน่วยงานภาคเอกชน (a private accredited entity) หรือโดยคู่สัญญาเอง (parties) ซึ่งประโยชน์ในการกำหนดความน่าเชื่อถือทางเทคนิคนี้จะทำให้เกิดความแน่นอนในเทคนิคและเกิดความเชื่อถือในการใช้ลายมือชื่อนั้น

---

[67] References to UNCITRAL documents:., A/CN.9/WG.IV/WP.88, p.27-28 para.75 และ UNCITRAL, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, para.53 and paras.56-58

2.4.2 ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

มาตรา 26 ตามพระราชบัญญัติฯ ได้บัญญัติเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ โดยกฎหมายได้บัญญัติหลักเกณฑ์บางประการ ซึ่งหากเทคโนโลยีใดก็ตามที่มีคุณสมบัติหรือหลักเกณฑ์ตามที่กฎหมายกำหนด ก็ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

หลักการตามมาตรานี้สืบเนื่องมาจากปัจจุบันมีการพัฒนาเทคโนโลยีหลายชนิดเพื่อนำมาใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์ ซึ่งเทคโนโลยีแต่ละชนิดนั้นมีระดับความน่าเชื่อถือ ความปลอดภัยและหลักการในทางเทคโนโลยีที่แตกต่างกัน บางชนิดการทำซ้ำหรือปลอมแปลงสามารถทำได้โดยง่าย ในขณะที่บางชนิดการทำซ้ำหรือการปลอมแปลงอาจทำได้ยากมากหรืออาจต้องใช้ระยะเวลานาน หรือแม้กระทั่งบางชนิดอาจมีคุณสมบัติบางประการที่เทคโนโลยีอื่นไม่มี ด้วยเหตุนี้จึงได้มีการแยกระดับความน่าเชื่อถือของเทคโนโลยีออกจากกันโดยเรียกเทคโนโลยีลายมือชื่ออิเล็กทรอนิกส์ที่มีคุณสมบัติตามที่กฎหมายกำหนดว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

ทั้งนี้ ลักษณะหรือคุณสมบัติในการพิจารณาว่าเทคโนโลยีใด เป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้นั้น ให้พิจารณาจากหลักเกณฑ์ ดังต่อไปนี้

(1) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ได้เชื่อมโยงไปยังเจ้าของลายมือชื่อ โดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(2) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ โดยไม่มีการควบคุมของบุคคลอื่น

(3) การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้ และ

(4) ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรองรับความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

สำหรับคำว่า "ข้อมูลที่ใช้ในการสร้างลายมือชื่อ" นั้น หมายความถึง กุญแจลับ (Secret keys) รหัสลับ (Codes) หรือองค์ประกอบอื่น อันเป็นส่วนสำคัญที่ใช้ในขั้นตอนของการสร้างลายมือชื่อ ซึ่งให้ความเชื่อมโยงที่ปลอดภัยระหว่างผู้สร้างลายมือชื่อและลายมือชื่ออิเล็กทรอนิกส์นั้น[68] ตัวอย่างเช่น การสร้างและใช้ลายมือชื่อดิจิทัลที่วางอยู่บนพื้นฐานของวิทยาการเข้ารหัสแบบอสมมาตร (Asymetric cryptography) นั้น จะมีความเชื่อมโยงระหว่างผู้ลงลายมือชื่อกับกุญแจคู่ที่สร้างขึ้นเท่านั้น เพราะหากใช้กุญแจคู่ที่ไม่ใช่คู่ที่ผู้ลงลายมือชื่อสร้างขึ้นก็จะไม่สามารถยืนยันตัวบุคคลที่สร้างกุญแจคู่นั้นได้ ความเชื่อมโยงระหว่างผู้ลงลายมือชื่อและลายมือชื่ออิเล็กทรอนิกส์ที่ชัดเจนอีกตัวอย่าง ก็คือการใช้เทคโนโลยีชีวภาพ (Biometric devices) ในการระบุตัวบุคคล เช่น การใช้ลายพิมพ์นิ้วมือ หรือฝ่ามือ เป็นต้น ก็ต้องอาศัยลักษณะทางชีวภาพของผู้ลงลายมือชื่อในการตรวจสอบเพื่อยืนยันตัวบุคคลนั้น

เทคโนโลยีบางชนิดนั้นดังที่ได้กล่าวมาแล้วว่า มีคุณสมบัติที่พิเศษไปจากเทคโนโลยีชนิดอื่น ๆ กล่าวคือด้วยกลไกการทำงานทำให้ผู้รับข้อมูลสามารถทราบได้ว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการเปลี่ยนแปลงหรือไม่ภายหลังจากที่มีการลงลายมือชื่อแล้ว เทคโนโลยีดังกล่าวก็คือลายมือชื่อดิจิทัลที่อยู่บนพื้นฐานของระบบกุญแจคู่ ด้วยเหตุนี้ เทคโนโลยีที่มีอยู่ในปัจจุบันที่มีคุณสมบัติหรือลักษณะเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ตามกฎหมายนี้คือ "ลายมือชื่อดิจิทัล" ทั้งนี้ หากในอนาคตมี

---

[68] References to UNCITRAL documents A/CN.9/WG.IV/WP.88, p.34 para.94 และ UNCITRAL, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, A/CN.9/483, paras.65 and 67

เทคโนโลยีชนิดอื่นที่มีคุณสมบัติหรือลักษณะตามที่กฎหมายกำหนดก็อาจถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้เช่นกัน

2.5 หลักการพื้นฐานตามหมวด 2 ของพระราชบัญญัติฯ

พระราชบัญญัติฯ ในหมวดที่ 2 ว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ ได้บัญญัติขึ้นเพื่อเสริมหลักการตามมาตรา 9 กล่าวคือ เพื่อกำหนดแนวทางในการพิจารณาเกี่ยวกับวิธีการที่น่าเชื่อถือซึ่งเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี ทั้งนี้ หลักการพื้นฐานที่สำคัญตามหมวดที่ 2 ของพระราชบัญญัติ มีดังต่อไปนี้

2.5.1 ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ (มาตรา 26)[69]

หลักการตามมาตรา 26 เป็นการกำหนดหลักการสำคัญเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ โดยพิจารณาจากลักษณะตามที่กฎหมายกำหนด ซึ่งเป็นการกำหนดหลักการสำคัญเกี่ยวกับความน่าเชื่อถือในทางเทคนิค (Technical reliability) โดยมีลักษณะที่สำคัญคือ หากข้อมูลที่ใช้ในการสร้างลายมือชื่อนั้นเชื่อมโยงเป็นการเฉพาะกับผู้สร้างลายมือชื่อ ข้อมูลที่ใช้ในขณะที่สร้างลายมือชื่อนั้นอยู่ภายใต้การควบคุมของผู้สร้างลายมือชื่อ และการเปลี่ยนแปลงใดๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้

---

[69] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Signatures 2001, Singapore Electronic Transactions Act 1998 , India Information Technology Act 2000 หรือ Brunei Electronic Transaction Order 2000 เป็นต้น

สำหรับการพิจารณาในประเด็นความเชื่อมโยงระหว่างข้อมูลที่ใช้ในการสร้างลายมือชื่อและผู้สร้างลายมือชื่อนั้น ในกรณีที่มีผู้ใช้ข้อมูลสำหรับสร้างลายมือชื่อร่วมกันหลายคนโดยเฉพาะอย่างยิ่งในกรณีของนิติบุคคล ข้อมูลที่ใช้ในการสร้างลายมือชื่อนั้นต้องสามารถระบุตัวบุคคลแต่ละคนที่ใช้ลายชื่ออิเล็กทรอนิกส์ได้ด้วย [70]

การพิจารณาวิธีการที่น่าเชื่อถือ นอกจากจะพิจารณาจากข้อมูลซึ่งมีความเชื่อมโยงกับผู้สร้างลายมือชื่อ และข้อมูลสำหรับการสร้างลายมือชื่อนั้นต้องอยู่ภายใต้การควบคุมของผู้สร้างลายมือชื่อแล้ว ความถูกต้องครบถ้วน (Integrity) ของลายมือชื่ออิเล็กทรอนิกส์และข้อความที่มีการใช้หรือมีการลงลายมือชื่ออิเล็กทรอนิกส์ในขณะที่มีการสร้างลายมือชื่ออิเล็กทรอนิกส์ก็เป็นสิ่งที่ต้องคำนึงถึงเช่นกัน ดังนั้น หากมีการเปลี่ยนแปลงแก้ไขลายมือชื่ออิเล็กทรอนิกส์หรือข้อความที่มีลายมือชื่ออิเล็กทรอนิกส์นั้น หลังจากมีการลงลายมือชื่ออิเล็กทรอนิกส์ก็อาจถือได้ว่าเป็นกรณีข้อมูลอิเล็กทรอนิกส์นั้นไม่มีความถูกต้องครบถ้วน

นอกจากนั้น เพื่อให้เกิดความแน่นอนในการใช้เทคโนโลยีในการลงลายมือชื่ออิเล็กทรอนิกส์ ในการพิจารณาคดีที่เกี่ยวกับเทคนิคในการสร้างลายมือชื่อนั้นให้พิจารณาในขณะที่มีการสร้างลายมือชื่ออิเล็กทรอนิกส์มิใช่ในขณะที่มีการพิจารณาคดีข้อพิพาทนั้น และคู่สัญญามีอิสระที่จะแสดงให้ศาลหรืออนุญาโตตุลาการเห็นว่าวิธีการในทางเทคโนโลยีที่คู่สัญญาเลือกใช้นั้นเป็นไปตามข้อกำหนดในมาตรานี้แล้ว

ในการพิจารณามาตรฐานเทคโนโลยีลายมือชื่ออิเล็กทรอนิกส์อันเป็นกลไกที่ทำให้เกิดความน่าเชื่อถือตามที่กำหนดไว้ในมาตรา 26 นั้นจะต้องคำนึงถึงมาตรฐานระหว่างประเทศที่เป็นที่ยอมรับด้วย (Recognized international standards) ทั้งนี้ไม่ได้จำกัดเฉพาะมาตรฐานที่พัฒนามาจากองค์การระหว่างประเทศ เช่น International Standards Organization (ISO) , Internet Engineering Task Force (IETF) เท่านั้น แต่หมายรวมถึงแนวปฏิบัติทางการค้าและอุตสาหกรรม (Industry

---

[70] References to UNCITRAL documents: A/CN.9/WG.IV/WP.88, para.120

practices and trade usage) ด้วย อย่างไรก็ตาม แม้ไม่มีมาตรฐานดังที่กล่าวมาข้างต้น ก็ไม่อาจใช้เป็นข้ออ้างในการไม่พิจารณาเทคโนโลยีลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวได้ [71]

2.5.2 แนวปฏิบัติของเจ้าของลายมือชื่อ (มาตรา 27) [72]

"เจ้าของลายมือชื่อ" นั้น กฎหมายฉบับนี้ได้วางหลักการพื้นฐานว่า เจ้าของลายมือชื่อจะต้องใช้ความระมัดระวังตามสมควร (Reasonable care) เพื่อมิให้มีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต และในกรณีที่รู้หรือควรจะได้รู้ว่าข้อมูลนั้นได้ถูกล่วงรู้ (Compromised) เจ้าของลายมือชื่อจะต้องแจ้งให้บุคคลที่เกี่ยวข้องหรือผู้ให้บริการลายมือชื่ออิเล็กทรอนิกส์ทราบโดยไม่ชักช้า และ

ผู้สร้างลายมือชื่อต้องกระทำการด้วยความระมัดระวังเพื่อให้ข้อความที่ปรากฏในใบรับรองนั้นถูกต้อง ครบถ้วนตลอดเวลา

บทบัญญัติในมาตรา 27 รวมทั้ง มาตรา 28 มาตรา 30 นั้นเป็นการวางกฎเกณฑ์เกี่ยวกับหน้าที่และความรับผิดของคู่สัญญาฝ่ายต่าง ๆที่เกี่ยวข้อง เช่น เจ้าของลายมือชื่อ คู่กรณีที่เกี่ยวข้อง และผู้ให้บริการออกใบรับรอง อย่างไรก็ตาม พัฒนาการทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็วส่งผลต่อทั้งทางเทคนิคและพาณิชย์อิเล็กทรอนิกส์ ประกอบกับในบางประเทศมีการกำหนดกฎเกณฑ์เกี่ยวกับการพาณิชย์อิเล็กทรอนิกส์แบบกำกับดูแลตนเอง (Self regulation) จึงเป็นการยากที่จะกำหนดกฎเกณฑ์อันเป็นที่ยอมรับร่วมกันได้ทั้งหมด ด้วยเหตุนี้จึง ได้กำหนดมาตรฐานหรือแนวทางปฏิบัติขั้นต่ำหรือประมวลจริยธรรมขั้นต่ำ (Minimal code of conduct) สำหรับคู่กรณีฝ่ายต่าง ๆ ไว้

---

[71] Ibid., A/CN.9/WG.IV/WP.88, paras.127-131

[72] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Signatures 2001 Article 8

หลักการของมาตรา 27 แยกเป็น 2 ส่วนสำคัญ ส่วนแรกเป็นบทบัญญัติตามมาตรา 27(1) เกี่ยวกับแนวทางปฏิบัติของผู้สร้างลายมือชื่อส่วนที่สอง ตามบทบัญญัติของ มาตรา 27 (2) กำหนดเกี่ยวกับความรับผิดของผู้สร้างลายมือชื่อ สำหรับบทบัญญัติส่วนแรกนั้นจะแบ่งออกเป็น 2 กรณี กรณีแรกตามบทบัญญัติมาตรา 27 (1) และ (2) ซึ่งใช้กับลายมือชื่ออิเล็กทรอนิกส์ทุกประเภท และกรณีที่สองตามบทบัญญัติในมาตรา 27 (3) ใช้กับลายมือชื่ออิเล็กทรอนิกส์ที่มีใบรับรอง สำหรับกรณี มาตรา 27 (1) กำหนดให้ผู้สร้างลายมือชื่อต้องใช้ความระมัดระวังตามสมควรเพื่อมิให้มีการใช้ข้อมูลสำหรับสร้างลายมือชื่อของตนโดยปราศจากอำนาจหรือไม่ได้รับอนุญาต อย่างไรก็ตาม คู่กรณีหรือคู่สัญญาอาจตกลงเปลี่ยนแปลงโดยกำหนดมาตรฐานเป็นอย่างอื่นได้หากเห็นว่าเหมาะสม ทั้งนี้เป็นไปตามบทบัญญัติในมาตรา 5

นอกจากนั้น บทบัญญัติมาตรา 27 (2) ก็ได้กำหนดให้ผู้สร้างลายมือชื่อแจ้งให้บุคคลซึ่งผู้สร้างลายมือชื่อเชื่อว่าน่าจะเชื่อถือลายมือชื่ออิเล็กทรอนิกส์และผู้ให้บริการเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ทราบ หากผู้สร้างลายมือชื่อรู้ว่าข้อมูลสำหรับสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นถูกล่วงรู้ (Compromise) โดยบุคคลอื่นหรือปรากฏพฤติการณ์ที่ผู้สร้างลายมือชื่อเห็นว่ามีความเสี่ยงที่ข้อมูลสำหรับสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นถูกล่วงรู้ ทั้งนี้ ผู้ซึ่งเชื่อถือลายมือชื่ออิเล็กทรอนิกส์ในที่นี้ อาจจะรวมถึงผู้ให้บริการเกี่ยวกับใบรับรอง หรือผู้ให้บริการเกี่ยวกับการเพิกถอนใบรับรองในกรณีที่มีการให้บริการเฉพาะการเพิกถอนใบรับรอง ผู้ให้บริการเกี่ยวกับการระบุเวลาในการทำธุรกรรมทางอิเล็กทรอนิกส์ (Timestamp) หรือการให้บริการอื่น ๆที่เกี่ยวข้อง

สำหรับมาตรฐานหรือแนวทางปฏิบัติขั้นต่ำในกรณีที่สองจะใช้กับลายมือชื่ออิเล็กทรอนิกส์ซึ่งมีการรับรองโดยใบรับรองนั้น ตามบทบัญญัติของมาตรา 27 (3) กำหนดให้ต้องใช้ความระมัดระวังตามสมควรในการยืนยันว่าใบรับรองนั้นแสดงราย

ละเอียดต่าง ๆ ของผู้สร้างลายมือชื่อได้อย่างถูกต้องและครบถ้วน นับตั้งแต่เวลาที่มีการยื่นคำขอใช้บริการเกี่ยวกับใบรับรองจนถึงวันที่ใบรับรองหมดอายุ [73]

2.5.3 แนวปฏิบัติของผู้ให้บริการออกใบรับรอง (มาตรา 28)[74]

บทบัญญัติตามมาตรา 28 นั้น เป็นการกล่าวถึงหลักพื้นฐานเกี่ยวกับการให้บริการในการรับรองตัวบุคคลซึ่งปรากฏตามแนวปฏิบัติ (Certification practices statement) ที่เผยแพร่ให้ผู้ใช้บริการหรือประชาชนทั่วไปได้รับทราบ การดำเนินการโดยใช้ความระมัดระวังตามสมควรเกี่ยวกับการรับรองความถูกต้องและครบถ้วนของข้อมูลที่แสดงในใบรับรองตั้งแต่ขั้นตอนการขอใช้บริการจนถึงการหมดอายุของใบรับรอง จัดให้มีวิธีการที่เข้าถึงเพื่อตรวจสอบข้อมูลต่าง ๆ ที่แสดงในใบรับรอง เช่น ข้อมูลสำหรับสร้างลายมือชื่อที่สมบูรณ์ ก่อนหรือในขณะออกใบรับรอง วิธีการที่ใช้ในการระบุตัวผู้ลงลายมือชื่อ เป็นต้น รวมถึงการให้บริการในกรณีที่ข้อมูลสำหรับการสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นถูกล่วงรู้โดยบุคคลที่สามซึ่งมิใช่ผู้สร้างลายมือชื่อและกรณีที่มีการเพิกถอนใบรับรอง ตลอดจนการใช้ระบบ วิธีการ และบุคลากรที่เชื่อถือได้ในการให้บริการ

อย่างไรก็ตาม สำหรับข้อกำหนดเกี่ยวกับการเพิกถอนใบรับรองนั้น ตามกฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ ได้แนะนำมิให้นำบทบัญญัติที่เกี่ยวกับการเพิกถอนที่กำหนดไว้ข้างต้นใช้กับใบรับรองบางประเภท เช่น ใบรับรองซึ่ง

---

[73] References to UNCITRAL documents,A/CN.9/WG.IV/WP.88, paras.132-136

[74] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Signatures 2001 Article 9

ใช้ได้เพียงครั้งเดียว (One-time certificates) หรือใบรับรองซึ่งมีราคาถูกอันเหมาะสำหรับการใช้กับการทำธุรกรรมที่มีความเสี่ยงน้อย แต่ทั้งนี้ก็มิได้หมายความว่าข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประกอบการรับรองที่กำหนดข้างต้นจะใช้แต่เพียงกับใบรับรองซึ่งมีราคาแพงเพราะใช้เทคโนโลยีที่มีความปลอดภัยสูงเท่านั้น [75]

2.5.4 ความน่าเชื่อถือ (มาตรา 29) [76]

บทบัญญัติตามมาตรา 29 เป็นบทบัญญัติที่กำหนดเกี่ยวกับระบบ วิธีการและบุคลากรที่เชื่อถือได้ในการให้บริการ ซึ่งเป็นบทบัญญัติที่เสริมมาตรา 28 (6) ให้มีความชัดเจนมากขึ้น ทั้งนี้ หลักเกณฑ์ตามมาตรา 29 ได้บัญญัติปัจจัยกว้าง ๆ ที่ใช้ในการพิจารณาความน่าเชื่อถือ ซึ่งทำให้ความหมายของคำว่า ความน่าเชื่อถือ (Trustworthiness) มีความยืดหยุ่นและเปลี่ยนแปลงไปตามบริบทของการออกใบรับรอง [77]

ในการพิจารณาว่า ระบบ วิธีการและทรัพยากรบุคคลใด ๆ ของผู้ประกอบการรับรองมีความน่าเชื่อถือตาม มาตรา 28 (6) หรือไม่ ขึ้นอยู่กับปัจจัยดังต่อไปนี้

(1) สถานภาพทางการเงิน บุคลากร และสินทรัพย์ที่มีอยู่

(2) คุณภาพของระบบฮาร์ดแวร์และซอฟต์แวร์

---

[75] References to UNCITRAL documents, A/CN.9/WG.IV/WP.88, paras.137-141

[76] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Signatures 2001 Article 10

[77] References to UNCITRAL documents, A/CN.9/WG.IV/WP.88, para.142

(3) วิธีการออกใบรับรอง การขอใบรับรองและการเก็บรักษาข้อมูลการให้บริการนั้น

(4) การจัดให้มีข้อมูลข่าวสารเกี่ยวกับเจ้าของลายมือชื่อที่ระบุในใบรับรองและผู้ที่อาจคาดหมายได้ว่าจะเป็นคู่กรณีที่เกี่ยวข้อง

(5) **ความสม่ำเสมอและขอบเขตในการตรวจสอบโดยองค์กรอิสระ**

(6) องค์กรที่ให้การรับรองหรือให้บริการออกใบรับรองเกี่ยวกับการปฏิบัติหรือการมีอยู่ของสิ่งที่กล่าวมาใน มาตรา 29 (1) ถึง (5)

(7) กรณีใด ๆ ที่คณะกรรมการประกาศกำหนด

2.5.5 แนวปฏิบัติของคู่กรณีที่เกี่ยวข้อง (มาตรา 30)[78]

บทบัญญัติตามมาตรา 30 ได้วางหลักเกณฑ์เกี่ยวกับแนวปฏิบัติของคู่กรณีที่เกี่ยวข้อง โดยมีหลักการสำคัญที่ว่า คู่กรณีที่เกี่ยวข้องนั้นจะต้องใช้ความระมัดระวังตามสมควรในการตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์นั้น หรือในกรณีที่ลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวมีใบรับรองก็จะต้องใช้ความระมัดระวังในการตรวจสอบถึงความสมบูรณ์ การพักใช้หรือการเพิกถอนใบรับรองนั้น รวมทั้งตรวจสอบข้อจำกัดใด ๆ ที่เกี่ยวกับใบรับรองดังกล่าวด้วย หลักการตามมาตรา 30 นี้วางอยู่บนแนวคิดที่ว่า คู่กรณีที่เกี่ยวข้องควรตระหนักไว้เสมอว่ามีความเหมาะสมเพียงใดในการให้ความเชื่อถือใบรับรองนั้นในกรณีที่ต่างกันไป

อย่างไรก็ตาม แม้บทบัญญัติตามมาตรา 30 จะสร้างภาระให้แก่คู่กรณีที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งเมื่อบุคคลนั้นอยู่ในฐานะผู้บริโภค แต่ไม่ได้หมายความว่ากฎหมายฉบับนี้จะมีผลลบล้างกฎเกณฑ์ใด ๆซึ่งบัญญัติขึ้นเพื่อคุ้มครองผู้บริโภค (ตาม

---

[78] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Signatures 2001 Article 11

มาตรา 3) แต่กฎหมายฉบับนี้มีส่วนสำคัญในการสร้างความรู้ความเข้าใจให้กับทุกๆ ฝ่ายที่เกี่ยวข้อง ซึ่งรวมถึงมาตรฐานในการดำเนินการอย่างเหมาะสมของคู่กรณีที่เกี่ยวข้องให้เป็นไปตามที่กำหนดไว้ในกฎหมาย นอกจากนี้ การกำหนดมาตรฐานในการดำเนินการตรวจสอบความน่าเชื่อถือของลายมือชื่อโดยจัดให้มีวิธีการที่เข้าถึงได้ก็อาจมีส่วนสำคัญในการพัฒนาระบบโครงสร้างกุญแจสาธารณะ [79]

ทั้งนี้ คำว่า "คู่กรณีที่เกี่ยวข้อง" ตามคำนิยามในมาตรา 4 หมายความว่า "ผู้ซึ่งอาจกระทำการใดๆ โดยขึ้นอยู่กับใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์" ซึ่งตามคำนิยามดังกล่าวคำว่า "คู่กรณีที่เกี่ยวข้อง" จึงอาจครอบคลุมถึง คู่กรณี ซึ่งเชื่อถือลายมือชื่ออิเล็กทรอนิกส์นั้น โดยรวมถึงบุคคลใดๆ ทั้งที่มีหรือไม่มีความผูกพันตามสัญญากับเจ้าของลายมือชื่อ หรือผู้ให้บริการออกใบรับรองเลย และเป็นไปได้ว่าผู้ให้บริการออกใบรับรองหรือเจ้าของลายมือชื่ออาจจะเป็นบุคคลที่เชื่อถือใบรับรองเสียเองก็ได้

2.5.6 การรับรองใบรับรองและลายมือชื่ออิเล็กทรอนิกส์ต่างประเทศ (มาตรา 31)[80]

บทบัญญัติตามมาตรา 31 เป็นการวางกฎเกณฑ์เกี่ยวกับการรับรองใบรับรองและการรับรองลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นในต่างประเทศ โดยบทบัญญัติตามความใน มาตรา 31 (1) ได้กำหนดหลักการที่ว่าไม่ให้นำหลักเกณฑ์เกี่ยวกับสถานที่ออกใบรับรองหรือสถานที่สร้างหรือใช้ลายมือชื่ออิเล็กทรอนิกส์ มากำหนดผลทางกฎหมายของใบรับรองและลายมือชื่ออิเล็กทรอนิกส์ ซึ่งหลักการดังกล่าวนี้วางอยู่บน

---

[79] References to UNCITRAL documents, A/CN.9/WG.IV/WP.88, paras.143-146

[80] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ UNCITRAL Model Law on Electronic Signatures 2001 Article 12

พื้นฐานของการไม่เลือกปฏิบัติ (Non-discrimination) กล่าวคือ ผลทางกฎหมายของใบรับรองและลายมือชื่ออิเล็กทรอนิกส์ไม่ได้พิจารณาจากประเด็นที่ว่าใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์นั้นถูกสร้างขึ้นที่ใด แต่พิจารณาจากความน่าเชื่อถือในทางเทคโนโลยีที่สร้างใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์นั้น ทั้งนี้ การพิจารณาผลทางกฎหมายของใบรับรองและลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นในต่างประเทศนั้น ได้มีการกำหนดหลักเกณฑ์ไว้ใน มาตรา 31 ว่า ผลทางกฎหมายของใบรับรองและลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นในต่างประเทศให้มีผลทางกฎหมายเช่นเดียวกับใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นในประเทศ หากใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวได้ใช้ระบบที่เชื่อถือได้ไม่น้อยไปกว่าระบบที่เชื่อถือได้ตามพระราชบัญญัตินี้

อย่างไรก็ตาม คำว่า “หากใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวได้ใช้ระบบที่เชื่อถือได้ไม่น้อยไปกว่าระบบที่เชื่อถือได้ตามพระราชบัญญัติ” นั้น ไม่ได้หมายความว่าระบบที่เชื่อถือได้ของใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ต่างประเทศจะต้องเหมือนกันทุกประการกับใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ในประเทศ เนื่องจากแต่ละประเทศอาจมีข้อกำหนดที่แตกต่างกัน และมีข้อควรพิจารณาว่าในทางปฏิบัติ ผู้ให้บริการออกใบรับรองรายเดียวกันอาจออกใบรับรองที่มีระดับความน่าเชื่อถือแตกต่างกันได้ ทั้งนี้ ขึ้นกับวัตถุประสงค์ในการใช้ ด้วยเหตุนี้ใบรับรองทุกใบจึงไม่ได้ให้ผลในทางกฎหมายที่เหมือนกัน ไม่ว่าจะเป็นใบรับรองในประเทศหรือต่างประเทศก็ตาม

ทั้งนี้ หลักเกณฑ์ในการพิจารณาว่าใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ใดมีความน่าเชื่อถือได้ตามความในมาตรา 3 1 วรรคสองหรือวรรคสาม ให้คำนึงถึงมาตรฐานระหว่างประเทศและปัจจัยอื่น ๆ ที่เกี่ยวข้องประกอบด้วย อาทิ อาจพิจารณาจากหลักเกณฑ์ตามมาตรา 26 มาตรา 28 และมาตรา 29 ประกอบกัน อย่างไรก็ตาม คำว่า “มาตรฐานระหว่างประเทศ” นี้ จะต้องตีความในความหมายกว้างเพื่อให้ครอบคลุมทั้งมาตรฐานในทางเทคโนโลยี และมาตรฐานทางการค้าในทางระหว่างประเทศ รวมทั้งมาตรฐานและบรรทัดฐานที่รัฐหรือองค์การระหว่างประเทศยอมรับ

ดังนั้น มาตรฐานในทางระหว่างประเทศจึงอาจเป็นได้ทั้งคำแถลง (Statement) เกี่ยวกับเทคโนโลยี กฎหมาย หรือแนวปฏิบัติทางการค้า (Commercial Practice) ไม่ว่าจะพัฒนามาจากภาครัฐหรือภาคเอกชนก็ตาม โดยมาตรฐานเช่นนี้อาจอยู่ในรูปของ ข้อกำหนด (Requirement) ข้อแนะนำ (Recommendation) แนวทาง (Guideline) ประมวลจริยธรรม (Codes of Conduct) หรือคำแถลงก็ได้ [81]

นอกเหนือจากหลักเกณฑ์ต่าง ๆ ดังที่ได้กล่าวมาแล้ว ในการรับรองใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ต่างประเทศ ตามบทบัญญัติมาตรา 5 ยังได้วางหลักการรับรองใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ต่างประเทศอาจเกิดจากความตกลงของคู่กรณีก็ได้

[81] References to UNCITRAL documents, A/CN.9/WG.IV/WP.88, paras.147-155

บทที่ 3
ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

3.1 ความนำ

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้บัญญัติหลักเกณฑ์เกี่ยวกับธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ไว้ในหมวด 3 (มาตรา 32 – มาตรา 34) โดยในหมวดนี้ได้มีการเพิ่มเติมเข้ามาชั้นการพิจารณาของวุฒิสภา ด้วยสภาพข้อเท็จจริงในภาคธุรกิจปัจจุบันที่การให้บริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์มีความหลากหลายมากขึ้น และคาดการณ์ว่าจะเพิ่มสัดส่วนขึ้นอย่างมากในอนาคต ดังนั้นจึงได้มีการแก้ไขเพื่อให้กฎหมายมีความยืดหยุ่นในการปรับใช้มากขึ้น โดยขยายรวมถึงการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์รูปแบบอื่น ๆ ด้วย

ทั้งนี้ ในการกำหนดบทบัญญัติในส่วนของธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ตั้งแต่มาตรา 32 ถึงมาตรา 34 นั้น มีวัตถุประสงค์หลักเพื่อการกำกับดูแลกิจการบางประเภทที่หากปล่อยให้มีการดำเนินการโดยเสรีแล้วอาจส่งผลเสียต่อส่วนรวม หรือมีความเสี่ยงบางประการเกิดขึ้นจากการประกอบธุรกิจดังกล่าว ดังนั้น

บทบัญญัติในหมวดนี้จึงได้วางกรอบกว้าง ๆเกี่ยวกับประเภทธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ที่อาจจำเป็นจะต้องกำกับดูแล รวมถึงการกำหนดกรอบของกฎเกณฑ์เกี่ยวกับวิธีการในการกำกับดูแลที่จะต้องมีการตราพระราชกฤษฎีกากำหนดรายละเอียดต่อไป

3.2 ประเภทของธุรกิจบริการที่ต้องมีการกำกับดูแล

พระราชบัญญัติฉบับนี้ไม่ได้กำหนดคำนิยามคำว่า "ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์" ไว้ว่าหมายถึงธุรกิจประเภทใดบ้าง ทั้งนี้ เนื่องจากต้องการให้คำนี้เป็นคำที่มีความหมายกว้าง ประกอบกับคำดังกล่าวเป็นคำที่ค่อนข้างยากต่อการให้คำจำกัดความ เพราะธุรกิจแต่ละประเภทจะมีลักษณะ ขั้นตอน และรูปแบบการให้บริการที่แตกต่างกัน ดังนั้นการจะบัญญัติคำนิยามให้คลุมถึงธุรกิจบริการทุกประเภทจึงเป็นเรื่องยาก ในขณะเดียวกันเหตุผลที่กฎหมายไม่ได้ระบุให้ชัดเจนว่าธุรกิจประเภทใดบ้างเป็นธุรกิจที่จะต้องมีการกำกับดูแลนั้น เนื่องจากกฎหมายต้องการวางหลักการที่เป็นกลางเพื่อให้สามารถรองรับได้ทุกเทคโนโลยีทั้งที่มีอยู่ในปัจจุบัน และที่อาจเกิดขึ้นในอนาคต และเพื่อให้กฎหมายสามารถปรับใช้หรือรองรับกับบริการรูปแบบใหม่ที่อาจเกิดขึ้นเนื่องจากการพัฒนาการทางเทคโนโลยีที่ค่อนข้างรวดเร็วได้ทันทีนั้น กฎหมายจึงได้บัญญัติให้อำนาจการกำกับดูแลธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์สามารถทำได้รวดเร็วมากขึ้น โดยการตราเป็นพระราชกฤษฎีกา ตามมาตรา 3 2 ทั้งนี้ หลักเกณฑ์การกำกับดูแลเกี่ยวกับธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ โดยการตราเป็นพระราชกฤษฎีกานั้น ตามมาตรา 3 2 วรรคหนึ่ง ได้บัญญัติไว้ดังนี้

"บุคคลย่อมมีสิทธิประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ แต่ในกรณีที่จำเป็นเพื่อรักษาความมั่นคงทางการเงินและทางพาณิชย์ หรือเพื่อประโยชน์ในการเสริมสร้างความน่าเชื่อถือและยอมรับในระบบข้อมูลอิเล็กทรอนิกส์ หรือเพื่อป้องกันความเสียหายต่อสาธารณชน ให้มีการตราพระราชกฤษฎีกากำหนดให้

การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ใดเป็นกิจการที่ต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตก่อนก็ได้"

อย่างไรก็ตาม เมื่อพิจารณาจากบทบัญญัติดังที่ได้กล่าวมาข้างต้นจะพบว่า แม้กฎหมายฉบับนี้มิได้ให้คำนิยามของคำว่า "ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์" ไว้ก็ตามซึ่งทำให้คำนี้เป็นคำที่มีความหมายกว้างครอบคลุมถึงธุรกิจทุกประเภทที่เกี่ยวข้อง อาทิ การให้บริการออกใบรับรอง (Certification Authority) การให้บริการเกี่ยวกับการรับรองเอกสารอิเล็กทรอนิกส์ การให้บริการด้านความปลอดภัยของเครือข่าย การให้บริการเกี่ยวกับการจัดเก็บเอกสารอิเล็กทรอนิกส์ หรือการให้บริการจัดทำ website เป็นต้น แต่ทั้งนี้มิได้หมายความว่าจะต้องมีการกำกับดูแลธุรกิจทุกประเภทที่เกี่ยวข้องดังที่ได้กล่าวมา เนื่องจากบทบัญญัติ ตามมาตรา 32 วรรคหนึ่ง ได้กำหนดให้การตราพระราชกฤษฎีกาเพื่อกำกับดูแลธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ตามความในมาตรานี้สามารถทำได้ต่อเมื่อเข้าเงื่อนไขหรือหลักเกณฑ์ในการพิจารณา 3 กรณี ดังนี้

(ก) เพื่อรักษาความมั่นคงทางการเงินหรือการพาณิชย์

(ข) เพื่อประโยชน์ในการสร้างเสริมความน่าเชื่อถือและยอมรับในระบบข้อมูลอิเล็กทรอนิกส์

(ค) เพื่อป้องกันความเสียหายต่อสาธารณชน

ดังนั้น หากธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ประเภทใดส่งผลกระทบต่อวัตถุประสงค์อย่างใดอย่างหนึ่งในสามประการข้างต้น ธุรกิจประเภทนั้นก็อาจจำเป็นที่จะต้องได้รับการพิจารณาโดยคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ซึ่งจัดตั้งขึ้นตามกฎมายนี้ว่าสมควรที่จะต้องมีการกำกับดูแลหรือไม่ นอกจากนี้ ตามมาตรา 32 วรรคสี่ ยังได้กำหนดเพิ่มเติมว่า ก่อนเสนอให้มีการตราพระราชกฤษฎีกาตามมาตรานี้ ต้องจัดให้มีการรับฟังความคิดของประชาชนตามความเหมาะสม และนำข้อมูลที่ได้รับมาประกอบการพิจารณาก่อนที่จะมีการตราพระราชกฤษฎีกาต่อไป

3.3 หลักเกณฑ์ และวิธีการกำกับดูแล

พระราชบัญญัติฯ ได้กำหนดวิธีการกำกับดูแลไว้ตามบทบัญญัติมาตรา 32 วรรคสอง ซึ่งกำหนดไว้ว่า

"ในการกำหนดให้กรณีใดต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตตามวรรคหนึ่ง ให้กำหนดโดยพิจารณาจากความเหมาะสมในการป้องกันความเสียหายตามระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจากการประกอบธุรกิจนั้น"

เมื่อพิจารณาจากบทบัญญัติดังกล่าวจะเห็นว่า กฎหมายได้กำหนดวิธีการในการกำกับดูแลธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ไว้สามรูปแบบ ดังนี้

(ก) ต้องแจ้งให้ทราบ

(ข) ต้องขึ้นทะเบียน

(ค) ต้องได้รับใบอนุญาต

โดยธุรกิจใดต้องใช้รูปแบบใดในการกำกับดูแลนั้น กฎหมายให้พิจารณาถึงความเหมาะสมในการป้องกันความเสียหายที่อาจจะเกิดขึ้นจากการประกอบธุรกิจดังกล่าว กล่าวคือ ถ้าธุรกิจใดอาจส่งผลกระทบเสียหายอย่างรุนแรงต่อวัตถุประสงค์ที่กฎหมายมุ่งจะคุ้มครอง การที่จะประกอบธุรกิจดังกล่าวก็อาจต้องได้รับใบอนุญาตก่อน ส่วนธุรกิจที่ส่งผลกระทบเสียหายที่อาจไม่รุนแรงมากนัก ก็อาจต้องขึ้นทะเบียน หรือต้องแจ้งให้ทราบเท่านั้น

ทั้งนี้ กฎหมายได้กำหนดรายละเอียดในแต่ละรูปแบบของการกำกับดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ไว้ในมาตรา 33 และมาตรา 34 โดยบทบัญญัติในมาตรา 33 เป็นการบัญญัติรายละเอียดในกรณีของธุรกิจบริการที่มีพระราชกฤษฎีกากำหนดให้เป็นธุรกิจที่ต้องแจ้งให้ทราบหรือขึ้นทะเบียน และบทบัญญัติมาตรา 34 เป็นบทบัญญัติรายละเอียดในกรณีของธุรกิจบริการที่มีพระราช

กฤษฎีกากำหนดให้เป็นธุรกิจที่ต้องขออนุญาตก่อน โดยแต่ละมาตรามีรายละเอียดดังต่อไปนี้

สาระสำคัญของบทบัญญัติมาตรา 33 เป็นการกำหนดขั้นตอนในรายละเอียดสำหรับผู้ประกอบธุรกิจที่จะต้องดำเนินการ ในกรณีที่มีพระราชกฤษฎีกากำหนดให้ธุรกิจใดเป็นธุรกิจที่ต้องแจ้งให้ทราบหรือขึ้นทะเบียน ซึ่งมีสาระสำคัญโดยสังเขป ดังนี้

(ก) ผู้ประสงค์จะประกอบกิจการต้องแจ้งพนักงานเจ้าหน้าที่ทราบก่อนหรือได้รับขึ้นทะเบียนจากพนักงานเจ้าหน้าที่ก่อนจึงจะประกอบกิจการได้

(ข) การแจ้งให้ทราบหรือการขึ้นทะเบียนต้องปฏิบัติตามหลักเกณฑ์และวิธีการที่กำหนดไว้ในพระราชกฤษฎีกา โดยพระราชกฤษฎีกาจะต้องมีการกำหนดรายละเอียดอย่างน้อยในเรื่องดังต่อไปนี้

- พนักงานเจ้าหน้าที่ผู้รับแจ้งหรือรับขึ้นทะเบียน
- หลักเกณฑ์และวิธีการแจ้งหรือขึ้นทะเบียน
- หลักเกณฑ์เกี่ยวกับการประกอบธุรกิจที่ต้องแจ้งหรือขึ้นทะเบียน

(ค) ให้พนักงานเจ้าหน้าที่ออกใบรับแจ้งหรือใบขึ้นทะเบียนให้แก่ผู้แจ้งหรือผู้ขึ้นทะเบียนไว้เป็นหลักฐานนับแต่วันที่รับแจ้งหรือรับขึ้นทะเบียน

(ง) ผู้แจ้งหรือผู้ขึ้นทะเบียนสามารถประกอบธุรกิจได้นับแต่วันที่พนักงานเจ้าหน้าที่รับแจ้งหรือรับขึ้นทะเบียน

(จ) ในกรณีที่การแจ้งหรือการขึ้นทะเบียนไม่ถูกต้องครบถ้วน และพนักงานเจ้าหน้าที่ตรวจพบในภายหลัง พนักงานเจ้าหน้าที่มีอำนาจสั่งให้ผู้แจ้งหรือผู้ขึ้นทะเบียนแก้ไขให้ถูกต้องครบถ้วนภายใน 7 วัน

(ฉ) ผู้แจ้งหรือผู้ขึ้นทะเบียนต้องประกอบกิจการตามหลักเกณฑ์ที่กำหนดไว้ในพระราชกฤษฎีกา และตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกาศกำหนด

(ช) ถ้าผู้แจ้งหรือขึ้นทะเบียนไม่ปฏิบัติตามคำสั่งพนักงานเจ้าหน้าที่หรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ในพระราชกฤษฎีกา คณะกรรมการธุรกรรม

ทางอิเล็กทรอนิกส์มีอำนาจสั่งให้บุคคลดังกล่าวชำระค่าปรับทางปกครองซึ่งกฎหมายกำหนดไว้ไม่ให้เกิน 1,000,000 บาท

(ซ) นอกจากลงโทษปรับทางปกครองแล้ว ในกรณีที่เห็นสมควร คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์อาจสั่งให้บุคคลดังกล่าวกระทำการใด ๆเพื่อแก้ไขให้ถูกต้องด้วยก็ได้

(ฌ) หลักเกณฑ์เกี่ยวการลงโทษปรับทางปกครองนั้น กฎหมายกำหนดให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นผู้ประกาศกำหนด

(ญ) ในกรณีที่มีการฝ่าฝืนไม่ชำระค่าปรับทางปกครอง กฎหมายกำหนดให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม

(ฎ) กฎหมายกำหนดให้อำนาจพนักงานเจ้าหน้าที่ในการฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ ในกรณีที่ผู้ถูกลงโทษปรับทางปกครองไม่ชำระค่าปรับ กฎหมายกำหนดให้อำนาจศาลปกครองในการพิพากษาและบังคับให้มีการยึดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับ ถ้าศาลเห็นว่าคำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมาย

(ฏ) คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มีอำนาจออกคำสั่งห้ามมิให้ประกอบธุรกิจตามที่แจ้งหรือขึ้นทะเบียน ถ้าผู้ประกอบการธุรกิจดังกล่าวไม่ปฏิบัติตามคำสั่งของคณะกรรมการหรือกระทำความผิดซ้ำอีก

สำหรับสาระสำคัญของบทบัญญัติมาตรา 34 เป็นการกำหนดขั้นตอนในรายละเอียดสำหรับผู้ประกอบธุรกิจที่จะต้องดำเนินการ ในกรณีที่มีพระราชกฤษฎีกากำหนดให้ธุรกิจใดเป็นธุรกิจที่ต้องขออนุญาตก่อนประกอบการซึ่งมีสาระสำคัญโดยสังเขป ดังนี้

(ก) ผู้ประสงค์จะประกอบธุรกิจที่มีพระราชกฤษฎีกากำหนดว่าเป็นธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ที่ต้องได้รับใบอนุญาต ต้องยื่นคำขอต่อพนักงานเจ้าหน้าที่

(ข) รายละเอียดเกี่ยวกับกฎเกณฑ์การอนุญาตนั้นกฎหมายให้ตราเป็นพระราชกฤษฎีกา โดยพระราชกฤษฎีกาจะต้องกำหนดรายละเอียดอย่างน้อยในเรื่องต่าง ๆ ดังต่อไปนี้

- พนักงานเจ้าหน้าที่ผู้รับคำขอใบอนุญาต
- คุณสมบัติของผู้ขอรับใบอนุญาต
- หลักเกณฑ์และวิธีการขออนุญาต
- การออกใบอนุญาต
- การต่ออายุใบอนุญาต
- การคืนใบอนุญาต
- การสั่งพักใช้หรือเพิกถอนใบอนุญาต
- หลักเกณฑ์เกี่ยวกับการประกอบธุรกิจที่ต้องได้รับใบอนุญาต

(ค) ผู้ได้รับใบอนุญาตต้องประกอบธุรกิจให้เป็นไปตามหลักเกณฑ์ที่กำหนดไว้ในพระราชกฤษฎีกาและตามที่คณะกรรมการประกาศกำหนด และตามเงื่อนไขที่กำหนดในใบอนุญาต

(ง) คณะกรรมการมีอำนาจลงโทษปรับทางปกครองแก่ผู้ประกอบการที่ไม่ปฏิบัติตาม โดยปรับได้ไม่เกิน 2,000,000 บาท

(จ) นอกจากลงโทษปรับทางปกครองแล้ว ในกรณีที่เห็นสมควร คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์อาจสั่งให้บุคคลดังกล่าวกระทำการใด ๆ เพื่อแก้ไขให้ถูกต้องเหมาะสมด้วยก็ได้

(ฉ) ให้นำมาตรา 33 วรรคห้า เกี่ยวกับโทษปรับทางปกครอง การฟ้องคดีต่อศาลปกครอง และการบังคดีของศาลปกครองในรูปแบบการกำกับดูแลแบบแจ้งให้ทราบ หรือขึ้นทะเบียนมาใช้กับการกำกับดูแลแบบ ต้องได้รับใบอนุญาตด้วยโดยอนุโลม

(ช) คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มีอำนาจสั่งเพิกถอนใบอนุญาต ในกรณีที่ผู้ได้รับใบอนุญาตไม่ปฏิบัติตามคำสั่งของคณะกรรมการ หรือกระทำการฝ่าฝืนซ้ำอีก

3.4 ตัวอย่างประเภทของธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ที่มีการกำกับดูแลในต่างประเทศ

ประเภทของธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ที่มักจะมีการกำกับดูแลในต่างประเทศ เช่น ธุรกิจบริการเกี่ยวกับใบรับรองลายมือชื่อดิจิทัล (Certificate Service Provider) หรือธุรกิจการรับรองขั้นตอนการเก็บเอกสารอิเล็กทรอนิกส์ เป็นต้น โดยมีรายละเอียดพอสังเขปดังต่อไปนี้

3.4.1 ธุรกิจบริการเกี่ยวกับใบรับรองลายมือชื่อดิจิทัล (Certificate Service Provider)

ธุรกิจบริการเกี่ยวกับใบรับรองลายมือชื่อดิจิทัล (Certificate Service Provider) หรือที่บางครั้งเรียกกันว่า"ผู้ประกอบการรับรอง"(Certification authority) นั้น เป็นธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ประเภทหนึ่งที่ในหลาย ๆ ประเทศมีการกำกับดูแล ทั้งนี้ เนื่องจากธุรกิจประเภทนี้เป็นธุรกิจที่เกี่ยวกับการเสริมสร้างความเชื่อถือและยอมรับในระบบข้อมูลอิเล็กทรอนิกส์โดยใช้กลไกทางเทคโนโลยีบางประการ เพื่อให้บุคคลที่ติดต่อสื่อสารด้วยวิธีการทางอิเล็กทรอนิกส์โดยเฉพาะอย่างยิ่งเครือข่ายอินเทอร์เน็ตนั้น สามารถเชื่อถือได้ว่าเป็นบุคคลนั้นจริง

ทั้งนี้ ดังที่ได้กล่าวมาแล้วในบทที่ 2 ว่า ผู้ประกอบการรับรอง หรือ CA นั้น เกิดขึ้นสืบเนื่องจากเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) ซึ่งนำมาใช้ในการสร้างลายมือชื่อดิจิทัล อันเป็นลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่ง โดยกลไกในการสร้างและตรวจสอบลายมือชื่อดิจิทัลนั้นจะต้องมีกุญแจคู่ อันประกอบด้วยกุญแจส่วนตัวซึ่งใช้ในการสร้างลายมือชื่อดิจิทัล และกุญแจสาธารณะซึ่งใช้ในการตรวจสอบลายมือชื่อดิจิทัล

โดยในการตรวจสอบลายมือชื่อดิจิทัลนั้น ผู้ตรวจสอบจะต้องสามารถเข้าถึงกุญแจสาธารณะของผู้ลงลายมือชื่อ และจะต้องมั่นใจได้ว่ากุญแจสาธารณะนั้นสัมพันธ์กับกุญแจส่วนตัวของผู้ลงลายมือชื่อ อย่างไรก็ตามเป็นที่ทราบกันดีอยู่แล้วว่ากุญแจส่วนตัวและกุญแจสาธารณะนั้นไม่ได้มีความสัมพันธ์ใด ๆกับบุคคล เพราะกุญแจส่วนตัวและกุญแจสาธารณะเป็นเพียงตัวเลขที่ถูกสร้างขึ้นมาเท่านั้น ด้วยเหตุนี้กลไกการทำงานจึงต้องสร้างความน่าเชื่อถือระหว่างบุคคลกับกุญแจคู่ และเพื่อให้กุญแจสาธารณะบรรลุวัตถุประสงค์ของการใช้งานจึงจำเป็นที่จะต้องทำให้บุคคลอื่น ๆ สามารถหาหรือเข้าถึงกุญแจสาธารณะได้โดยง่าย แม้ว่าบุคคลเหล่านั้นจะไม่เคยรู้จักผู้สร้างลายมือชื่อหรือไม่เคยมีความสัมพันธ์ใด ๆกันมาก่อน ด้วยเหตุดังกล่าว คู่สัญญาจึงจำเป็นที่จะต้องให้ความเชื่อถือในกุญแจคู่ที่ถูกสร้างขึ้นมานั้น [82]

ความน่าเชื่อถือระหว่างคู่สัญญาอาจเกิดขึ้นจากการที่คู่สัญญาเชื่อถือซึ่งกันและกัน เช่น เคยติดต่อกันมาก่อน เคยสื่อสารกันในระบบปิด (closed-system) หรืออื่น ๆ ซึ่งในการทำธุรกรรมระหว่างบุคคล 2 ฝ่ายที่มีความเชื่อถือระหว่างกันนั้น การติดต่อสื่อสารเพื่อให้อีกฝ่ายทราบกุญแจสาธารณะของตนสามารถทำได้โดยง่าย อย่างไรก็ตามวิธีเดียวกันอาจทำไม่ได้หรือทำได้ยากหากบุคคล 2 ฝ่ายไม่ได้ติดต่อกันบ่อยครั้ง ติดต่อสื่อสารกันในระบบเปิด (เช่น อินเทอร์เน็ต) ไม่เคยมีข้อตกลงใด ๆ กันมาก่อน หรือไม่เคยมีกฎหมายใดที่กำหนดความสัมพันธ์ระหว่างบุคคล 2 ฝ่ายนั้นไว้ นอกจากนี้ ด้วยเหตุที่ระบบกุญแจคู่เป็นเทคโนโลยีที่ใช้กระบวนการทางคณิตศาสตร์ขั้นสูง ดังนั้นผู้ใช้จะต้องเชื่อถือในทักษะ ความรู้ และการจัดการระบบกุญแจคู่ของคู่สัญญาที่สร้างกุญแจส่วนตัวและกุญแจสาธารณะนั้นขึ้น

การแก้ปัญหาต่าง ๆดังที่กล่าวมาข้างต้นวิธีหนึ่งคือการใช้บุคคลที่สามในการกำหนดความเกี่ยวเนื่องระหว่างเจ้าของลายมือชื่อดิจิทัลกับกุญแจสาธารณะ โดยบุคคลที่สามนี้โดยทั่วไปเรียกกันว่า “ผู้ประกอบการรับรอง” (Certification Authority หรือ

---

[82] UNCITRAL Model Law On Electronic Signatures 2001

Certification service provider หรือ Supplier of certification services) ซึ่งเป็นบุคคลฝ่ายที่สาม ทำหน้าที่สร้างกุญแจคู่ตามคำขอของผู้ขอใช้บริการ ออกใบรับรอง ยืนยันตัวบุคคลผู้ขอใช้บริการ จัดเก็บกุญแจสาธารณะในฐานข้อมูล เปิดเผยกุญแจสาธารณะต่อสาธารณชนที่ติดต่อทางเครือข่าย ยืนยันตัวบุคคลที่เป็นเจ้าของกุญแจสาธารณะตามคำขอของบุคคลทั่ว ๆ ไป และให้บริการอื่น ๆ ที่เกี่ยวข้อง

ด้วยความสำคัญดังที่ได้กล่าวมาแล้ว ทำให้ปัจจุบันบางประเทศมีการกำกับดูแลผู้ให้บริการออกใบรับรอง ซึ่งสามารถแบ่งออกได้เป็น 2 รูปแบบหลัก กล่าวคือ

- **แบบสมัครใจ** (Voluntary certification system) ระบบนี้จะไม่บังคับให้ผู้ประกอบการรับรองต้องขออนุญาตประกอบการจากหน่วยงานของรัฐ กล่าวคือ ผู้ประกอบการที่มีความพร้อมในทางเทคโนโลยีระดับหนึ่งสามารถให้บริการได้เลยโดยไม่ต้องขออนุญาตหรือจะขออนุญาตก่อนก็ได้ อย่างไรก็ตาม ประเทศที่เลือกใช้ระบบนี้ส่วนใหญ่ในกฎหมายจะกำหนดชัดเจนถึงความแตกต่างระหว่างผู้ประกอบการที่ขออนุญาตกับผู้ประกอบการที่ไม่ได้ขออนุญาต โดยจะได้รับประโยชน์จากบทบัญญัติของกฎหมายแตกต่างกัน เช่น การจำกัดความรับผิดของผู้ประกอบการ หรือได้รับบทสันนิษฐานว่าลายมือชื่อที่ใช้ใบรับรองจากผู้ประกอบการรับรองที่ได้รับอนุญาตเป็นลายมือชื่อแบบปลอดภัย นอกจากนี้ ผู้ที่ได้รับใบอนุญาตก็จะได้รับความเชื่อถือจากผู้ใช้บริการในระดับหนึ่งในการจะเข้าไปขอใช้บริการที่มีอยู่ เป็นต้น

- **แบบบังคับ** (Mandatory licensing system) รัฐที่เลือกใช้ระบบนี้จะบังคับให้ผู้ประกอบการรับรองต้องขออนุญาตประกอบการจากหน่วยงานของรัฐก่อนที่ประกอบการ หากประกอบการโดยไม่ได้รับอนุญาต ผู้ประกอบการรับรองนั้นจะถูกลงโทษตามกฎหมายซึ่งอาจมีทั้งโทษจำคุกและโทษปรับ

ตารางแสดงระบบการกำกับการประกอบการรับรองในบางประเทศ

ประเทศ	แบบสมัครใจ	แบบบังคับ
เยอรมัน	/	
ญี่ปุ่น	/	
มาเลเซีย		/
สิงคโปร์	/	
เกาหลีใต้	/	

3.4.2 ธุรกิจตรวจสอบระบบการจัดทำภาพเอกสาร (Image system)

ธุรกิจประเภทนี้จะมีส่วนเกี่ยวข้องหรือมีส่วนสัมพันธ์อย่างยิ่งกับหลักเกณฑ์การรับฟังพยานหลักฐานในรูปของข้อมูลอิเล็กทรอนิกส์ ทั้งนี้ จะเห็นได้จากตัวอย่างกรณีของประเทศสิงคโปร์ ซึ่งได้กำหนดหลักเกณฑ์ในการรับฟังพยานหลักฐานในรูปข้อมูลอิเล็กทรอนิกส์ในรายละเอียดไว้ใน The Evidence Act (Chapter 97) ใน Section 35 ดังนี้

"เว้นแต่จะมีกฎหมายบัญญัติไว้เป็นอย่างอื่น ในกรณีมีการนำเสนอพยานหลักฐานในรูปข้อมูลอิเล็กทรอนิกส์ (computer output) ศาลจะรับฟังพยานหลักฐานดังกล่าวได้ต่อเมื่อได้มีการปฏิบัติตามเงื่อนไขดังต่อไปนี้

(1) แสดงให้เห็นได้ว่าคู่ความได้ตกลงกันให้สามารถนำเสนอพยานหลักฐานในรูปข้อมูลอิเล็กทรอนิกส์ในกระบวนพิจารณาไม่ว่าในเวลาใดก็ตาม โดยไม่คำนึงว่าจะมีการโต้แย้งถึงความแท้จริงหรือความถูกต้องของเนื้อความหรือไม่

(2) ได้ผ่านการกระบวนการรับรอง (approved process) หรือ

(3) - - - "

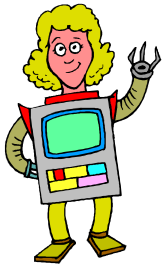
ทั้งนี้ คำว่า "กระบวนการรับรอง (approved process)" ในที่นี้ หมายถึง กระบวนการรับรองตามบทบัญญัติหรือข้อกำหนดที่ออกโดยรัฐมนตรี หรือโดยบุคคลหรือองค์กร**ที่ได้รับการแต่งตั้ง**จากรัฐมนตรีเป็นผู้ประกอบการรับรอง (Certifying Authority) ซึ่งการให้การรับรองโดยบุคคลหรือองค์กรที่ได้รับการแต่งตั้งข้างต้น จะอยู่ในรูปใบรับรองที่ลงนามโดยบุคคลที่มีตำแหน่งหน้าที่รับผิดชอบเกี่ยวกับการปฏิบัติการหรือบริหารของผู้ประกอบการรับรอง (certifying authority) และมีวัตถุประสงค์เพื่อแสดงว่าเห็นชอบด้วยกับกระบวนการรับรองดังกล่าวนั้น

ประโยชน์ที่ได้รับในกรณีที่ระบบการจัดทำภาพเอกสาร (Image system) ได้ผ่านกระบวนการการตรวจสอบจากผู้ประกอบการรับรองที่ได้รับการแต่งตั้งจากรัฐมนตรีนั้น ให้สันนิษฐานว่าเอกสารภาพที่จัดทำขึ้นนั้นสามารถแสดงถึงเอกสารเดิม (original document) ได้อย่างถูกต้อง เว้นแต่พิสูจน์ให้เห็นเป็นอย่างอื่น

3.5 บทสรุป

จากตัวอย่างธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ที่กล่าวมาข้างต้น แสดงให้เห็นว่า นอกจากการประกอบการรับรองลายมือชื่อดิจิทัล (Certification Authority) แล้วปัจจุบันยังมีการประกอบการรับรองประเภทอื่น ๆที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์และถือว่าเป็นธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์อาจต้องนำมาพิจารณาว่าจำเป็นต้องมีการกำกับดูแลหรือไม่ หรือควรกำกับดูแลในรูปแบบใดอันจะก่อให้เกิดประโยชน์สูงสุดต่อผู้ประกอบการ และผู้ใช้บริการในเวลาเดียวกัน

บทที่ 4
ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ และคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์



4.1 ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ (มาตรา 35)[83]

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้บัญญัติหลักเกณฑ์เกี่ยวกับการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ไว้ในหมวด 4 มาตรา 35 โดยมีหลักการ ดังต่อไปนี้

[83] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติในลักษณะนี้ ได้แก่ Singapore Electronic Transactions Act 1998 Section 47 , Philippines Electronic Commerce Act 2000 Section 27, India Information Technology Act 2000 Section 6 , State of Illinois Electronic Commerce Security Act Section 25 **หรือ** Brunei Electronic Transaction Order 2000 Section 47 เป็นต้น

"คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใด ๆตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับ และให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด ทั้งนี้ ในพระราชกฤษฎีกาอาจกำหนดให้บุคคลที่เกี่ยวข้องต้องกระทำหรืองดเว้นกระทำการใด ๆ หรือให้หน่วยงานของรัฐออกระเบียบเพื่อกำหนดรายละเอียดในบางกรณีด้วยก็ได้

ในการออกพระราชกฤษฎีกาตามวรรคหนึ่ง พระราชกฤษฎีกาดังกล่าวอาจกำหนดให้ผู้ประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ต้องแจ้งให้ทราบต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาต แล้วแต่กรณี ก่อนประกอบกิจการก็ได้ ในกรณีนี้ให้นำบทบัญญัติในหมวด ๓ และบทกำหนดโทษที่เกี่ยวข้องมาใช้บังคับโดยอนุโลม"

มาตรานี้มีวัตถุประสงค์เพื่อส่งเสริมให้หน่วยงานภาครัฐใช้เทคโนโลยีสารสนเทศในการให้บริการประชาชน เพื่อเพิ่มศักยภาพในการบริการประชาชนให้ทันสมัย รวดเร็ว และสะดวกสบายมากยิ่งขึ้น รวมทั้งเป็นทางเลือกใหม่อีกทางหนึ่งให้แก่ประชาชนในการได้รับบริการ ไม่ว่าจะเป็นคำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน หรือการดำเนินงานต่าง ๆ

โดยปัจจุบัน หน่วยงานของรัฐบางหน่วยงานได้เริ่มมีการให้บริการด้วยวิธีการทางอิเล็กทรอนิกส์มากขึ้น นอกเหนือไปจากการนำข้อมูลเผยแพร่ทาง web site อาทิ

- กรมศุลกากรใช้ระบบการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI) ในการยื่นใบขนสินค้าและออกของให้กับผู้นำเข้าสินค้า (www.customs.go.th)

- การให้บริการค้นหาและจองชื่อนิติบุคคลออนไลน์และตรวจค้นข้อมูลธุรกิจออนไลน์ผ่านทางอินเทอร์เน็ต (www.thairegistration.com)

- การยื่นแบบแสดงรายการและชำระภาษี ภ.พ. 30, ภ.พ. 36, ภ.ธ. 40 , ภ.ง.ด. 54 และ ภ.ง.ด. 91 ผ่านทางอินเทอร์เน็ต

4.1.1 หลักเกณฑ์การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

ในการทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ ตามกฎหมายนี้จะต้องดำเนินการตามหลักเกณฑ์ที่กำหนดไว้ในมาตรา 35 โดยมีสาระสำคัญ กล่าวคือ "การดำเนินการใด ๆตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดในพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับ . . . "

จากหลักเกณฑ์ดังกล่าวพิจารณาได้ว่า ในการทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานภาครัฐหรือโดยหน่วยงานภาครัฐจะทำได้เมื่อมีการตราพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการที่หน่วยงานของรัฐจะต้องปฏิบัติก่อน จึงจะสามารถมีผลโดยชอบตามกฎหมายฉบับนี้

ทั้งนี้ เนื่องจากพระราชบัญญัติฉบับนี้เป็นกฎหมายที่รับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์เฉพาะในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง (มาตรา 8) เท่านั้น อาทิ การขอจดทะเบียนนิติบุคคล ดังนั้น การให้บริการอื่น ๆ ที่กฎหมายมิได้กำหนดให้ต้องทำเป็นหนังสือ หลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง แม้ไม่มีพระราชกฤษฎีกาประกาศหลักเกณฑ์และวิธีการไว้ ก็สามารถออกระเบียบหรือหลักเกณฑ์ต่าง ๆ ได้เองเพื่อให้สอดคล้องกับกฎหมายหรือขั้นตอนปฏิบัติที่หน่วยงานนั้น ๆ ดำเนินการอยู่ได้

อย่างไรก็ตาม พระราชกฤษฎีกาตามมาตรานี้อาจกำหนดหลักเกณฑ์กว้าง ๆ เพื่อเป็นหลักเกณฑ์กลางสำหรับทุกหน่วยงานที่จะต้องคำนึงถึง แต่สำหรับการออกรายละเอียดนั้น อาจจำเป็นที่จะต้องให้แต่ละหน่วยงานออกระเบียบภายในของตนเอง เพราะแต่ละหน่วยงานจะมีวิธีการและขั้นตอนในรายละเอียดการปฏิบัติที่แตกต่างกัน ทั้งนี้ หน่วยงานภาครัฐแต่ละหน่วยงานอาจเสนอให้มีการตราพระราชกฤษฎีกากำหนดรายละเอียดเกี่ยวกับขั้นตอนและวิธีการต่าง ๆได้ โดยแต่ละหน่วยงานเสนอมายังคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ซึ่งจะมีการจัดตั้งขึ้นในอนาคต เพื่อให้คณะกรรมการเสนอไปยังนายกรัฐมนตรีในการนำเข้าสู่การพิจารณาของคณะรัฐมนตรีต่อไป

อนึ่ง เนื่องจากในการดำเนินงานของรัฐ โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวกับวิธีปฏิบัติราชการทางปกครอง เช่น คำสั่งทางปกครองนั้น แม้พระราชบัญญัติฯ จะรับรองผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้มีเท่าเทียมกับกระดาษ แต่ก็เป็นเพียงการเปลี่ยนสื่อกลางที่ใช้บันทึกข้อความในรูปของข้อมูลอิเล็กทรอนิกส์เท่านั้น ซึ่งกฎเกณฑ์และเงื่อนไขของกฎหมายฉบับต่าง ๆ โดยเฉพาะอย่างยิ่งกฎหมายที่มีลักษณะเฉพาะ เช่น กฎหมายวิธีปฏิบัติราชการทางปกครองก็ยังคงต้องนำมาบังคับใช้ และอาจจำเป็นต้องนำหลักการสำคัญบางประการภายใต้กฎหมายเฉพาะซึ่งอาจจะไม่เอื้อต่อการทำธุรกรรมทางอิเล็กทรอนิกส์มากำหนดไว้ในพระราชกฤษฎีกาให้ชัดเจน

4.1.2 บทบัญญัติกฎหมายต่างประเทศ

บทบัญญัติกฎหมายต่างประเทศในลักษณะเดียวกับมาตรา 35 กล่าวคือการกำหนดให้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานของรัฐ ก็ได้มีบัญญัติไว้ในหลายประเทศ อาทิ

Electronic Transaction Act 1998 Section 47 ประเทศสิงคโปร์

Electronic Transaction Order 2000 Section 47 ประเทศบรูไน

Electronic Commerce Act 2000 Section 27 ประเทศฟิลิปปินส์

ซึ่งได้กำหนดหลักเกณฑ์เกี่ยวกับการใช้ข้อมูลอิเล็กทรอนิกส์ และลายมือชื่ออิเล็กทรอนิกส์ของหน่วยงานภาครัฐไว้ว่า ในกรณีที่หน่วยงานของรัฐต้องดำเนินการในกรณีซึ่งมีกฎหมายบัญญัติให้ต้องยื่นเอกสาร การสร้างหรือการเก็บรักษาเอกสาร การออกใบอนุญาต การอนุมัติ วิธีการชำระเงิน หรือการดำเนินการอื่นใด หน่วยงานของรัฐเช่นว่านั้นสามารถดำเนินการให้อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ได้ ในการนี้ หน่วยงานของรัฐหน่วยงานใดที่ประสงค์จะดำเนินการด้วยวิธีการดังกล่าวอาจกำหนดหลักเกณฑ์ในรายละเอียดต่าง ๆ ได้แก่

(1) รูปแบบของการยื่น การสร้าง หรือการเก็บรักษาเอกสาร

(2) ในกรณีที่ต้องลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ อาจกำหนดประเภทของลายมือชื่ออิเล็กทรอนิกส์ที่จำเป็นต้องใช้ อาทิ ลายมือชื่อดิจิทัล หรือลายมือชื่ออิเล็กทรอนิกส์อื่นใดที่มีความปลอดภัย (secure electronic signature)

(3) วิธีดำเนินการและรูปแบบของการใช้ลายมือชื่ออิเล็กทรอนิกส์ในข้อมูลอิเล็กทรอนิกส์ รวมไปถึงการระบุหลักเกณฑ์ซึ่งผู้ให้บริการรับรองจะต้องปฏิบัติตามหากมีการใช้บริการของผู้ประกอบการรับรองดังกล่าวในการยื่นเอกสาร

(4) กระบวนการควบคุมและวิธีการที่เหมาะสมเพื่อสร้างความเชื่อมั่นในระดับที่สมควรเกี่ยวกับการรักษาความถูกต้องแท้จริง (integrity) ความปลอดภัย (security) และการรักษาความลับของข้อมูลอิเล็กทรอนิกส์หรือการชำระเงิน

(5) ข้อกำหนดอื่นใดเกี่ยวกับข้อมูลอิเล็กทรอนิกส์หรือการชำระเงิน เพื่อให้มีผลเช่นเดียวกับการกระทำในรูปกระดาษ

อย่างไรก็ตาม บทบัญญัติดังกล่าวก็มิได้เป็นการบังคับให้หน่วยงานของรัฐจะต้องยอมรับ หรือจัดทำเอกสารในรูปข้อมูลอิเล็กทรอนิกส์ กล่าวคือ หากหน่วยงานของรัฐหน่วยงานใดประสงค์จะใช้วิธีการแบบดั้งเดิม คือระบบกระดาษก็สามารถทำได้ โดยขึ้นอยู่กับความพร้อมของหน่วยงานนั้น ๆในการนำวิธีการทางอิเล็กทรอนิกส์มาใช้ ซึ่งบทบัญญัติของประเทศสิงคโปร์และประเทศบรูไนจะมีความแตกต่างจากประเทศฟิลิปปินส์ที่ว่า บทบัญญัติตามกฎหมายของฟิลิปปินส์กำหนดให้หน่วยงานของรัฐยอมรับให้มีการยื่นเอกสาร การสร้างหรือการเก็บรักษาเอกสาร การออกใบอนุญาต การอนุมัติ วิธีการชำระเงิน หรือการออกใบเสร็จการชำระเงิน ผ่านระบบที่ใช้ข้อมูล

อิเล็กทรอนิกส์ ภายในสองปีนับแต่วันที่กฎหมาย Electronic Commerce Act 2000 มีผลใช้บังคับ (Section 27) ทั้งนี้ หน่วยงานของรัฐอาจกำหนดหลักเกณฑ์หรือข้อกำหนดในรายละเอียดในลักษณะเช่นเดียวกับประเทศสิงคโปร์และบรูไนด้วยก็ได้ โดยจะต้องเปิดให้มีการรับฟังความคิดเห็นจากประชาชนด้วย

4.2 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (มาตรา 36 – มาตรา 43)[84]

ดังที่ได้กล่าวมาแล้วในบทแรกว่ากฎหมายฉบับนี้เกิดจากการรวมหลักการของกฎหมายสองฉบับเข้าด้วยกัน กล่าวคือ กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และกฎหมายลายมือชื่ออิเล็กทรอนิกส์ ซึ่งบทบัญญัติในส่วนที่เกี่ยวกับคณะกรรมการนี้เป็นบทบัญญัติที่มาจากกฎหมายลายมือชื่ออิเล็กทรอนิกส์ ที่ประสงค์ให้ทำหน้าที่กำกับดูแลผู้ประกอบธุรกิจเกี่ยวกับการรับรองลายมือชื่ออิเล็กทรอนิกส์ โดยขณะนั้นใช้ชื่อว่า “คณะกรรมการลายมือชื่ออิเล็กทรอนิกส์” ต่อมาเมื่อกฎหมายฉบับนี้เข้าสู่การพิจารณาของวุฒิสภาก็ได้เปลี่ยนชื่อจาก “คณะกรรมการลายมือชื่ออิเล็กทรอนิกส์” เป็น “คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์” เพื่อรองรับการทำธุรกรรมทาง

---

[84] กฎหมายของหลายประเทศได้มีการจัดตั้งคณะกรรมการขึ้นเช่นกัน ทั้งนี้ส่วนใหญ่เป็นการจัดตั้งคณะกรรมการเพื่อดูแลเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์โดยเฉพาะ อาทิ Singapore Electronic Transactions Act 1998 Section 47 , India Information Technology Act 2000 Section 6 , Malaysia Digital Signature Act หรือ Brunei Electronic Transaction Order 2000 Section 47 เป็นต้น อย่างไรก็ตามในประเทศเกาหลีใต้ได้มีการจัดตั้งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ขึ้นภาย Basic Law on Electronic Commerce ขึ้น แต่ทำหน้าที่ในการส่งเสริมสนับสนุนการทำพาณิชย์อิเล็กทรอนิกส์

อิเล็กทรอนิกส์ในอนาคตที่มีความหลากหลายมากขึ้น ไม่ใช่เฉพาะแต่เพียงการประกอบการรับรองเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์เท่านั้น

เหตุผลสำคัญประการหนึ่งของการกำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ คือ สืบเนื่องจากการประกอบวิชาชีพของผู้ประกอบการรับรองหรือผู้ให้บริการเกี่ยวกับใบรับรองลายมือชื่ออิเล็กทรอนิกส์ซึ่งใช้ในการระบุตัวบุคคล อันมีความสำคัญอย่างยิ่งต่อผลผูกพันของการก่อนิติสัมพันธ์ระหว่างบุคคลและต่อการใช้สิทธิทางแพ่งของบุคคลในการดำเนินคดีกรณีที่เกิดความรับผิดขึ้น นอกจากนั้นยังเอื้อประโยชน์ต่อการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ แต่ในขณะเดียวกันหากมีการใช้เทคโนโลยีการเข้ารหัสก็อาจส่งผลกระทบต่อความมั่นคงของประเทศในกรณีที่มีการใช้ในทางมิชอบเกิดขึ้น ประกอบกับพัฒนาการทางเทคโนโลยีที่มีความเปลี่ยนแปลงอย่างรวดเร็วและมีความซับซ้อนเพิ่มขึ้น ดังนั้น จึงจำเป็นอย่างยิ่งที่จะต้องกำหนดให้มีการจัดตั้งคณะกรรมการธุรกรรมทางเล็กทรอนิกส์ เพื่อทำหน้าที่ในการวางนโยบายการส่งเสริมและพัฒนาระบบการรับรอง การสร้าง และการใช้ลายมือชื่ออิเล็กทรอนิกส์ รวมทั้งควบคุมและกำกับดูแลการประกอบการรับรอง โดยวางระเบียบกำหนดมาตรฐานด้านเทคนิคและมาตรการอันจำเป็นในการประกอบการรับรองลายมือชื่ออิเล็กทรอนิกส์ และกำหนดอัตราค่าบริการหรือค่าธรรมเนียม พร้อมทั้งหลักเกณฑ์เกี่ยวกับการขอใบอนุญาต การพักใช้และเพิกถอนใบอนุญาตของผู้ประกอบการรับรอง ดังนั้น การปฏิบัติหน้าที่ของคณะกรรมการดังกล่าวจึงต้องอาศัยผู้มีความรู้ ประสบการณ์ และความเชี่ยวชาญจากหลากหลายสาขา ทั้งนี้โดยมีรายละเอียดดังต่อไปนี้

4.2.1 บทบาทและอำนาจหน้าที่ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 37 ของพระราชบัญญัติฉบับนี้ได้กำหนดบทบาทและอำนาจหน้าที่ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ไว้ โดยมีอำนาจหน้าที่ดังต่อไปนี้

(1) เสนอแนะต่อคณะรัฐมนตรีเพื่อวางนโยบายการส่งเสริมและพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ตลอดจนการแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้อง

(2) ติดตามดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

(3) เสนอแนะหรือให้คำปรึกษาต่อรัฐมนตรีเพื่อการตราพระราชกฤษฎีกาตามพระราชบัญญัตินี้

(4) ออกระเบียบหรือประกาศเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์เพื่อให้เป็นไปตามพระราชบัญญัตินี้หรือตามพระราชกฤษฎีกาที่ออกตามพระราชบัญญัตินี้

(5) ปฏิบัติการอื่นใดเพื่อให้เป็นไปตามพระราชบัญญัตินี้ หรือกฎหมายอื่น

4.2.2 ที่มาของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

จากหลักเกณฑ์ตามที่กำหนดไว้ในพระราชบัญญัติฯ จะเห็นได้ว่าคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มีจำนวนทั้งสิ้น 14 คน ประกอบไปด้วยกรรมการโดยตำแหน่ง และกรรมการผู้ทรงคุณวุฒิ ดังนี้

(1) รัฐมนตรีว่าการประทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม เป็นประธานกรรมการ

(2) กรรมการผู้ทรงคุณวุฒิ จำนวน 12 คน ซึ่งคณะรัฐมนตรีเป็นผู้แต่งตั้ง

(3) ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติเป็นกรรมการและเลขานุการ

สำหรับหลักเกณฑ์และวิธีการสรรหากรรมการ รวมทั้งการเสนอชื่อบุคคลที่เห็นสมควรต่อคณะรัฐมนตรีเพื่อพิจารณาแต่งตั้งเป็นคณะกรรมการ ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด ซึ่งคำว่ารัฐมนตรีในที่นี้ ตามคำนิยาม มาตรา 4 ของพระราชบัญญัติฯ หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัติ ซึ่งหมายถึงนายกรัฐมนตรี ดังนั้น ในการกำหนดหลักเกณฑ์และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิจึงต้องจัดทำเป็นระเบียบสำนักนายกรัฐมนตรีต่อไป

4.2.3 องค์ประกอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้กำหนดให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกอบด้วยจำนวนทั้งสิ้น 14 คน ซึ่งแยกพิจารณาได้ดังนี้

(ก) **คณะกรรมการโดยตำแหน่ง 2 คน** ได้แก่

- รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม เป็นประธานกรรมการ
- ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เป็นกรรมการและเลขานุการ

(ข) **คณะกรรมการผู้ทรงคุณวุฒิ** 12 **คน**

ซึ่งกฎหมายฉบับนี้ได้กำหนดให้คณะกรรมการผู้ทรงคุณวุฒิต้องมาจากผู้ทรงคุณวุฒิในด้านต่าง ๆ ดังต่อไปนี้ด้านละสองคน ได้แก่

- การเงิน
- การพาณิชย์อิเล็กทรอนิกส์
- นิติศาสตร์
- วิทยาการคอมพิวเตอร์
- วิทยาศาสตร์หรือวิศวกรรมศาสตร์
- สังคมศาสตร์

ทั้งนี้ กรรมการผู้ทรงคุณวุฒิคนหนึ่งของแต่ละด้านต้องมาจากภาคเอกชน ด้วย เหตุผลที่ว่า คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เป็นคณะกรรมการที่มีบทบาทสำคัญในการเสนอแนะให้มีการวางนโยบายการส่งเสริมและพัฒนาธุรกรรมทาง

อิเล็กทรอนิกส์ ตลอดจนเสนอแนะให้มีการตราพระราชกฤษฎีกาตามกฎหมายนี้ ดังนั้นจึงจำเป็นที่จะต้องมีผู้แทนจากภาคเอกชนเพื่อให้การเสนอแนะการวางนโยบายและการตราพระราชกฤษฎีกา มีความสอดคล้องกับแนวปฏิบัติที่มีอยู่ไม่ว่าในประเทศหรือต่างประเทศ รวมทั้งเพื่อมิให้หลักเกณฑ์ต่าง ๆ ที่อาจเกิดขึ้นในอนาคตเป็นหลักเกณฑ์ที่ไม่เอื้อหรือไม่ส่งเสริมต่อการทำธุรกรรมทางอิเล็กทรอนิกส์

4.2.4 วาระการดำรงตำแหน่งของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

กฎหมายฉบับนี้กำหนดให้กรรมการผู้ทรงคุณวุฒิมีวาระการดำรงตำแหน่งสามปี และกรรมการซึ่งพ้นจากตำแหน่งอาจได้รับแต่งตั้งอีกได้ แต่ไม่เกินสองวาระติดกันนอกจากการพ้นจากตำแหน่งของกรรมการผู้ทรงคุณวุฒิตามวาระแล้ว กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งเมื่อ

- ตาย
- ลาออก
- คณะรัฐมนตรีให้ออกเพราะมีความประพฤติเสื่อมเสีย บกพร่อง หรือไม่สุจริตต่อหน้าที่ หรือหย่อนความสามารถ
- เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ
- ได้รับโทษจำคุกโดยต้องคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

4.3 บทกำหนดโทษ (มาตรา 44 - มาตรา 46)[85]

เนื่องจากร่างพระราชบัญญัติฯได้กำหนดหน้าที่ของบุคคลหลายฝ่ายที่เกี่ยวข้อง กล่าวคือ ผู้ถือใบรับรอง หรือผู้ประกอบการรับรอง เป็นต้น จึงได้มีการกำหนดบทลงโทษกรณีฝ่าฝืนบทบัญญัติของกฎหมายเอาไว้ด้วย ทั้งนี้ เนื่องจากมาตรา 35 กำหนดให้คณะกรรมการลายมือชื่ออิเล็กทรอนิกส์อาจเสนอให้มีการตรากฎหมายกำหนดให้ผู้ที่ประสงค์จะประกอบธุรกิจบางประเภทจำเป็นต้องแจ้ง หรือขึ้นทะเบียน หรือขออนุญาต เพราะอาจเป็นกิจการที่กระทบต่อความมั่นคงทางการเงินหรือพาณิชย์ และได้มีการกำหนดหลักเกณฑ์และวิธีการแจ้ง หรือขึ้นทะเบียน หรือรับอนุญาตตามร่างพระราชบัญญัติฯ มาตรา 36 และ37 ตามลำดับ จึงต้องมีการกำหนดโทษไว้ด้วยในกรณีที่มีการฝ่าฝืนบทบัญญัติของกฎหมาย โดยมีทั้งโทษจำคุกและปรับ นอกจากนี้ยังได้กำหนดโทษของผู้จัดการนิติบุคคลหรือผู้แทนนิติบุคคลไว้ด้วย

---

[85] ตัวอย่างกฎหมายต่างประเทศที่มีการบัญญัติบทบัญญัตินี้ ได้แก่ Singapore Electronic Transactions Act 1998 Section 42(3) และ Section 49 , Malaysia Digital Signature Act Section 4(2)และ Section 74 , Ireland Electronic Commerce Bill 2000 Section 30 หรือ Brunei Electronic Transaction Order 2000 Section 42(3)และ Section 49 เป็นต้น

บรรณานุกรม

หนังสือไทย

1. ครรชิต มาลัยวงศ์, ***ก้าวไกลไปกับคอมพิวเตอร์ : สาระคอมพิวเตอร์ที่ข้าราชการต้องรู้*** (กรุงเทพฯ : ซีเอ็ดยูเคชั่น), 2539
2. จำปี โสตถิพันธุ์, ***นิติกรรม-สัญญา*** (กรุงเทพฯ : บริษัทสำนักพิมพ์วิญญูชน จำกัด), 2542
3. ฉัททวุฒิ พืชผล, ***เปิดโลกการค้าอิเล็กทรอนิกส์*** (กรุงเทพฯ: โปรวิชั่น), 2541
4. ชนม์ชนก วีรวรรณ, ***การ์ตูนไกด์ ท่องอินเตอร์เน็ต*** (ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ), 2537
5. พงษ์ระพี เตชพาพงษ์, ***คอมพิวเตอร์เข้าใจง่าย*** (กรุงเทพฯ : ซีเอ็ดยูเคชั่น), 2539
6. พิพัฒน์ หิรัณย์วณิชชากร, ***ระบบการสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์*** (กรุงเทพฯ : ซีเอ็ดยูเคชั่น), 2543
7. ยืน ภู่สุวรรณ, ***บนเส้นทางพาณิชย์อิเล็กทรอนิกส์*** (กรุงเทพฯ: ซีเอ็ดยูเคชั่น), 2543
8. ลอง, ลารี, ***เทคโนโลยีคอมพิวเตอร์และสารสนเทศ*** (กรุงเทพฯ : เพียร์สัน เอ็ดดูเคชั่น อินโดไชน่า), 2543
9. ศรีไพร ศักดิ์รุ่งพงศากุล, ***เทคโนโลยีคอมพิวเตอร์ และสารสนเทศ*** (กรุงเทพฯ: ซีเอ็ดยูเคชั่น), 2544

10. สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, แบบสำรวจแนวทางการจัดทำแผนปฏิบัติการ e-Government, และ เอกสารแนะนำโครงการที่ได้รับรางวัล ***"โครงการเทคโนโลยีสารสนเทศภาครัฐดีเด่น"***, ครั้งที่ 1 พ.ศ. 2543
11. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

หนังสือต่างประเทศ

1. George B. Delta, Jeffrey H. Matsuura, ***Law of the INTERNET*** (the United States of America : Permisions Aspen Law &Business)
2. J. Christopher Westland, Theodore H.K. Clark, GLOBAL ***ELECTRONIC COMMERCE : Theory and Case Studies***,(United States of America : Library of Congress),1999
3. Jonathan Rosenoer, CyberLaw : ***THE LAW OF THE INTERNET***, (San Francisco : R.R. Donnelley and Sons, Harrisonburg VA.), 1996
4. UNCITRAL.,***ELECTRONIC DATA INTERCHANGE Report of the Secretary-General Twenty-fourth session*** *Vienna,10 - 28 June 1991*

5. UNCITRAL., ***UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5bis as adopted in 1998*** (Austria : United Nations Publication,), 1999

6. UNCITRAL., ***Planning of future work on electronic commerce : Digital Signatures, Certification Authorities and related legal issues 31st session****, 18-28 February 1997, New York*

7. UNCITRAL*., **Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 38th session**, 12-23 March 2001, New York*

8. Whitfield Diffie, Susan Landau, Privacy on the line: The Politics of Wiretapping and Encryption (London : The MIT Press), 1999

ภาคผนวก

พระราชบัญญัติ
ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
พ.ศ. ๒๕๔๔

ภูมิพลอดุลยเดช ป.ร.
ให้ไว้ ณ วันที่ ๒ ธันวาคม พ.ศ. ๒๕๔๔
เป็นปีที่ ๕๖ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรให้มีกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๙ ประกอบกับมาตรา ๕๐ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของรัฐสภา ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ พระราชบัญญัตินี้ให้ใช้บังคับแก่ธุรกรรมในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ เว้นแต่ธุรกรรมที่มีพระราชกฤษฎีกากำหนดมิให้นำพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับ

ความในวรรคหนึ่งไม่มีผลกระทบกระเทือนถึงกฎหมายหรือกฎใดที่กำหนดขึ้นเพื่อคุ้มครองผู้บริโภค

พระราชบัญญัตินี้ให้ใช้บังคับแก่ธุรกรรมในการดำเนินงานของรัฐตามที่กำหนดในหมวด ๔

มาตรา ๔ ในพระราชบัญญัตินี้

"**ธุรกรรม**" หมายความว่า การกระทำใด ๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐตามที่กำหนดในหมวด ๔

"**อิเล็กทรอนิกส์**" หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น

"**ธุรกรรมทางอิเล็กทรอนิกส์**" หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน

"**ข้อความ**" หมายความว่า เรื่องราวหรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ

"**ข้อมูลอิเล็กทรอนิกส์**" หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

"**ลายมือชื่ออิเล็กทรอนิกส์**" หมายความว่า อักษร อักขระ ตัวเลข เสียง หรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

"**ระบบข้อมูล**" หมายความว่า กระบวนการประมวลผลด้วยเครื่องมืออิเล็กทรอนิกส์สำหรับสร้าง ส่ง รับ เก็บรักษา หรือประมวลผลข้อมูลอิเล็กทรอนิกส์

"**การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์**" หมายความว่า การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

"**ผู้ส่งข้อมูล**" หมายความว่า บุคคลซึ่งเป็นผู้ส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีการที่ผู้นั้นกำหนด โดยบุคคลนั้นอาจจะส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

"**ผู้รับข้อมูล**" หมายความว่า บุคคลซึ่งผู้ส่งข้อมูลประสงค์จะส่งข้อมูลอิเล็กทรอนิกส์ให้และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

"**บุคคลที่เป็นสื่อกลาง**" หมายความว่า บุคคลซึ่งกระทำการในนามผู้อื่นในการส่ง รับ หรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์อันใดอันหนึ่งโดยเฉพาะ รวมถึงให้บริการอื่นที่เกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น

"**ใบรับรอง**" หมายความว่า ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์

"**เจ้าของลายมือชื่อ**" หมายความว่า ผู้ซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์และสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นในนามตนเองหรือแทนบุคคลอื่น

"**คู่กรณีที่เกี่ยวข้อง**" หมายความว่า ผู้ซึ่งอาจกระทำการใด ๆ โดยขึ้นอยู่กับใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์

"**หน่วยงานของรัฐ**" หมายความว่า กระทรวง ทบวง กรม ส่วนราชการที่เรียกชื่ออย่างอื่นและมีฐานะเป็นกรม ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจที่ตั้งขึ้นโดยพระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใด ๆ

"**คณะกรรมการ**" หมายความว่า คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

"**รัฐมนตรี**" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๕ บทบัญญัติมาตรา ๑๓ ถึงมาตรา ๒๔ และบทบัญญัติมาตรา ๒๖ ถึงมาตรา ๓๑ จะตกลงกันเป็นอย่างอื่นก็ได้

มาตรา ๖ ให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัตินี้

หมวด ๑
ธุรกรรมทางอิเล็กทรอนิกส์

มาตรา ๗ ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

มาตรา ๘ ภายใต้บังคับบทบัญญัติแห่งมาตรา ๙ ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว

มาตรา ๙ ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(๑) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(๒) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์

ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

มาตรา ๑๐ ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

(๑) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ

(๒) สามารถแสดงข้อความนั้นในภายหลังได้

ความถูกต้องของข้อความตาม (๑) ให้พิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงใดของข้อความ เว้นแต่การรับรองหรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใด ๆ ที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงข้อความซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้น

ในการวินิจฉัยความน่าเชื่อถือของวิธีการรักษาความถูกต้องของข้อความตาม (๑) ให้พิเคราะห์ถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง รวมทั้งวัตถุประสงค์ของการสร้างข้อความนั้น

มาตรา ๑๑ ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษาความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

มาตรา ๑๒ ภายใต้บังคับบทบัญญัติมาตรา ๑๐ ในกรณีที่กฎหมายกำหนดให้เก็บรักษาเอกสารหรือข้อความใด ถ้าได้เก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการเก็บรักษาเอกสารหรือข้อความตามที่กฎหมายต้องการแล้ว

(๑) ข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง

(๒) ได้เก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นให้อยู่ในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์นั้น หรืออยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับให้ปรากฏอย่างถูกต้องได้ และ

(๓) ได้เก็บรักษาข้อความส่วนที่ระบุถึงแหล่งกำเนิด ต้นทางและปลายทางของข้อมูลอิเล็กทรอนิกส์ ตลอดจนวันและเวลาที่ส่งหรือได้รับข้อความดังกล่าว ถ้ามี

ความในวรรคหนึ่ง มิให้ใช้บังคับกับข้อความที่ใช้เพียงเพื่อวัตถุประสงค์ในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์

หน่วยงานของรัฐที่รับผิดชอบในการเก็บรักษาเอกสารหรือข้อความใด อาจกำหนดหลักเกณฑ์รายละเอียดเพิ่มเติมเกี่ยวกับการเก็บรักษาเอกสารหรือข้อความนั้นได้ เท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติในมาตรานี้

มาตรา ๑๓ คำเสนอหรือคำสนองในการทำสัญญาอาจทำเป็นข้อมูลอิเล็กทรอนิกส์ก็ได้ และห้ามมิให้ปฏิเสธการมีผลทางกฎหมายของสัญญาเพียงเพราะเหตุที่สัญญานั้นได้ทำคำเสนอหรือคำสนองเป็นข้อมูลอิเล็กทรอนิกส์

มาตรา ๑๔ ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล การแสดงเจตนาหรือคำบอกกล่าวอาจทำเป็นข้อมูลอิเล็กทรอนิกส์ก็ได้

มาตรา ๑๕ บุคคลใดเป็นผู้ส่งข้อมูลไม่ว่าจะเป็นการส่งโดยวิธีใด ให้ถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้นั้น

ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล ให้ถือว่าเป็นข้อมูลอิเล็กทรอนิกส์ของผู้ส่งข้อมูล หากข้อมูลอิเล็กทรอนิกส์นั้นได้ส่งโดย

(๑) บุคคลผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูลเกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น หรือ

(๒) ระบบข้อมูลที่ผู้ส่งข้อมูลหรือบุคคลผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูลได้กำหนดไว้ล่วงหน้าให้สามารถทำงานได้โดยอัตโนมัติ

มาตรา ๑๖ ผู้รับข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูลและชอบที่จะดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์นั้นได้ ถ้า

(๑) ผู้รับข้อมูลได้ตรวจสอบโดยสมควรตามวิธีการที่ได้ตกลงกับผู้ส่งข้อมูลว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูล หรือ

(๒) ข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นเกิดจากการกระทำของบุคคลซึ่งใช้วิธีการที่ผู้ส่งข้อมูลใช้ในการแสดงว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นของผู้ส่งข้อมูล ซึ่งบุคคลนั้นได้ล่วงรู้โดยอาศัยความสัมพันธ์ระหว่างบุคคลนั้นกับผู้ส่งข้อมูลหรือผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูล

ความในวรรคหนึ่งมิให้ใช้บังคับ ถ้า

(๑) ในขณะนั้นผู้รับข้อมูลได้รับแจ้งจากผู้ส่งข้อมูลว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นมิใช่ของผู้ส่งข้อมูล และในขณะเดียวกันผู้รับข้อมูลมีเวลาพอสมควรที่จะตรวจสอบข้อเท็จจริงตามที่ได้รับแจ้งนั้น หรือ

(๒) กรณีตามวรรคหนึ่ง (๒) เมื่อผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์นั้นไม่ใช่ของผู้ส่งข้อมูล หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควร หรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา ๑๗ ในกรณีตามมาตรา ๑๕ หรือมาตรา ๑๖ วรรคหนึ่ง ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล ผู้รับข้อมูลมีสิทธิถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับนั้นถูกต้องตามเจตนาของผู้ส่งข้อมูล และสามารถดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์นั้นได้ เว้นแต่ผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์ที่

ได้รับนั้นมีข้อผิดพลาดอันเกิดจากการส่ง หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควรหรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา ๑๘ ผู้รับข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับแต่ละชุดเป็นข้อมูลที่แยกจากกัน และสามารถดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์แต่ละชุดนั้นได้ เว้นแต่ข้อมูลอิเล็กทรอนิกส์ชุดนั้นจะซ้ำกับข้อมูลอิเล็กทรอนิกส์อีกชุดหนึ่ง และผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นข้อมูลอิเล็กทรอนิกส์ซ้ำ หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควรหรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา ๑๙ ในกรณีที่ต้องมีการตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ ไม่ว่าผู้ส่งข้อมูลได้ร้องขอ หรือตกลงกับผู้รับข้อมูลไว้ก่อนหรือขณะที่ส่งข้อมูลอิเล็กทรอนิกส์หรือปรากฏในข้อมูลอิเล็กทรอนิกส์ ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(๑) ในกรณีที่ผู้ส่งข้อมูลมิได้ตกลงให้ตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ในรูปแบบหรือวิธีการใดโดยเฉพาะ การตอบแจ้งการรับอาจทำได้ด้วยการติดต่อสื่อสารจากผู้รับข้อมูล ไม่ว่าโดยระบบข้อมูลที่ทำงานโดยอัตโนมัติหรือโดยวิธีอื่นใด หรือด้วยการกระทำใด ๆ ของผู้รับข้อมูลซึ่งเพียงพอจะแสดงต่อผู้ส่งข้อมูลว่าผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์นั้นแล้ว

(๒) ในกรณีที่ผู้ส่งข้อมูลกำหนดเงื่อนไขว่าจะถือว่ามีการส่งข้อมูลอิเล็กทรอนิกส์ต่อเมื่อได้รับการตอบแจ้งการรับจากผู้รับข้อมูล ให้ถือว่ายังไม่มีการส่งข้อมูลอิเล็กทรอนิกส์จนกว่าผู้ส่งข้อมูลจะได้รับการตอบแจ้งการรับแล้ว

(๓) ในกรณีที่ผู้ส่งข้อมูลมิได้กำหนดเงื่อนไขตามความใน (๒) และผู้ส่งข้อมูลมิได้รับการตอบแจ้งการรับนั้นภายในเวลาที่กำหนดหรือตกลงกัน หรือภายในระยะเวลาอันสมควรในกรณีที่มิได้กำหนดหรือตกลงเวลาไว้

(ก) ผู้ส่งข้อมูลอาจส่งคำบอกกล่าวไปยังผู้รับข้อมูลว่าตนยังมิได้รับการตอบแจ้งการรับ และกำหนดระยะเวลาอันสมควรให้ผู้รับข้อมูลตอบแจ้งการรับ และ

(ข) หากผู้ส่งข้อมูลมิได้รับการตอบแจ้งการรับภายในระยะเวลาตาม (ก) เมื่อผู้ส่งข้อมูลบอกกล่าวแก่ผู้รับข้อมูลแล้ว ผู้ส่งข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมิได้มีการส่งเลยหรือผู้ส่งข้อมูลอาจใช้สิทธิอื่นใดที่ผู้ส่งข้อมูลมีอยู่ได้

มาตรา ๒๐ ในกรณีที่ผู้ส่งข้อมูลได้รับการตอบแจ้งการรับจากผู้รับข้อมูลให้สันนิษฐานว่าผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องแล้ว แต่ข้อสันนิษฐานดังกล่าวมิให้ถือว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นถูกต้องตรงกันกับข้อมูลอิเล็กทรอนิกส์ที่ผู้ส่งข้อมูลได้ส่งมา

มาตรา ๒๑ ในกรณีที่ปรากฏในการตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์นั้นเองว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับเป็นไปตามข้อกำหนดทางเทคนิคที่ผู้ส่งข้อมูลและผู้รับข้อมูลได้ตกลงหรือระบุไว้ในมาตรฐานซึ่งใช้บังคับอยู่ ให้สันนิษฐานว่าข้อมูลอิเล็กทรอนิกส์ที่ส่งไปนั้นได้เป็นไปตามข้อกำหนดทางเทคนิคทั้งหมดแล้ว

มาตรา ๒๒ การส่งข้อมูลอิเล็กทรอนิกส์ให้ถือว่าได้มีการส่งเมื่อข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่อยู่นอกเหนือการควบคุมของผู้ส่งข้อมูล

มาตรา ๒๓ การรับข้อมูลอิเล็กทรอนิกส์ให้ถือว่ามีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลของผู้รับข้อมูล

หากผู้รับข้อมูลได้กำหนดระบบข้อมูลที่ประสงค์จะใช้ในการรับข้อมูลอิเล็กทรอนิกส์ไว้โดยเฉพาะ ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่ผู้รับข้อมูลได้กำหนดไว้นั้น แต่ถ้าข้อมูลอิเล็กทรอนิกส์ดังกล่าวได้ส่งไปยังระบบข้อมูลอื่นของผู้รับข้อมูลซึ่งมิใช่ระบบข้อมูลที่ผู้รับข้อมูลกำหนดไว้ ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ได้เรียกข้อมูลอิเล็กทรอนิกส์จากระบบข้อมูลนั้น

ความในมาตรานี้ให้ใช้บังคับแม้ระบบข้อมูลของผู้รับข้อมูลตั้งอยู่ในสถานที่

อีกแห่งหนึ่งต่างหากจากสถานที่ที่ถือว่าผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์ตามมาตรา ๒๔

มาตรา ๒๔ การส่งหรือการรับข้อมูลอิเล็กทรอนิกส์ ให้ถือว่าได้ส่ง ณ ที่ทำการงานของผู้ส่งข้อมูล หรือได้รับ ณ ที่ทำการงานของผู้รับข้อมูล แล้วแต่กรณี

ในกรณีที่ผู้ส่งข้อมูลหรือผู้รับข้อมูลมีที่ทำการงานหลายแห่ง ให้ถือเอาที่ทำการงานที่เกี่ยวข้องมากที่สุดกับธุรกรรมนั้นเป็นที่ทำการงานเพื่อประโยชน์ตามวรรคหนึ่ง แต่ถ้าไม่สามารถกำหนดได้ว่าธุรกรรมนั้นเกี่ยวข้องกับที่ทำการงานแห่งใดมากที่สุด ให้ถือเอาสำนักงานใหญ่เป็นสถานที่ที่ได้รับหรือส่งข้อมูลอิเล็กทรอนิกส์นั้น

ในกรณีที่ไม่ปรากฏที่ทำการงานของผู้ส่งข้อมูลหรือผู้รับข้อมูล ให้ถือเอาถิ่นที่อยู่ปกติเป็นสถานที่ที่ส่งหรือได้รับข้อมูลอิเล็กทรอนิกส์

ความในมาตรานี้มิให้ใช้บังคับกับการส่งและการรับข้อมูลอิเล็กทรอนิกส์โดยวิธีการทางโทรเลขและโทรพิมพ์ หรือวิธีการสื่อสารอื่นตามที่กำหนดในพระราชกฤษฎีกา

มาตรา ๒๕ ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้

หมวด ๒
ลายมือชื่ออิเล็กทรอนิกส์

มาตรา ๒๖ ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(๑) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(๒) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการ

ควบคุมของบุคคลอื่น

(๓) การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้ และ

(๔) ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

บทบัญญัติในวรรคหนึ่ง ไม่เป็นการจำกัดว่าไม่มีวิธีการอื่นใดที่แสดงได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หรือการแสดงพยานหลักฐานใดเกี่ยวกับความไม่น่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

มาตรา ๒๗ ในกรณีมีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์เพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ที่จะมีผลตามกฎหมาย เจ้าของลายมือชื่อต้องดำเนินการดังต่อไปนี้

(๑) ใช้ความระมัดระวังตามสมควรเพื่อมิให้มีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

(๒) แจ้งให้บุคคลที่คาดหมายได้โดยมีเหตุอันควรเชื่อว่าจะกระทำการใดโดยขึ้นอยู่กับลายมือชื่ออิเล็กทรอนิกส์หรือให้บริการเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ทราบโดยมิชักช้า เมื่อ

(ก) เจ้าของลายมือชื่อรู้หรือควรได้รู้ว่าข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นสูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบหรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(ข) เจ้าของลายมือชื่อรู้จากสภาพการณ์ที่ปรากฏว่ากรณีมีความเสี่ยงมากพอที่ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ สูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(๓) ในกรณีมีการออกใบรับรองสนับสนุนการใช้ลายมือชื่ออิเล็กทรอนิกส์จะต้องใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้องและสมบูรณ์ของการแสดงสาระสำคัญทั้งหมด ซึ่งกระทำโดยเจ้าของลายมือชื่อเกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรอง หรือตามที่มีการกำหนดในใบรับรอง

มาตรา ๒๘ ในกรณีมีการให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ให้มีผลทางกฎหมายเสมือนหนึ่งลงลายมือชื่อ ผู้ให้บริการออกใบรับรองต้องดำเนินการ ดังต่อไปนี้

(๑) ปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ตนได้แสดงไว้

(๒) ใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้องและความสมบูรณ์ของการแสดงสาระสำคัญทั้งหมดที่ตนได้กระทำเกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรอง หรือตามที่มีการกำหนดในใบรับรอง

(๓) จัดให้มีวิธีการในการเข้าถึงโดยสมควร ให้คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบข้อเท็จจริงในการแสดงสาระสำคัญทั้งหมดจากใบรับรองได้ ในเรื่องดังต่อไปนี้

(ก) การระบุผู้ให้บริการออกใบรับรอง

(ข) เจ้าของลายมือชื่อซึ่งระบุในใบรับรองได้ควบคุมข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ในขณะมีการออกใบรับรอง

(ค) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์มีผลใช้ได้ในขณะหรือก่อนที่มีการออกใบรับรอง

(๔) จัดให้มีวิธีการเข้าถึงโดยสมควร ให้คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบกรณีดังต่อไปนี้จากใบรับรองหรือจากวิธีอื่น

(ก) วิธีการที่ใช้ในการระบุตัวเจ้าของลายมือชื่อ

(ข) ข้อจำกัดเกี่ยวกับวัตถุประสงค์และคุณค่าที่มีการนำข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์หรือใบรับรอง

(ค) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์มีผลสมบูรณ์ใช้ได้และไม่สูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(ง) ข้อจำกัดเกี่ยวกับขอบเขตความรับผิดที่ผู้ให้บริการออกใบรับรองได้ระบุไว้

(จ) การมีวิธีการให้เจ้าของลายมือชื่อส่งคำบอกกล่าวเมื่อมีเหตุตามมาตรา ๒๗ (๒)

(ฉ) การมีบริการเกี่ยวกับการเพิกถอนใบรับรองที่ทันการ

(๕) ในกรณีที่มีบริการตาม (๔) (จ) บริการนั้นต้องมีวิธีการที่ให้เจ้าของลายมือชื่อสามารถแจ้งได้ตามหลักเกณฑ์ที่กำหนดตามมาตรา ๒๗ (๒) และในกรณีที่มีบริการตาม (๔) (ฉ) บริการนั้นต้องสามารถเพิกถอนใบรับรองได้ทันการ

(๖) ใช้ระบบ วิธีการ และบุคลากรที่เชื่อถือได้ในการให้บริการ

มาตรา ๒๙ ในการพิจารณาความเชื่อถือได้ของระบบ วิธีการ และบุคลากรตามมาตรา ๒๘ (๖) ให้คำนึงถึงกรณีดังต่อไปนี้

(๑) สถานภาพทางการเงิน บุคลากร และสินทรัพย์ที่มีอยู่

(๒) คุณภาพของระบบฮาร์ดแวร์และซอฟต์แวร์

(๓) วิธีการออกใบรับรอง การขอใบรับรอง และการเก็บรักษาข้อมูลการให้บริการนั้น

(๔) การจัดให้มีข้อมูลข่าวสารเกี่ยวกับเจ้าของลายมือชื่อ ที่ระบุในใบรับรองและผู้ที่อาจคาดหมายได้ว่าจะเป็นคู่กรณีที่เกี่ยวข้อง

(๕) ความสม่ำเสมอและขอบเขตในการตรวจสอบโดยผู้ตรวจสอบอิสระ

(๖) องค์กรที่ให้การรับรองหรือให้บริการออกใบรับรองเกี่ยวกับการปฏิบัติหรือการมีอยู่ของสิ่งที่กล่าวมาใน (๑) ถึง (๕)

(๗) กรณีใด ๆ ที่คณะกรรมการประกาศกำหนด

มาตรา ๓๐ คู่กรณีที่เกี่ยวข้องต้องดำเนินการ ดังต่อไปนี้

(๑) ดำเนินการตามสมควรในการตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

(๒) ในกรณีลายมือชื่ออิเล็กทรอนิกส์มีใบรับรอง ต้องมีการดำเนินการตามสมควร ดังนี้

(ก) ตรวจสอบความสมบูรณ์ของใบรับรอง การพักใช้ หรือการเพิกถอนใบรับรอง และ

(ข) ปฏิบัติตามข้อจำกัดใด ๆ ที่เกี่ยวกับใบรับรอง

มาตรา ๓๑ ใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ให้ถือว่ามีผลทางกฎหมายโดยไม่ต้องคำนึงถึง

(๑) สถานที่ออกใบรับรองหรือสถานที่สร้างหรือใช้ลายมือชื่ออิเล็กทรอนิกส์ หรือ

(๒) สถานที่ทำการงานของผู้ออกใบรับรองหรือเจ้าของลายมือชื่ออิเล็กทรอนิกส์

ใบรับรองที่ออกในต่างประเทศให้มีผลตามกฎหมายในประเทศเช่นเดียวกับใบรับรองที่ออกในประเทศ หากการออกใบรับรองดังกล่าวได้ใช้ระบบที่เชื่อถือได้ไม่น้อยกว่าระบบที่เชื่อถือได้ตามพระราชบัญญัตินี้

ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างหรือใช้ในต่างประเทศให้ถือว่ามีผลตามกฎหมายในประเทศเช่นเดียวกับลายมือชื่ออิเล็กทรอนิกส์ที่สร้างหรือใช้ในประเทศ หากการสร้างหรือใช้ลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวได้ใช้ระบบที่เชื่อถือได้ไม่น้อยกว่าระบบที่เชื่อถือได้ตามพระราชบัญญัตินี้

ในการพิจารณาว่าใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ใดมีความเชื่อถือได้ตามวรรคสองหรือวรรคสาม ให้คำนึงถึงมาตรฐานระหว่างประเทศและปัจจัยอื่น ๆ ที่เกี่ยวข้องประกอบด้วย

หมวด ๓
ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

มาตรา ๓๒ บุคคลย่อมมีสิทธิประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ แต่ในกรณีที่จำเป็นเพื่อรักษาความมั่นคงทางการเงินและการพาณิชย์ หรือเพื่อประโยชน์ในการเสริมสร้างความเชื่อถือและยอมรับในระบบข้อมูล

อิเล็กทรอนิกส์ หรือเพื่อป้องกันความเสียหายต่อสาธารณชน ให้มีการตราพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ใดเป็นกิจการที่ต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตก่อนก็ได้

ในการกำหนดให้กรณีใดต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตตามวรรคหนึ่ง ให้กำหนดโดยพิจารณาจากความเหมาะสมในการป้องกันความเสียหายตามระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจากการประกอบธุรกิจนั้น

ในการนี้ จะกำหนดให้หน่วยงานของรัฐแห่งหนึ่งแห่งใดเป็นผู้รับผิดชอบในการควบคุมดูแลในพระราชกฤษฎีกาดังกล่าวก็ได้

ก่อนเสนอให้ตราพระราชกฤษฎีกาตามวรรคหนึ่ง ต้องจัดให้มีการรับฟังความคิดเห็นของประชาชนตามความเหมาะสม และนำข้อมูลที่ได้รับมาประกอบการพิจารณา

มาตรา ๓๓ ในกรณีที่มีพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ใดเป็นกิจการที่ต้องแจ้งให้ทราบ หรือต้องขึ้นทะเบียน ให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวต้องแจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาก่อนเริ่มประกอบธุรกิจนั้น

หลักเกณฑ์และวิธีการแจ้งหรือขึ้นทะเบียนตามวรรคหนึ่ง ให้เป็นไปตามที่กำหนดในพระราชกฤษฎีกา และเมื่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาได้รับแจ้งหรือรับขึ้นทะเบียนให้ออกใบรับแจ้งหรือใบรับขึ้นทะเบียนเพื่อเป็นหลักฐานการแจ้งหรือการขึ้นทะเบียนในวันที่ได้รับแจ้งหรือรับขึ้นทะเบียน และให้ผู้แจ้งหรือผู้ขึ้นทะเบียนประกอบธุรกิจนั้นได้ตั้งแต่วันที่ได้รับแจ้งหรือรับขึ้นทะเบียน แต่ถ้าพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาตรวจพบในภายหลังว่าการแจ้งหรือขึ้นทะเบียนไม่ถูกต้องหรือไม่ครบถ้วน ให้มีอำนาจสั่งผู้แจ้งหรือผู้ขึ้นทะเบียนแก้ไขให้ถูกต้องหรือครบถ้วนภายในเจ็ดวันนับแต่วันที่ได้รับคำสั่งดังกล่าว

ในการประกอบธุรกิจ ผู้แจ้งหรือผู้ขึ้นทะเบียนตามวรรคหนึ่งต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกาและตามที่คณะกรรมการประกาศกำหนด

ถ้าผู้แจ้งหรือผู้ขึ้นทะเบียนตามวรรคหนึ่งไม่แก้ไขการแจ้งหรือขึ้นทะเบียนให้

ถูกต้องหรือครบถ้วนตามวรรคสอง หรือฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์การประกอบธุรกิจตามวรรคสาม ให้คณะกรรมการพิจารณามีคำสั่งลงโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท โดยคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด และในกรณีที่เห็นสมควรคณะกรรมการอาจมีคำสั่งให้ผู้นั้นดำเนินการใด ๆ เพื่อแก้ไขให้ถูกต้องหรือเหมาะสมได้

หลักเกณฑ์ในการพิจารณาลงโทษปรับทางปกครองให้เป็นไปตามที่คณะกรรมการกำหนดและถ้าผู้ถูกลงโทษปรับทางปกครองไม่ยอมชำระค่าปรับทางปกครอง ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม และในกรณีไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคำสั่ง ให้คณะกรรมการมีอำนาจฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ ในการนี้ ถ้าศาลปกครองเห็นว่าคำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมายก็ให้ศาลปกครองมีอำนาจพิจารณาพิพากษาและบังคับให้มีการยึดหรืออายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้

ในกรณีผู้กระทำผิดตามวรรคสี่ไม่ดำเนินการแก้ไขตามคำสั่งของคณะกรรมการหรือกระทำความผิดซ้ำอีก ให้คณะกรรมการมีอำนาจออกคำสั่งห้ามมิให้ผู้นั้นประกอบธุรกิจตามที่ได้แจ้งหรือขึ้นทะเบียนอีกต่อไป

มาตรา ๓๔ ในกรณีที่มีพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์กรณีใดเป็นกิจการที่ต้องได้รับใบอนุญาต ให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวยื่นคำขอรับใบอนุญาตต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกา

คุณสมบัติของผู้ขอรับใบอนุญาต หลักเกณฑ์และวิธีการขออนุญาต การออกใบอนุญาต การต่ออายุใบอนุญาต การคืนใบอนุญาต และการสั่งพักใช้หรือเพิกถอนใบอนุญาต ให้เป็นไปตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกา

ในการประกอบธุรกิจ ผู้ได้รับใบอนุญาตตามวรรคหนึ่ง ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกา ประกาศที่คณะกรรมการกำหนดหรือเงื่อนไขในใบอนุญาต

ในกรณีที่ผู้ได้รับใบอนุญาตฝ่าฝืนหรือปฏิบัติไม่ถูกต้องตามหลักเกณฑ์การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ตามวรรคสาม ให้คณะกรรมการพิจารณามีคำสั่งลงโทษปรับทางปกครองไม่เกินสองล้านบาท โดยคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด และในกรณีที่เห็นสมควร คณะกรรมการอาจมีคำสั่งให้ผู้นั้นดำเนินการใด ๆ เพื่อแก้ไขให้ถูกต้องหรือเหมาะสมได้ ทั้งนี้ ให้นำความในมาตรา ๓๓ วรรคห้า มาใช้บังคับโดยอนุโลม

ถ้าผู้กระทำความผิดตามวรรคสี่ไม่ดำเนินการแก้ไขตามคำสั่งของคณะกรรมการหรือกระทำความผิดซ้ำอีก ให้คณะกรรมการมีอำนาจออกคำสั่งเพิกถอนใบอนุญาต

หมวด ๔
ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

มาตรา ๓๕ คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด ทั้งนี้ ในพระราชกฤษฎีกาอาจกำหนดให้บุคคลที่เกี่ยวข้องต้องกระทำหรืองดเว้นกระทำการใด ๆ หรือให้หน่วยงานของรัฐออกระเบียบเพื่อกำหนดรายละเอียดในบางกรณีด้วยก็ได้

ในการออกพระราชกฤษฎีกาตามวรรคหนึ่ง พระราชกฤษฎีกาดังกล่าวอาจกำหนดให้ผู้ประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ต้องแจ้งให้ทราบต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาต แล้วแต่กรณี ก่อนประกอบกิจการก็ได้ ในกรณีนี้ ให้นำบทบัญญัติในหมวด ๓ และบทกำหนดโทษที่เกี่ยวข้องมาใช้บังคับโดยอนุโลม

หมวด ๕
คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

มาตรา ๓๖ ให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วย รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อมเป็นประธานกรรมการ และกรรมการซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้ทรงคุณวุฒิที่ได้รับการสรรหาอีกจำนวนสิบสองคน โดยในจำนวนนี้เป็นผู้ทรงคุณวุฒิในด้านดังต่อไปนี้ด้านละสองคน

(๑) การเงิน

(๒) การพาณิชย์อิเล็กทรอนิกส์

(๓) นิติศาสตร์

(๔) วิทยาการคอมพิวเตอร์

(๕) วิทยาศาสตร์หรือวิศวกรรมศาสตร์

(๖) สังคมศาสตร์

ทั้งนี้ ผู้ทรงคุณวุฒิคนหนึ่งของแต่ละด้านต้องมาจากภาคเอกชน และให้ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ เป็นกรรมการและเลขานุการ

หลักเกณฑ์และวิธีการสรรหาและการเสนอชื่อบุคคลที่เห็นสมควรต่อคณะรัฐมนตรีเพื่อพิจารณาแต่งตั้งเป็นคณะกรรมการตามวรรคหนึ่ง ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด

ให้เลขานุการแต่งตั้งผู้ช่วยเลขานุการอีกไม่เกินสองคน

มาตรา ๓๗ ให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ มีอำนาจหน้าที่ดังต่อไปนี้

(๑) เสนอแนะต่อคณะรัฐมนตรีเพื่อวางนโยบายการส่งเสริมและพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ตลอดจนการแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้อง

(๒) ติดตามดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

(๓) เสนอแนะหรือให้คำปรึกษาต่อรัฐมนตรีเพื่อการตราพระราชกฤษฎีกาตามพระราชบัญญัตินี้

(๔) ออกระเบียบหรือประกาศเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์เพื่อให้เป็นไปตามพระราชบัญญัตินี้ หรือตามพระราชกฤษฎีกาที่ออกตามพระราชบัญญัตินี้

(๕) ปฏิบัติการอื่นใดเพื่อให้เป็นไปตามพระราชบัญญัตินี้ หรือกฎหมายอื่น

ในการปฏิบัติการตามพระราชบัญญัตินี้ให้คณะกรรมการเป็นเจ้าพนักงานตามประมวลกฎหมายอาญา

มาตรา ๓๘ กรรมการผู้ทรงคุณวุฒิมีวาระการดำรงตำแหน่งสามปี กรรมการซึ่งพ้นจากตำแหน่งอาจได้รับแต่งตั้งอีกได้ แต่ไม่เกินสองวาระติดต่อกัน

มาตรา ๓๙ นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา ๓๘ กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่ง เมื่อ

(๑) ตาย

(๒) ลาออก

(๓) คณะรัฐมนตรีให้ออกเพราะมีความประพฤติเสื่อมเสีย บกพร่อง หรือไม่สุจริตต่อหน้าที่หรือหย่อนความสามารถ

(๔) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๕) ได้รับโทษจำคุกโดยต้องคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

มาตรา ๔๐ ในกรณีที่กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งตามมาตรา ๓๙ ให้ถือว่าคณะกรรมการประกอบด้วยกรรมการเท่าที่เหลืออยู่ และให้ดำเนินการแต่งตั้งกรรมการใหม่แทนภายในหกสิบวันนับแต่วันที่กรรมการพ้นจากตำแหน่ง

ให้กรรมการซึ่งได้รับแต่งตั้งแทนอยู่ในตำแหน่งเท่ากับวาระที่เหลืออยู่ของผู้ซึ่งตนแทน

มาตรา ๔๑ การประชุมของคณะกรรมการต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมดจึงเป็นองค์ประชุม

ถ้าประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้คณะกรรมการเลือกกรรมการคนหนึ่งทำหน้าที่ประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากันให้ประธานออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

มาตรา ๔๒ คณะกรรมการมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติการอย่างหนึ่งอย่างใดแทนคณะกรรมการก็ได้

ให้นำความในมาตรา ๔๑ มาใช้บังคับแก่การประชุมของคณะอนุกรรมการโดยอนุโลม

มาตรา ๔๓ ให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ทำหน้าที่เป็นหน่วยงานธุรการของคณะกรรมการ

หมวด ๖
บทกำหนดโทษ

มาตรา ๔๔ ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่แจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาตามมาตรา ๓๓ วรรคหนึ่ง หรือโดยฝ่าฝืนคำสั่งห้ามการประกอบธุรกิจของคณะกรรมการตามมาตรา ๓๓ วรรคหก ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๕ ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่ได้รับใบอนุญาตตามมาตรา ๓๔ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๖ บรรดาความผิดตามพระราชบัญญัตินี้ที่กระทำโดยนิติบุคคล ผู้จัดการหรือผู้แทนนิติบุคคลหรือผู้ซึ่งมีส่วนร่วมในการดำเนินงานของนิติบุคคล ต้องรับผิดในความผิดนั้นด้วย เว้นแต่พิสูจน์ได้ว่าตนมิได้รู้เห็นหรือมีส่วนร่วมในการกระทำความผิดนั้น

ผู้รับสนองพระบรมราชโองการ
พันตำรวจโท ทักษิณ ชินวัตร
นายกรัฐมนตรี

<u>หมายเหตุ</u>:- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่การทำธุรกรรมในปัจจุบันมีแนวโน้มที่จะปรับเปลี่ยนวิธีการในการติดต่อสื่อสารที่อาศัยการพัฒนาการเทคโนโลยีทางอิเล็กทรอนิกส์ซึ่งมีความสะดวก รวดเร็ว และมีประสิทธิภาพ แต่เนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวมีความแตกต่างจากวิธีการทำธุรกรรมซึ่งมีกฎหมายรองรับอยู่ในปัจจุบันเป็นอย่างมาก อันส่งผลให้ต้องมีการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือ หรือหลักฐานเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือ และมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม ควรกำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ทำหน้าที่วางนโยบายกำหนดหลักเกณฑ์เพื่อส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ ติดตามดูแลการประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งมีหน้าที่ในการ

ส่งเสริมการพัฒนาการทางเทคโนโลยีเพื่อติดตามความก้าวหน้าของเทคโนโลยี ซึ่งมีการเปลี่ยนแปลงและพัฒนาศักยภาพตลอดเวลาให้มีมาตรฐานน่าเชื่อถือ ตลอดจนเสนอแนะแนวทางแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้อง อันจะเป็นการส่งเสริมการใช้ธุรกรรมทางอิเล็กทรอนิกส์ทั้งภายในประเทศและระหว่างประเทศ ด้วยการมีกฎหมายรองรับในลักษณะที่เป็นเอกรูป และสอดคล้องกับมาตรฐานที่นานาประเทศยอมรับ จึงจำเป็นต้องตราพระราชบัญญัตินี้

UNCITRAL Model Law

on Electronic Commerce

1996

with additional article 5 bis as adopted in 1998

Part one. Electronic commerce in general

Chapter I.
General provisions

Article 1. Sphere of application*

This Law** applies to any kind of information in the form of a data message used in the context*** of commercial**** activities.

* The Commission suggests the following text for States that might wish to limit the applicability of this Law to international data messages:

"This Law applies to a data message as defined in paragraph (1) of article 2 where the data message relates to international commerce."

** This Law does not override any rule of law intended for the protection of consumers.

*** The Commission suggests the following text for States that might wish to extend the applicability of this Law: "This Law applies to any kind of information in the form of a data message, except in the following situations: [...]."

**** The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road

Article 2. Definitions

For the purposes of this Law:

(a) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(b) "Electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information;

(c) "Originator" of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;

(d) "Addressee" of a data message means a person

who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;

(e) "Intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;

(f) "Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages.

Article 3. Interpretation

(1) In the interpretation of this Law, regard is to be had to its origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 4. Variation by agreement

(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement.

(2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II.

Chapter II.
Application of legal requirements to
data messages

Article 5. Legal recognition of data messages

Information shall not be denied legal effect, validity or enforce-ability solely on the grounds that it is in the form of a data message.

Article 5 bis. Incorporation by reference

(as adopted by the Commission at its thirty-first session, in June 1 9 9 8)

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

A r t i c l e 6 . W r i t i n g

(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 this article do not apply to the following: [. . .] .

A r t i c l e 7 . S i g n a t u r e

(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 or whether the law simply provides consequences for the absence of a signature.

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

A r t i c l e 8 . O r i g i n a l

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if :

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(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 presented or retained in its original form.

(3) For the purposes of subparagraph (a) of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(4) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

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

Article 9. Admissibility and evidential weight of data messages

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

Article 10. Retention of data messages

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(d) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(2) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

Chapter III.
Communication of data messages

Article 11. Formation and validity of contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

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

Article 12. Recognition by parties of data messages

(1) As between the originator and the addressee of a data

message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

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

Article 13 Attribution of data messages

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose;or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as

received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Article 14. Acknowledgement of receipt

(1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or otherwise, or

(b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

Article 15. Time and place of dispatch and receipt of data messages

(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 or 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:

(a) 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;

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

Paragraph (2) 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).

(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:

(a) 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;

(b) 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: [. . .] .

Part two. Electronic commerce in specific areas

Chapter I. Carriage of goods

Article 16. Actions related to contracts of carriage of goods

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

(a) (i) furnishing the marks, number, quantity or weight of goods;

(ii) stating or declaring the nature or value of goods;

(iii) issuing a receipt for goods;

(iv) confirming that goods have been loaded;

(b) (i) notifying a person of terms and conditions of the contract;

(ii) giving instructions to a carrier;

(c) (i) claiming delivery of goods;

(ii) authorizing release of goods;

(iii) giving notice of loss of, or damage to, goods;

(d) giving any other notice or statement in connection with the performance of the contract;

(e) undertaking to deliver goods to a named person or a person authorized to claim delivery;

(f) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;

(g) acquiring or transferring rights and obligations under the contract.

Article 17. Transport documents

(1) Subject to paragraph (3), where the law requires that any action referred to in article 16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

(4) For the purposes of paragraph (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(5) Where one or more data messages are used to effect any action in subparagraphs (f) and (g) of article 16, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

(6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.

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

A/CN.9/WG.IV/WP.88

United Nations Commission on International Trade Law
Working Group on Electronic Commerce
Thirty-eighth session
New York, 12 - 23 March 2001

UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001)

(as approved by the UNCITRAL Working Group on Electronic Commerce at its thirty-seventh session, held at Vienna from 18 to 29 September 2000)

Article 1. Sphere of application

This Law applies where electronic signatures are used in the context* of commercial** activities. It does not override any rule of law intended for the protection of consumers.

* The Commission suggests the following text for States that might wish to extend the applicability of this Law:

"This Law applies where electronic signatures are used, except in the following situations: [...]."

** The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

Article 2. Definitions

For the purposes of this Law:

(a) "Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message;

(b) "Certificate" means a data message or other record confirming the link between a signatory and signature creation data;

(c) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(d) "Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;

(e) "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;

(f) "Relying party" means a person that may act on the basis of a certificate or an electronic signature.

Article 3. Equal treatment of signature technologies

Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6 (1) or otherwise meets the requirements of applicable law.

Article 4. Interpretation

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 5. Variation by agreement

The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.

Article 6. Compliance with a requirement for a signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which 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 referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if:

(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(4) Paragraph (3) does not limit the ability of any person:

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph (1), the reliability of an electronic signature; or

(b) to adduce evidence of the non-reliability of an electronic signature.

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

Article 7. Satisfaction of article 6

(1) [Any person, organ or authority, whether public or private, specified by the enacting State as competent] may determine which electronic signatures satisfy the provisions of article 6.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

(3) Nothing in this article affects the operation of the rules of private international law.

Article 8. Conduct of the signatory

(1) Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

(a) exercise reasonable care to avoid unauthorized use of its signature creation data;

(b) without undue delay, notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

(i) the signatory knows that the signature creation data have been compromised; or

(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

(c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.

(2) A signatory shall be liable for its failure to satisfy the requirements of paragraph (1).

Article 9. Conduct of the certification service provider

(1) Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:

(a) act in accordance with representations made by it with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to ascertain from the certificate:

(i) the identity of the certification service provider;

(ii) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(iii) that signature creation data were valid at or before the time when the certificate was issued;

(d) provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise:

(i) the method used to identify the signatory;

(ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(iii) that the signature creation data are valid and have not been compromised;

(iv) any limitation on the scope or extent of liability stipulated by the certification service provider;

(v) whether means exist for the signatory to give notice pursuant to article 8 (1) (b);

(vi) whether a timely revocation service is offered;

(e) where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8(1)(b) and, where services under subparagraph d (vi) are offered, ensure the availability of a timely revocation service;

(f) utilize trustworthy systems, procedures and human resources in performing its services.

(2) A certification service provider shall be liable for its failure to satisfy the requirements of paragraph (1).

Article 10. Trustworthiness

For the purposes of article 9(1)(f), in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:

(a) financial and human resources, including existence of assets;

(b) quality of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to signatories identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or

(g) any other relevant factor.

Article 11. Conduct of the relying party

A relying party shall bear the legal consequences of its failure to:

(a) take reasonable steps to verify the reliability of an electronic signature; or

(b) where an electronic signature is supported by a certificate, take reasonable steps to:

(i) verify the validity, suspension or revocation of the certificate; and

(ii) observe any limitation with respect to the certificate.

Article 12. Recognition of foreign certificates and electronic signatures

(1) In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had to:

(a) the geographic location where the certificate is issued or the electronic signature created or used; or

(b) the geographic location of the place of business of the issuer or signatory.

(2) A certificate issued outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as a certificate issued in *[the enacting State]* if it offers a substantially equivalent level of reliability.

(3) An electronic signature created or used outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as an electronic signature created or used in *[the enacting State]* if it offers a substantially equivalent level of reliability.

(4) In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph (2) or (3), regard shall be had to recognized international standards and to any other relevant factors.

(5) Where, notwithstanding paragraphs (2), (3) and (4), parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

กฎหมายธุรกรรมทางอิเล็กทรอนิกส์
และกฎหมายลายมือชื่ออิเล็กทรอนิกส์ของต่างประเทศ

1. องค์การระหว่างประเทศ

ประเทศ	ชื่อกฎหมาย	URL
APEC	• A REFERENCE FRAMEWORK FOR ACTION ON ELECTRONIC COMMERCE • APEC BLUEPRINT FOR ACTION ON ELECTRONIC COMMERCE	http://www.dcita. gov.au
ASEAN	• REFERENCE FRAMEWORK FOR ELECTRONIC COMMERCE LEGAL INFRASTRUCTURE	http://www.asean. or.id
EUROPEAN UNION	• Directive 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, In the Internal Market (Directive on electronic commerce) • Directive 1999/93/EC OF THE	http://europa.eu.int

	EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures	
ICC	• General Usage for International Digitally Ensured Commerce	http://www.iccwbo.org/home/guidec/ guidec.asp
OECD	• Guidelines for cryptography policy	http://www.oecd.org/dsti/sti/it/secur/prod/crypto2.htm
UNICTRAL	• UNICITRAL MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT 1996 • UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURE	http://www.uncitral. org

2. ประเทศในกลุ่มทวีปเอเชีย

ประเทศ	ชื่อกฎหมาย	URL
Brunei	• Electronic Transaction Order 2000	-
Hong Kong	• Electronic Transactions Ordinance	http://www.info.gov.hk/itbb/english/it/eto. htm
India	• The Information Technology Act 2000 • Information Technology (Certifying Authorities) Rules,2000	http://caselaw.delhi.nic.in/incodis/current/ INFTECH.HTM
Japan	• Law Concerning Electronic Signatures and Certification Services	http://www.mpt.go.jp/eng/Resources/Legialation/eSignLaw/ eSignLaw.pdf
Malaysia	• Digital Signature Act 1997 (Act 562) • Digital Signature Regulation 1998	http://www.cca.gov. my
Philippine	• Electronic Commerce Act 2000 • Implementing Rules and Regulations of The Electronic Commerce Act	http://www.neda. gov.ph
	• Electronic Transaction Act 1998	http://www.cca.gov.sg

Singapore	• Singapore Electronic Transactions (Certification Authority) Regulations of 1999 • Security Guidelines for Certification Authority • Information Technology Security Guidelines	
South Korea	• The Basic Law on Electronic Commerce • Digital Signature Act	http://www.mocie. go.kr

3. ประเทศในกลุ่มทวีปยุโรป

ประเทศ	ชื่อกฎหมาย	URL
Austria	• Austrian Federal Electronic signature Law	http://www.bmck.com/ecommerce/austrianesig.pdf
Australia	• Electronic Transaction Act 1999 • Electronic Transactions (Victoria) Act 2000 • Electronic Transactions (New South Wales) Bill 2000	http://www.law.gov.au/publications/ecommerce/interim3.html
Denmark	• Draft Bill for Act on Digital Signature	http://www.fsk.dk/fsk/div/hearing/draft.html
England	• Electronic Communications Act 2000	http://www.hmso.gov.uk/acts/acts2000/20000007.htm
Finland	• Act on Electronic Service in the Administration	http://www.om.fi/2838.htm
Germany	• Digital Signature Act	http://www.iid.de/rahmen/iukdgebt.html หรือ http://www.iuscomp.org/

		gla/statutes/SiG.htm
Hungary	• Hungary E-Signature Bill	-
Ireland	• Electronic Commerce Bill, 2000	http://www.irlgov.ie/tec/communications/ecommercebill2000.pdf
Italy	• Presidential Decree No. 513 of 10 November 1997	http://www.aipa.it/english[4/law[3/pdecree51397.asp
Netherlands	• State Ordinance containing rules concerning agreements which are concluded electronically (Nation Ordinance on Electronic Agreement)	-
New Zealand	• Electronic Transactions Bill 2000	http://www.med.govt.nz/irdev/elcom/transactions/bill/index.html
Poland	• POLAND DIGITAL SIGNATURE ACT	http://venus.ci.uw.edu.pl/~dancop/ustawa.pdf ** ภาษาโปแลนด์
Switzerland	• Decree on electronic certification services	http://www.bakom.ch/eng/subsubpage/docs/1335/1335.pdf

4. ประเทศในกลุ่มทวีปอเมริกา

ประเทศ	ชื่อกฎหมาย	URL
Brazil	• Brazil Draft Signature Bill (Anteprojeito de Lei)	http://www.natlaw.com/ecommerce/docs/ e-commercebill-brazil.htm **ภาษาสเปน
Canada	• Uniform Electronic Commerce Act • Personal Information Protection and Electronic Document Act	http://www.law.ualberta.ca/alri/ulc/current/euecafin.htm และ http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_1/C-6TOCE.html
Colombia	• Draft Proposal of Law on Electronic	http://www.qmw.ac.uk/~

	Commerce, Digital Signatures and Certification Authorities	tl6345/colombia_en. htm
Ecuador	• Ecuador Law Governing Electronic Commerce, Electronic Signatures, and Data Messages	http://www.natlaw.com/ecommerce/docs/ecommercebill-ecuador.htm
Mexico	• Electronic Communication Act 2000	http://www.natlaw.com/ecommerce/docs/e-commerce-iniciative-mexico.htm ** ภาษาสเปน
Peru	• Peru Draft Bill - Proyecto de Firmas Electronicas	http://www.natlaw.com/ecommerce/docs/e-commerce-peru-firmaycert.htm ** ภาษา สเปน
United state of America	• Digital Signature Guidelines [American Bar Association]	http://www.abanet.org/scitech/ec/isc/ dsgfree.html
United state of America	• ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT	http://www.ecommerce.gov/ecomnews/ElectronicSignatures_s761.pdf
United state of America	• Uniform Electronic Transaction Act	http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.pdf
California	• Digital Signature Regulations	http://www.ss.ca.gov/digsig/regulations.htm
Gorgia	• Electronic Records, Signature Act	http://www.state.ga.us/Legis/1999_00/leg/fulltext/sb62.htm
Illinois	• Electronic Commerce Security Act	http://www.legis.state.il.us/legisnet/legisnet90/hbgroups/hb/900HB3180LV.html
Utah	• Utah Digital Signature Act	http://www.jmls.edu/cyber/statutes/udsa.html

5. เว็บไซต์ที่น่าสนใจเกี่ยวกับกฎหมาย Electronic Commerce & Electronic Signature

ชื่อเว็บไซต์	URL
Baker & McKenzie	http://www.bmck.com/ecommerce/countrycomp.htm
Crypto Law Survey	http://cwis.kub.nl/~frw/ people/koops/cls2.htm
Digital Signature Law	http://www.wolfenet.com/ ~dhillis/digsiglaw/#us
European Union	http://europa.eu.int/ISPO/ ecommerce/issues/digisig/ digisign5.htm หรือ http://www.eurocert.net/ legislature.html
Find law	http://www.findlaw.com
Internet law & Policy Forum (ILPF)	http://www.ilpf.org/digsig/ analysis_IEDSII.htm
Law.com	http://www.law.com
McBride Baker & Coles (MBC)	http://www.mbc.com
U.S. Code	http://www.access.gpo.gov/congress/cong013.html หรือ http://www.law.cornell.edu/uscode
U.S. Code of Federal Regulations (CFR)	http://www.gpo.ucop.edu/ search/cfr.html

ตารางแสดงผู้ให้บริการออกใบรับรอง
(Certification Authority) ในภูมิภาคต่าง ๆ ของโลก

Africa		
ประเทศ	**ผู้ให้บริการออกใบรับรอง**	URL
South Africa	Thawte Consulting	http://www.thawte.com
	Compu Source	http://compusource.co.za
	Bankgate	http://www.bankgate.com/market/index.htm
	South African Certification Authority	https://www.saca.net/secured.htm
Asia		
ประเทศ	**ผู้ให้บริการออกใบรับรอง**	URL

Hong Kong	Hong kong Post e-Cert	http://www.hongkongpost.gov.hk
	Hitrust	http://www.hitrust.com.hk
	Hong Kong University (HKU CA)	http://www.hkuca.hku.hk
India	SafeScrypt Ltd.	http://www.safescrypt.com
Israel	Comsign	http://www.comsign.co.il
Japan	Initiative for Computer Authentication Technology (ICAT)	http://www.icat.or.jp/English/index.html
	Verisign Inc	http://www.verisign.co.jp
	IPRA	http://bs.mit.edu:8001/ipra.html
	MEIJI	http://www.isc.meiji.ac.jp
	JAMI	http://jami-ca.osaka med.ac.jp/ca
	ISIT	http://www.k-isit.or.jp/dccf
	WIDE Moca	http://moca.wide.ad.jp
ประเทศ	**ผู้ให้บริการออกใบรับรอง**	URL
Japan	Thawte CA sponsored by MEDIX Inc.	http://www.jp.thawte.com
	Verisign Japan KK	http://www.verisign.co.jp
Korea	Crosscert	http://www.crosscert.com
	KAIST network	http://camis.kaist.ac.kr/kaist-ca
	KICA	http://www.sigate.co.kr
	KFTC	http://www.yessign.com
	NCA	http://sign.nca.or.kr
	SoftForum	http://www.softforum.co.kr
Malaysia	Digicert	http://www.digicert.com.my
	Trustgate	http://www.trustgate.com
	Mtrust	http://www.mtrust.com.my
Singapore	Netrust	http://www.netrust.com.sg
	Baltimore Technologies (Singapore)	http://www.baltimore.com/contact_us/singapore.html

	ID.Safe	http://www.id-safe.com.sg
Thailand	Government Information Technology Services	http://www.gits.net.th
	Thaidigital ID	http://www.thaidigitalid.com
Taiwan	Hitrust	http://www.hitrust.com.tw
Europe		
ประเทศ	**ผู้ให้บริการออกใบรับรอง**	URL
Australia	a-sign (Datakom GmbH)	http://a-sign.datakom.at
	Globalsign Austria	http://www.globalsign.at
Belgium	Belgacom E-Trust	http://www.e-trust.be
	Belsign	http://www.belsign.be
	Isabel (Interbank Standards Association Belgium)	http://www.isabel.be/en/home/index.html
Czech	PVT CA	http://www.ica.cz
ประเทศ	**ผู้ให้บริการออกใบรับรอง**	URL
Denmark	Kmd-CA	http://www.kmd-ca.dk/index.htm
	Tele Danmark certificeringscenter	http://www.certifikat.dk
Finland	Vaestorekisterikeskus : The Finish Population Register's CA	http://www.fineid.fi/Default.asp?todo=setlang&lang=uk
France	Certplus	http://www.certplus.com
	Thawte Francophone	http://www.fr.thawte.com
	PCA of the German Research Network	http://www.pca.dfn.de/eng/dfnpca
	Policy Certification Authority	http://www.pca.dfn.de
	Dunkel	http://www.dunkel.de
	D-Trust	http://www.d-trust.net/internet/content/secure-index.html
	IN-CA : Individual Network e.v.	http://www.in-ca.individual.net

Germany	Krypto-Kampagne:	http://www.heise.de/ct/pgpCA/default.shtml
	Regulierungsbehörde	http://www.nrca-ds.de
	Deutsche Telekom	http://srv15.telesec.de
	Deutsche Post	http://www.signtrust.de/start.htm
	Bundesnotarkammer	http://dir.bnotk.de
	DATEV eG	http://www.zs.datev.de
	Medizon AG	http://www.medizon.de/index1.htm
	TC TrustCenter:	http://www.trustcenter.de/set_de.htm
	IKS Certification Authority:	http://www.iks-jena.de/produkte/ca/index.en.html
	GeFoKom CA	http://www.mayn.de/ca
	Rus Test Certification Authority (RTCA)	http://ca.uni-stuttgart.de
ประเทศ	**ผู้ให้บริการออกใบรับรอง**	URL
Germany	TI-TC Trustcenter of the Institute of Telematics	http://www.ti.fhg.de/trust_center.en.html
	Deutschland Chamber Association of Digital Acceptance (DE-CODA)	http://www.ihk.de/de-coda/inside.htm
Greece	Globalsign Greece	http://www.globalsign.gr
Hungary	Netlock Ltd.	http://www.netlock.net
	Adacom	http://www.adacom.com
Ireland	Software and System Engineering Limited	http://www.sse.ie
	Eurotrust	http://www.baltimore.com/projects/eurotrust.html
	Certification Authority Tin (Telecom Italia Net)	http://security.tin.it
	Telecom Italia Net CA	http://security.tin.it
	Trustitalia	http://www.trustitalia.it

Italy	SSB-SpA CA	http://ca.ssb.net/english
	SIA Certifiation Authority	https://ca.sia.it/home
	University of Torino	http://ca.unito.it
	Globalsign Italy	http://www.globalsign.it
	Politecnico di Torino	http://ca.polito.it/crl/en_index.html
	Alinet Italia	http://ca.alinet.it
	Finital S.p.A.	http://ca.finital.it
Lithuania	Interneto Projektai	http://www.ip.lt
Luxembourg	Globalsign Luxembourg	http://www.cc.lu./e_commer.htm
The Netherlands	Roccade	http://www.megasign.nl
	PTT Post with KeyMail	http://www.keymail.nl
	SURFnet PCA	http://pki.surfnet.nl
	InterPay	http://www.i-pay.com
	DigiNotar	http://www.diginotar.nl
ประเทศ	**ผู้ให้บริการออกใบรับรอง**	URL
The Netherlands	KPN Telecom	http://certificaat.kpn.com
	Roccade Megaplex	http://www.megasign.nl
	NLsign	http://www.nlsign.nl
Norway	UNINETT	http://www.uninett.no/pca/index-e.html
Portugal	Certipor	http://www.certipor.com
	Multicert	http://www.multicert.com
Slovenia	Slovenian SI-CA	http://www.e5.ijs.si/cert/sipca_cert.html
	Internet Publishing Services (IPS)	http://www.ips.es
	Acepta.com	http://www.acepta.com
	AD AEQUITATEM	http://aequitas.encomix.es/indexi.htm
	Siscer	http://www.siscer.com/siscer.en.html

Spain	FESTE	http://www.feste.org
	Agencia de Certificación Electrónica (ACE)	http://www.ace.es/english
	Cámbra de Comerç de Barcelona	http://www.cambrabcn.es/comerc_electronic/p-01.htm
Sweden	COST	http://www.cost.se
	PostNet	http://www.postnet.se
	Telia	http://www.e-commerce.telia.com/tec/id
Switzerland	SwissKey	http://www.swisskey.ch
	Entrust Europe	http://www.entrust.ch
The United Kingdom	Endorse	http://www.endorse.co.uk
	BT Trustwise	http://www.trustwise.com
	The Global Trust Register	http://www.cl.cam.ac.uk/Research/Security/Trust-Register/index.html
	Inter Clear	https://www.interclear.net/
ประเทศ	**ผู้ให้บริการออกใบรับรอง**	URL
The United Kingdom	TrueTrust	http://www.truetrust.co.uk/
	Globalsign UK	http://www.globalsign.net/
	Viacode	http://www.royalmail.com/at_home/net_security/default.htm
	Messaging Direct	http://www.messagingdirect.com/index.html
Middle East		
Lebanon	Globalsign Lebanon	http://www.globalsign.com.lb
South America		
Argentina	Argentina Governmental PKI and Licensing Authority	http://www.pki.gov.ar
	Argentina Ministry of Economy	http://www.mecon.ar/firma_digital.htm
	Certisur	http://www.certisur.com

	Government Pilot CAs	http://www.pki.gov.ar/acl/piloto.html
Brazil	Certisign	http://www.certisign.com.br
	Certisign	http://www.certisign.com.br
Canada	Entrust - Certification Products	http://www.entrust.com
	Government of Canada Public Key Infrastructure	http://www.cse.dnd.ca/cse/english/gov.html
	CREN	http://www.cren.net/ca/index.html
	Keywitness	http://www.keywitness.ca
	OnWatch Key Management Centre	http://www.public-key.com
	Webtrust	http://www.bennettgold.ca
	Silanis Technology	http://www.silanis.com
	XCert	http://www.xcert.com
	CIBC	http://www.cibc.com
	VPN Tech Inc.	http://www.vpntech.com
ประเทศ	**ผู้ให้บริการออกใบรับรอง**	URL
The United States of	AlphaTrust.com	http://www.mayn.de/ca
	Certco	http://www.certco.com
	ACES Access Certificates for Electronic Servies	http://hydra.gsa.gov/aces
	eOriginal, Inc.	http://www.das-inc.com
	Baltimore Technologies plc.	http://www.baltimore.com
	Entegrity Solution Corporation	http://www2.entegrity.com/index.shtml
	Equifax Secure, Inc.	http://www.equifaxsecure.com/ebusinessid
	GTE Cybertrust	http://www.cybertrust.gte.com/
	MIT Internet PCA Registration Authority	http://bs.mit.edu:8001/ipra. html
	Cybergard	http://www.cybg.com/index_ie.asp

America	PenOP - Signature Dynamics Authentication Technology	http://www.penop.com
	Columbia CA	http://www.columbia.edu/acis/rad/columbiaca
	ARINC	http://www.arinc.com/digsig
	Universal Secured Encryption Repository Company (USERFirst)	http://www.usertrust.com
	Arcanvs	http://www.arcanvs.com
	Verisign	http://www.verisign.com
	SET Certificate Authority	http://www.setco.org
	SUN Certification Authorities	http://www.sun.com/security/product/ca.html
	TradeWave Corporation	http://www.tradewave.com
	Valicert (Complementary service to CAs)	http://www.valicert.com
	Digital Signature Trust Company	http://www.digsigtrust.com
	ID Certify,Inc	http://www.idcertify.com
Oceania		
ประเทศ	**ผู้ให้บริการออกใบรับรอง**	URL
Australia	Signet	http://www.signet.org.au/Signet/serv01.htm
	Esign	http://www.esign.com.au
	Government Public Key Authority	http://www.govonline.gov.au/projects/publickey/index.asp
	Baltimore Certificates Australia Pty Limited	http://www.certificates-australia.com.au/
	KeyPost	http://www.auspost.com.au/keypost
	SPYRUS	http://www.spyrus.com.au
New Zealand	128i - New Zealand's Certification Authority	http://www.128i.com
Global		
	Cybertrust	http://www.cybertrust.com/

	Certco	http://www.certco.com
	Verisign	http://www.verisign.com/
	BBN	http://www.bbn.com/
	Entrust	http://www.entrust.com/
	XCert	http://www.xcert.com/
	NetDox	http://www.netdox.com/
	IBM	http://www-4.ibm.com/software
	CivilLink-US government service by ameritech	http://www.civillink.com
	GlobalSign	http://www.globalsign.net
	Terisa Systems	http://www.terisa.com/
	EuroSign - The European Certification Authority	http://eurosign.com/
	Open Market Incorporated	http://www.openmarket.com/
	SUN Certificate Authorities	http://www.sun.com/security/product/ca.html
	Thawte Certification Division	http://www.thawte.com
ประเทศ	**ผู้ให้บริการออกใบรับรอง**	URL
	Trade Authority	http://www.tradewave.com/products/tradeauthority.html
	InterClear	http://www.jp.thawte.com
	The USERTRUST Network	http://www.usertrust.com
	128I Ltd.	http://www.128i.com
	WildID LLC	http://www.wildid.com
	Addtrust	http://www.addtrust.com
	E-Certify Corporation	http://www.e-certify.com
	Freecert.com	http://www.freecerts.com
	beTRUSTed	http://betrusted.com
	Equifax Secure	http://www.equifaxsecure.com
Org.		
	FP5 Certification Service : Fifth Framework programme	http://fp5-csp.org/frames.html

	of the European Community	
	The European Commission	http://europa.eu.int/comm/internal_market/en/media/sign/index.htm
	The European Electronic Signature Standardization Initiative	http://www.ict.etsi.org/eessi/EESSI-homepage.htm
	European Telecommunications Standards Institute	http://www.etsi.org/sec/el-sign.htm
	European Electronic Messaging Association	http://www.eema.org
	European Certification Authority Forum	http://www.eema.org/ecaf
	European Committee for Standardization	http://www.cenorm.be/isss/workshop/e-sign
	International Secure Electronic Transactions Organisation	http://www.iseto.ch
	EuPKI	http://www.europki.org

รายนามที่ปรึกษา
โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ

รายชื่อที่ปรึกษาทางวิชาการ	สถานที่ทำงาน
ศ.คนึง ฦาไชย	สถาบันกฎหมายอาญา (ประธานสถาบันกฎหมายอาญา)
ศ.ดร.อรุณ ภาณุพงศ์	กระทรวงการต่างประเทศ (ผู้อำนวยการศูนย์ศึกษาการต่าง ประเทศ)
ศ.ชัยวัฒน์ วงศ์วัฒนศานต์	สำนักงานคณะกรรมการกฤษฎีกา (เลขาธิการคณะกรรมการกฤษฎีกา)
นายไพโรจน์ วายุภาพ	สำนักงานศาลยุติธรรม เนติบัณฑิตยสภา (ผู้ พิพากษาหัวหน้าคณะศาลอุทธรณ์ภาค)
นายไชยวัฒน์ บุนนาค	บริษัท ที่ปรึกษากฎหมายสากล จำกัด
ดร.เลอสรร ธนสุกาญจน์	จุฬาลงกรณ์มหาวิทยาลัย
รศ.ดร.พันธุ์ทิพย์ สายสุนทร	คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
ดร.พินัย ณ นคร	คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

รายนามคณะทำงานฝ่ายเลขานุการ
ยกร่างกฎหมายเทคโนโลยีสารสนเทศ

ที่ปรึกษา

1. ศ.ดร.ไพรัช ธัชยพงษ์
   ผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

   2. ดร.ทวีศักดิ์ กออนันตกูล
   ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

3. ดร.ชฎามาศ ธุวะเศรษฐกุล
   ผู้อำนวยการสำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ

คณะทำงานฝ่ายเลขานุการ

ทีมกฎหมาย

1. นางสุรางคณา แก้วจำนงค์
   หัวหน้าโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ
2. นางสาวอรดา เทพยายน
3. นางสาวพรพักตร์ สถิตเวโรจน์
4. นายเที่ยงธรรม แก้วรักษ์
5. นายวินัย แท่นประเสริฐกุล
6. นายสุระชัย กอทอง
7. นายปฏิวัติ อุ่นเรือน

8. นายยุทธพงศ์ จินันทุยา
9. นางสาวธิตินันท์ ฤกษ์อาษา
10. นายรุ่งศักดิ์ ลีลาวุฒารักษ์
11. นางสาวกนกอร ฉวาง
12. นางสาวณราพร ธีรกัลยาณพันธุ์
13. นางสาวชนิดา ปางพฤตินันท์

<u>ทีมวิศวกรและวิทยาการคอมพิวเตอร์</u>

ฝ่ายหน่วยเทคโนโลยีความปลอดภัยข้อมูล

1. ดร.จุณวิทย์ ชลิดาพงศ์
   หัวหน้าหน่วยเทคโนโลยีความปลอดภัยข้อมูล
2. นายชัยชนะ มิตรพันธ์*
3. นายโสพส พานิชปรีชา
4. นายวีระชาติ วงศ์สวัสดิ์
5. นายสันต์ทศน์ สุริยันต์
6. นางสาวนันทนา พจนานันทกุล
7. นางสาวชลธร ชุณหวิกสิต
8. นางสาวฐิติมา รัตนประกาย

ฝ่ายงานเทคโนโลยีเพื่อการศึกษาและพัฒนาทรัพยากรมนุษย์

1. นายบุญเลิศ อรุณพิบูลย์
2. นายภาคภูมิ เอี่ยมวิตกุศล
3. นายวิโรจน์ ไววุฒิวรกุล

* อยู่ระหว่างการศึกษาต่อในระดับปริญญาเอก ณ สหพันธรัฐเยอรมันนี