บทที่ 3
กฎหมายเกี่ยวกับลายมือชื่อดิจิตอล

ปัจจุบันการทำธุรกรรมหรือนิติกรรมสัญญาใดๆ ต้องกระทำการตามที่กฎหมายกำหนดไว้ในเรื่องนั้นจึงจะมีผลผูกพันตามกฎหมาย กฎหมายอาจจะกำหนดให้ธุรกรรมหรือนิติกรรมสัญญาบางลักษณะต้องทำเป็นหนังสือ (Writing) โดยต้องมีการลงลายมือชื่อของผู้ที่ทำหนังสือ[1] ผู้ที่เป็นฝ่าย หรือผู้ที่เกี่ยวข้องกับธุรกรรมหรือนิติกรรมสัญญาดังกล่าว หรือกำหนดให้ต้องมีหลักฐานเป็นหนังสือ และลงลายมือชื่อของฝ่ายที่เป็นผู้รับผิดในธุรกรรมหรือนิติกรรมสัญญาดังกล่าว เพื่อให้เป็นหลักฐานเมื่อมีการฟ้องร้องคดีต่อศาล การที่กฎหมายกำหนดให้ต้องลงลายมือชื่อนั้นเพื่อแสดงว่าผู้ลงลายมือชื่อเห็นชอบ รับรู้ หรือรับรองเนื้อหาสาระของเอกสารนั้น ซึ่งตลอดมาการลงลายมือชื่อธรรมดา (Traditional Hand-written) ก็สามารถที่จะตอบสนองต่อความต้องการดังกล่าวของกฎหมายได้เป็นอย่างดี เพราะการพาณิชย์ส่วนใหญ่ยังเป็นการพาณิชย์ที่ใช้กระดาษเป็นพื้นฐาน (Paper-based Commerce)

การประกอบธุรกรรมทางธุรกิจต่างๆ ได้เริ่มแปลี่ยนแปลงหลักการและรูปแบบการดำเนินการจากเดิมใช้เอกสารที่เป็นกระดาษเป็นหลัก มาเป็นข้อมูลอิเล็กทรอนิกส์ที่อาศัยเครื่องคอมพิวเตอร์เป็นเครื่องมือในการจัดเก็บข้อมูล ความแตกต่างระหว่างการพาณิชย์ที่ใช้กระดาษ (Paper-based Commerce) และการพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce) จึงมีความสำคัญอย่างยิ่งต่อการพัฒนากฎหมายที่เกี่ยวข้อง ทั้งนี้เนื่องจากคุณลมบัติต่างๆ ที่ปรากฏบนธุรกรรมที่ใช้กระดาษ จะไม่สามารถกระทำได้ในรูปของอิเล็กทรอนิกส์ ยกตัวอย่างเช่นข้อความหรือข้อมูลอิเล็กทรอนิกส์ที่เก็บในเครื่องคอมพิวเตอร์จะเป็นกลุ่มของตัวเลข Binary หรือ Bits (ตัวเลข "ศูนย์" กับ "หนึ่ง") ซึ่งจะแสดงค่าเป็นตัวหนังสือหรือตัวเลขตามลักษณะของข้อมูลที่เก็บไว้ในหน่วยความจำ การเปลี่ยนแปลงค่าใดๆ สามารถกระทำได้โดยใช้กระแสไฟฟ้าเพียงเล็กน้อยเท่านั้น ดังนั้นหากปราศจากระบบการป้องกันที่ดีพอแล้ว ข้อมูลต่างๆ ที่เก็บในเครื่องคอมพิวเตอร์จะถูกเปลี่ยนแปลงอย่างปราศจากร่องรอยใดๆ

นอกจากนี้ ความแตกต่างประการสำคัญระหว่างการพาณิชย์ที่ใช้กระดาษ (Paper-based Commerce) และการพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce) ก็คือกฎหมายต่างๆ ที่ใช้รองรับการประกอบธุรกรรมบนกระดาษไม่สามารถนำมาใช้ได้กับกับสื่ออิเล็กทรอนิกส์ โดยเฉพาะในเรื่องของการลงลายมือชื่อ (Hand-written Signature) ซึ่งไม่สามารถกระทำได้บนสื่ออิเล็กทรอนิกส์ ทำให้การทำธุรกรรมหรือนิติกรรมสัญญาบางลักษณะที่กฎหมายกำหนดในต้องมีการลงลายมือชื่อไม่สามารถกระทำได้อย่างที่เคยปฏิบัติกันมา

---

[1] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 9

3.1 กฎหมายกับลายมือชื่อ

3.1.1 ประวัติของการลงลายมือชื่อ

ในอดีตกาลชาวอัสซีเรียน (Assyrians) และชาวจีน (Chinese) ได้เริ่มทำการบันทึกพร้อมทั้งประทับลายนิ้วมือและลงชื่อในเอกสารทางกฎหมาย ชาวบาบิโลน (Babylonians) ได้ทำเอกสาร (Document) บนโต๊ะดินเหนียวและประทับลายนิ้วมือของตนลงในดินเหนียวเพื่อเป็นการยืนยันความถูกต้องของเอกสาร[2] ในปี ค.ศ.1677 รัฐสภาของประเทศอังกฤษได้ออก Statute of Frauds ที่กำหนดให้นิติกรรมสัญญาบางอย่างต้องทำเป็นหนังสือ (พร้อมลงลายมือชื่อ) จึงจะมีผลตามกฎหมาย[3] ในปัจจุบันนี้กฎหมายจะวางข้อกำหนดอย่างชัดเจนในการใช้เครื่องมือในการตรวจสอบความถูกต้องแท้จริง (Authentication) โดยใช้ลายมือชื่อเพื่อวัตถุประสงค์ในเรื่องของแบบของนิติกรรมสัญญาและในเรื่องของพยานหลักฐาน หากนิติกรรมสัญญาไม่ได้ทำตามแบบที่กฎหมายกำหนด นิติกรรมสัญญาเหล่านั้นอาจจะไม่มีผลทางกฎหมาย หรือถ้ามีผลทางกฎหมายแต่ศาลก็จะไม่ยอมรับบังคับให้ หรือในบางกรณีการถือครองเอกสารที่ได้รับการตรวจสอบความถูกต้องแท้จริงจะก่อให้เกิดสิทธิกับผู้ถือเอกสารดังกล่าว เช่น กรณีของการถือตั๋วแลกเงิน เช็คผู้ถือ หรือใบตราส่ง สำหรับใบตราส่งการโอนใบตราส่งจะเป็นการแสดงว่ากรรมสิทธิในสินค้าที่ระบุในใบตราส่งได้โอนไปด้วย

"นิติกรรม หมายความว่า การใดๆ อันทำลงโดยชอบด้วยกฎหมายและด้วยใจสมัครมุ่งโดยตรงต่อการผูกนิติสัมพันธ์ขึ้นระหว่างบุคคล เพื่อจะก่อ เปลี่ยนแปลง โอน สงวน หรือระงับซึ่งสิทธิ"[4] เพราะฉะนั้นเนื้อหาของนิติกรรมดังกล่าวย่อมจะต้องมีอยู่พร้อมที่จะสามารถยืนยันถึงสิทธิ หน้าที่และความรับผิดชอบของผู้เป็นฝ่ายในนิติกรรมเมื่อเกิดปัญหาหรือข้อพิพาทขึ้น กระบวนการในการรับรองการมีอยู่ของนิติกรรมหรือความถูกต้องของนิติกรรม กระบวนการดังกล่าวเรียกว่า "การพิสูจน์ความถูกต้องแท้จริง" (Authentication)

---

[2] Vincent J. Gnoffo, Requiring A thumbrint for Notorized Transactions : The Battle Against Document Fraud, 31 J. Marshall L. Rev. 803, 806 (1998) Referent in John C. Anderson and Michael L. Closen, :" Document Authentication in Electronic Commerce: The Misleading Notary Public Analog for The Digital Signature Certification Authority", Id., p.840

[3] John C. Anderson and Michael L. Closen, :"Document Authentication in Electronic Commerce: The Misleading Notary Public Analog for The Digital Signature Certification Authority", Id., p.841

[4] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 149

เพื่อวัตถุประสงค์ในการตรวจสอบความถูกต้องแท้จริง สังคมและกฎหมายได้พัฒนาเครื่องมือเพื่อใช้ในการการพิสูจน์ความถูกต้องแท้จริง ไม่ว่าจะเป็นการประทับลายนิ้วมือหรือการประทับตราประจำตัวลงบนวัสดุต่างๆ เช่น ดินเหนียวหรือครั่ง เป็นต้น ซึ่งเป็นเครื่องมือที่ใช้ยืนยันความแน่นอนของเจตนา[5] ในปัจจุบันลายมือชื่อ (Hand-written Signature) เป็นเครื่องมือในการตรวจสอบความถูกต้องแท้จริงที่เป็นที่นิยมที่สุด ทั้งได้รับการรับรองโดยกฎหมาย โดยการลงลายมือชื่อในเอกสารที่เป็นกระดาษ ผู้ลงนามจะแสดงว่าตนเป็นผู้เขียนหรือทำเอกสารนั้น และรับรองว่าข้อมูลหรือข้อความในเอกสารมีความถูกต้องสมบูรณ์ ทั้งตนมีเจตนาที่จะผูกพันตามข้อความที่ปรากฏในเอกสาร นอกจากนั้นในบางกรณีการลงลายมือชื่อยังเป็นเครื่องแสงหรือยืนยันว่าข้อเท็จจริงตามข้อมูลหรือข้อความที่ปรากฏในเอกสารได้กระทำเสร็จสมบูรณ์แล้ว เช่น ลงลายมือชื่อเพื่อแสดงว่าได้รับสิ่งของหรือเอกสารตามที่ระบุไว้เรียบร้อยแล้ว เป็นต้น แต่ก็มิได้หมายความว่าลายมือชื่อจะเป็นเครื่องมือเพียงอย่างเดียวที่กฎหมายยอมรับ กฎหมายยังยอมรับเครื่องหมายอื่นๆ ให้ใช้แทนลายมือชื่อได้ แต่ต้องกระทำตามที่กฎหมายกำหนดไว้[6]

3.1.2 วัตถุประสงค์ของลายมือชื่อในทางกฎหมาย

วัตถุประสงค์หรือความจำเป็นที่ต้องมีลายมือชื่อทั้งในทางปฏิบัติและในทางกฎหมายนั้น เป็นเพราะต้องการที่จะแยกระบุว่าลายมือชื่อ สัญลักษณ์ ตราเครื่องมือหริอสิ่งอื่นใดที่มีลักษณะใกล้เคียงกันเป็นเครื่องมือ หรือตราที่แท้จริงของผู้ของกระทำการลงลายมือชื่อหรือประทับตรานั้น ลายมือชื่อยังเป็นเครื่องบอกให้ทราบถึงความมีผลและความถูกต้องแท้จริงของเอกสาร ทั้งยังแสดงให้ผู้ลงลายมือชื่อทราบว่าข้อความในเอกสารที่ทำการลงลายมือชื่อมีว่าอย่างไร

ลายมือชื่อไม่ใช่ส่วนหนึ่งของสาระสำคัญของธุรกรรม (Transaction) หรือนิติกรรมสัญญา แต่ลายมือชื่อเป็นการแสดงออกถึงหรือเป็นแบบฟอร์มของธุรกรรมหรือนิติกรรมสัญญา[7]

---

[5] กฤษณะ ช่างกล่อม. (ร่าง) รายงานการศึกษาวิจัยเรื่องกฎหมายลายมือชื่อดิจิตอล หน้า 58

[6] มาตรา 9 ประมวลกฎหมายแพ่งและพาณิชย์

[7] Information Security Committee, Electronic Commerce Division, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce. Id., p.4

วัตถุประสงค์ของลายมือชื่อในทางกฎหมาย คือ [8]

3.1.2.1 พยานหลักฐาน (Evidence)

ลายมือชื่อเป็นเครื่องมือในการตรวจสอบความถูกต้องแท้จริงของเอกสาร โดยลายมือชื่อ (Hand-written Signature) จะสร้างพยานหลักฐานจากคุณสมบัติทางเคมีของหมึก (Ink) ในการติดตรึงกับกระดาษและลักษณะอันเป็นส่วนบุคคลของลายมือชื่อที่สามารถระบุถึงผู้ลงลายมือชื่อได้ เมื่อผู้ลงลายมือชื่อทำการลงลายมือชื่อ (หรือทำการอื่นใดที่กฎหมายยอมรับว่ามีผลเหมือนกับการลงลายมือชื่อ) ในเอกสาร เอกสารดังกล่าวถือได้ว่าเป็นผลมาจากการกระทำของผู้ลงลายมือชื่อ อย่างเช่น ตามมาตรา 456 ประมวลกฎหมายแพ่งและพาณิชย์ วรรคสองและสาม ซึ่งกำหนดให้สัญญาซื้อขายสังหาริมทรัพย์ที่มีราคาห้าร้อยบาทหรือกว่านั้น จะต้องมีหลักฐานเป็นหนังสือลงลายมือชื่อฝ่ายผู้ต้องรับผิด* จึงจะฟ้องร้องบังคับคดีกันได้ ซึ่งจะเห็นได้ว่ากฎหมายมีเจตนาให้มีการทำสัญญาซื้อขายสังหาริมทรัพย์ที่มีราคาตั้งแต่ห้าร้อยบาทขึ้นไปเป็นหนังสือ พร้อมทั้งมีการลงลายมือชื่อ เพื่อใช้เป็นหลักฐานในการฟ้องร้องคดีในชั้นศาล แม้ว่าสัญญาซื้อขายสังหาริมทรัพย์ดังกล่าวมิได้ทำเป็นหนังสือและลงลายมือชื่อก็ตาม สัญญาซื้อขายดังกล่าวก็มีผลสมบูรณ์ตามกฎหมาย แต่ไม่สามารถที่จะฟ้องร้องบังคับคดีได้เท่านั้น เพราะขาดหลักฐานที่จะใช้พิสูจน์ในศาล เพราะฉะนั้นการลงลายมือชื่อตามมาตรานี้จึงใช้เป็นพยานหลักฐานถึงความมีอยู่ของสัญญาซื้อขายนั่นเอง

นอกจากนี้ลายมือชื่อยังเป็นพยานหลักฐานว่าข้อความในเอกสารมิได้ถูกแก้ไขหรือถูกแก้ไขโดยผู้ลงลายมือชื่อ เช่นในนิติกรรมสัญญาผู้ลงลายมือชื่อมักนิยมลงลายมือชื่อหรือลงนามย่อกำกับในส่วนท้ายของกระดาษทุกแผ่นในนิติกรรมสัญญา หรือทำการลงลายมือชื่อหรือลงนามย่อกำกับกำกับในทุกๆ ส่วนที่มีการแก้ไข เป็นต้น

3.1.2.2 ระเบียบพิธี (Ceremony)

การลงลายมือชื่อในเอกสารคือการเตือนให้ผู้ลงลายมือชื่อให้ความสนใจถึงผลในทางกฎหมายของการกระทำของผู้ลงลายมือชื่อ ซึ่งในที่นี้คือการลงลายมือชื่อ เมื่อทำการลงลายมือชื่อแล้วผู้ลงลายมือชื่อก็จะเกิดความผูกพันตามกฎหมาย ทั้งยังเป็นการป้องกันมิให้เกิดความผูกพันโดยไม่ได้ตั้งใจ (Inconsiderate Engagements) รวมถึงเป็นระเบียบพิธีการที่จะแสดงออกถึง

---

[8] Information Security Committee, Electronic Commerce Division, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce. Id., p.5

* โปรดดู ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 456

ความสมบูรณ์ของการทำนิติกรรมสัญญาหรือธุรกรรมใดๆ ซึ่งจะเห็นได้จากการที่ประมวลกฎหมายแพ่งและพาณิชย์มาตรา 9 วรรคแรก บัญญัติไว้ว่า "เมื่อมีกิจการอันใดซึ่งกฎหมายบังคับให้ทำเป็นหนังสือ บุคคลผู้จะต้องทำหนังสือไม่จำเป็นจะต้องเขียนเอง แต่หนังสือนั้นต้องลงลายมือชื่อของบุคคลนั้น"

3.1.2.3 แสดงออกซึ่งความยอมรับหรือความเห็นชอบ (Approval)

การลงลายมือชื่อในทางกฎหมาย จารีตประเพณี หรือข้อปฏิบัติใดๆ ต่างให้ความหมายอย่างชัดเจนว่า ผู้ลงลายมือชื่อในเอกสารให้การยอมรับ ให้ความเห็นชอบ ให้อำนาจหรืออนุญาตในเอกสารดังกล่าว เช่น ในกรณีที่ลูกจ้างทำการยื่นใบลาเพื่อขอลาพักผ่อนต่อนายจ้าง ถ้านายจ้างลงลายมือชื่อในใบลานั่น แสดงว่านายจ้างยอมรับหรือให้ความเห็นชอบในการลาพักผ่อนดังกล่าวของลูกจ้าง เป็นต้น หรือผู้ลงลายมือชื่อในเอกสารมีความตั้งใจที่จะให้ข้อความหรือตัวเอกสารดังกล่าวมีผลในทางกฎหมาย เช่น การลงลายมือชื่อในสัญญาซื้อขายคอมพิวเตอร์ หรือลงลายมือชื่อในตั๋วแลกเงิน เป็นต้น

3.1.2.4 เป็นเครื่องมือที่มีเหตุผลที่ดีและมีประสิทธิภาพที่สุด (Efficiency and logistics)

ลายมือชื่อในเอกสารเป็นการสื่อที่ชัดเจนและแสดงออกว่าข้อความหรือเงื่อนไขใดๆ ที่ปรากฏในเอกสารนั้นเป็นข้อความสุดท้าย (Finality) ที่ผู้ลงลายมือชื่อได้เห็นชอบด้วยในการธุรกรรมใดๆ ทั้งยังเป็นเครื่องมือที่มีเหตุผลและมีประสิทธิภาพที่สุดในการแสดงออกถึงเจตนาใดๆ เช่น การลงลายมือชื่อในตราสารเปลี่ยนมือ (Negotiable Instrument) เพื่อทำการเปลี่ยนมือ ซึ่งง่าย สะดวก รวดเร็ว และมีสิ่งขัดขวางน้อย เป็นต้น ทั้งลายมือชื่อ (หรือสิ่งอื่นใดที่กฎหมายยอมรับว่ามีผลเหมือนกับการลงลายมือชื่อ) ยังเป็นเครื่องมือที่ดีที่สุดที่สามารถมีผลเป็นพยานหลักฐาน เป็นระเบียบพิธี และเป็นการแสดงออกซึ่งการยอมรับหรือเห็นชอบตามจุดประสงค์ทั้งสามข้อข้างต้น

การทำนิติกรรมสัญญาตามแบบที่กฎหมายกำหนดรวมไปถึงการลงลายมือชื่อนั้น ในแต่ละระบบกฎหมายและในแต่ละช่วงเวลาก็มีความแตกต่างกันออกไป ผลของการไม่ได้นำนิติกรรมสัญญาตามแบบที่กฎหมายกำหนดก็แตกต่างกันออกไป โดยขึ้นอยู่กับประเภทของนิติกรรมสัญญานั้น ใน Statute of Frauds ตามแบบแผนของ Common Law การไม่ทำนิติกรรมสัญญาตาม

แบบที่กำหนดไม่ได้หมายความว่านิติกรรมสัญญานั้นไม่ถูกต้อง แต่ศาลจะไม่ยอมรับบังคับนิติกรรมสัญญาดังกล่าวให้[9]

จากวัตถุประสงค์ของลายมือชื่อข้างต้น ลายมือชื่อเป็นเครื่องมือในการตรวจสอบความถูกต้องแท้จริงที่มีคุณสมบัติดังนี้

1. การตรวจสอบความถูกต้องแท้จริงของผู้ลงลายมือชื่อ (Signer Authentication) ลายมือชื่อสามารถชี้บอกถึงตัวบุคคลผู้ทำการลงลายมือชื่อในเอกสาร ข้อความ หรือบันทึกได้ และเป็นการยากที่บุคคลอื่นจะสามารถทำการลอกเลียนแบบให้เหมือน หรือกระทำการลงลายมือชื่อโดยไม่มีอำนาจ
2. การตรวจสอบความถูกต้องแท้จริงของเอกสารหรือข้อความ (Document or Message Authentication) ลายมือชื่อสามารถชี้บอกได้ว่าสิ่งใดหรือข้อความใดที่ได้รับการลงลายมือชื่อ ซึ่งจะมีผลทำให้สิ่งหรือข้อความนั้นยากที่จะปลอมแปลงหรือทำการเปลี่ยนแปลงโดยที่ไม่สามารถตรวจจับได้ภายหลังจากที่ได้ทำการลงลายมือชื่อ
3. เป็นการแสดงการถึงยอมรับ (Affirmative Act) การลงลายมือชื่อเป็นการแสดงออกถึงการยอมรับ ที่เป็นส่วนหนึ่งของหน้าที่ของลายมือชื่อในเรื่องของระเบียบพิธีการและการแสดงออกซึ่งการยอมรับหรือความเห็นชอบ และสร้างความรู้สึกว่านิติกรรมหรือธุรกรรมนั้นมีผลในทางกฎหมาย
4. มีประสิทธิภาพ (Efficiency) ลายมือชื่อ วิธีการลงลายมือชื่อและวิธีการตรวจสอบเป็นวิธีการที่ดีที่สุดเท่าที่จะเป็นไปได้ ในการสร้างความมั่นใจในเรื่องของการตรวจสอบความถูกต้องแท้จริงของผู้ลงลายมือชื่อและการตรวจสอบความถูกต้องแท้จริงของเอกสารหรือข้อความ

3.1.3 คุณสมบัติและความสามารถของลายมือชื่อดิจิตอล

ในปัจจุบันจากการที่เทคโนโลยีในการติดต่อสื่อสารพัฒนาไปอย่างมาก การติดต่อสื่อสารแบบเดิม ด้วยการพบปะหน้าตากัน หรือเขียนจดหมายระหว่างกัน ถูกแทนที่ด้วยเทคโนโลยีเครือข่ายอิเล็กทรอนิกส์ที่ทันสมัย ทำให้การใช้ลายมือชื่อแบบเดิม (Hand-written Signature) ไม่สามารถกระทำได้ เพราะการติดต่อสื่อสารมิได้ทำกันบนกระดาษเป็นพื้นฐานเหมือนเช่นเดิม จึงเกิด

---

[9] Information Security Committee, Electronic Commerce Division, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, Id., p.6

ความต้องการเครื่องมือในการตรวจสอบความถูกต้องแท้จริงที่สามารถแทนที่ลายมือชื่อ (Hand-written Signature) ได้ ลายมือชื่อดิจิตอลจึงถูกคิดค้นขึ้น

ลายมือชื่อดิจิตอล คือ ชุดของตัวเลขที่เป็นผลมาจากการเข้ารหัสโดยวิธีการทางคณิตศาสตร์ ซึ่งกระบวนการดังกล่าวทำโดยเครื่องคอมพิวเตอร์หรือเครื่องอิเล็กทรอนิกส์ให้ปรากฏบนเอกสารอิเล็กทรอนิกส์ [10]

การใช้ลายมือชื่อดิจิตอลเกี่ยวข้องกับขบวนการ 2 ขบวนการ ขบวนการแรกเกี่ยวข้องกับผู้ลงลายมือชื่อ ขบวนการที่สองเกี่ยวข้องกับผู้รับเอกสารที่มีการลงลายมือชื่อดิจิตอล ดังนี้

1. การลงลายมือชื่อดิจิตอล (Digital Signature Creation) จะทำโดยการนำข้อความหรือข้อมูลที่จะทำการลงลายมือชื่อ มาทำการ Hash Function จากนั้นจะนำผลที่ได้ คือ Hash Value หรือ Hash Result มาทำการเข้ารหัสโดยกุญแจรหัสส่วนตัว (Private Key) ซึ่งผู้ลงลายมือชื่อเป็นผู้เดียวที่มีกุญแจรหัสดังกล่าว ผลที่ได้คือลายมือชื่อดิจิตอลของผู้นั้น ซึ่งลายมือชื่อดิจิตอลดังกล่าว มีความเกี่ยวพันกับข้อความที่ทำการลงลายมือชื่อ และมีความเกี่ยวพันกับตัวบุคคลผู้ลงลายมือชื่อ
2. การตรวจสอบลายมือชื่อดิจิตอล (Digital Signature Verification) คือขบวนการในการตรวจสอบลายมือชื่อดิจิตอล โดยอาศัยข้อมูลหรือข้อความต้นฉบับและกุญแจรหัสสาธารณะที่มีความเกี่ยวข้องกับกุญแจรหัสส่วนตัวที่ใช้ในการลงลายมือชื่อดิจิตอลว่า ลายมือชื่อดิจิตอลถูกสร้างขึ้น ด้วยค่า Hash Value หรือ Hash Result ที่ได้มาจากการนำข้อมูลหรือข้อความต้นฉบับมาทำการ Hash Function และถูกสร้างขึ้นด้วยกุญแจรหัสส่วนตัวที่มีความเกี่ยวเนื่องกับกุญแจรหัสสาธารณะดังกล่าวหรือไม่

จากขั้นตอนในการลงลายมือชื่อและการตรวจสอบตามที่ได้อธิบายในบทที่ 2 ลายมือชื่อดิจิตอลสามารถกระทำหน้าที่สำคัญสามประการในแนวความคิดพื้นฐานของความไว้วางใจและความเชื่อมั่นในเครือข่ายอิเล็กทรอนิกส์ตามที่ได้กล่าวไว้ในหัวข้อ 2.1.1 ได้เป็นอย่างดี ดังนี้

1. <u>การตรวจสอบความถูกต้องแท้จริงของต้นกำเนิดเอกสาร</u> (Origin Authentication) ลายมือชื่อดิจิตอลสามารถที่จะทำระบุได้ว่าใครเป็นผู้ลงลายมือชื่อ เพราะว่าขั้นตอนในการลงลายมือชื่อนั้น จะต้องมีการใช้กุญแจรหัสส่วนตัวซึ่งมีบุคคลผู้ลงลายมือชื่อเท่านั่นที่มีกุญแจรหัสดังกล่าว เพราะฉะนั้นการเก็บกุญแจรหัสส่วนตัวให้เป็นความลับและการเก็บรักษากุญแจสรหัสส่วนตัวให้มีอยู่ที่เจ้าของกุญแจ

---

[10] B. Schneier, Applied Cryptography, (USA : John Wiley & Sons Inc., 1994),p. 31 ; C. Davis, Legal Aspects of Digital Signature, (in Tolley's Computer and Practice, 1995) p.165 อ้างถึงใน กฤษณะ ช่างกล่อม, <u>(ร่าง) รายงานการศึกษาวิจัยเรื่องกฎหมายลายมือชื่อดิจิตอล</u> หน้า 64

รหัสส่วนตัวแต่เพียงผู้เดียว จึงเป็นสิ่งสำคัญอย่างมากในระบบลายมือชื่อดิจิตอล การตรวจสอบความถูกต้องแท้จริงของต้นกำเนิดเอกสาร ก็คือส่วนหนึ่งของการตรวจสอบความถูกต้องแท้จริงของบุคคลผู้ใช้ระบบ (Authentication of Users) นั่นเอง

2. การรักษาความถูกต้องสมบูรณ์ของข้อมูล (Integrity) ลายมือชื่อดิจิตอลสามารถที่จะตรวจสอบความถูกต้องหรือความสมบูรณ์ของข้อมูลที่ได้ทำการลงลายมือชื่อ โดยสามารถทราบได้ทันทีว่าข้อมูลที่มีการลงลายมือชื่อได้ถูกเปลี่ยนแปลงแก้ไขภายหลังจากที่ได้ทำการลงลายมือชื่อ ไม่ว่าด้วยจากเจตนาอันมิชอบ โดยความผิดพลาดของเครื่องมือ หรือโดยเหตุอื่นใดก็ตาม เพราะถ้ามีการแก้ไขข้อความที่ทำการลงลายมือชื่อดิจิตอลภายหลังการลงลายมือชื่อดิจิตอล จะทำให้การตรวจสอบยืนยันลายมือชื่อดิจิตอลไม่สามารถกระทำได้
3. การป้องกันการปฏิเสธความรับผิดชอบ (Non-repudiation) ลายมือชื่อดิจิตอลสามารถที่จะทำการป้องกันการปฏิเสธความรับผิดชอบของบุคคลที่กระทำการลงลายมือชื่อได้ เพราะในขั้นตอนการตรวจสอบยืนยันลายมือชื่อดิจิตอล จะมีการใช้ใบรับรองที่จะระบุชื่อของเจ้าของกุญแจรหัสและค่าของกุญแจรหัสสาธารณะที่มีความเกี่ยวพันกับกุญแจรหัสส่วนตัวที่บุคคลดังกล่าวยึดถือไว้ ถ้าสามารถใช้กุญแจรหัสสาธารณะที่ระบุในใบรับรองทำการตรวจสอบยืนยันลายมือชื่อดิจิตอลได้ บุคคลผู้ลงลายมือชื่อก็จะไม่สามารถปฏิเสธได้ว่าตนมิได้เป็นผู้ลงลายมือชื่อ

3.1.4 เปรียบเทียบลายมือชื่อ (Hand-written Signature) กับลายมือชื่อดิจิตอล

จากการที่ลายมือชื่อดิจิตอลถูกคิดค้นขึ้น เพื่อตอบสนองในการหาเครื่องมือที่ใช้พิสูจน์ความถูกต้องแท้จริง (Authentication) ของธุรกรรมที่กระทำผ่านเครือข่ายอิเล็กทรอนิกส์ เมื่อทำการศึกษาคุณสมบัติในการพิสูจน์ความถูกต้องแท้จริงของลายมือชื่อดิจิตอลจะพบว่า ลายมือชื่อดิจิตอลสามารถที่จะทำหน้าที่แทนลายมือชื่อ (Hand-written Signature) ได้เป็นอย่างดี ดังนี้

1. การตรวจสอบความถูกต้องแท้จริงของผู้ลงลายมือชื่อ (Signer Authentication) ลายมือชื่อดิจิตอลสามารถชี้บอกถึงตัวบุคคลผู้ทำการลงลายมือชื่อในเอกสาร ข้อความหรือบันทึกได้ และเป็นการยากที่บุคคลอื่นจะสามารถทำการลอกเลียนแบบให้เหมือน หรือกระทำการลงลายมือชื่อโดยไม่มีอำนาจ เพราะเพราะว่าขั้นตอนในการลงลายมือชื่อนั้น จะต้องมีการใช้กุญแจรหัสส่วนตัวซึ่งมีบุคคลผู้ลงลายมือชื่อเท่านั้นที่มีกุญแจรหัสส่วนตัวดังกล่าว ทั้งกุญแจรหัสส่วนตัวนี้ก็ยากที่จะทำการลอกเลียนแบบหรือสร้างขึ้นให้เหมือนกันได้

2. <u>การตรวจสอบความถูกต้องแท้จริงของเอกสารหรือข้อความ</u> (Document or Message Authentication) ลายมือชื่อดิจิตอลสามารถชี้บอกได้ว่าสิ่งใดหรือข้อความใดที่ได้รับการลงลายมือชื่อ ซึ่งจะมีผลทำให้สิ่งหรือข้อความนั้นยากที่จะปลอมแปลงหรือทำการเปลี่ยนแปลงโดยที่ไม่สามารถตรวจจับได้ภายหลังจากที่ได้ทำการลงลายมือชื่อ ซึ่งลายมือชื่อดิจิตอลสามารถทำหน้าที่นี้ได้ดียิ่งกว่าการลงลายมือชื่อ (Hand-written Signature) ในเอกสารที่เป็นกระดาษ เพราะการลงลายมือชื่อจะกระทำกันที่หน้าสุดท้าย และปลายกระดาษในนิติกรรมหรือสัญญาทุกๆ แผ่น มิได้ทำการลงลายมือชื่อกันทุกคำในนิติกรรมหรือสัญญา ข้อความที่ทำการลงลายมือชื่อจึงสามารถที่จะถูกแก้ไขเปลี่ยนแปลงได้ แต่ถ้ามีการแก้ไขข้อความที่ทำการลงลายมือชื่อดิจิตอลภายหลังการลงลายมือชื่อดิจิตอลแล้ว จะทำให้การตรวจสอบยืนยันลายมือชื่อดิจิตอลไม่สามารถกระทำได้เลย
3. <u>เป็นการแสดงการถึงยอมรับ</u> (Affirmative Act) การลงลายมือชื่อดิจิตอลเป็นการแสดงออกถึงการยอมรับ เนื่องจากในขั้นตอนการลงลายมือชื่อดิจิตอลจะต้องใช้กุญแจรหัสส่วนตัวของผู้ลงลายมือชื่อ ซึ่งสามารถทำหน้าที่ของลายมือชื่อในเรื่องของระเบียบพิธีการ ในการเตือนให้ผู้ลงลายมือชื่อตระหนักถึงความผูกพันในทางกฎหมาย รวมทั้งการแสดงออกซึ่งการยอมรับหรือความเห็นชอบ และสร้างความรู้สึกว่านิติกรรมหรือธุรกรรมนั้นมีผลในทางกฎหมาย ภายหลังจากที่ตนลงลายมือชื่อดิจิตอล
4. <u>มีประสิทธิภาพ</u> (Efficiency) ลายมือชื่อดิจิตอลมีวิธีการในการลงลายมือชื่อและวิธีการตรวจสอบ ที่เป็นวิธีการที่ดีที่สุดเท่าที่จะเป็นไปได้ในปัจจุบัน ในการสร้างความมั่นใจในเรื่องของการตรวจสอบความถูกต้องแท้จริงของผู้ลงลายมือชื่อและการตรวจสอบความถูกต้องแท้จริงของเอกสารหรือข้อความที่ได้ทำการติดต่อสื่อสารผ่านทางเครือข่ายอิเล็กทรอนิกส์ และเมื่อเปรียบเทียบกับลายมือชื่อ (Hand-written Signature) ที่ลงในเอกสารที่เป็นกระดาษ การตรวจสอบลายมือชื่อดังกล่าวอาจต้องอาศัยตัวอย่างของลายมือชื่อพร้อมทั้งเจ้าหน้าที่ที่เป็นผู้ชำนาญการ ซึ่งเป็นการสิ้นเปลืองค่าใช้จ่าย แรงงาน รวมทั้งเวลาอีกด้วย ลายมือชื่อดิจิตอลจึงเป็นเครื่องมือที่ดีที่สุดในปัจจุบันในการตรวจสอบความถูกต้องแท้จริงของข้อมูลหรือข้อความในการสื่อสารผ่านทางเครือข่ายอิเล็กทรอนิกส์ ทั้งยังเป็นที่ยอมรับในหลายประเทศทั่วโลก โดยได้มีการบัญญัติกฎหมายที่เกี่ยวข้องกับการใช้ลายมือชื่อดิจิตอล เพื่อรองรับการใช้ลายมือชื่อดิจิตอลในการสื่อสารผ่านทางเครือข่ายอิเล็กทรอนิกส์

3.1.5 ลายมือชื่อดิจิตอลกับกฎหมายในปัจจุบัน

3.1.5.1 ลายมือชื่อดิจิตอลกับกฎหมายไทย

ก่อนที่ร่างกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์จะผ่านความเห็นชอบของรัฐสภาและมีผลบังคับใช้ กฎหมายไทยมีบทบัญญัติที่เกี่ยวข้องกับการลงลายมือชื่ออยู่คือ ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 9 ซึ่งบัญญัติว่า "เมื่อมีกิจกรรมอันใดซึ่งกฎหมายบังคับให้ทำเป็นหนังสือบุคคลผู้จะต้องทำหนังสือไม่จำเป็นต้องเขียนเองแต่หนังสือนั้นจะต้องลงลายมือชื่อของบุคคลนั้น

ลายพิมพ์นิ้วมือ แกงได ตราประทับ หรือเครื่องหมายอื่นทำนองเช่นว่านั้นที่ทำลงในเอกสารแทนการลงลายมือชื่อ หากมีพยานลงลายมือชื่อรับรองไว้ด้วยสองคนแล้วให้ถือเสมอกับลงลายมือชื่อ

ความในวรรคสองไม่ให้ใช้บังคับแก่การลงพิมพ์นิ้วมือ แกงได ตราประทับหรือเครื่องหมายอื่นทำนองเช่นว่านั้น ซึ่งทำลงในเอกสารที่ทำต่อหน้าพนักงานเจ้าหน้าที่"

เหตุที่ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 9 บัญญัติบังคับให้ผู้ทำหนังสือต้องลงลายมือชื่อเป็นเพราะต้องการจะรับรองหรือยืนยันให้ทราบว่า บุคคลผู้นั้นเป็นผู้จะต้องผูกพันตนรับผิดชอบตามข้อความที่ได้ทำขึ้นอันระบุในหนังสือนั่นเอง เพราะหากมีแต่หนังสือไม่มีลายมือชื่อ ก็อาจจะหาผู้ต้องรับผิดหรือต้องผูกพันตนตามที่หนังสือระบุไว้ไม่ได้ คือไม่รู้ว่าใครเป็นผู้ต้องผูกพันตนรับผิดนั่นเอง นอกจากลายมือชื่อแล้ว กฎหมายยังยอมรับลายพิมพ์นิ้วมือ แกงได ตราประทับ หรือเครื่องหมายอื่นๆ ด้วย แต่ต้องมีพยานลงลายมือชื่อรับรองสองคน[11]

เมื่อพิจารณากฎหมายในทุกระบบ รวมทั้งกฎหมายไทย จะเห็นได้ว่าไม่มีระบบกฎหมายใดวางข้อบังคับว่าลายมือชื่อจะต้องเป็นเพียงชื่อของตัวบุคคลผู้ลงลายมือชื่อเท่านั้น ลายมือชื่ออาจปรากฏในรูปของชื่อเต็ม นามย่อ ชื่อเล่น ตราประทับ หรือแม้แต่กากบาท หากว่าผู้ที่เป็นเจ้าของมีเจตนาที่จะถือว่าสัญลักษณ์ดังกล่าวเป็นลายมือชื่อ ประเด็นสำคัญจึงมิได้อยู่ที่สัญลักษณ์ที่ใช้ หากอยู่ที่เจตนาเบื้องหลังสัญลักษณ์ดังกล่าวมากกว่า แต่อย่างไรก็ตามการยอมรับสัญลักษณ์ต่างๆ แทนการลงลายมือชื่อในกฎหมายไทยนั้น ก็จะต้องมีพยานทำการลงลายมือชื่อรับรองสองคน[12] หรือต้องเป็นการกระทำสัญลักษณ์นั้นต่อหน้าพนักงานเจ้าหน้าที่[13] จึงจะมีผลเสมือน

---

[11] เลอสรร ธนสุกาญจน์, จิตตภัทร เครือวรรณ์ และสุธรรม อยู่ในธรรม. แนวทางการพัฒนากฎหมายแลกเปลี่ยนข้อมูลด้วยสื่ออิเล็กทรอนิกส์ในประเทศไทย. (กรุงเทพมหานคร: ห้างหุ้นส่วนจำกัด พี.เจ.เพลท โปรเซสเซอร์, 2541), หน้า 73-74

[12] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 9 วรรค 2

[13] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 9 วรรค 3

การลงลายมือชื่อ (Hand-written Signature) เพราะฉะนั้นการลงลายมือชื่อดิจิตอลในกฎหมายไทยจึงยังไม่มีผลเป็นลายมือชื่อ เพราะลายมือชื่อดิจิตอลมิใช่ลายมือชื่อ (Hand-written Signature) ตามความหมายในประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 9 และถ้าจะใช้ในความหมายของสัญลักษณ์อื่นใดที่สามารถใช้แทนลายมือชื่อได้ตามมาตรา 9 วรรค 2 ก็จะมีอุปสรรคในเรื่องของการที่ต้องมีพยานลงลายมือชื่อรับรอง 2 คน (ตามมาตรา 9 วรรค 2) หรือถ้าจะให้ไปลงลายมือชื่อดิจิตอลต่อหน้าพนักงานเจ้าหน้าที่ (ตามมาตรา 9 วรรค 3) ก็จะติดปัญหาในเรื่องความสะดวก รวมไปถึงความพอเพียงของพนักงานเจ้าหน้าที่อีกด้วย เพราะฉะนั้นลายมือชื่อดิจิตอลจึงยังไม่ได้รับการยอมรับเป็นลายมือชื่อแบบหนึ่งที่สามารถใช้แทนการลงลายมือชื่อในกระดาษได้

ตามคำพิพากษาฎีกาที่ 3046/2537 ซึ่งข้อเท็จจริงมีอยู่ว่า โจทก์และจำเลยได้ทำการโทรพิมพ์ติดต่อซื้อขายข้าวนึ่งต่อกัน จากนั้นโจทก์ได้เปิดเลตเตอร์ออฟเครดิต (Letter of Credit, L/C) เพื่อชำระค่าข้าวนึ่งให้แก่จำเลย แต่จำเลยไม่สามารถจัดส่งข้าวนึ่งให้โจทก์ได้เพราะเงื่อนไขตามเลตเตอร์ออฟเครดิตที่กำหนดไว้จำเลยไม่สามารถปฏิบัติได้ ศาลฎีกาวินิจฉัยว่า "...ปัญหาตามฎีกาโจทก์มีว่า สัญญาซื้อขายข้าวนึ่งระหว่างโจทก์กับจำเลยทั้งสองได้เกิดขึ้นตามกฎหมายหรือไม่ เห็นว่าการการซื้อขายข้าวนึ่งระหว่างโจทก์กับจำเลยทั้งสองได้เกิดขึ้นแล้วเมื่อการเจรจายุติลงตามเอกสารโทรพิมพ์หมาย จ.5 ถึง จ.9 แต่ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 456 วรรคสอง กำหนดว่าสัญญาซื้อขายสังหาริมทรัพย์ซึ่งตกลงกันมีราคาห้าร้อยบาทหรือกว่านั้นขึ้นไป สัญญาจะซื้อจะขาย คำมั่นในการขายทรัพย์ที่มีราคาห้าร้อยบาทหรือกว่านั้นขึ้นไปต้องมีหลักฐานเป็นหนังสือลงลายมือชื่อฝ่ายผู้ต้องรับผิดด้วย หรือได้วางประจำ หรือได้ชำระหนี้บางส่วนแล้วจึงจะฟ้องร้องบังคับคดีได้ ตามเอกสารหมาย จ.5 ถึง จ.9 ไม่ปรากฏหลักฐานการชำระหนี้บางส่วนหรือการวางมัดจำหรือลายมือชื่อของจำเลยทั้งสองที่ต้องรับผิด โจทก์จึงไม่สามารถฟ้องร้องให้บังคับคดีแก่จำเลยทั้งสองได้ ที่โจทก์ฎีกาโต้แย้งว่ามีแกงไดในเอกสารดังกล่าว ศาลฎีกาตรวจแล้วเห็นว่า เป็นเรื่องที่มิได้โต้แย้งและว่ากล่าวมาก่อนในศาลชั้นต้น ทั้งไม่ปรากฏแกงไดในเอกสารดังโจทก์อ้างแต่อย่างใด คดีฟังได้ว่า สัญญาตกลงซื้อขายข้าวนึ่งระหว่างโจทก์กับจำเลยที่ 1 ไม่สามารถจะฟ้องร้องบังคับคดีกันได้ ไม่จำเป็นต้องวินิจฉัยฎีกาโจทก์ในปัญหาอื่นต่อไป ฎีกาโจทก์ฟังไม่ขึ้น"

จากคำพิพากษาศาลฎีกาข้างต้น ท่านศิริชัย วัฒนโยธินได้ให้ความเห็นท้ายคำพิพากษาศาลฎีกาไว้ดังนี้ "...จะเห็นได้ว่าศาลได้ให้การยอมรับสัญญาซื้อขายที่ได้กระทำผ่านทางเครื่องโทรพิมพ์ ทั้งศาลฎีกายังพิเคราะห์ข้อความจากโทรพิมพ์เป็นสำคัญ จึงเป็นการตีความในเอกสารทำให้เห็นว่าศาลฎีกา...ถือว่าโทรพิมพ์เป็นพยานเอกสารที่ใช้นำสืบพิสูจน์ข้อเท็จจริงได้เหมือนกับพยานเอกสารทั่วๆ ไป..." จะเห็นได้ว่าศาลฎีกาของไทยได้มีแนวความเห็นที่ให้การยอม

---

* โปรดดู คำพิพากษาฎีกาที่ 3046/2537 พร้อมความเห็นท้ายคำพิพากษาของท่านศิริชัย วัฒนโยธิน

รับเอกสารที่ได้จากการ Print out ของเครื่องโทรพิมพ์ ซึ่งเป็นเครื่องมือทางอิเล็กทรอนิกส์อย่างหนึ่ง เป็นเอกสารที่ใช้นำสืบในศาลได้เสมือนพยานเอกสารทั่วไป แต่ไม่ปรากฏว่าได้มีการลงลายมือชื่อของฝ่ายจำเลยซึ่งเป็นฝ่ายที่จะต้องรับผิดในคดีนี้ จึงทำให้ศาลฎีกาวินิจฉัยว่าสัญญาซื้อขายข้าวนึ่งในกรณีนี้มิได้มีการทำหลักฐานเป็นหนังสือ พร้อมทั้งลงลายมือชื่อฝ่ายที่ต้องรับผิด ทำให้ไม่สามารถฟ้องร้องบังคับคดีกันได้ อย่างไรก็ตามโดยปกติแล้วเอกสารที่ได้จากการ print out ของเครื่องโทรพิมพ์จะมีการบันทึกถึงต้นทางของการติดต่อสื่อสาร รวมทั้งในบางกรณีก็จะได้มีการประทับตราของผู้ที่ทำการจัดส่ง แต่ตามข้อเท็จจริงที่ปรากฏในฎีกามิได้มีการระบุว่าแกงไดที่ฝ่ายโจทก์อ้างถึงคืออะไร อย่างไรก็ตามศาลฎีกาก็ได้วินิจฉัยแล้วว่าไม่ปรากฏว่ามีแกงไดในเอกสารดังกล่าวแต่อย่างใด จึงเป็นที่น่าเสียดายว่าศาลฎีกามิได้ให้การยอมรับสัญลักษณ์ใดๆ ที่ปรากฏใน print out ของเครื่องโทรพิมพ์เป็นแกงได ซึ่งสามารถมีสถานะเป็นลายมือชื่อได้ เพราะฉะนั้นการลงลายมือชื่อดิจิตอลในเอกสารที่ทำการติดต่อทางเครือข่ายอิเล็กทรอนิกส์ก็น่าที่จะไม่ได้รับการยอมรับให้เป็นแกงไดหรือลายมือชื่อเช่นเดียวกัน

ในปัจจุบันได้มีการร่างพระราชบัญญัติการว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... และร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. ... ซึ่งได้ผ่านการทำประชาพิจารณ์ และได้ส่งให้คณะกรรมการกฤษฎีกาตรวจแก้ไข ต่อมาในวันที่ 25 กรกฎาคม พ.ศ. 2543 คณะรัฐมนตรีได้ให้มีการรวมร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. .... (25 มาตรา) และร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. ... (70 มาตรา) เข้าด้วยกัน รายละเอียดในส่วนนี้จะได้นำเสนอในบทที่ 5 ต่อไป

3.1.5.2 ลายมือชื่อดิจิตอลกับกฎหมายต่างประเทศและองค์กรระหว่างประเทศ

ตามกฎหมายของประเทศสหรัฐอเมริกาก็ได้มีบทบัญญัตินิยามลายมือชื่อไว้ว่า "any symbol executed or adopted by a party with present intention to authentication a writing"[14] และศาลของประเทศสหรัฐอเมริกายังได้ตัดสินยอมรับสัญลักษณ์ต่างๆ ว่าเป็นลายมือชื่อได้ เช่น ชื่อในเทเลกซ์* ชื่อที่เขียนด้วยเครื่องพิมพ์** เป็นต้น[15] เพราะฉะนั้นลายมือชื่อจึงมิใช่แค่

---

[14] U.C.C. § 1-201(39) (1998).

* โปรดดู Joseph Denunzio Fruit Co. v. Crane, 70 F. Supp. 117; Franklin County Coop. v. MFC Services, 441 So.2d 1376 (Miss. 1983); Hideca Petroleum Corp v. Tampimac Oil Int'l Ltd., 740 S.W.2d 838 (Tex. Ct. App. 1987).

** ในคดี Watson v. Tom Growney Equip. Inc., 721 P.2d 1302 (N.M. 1986), ซึ่งศาลได้มีคำวินิจฉัยว่า "ชื่อที่พิมพ์ในเอกสารคำสั่งซื้อก็เพียงพอที่จะถือว่าเป็นการลงลายมือชื่อ เพราะผู้ลงลายมือชื่อก็ทำการกรอกรายละเอียดอื่นๆ ในแบบฟอร์มคำสั่งซื้ออย่างระมัดระวัง" และโปรดดูในคดี re

อะตอมของหมึกบนกระดาษเท่านั้น แต่หมายถึงสัญลักษณ์อะไรก็ได้ที่สามารถแสดงออกถึงความตั้งใจหรือความประสงค์ของผู้ลงลายมือชื่อหรือผู้ทำสัญลักษณ์ได้ แม้แต่ชื่อที่พิมพ์ท้ายจดหมายอิเล็กทรอนิกส์ (E-mail) ก็สามารถเป็นลายมือชื่อได้* ถ้าชื่อดังกล่าวถูกพิมพ์ด้วยความตั้งใจที่จะให้เป็นลายมือชื่อ แต่การยอมรับดังกล่าวก็เป็นเพียงการวินิจฉัยของศาลเท่านั้นยังขาดหลักเกณฑ์ที่แน่นอนและขาดตัวบทกฎหมายที่รองรับอย่างชัดเจน มลรัฐต่างๆ ในประเทศสหรัฐอเมริกาจึงได้มีการยอมรับและบัญญัติกฎหมายที่เกี่ยวข้องกับลายมือชื่อดิจิตอลออกมาบังคับใช้ เช่น มลรัฐยูทาร์ มลรัฐแคลิฟอร์เนีย เป็นต้น ซึ่งในปัจจุบันเกือบจะทุกมลรัฐในประเทศสหรัฐอเมริกาได้มีการบัญญัติกฎหมายที่เกี่ยวข้องกับลายมือชื่อดิจิตอลหรือลายมือชื่ออิเล็กทรอนิกส์ออกมาใช้บังคับภายในรัฐของตนแล้ว

ในส่วนของประเทศอื่นๆ ก็ได้มีการยอมรับและบัญญัติกฎหมายเกี่ยวกับลายมือชื่อดิจิตอลออกมาบังคับใช้ เช่น ประเทศแคนาดา เดนมาร์ก ฝรั่งเศส เยอรมัน ญี่ปุ่น เป็นต้น รวมทั้งประเทศในภูมิภาคอาเซียน คือ ประเทศมาเลเซีย ซึ่งได้นำ The Utah Digital Signature Act มาเป็นต้นแบบในการร่าง The Digital Signature Act 1997 โดยจัดทำกฎหมายดังกล่าวนี้ในโครงการ The Multimedia Super Corridor[16] รวมทั้งประเทศสิงค์โปร์ก็ได้มีการออกกฎหมายลายมือชื่อดิจิตอลแล้วเช่นกัน

ในส่วนของกฎหมายแม่แบบของคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ หมวดที่ 1 มาตรา 7 [17] ได้บัญญัติว่า

"มาตรา 7 ลายมือชื่อ

Matter of Save-On Carpet of Arizona, Inc., 545 F.2d 1239 (9th Cir. 1976) ซึ่งได้วินิจฉัยว่าลายมือชื่อที่เป็นตัวพิมพ์ในรายงานทางการเงินตาม U.C.C. ก็มีคุณสมบัติที่เพียงพอตามข้อกำหนดในเรื่องของลายมือชื่อใน Statute of Frauds แล้ว

15 Information Security Committee, Electronic Commerce Division, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce. Id., p.13

* โปรดดู BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE, (1994), p. 102

16 Nagavalli Annamalai, Cyber Laws of Malasia – The Multimedia Super Corridor, Journal of International Banking Law, Vol.12, Issue 12, Sweet & Maxwell, December 1997, p. 473

17 Draft Uniform Rules on the Legal Aspect of Electronic Interchange and Related Means of Data Communication, Article 7

(1) ในกรณีที่กฎหมายกำหนดให้ต้องมีลายมือชื่อบุคคล ให้ถือว่ากรณีที่เกี่ยวกับข้อมูลข่าวสารเป็นไปตามข้อกำหนดนั้นแล้วหาก

(ก) ได้ใช้วิธีการที่สามารถระบุถึงตัวบุคคลดังกล่าว และแสดงถึงการรับรองข้อมูลที่บรรจุอยู่ในข้อมูลข่าวสารของบุคคลนั้น และ

(ข) วิธีการดังกล่าวมีความน่าเชื่อถือ และเหมาะสมกับวัตถุประสงค์ของการสร้างหรือสื่อสารข้อมูลข่าวสารนั้น เมื่อคำนึงถึงพฤติการณ์แวดล้อมต่างๆ ซึ่งรวมทั้งสัญญาใดๆ ที่เกี่ยวข้อง

(2) ให้ใช้บทบัญญัติในวรรคแรก ไม่ว่าข้อกำหนดของกฎหมายจะอยู่ในรูปของหน้าที่ที่ต้องกระทำหรือว่ากฎหมายเพียงแต่บัญญัติถึงผลในกรณีที่ไม่มีการลงลายมือชื่อ

(3) บทบัญญัติในมาตรานี้ไม่ใช้บังคับในกรณีดังต่อไปนี้..."

ซึ่งแสดงถึงความพยายามที่จะทำให้ลายมือชื่อดิจิตอลหรือลายมือชื่ออิเล็กทรอนิกส์อื่นใดเป็นที่ยอมรับและเป็นที่แพร่หลายในการประกอบการพาณิชย์อิเล็กทรอนิกส์ และในปัจจุบันคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ ก็ได้มีกฎหมายแม่แบบในเรื่องลายมือชื่ออิเล็กทรอนิกส์ (Draft Uniform Rules on Electronic Signature) พร้อมทั้งคำแนะนำในการออกกฎหมายล่าสุดคือเอกสารเลขที่ A/CN.9/WG.IV/WP.88 โดยมีวัตถุประสงค์ให้ประเทศต่างๆ ที่จะทำการร่างกฎหมายลายมือชื่อดิจิตอลหรือลายมือชื่ออิเล็กทรอนิกส์ ได้ใช้เป็นแนวทางในการร่างกฎหมาย เพื่อให้กฎหมายของประเทศต่างๆ มีแนวทางเดียวกัน

3.2 กฎหมายเกี่ยวกับลายมือชื่อดิจิตอล

จากที่ประเทศต่างๆได้เล็งเห็นถึงความสำคัญของการหาเครื่องมือที่จะมาทดแทนการลงลายมือชื่อ (Hand-written Signature) ในกระดาษ และได้ทำการยอมรับรวมถึงบัญญัติกฎหมายที่เกี่ยวข้องกับการใช้ลายมือชื่อดิจิตอล หรือรู้จักกันในบริบทที่ว่า "กฎหมายลายมือชื่อดิจิตอล" ซึ่งมีหลักการที่สำคัญคือ

3.2.1 หลักการของกฎหมายเกี่ยวกับลายมือชื่อดิจิตอล

เนื่องด้วยความก้าวหน้าทางเทคโนโลยีและการติดต่อสื่อสาร ทำให้มีการประกอบธุรกรรมทางอิเล็กทรอนิกส์กันอย่างแพร่หลาย อีกทั้งลักษณะของการประกอบธุรกรรมทางอิเล็กทรอนิกส์นั้น ผู้ประกอบธุรกรรมไม่จำเป็นต้องมีความสัมพันธ์กันล่วงหน้าหรืออยู่ในที่เดียวกัน แต่สามารถอยู่ที่ใดก็ได้บนเครือข่ายอิเล็กทรอนิกส์ เมื่อเป็นสื่ออิเล็กทรอนิกส์ซึ่งเป็นสื่อที่มองไม่เห็นตัว หรือมีรูปร่างเหมือนเช่นสื่อกระดาษ จึงทำให้หลายคนขาดความเชื่อมั่นหรือไม่แน่ใจ แต่

ด้วยวิวัฒนาการทางเทคโนโลยี การกระทำธุรกรรมอิเล็กทรอนิกส์มีความจำเป็นและมีความสำคัญ ดังนั้นจึงจำเป็นต้องมีการตรากฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ (Electronic Data, Electronic Message, Electronic Document and Electronic Record) ให้เสมอกับการทำเป็นหนังสือหรือหลักฐานเป็นหนังสือตามที่กฎหมายกำหนด ทั้งยังจะต้องรับรองลายมือชื่ออิเล็กทรอนิกส์ที่ใช้กับนิติกรรมสัญญา หรือเอกสารต่างๆ ที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์เพื่อประโยชน์ในการระบุตัวและตรวจสอบตัวบุคคลผู้ส่ง สร้าง รับ หรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์ ดังนั้นการใช้ลายมือชื่ออิเล็กทรอนิกส์จึงเป็นการสร้างความเชื่อมั่นให้แก่ผู้ประกอบธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งอาจไม่มีความกันล่วงหน้าหรืออยู่ต่างที่กันในการประกอบธุรกรรมอิเล็กทรอนิกส์

สิ่งที่ทำให้หลายคนเป็นกังวลอยู่ที่ข้อมูลอิเล็กทรอนิกส์ได้รับการแก้ไขได้ง่าย และหากมีใครแอบแก้ไขก็จะหาร่องรอยได้ยาก การลงลายมือชื่อดิจิตอลเปรียบเทียบได้กับการลงลายมือชื่อ (Hand-written Signature) ลงในกระดาษเพื่อกำกับเอกสารต่างๆ ที่มีวัตถุประสงค์เพื่อรับรองข้อความในเอกสาร และระบุถึงที่มาของเอกสารนั้น เพื่อให้ลายมือชื่อดิจิตอลมีสถานะเดียวกับลายมือชื่อที่มีการรับรองตามประมวลกฎหมายแพ่งและพาณิชย์ จึงต้องมีการรับรองสถานะทางกฎหมายของลายมือชื่อดิจิตอลให้เสมอกับลายมือชื่อ (Hand-written Signature) ตามประมวลกฎหมายแพ่งและพาณิชย์ ด้วยเหตุนี้จึงต้องมีการวางหลักเกณฑ์และวิธีการที่เชื่อถือได้ในการสร้างลายมือชื่อดิจิตอลไว้ในกฎหมาย เพื่อเป็นกลไกในการสร้างความเชื่อมั่นต่อการประกอบธุรกรรมทางอิเล็กทรอนิกส์ โดยกฎหมายดังกล่าวคำนึงถึงหลักเกี่ยวกับการตรวจสอบความถูกต้องแท้จริงของบุคคลผู้ใช้ระบบ (Authentication of Users) การรักษาความถูกต้องของข้อมูล (Integrity) และ การห้ามปฏิเสธความรับผิด (Non-repudiation) รวมถึงคุณสมบัติของลายมือชื่อในทางกฎหมาย คือ การเป็นพยานหลักฐาน (Evidence) การเป็นระเบียบพิธี (Ceremony) การแสดงออกซึ่งความยอมรับหรือความเห็นชอบ (Approval) และการเป็นเครื่องมีที่ดีและมีประสิทธิภาพที่สุด (Efficiency and logistics) ตลอดจนในเรื่องของผู้ประกอบการรับรองและวางโครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะ ที่เป็นพื้นฐานในการใช้ลายมือชื่อดิจิตอลอีกด้วย

3.2.2 รูปแบบในการร่างกฎหมายลายมือชื่อดิจิตอล

กฎหมายเกี่ยวกับลายมือชื่อดิจิตอลในปัจจุบัน ทั้งที่มีการบังคับใช้ในประเทศต่างๆ แล้ว และที่อยู่ระหว่างการพิจารณายกร่างกฎหมายอยู่นั้น ก็มีแนวทางในการร่างกฎหมายหรือแนวทางในการใช้บังคับกฎหมายที่แตกต่างกัน บางประเทศก็กำหนดกฎเกณฑ์ให้ครอบคลุมแต่เพียงลายมือชื่ออิเล็กทรอนิกส์ เพื่อรองรับเทคโนโลยีในอนาคตและรักษาความเป็นกลางทางเทคโนโลยี (Technology Neutrality) แต่บางประเทศก็บัญญัติครอบคลุมแต่เพียงลายมือชื่อดิจิตอลที่มีความปลอดภัยสูงและมีการใช้กันแพร่หลายที่สุดในขณะนี้เท่านั้น ซึ่งเมื่อทำการศึกษาจากกฎหมายที่เกี่ยว

กับลายมือชื่อดิจิตอลของมลรัฐต่างๆ ในประเทศสหรัฐอเมริกาและประเทศต่างๆ จะพบว่าสามารถที่จะแยกแนวทางในการร่างกฎหมายหรือใช้บังคับกฎหมายเกี่ยวกับลายมือชื่อดิจิตอลดังนี้

3.2.2.1 รูปแบบที่เน้นรักษาความเป็นกลางทางเทคโนโลยี (technology-neutral approach)

การร่างกฎหมายแบบรักษาความเป็นกลางทางเทคโนโลยีนี้มีข้อดีคือ มีความยืดหยุ่น เนื่องจากเทคโนโลยีสารสนเทศนั้นมีการเปลี่ยนแปลงรวดเร็ว จึงไม่สามารถคาดเดาได้ว่าเทคโนโลยีใดจะเป็นเทคโนโลยีที่เหมาะสมในกฎหมาย ในบางกรณีเทคโนโลยีที่ใช้ในการร่างกฎหมายอาจจะล้าสมัยก่อนที่จะร่างกฎหมายเสร็จด้วยซ้ำ ยิ่งไปกว่านั้นการที่กฎหมายเฉพาะเจาะจงให้ใช้เทคโนโลยีใดเทคโนโลยีหนึ่งจะส่งผลให้เป็นการบิดเบือนสภาพและความต้องการของตลาด (Market-distorting) ได้ แนวการร่างกฎหมายแบบนี้สามารถแบ่งได้อีกสองรูปแบบคือ

3.2.2.1.1 รูปแบบที่รักษาความเป็นกลางทางเทคโนโลยี (Technology-Neutral Approach)

ในรูปแบบนี้กำหนดให้ลายมือชื่ออิเล็กทรอนิกส์มีคุณสมบัติครบตามที่กำหนดก่อนที่จะได้รับรองสถานะทางกฎหมาย ซึ่งข้อกำหนดดังกล่าวมาจากคำตัดสิน (Decision) ของ U.S. Comptroller General ซึ่งได้ถูกนำไปใช้ครั้งแรกในกฎหมายของมลรัฐ California ปลายปี 1995*

ภายในบทบัญญัติของกฎหมายที่ใช้รูปแบบดังกล่าวนี้ในการร่าง ลายมือชื่ออิเล็กทรอนิกส์จะได้รับการรับรองตามกฎหมายถ้า (1) เป็นเอกลักษณ์เฉพาะของผู้ใช้ลายมือชื่อ (Unique to the Person Using It) (2) สามารถตรวจสอบยืนยันความถูกต้อง (Capable of Verification) (3) ลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมในการใช้ของเจ้าของลายมือชื่อแต่เพียงผู้เดียว (Under the Sole Control of the Person Using It) (4) มีความเชื่อมโยงกับข้อมูลที่ทำการลงลายมือชื่อ (Linkage to the Data Signed) ในลักษณะที่หากข้อมูลดังกล่าวมีการเปลี่ยนแปลงแก้ไขแล้วลายมือชื่อจะไม่มีความถูกต้อง ในกฎหมายบางฉบับได้ขยายรูปแบบนี้โดยทำการรวมข้อกำหนดทั้งสี่ข้อนี้ในคำนิยามของคำว่าลายมือชื่ออิเล็กทรอนิกส์ (ในลักษณะที่ว่าจะสัญลักษณ์อิเล็กทรอนิกส์ใดๆ จะไม่ถือเป็นลายมือชื่ออิเล็กทรอนิกส์ ถ้าไม่มีคุณสมบัติครบตามสี่ข้อนี้) และกำหนดให้ลายมือชื่ออิเล็กทรอนิกส์เท่านั้นที่ได้รับการรับรองสถานะทางกฎหมาย ในบางกรณีการ

---

* โปรดดู U.S. Comptroller General, Matter of National Institute of Standards and Technology" Use of Electronic Data Interchange Technology to Create Valid Obligations, 71 Comp. Gen. 109 (1991); (Dec. 13, 1991); CAL. GOV'T. CODE §16.5 (West 1999).

ร่างกฎหมายในรูปแบบนี้จะมีการกำหนดคุณสมบัติของความปลอดภัยโดยเป็นเงื่อนไขเบื้องต้นของความสมบูรณ์ของลายมือชื่ออิเล็กทรอนิกส์ ประมาณหนึ่งในสามของมลรัฐในประเทศสหรัฐอเมริกาได้ใช้รูปแบบนี้ในการร่างกฎหมาย*

ข้อกำหนดทั้งสี่ได้กำหนดเงื่อนไขที่มิได้เป็นเงื่อนไขของลายมือชื่อธรรมดา (Hand-written Signature) ที่ลงบนเอกสารที่เป็นกระดาษ ข้อกำหนดแต่ละข้อมีรายละเอียด ดังนี้

(1) เป็นเอกลักษณ์เฉพาะของผู้ใช้ลายมือชื่อ (Unique to the Person Using It) ข้อกำหนดนี้กำหนดขึ้นเพื่อสนับสนุนข้อสันนิษฐานที่ว่าจะไม่มีบุคคลมากกว่าหนึ่งคนที่สามารถลงลายมือชื่ออิเล็กทรอนิกส์ที่เหมือนกันได้ เช่นเดียวกันกับข้อสันนิษฐานที่ว่าแต่ละคนย่อมมีวิธีการเฉพาะตัวในการลงลายมือชื่อ (Hand-written Signature) ของตนในกระดาษ ลายมือชื่ออิเล็กทรอนิกส์ที่ใช้เทคโนโลยี Biometrics เป็นพื้นฐาน เช่น การใช้ retinal scan หรือ Fingerprint ฯลฯ สามารถตอบสนองข้อกำหนดนี้ได้เป็นอย่างดี ในส่วนของลายมือชื่อดิจิตอลจะ

---

* Thomas J. Smedinghoff and Ruth Hill Bro, "Moving with Change: Electronic Signature Legislation as A Vehicle for Advancing E-COMMERCE", Id., footnote 62, p.738

"โปรดดู ALASKA STAT. § 09.25.510 (Michie 1999) นำไปใช้ได้กับการติดต่อสื่อสารทุกรูปแบบ.; CAL. GOV'T CODE § 16.5 ใช้ได้เฉพาะกับการติดต่อสื่อสารกับหน่วยงานของรัฐ.; GA. CODE ANN. § 10-12-4 (Michie 1998) นำไปใช้ได้กับการติดต่อสื่อสารทุกรูปแบบ.; IDAHO CODE § 67-2357 (1998) ใช้ได้เฉพาะการจัดหรือออกเอกสารที่ออกโดยหรือกับรัฐและหน่วยงานท้องถิ่น.; 15 ILL. COMP. STAT. 405/14.01 ใช้ได้เฉพาะกับการติดต่อสื่อสารระหว่างหน่วยงานของรัฐและที่ปรึกษาทางด้านการเงิน.; 205 ILL. COMP. STAT. 705/5 (West 1998) ใช้ได้เฉพาะกับการติดต่อสื่อสารระหว่างสถาบันการเงินกับลูกค้าของสถาบันการเงิน.; IOWA CODE ANN. § 1555A.27 (West 1999) (limiting application to prescriptions); KAN. STAT. ANN. § 60-2616 (1997) นำไปใช้ได้กับการติดต่อสื่อสารทุกรูปแบบ.; KY. REV. STAT. ANN. § 369.020 (Banks-Baldwin 1999) นำไปใช้ได้กับการติดต่อสื่อสารทุกรูปแบบ.; MD. CODE. ANN. STATE GOV'T § 8-504 (1998) ใช้ได้เฉพาะกับการติดต่อสื่อสารภายในหน่วยงานของรัฐ.; NEB. REV. STAT. § 86-1701 (1998) นำไปใช้ได้กับการติดต่อสื่อสารทุกรูปแบบ.; N.H. REV. STAT. ANN. § 294-D:4 (1999) ใช้ได้เฉพาะการติดต่อสื่อสารระหว่างภาครัฐกับหน่วยงานของรัฐหรือหน่วยงานที่เป็นตัวแทนของรัฐ.; N.C. GEN. STAT. § 66-58.1 (1999) ใช้ได้เฉพาะกับการจัดเอกสารของหน่วยงานมหาชน.; OKLA. STAT. ANN. TIT. 15 § 965 (West 1999) นำไปใช้ได้กับการติดต่อสื่อสารทุกรูปแบบ.; R.I. GEN. LAWS § 42-127-4 (1998) ใช้ได้เฉพาะกับธุรกรรมระหว่างหน่วยงานมหาชน."

เป็นไปตามข้อกำหนดนี้ถ้ามีมาตรฐานในการสร้างคู่กุญแจรหัสและความยาวของคู่กุญแจรหัสมีมากพอที่จะสามารถรักษาความปลอดภัยได้ อย่างไรก็ตามข้อกำหนดนี้มิได้ใช้ในกรณีของการลงลายมือชื่อในเอกสารที่เป็นกระดาษ เพราะฉะนั้นการพิมพ์ชื่อหรือการทำเครื่องหมาย X ด้านล่างของเอกสารที่เป็นกระดาษสามารถเป็นลายมือชื่อได้ตามกฎหมาย {U.C.C. § 1-201(39) ของประเทศสหรัฐอเมริกา} แต่กลับไม่เป็นลายมือชื่ออิเล็กทรอนิกส์ถ้าได้ทำลงในเอกสารอิเล็กทรอนิกส์ภายใต้ข้อกำหนดนี้

(2) สามารถตรวจสอบยืนยันความถูกต้อง (Capable of Verification) ข้อกำหนดนี้มิได้หมายความว่าตัวของลายมือชื่ออิเล็กทรอนิกส์เอง จะต้องมีชื่อของผู้ลงลายมือชื่อปรากฏอยู่ แต่เป็นการมุ่งหมายถึงความสามารถที่จะตรวจสอบตัวบุคคลผู้ทำการลงลายมือชื่อได้ อย่างไรก็ตามการตรวจสอบโดยใช้ข้อมูลที่อ้างอิงจากแหล่งอื่นก็ถือว่าเป็นไปตามข้อกำหนดนี้ได้ เช่น ภายใต้ข้อกำหนดของ the California Digital Signature ลายมือชื่อดิจิตอลก็สามารถที่จะตรวจสอบได้ถ้าผู้รับเอกสารที่ลงลายมือชื่อดิจิตอลสามารถที่จะตรวจสอบลายมือชื่อดังกล่าวได้ โดยการใช้กุญแจรหัสสาธารณะของผู้ลงลายมือชื่อ เป็นต้น {*See* CAL. GOV'T CODE § 22003 (West 1999)}

(3) ลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมในการใช้ของเจ้าของลายมือชื่อแต่เพียงผู้เดียว (Under the Sole Control of the Person Using It) ภายใต้ข้อกำหนดของ the California Digital Signature กำหนดว่าลายมือชื่อดิจิตอลอยู่ภายใต้การควบคุมในการใช้ของเจ้าของลายมือชื่อแต่เพียงผู้เดียว เมื่อบุคคลผู้ถือกุญแจรหัสส่วนตัวได้ทำหน้าที่ในการรักษากุญแจรหัสส่วนตัวอย่างมีเหตุผลและป้องกันที่จะไม่ให้กุญแจรหัสส่วนตัวถูกเปิดเผย[18] ซึ่งข้อกำหนดนี้ไม่ชัดเจนในกรณีที่ผู้อื่นได้รับอำนาจในการลงลายมือชื่อ เช่น ในกรณีของการใช้กุญแจรหัสส่วนตัวของผู้อื่นในการลงลายมือชื่อในเอกสารโดยได้รับอำนาจอย่างถูกต้อง เป็นต้น ว่าจะสามารถเป็นไปตามข้อกำหนดนี้หรือไม่

(4) มีความเชื่อมโยงกับข้อมูลที่ทำการลงลายมือชื่อ (Linkage to the Data Signed) ข้อกำหนดสุดท้ายนี้กำหนดให้ลายมือชื่ออิเล็กทรอนิกส์ต้องมีความเกี่ยวพันกับข้อความที่ทำการลงลายมือชื่อในลักษณะที่ว่า ถ้าข้อความที่ทำการลงลายมือชื่อถูกเปลี่ยนแปลงแก้ไขภายหลังการลงลายมือชื่อ ผู้ที่ได้รับเอกสารดังกล่าวจะต้องสามารถรู้ได้ว่าข้อความที่ตนได้รับถูกเปลี่ยนแปลงแก้ไข ข้อกำหนดนี้มีความสำคัญมาสำหรับลายมือชื่อที่มีความปลอดภัย เพราะสัญลักษณ์ทางอิเล็กทรอนิกส์อื่นๆ สามารถที่จะสร้างขึ้นหรือทำการคัดลอกให้เหมือนได้* อย่างไรก็

---

[18] CAL. GOV'T CODE § 22003

* โปรดดู Food and Drug Administration Regulations on Electronic Records and Electronic Signatures, 21 C.F.R. § 11.70 (1999), ซึ่งกำหนดว่า "ลายมือชื่ออิเล็กทรอนิกส์...จะต้อง

ตามจึงเกิดคำถามที่ว่าข้อกำหนดนี้ควรที่จะใช้กับลายมือชื่ออิเล็กทรอนิกส์ทุกประเภทหรือไม่ และควรนำไปใช้กับลายมือชื่อที่ลงในกระดาษหรือไม่

The Draft European Directive ก็ได้ยึดแนวทางดังกล่าวนี้[19] อย่างไรก็ตามความหมายของข้อกำหนดเบื้องต้น ทั้ง 4 ประการข้างต้นยังไม่ชัดเจนนัก และในบางกรณีข้อกำหนดในบางข้อยังสร้างผลกระทบที่สำคัญและอุปสรรคที่ไม่จำเป็นขึ้น[20]

3.2.2.1.2 รูปแบบที่รักษาความเป็นกลางทางเทคโนโลยี และเพิ่มเติมข้อสันนิษฐาน (Technology-Neutral Plus Approach)

จากการที่ Uniform Commercial Code (U.C.C.) ได้นิยามลายมือชื่อว่า คือสัญลักษณ์ที่ทำขึ้นด้วยเพื่อใช้ในการตรวจสอบความถูกต้องแท้จริง (any symbol made with an intent to authenticate)[21] มลรัฐหลายๆ แห่งในประเทศสหรัฐอเมริกาจึงได้บัญญัติกฎหมายลายมือชื่ออิเล็กทรอนิกส์ในแนวทางเดียวกัน โดยให้คำนิยามของลายมือชื่ออิเล็กทรอนิกส์ว่า "สัญลักษณ์ในทางอิเล็กทรอนิกส์ใดๆ ที่อยู่บนข้อความหรือข้อมูลมีคุณสมบัติใช้แทนลายมือชื่อได้" (any form of electronic symbol on a message can qualify as signature) อย่างเช่น มลรัฐ Illinois ซึ่งได้ให้คำนิยามไว้ใน The Ellinois Electronic Commerce Security Act ว่า "สัญลักษณ์ใดๆ หรือวิธีการรักษาความปลอดภัยใดๆ ที่ถูกใช้หรือนำมาใช้ไม่ว่าจะเป็นการใช้วิธีการในทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดก็ตามที่ใช้หรือถูกใช้ในนามของบุคคลโดยตั้งใจใช้ยืนยันความถูกต้องแท้จริงของข้อมูล"* เป็นต้น มลรัฐเหล่านี้ได้ยึดถือแนวทางในความเป็นกลางทางเทคโนโลยี (technology-

---

เชื่อมโยงกับข้อมูลอิเล็กทรอนิกส์เพื่อเป็นประกันว่าลายมือชื่อดังกล่าวไม่สามารถที่จะตัดทอน ทำซ้ำ หรือการเปลี่ยนแปลงในทำนองเดียวกันเพื่อบิดเบือนข้อมูลอิเล็กทรอนิกส์"

[19] โปรดดู European Commission, Proposal for European Parliament and Council Directive on a Common Framework for Electronic Signatures, (May 13, 1998) <http://www.ispo.cec.be/eif/policy/com98297.html> "อย่างไรก็ตามร่างข้อกำหนดของ European ไม่ได้กำหนดให้ต้องเป็นไปตามองค์ประกอบเหล่านี้จึงจะถือเป็นลายมือชื่อที่มีผลทางกฎหมาย."

[20] Thomas J. Smedinghoff and Ruth Hill Bro, "Moving with Change: Electronic Signature Legislation as A Vehicle for Advancing E-COMMERCE", Id., p. 739

[21] U.C.C. _ 201(39) (1999) (emphasis added).

* Thomas J. Smedinghoff and Ruth Hill Bro, "Moving with Change: Electronic Signature Legislation as A Vehicle for Advancing E-COMMERCE", Id., footnote 59, p.737

"โปรดดู ARIZ. REV. STAT. ANN. _ 41-132(D)(4) (West 1998) (defining electronic signature an "electronic or digital method of identification that is executed or adopted by a person with the intent to be bound by or to authenticate a record" 47-56); FLA STAT ANN _ 282.72(4) (West 1998) ("Electronic signature means any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing."); 5 ILL. COMP. STAT. 175/5-105 (effective July 1, 1999) ("[A]ny symbol executed or adopted, or any security procedure employed or adopted, using electronic means or otherwise, by or on behalf of a person with intent to authenticate a record."); IND. CODE ANN. _ 5-24-2-2 (West 1998) ("[A]n electronic identifier, created by computer, executed or adopted by the party using it with the intent to authenticate a writing."); MISS. CODE ANN. _ 25-63-1 (1998) ("[A]ny word, group of letters, name, including a trader-assumed name, mark, characters or symbols made manually, by device, by machine, or manifested by electronic or similar means, executed or adopted by a party with the intent to authenticate a writing."); N.H. REV. STAT. ANN. _ 506:8 (1999) ("Electronic signature means a digital signature, executed or adopted by a party with an intent to authenticate a writing."); OHIO REV. CODE ANN. _ 3701.75 ("[A]ny of the following attached to or associated with an electronic record by an individual to authenticate the record: (a) a code consisting of a combination of letters, numbers, characters, or symbols that is adopted or executed by an individual as that individual's electronic signature; (b) a computer-generated signature code created for an individual; (c) an electronic image of an individual's handwritten signature created by using a pen computer."); OR. REV. STAT. _ 192.835 (1998) ("[A]ny letters, characters or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing."); S.C. CODE ANN. _ 26-5-330 (Law. Co-op 1998) ("[A]ny identifier or authentication technique attached to or logically associated with an electronic record that is intended by the party using it to have the same force and effect as a manual signature."); TEX. BUS. & COM. CODE ANN. _ 2.108 (West 1998) ("[A]n electronic identifier, created by a computer, intended by the party using it to have the same force and effect as the use of a manual signature."); VA. CODE ANN. __ 59.1-467, 59.1-468, 59.1-469 (Michie 1998) ("[A]n electronic identifier, created by a computer, intended by the party using it to have the same force and effect as the use of a manual signature."); W. VA. CODE _ 39-5-2(e) (1998) ("[A]ny identifier or authentication technique attached to or logically associated with an electronic record that is intended by the person using it to have the same force and effect as a

neutral approach) โดยไม่บัญญัติให้ใช้ลายมือชื่ออิเล็กทรอนิกส์แบบใดแบบหนึ่งโดยเฉพาะ คำนึงถึงแต่คุณสมบัติที่ได้จากการลงลายมือชื่ออิเล็กทรอนิกส์เหล่านั้น ข้อกำหนดที่สำคัญมีเพียงข้อเดียว คือการคงอยู่ของสัญลักษณ์หรือวิธีการที่ปลอดภัยและความตั้งใจที่จะให้สัญลักษณ์หรือวิธีการที่ปลอดภัยดังกล่าวเป็นเครื่องมือตรวจสอบความถูกต้องแท้จริงของผู้ลงลายมือชื่อ (Signer) ได้ ซึ่ง Uniform Electronic Transactions Act ของประเทศสหรัฐอเมริกาก็ใช้แนวทางนี้[22]

การร่างกฎหมายแนวนี้จะให้สถานะและผลทางทางกฎหมายต่อลายมือชื่ออิเล็กทรอนิกส์ทุกประเภท (รวมถึงลายมือชื่อดิจิตอลด้วย) โดยให้อำนาจศาลหรือผู้พิพากษาเป็นผู้ตัดสินใจในการให้น้ำหนักของพยานหลักฐาน โดยให้พิจารณาจากระบบของลายมือชื่ออิเล็กทรอนิกส์ที่นำมาใช้เป็นรายกรณีไป[23] เช่น The Ellinois Electronic Commerce Security Act ได้สร้างระดับชั้นของลายมือชื่อที่มีความน่าเชื่อถือ เรียกว่า "Secure electronic signature"* โดยเพิ่มเติมข้อกำหนดที่แน่นอนเกี่ยวกับคุณสมบัติของลายมือชื่อ** แนวความคิดในเรื่องของ "Secure electronic record" และ "Secure electronic signature" ถูกยกขึ้นครั้งแรก เมื่อวันที่ 14 ตุลาคม 1997 โดยปรากฏในร่าง "Illinois Electronic Commerce Security Act" ซึ่งถูกนำมาเผยแพร่เพื่อการประชา

---

manual signature."); WIS. STAT. ANN. _ 137.04(2) (West 1999) ("[A]ny combination of words, letters, symbols or characters that is attached to or logically associated with an electronic record and used by a person for the purpose of authenticating a document that has been created in or transformed into an electronic format.")."

[22] See Uniform Electronic Transaction Act, _ 102(8) (May 10, 1999 Interim Draft), <http://www.law.upenn.edu/library/ulc/ulc.htm#ueccta >

[23] W. Everett Lupton, "The Digital Signature: Your Identity by the Numbers", The Richmond Journal of Law & Technology, Vol. VI, Issue 2, Fall 1999, http://www.richmond.edu/jolt/v6i2/note2.html (Visited 20/12/2543)

* Thomas J. Smedinghoff and Ruth Hill Bro, "Moving with Change: Electronic Signature Legislation as A Vehicle for Advancing E-COMMERCE", Id , footnote 84, p.747

"5 ILL. COMP. STAT. 175/10-110 (effective July 1, 1999). พระราชบัญญัตินี้ให้คำนิยามของระดับชั้นความปลอดภัยของข้อมูลอิเล็กทรอนิกส์เช่นเดียวกัน."

** Ibid., footnote 85, p.737

"โปรดดู 5 ILL. COMP. STAT. 175/10-110(a). "ลายมือชื่ออิเล็กทรอนิกส์จะต้อง (1) สร้างขึ้นโดยวิธีการที่สมเหตุสมผลในทางการค้าภายใต้พฤติการณ์ที่เกิดขึ้น (2) ประยุกต์ใช้โดยฝ่ายที่เกี่ยวข้องเพื่อทำการตรวจสอบลายมือชื่อโดยวิธีการที่เชื่อถือได้ และ (3) ฝ่ายที่เกี่ยวข้องเข้าทำการเกี่ยวข้องกับลายมือชื่อโดยสุจริตและมีเหตุผล."

พิจารณ์โดย "The Illinois Commission on Electronic Commerce and Crime" แนวความคิดนี้ได้ถูกบรรจุในร่างสุดท้ายของ "The Illinois Electronic Commerce Security Act" เช่นเดียวกันกับการที่ได้บรรจุไว้ในกฎหมายของมลรัฐเซาท์ดาร์โกต้าและประเทศสิงค์โปร์ และยังได้ถูกใช้ในร่างกฎหมายแม่แบบของ UNCITRAL ซึ่งต่อมาภายหลักเปลี่ยนชื่อเป็น "enhanced electronic signature" [24]

ลายมือชื่ออิเล็กทรอนิกส์จะเป็น Secure electronic signature ก็ต่อเมื่อผู้เป็นฝ่ายในธุรกรรมได้ตกลงกันที่จะใช้วิธีการดังกล่าว หรือถ้าใช้เทคโนโลยีที่กำหนดไว้ได้รับการยอมรับจาก Secretary of State ในการสร้างลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวขึ้น ในเรื่องของความเชื่อถือได้ (trustworthy) ลายมือชื่ออิเล็กทรอนิกส์ต้อง[25]

- วิธีการลงลายมือชื่อต้องมีลักษณะเป็นการเฉพาะตัวสำหรับผู้ลงลายมือชื่อ (is unique to the signer within the context in which it is used)
- สามารถใช้ระบุตัวบุคคลผู้ทำการลงลายมือชื่อ (can be used to objectively identify the person signing the electronic record)
- ต้องเชื่อถือได้ว่าลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวถูกสร้างหรือทำการลงลายมือชื่อโดยบุคคลที่ถูกระบุว่าเป็นผู้ลงลายมือชื่อ (was reliably created by such identified person)*
- เมื่อลงลายมือชื่อแล้วจะกลายเป็นส่วนหนึ่งของข้อมูลที่ลงลายมือชื่อ ในลักษณะที่ว่าถ้ามีการเปลี่ยนแปลงแก้ไขข้อ

---

[24] Thomas J. Smedinghoff and Ruth Hill Bro, "Moving with Change: Electronic Signature Legislation as A Vehicle for Advancing E-COMMERCE", Id., footnote 89, p.748

"โปรดดู 5 ILL. COMP. STAT. 175; S.C. CODE § 26-5-330 (Law Co-op 1998); UNCITRAL, Draft Articles on Electronic Signatures (December 15, 1998) http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-80.htm; CCA, Singapore Electronic Transactions Act 1998, § 18(2)(b), http:// www.cca.gov.sg/eta/framecontent.htm"

[25] Thomas J. Smedinghoff and Ruth Hill Bro, Id., p.747

* ลายมือชื่ออิเล็กทรอนิกส์จะเชื่อถือได้ว่าได้สร้างโดยบุคคลเฉพาะเจาะจง ถ้าส่วนหนึ่งของวิธีการลงลายมือชื่อหรือเครื่องมือที่ใช้ในการลงลายมือชื่อหรืออย่างอื่นที่มีลักษณะทำนองเดียวกันอยู่ภายใต้การควบคุมของผู้ที่เป็นเจ้าของลายมือชื่อ (sole control of such person)

มูลภายหลังการลงลายมือชื่อไม่ว่าโดยตั้งใจหรือไม่ จะทำให้ลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวไม่สมบูรณ์ (is creates and is linked to the electronic record to which it relates in manner such that if the record or the signature is intentionally or unintentionally changes after signing the electronic signature is invalidated)

ลายมือชื่ออิเล็กทรอนิกส์ที่เป็น Secure electronic signature จะได้รับข้อสันนิษฐานตามกฎหมายว่าลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวเป็นลายมือชื่อที่แท้จริงของผู้ที่ถูกระบุว่าเป็นเจ้าของลายมือชื่อ ข้อสันนิษฐานเดียวกันนี้ปรากฏในกฎหมายของมลรัฐ South Carolina และ กฎหมายของประเทศ Singapore

ข้อกำหนดสี่ประการนี้คล้ายกับข้อกำหนดทั้งสี่ประการในข้อ 3.2.2.1.1 ที่ได้กล่าวถึงข้างต้น แต่มีข้อแตกต่างที่สำคัญอยู่ 2 ประการคือ ประการแรกคุณสมบัติของลายมือชื่ออิเล็กทรอนิกส์ที่เป็นไปตามข้อกำหนดสี่ประการนี้มิใช่ข้อกำหนดเบื้องต้นในการได้รับการรับรองสถานะลายมือชื่อตามกฎหมาย แต่เป็นเงื่อนไขเบื้องต้นที่จะได้รับสถานะเป็น Secure electronic signature ซึ่งจะได้รับประโยชน์จากข้อสันนิษฐานตามกฎหมายเพิ่มเติมจากการยอมรับว่ามีสถานะเป็นลายมือชื่อตามกฎหมาย ประการสุดท้ายคือความแตกต่างในตัวข้อกำหนดทั้งสี่เอง คือในส่วนของข้อกำหนดที่หนึ่งนั้นลายมือชื่ออิเล็กทรอนิกส์แค่มีความสัมพันธ์กับลักษณะเป็นการเฉพาะตัวสำหรับผู้ลงลายมือชื่อ มิใช่เป็นการเฉพาะตัวอย่างเด็ดขาดเหมือนในข้อกำหนดในข้อ 3.2.2.1.1 ข้อกำหนดที่สองจับประเด็นไปยังวัตถุประสงค์ในการระบุตัวบุคคล มากกว่าความสามารถในการตรวจสอบความสมบูรณ์ของลายมือชื่อ ในส่วนข้อกำหนดที่สามจะเป็นการปฏิเสธข้อกำหนดในเรื่อง "Sole Control" แต่จับประเด็นไปยังการสร้างความมั่นใจว่าผู้ที่ถูกระบุว่าเป็นผู้ลงลายมือชื่อเป็นผู้ที่ทำการลงลายมือชื่อจริง

3.2.2.2 รูปแบบโครงสร้างของระบบกุญแจรหัสสาธารณะ (Public Key Infrastructure)

รูปแบบในการร่างกฎหมายแบบนี้ เป็นการร่างโดยเน้นใช้เทคโนโลยีลายมือชื่อดิจิตอลโดยเฉพาะ หรือเรียกอีกอย่างว่ารูปแบบการร่างแบบเน้นใช้เทคโนโลยีเฉพาะ (Technology-specific Approach) ยกตัวอย่างเช่น The Utah Digital Signature Act ("Utah Act") ซึ่งเป็นกฎหมายลายมือชื่อดิจิตอลฉบับแรก Utah Act ได้สร้างหน้าที่พิเศษขึ้นสำหรับผู้ประกอบการรับรอง (Certification Authority) และผู้ถือใบรับรอง (Subscriber)[26] วิธีการในการอนุญาตและออกข้อ

---

[26] โปรดดู UTAH CODE ANN. Sections 46-3-301 to 46-3-309. (1998)

กำหนดของผู้ประกอบการรับรอง (Certification Authority)[27] ข้อสันนิษฐานทางกฎหมายของฝ่ายต่างๆ [28] และในเรื่องความสมบูรณ์ของเอกสารที่ลงลายมือชื่อดิจิตอล[29] บทบัญญัติหลายๆ มาตราของ Utah Act ได้รับการยอมรับโดย American Bar Associate (ABA) นำมาใช้ใน Digital Signature Guideline

แนวทางที่เป็นมาตรฐานของการร่างกฎหมายรูปแบบนี้ก็คือ กฎหมายของมลรัฐยูทาร์ ซึ่งจะแบ่งออกเป็นสี่ส่วนด้วยกันคือ หนึ่งการอนุญาตให้ประกอบการออกใบรับรอง สองการออก การระงับ และการเพิกถอนใบรับรองที่ออกโดยผู้ประกอบการรับรอง สามหน้าที่การประกันคุณภาพและหน้าที่ของผู้ประกอบการรับรองที่ได้รับอนุญาต และสี่กฎเกณฑ์ที่เกี่ยวกับการรับรองและความสมบูรณ์ของลายมือชื่อดิจิตอล [30] มลรัฐที่ออกกฎหมายในแนวทางนี้มีอยู่ 5 มลรัฐ คือ[31] Minnesota Missouri New Hampshire Utah และ Washington* โดยที่กฎหมายที่ใช้รูปแบบนี้ในการร่างจะอยู่บนข้อสันนิษฐานที่เห็นได้อย่างชัดเจนว่า ใบรับรองที่ออกโดยผู้ประกอบการรับรองที่ได้รับอนุญาตนั้นเชื่อถือได้ และลายมือชื่อดิจิตอลที่สร้างโดยใช้กุญแจรหัสส่วนตัวที่มีความเกี่ยวพันกับกุญแจรหัสสาธารณะที่ปรากฏในใบรับรองคือลายมือชื่อที่เชื่อถือได้ ซึ่งเป็นการที่กฎหมายได้มอบคุณสมบัติของความน่าเชื่อถือให้แก่ข้อมูลที่ได้ทำการตรวจสอบโดยใบรับรองที่ออกโดยผู้ประกอบการรับรองที่ได้รับอนุญาต**

---

27 โปรดดู Ibid., Sections 46-3-201 to 46-3-204.

28 โปรดดู Ibid., Section 46-3-401.

29 โปรดดู Ibid., Section 46-3-402.

30 กฤษณะ ช่างกล่อม, (ร่าง) รายงานการศึกษาวิจัยเรื่องกฎหมายลายมือชื่อดิจิตอล เรื่องเดิม, หน้า 90

31 Thomas J. Smedinghoff and Ruth Hill Bro, "Moving with Change: Electronic Signature Legislation as A Vehicle for Advancing E-COMMERCE", Id., p. 740

* Ibid., footnote 66, p.740

"MINN. STAT. ANN. § 325K.20 (West 1998); MO ANN. STAT. § 28.657 (West 1999); N.H. REV. STAT. ANN. § 294-D:4 (1999); UTAH CODE ANN. § 46-3-101 (1998); WASH. REV. CODE ANN. § 19.34.900 (West 1998) กฎหมายของมลรัฐเหล่านี้มิได้ห้ามหรือทำให้ไม่สามาใช้บังคับได้สำหรับการใช้ลายมือชื่ออิเล็กทรอนิกส์แบบอื่นๆ โดยปล่อยประเด็นนี้ไว้. และโปรดดูตัวอย่างใน UTAH CODE ANN. § 46-3-101 (1998) ไม่มีส่วนใดในบทนี้ที่มิให้เครื่องหมายอื่นใดมีสถานะเช่นเดียวกันกับลายอชื่อภายใต้กฎหมายอื่นที่ใช้บังคับอยู่ เช่น Utah Uniform Commercial Code Section 70A-1-201(39)."

** Ibid., footnote 94, p.749

3.2.3 ประเภทของธุรกรรมที่กฎหมายยอมรับให้ใช้ลายมือชื่อดิจิตอล

ในการร่างกฎหมายลายมือชื่อดิจิตอลหรือลายมือชื่ออิเล็กทรอนิกส์นั้น มักจะมีคำถามอยู่เสมอว่า การที่จะยอมรับให้ใช้ลายมือชื่อดิจิตอลและ/หรือลายมือชื่ออิเล็กทรอนิกส์ในการประกอบธุรกรรมอิเล็กทรอนิกส์นั้น ควรที่จะกำหนดหรือไม่ว่าธุรกรรมประเภทใดบ้างที่อนุญาตให้มีการใช้ลายมือชื่อดิจิตอลและ/หรือลายมือชื่ออิเล็กทรอนิกส์ ในต่างประเทศโดยเฉพาะประเทศสหรัฐอเมริกา ประมาณ 40 เปอร์เซ็นต์ของรัฐที่ทำการออกกฎหมายเกี่ยวกับลายมือชื่อดิจิตอลและ/หรือลายมือชื่ออิเล็กทรอนิกส์ ได้ยอมรับให้มีการใช้ลายมือชื่อดิจิตอลและ/หรือลายมือชื่ออิเล็กทรอนิกส์กับธุรกรรมอิเล็กทรอนิกส์ทุกประเภท* ในขณะรัฐอื่นๆ อนุญาตให้ใช้ลายมือชื่อดิจิตอลและ/หรือลายมือชื่ออิเล็กทรอนิกส์เฉพาะในธุรกรรมบางกลุ่มเท่านั้น เช่น ธุรกรรมที่ Uniform Commercial Code กำหนดให้ต้องมีการลงลายมือชื่อ รายการบันทึกทางการแพทย์ หรือ

"โปรดดูตัวอย่างใน UTAH CODE ANN. § 406(3). "The Utah Digital Signature Act บัญญัติว่า ถ้าลายมือชื่อดิจิตอลได้ถูกตรวจสอบโดยกุญแจรหัสสาธารณะที่แสดงอยู่ในใบรับรองที่ถูกต้องและใบรับรองดังกล่าวออกโดยองค์กรผู้ออกใบรับรองที่ได้รับอนุญาตแล้ว ศาลของมลรัฐ Utah จะสันนิษฐานว่า (a) ลายมือชื่อดิจิตอลคือลายมือชื่อของผู้ถือใบรับรองที่ปรากฏชื่อในใบรับรอง และ (b) การลงลายมือชื่อดิจิตอลดังกล่าวได้กระทำโดยมีเจตนาที่จะลงลายมือชื่อในข้อความดังกล่าว."

* Ibid., footnote 68, p.741

"สำหรับกฎหมายลายมือชื่ออิเล็กทรอนิกส์ของมลรัฐต่างๆ ที่อนุญาตให้ใช้ลายมือชื่ออิเล็กทรอนิกส์กับธุรกรรมทุกรูปแบบมีดังนี้: ALASKA STAT. § 09.25.510 (Michie 1999); FLA. STAT. ANN. § 282.72 (West 1998); GA. CODE ANN. § 10-12-4 (Michie 1998); 5 ILL. COMP. STAT. 175/5-105 (effective July 1, 1999); KAN. STAT. ANN. §60-2616 (1997); KY. REV. STATUS. ANN. §369.020 (Banks-Baldwin 1999); MINN. STAT. ANN. § 325K.20 (West 1998) ใช้ได้เฉพาะลายมือชื่อดิจิตอลเท่านั้น.; MISS. CODE ANN. § 25-63-1 (1998); MO. ANN. STAT. § 28.657 (West 1999) ใช้ได้เฉพาะลายมือชื่อดิจิตอลเท่านั้น.; NEB. REV. STAT. § 86-1701 (1998); N.H. REV. STAT. ANN. § 294 D:4 (1999); OKLA. STAT. ANN. tit. 15 § 965 (West 1999); OR. REV. STAT. § 192.835 (1998); S.C. CODE ANN. § 26-5-330 (Law. Co-op 1998); UTAH CODE ANN. § 46-3-101 (1998) ใช้ได้เฉพาะลายมือชื่อดิจิตอลเท่านั้น.; VA. CODE ANN. §§ 59.1-467, 59.1-468, 59.1-469 (Michie 1998); WASH. REV. CODE ANN. § 19/34/900 (West 1998) ใช้ได้เฉพาะลายมือชื่อดิจิตอลเท่านั้น.; W.VA. CODE § 39-5-2 (1999); WIS. STAT. ANN. § 137.04(2) (West 1999). กฎหมายในบางรัฐมิได้มีข้อจำกัดสำหรับข้อยกเว้น เช่น ในเรื่องของเจตนา. โปรดดูตัวอย่างใน 5 ILL. COMP. STAT. 175/5-120 (effective July 1, 1999)."

รายการบันทึกของรถยนต์ประเภทต่างๆ เป็นต้น* ในบางรัฐมีเงื่อนไขในการอนุญาตใช้ โดยขึ้นอยู่กับผู้เป็นฝ่าย (Party) ที่เกี่ยวข้องในธุรกรรม ยกตัวอย่างเช่นอนุญาตให้เฉพาะในกรณีที่ทั้งสองฝ่ายเป็นองค์กรของรัฐ** ในขณะที่บางรัฐกำหนดแค่ให้ต้องมีอย่างน้อยหนึ่งฝ่ายที่เป็นองค์กรของรัฐ*** หรือให้ใช้เฉพาะธุรกรรมที่เกี่ยวข้องกับภาคธุรกิจเฉพาะด้านเท่านั้น เช่น สถาบันการเงิน เป็นต้น†

---

* Ibid., footnote 69, p.740

กฎหมายลายมือชื่ออิเล็กทรอนิกส์ของรัฐเหล่านี้เกี่ยวข้องกับธุรกรรมเฉพาะประเภท. โปรดดูตัวอย่างใน ALA. CODE § 40-30-5 (1998) ใช้ได้กับการแจ้งขอคืนภาษีและเอกสารอื่นที่เกี่ยวข้องกับ Department of Revenue.; COLO. REV. STAT. ANN. § 4-9-413 (West 1999) ใช้ได้กับระบบการจดแจ้งเอกสารทางอิเล็กทรอนิกส์ของหนังสือแสดงฐานะทางการเงินตาม U.C.C.; CONN. GEN. STAT. ANN. § 42a-9-402 (West 1999) ใช้ได้เฉพาะบันทึกทางการแพทย์ที่จัดเก็บในโรงพยาบาล.; DEL. CODE ANN. tit. 29 § 2706(a), 5942(a) (1998) ใช้ได้เฉพาะกับเอกสารบางอย่างที่เกี่ยวข้องกับงบประมาณ บัญชี และการเงิน.; HAW. REV. STAT. ANN. § 231-8.5 ใช้ได้กับการจดแจ้งเอกสารอิเล็กทรอนิกส์ของศาล; IOWA CODE ANN. § 48A.13 .ใช้ได้กับการลงทะเบียนเพื่อขอสิทธิเลือกตั้ง.; IOWA CODE ANN. § 155A.27 (West 1999) ใช้ได้กับใบสั่งยาของแพทย์.; LA. REV. STAT. ANN. § 2144 (West 1999) ใช้ได้กับบันทึกทางการแพทย์.; ME. REV. STAT. ANN. tit. 29-A, § 1401 (West 1998) ใช้ได้ภายใต้ The Motor Vehicle Code.; OHIO REV. CODE ANN. § 3701.75 (West 1999) ใช้ได้กับบันทึกการตรวจสุขภาพที่ได้รับอนุญาต.; การใช้ลายมือชื่ออิเล็กทรอนิกส์กับธุรกรรมประเภทอื่นๆ มีสถานะที่ไม่ชัดเจนเพราะมิได้มีการกล่าวถึงไว้ในกฎหมาย.

** Ibid., footnote 70, p.740

"ในบางรัฐจำกัดการใช้ลายมือชื่ออิเล็กทรอนิกส์สำหรับธุรกรรมกับหน่วยงานภาครัฐเท่านั้น. โปรดดู ARIZ. REV. STAT. ANN. § 41-132 ใช้ได้เฉพาะกับหน่วยงานของรัฐ และสำหรับการจดแจ้งเอกสารกับ Secretary of State.; DEL. CODE ANN. tit. 29 § 2706(a), 5942(a) (1998) ใช้ได้เฉพาะกับเอกสารบางอย่างที่เกี่ยวข้องกับงบประมาณ บัญชี และการเงิน.; KY. REV. STAT. ANN. § 369.020 (Banks-Baldwin 1999) ใช้ได้เฉพาะหน่วยงานของรัฐในเรื่องของสัญญาก่อสร้าง.; MD. CODE ANN. STATE GOV'T § 8-504 (1998) ใช้ได้เฉพาะการติดต่อสื่อสารภายในหน่วยงานของรัฐ.; N.H. REV STAT. ANN. § 294-D:4 (1999) ใช้ได้เฉพาะการติดต่อสื่อสารภายในหน่วยงานของรัฐ.; R.I GEN. LAWS § 42-27-4 (1998) ใช้ได้เฉพาะการติดต่อสื่อสารภายในหน่วยงานของรัฐ."

*** Ibid., footnote 71, p.741

อย่างไรก็ตาม ทางผู้เขียนมีความเห็นว่า ในระยะแรก ควรมีการกำหนดประเภทของธุรกรรมที่อนุญาตให้มีการใช้ลายมือชื่อดิจิตอลและ/หรือลายมือชื่ออิเล็กทรอนิกส์แทนการลงลายมือชื่อธรรมดา (Hand-written Signature) ได้ เพื่อทำการศึกษาถึงความเหมาะสมและผลกระทบที่เกิดขึ้นจากการใช้ลายมือชื่อดิจิตอลและ/หรือลายมือชื่ออิเล็กทรอนิกส์ และเพื่อเป็นการจำกัดขนาดของผลกระทบหรือความเสียหายที่จะเกิดขึ้นถ้ามี จากนั้นทำการปรับปรุงแก้ไขกฎหมายที่เกี่ยวข้อง และกฎหมายลายมือชื่อดิจิตอลและ/หรือลายมือชื่ออิเล็กทรอนิกส์ให้เหมาะสมกับลักษณะทางสังคมภายในประเทศและเป็นให้ไปตามมาตราฐานโลก แล้วจึงค่อยอนุญาตให้สามารถใช้ลายมือชื่อดิจิตอลและ/หรือลายมือชื่ออิเล็กทรอนิกส์กับธุรกรรมอิเล็กทรอนิกส์ทุกประเภท เพราะการทำธุรกรรมทาง

"ในบางรัฐอนุญาติให้ใช้ลายมือชื่ออิเล็กทรอนิกส์เฉพาะธุรกรรมที่อย่างน้อยฝ่ายใดฝ่ายหนึ่งคือหน่วยงานของรัฐ. โปรดดู ALA. CODE § 4-30-5 (1998) ใช้ได้กับการแจ้งการขอคืนภาษีและเอกสารอื่นของ Department of Revenue; CAL. GOV'T CODE § 22003 (West 1999) ใช้ได้กับการติดต่อสื่อสารกับหน่วยงานของรัฐ.; COLO. REV. STAT. ANN. (West 1999) ใช้ได้กับระบบการจดแจ้งเอกสารทางอิเล็กทรอนิกส์ของหนังสือแสดงฐานะทางการเงินตาม U.C.C.; IDAHO CODE § 67-23-57 (1998) ใช้ได้กับการจดแจ้งและการออกเอกสารโดยและที่เกี่ยวข้องกับรัฐหรือหน่วยงานท้องถิ่น.; IND. CODE ANN. § 5-24-2-2 (West 1998) ใช้ได้กับธุรกรรมที่ติดต่อกับรัฐ.; IOWA CODE ANN. § 48A.13 (West 1998) ใช้ได้กับการลงทะเบียนเพื่อขอใช้สิทธิเลือกตั้ง; ME. REV. STAT. ANN. tit. 29-A §§ 1401, 1205, and 1410 ใช้ได้กับการติดต่อที่ต้องใช้แบบฟอร์มภายใต้ The Motor Vehicle Code.; MO. ANN. STAT. § 28.621 (West 1999) ใช้ได้กับการจดแจ้งเอกสารที่เกี่ยวกับ The Secretary of State สำหรับองค์กรธุรกิจที่ดำเนินการภายใต้กฎหมาย.; MONT. CODE ANN. §§ 2-15-401, 2-15-404 (1999) อนุญาตให้ Secretary of State ดำเนินการระบบการจดแจ้งเอกสารทางอิเล็กทรอนิกส์.; NEV. REV. STAT. ANN. § 239.042 (Michie 1997) ใช้ได้กับธุรกรรมทางการเงินกับภาครัฐ.; N.M. STAT. ANN. § 14-3-15.2 (Michie 1998) ใช้ได้กับเอกสารและการจดแจ้งเอกสารมหาชน.; N.C. GEN. STAT. § 66-58.1 (1999) ใช้ได้เฉพาะกับการจดแจ้งกับองค์กรมหาชน.; N.D. CENT. CODE § 1-08-12 (1997) ใช้ได้เฉพาะกับระบบการจดแจ้งเอกสารกับองค์กรมหาชน.; TEX. GOV'T CODE ANN. § 403.027 (West 1998) ใช้ได้กับธุรกรรมที่ติดต่อกับที่ปรึกษาทางการเงินหรือกับองค์กรมหาชน.; WYO. STAT. ANN. § 9-1-306 (Michie 1998) ใช้ได้เฉพาะกับการจดแจ้งกับ Secretary of State.; การใช้ลายมือชื่ออิเล็กทรอนิกส์กับธุรกรรมประเภทอื่นๆ มีสถานะที่ไม่ชัดเจนเพราะมิได้มีการกล่าวถึงไว้ในกฎหมาย."

† Ibid., footnote 72, p.741

โปรดดูตัวอย่างใน The Illinois Financial Institutions Digital Signature Act 1999, 1997 H.B. 597 (arguably superceded by 5 ILL. COMP. STAT. 175/5-105) (effective July 1, 1999)

อิเล็กทรอนิกส์เป็นเพียงการใช้เทคโนโลยีให้เกิดประสิทธิภาพในการดำเนินธุรกิจหรือในการประกอบนิติกรรมสัญญา ไม่ได้มีการเปลี่ยนแปลงวัตถุประสงค์ของการประกอบธุรกิจหรือการประกอบนิติกรรมสัญญาแต่อย่างใด เพราะฉะนั้นเมื่อมีการออกกฎหมายรับรองสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือและรับรองสถานะของลายมือชื่อดิจิตอลและ/หรือลายมือชื่ออิเล็กทรอนิกส์แล้ว การใช้ดิจิตอลและ/หรือลายมือชื่ออิเล็กทรอนิกส์จึงควรจะสามารถใช้ในการประกอบธุรกรรมหรือทำนิติกรรมสัญญาทางอิเล็กทรอนิกส์ได้ทุกชนิดเหมือนกับการลงลายมือชื่อธรรมดา (Hand-written Signature) ในปัจจุบัน

3.2.4 ผลของการใช้ลายมือชื่อดิจิตอลตามกฎหมายลายมือชื่อดิจิตอล

3.2.4.1 ผลเกี่ยวกับข้อกำหนดในเรื่องลายมือชื่อ (Signature Requirement)

ผลของการลงลายมือชื่อดิจิตอลหรือลายมือชื่ออิเล็กทรอนิกส์ตามกฎหมายลายมือชื่อดิจิตอลหรือกฎหมายลายมือชื่ออิเล็กทรอนิกส์นั้น แบ่งออกเป็น 2 ลักษณะด้วยกัน

ลักษณะแรกคือตามกฎหมายลายมือชื่อดิจิตอลหรือกฎหมายลายมือชื่ออิเล็กทรอนิกส์จะบัญญัติไว้เพียงแค่ว่า เมื่อกฎหมายต้องการกำหนดให้มีการลงลายมือชื่อ ให้ถือว่าการลงลายมือชื่อดิจิตอลหรือลายมือชื่ออิเล็กทรอนิกส์ได้เป็นไปตามกฎหมายดังกล่าวแล้ว* เช่น South Dakota Uniform Electronic Transactions Act (2000 Senate Bill 193) เป็นต้น หรือบัญญัติในลักษณะที่ว่า การใช้ลายมือชื่อดิจิตอลมีผลหรือมีสภาพบังคับเหมือนกับการใช้ลายมือชื่อธรรมดา** เช่น Maryland Digital Signature Pilot Program (1998 Maryland House Bill 523) เป็นต้น

ลักษณะที่สองจะเป็นการบัญญัติในลักษณะที่ว่า การลงลายมือชื่อดิจิตอลด้วยกุญแจรหัสส่วนตัวที่มีความเกี่ยวพันกับกุญแจรหัสสาธารณะที่ระบุในใบรับรองที่ออกโดยผู้ประกอบการรับรองตามกฎหมายในเอกสารหรือข้อมูลอิเล็กทรอนิกส์แล้ว เมื่อผู้รับทำการตรวจสอบลายมือชื่อดิจิตอลดังกล่าวด้วยใบรับรองที่ออกโดยผู้ประกอบการรับรอง (ประเทศส่วนใหญ่กำหนดให้ต้องเป็นใบรับรองที่ออกโดยผู้ประกอบการรับรองที่ได้รับอนุญาตแล้วเท่านั้น[32] จึงจะได้รับประโยชน์จากข้อสันนิษฐานดังกล่าว) ผลออกมาว่าถูกต้องเป็นลายมือชื่อที่แท้จริง จะได้รับ

---

* If a law requires a signature, an electronic signature satisfies the law

** The use of a digital signature shall have the same force and effect as the use of a manual signature.

[32] Section 20 ของ Electronic Transactions Act 1998 ของประเทศสิงค์โปร์

สถานะว่าเป็น "ลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย" (Secure Electronic Signature)* ลายมือชื่อดิจิตอลดังกล่าวจะได้รับข้อสันนิษฐานตามกฎหมายว่า เป็นลายมือชื่อที่แท้จริงของเจ้าของลายมือชื่อที่ปรากฏชื่อในเอกสารหรือปรากฏในใบรับรอง และการลงลายมือชื่อดิจิตอลดังกล่าวเป็นการลงลายมือชื่อด้วยความตั้งใจของผู้ลงลายมือชื่อ ซึ่งมีผลทำให้ธุรกรรมหรือนิติกรรมสัญญาที่ทำการลงลายมือชื่อจะมีผลตามกฎหมาย แต่อย่างไรก็ตามข้อสันนิษฐานดังกล่าว มิได้เป็นข้อสันนิษฐานที่เด็ดขาด ผลของข้อสันนิษฐานทำให้ผู้ที่ต้องการปฏิเสธว่าลายมือชื่อดิจิตอลดังกล่าวเป็นของปลอมหรือตนมิได้เป็นผู้ลงลายมือชื่อดิจิตอลตกเป็นผู้มีภาระนำการนำสืบเพื่อพิสูจน์ข้อกล่าวอ้างดังกล่าว ตัวอย่างของกฎหมายลายมือชื่อดิจิตอลที่บัญญัติในลักษณะอย่างนี้คือ Utah Digital Signature Act เป็นต้น

3.2.4.2 ผลเกี่ยวกับข้อกำหนดในเรื่องการทำเป็นหนังสือ (Writing Requirement)

3.2.4.2.1 ผลในเรื่องของการทำเป็นหนังสือตามกฎหมาย

ข้อมูลที่ได้ทำการลงลายมือชื่อดิจิตอลแนบท้ายข้อมูล และลายมือชื่อดิจิตอลดังกล่าวได้ทำการตรวจสอบด้วยกุญแจรหัสสาธารณะที่ระบุในใบรับรองที่ถูกต้องและสมบูรณ์ ข้อมูลดังกล่าวสามารถใช้บังคับได้เสมือนหนึ่งได้ทำเป็นหนังสือในกระดาษตามกฎหมาย และจากความสามารถในการรักษาความถูกต้องสมบูรณ์ของข้อมูลที่ได้จากการใช้ลายมือชื่อดิจิตอล ซึ่งมีผลที่ดีกว่าการรักษาความถูกต้องสมบูรณ์ของการเขียนบนกระดาษ ทำให้การแก้ไขเปลี่ยนแปลงในข้อมูลสามารถตรวจพบได้ เพราะฉะนั้นข้อมูลที่ได้ทำการลงลายมือชื่อดิจิตอลจึงมีผลเท่าการทำเป็นหนังสือตามกฎหมาย (Writing Requirement) ทั้งนี้เพื่อเป็นการสอดคล้องกับกฎหมายแม่แบบของสหประชาชาติว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ ของ UNCITRAL ที่บัญญัติไว้ในมาตรา 5 ว่า "A Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message." และในมาตรา 6 ว่า "Where the law requires

---

* ในกฎหมายเหล่านี้ คำว่า "ลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย" (Secure electronic signature) หมายถึง ลายมือชื่อที่สร้างขึ้นโดนวิธีการที่มีลักษณะเฉพาะตัวของบุคคลผู้ลงลายมือชื่อ (Unique to that person) และวิธีการดังกล่าวจะอยู่ภายใต้การควบคุมของบุคคลนั้นโดยเฉพาะ (under the sole control of that person)

โปรดดู Section 17 ของ Electronic Transactions Act 1998 ของประเทศสิงคโปร์ และ Section 10-110 ของ Electronic Commerce Secrurity Act 1999 ของมลรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา

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."

3.2.4.2.2 ผลในเรื่องของต้นฉบับและสำเนาเอกสาร

สำเนาของข้อมูลที่ได้ลงลายมือชื่อดิจิตอลมีผลและสมบูรณ์ตามกฎหมายเสมือนหนึ่งต้นฉบับเอกสารตามกฎหมายลักษณะพยาน หรือหลักกฎหมายลักษณะพยานเรื่อง "Best Evidence rule" ของ Common Law จากเหตุผลในทางปฏิบัติที่ว่า ไม่ว่าจะเป็นต้นฉบับหรือสำเนาของเอกสารอิเล็กทรอนิกส์ก็อยู่ในรูปของ Bit ไม่ใช่อะตอมของหมึก และไม่สามารถแยกความแตกต่างของต้นฉบับและสำเนาเอกสารได้ และในความเป็นจริงในทางอิเล็กทรอนิกส์จะมีแต่สำเนาเอกสารเท่านั้น อย่างไรก็ตามความเท่ากันของต้นฉบับและสำเนาของเอกสารอิเล็กทรอนิกส์นี้เฉพาะในส่วนของกฎหมายลักษณะพยานเท่านั้น ไม่รวมไปถึงในส่วนของกฎหมายตั๋วเงินและกฎหมายอื่นที่เอกสารต้นฉบับจะเป็นเอกสารที่ใช้แสดงสิทธิ (Title of Document) ตามกฎหมาย[33]

3.3 ข้อกำหนดเกี่ยวกับผู้ประกอบการรับรอง

3.3.1 บุคคลผู้ทำหน้าที่เป็นผู้ประกอบการรับรอง[34]

3.3.1.1 การกำหนดให้ภาครัฐทำหน้าที่เป็นผู้ประกอบการรับรอง

จากการที่ผู้ประกอบการรับรองมีหน้าที่หลักในการออกใบรับรองดิจิตอลเพื่อทำการรับรองว่าผู้ถือใบรับรองได้เป็นเจ้าของกุญแจรหัสส่วนตัวที่มีความเกี่ยวพันกับกุญแจรหัสสาธารณะที่ปรากฏในใบรับรองจริง หน่วยงานภาครัฐที่เคยทำหน้าที่ในการออกเอกสารที่ใช้ยืนยันตัวบุคคลหรือข้อมูลต่างๆ เช่น บัตรประจำตัวประชาชน สำเนาทะเบียนบ้าน เป็นต้น ต่างได้รับความเชื่อถือและความเชื่อมั่นของสถานะทางกฎหมายของหน่วยงานเหล่านั้นอยู่แล้ว และโดยลักษณะขององค์กรเองย่อมที่จะสามารถสร้างความเชื่อมั่นซึ่งเป็นพื้นฐานในการทำหน้าที่เป็นผู้ประกอบการรับรอง (Certification Authority) ได้เป็นอย่างดีอยู่แล้ว ประกอบกับเมื่อพิจารณาถึงกิจ

---

[33] Information Security Committee, Electronic Commerce Division, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce. Id., Section 5.5, pp.114-117

[34] กฤษณะ ช่างกล่อม, (ร่าง) รายงานการศึกษาวิจัยเรื่องกฎหมายลายมือชื่อดิจิตอล หน้า 71-73

กรรมของผู้ประกอบการรับรองซึ่งมีผลกระทบถึงความมั่นคงทางสังคม รวมทั้งสิทธิหน้าที่ความรับผิดของสาธารณชนที่ประกอบธุรกรรมอิเล็กทรอนิกส์หรือการพาณิชย์อิเล็กทรอนิกส์ ทั้งการที่จะให้ภาคเอกชนเป็นผู้ประกอบการรับรองอาจทำให้เกิดความเสียหายขึ้นต่อสังคมได้ จึงมีผู้เสนอให้ภาครัฐทำหน้าที่เป็นผู้ประกอบการรับรอง ซึ่งเมื่อพิจารณาในแง่นี้แล้วหน่วยงานภาครัฐมีความเหมาะสมที่จะทำหน้าที่เป็นผู้ประกอบการรับรอง

อย่างไรก็ตาม ในกรณีที่หน่วยงานภาครัฐทำหน้าที่เป็นผู้ประกอบการรับรอง อาจจะมีปัญหาสำคัญสองปัญหาคือ 1. หน่วยงานภาครัฐสามารถที่จะใช้หลักความคุ้มกันของรัฐ (State Immunity) กับกิจกรรมที่หน่วยงานของรัฐทำในฐานะที่เป็นผู้ประกอบการรับรอง 2. การที่ภาครัฐทำหน้าที่เป็นผู้ประกอบการรับรองจะทำให้เป็นการขัดกับหลักการแข่งขันโดยเสรี เพราะภาครัฐเข้ามาดำเนินกิจการที่มีลักษณะเป็นการค้าหากำไรเสียเอง

3.3.1.2 การกำหนดให้ภาคเอกชนทำหน้าที่เป็นผู้ประกอบการรับรอง

เนื่องมาจากการบัญญัติกฎหมายมักจะตามหลังวิธีการปฏิบัติทางการค้าใหม่ที่เกิดขึ้นเสมอ ทำให้ในปัจจุบันผู้ประกอบการรับรองส่วนใหญ่ที่มีอยู่แล้วก็เป็นหน่วยงานภาคเอกชน ซึ่งก็มีศักยภาพสูงทั้งในด้านเทคนิค การจัดการ ทุนในการดำเนินงานที่เพียงพอที่จะให้บริการออกใบรับรอง นอกจากนั้นแล้ว ในการประกอบธุรกรรมแบบเดิมที่ใช้กระดาษเป็นพื้นฐาน หน่วยงานภาคเอกชน เช่น สถาบันการเงิน ผู้ให้บริการบัตรเครดิต เป็นต้น ก็สามารถทำหน้าที่ของตนได้อย่างมีประสิทธิภาพ มีระบบการบริการที่ดีและมีความรวดเร็วกว่าระบบการทำงานของภาครัฐ รวมทั้งก็ได้รับความไว้วางใจและความพอใจในการบริการในระดับสูงจากประชาชนโดยทั่วไป ภาคเอกชนจึงถูกพิจารณาว่ามีศักยภาพที่เพียงพอในการปฏิบัติหน้าที่เป็นผู้ประกอบการรับรอง จากความได้เปรียบในหลายๆ ด้าน รวมทั้งความรู้ความสามารถทางด้านเทคโนโลยีการเข้ารหัสในระดับสูงที่มีความจำเป็นในการทำหน้าที่เป็นผู้ประกอบการรับรอง ซึ่งภาครัฐมักจะมีความสามารถทางเทคโนโลยีที่ด้อยกว่า ทั้งภาคเอกชนน่าจะตอบสนองความต้องการของผู้ใช้บริการที่เป็นภาคเอกชนด้วยกันเองได้ดีกว่า

อย่างไรก็ตามเมื่อพิจารณาจากกิจกรรมของผู้ประกอบการรับรองจะเห็นได้ว่ากิจกรรมหลายอย่าง รวมไปถึงการออกใบรับรองมีส่วนเกี่ยวข้องกับความสงบเรียบร้อยของสังคมและเสรีภาพขั้นพื้นฐานของประชาชน ซึ่งภาครัฐมีหน้าที่ในการรับประกันและทำหน้าที่ดูแลในเรื่องต่างๆ เหล่านี้ การที่ปล่อยให้หน่วยงานภาคเอกชนเป็นผู้ดำเนินกิจการที่มีผลกระทบต่อเรื่องเหล่านี้ จะทำให้เกิดความเสี่ยงกับสังคม ในเรื่องที่มีความสำคัญ เช่น การคุ้มครองผู้บริโภค มาตรฐานการบริการที่ดี เป็นต้น และการคุ้มครองสิทธิขั้นพื้นฐานของประชาชน เช่น สิทธิในความเป็นส่วนตัว (Privacy) เป็นต้น ซึ่งภาคเอกชนคงจะทำหน้าที่เหล่านี้ได้ไม่ดีนักเพราะภาคเอกชนเป็นองค์กรที่จัดตั้งขึ้นโดยมีวัตถุประสงค์เพื่อมุ่งหวังในทางการค้าหากำไร จากลักษณะทางธรรมชาติของ

วัตถุประสงค์ดังกล่าวมีลักษณะที่ขัดกับการคุ้มครองสิทธิขั้นพื้นฐานของประชาชน รวมไปถึงในการคุ้มครองผู้บริโภคและมาตรฐานการบริการที่ดี ซึ่งจะส่งผลให้ภาคเอกชนไม่สามารถทำหน้าที่ในการเป็นผู้ประกอบการรับรองอย่างเอื้ออำนวยประโยชน์ต่อสังคม

3.3.1.3 การจัดระบบร่วมกันของภาครัฐและเอกชนในลักษณะของการจัดเป็นโครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะ

เนื่องจากในสังคมภาครัฐและภาคเอกชนจะต้องมีความร่วมมือกัน โดยมิอาจละเลยฝ่ายใดฝ่ายหนึ่งได้ เช่นเดียวกันหากพิจารณาถึงประเภทในการให้บริการของผู้ประกอบการรับรองซึ่งจะมีความหลากหลายเป็นอย่างมาก เช่น การให้บริการออกใบรับรองในกิจกรรมทางทหาร การให้บริการออกใบรับรองในกิจกรรมทางการเงิน การให้บริการออกใบรับรองในกิจกรรมแพทย์ หรือ การให้บริการออกใบรับรองในกิจกรรมที่เกี่ยวกับการทำธุรกิจการค้าโดยทั่วไป เป็นต้น นอกจากนั้นแล้วหากพิจารณาในแง่ที่ว่าให้ภาครัฐหรือภาคเอกชนภาคใดภาคหนึ่งทำหน้าที่เป็นผู้ประกอบการรับรอง ก็จะพบจุดด้อยอย่างที่ได้กล่าวถึงไปแล้วในหัวข้อ 3.3.1.1 และหัวข้อ 3.3.1.2 ดังนั้นจึงเป็นการไม่เหมาะสมที่จะกำหนดภาครัฐหรือภาคเอกชนเพียงภาคเดียวทำหน้าที่เป็นผู้ประกอบการรับรอง

เพราะฉะนั้นจึงมีแนวความคิดให้สร้างระบบที่ภาคเอกชนสามารถมีบทบาทในการพัฒนาภาคธุรกิจได้เช่นเดิม แต่ภาครัฐก็สามารถสนับสนุนภาคเอกชนและสามารถมีบทบาทในการคุ้มครองความมั่นคงและปลอดภัยของสังคมและสิทธิขั้นพื้นฐานของประชาชนได้ จึงได้มีการพัฒนาโครงสร้างพื้นฐานของระบบกุญแจรหัสสาธารณะ (Public Key Infrastructure) โดยให้มีหน่วยงานภาครัฐทำหน้าที่เป็นผู้ประกอบการรับรองในระดับสูงหรือผู้ประกอบการรับรองในระดับนโยบายคอยทำหน้าที่ในการกำกับดูแลนโยบาย วิธีการปฏิบัติงาน เงินทุน มาตรฐานทางเทคโนโลยีที่ใช้ วิธีการในการออกใบรับรอง รวมตลอดไปถึงคอยสอดส่องดูแลว่าผู้ประกอบการรับรองได้ปฏิบัติตามหน้าที่ที่บัญญัติไว้ในกฎหมายหรือไม่ ทั้งยังมีอำนาจในการออกข้อกำหนดต่างๆ ตามกฎหมาย เพื่อใช้ในการกำกับดูแลผู้ประกอบการรับรอง ในส่วนต่อมาก็จะจัดทำเงื่อนไขหรือวิธีการในการที่จะเป็นผู้ประกอบการรับรอง ในบางประเทศก็เปิดเสรี คือ บุคคลใดก็สามารถที่จะปฏิบัติหน้าที่เป็นผู้ประกอบการรับรองได้ แต่อาจจะต้องมีการขึ้นทะเบียน หรือในบางประเทศก็จะใช้ระบบในการขอใบอนุญาต ซึ่งก็แล้วแต่ว่ารัฐบาลและประชาชนในประเทศนั้นๆ เห็นสมควร ซึ่งความสัมพันธ์ของผู้ประกอบการรับรองภาครัฐกับผู้ประกอบการรับรองภาคเอกชนจะมีลักษณะเป็นความสัมพันธ์ในแบบลำดับชั้น (Hierarchy) โดยผู้ประกอบการรับรองภาครัฐจะทำหน้าที่เป็นผู้ประกอบการรับรองในระดับชั้นสูง ที่ทำการดูแลและให้การรับรองผู้ประกอบการรับรองภาคเอกชนที่อยู่ในระดับต่ำกว่า (ตามที่ได้อธิบายในบทที่ 2 หัวข้อ 2.3.6) ซึ่งการจัดระบบแบบสามารถที่จะ

ตอบสนองต่อความต้องการของระบบลายมือชื่อดิจิตอลได้ดีกว่า ทั้งยังเป็นประโยชน์ต่อสังคมโดยส่วนรวมอย่างแท้จริง

3.3.2 ข้อกำหนดเกี่ยวกับผู้ประกอบการรับรองตามกฎหมาย

ข้อกำหนดเกี่ยวกับผู้ประกอบการรับรองนี้ ก็แตกต่างกันออกไปในรายละเอียดของแต่ละประเทศที่ได้มีการออกกฎหมายเกี่ยวกับลายมือชื่อดิจิตอล บางประเทศได้มีบทบัญญัติที่กล่าวถึงข้อกำหนดต่างๆ ที่ผู้ประกอบการรับรองมีหน้าที่จะต้องปฏิบัติตาม เช่น The Utah Digital Signature Act หรือ ใน the Electronic Transaction Act ของประเทศสิงคโปร์ หรือในบางประเทศก็มิได้มีบทบัญญัติที่กล่าวถึงผู้ประกอบการรับรองอยู่เลย เช่น ประเทศเบลเยี่ยม เป็นต้น อย่างไรก็ตามก็มีแนวทางที่คณะกรรมาธิการกฎหมายการค้าระหว่างประเทศของสหประชาชาติ (United Nations Commission on International Trade Law หรือ UNCITRAL) ได้นำไปใช้ใน Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signature มาตรา 9[35] ซึ่งมีหลักการสำคัญดังนี้

---

[35] United Nations, Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signature (A/CN.9/WG.IV/WP.88), 30 January 2001, www.un.or.at/uncitral (visited Feb. 2 2001), p.7

"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;

1. ถ้าจำเป็นต้องมีหน่วยงานที่ให้บริการจัดหาใบรับรอง (Certification service provider) เพื่อรองรับความมีผลทางกฎหมายเสมือนการลงลายมือชื่อของลายมือชื่ออิเล็กทรอนิกส์ หน่วยงานที่ให้บริการจัดหาใบรับรองจะต้อง
   (a) หน่วยงานที่ให้บริการจัดหาใบรับรองจะปฏิบัติตามนโยบายและแนวทางปฏิบัติที่ได้ประกาศหรือเผยแพร่เอาไว้
   (b) หน่วยงานที่ให้บริการจัดหาใบรับรองจะต้องเอาใจใส่อย่างมีเหตุผล (reasonable care) ที่จะทำให้มั่นใจถึงความถูกต้องและสมบูรณ์ของข้อมูลหรือเนื้อหาที่ตนได้แสดงออกซึ่งเกี่ยวข้องกับใบรับรองตลอด

(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)"

ระยะเวลาที่ใบรับรองมีผลบังคับใช้ หรือข้อมูลหรือเนื้อหาที่มีอยู่ในใบรับรอง

(c) หน่วยงานที่ให้บริการจัดหาใบรับรองต้องจัดหาวิธีการที่ทำให้บุคคลผู้ที่ต้องการใช้ใบรับรองสามารถเข้าใจอย่างชัดเจนจากใบรับรองว่า

(i) ชื่อของหน่วยงานที่ให้บริการจัดหาใบรับรอง

(ii) ชื่อของเจ้าของลายมือชื่อที่ระบุในใบรับรอง เป็นบุคคลผู้ที่ครอบครอง ข้อมูลที่ใช้ในการสร้างลายมือชื่อ (the signature creation data) ในเวลาที่ออกใบรับรอง

(iii) ข้อมูลที่ใช้ในการสร้างลายมือชื่อ (the signature creation data) สามารถใช้งานได้ถูกต้อง ในเวลาหรือก่อนเวลาที่ออกใบรับรอง

(d) หน่วยงานที่ให้บริการจัดหาใบรับรองต้องจัดหาวิธีการที่ทำให้บุคคลผู้ที่ต้องการใช้ใบรับรองสามารถเข้าใจอย่างชัดเจนจากใบรับรองหรือแหล่งข้อมูลอื่นที่เกี่ยวข้องว่า

(i) วิธีการใช้ลายมือชื่อในการระบุเจ้าของลายมือชื่อ

(ii) ข้อจำกัดในจุดประสงค์หรือคุณค่าของข้อมูลที่ใช้ในการสร้างลายมือชื่อ (the signature creation data) หรือใบรับรองในการใช้

(iii) ข้อมูลที่ใช้ในการสร้างลายมือชื่อ (the signature creation data) สามารถใช้งานได้อย่างถูกต้องและไม่ได้หลุดจากการควบคุมของเจ้าของลายมือชื่อ (compromised)

(iv) ข้อจำกัดของขอบเขตความรับผิดตามเงื่อนไขของหน่วยงานที่ให้บริการจัดหาใบรับรอง

(v) ได้รับการแจ้งจากเจ้าของลายมือชื่อตามรายละเอียดในมาตรา 8 (1) (b)

(vi) จะต้องเพิกถอนใบรับรองให้ทันเวลาเมื่อมีการร้องขอ

(e) เมื่อการเหตุการณ์ตามข้อ (d) (v) ให้ทำการแสดงการแจ้งดังกล่าวของเจ้าของลายมือชื่อ และเมื่อเกิดเหตุการณ์ตามข้อ (d) (vi) ให้ทำให้มั่นใจว่าได้ทำการเพิกถอนใบรับรองทันต่อเวลา

(f) หน่วยงานที่ให้บริการจัดหาใบรับรองจะต้องใช้ระบบ วิธีการ และบุคคลากรที่เชื่อถือได้ในการดำเนินงานให้บริการจัดหาใบรับรองของตน

2. หน่วยงานที่ให้บริการจัดหาใบรับรองจะต้องมีความรับผิดในกรณีที่ไม่สามารถปฏิบัติตามข้อกำหนดในวรรคหนึ่งได้

เมื่อพิจารณาหลักการข้างต้นแล้ว ผู้ประกอบการรับรอง (หน่วยงานที่ให้บริการจัดหาใบรับรอง) จะต้องทำตามข้อกำหนดของกฎหมายในเรื่องของ หนึ่งจะต้องมีการจัดทำถ้อยแถลงแนวทางปฏิบัติในการออกใบรับรอง (Certification Practice Ststement หรือ CPS) ต้องใช้ความระมัดระวังในการตรวจสอบความถูกต้องของหลักฐานต่างๆ ที่ใช้ในการออก ระงับการใช้ชั่วคราวหรือเพิกถอนใบรับรอง อำนวยความสะดวกให้แก่ผู้ใช้บริการหรือผู้ถือใบรับรองในการแจ้งระงับหรือยกเลิกการใช้ลายมือชื่อดิจิตอล จัดหาวิธีการที่ทำให้ผู้ที่ต้องการใช้ใบรับรองในการตรวจสอบลายมือชื่อดิจิตอลทราบข้อมูลต่างๆ ที่เกี่ยวข้องกับการใช้ใบรับรอง เช่น วิธีการใช้ลายมือชื่อระบุตัวบุคคล ข้อจำกัดในการใช้ใบรับรอง ข้อมูลเกี่ยวกับสถานะของใบรับรองว่าถูกระงับการใช้ชั่วคราวหรือถูกเพิกถอนไปแล้ว เป็นต้น รวมทั้งผู้ประกอบการรับรองจะต้องใช้ระบบ เทคโนโลยี ขั้นตอนและบุคคลากรที่เชื่อถือได้ในการให้บริการออกใบรับรองของตน ซึ่งรายละเอียดเกี่ยวกับหน้าที่เหล่านี้จะได้อธิบายอย่างละเอียดในบทที่ 4 ต่อไป

3.3.3 การกำกับดูแลผู้ประกอบการรับรอง

หน้าที่หลักของผู้ประกอบการรับรองคือทำการออกใบรับรองที่ทำหน้าที่ในการรับรองกุญแจรหัสที่ใช้ในขบวนการลงลายมือชื่อและตรวจสอบลายมือชื่อ ซึ่งจะต้องเป็นไปตามมาตรฐานทางเทคโนโลยี กระบวนการในการรักษาความปลอดภัย และวิธีการที่ใช้ในการออกใบรับรองตามที่ระบุใน ถ้อยแถลงแนวทางปฏิบัติในการออกใบรับรอง (CPS) จึงมีแนวความคิดว่าการกำกับดูแลผู้ประกอบการรับรองนั้นควรใช้กลไกของตลาดเป็นตัวกำหนด โดยอยู่บนสมมติฐานที่หากผู้ประกอบการรับรองรายใดที่ไม่มีมาตรฐานก็จะไม่ได้รับความไว้วางใจและในที่สุดก็จะไม่มีผู้ใช้บริการ หรือให้ใช้ระบบการกำกับดูแลตนเอง (Self-regulation) ก็ได้

อย่างไรก็ตามสิ่งที่กล่าวมานี้น่าที่จะไม่เพียงพอ เพราะในระบบการใช้กลไกตลาด กว่าที่ผู้ประกอบการรับรองที่ไม่มีมาตรฐานจะปิดตัวลง ก็คงสร้างความเสียหายให้เกิดขึ้นแล้ว รวมทั้งในระบบกำกับดูแลตนเองก็ไม่มีสิ่งที่จะสามารถสร้างความมั่นใจได้เพียงพอ กับระบบที่มีความสำคัญต่อสังคม รวมไปถึงในระดับสังคมระหว่างประเทศอีกด้วย การกำกับดูแลจึงมีความจำเป็นที่จะต้องมีความสอดคล้องกับความสำคัญของระบบลายมือชื่อดิจิตอลและสอดคล้องกับมาตรฐานที่นานาอารยะประเทศยอมรับ

วิธีการกำกับดูแลที่นิยมใช้กันอยู่ทั่วไปในทุกๆ ประเทศที่มีกฎหมายเกี่ยวกับลายมือชื่อดิจิตอลก็คือ การจัดตั้งองค์กรเพื่อทำหน้าที่ออกใบอนุญาตสำหรับผู้ที่ต้องการจะทำหน้าที่เป็นผู้ประกอบการรับรอง เนื่องมาจากเหตุผลในทางนโยบายสาธารณะของแต่ละประเทศ คงจะมีแต่องค์กรของรัฐที่มีความเหมาะสมที่จะอนุญาตหรือไม่อนุญาตให้องค์กรหรือหน่วยงานใดกระทำการเป็น

ผู้ประกอบการรับรอง[36] โดยกฎเกณฑ์ในการออกใบอนุญาตควรที่จะส่งเสริมให้ผู้ที่มีชื่อเสียงในทางวิชาชีพและจรรยาบรรณเป็นผู้เข้ามาประกอบกิจการเป็นผู้ประกอบการรับรอง ตัวอย่างเช่น โนตารีพับลิก (Notary Public) บริษัทที่เป็นที่ปรึกษาทางกฎหมาย และธนาคาร เป็นต้น อย่างไรก็ดีนโยบายในการให้ใบอนุญาตสำหรับผู้ประกอบการรับรองควรจะควบคุมและจำกัดเฉพาะกิจการที่มีความสำคัญต่อความสงบเรียบร้อยของสังคมหรือกระทบต่อสิทธิขั้นพื้นฐานของประชาชนเท่านั้น อย่างไรก็ตามนโยบายการให้ใบอนุญาตมีอยู่หลายแนวทางด้วยกัน ซึ่งมีสาระสำคัญที่จำเป็นที่จะต้องนำมาพิจารณาดังนี้

3.3.3.1 บุคคลผู้ทำหน้าที่ในการให้ใบอนุญาต

จากที่ได้กล่าวไว้แล้วในหัวข้อ 3.3.1.3 ว่าภาครัฐจะมีการจัดตั้งผู้ประกอบการรับรองในระดับสูงซึ่งทำหน้าที่ในการกำกับดูแลผู้ประกอบการรับรองของภาคเอกชน ซึ่งองค์กรดังกล่าวก็ควรที่จะเป็นผู้ทำหน้าที่ในการให้ใบอนุญาตด้วย แต่เนื่องจากระบบลายมือชื่อดิจิตอลเป็นระบบที่ใช้บนเครือข่ายทางอิเล็กทรอนิกส์ที่ใช้ในการติดต่อสื่อสารทั่วโลก การใช้ลายมือชื่อดิจิตอลจึงมีการใช้ในระดับระหว่างประเทศ ซึ่งส่งผลให้การออกใบรับรองย่อมต้องมีผลกระทบในระดับระหว่างประเทศ จึงมีแนวความคิดให้ กลุ่มประเทศ เช่น สหภาพยุโรป หรือ หน่วยงานระหว่างประเทศ เป็นผู้มีอำนาจในการออกใบอนุญาตผู้ประกอบการรับรอง แต่อย่างไรก็ตามการที่จะให้ประเทศต่างๆ ที่มีอำนาจอธิปไตยให้ความเห็นชอบกับนโยบายของกลุ่มประเทศของตน หรือนโยบายหน่วยงานระหว่างประเทศหน่วยงานใดหน่วยงานหนึ่งย่อมเป็นไปไม่ได้ ทั้งในแต่ละประเทศก็มีระบบกฎหมายและระบบทางสังคม รวมไปถึงสิทธิขั้นพื้นฐานของประชาชนที่แตกต่างกันจึงเป็นเรื่องที่ยากจนถึงเป็นไปไม่ได้ที่จะสามารถมีนโยบายในการออกใบอนุญาตผู้ประกอบการรับรองร่วมกัน

แนวทางที่เป็นไปได้มากกว่าคือ การให้ภาครัฐของแต่ละประเทศทำหน้าที่เป็นผู้ออกใบอนุญาต โดยจัดตั้งองค์กรขึ้นมาเพื่อทำหน้าที่ในการออกใบอนุญาตหรือจะใช้ผู้ประกอบการรับรองภาครัฐที่มีอยู่หรือที่จะจัดตั้งขึ้นในการทำหน้าที่เป็นผู้ประกอบการรับรองในระดับสูงรวมทั้งทำหน้าที่ในการออกใบอนุญาตด้วย เพื่อความเหมาะสมต่อสภาพสังคมภายในประเทศ รวมทั้งต่อระบบกฎหมายและสิทธิขั้นพื้นฐานของประชาชนภายในประเทศของตน

---

[36] United Nations, "Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signature" (A/CN.9/WG.IV/WP.88), <www.un.or.at/uncitral >.(visited Feb. 2 2001) , 30 January 2001, p.23

3.3.3.2 แนวทางการกำกับดูแลด้วยระบบใบอนุญาต

แนวทางในการกำกับดูแลด้วยระบบใบอนุญาตสามารถที่จะแบ่งได้เป็น 2 แนวทางคือ

3.3.3.2.1 ระบบใบอนุญาตแบบบังคับ (Mandatory Licensing scheme)

ในระบบการกำกับดูแลด้วยระบบในอนุญาตแบบบังคับนี้ จะเป็นระบบที่ผู้ประกอบการรับรองทุกองค์กรภายในประเทศจะสามารถดำเนินการได้ก็ต่อเมื่อได้รับใบอนุญาตที่ถูกต้องตามกฎหมาย หรือพูดอีกอย่างว่าเป็นกิจการควบคุม เช่นเดียวกันกับกิจการธนาคารพาณิชย์ ที่อยู่ภายในพระราชบัญญัติธนาคารพาณิชย์ เป็นต้น ตัวอย่างของกฎหมายเกี่ยวกับลายมือชื่อดิจิตอลที่ใช้ระบบนี้ก็คือ กฎหมายของประเทศอิตาลีซึ่งกำหนดให้ผู้ประกอบการรับรองทุกแห่งจะต้องจดทะเบียนกับหน่วยงานกำกับดูแล และต้องปฏิบัติตามข้อกำหนดด้านการเงินและด้านเทคนิคต่างๆ เช่นจะต้องมีเงินทุนจดทะเบียนไม่ต่ำกว่า 705 ล้านดอลลาร์สหรัฐ และพนักงานของผู้ประกอบการรับรองจะต้องมีคุณสมบัติเช่นเดียวกันกับพนักงานของธนาคารพาณิชย์เป็นต้น[37] ตัวอย่างของประเทศที่ใช้ระบบใบอนุญาตแบบบังคับ คือ ประเทศ Malaysia ภายใต้มาตรา 4 ของ Malaysian Digital Signature Act 1997 ผู้ประกอบการรับรองจะต้องได้รับใบอนุญาตจึงจะสามารถดำเนินกิจการเป็นผู้ประกอบการรับรองได้[38]

---

[37] สมเกียรติ ตั้งกิจวานิชย์. รายงานการวิจัยเรื่อง ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง. สถาบันวิจัยเพื่อการพัฒนาประเทศไทย. หน้า 35

[38] "**Section 4 (1)** No person shall carry on or operate, or hold himself uot as carrying on or operating, as a certification authority unless that person holds a valid license issued under this Act.

Section 4 (2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding ten years or to both, and in the case of a continuing offence shall in addition be liable to a daily fine not exceeding five thousand ringgit for each day the offence countinues to be committed...".

3.3.3.2.2 ระบบใบอนุญาตแบบสมัครใจ (Voluntary Licensing scheme)[39]

อีกทางเลือกหนึ่งก็คือการกำกับดูแลผู้ประกอบการรับรองด้วยระบบใบอนุญาตแบบสมัครใจดังที่ปรากฏในกฎหมายธุรกรรมอิเล็กทรอนิกส์ของสิงคโปร์ ซึ่งอนุญาตให้มีทั้งผู้ประกอบการรับรองที่ได้รับอนุญาต (Licensed CA) และผู้ประกอบการรับรองที่ไม่ได้รับอนุญาต (Unlicensed CA) โดยกำหนดให้ผู้ประกอบการรับรองในกลุ่มแรกสามารถที่จะมีเงื่อนไขในการประกอบกิจการที่เข้มงวดกว่า ในขณะเดียวกันก็จูงใจให้ผู้ประกอบการรับรองต่างๆ เข้าสู่ระบบใบอนุญาตโดยกำหนดให้ผู้ประกอบการรับรองที่ได้รับใบอนุญาตไม่ต้องมีความรับผิดในกรณีที่มีผู้ปลอมแปลงใบรับรอง และสามารถจำกัดความรับผิดสูงสุดในบางกรณีได้ ทั้งใบรับรองที่ออกโดยผู้ประกอบการรับรองรับอนุญาตจะได้รับประโยชน์จากข้อสันนิษฐานทางกฎหมายในเรื่องของความถูกต้องที่สูงกว่า

ตัวอย่างของสิ่งที่เป็นเงื่อนไขในการประกอบกิจการผู้ประกอบการรับรองที่ได้รับใบอนุญาตตามกฎหมายธุรกรรมอิเล็กทรอนิกส์ของประเทศสิงคโปร์ได้แก่

- เงื่อนไขในการขอรับใบอนุญาต การต่ออายุและการเพิกถอนใบอนุญาต
- เงินทุนจดทะเบียนขั้นต่ำในการประกอบกิจการผู้ประกอบการรับรอง ซึ่งจะช่วยให้ผู้ประกอบการรับรองมีความสามารถที่จะชดใช้ความเสียหายแก่ผู้ที่ได้รับความเสียหายจากการออกใบรับรองที่ผิดพลาด
- มาตรฐานในการออกใบรับรองในด้านต่างๆ เช่น ความสามารถของบุคลากรที่เป็นพนักงานของผู้ประกอบการรับรอง
- รูปแบบและเนื้อหาของใบรับรองที่ออก
- สิ่งที่ต้องรายงานต่อหน่วยงานกำกับดูแลและเอกสารที่ต้องจัดเก็บ
- การแต่งตั้งและจ่ายค่าตอบแทนให้แก่ผู้ตรวจสอบ (Auditor)

---

[39] สมเกียรติ ตั้งกิจวานิชย์, รายงานการวิจัยเรื่อง ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง, สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, หน้า 35-36

แนวทางการกำกับดูแลผู้ประกอบการรับรองด้วยระบบใบอนุญาตแบบสมัครใจของประเทศสิงคโปร์ เป็นแนวทางที่สอดคล้องกับร่างข้อกำหนดของสหภาพยุโรป (EU Directive) ซึ่งห้ามประเทศสมาชิกออกกฎหมายบังคับให้ผู้ประกอบการรับรองทุกแห่งต้องขอใบอนุญาตประกอบการ ในกรณีที่ประเทศสมาชิกต้องการใช้ระบบใบอนุญาต ร่างข้อกำหนดดังกล่าวก็ให้ใช้ระบบใบอนุญาตแบบสมัครใจมาใช้ โดยเงื่อนไขในการขอใบอนุญาตต้องมีความชัดเจนและโปร่งใส และไม่มีลักษณะเป็นการเลือกปฏิบัติ

3.3.3.3 กิจกรรมของผู้ประกอบการรับรองที่อยู่ในขอบเขตของการกำกับดูแล

กิจกรรมของผู้ประกอบการรับรองที่อยู่ควรในขอบเขตของการกำกับดูแลมีดังนี้[40]

3.3.3.3.1 การใช้เทคโนโลยีที่สามารถไว้วางใจได้ (Trustworthy Technology) และเจ้าหน้าที่ที่สามารถไว้วางใจได้ (Trustworthy Employee)

ผู้ประกอบการรับรองจะต้องใช้ระบบที่มีความน่าเชื่อถือ (Trustworthy Technology) และเจ้าหน้าที่ผู้ให้บริการในการออกใบรับรอง ส่วนระดับของความน่าเชื่อถือและความปลอดภัยควรที่จะกำหนดในกฎหมายหรือระเบียบข้อบังคับ รวมทั้งต้องแสดงไว้ในถ้อยแถลงแนวทางปฏิบัติในการออกใบรับรอง (CPS) เพื่อเป็นหลักประกันและสร้างความมั่นใจในความน่าเชื่อถือของผู้ประกอบการรับรอง

3.3.3.3.2 เงินทุนในการประกอบกิจการและฐานะทางการเงิน

ในการประกอบกิจการเป็นผู้ประกอบการรับรองนี้ นอกจากจะต้องมีหลักประกันในเรื่องของความน่าเชื่อถือจากการใช้เทคโนโลยีและเจ้าหน้าที่ที่สามารถไว้วางใจได้แล้ว ผู้ประกอบการรับรองยังต้องมีเงินทุนในการประกอบกิจการและฐานะทางการเงินที่สามารถสร้างความน่าเชื่อถือให้เกิดขึ้น เงินทุนในการประกอบกิจการและฐานะทางการเงินจะเป็นสิ่งที่สร้างความน่าเชื่อถือ ทั้งยังเป็นส่วนหนึ่งของหลักประกันว่าผู้ประกอบการรับรองมีเงินทุนที่เพียงพอที่จะใช้เทคโนโลยีและเจ้าหน้าที่ที่สามารถไว้วางใจได้ รวมทั้งเพียงพอที่จะชดใช้ความเสียหายต่างๆ ที่เกิดขึ้นจากความผิดพลาดของผู้ประกอบการรับรองหรือเจ้าหน้าที่ของผู้ประกอบการรับรองแก่ผู้ที่ได้รับความเสียหาย

---

[40] กฤษณะ ช่างกล่อม. (ร่าง) รายงานการศึกษาวิจัยเรื่องกฎหมายลายมือชื่อดิจิตอล หน้า 75-76

3.3.3.3.3 การเก็บรักษาเอกสาร (Record keeping)

ผู้ประกอบการรับรองที่มีประสิทธิภายจำเป็นที่จะต้องเก็บเอกสารที่เกี่ยวข้องดังต่อไปนี้

- หลักฐานที่เกี่ยวข้องกับเจ้าของคู่กุญแจรหัสหรือเจ้าของลายมือชื่อดิจิตอล
- วันที่ออกใบรับรอง
- วันที่ใบรับรองหมดอายุ
- การเพิกถอนหรือระงับการใช้ใบรับรองชั่วคราว
- กระบวนการทางเทคนิคที่ใช้ในการสร้างใบรับรอง และการประทับเวลา (Time Stamp) เป็นต้น

ซึ่งเอกสารเหล่านี้ไม่ว่าจะเป็นเอกสารที่เป็นกระดาษหรือในรูปของเอกสารอิเล็กทรอนิกส์ เหล่านี้มีความจำเป็นที่จะต้องใช้เป็นหลักฐานในการพิสูจน์ความถูกต้องแท้จริง ในขณะที่มีการดำเนินคดีในกรณีที่ผู้ประกอบการรับรองถูกเรียกตัวให้เป็นพยานบุคคลในศาล จึงจำเป็นต้องมีข้อกำหนดให้ต้องทำการเก็บเอกสารเหล่านี้ไว้ภายในระยะเวลาที่กำหนด ซึ่งจะต้องสอดคล้องกับกฎหมายว่าด้วยเรื่องของอายุความ และจะต้องกำหนดให้มีการทำข้อมูลสำรองและระบบการกู้ข้อมูลในกรณีที่เกิดความเสียหายของข้อมูลขึ้น

3.3.3.3.4 การตรวจสอบ (Audit)

มีความจำเป็นอย่างยิ่งที่กิจกรรมของผู้ประกอบการรับรองจะต้องมีการตรวจสอบเป็นระยะๆ ซึ่งกฎหมายที่เกี่ยวกับการตรวจสอบบัญชีน่าจะไม่สามารถครอบคลุมได้อย่างเพียงพอ เพราะในกฎหมายดังกล่าวนี้ได้ทำการบัญญัติไว้เฉพาะหลักเกณฑ์ในการตรวจสอบสำหรับการตรวจสอบทางบัญชีเท่านั้น ซึ่งการตรวจสอบผู้ประกอบการรับรองจำเป็นที่จะต้องมีการตรวจสอบทั้งทางด้านกฎหมายและทางด้านเทคนิค ซึ่งจะต้องอาศัยผู้ตรวจสอบพิเศษเฉพาะด้าน จึงมีความจำเป็นที่จะต้องกำหนดหลักเกณฑ์การตรวจสอบไว้เพิ่มเติม

3.3.3.3.5 การกำกับดูแลและการบังคับใช้ (Supervision and Enforcement)

ต้องมีการกำหนดขอบอำนาจขององค์กรที่ทำหน้าที่ในการกำกับดูแลผู้ประกอบการรับรองอย่างชัดเจน ไม่ว่าจะใช้ระบบการกำกับดูแลด้วยระบบใบอนุญาตหรือโดยใช้ระบบการกำกับดูแลตนเอง (Self Regulation)

3.3.3.3.6 กระบวนการรับเรื่องราวร้องทุกข์

กระบวนการกำกับดูแลที่ดี จำเป็นที่จะต้องให้มีกระบวนการในการรับเรื่องราวร้องทุกข์ ซึ่งต้องมีการกำหนดขั้นตอนและวิธีการรับเรื่องราวร้องทุกข์ รวมทั้งกระบวนการในการระงับข้อพิพาทเบื้องต้นอย่างรัดกุมและเป็นธรรม

3.3.3.3.7 ค่าธรรมเนียม (Fees)

อัตราค่าบริการเป็นประเด็นที่สำคัญอย่างหนึ่ง เพราะมีผลกระทบต่อส่วนรวม ซึ่งรัฐมีหน้าที่ในการให้ความดูแลให้มีความสงบเรียบร้อย จึงควรมีการกำกับดูแลให้สอดคล้องกับความเป็นจริงและเป็นธรรมกับผู้บริโภค ซึ่งเป็นบุคคลส่วนใหญ่ของประเทศ

3.3.3.3.8 อำนาจของผู้ประกอบการรับรองในการออกข้อบังคับ

ผู้ประกอบการรับรองสามารถที่จะออกกฎข้อบังคับให้มีผลต่อผู้ใช้บริการหรือผู้ถือใบรับรอง (Subscriber) โดยกำหนดไว้ในข้อสัญญาที่ผู้ถือใบรับรองทำกับผู้ประกอบการรับรอง และผู้ประกอบการรับรองยังสามารถกำหนดไว้ในถ้อยแถลงแนวทางปฏิบัติในการออกใบรับรอง (CPS) ของตน ซึ่งในจุดนี้กฎหมายจะต้องเข้ามากำกับดูแลในการวางข้อกำหนดของสัญญาให้เกิดความเป็นธรรมกับผู้ถือใบรับรองซึ่งเป็นผู้บริโภค โดยอาจใช้ข้อกฎหมายคุ้มครองผู้บริโภค รวมไปถึงข้อกฎหมายเกี่ยวกับข้อสัญญาที่ไม่เป็นธรรมมาเป็นตัวพิจารณา

3.3.3.3.9 การเลิกกิจการของผู้ประกอบการรับรอง

ในกรณีที่ผู้ประกอบการรับรองต้องการที่จะเลิกกิจการ มีความจำเป็นที่กฎหมายจะต้องวางข้อกำหนดในเรื่องดังกล่าวต่อไปนี้

- การโอนเอกสารหรือใบรับรองไปให้ผู้ประกอบการรับรองรายอื่น
- ว่างข้อกำหนดเกี่ยวกับการเลิกกิจการ รวมทั้งยังจะต้องกำหนดหน้าที่ในการเก็บรักษาเอกสารที่เกี่ยวข้องตามระยะเวลาที่กำหนด
- ระยะเวลาความรับผิดภายหลังที่ผู้ประกอบการรับรองได้เลิกกิจการไปแล้ว เป็นต้น

3.4 การรับรองลายมือชื่อและผู้ประกอบการรับรองของต่างประเทศ

ในการใช้ลายมือชื่อดิจิตอลในการสื่อสารทางอิเล็กทรอนิกส์นั้น คงจะหลีกเลี่ยงไม่ได้ที่จะต้องมีการติดต่อสื่อสารกันระหว่างประเทศ จึงเกิดประเด็นขึ้นมาว่าจะยอมรับหรือรับรองลายมือชื่อ

ลายมือชื่อดิจิตอลและผู้ประกอบการรับรองของต่างประเทศอย่างไร ซึ่งประเด็นดังกล่าวนี้เชื่อว่าในเวทีการเจรจาการค้าระหว่างประเทศว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ในอนาคต จะมีความสำคัญเป็นอย่างสูง โดยประเทศที่พัฒนาแล้วคงจะพยายามผลักดันให้ประเทศอื่นๆ ยอมรับหรือรับรองลายมือชื่อดิจิตอลและผู้ประกอบการรับรองของต่างประเทศ โดยใช้หลักการไม่เลือกปฏิบัติ (Non-discrimination) ซึ่งเป็นแนวทางที่คณะกรรมาธิการกฎหมายการค้าระหว่างประเทศของสหประชาชาติ (United Nations Commission on International Trade Law หรือ UNCITRAL) ได้นำไปใช้ใน Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signature มาตรา 12[41] ซึ่งได้บัญญัติหลักการการไม่เลือกปฏิบัติต่อลายมือชื่อดิจิตอลและใบรับรองที่ออกโดยผู้ประกอบการรับรองต่างชาติไว้ดังนี้

---

[41] United Nations, Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signature (A/CN.9/WG.IV/WP.88), Id., p.9

"**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."

1. ในการพิจารณาว่าลายมือชื่ออิเล็กทรอนิกส์ และใบรับรองใดจะมีผลตามกฎหมายหรือไม่จะไม่นำประเด็นดังต่อไปนี้มาพิจารณา
   (a) สถานที่ทางภูมิศาสตร์ที่ออกใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ได้รับการสร้างหรือใช้ หรือ
   (b) สถานที่ทางภูมิศาสตร์ที่ประเป็นสถานประกอบการของผู้ออกใบรับรองหรือผู้ที่สร้างหรือใช้ลายมือชื่ออิเล็กทรอนิกส์
2. ใบรับรองที่ออกโดยผู้ประกอบการรับรองในต่างประเทศจะมีผลทางกฎหมายเช่นเดียวกันกับใบรับรองที่ออกโดยผู้ประกอบการรับรองในประเทศ หากระดับของความน่าเชื่อถือของใบรับรองดังกล่าว มีระดับความน่าเชื่อถือที่เท่าเทียมกันอย่างแท้จริง (substantially equivalent level of reliability) กับใบรับรองที่ออกโดยผู้ประกอบการรับรองในประเทศ
3. ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นหรือใช้ในต่างประเทศจะมีผลทางกฎหมายเช่นเดียวกันกับลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นหรือใช้ภายในประเทศ หากระดับของความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์ดังกล่าว มีระดับความน่าเชื่อถือที่เท่าเทียมกันอย่างแท้จริง กับลายมือชื่ออิเล็กทรอนิกส์ที่สร้างหรือใช้ภายในประเทศ
4. ในการพิจารณาว่าลายมือชื่ออิเล็กทรอนิกส์และใบรับรองใด มีระดับความน่าเชื่อถือที่เท่าเทียมกันอย่างแท้จริง (a substantially equivalent level of reliability) ตาม ข้อ 2. และ 3. จะต้องใช้มาตรฐานที่เป็นที่ยอมรับระหว่างประเทศ และปัจจัยอื่นๆ ที่เกี่ยวข้องในการพิจารณา
5. คู่กรณีมีอิสระที่ตกลงกันในเรื่องการใช้ลายมือชื่ออิเล็กทรอนิกส์หรือประเภทของใบรับรอง แม้ว่าจะเป็นกรณีที่เป็นการติดต่อระหว่างประเทศก็ตาม เว้นแต่ข้อตกลงดังกล่าวจะไม่ถูกต้องหรือไม่มีผลตามกฎหมายที่บังคับใช้อยู่

หลักการตามข้อ 1-5 นี้ ได้สนับสนุนหลักการไม่เลือกปฏิบัติ โดยในข้อ 1. เพื่อเป็นการยืนยันว่าสถานที่ที่ออกใบรับรอง หรือสถานที่ที่ใช้สร้างหรือใช้ลายมือชื่ออิเล็กทรอนิกส์จะไม่เป็นปัจจัยที่นำมาใช้พิจารณาความมีผลทางกฎหมาย ในส่วนของคำว่า "substantially equivalent level of reliability" ในข้อที่ 2. และ 3. นั้นบัญญัติขึ้นป้องกันการสร้างภาระที่ไม่มีเหตุผลในการรับรองหรือยอมรับ ใบรับรองที่ออกในต่างประเทศหรือลายมือชื่ออิเล็กทรอนิกส์ที่สร้างหรือใช้ในต่างประเทศทั้งยังเป็นการยอมรับถึงระดับความน่าเชื่อถือที่กำหนดในกฎหมายของแต่ประเทศ อย่างไรก็ตามมิได้หมายความว่าความน่าเชื่อถือจะต้องเป็นอย่างเดียวกันกับใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ในประเทศ แต่ใช้ระดับของความน่าเชื่อถือเป็นตัววัด และระดับของความน่าเชื่อถือดังกล่าวจะต้องเป็นระดับของความน่าเชื่อถือในใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ประเภทเดียวกัน

ในการประเมินระดับความน่าเชื่อถือที่เท่าเทียมกันอย่างแท้จริง (a substantially equivalent level of reliability) ในข้อ 2. และ 3. นั้น จะต้องใช้มาตรฐานที่เป็นที่ยอมรับระหว่างประเทศ ซึ่งมาตรฐานที่เป็นที่ยอมรับระหว่างประเทศ หมายความถึงมาตรฐานในทางเทคนิค ในทางการค้า และข้อปฏิบัติต่างๆ ที่ได้รับการยอมรับในระดับรัฐบาลระหว่างประเทศ หรืออาจเป็นถ้อยแถลงยอมรับข้อปฏิบัติในทางเทคนิค กฎหมาย และการค้า โดยที่มาตรฐานที่เป็นที่ยอมรับระหว่างประเทศดังกล่าวอาจอยู่ในรูปของข้อกำหนด ข้อแนะนำ ระเบียบปฏิบัติ ถ้อยแถลง หรือสิ่งอื่นที่มีลักษณะเดียวกัน เป็นต้น

ในส่วนข้อที่ 5. นั้นเพื่อเปิดกว้างให้แก่คู่กรณีหรือคู่สัญญาที่จะสามารถตกลงกันยอมรับลายมือชื่ออิเล็กทรอนิกสหรือใบรับรองแบบใดๆ หรือที่ออกหรือใช้ในประเทศอื่นๆ ซึ่งอาจจะแตกต่างไปจากที่มีในกฎหมาย รวมทั้งยังแสดงให้เห็นถึงเจตนาที่จะไม่สนับสนุนให้มีการบัญญัติข้อกำหนดใดๆ ในลักษณะที่เป็นการตายตัวว่าถ้าปฏิบัติตามข้อกำหนดดังกล่าวจึงจะมีผลหรือยอมรับว่าเป็นลายมือชื่อตามกฎหมาย อย่างไรก็ตามเว้นแต่ว่าข้อตกลงดังกล่าวจะไม่ถูกต้องหรือไม่มีผลบังคับใช้ตามกฎหมายที่ใช้บังคับอยู่ของประเทศนั้นๆ และข้อ 5. นี้จะไม่มีผลต่อสถานะในทางกฎหมายของบุคคลที่สาม (Third Parties)

3.5 ข้อพิจารณาอื่นเกี่ยวกับกฎหมายลายมือชื่อดิจิตอล

3.5.1 นโยบายเกี่ยวกับเทคโนโลยีการเข้ารหัส

เดิมเทคโนโลยีการเข้ารหัสถือเป็นเทคโนโลยีที่ใช้เฉพาะการทหาร อย่างไรก็ตามการประยุกต์ใช้เทคโนโลยีการเข้ารหัสในด้านอื่นๆ ในปัจจุบันทำให้เทคโนโลยีดังกล่าวพ้นสภาพจากการเป็นเทคโนโลยีด้านการทหารเพียงอย่างเดียว (Single use) มาสู่เทคโนโลยีที่สามารถใช้งานสองด้าน (Dual Use)[42] ทั้งด้านการทหารและด้านพลเรือน เทคโนโลยีการเข้ารหัสหลายๆ อย่างถูกจัดเป็นอาวุธยุทโธปกรณ์ (Munitions) แต่อย่างไรก็ตามในปัจจุบันภาคธุรกิจได้นำเทคโนโลยีการเข้ารหัสมาใช้ในการประกอบการพาณิชย์อิเล็กทรอนิกส์ เช่น ในการเข้ารหัสธุรกรรมซื้อขายสินค้าผ่านเครือข่าย Internet เพื่อป้องกันการถูกดักฟัง หรือทำการเข้ารหัสสัญญาณภาพของเคเบิลทีวีเพื่อป้องกันผู้ที่ไม่ใช่สมาชิกสามารถรับชมรายการต่างๆ ได้ เป็นต้น รวมทั้งการเข้ารหัสก็ยังเป็นส่วนหนึ่งของขบวนการในการลงลายมือชื่อหรือตรวจสอบลายมือชื่อดิจิตอลอีกด้วย

---

[42] Kurt M. Saunders, "The Regulation of Internet Encryption Technology: Separating The Wheat from The Chaff", John Marshall Journal of Computer & Information Law, Vol.XVII, Number 3, Spring 1999, p.950

การที่เทคโนโลยีดังกล่าวกลายเป็นเทคโนโลยีที่สามารถนำมาใช้ทั้งทางด้านการทหารและด้านพลเรือนทำให้เกิดปัญหาว่า จะสร้างความสมดุลย์ระหว่างการความสามารถของรัฐในการคุ้มครองประชาชนจากภัยคุกคามต่างๆ กับการคุ้มครองความเป็นส่วนตัว (Privacy) และเสรีภาพในการสื่อสารของประชาชน ตลอดจนความมั่นใจในการดำเนินธุรกิจอย่างไร กล่าวคือหากรัฐมีนโยบายให้ประชาชนและภาคธุรกิจสามารถใช้เทคโนโลยีการเข้ารหัสโดยเสรี รัฐอาจประสบปัญหาในการในการบังคับใช้กฎหมายเพื่อตรวจจับการสื่อสารของอาชญากร ผู้ก่อการร้าย หรือรัฐบาลของประเทศที่เป็นศัตรู ซึ่งจะใช้เทคโนโลยีการเข้ารหัสในการสื่อสารกัน ในทางตรงกันข้ามการรัฐมีนโยบายในการควบคุมการใช้เทคโนโลยีการเข้ารหัสที่เข้มงวด ก็จะปิดโอกาสของภาคธุรกิจและประชาชนในการใช้ประโยชน์จากเทคโนโลยีดังกล่าว รวมทั้งเป็นการละเมิดต่อสิทธิขั้นพื้นฐานของประชาชน คือความเป็นส่วนตัวและเสรีภาพในการสื่อสารของประชาชน[43]

ประเทศต่างๆ ได้แก้ไขปัญหานี้โดยอนุญาตให้ประชาชนมีเสรีภาพในการใช้เทคโนโลยีการเข้ารหัส แต่กำหนดให้รัฐสามารถเข้าถึงและถอดรหัสข้อมูลที่ทำการเข้ารหัสได้โดยชอบด้วยกฎหมายหรือที่เรียกกันว่า "การเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยหน่วยงานของรัฐ" (lawful State access)[44] ในสภาพแวดล้อมบางอย่าง เช่น เมื่อมีข้อสงสัยว่าการสื่อสารที่เข้ารหัสดังกล่าวจะเป็นการสื่อสารเพื่อกระทำการอันเป็นการผิดหรือละเมิดกฎหมาย เช่น เป็นการสื่อสารเพื่อการฟอกเงิน การหลบเลี่ยงภาษี หรือการก่อการร้าย เป็นต้น นโยบายที่ใช้ในการควบคุมการผลิต การใช้ประโยชน์ การส่งออกหรือนำเข้าเทคโนโลยีการเข้ารหัสนี้เรียกว่า "นโยบายเกี่ยวกับเทคโนโลยีการเข้ารหัส"(Encryption Policy)

ในประเทศอื่นโดยเฉพาะประเทศอุตสาหกรรมในคะวันตกส่วนใหญ่จะไม่มีข้อจำกัดในการนำเข้าเทคโนโลยีการเข้ารหัส แต่จะมีข้อจำกัดในการส่งออกเทคโนโลยีการเข้ารหัสที่มีความแข็งแกร่งมากๆ เช่น ประเทศสหรัฐอเมริกา การส่งออกเทคโนโลยีการเข้ารหัสแต่เดิมอยู่ถูกห้ามการส่งออกภายใต้ Export Administration Regulation (EAR) แต่ในปี ค.ศ. 1996 เทคโนโลยีการเข้ารหัสถูกย้ายจากรายชื่ออาวุธยุทโธปกรณ์ของ Arms Export Control Act (AECA) ไปสู่รายชื่อควบคุมของภายใต้ Export Administration Act (EAA)[45] ปัจจุบันเทคโนโลยีการเข้ารหัสทั้งหมดดูแลโดย Commerce Department ยกเว้นในส่วนของการพัฒนาเพื่อใช้ในกิจการทหาร[46]

---

[43] สมเกียรติ ตั้งกิจวานิชย์, รายงานการวิจัยเรื่อง ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง. สถาบันวิจัยเพื่อการพัฒนาประเทศไทย. หน้า 25

[44] เรื่องเดียวกัน, หน้า 25

[45] โปรดดู Exec. Order No.13,026, 61 Fed.Reg. 58,767, 68,572 (1996) refer in Kurt M. Saunders, Id., p. 950

[46] Kurt M. Saunders, Id., p. 950

นอกเหนือจากการส่งออกหรือนำเข้าแล้ว วิธีการในการควบคุมเทคโนโลยีการเข้ารหัสอื่นๆ คือ การจำกัดความยาวของกุญแจรหัส (Key Length) ที่สามารถใช้ได้ การจำกัดความยาวของกุญแจรหัสที่สามารถใช้ได้นี้ทำให้รัฐหรือหน่วยงานของรัฐสามารถทำการถอดรหัสข้อมูลที่ต้องการทำการตรวจสอบได้โดยการใช้เครื่องคอมพิวเตอร์ที่มีสมถณะสูงๆในการถอดรหัส อย่างไรก็ตามการควบคุมโดยวิธีการนี้จะทำให้ระบบการเข้ารหัสข้อมูลโดยรวมมีประสิทธิภาพต่ำลงและเสี่ยงต่อการถูกผู้อื่นนอกจากรัฐหรือหน่วยงานของรัฐถอดรหัสด้วยวิธีการเดียวกัน เพราะยิ่งใช้กุญแจรหัสที่มีขนาดยาวเท่าไรในการเข้ารหัสก็จะยิ่งมีความปลอดภัยสูงเท่านั้น เพราะฉะนั้นการควบคุมเทคโนโลยีการเข้ารหัสโดยการอนุญาตให้ใช้เทคโนโลยีการเข้ารหัสที่มีความแข็งแกร่ง (strong Encryption) แต่กำหนดให้มีระบบการฝากเก็บกุญแจรหัส (Key Escrow) หรือระบบการกู้กุญแจรหัส (Key Recovery) จึงเป็นอีกทางเลือกหนึ่ง นอกจากนี้ระบบการเก็บหรือการกู้กุญแจรหัสยังเป็นสิ่งที่ภาคธุรกิจและผู้ใช้โดยทั่วไปมักมีความต้องการอยู่แล้ว เพื่อให้มีหลักประกันว่าตนสามารถถอดรหัสข้อมูลในกรณีที่ทำกุญแจรหัสสูญหายหรือในกรณีที่พนักงานที่เป็นผู้เก็บกุญแจรหัสลาออกหรือเสียชีวิต โดยยังไม่ได้ส่งมอบกุญแจรหัสดังกล่าวให้แก่ผู้ที่มีอำนาจ จึงดูเหมือนว่าวิธีการนี้จะเป็นวิธีการที่เหมาะสมกว่า อย่างไรก็ตามระบบการฝากกุญแจรหัสและระบบการกู้กุญแจรหัสดังกล่าว ประเทศสหรัฐอเมริกาในเคยนำมาใช้ในช่วงต้นปี 1996 และปี 1997 ตามลำดับ แต่ถูกต่อต้านอย่างรุนแรงจากองค์กรสิทธิมนุษยชนต่างๆ ภายในประเทศ รวมทั้งจากประชาชนด้วยเหตุผลว่ามาตรการดังกล่าวเป็นการละเมิดสิทธิความเป็นส่วนตัว (privacy) และเสรีภาพในการแสดงออก (free speech) ของประชาชน ซึ่งเป็นการขัดต่อรัฐธรรมนูญของประเทศสหรัฐอเมริกาในส่วนของ First Amendment และ Fifth Amendment ตามลำดับ

ในฐานะที่ประเทศไทยมิใช่ประเทศผู้ผลิตเทคโนโลยีการเข้ารหัส การเปิดกว้างให้ประชาชนและภาคธุรกิจสามารถเลือกใช้เทคโนโลยีการเข้ารหัสได้ตามความต้องการ โดยไม่มีข้อจำกัดในเรื่องของการนำเข้าและการใช้ภายในประเทศน่าจะเป็นผลดี ทั้งยังเอื้ออำนวยให้เกิดการรับนวัตกรรมทางเทคโนโลยีใหม่ๆ จากต่างประเทศ และส่งเสริมการใช้เทคโนโลยีดังกล่าวในการพาณิชย์อิเล็กทรอนิกส์ อย่างไรก็ตามในอนาคตหน่วยงานทางด้านความมั่นคงและหน่วยงานที่บังคับใช้กฎหมายต่างๆ อาจเล็งเห็นถึงความจำเป็นในการควบคุมเทคโนโลยีการเข้ารหัส โดยเฉพาะในเรื่องของการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย เพื่อป้องกันการก่อการร้าย อาชญากรรม หรือการละเมิดกฎหมายอื่นๆ ซึ่งการควบคุมเทคโนโลยีการเข้ารหัสนี้จะต้องคำนึงถึงบทบัญญัติในมาตรา 37 ของรัฐธรรมนูญฉบับปัจจุบันคือ

"บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบด้วยกฎหมาย การตรวจ การกักหรือการเปิดเผยสิ่งสื่อสารที่บุคคลมีติดต่อถึงกันรวมทั้งการกระทำด้วยประการอื่นใดเพื่อให้ล่วงรู้ถึงข้อความในสิ่งสื่อสารทั้งหลายที่บุคคลมีติดต่อถึงกันจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตาม

บทบัญญัติแห่งกฎหมายเฉพาะเพื่อรักษาความมั่นคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน"

จะเห็นได้ว่าเจตนารมย์ของบทบัญญัติดังกล่าวคือ การรับประกันเสรีภาพในการสื่อสารและความเป็นส่วนตัวของประชาชน อย่างไรก็ตามมาตราดังกล่าวมิได้ห้ามให้รัฐกำหนดนโยบายเทคโนโลยีการเข้ารหัสเพื่อประโยชน์ในการรักษาความมั่นคงของรัฐ ความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ซึ่งอาจตีความได้ว่ารัฐธรรมนูญมิได้ปิดกันการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายของหน่วยงานของรัฐ อย่างไรก็ตามเพื่อคุ้มครองเสรีภาพในการสื่อสารของประชาชนและส่งเสริมการใช้เทคโนโลยีการเข้ารหัสในการพาณิชย์อิเล็กทรอนิกส์ การเข้าถึงข้อมูลโดยชอบด้วยกฎหมายของรัฐควรมีแนวทางดังต่อไปนี้

1. กำหนดขอบเขตการแทรกแซงของรัฐเฉพาะในกรณีการใช้เทคโนโลยีการเข้ารหัสในการรักษาความลับ (Confidentiality) ของข้อมูลเท่านั้น โดยไม่ให้รัฐแทรกแซงการใช้เทคโนโลยีการเข้ารหัสในการระบุตัวบุคคล (Authentication) หรือรักษาความถูกต้องของข้อมูล (Integrity)
2. กำหนดหลักเกณฑ์ที่ชัดเจนในการอนุญาตให้รัฐเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย เช่น ให้ทำได้ต่อเมื่อได้รับคำสั่งหรือหมายศาลเท่านั้น[47]
3. กำหนดระยะเวลาที่แน่นอนในการอนุญาตให้รัฐเข้าถึงข้อมูลโดยชอบด้วยกฎหมายและอนุญาตให้เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้องกับเรื่องที่ต้องการตรวจสอบเท่านั้น
4. กำหนดให้บุคคลซึ่งช่วยเหลือรัฐในการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย เช่น ผู้รักษากุญแจรหัสส่วนตัวที่เกี่ยวข้องไม่มีความผิดจากการกระทำดังกล่าว
5. วางระบบตรวจสอบที่มีความโปร่งใส เช่น กำหนดให้มีการเก็บบันทึกการเข้าถึงโดยชอบด้วยกฎหมายเพื่อให้สามารถตรวจสอบภายนอกได้

3.5.1.1 ตัวอย่างนโยบายการเข้ารหัสของประเทศต่างๆ

ตามกฎหมายของประเทศสหรัฐอเมริกาเทคโนโลยีการเข้ารหัสถือเป็นสินค้ายุทโธปกรณ์ การส่งออกเทคโนโลยีดังกล่าวถูกควบคุมด้วยกฎหมายว่าด้วยการค้าอาวุธ (Defense Trade Regulation) ซึ่งเดิมเรียกว่ากฎหมายการค้าอาวุธระหว่างประเทศ (International Traffic in

---

[47] สมเกียรติ ตั้งกิจวานิชย์, รายงานการวิจัยเรื่อง ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง. สถาบันวิจัยเพื่อการพัฒนาประเทศไทย. หน้า 30

ข้อเสนอดังกล่าวมีเนื้อหาคล้ายกับบทบัญญัติในมาตราที่ 238 ของรัฐธรรมนูญที่ว่า "ในคดีอาญา การค้นในที่รโหฐานจะกระทำมิได้ เว้นแต่จะมีคำสั่งหรือหมายของศาล หรือมีเหตุให้ค้นได้โดยไม่ต้องมีคำสั่งหรือหมายของศาล ทั้งนี้ ตามที่กฎหมายบัญญัติ"

Arms Regulation หรือ TRAR) กฎหมายดังกล่าวกำหนดให้การส่งออกเทคโนโลยีการเข้ารหัสจะกระทำได้ก็ต่อเมื่อได้รับใบอนุญาตจากกระทรวงพาณิชย์ของสหรัฐ (Ministry of Commerce) เท่านั้น อย่างไรก็ตามในระยะหลังรัฐบาลสหรัฐอเมริกาเริ่มตระหนักว่านโยบายดังกล่าวไม่เป็นผลดีต่ออุตสาหกรรมคอมพิวเตอร์ของสหรัฐเอง โดยจะกลายเป็นการผลักดันให้ผู้ประกอบการของสหรัฐต้องย้ายฐานการผลิตไปต่างไปประเทศที่มีนโยบายที่ผ่อนคลายกว่า จึงได้เริ่มผ่อนคลายข้อจำกัดดังกล่าวลงจนในที่สุดยินยอมให้ผู้ผลิตสามารถส่งออกเทคโนโลยีการเข้ารหัสที่มีความยาวของกุญแจรหัสไม่เกิน 40 บิท และ 56 บิท ในกรณีการส่งออกเพื่อการใช้ในสถาบันหรือธุรกรรมการเงิน ต่อมาในเดือนกันยายน ค.ศ. 1999 รัฐบาลสหรัฐได้ผ่อนคลายกฎระเบียบในการส่งออกอีกครั้งหนึ่ง โดยลดข้อจำกัดในการส่งออกผลิตภัณฑ์เทคโนโลยีการเข้ารหัสที่มีความยาวของกุญแจรหัสไม่เกิน 64 บิท โดยให้ผู้ส่งออกขออนุญาตกระทรวงพาณิชย์ครั้งเดียวสำหรับผลิตภัณฑ์แต่ละรุ่น ส่งผลิตภัณฑ์เทคโนโลยีการเข้ารหัสที่มีความยาวกุญแจรหัสเกิน 64 บิท ก็จะสามารถส่งออกได้เป็นกรณีพิเศษ หากเป็นเทคโนโลยีที่ออกแบบให้ใช้กับผู้ใช้ทั่วไป (End User) ที่ไม่ต้องการการสนับสนุนทางเทคนิคมาก และประเทศที่ส่งออกต้องไม่ใช่ประเทศที่อยู่ในบัญชีรายชื่อต้องห้าม[48]

ส่วนในประเทศแคนาดาไม่มีข้อจำกัดในการส่งออกเทคโนโลยีการเข้ารหัสใดๆ ไปยังสหรัฐอเมริกา นอกจากนี้ยังไม่มีข้อจำกัดใดๆ ในเรื่องการนำเข้าและการใช้เทคโนโลยีการเข้ารหัสภายในประเทศ อย่างไรก็ตามแคนาดามีนโยบายการควบคุมการส่งออกเทคโนโลยีการเข้ารหัสเช่นเดียวกันกับสหรัฐ ในอดีตแคนาดาเคยอนุญาตให้ส่งออกเทคโนโลยีการเข้ารหัสที่มีความยาวของกุญแจรหัสไม่เกิน 40 บิทเท่านั้น ยกเว้นสถาบันการเงินต่างๆ ได้รับอนุญาตให้ส่งออกเทคโนโลยีการเข้ารหัสแบบ DES (Data Encryption Standard) ซึ่งเป็นการเข้ารหัสแบบสมมาตรซึ่งใช้กุญแจรหัสเดียวในการเข้ารหัสและถอดรหัส ที่มีความยาวกุญแจรหัสไม่เกิน 56 บิทได้ ต่อมาในปี 1996 แคนาดาได้ทดลองเปิดการส่งออกเทคโนโลยีการเข้ารหัสที่มีความยาวกุญแจรหัสไม่เกิน 56 บิทไปยังประเทศต่างๆ เป็นการทั่วไป[49]

แผนภูมิที่ 3.1 ในหน้าต่อไปจะเป็นบทสรุปข้อจำกัดในการใช้ การส่งออกและนำเข้าเทคโนโลยีการเข้ารหัสของประเทศต่างๆ บางประเทศ

---

[48] สมเกียรติ ตั้งกิจวานิชย์, รายงานการวิจัยเรื่อง ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง, สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, หน้า 27-28

[49] เรื่องเดียวกัน, หน้า 28

ประเทศ	ข้อจำกัดในการส่งออก-นำเข้า	ข้อจำกัดในการใช้ในประเทศ
ออสเตรเลีย	ต้องขออนุญาตเป็นรายลักษณ์อักษรในการส่งออกอุปกรณ์และซอฟต์แวร์ที่ใช้เทคโนโลยีการเข้ารหัส	ไม่มีข้อจำกัด
แคนาดา	เป็นไปตามข้อตกลงวัสเซนนาร์ ไม่มีข้อจำกัดในการส่งออกหรือนำเข้าจากสหรัฐอเมริกา	ไม่มีข้อจำกัด
ฝรั่งเศส	ต้องสำแดงอุปกรณ์ที่รักษาความถูกต้อง (Authentication only or Integrity only) และต้องขออนุญาตนำเข้าหรือส่งออกอุปกรณ์ที่ใช้เทคโนโลยีการเข้ารหัสอื่นๆ	สามารถใช้การเข้ารหัสในการรักษาความลับได้หากมีการเก็บกุญแจรหัสไว้กับบุคคลที่สามที่เชื่อถือได้ การใช้งานอื่นๆ เช่นเพื่อรับรอง และระบุตัวบุคคลไม่มีข้อจำกัด
ญี่ปุ่น	เป็นไปตามข้อตกลงวัสเซนนาร์ และการส่งออกเกินกว่า 5 หมื่นหน่วยต้องขออนุญาตเป็นพิเศษ	ไม่มีข้อจำกัด
สิงค์โปร์	ไม่ทราบแน่ชัด	การเข้ารหัสโดยฮาร์ดแวร์ (hardware encryption) จะต้องได้รับอนุญาตก่อน
เกาหลีใต้	ห้ามการนำเข้าและส่งออก	ไม่ทราบแน่ชัด
สหรัฐอเมริกา	ห้ามการส่งออกเทคโนโลยีการเข้ารหัสที่มีขีดความสามารถสูง	ไม่มีข้อจำกัด
ปากีสถาน	ไม่มีข้อจำกัด	ห้ามการเข้ารหัสเสียง (Voice-encryption)
รัสเซีย	ต้องมีใบอนุญาตในการส่งออกหรือนำเข้า	ห้ามการเข้ารหัสโดยไม่ได้รับอนุญาต
จีน	ห้ามนำเข้าและส่งออกอุปกรณ์ที่เข้ารหัสเสียง (Voice-encryption device)	ไม่ทราบแน่ชัด

แผนภูมิ 3-1[50] : นโยบายการเข้ารหัสของประเทศต่างๆ

---

[50] ที่มา: สมเกียรติ ตั้งกิจวานิชย์, รายงานการวิจัยเรื่อง ลายมือชื่ออิเล็กทรอนิกส์และองค์กรออกใบรับรอง, สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, หน้า 32

3.5.2 นโยบายเกี่ยวกับเทคโนโลยีลายมือชื่อดิจิตอล

ในขั้นต้นต้องทำความเข้าใจก่อนว่าเทคโนโลยีลายมือชื่อดิจิตอลไม่ใช่เทคโนโลยีการเข้ารหัส ตามที่ได้อธิบายถึงเทคโนโลยีลายมือชื่อมาแล้วในบทที่ 2 เทคโนโลยีลายมือชื่อดิจิตอลใช้การเข้ารหัสแบบกุญแจรหัสสาธารณะเป็นส่วนหนึ่งของขบวนการรักษาความปลอดภัย (security) และตรวจสอบความถูกต้องแท้จริง (Authentication) ในการติดต่อระหว่างเครือข่าย เพราะฉะนั้นการเข้ารหัสและความปลอดภัยจึงเป็นเรื่องสำคัญต่อขบวนการลงลายมือชื่อและตรวจสอบลายมือชื่อดิจิตอล จุดประสงค์หลักของลายมือชื่อดิจิตอล คือ สร้างความมั่นใจในเรื่องของตัวบุคคลผู้ทำการส่งข้อมูลและข้อมูลจะไม่ถูกแก้ไขเปลี่ยนแปลงภายหลังการลงลายมือชื่อ รวมทั้งยังมีความสำคัญต่อการป้องกันการปฏิเสธความรับผิดอีกด้วย ซึ่งจุดประสงค์เหล่านี้มิได้มีผลกระทบต่อความปลอดภัยของประเทศหรือวัตถุประสงค์ในการบังคับใช้กฎหมาย เพราะการเข้ารหัสมิได้ถูกใช้ในฐานะของการรักษาความลับ แต่เป็นเพียงส่วนหนึ่งของขบวนการลงลายมือชื่อหรือตรวจสอบลายมือชื่อเท่านั้น จากข้อจำกัดในการใช้และคุณสมบัติที่สามารถตามหาตัวผู้ใช้ได้ของการเข้ารหัสที่ใช้ในเทคโนโลยีลายมือชื่อดิจิตอล ความกังวลเกี่ยวกับการที่อาชญากรหรือผู้ก่อการร้ายจะนำการเข้ารหัสในเทคโนโลยีลายมือชื่อดิจิตอลมาใช้จึงน่าที่จะมากเกินไป[51] ด้วยเหตุนี้เงื่อนไขเบื้องต้นที่สำคัญในการร่างนโยบายลายมือชื่อดิจิตอลคือ ความชัดเจน ความเข้าใจและรู้ถึงความแตกต่างของการใช้เทคโนโลยีการเข้ารหัสที่ไม่เป็นอันตรายในเทคโนโลยีลายมือชื่อดิจิตอล

อย่างไรก็ตามการเข้ารหัสก็เป็นส่วนหนึ่งของเทคโนโลยีลายมือชื่อดิจิตอล เป้าประสงค์ของนโยบายระดับชาติจึงต้องเผชิญหน้ากับประเด็นในเรื่องของระบบ Key Recovery ถ้าจุดประสงค์ของระบบ Key Recovery คือความสามารถที่จะถอดรหัสข้อมูลอิเล็กทรอนิกส์ที่น่าสงสัย ความกังวลดังกล่าวในส่วนของเทคโนโลยีลายมือชื่อดิจิตอลควรที่จะน้อยที่สุด เพราะข้อมูลที่ทำการลงลายมือชื่อดิจิตอลมีคุณสมบัติในการระบุและติดตามผู้ทำการลงลายมือชื่อได้เช่นเดียวกันกับการลงลายมือชื่อ (Hand-written Signature) ในกระดาษ ยิ่งไปกว่านั้นจากคุณสมบัติในการติดตามที่มีมาตั้งแต่ต้นของลายมือชื่อดิจิตอล จะเป็นตัวขัดขวางที่สำคัญที่อาชญากรหรือผู้ก่อการร้ายจะนำเทคโนโลยีดังกล่าวไปใช้ แม้ว่าการสร้างการเข้ารหัสที่แข็งแกร่งเพื่อนำไปใช้ในเทคโนโลยีลายมือชื่อดิจิตอล จะเป็นผลให้อาชญากรหรือผู้ก่อการร้ายสามารถเข้าถึงการเข้ารหัสที่แข็งแกร่งได้ แต่ในทางปฏิบัติบุคคลเหล่านั้นก็สามารถที่จะจัดหาเทคโนโลยีการเข้ารหัสที่แข็งแกร่งจากประเทศอื่นหรือโดยวิธีการอื่นได้ การจำกัดการส่งออกเทคโนโลยีการเข้ารหัสที่แข็งแกร่งหรือการวางเงื่อนไขให้มีการสร้างระบบ Key Recovery จะเป็นการขยายความหวาดหวั่นของสาธารณะชนต่อขบวนการ

---

[51] Raneta Lawson Mack, "Digital Signature, The Electronic Economy and The Protection of National Security: Some Distinction with An Economic Difference", John Marshall Journal of Computer & Information Law, Vol.XVII, Number 3, Spring 1999, p.998

และขัดขวางการเข้าสู่การพาณิชย์อิเล็กทรอนิกส์ เพราะเหตุผลในเรื่องของความปลอดภัยเล็กน้อยของประเทศ[52] และเมื่อพิจารณาจากความจริงที่ว่าผู้ใช้เทคโนโลยีลายมือชื่อดิจิตอลส่วนใหญ่เป็นผู้ที่ปฏิบัติตามกฎหมาย ต้นทุนและข้อจำกัดในทางเลือกที่ลดลงของระบบ Key Recovery จะเป็นประโยชน์ต่อการใช้เทคโนโลยีลายมือชื่อดิจิตอลในการติดต่อผ่านทางเครือข่าย อีกทางเลือกหนึ่งก็คือการสร้างข้อจำกัดการเข้ารหัสในเทคโนโลยีลายมือชื่อดิจิตอล โดยให้สามารถใช้ได้ในจุดประสงค์เฉพาะการตรวจสอบความถูกต้องแท้จริง (Authenticating) และการตรวจสอบ (Verifying) ของการใช้ลายมือชื่อดิจิตอลเท่านั้น ซึ่งจะทำให้อาชญากรและผู้ก่อการร้ายไม่สามารถนำการเข้ารหัสที่ใช้ในเทคโนโลยีลายมือชื่อดิจิตอลไปใช้รักษาความลับได้

นับจากที่เทคโนโลยีลายมือชื่อดิจิตอลถูกใช้ในการตรวจสอบความถูกต้องแท้จริง (Authenticate) และการตรวจสอบ (Verify) ในการระบุตัวบุคคลหรือองค์กรผู้ทำการติดต่อ การขยายตัวและการแพร่กระจายของเทคโนโลยีลายมือชื่อดิจิตอลต้องอาศัยการสร้างองค์กรอิสระที่จะรับประกันหรือรับรองการระบุตัวผู้ถือคู่กุญแจรหัส และเพื่อการเสริมสร้างความน่าเชื่อถือและส่งเสริมให้ใช้เทคโนโลยีลายมือชื่อดิจิตอลแทนการลงลายมือชื่อ (Hand-written Signature) ในกระดาษ จึงต้องสร้างความมั่นใจในเรื่องของความสมบูรณ์และการเป็นเจ้าของลายมือชื่อดิจิตอล ผู้ประกอบการรับรอง (Certification Authority) จึงเป็นเครื่องมือที่สำคัญในการพัฒนาและการยอมรับทางกฎหมายของเทคโนโลยีลายมือชื่อดิจิตอล ผู้ประกอบการรับรองทำหน้าที่ในการตรวจสอบความถูกต้องแท้จริงของความเป็นเจ้าของกุญแจรหัสสาธารณะและทำการออกใบรับรองดิจิตอลเพื่อรับประกันการระบุตัวผู้ถือคู่กุญแจรหัสและความสมบูรณ์ของลายมือชื่อดิจิตอล* เพื่อสร้างความมั่นใจในตัวใบรับรองดิจิตอลว่าสามารถเชื่อถือได้ ผู้ประกอบการรับรองต้องกำหนดมาตรฐานขั้นต่ำในการตรวจสอบ การระบุตัวบุคคล และการออกใบรับรองดิจิตอล รวมทั้งต้องมีวิธีการเพื่อความปลอดภัยพื้นฐานในการป้องกันการฉ้อโกงหรือการทุจริต

กฎหมายที่เกี่ยวข้องกับเทคโนโลยีลายมือชื่อดิจิตอลจะต้องกำหนดมาตรฐานในการให้ใบอนุญาตแก่องค์กรสาธารณะ หน่วยงานราชการ หรือหน่วยงานเอกชนที่ต้องการจะเป็นผู้ประกอบการรับรอง ทั้งยังจะต้องกำหนดให้ผู้ประกอบการรับรองต่างๆจะต้องมีมาตรฐานที่แน่นอนและชัดเจนในการออกใบรับรอง เมื่อผู้ประกอบการรับรองเป็นส่วนสำคัญในการสร้างความมั่นใจให้แก่เทคโนโลยีลายมือชื่อดิจิตอล เพราะฉะนั้นนโยบายลายมือชื่อดิจิตอลควรที่จะกำหนดอย่างชัดเจนถึงประเด็นปัญหาในเรื่องที่ว่าผู้ประกอบการรับรองควรเป็นภาครัฐหรือเอกชน รวมทั้งประเด็น

---

[52] Raneta Lawson Mack, Id., p.999

* การรับประกันในบางกรณีหมายความว่า องค์กรผู้ออกใบรับรองมีหน้าที่ในทางกฎหมายที่จะรับประกันผู้ที่เข้าเกี่ยวข้องกับใบรับรองที่ออกโดยองค์กรผู้ออกใบรับรองดังกล่าวอย่างสมเหตุผล (Reasonable relies upon the digital certificate issued by the CA)

ปัญหาที่ว่าผู้ประกอบการรับรองควรเก็บรักษากุญแจรหัสส่วนตัวที่มีความเกี่ยวเนื่องกับกุญแจรหัสสาธารณะที่ตนออกหรือไม่ (สำหรับในกรณีที่ถูกองค์กรของรัฐ เช่น ศาล เรียกดูหรือเรียกให้ส่งกุญแจรหัสส่วนตัวดังกล่าวตามกฎหมาย)

นโยบายลายมือชื่อดิจิตอลควรที่จะกำหนดฐานะในทางกฎหมายของลายมือชื่อดิจิตอลอย่างชัดเจน เพื่อสนับสนุนการใช้เทคโนโลยีลายมือชื่อดิจิตอลควรที่จะให้ลายมือชื่อดิจิตอลมีผลและได้รับฐานะในทางกฎหมายเสมือนกับลายมือชื่อธรรมดา (Hand-written Signature) รวมทั้งผู้ทำธุรกรรมที่สื่อสารผ่านทางเครือข่ายต้องเข้าใจอย่างชัดเจนว่าธุรกรรมที่ลงลายมือชื่อดิจิตอลดังกล่าวมีผลผูกพันเสมือนหนึ่งการลงลายมือชื่อในเอกสารที่เป็นกระดาษ

ในประการสุดท้ายนโยบายลายมือชื่อดิจิตอลจะต้องกำหนดว่า ในสถานการณ์ใดที่รัฐหรือหน่วยงานของรัฐจะได้รับอำนาจที่จะเข้าถึงคู่กุญแจรหัสหรือข้อมูลอื่นในใบรับรองดิจิตอล ข้อกำหนดดังกล่าวนี้ขึ้นอยู่กับเขตอำนาจของรัฐและประเภทของข้อมูลที่รัฐหรือหน่วยงานของรัฐต้องการ ซึ่งจะต้องเป็นเรื่องที่มีความสำคัญหรือมีเหตุผลเหนือสิทธิพื้นฐานของประชาชน เพราะเมื่อรัฐหรือหน่วยงานของรัฐสามารถเข้าถึงคู่กุญแจรหัสได้ จะมีผลทำให้รัฐหรือหน่วยงานของรัฐสามารถที่จะปลอมแปลงลายมือชื่อของประชาชนได้ด้วยเช่นกัน รวมทั้งจะต้องตระหนักด้วยว่าการใช้เทคโนโลยีลายมือชื่อดิจิตอลส่วนใหญ่จะเป็นการใช้โดยบุคคลหรือหน่วยงานที่ปฏิบัติตามกฎหมาย

3.5.3 กฎหมายคุ้มครองผู้บริโภค

ในกฎหมายเกี่ยวกับลายมือชื่อดิจิตอล โดยเฉพาะที่ใช้รูปแบบในการร่างที่เน้นรูปแบบโครงสร้างของระบบกุญแจรหัสสาธารณะ (Public Key Infrastructure) นั้น จะต้องมีการกำหนดในเรื่องความรับผิดของแต่ละฝ่ายที่เกี่ยวข้องกับการใช้ลายมือชื่อดิจิตอล โดยเฉพาะความรับผิดของผู้ลงลายมือชื่อหรือผู้ถือใบรับรอง (Subscriber) และผู้ประกอบการรับรอง (Certification Authority) รวมไปถึงความรับผิดของผู้ประกอบการรับรองต่อผู้ใช้ใบรับรอง จากการที่ในการใช้ลายมือชื่อดิจิตอล ผู้ประกอบการรับรองคือบุคคลที่สามที่ไว้วางใจได้ (Trusted Third Party) ที่ทำหน้าที่เป็นผู้ออกใบรับรองของการตรวจสอบความถูกต้องแท้จริงของผู้ที่ทำธุรกรรมและความสมบูรณ์ของข้อมูลในธุรกรรม ซึ่งเป็นส่วนสำคัญที่ทำให้ระบบของลายมือชื่อดิจิตอลสามารถใช้งานได้และมีความน่าเชื่อถือ จึงทำให้กฎหมายเกี่ยวกับลายมือชื่อดิจิตอลได้มีการจำกัดความรับผิดของผู้ประกอบการรับรอง เพื่อเป็นแรงจูงใจให้มีผู้สนใจดำเนินกิจการเป็นผู้ประกอบการรับรอง รวมทั้งผู้ประกอบการรับรองเองยังสามารถจำกัดความรับผิดของตนต่อผู้ถือใบรับรองโดยผ่านทางสัญญาที่ได้ทำกับผู้ถือใบรับรอง และโดยระบุในถ้อยแถลงแนวทางปฏิบัติในการออกใบรับรอง (Certification Practice Statement or CPS) นอกจากนี้ยังสามารถจำกัดความรับผิดต่อผู้ใช้ใบรับรองในการระบุตัวผู้ถือใบรับรอง (Relying Party) โดยการระบุในใบรับรองเองหรือทำการระบุในนโยบายในการออกใบรับ

รอง ทำให้ผู้ถือใบรับรองและผู้ใช้ใบรับรองตกเป็นผู้มีความเสี่ยงสูงจากความรับผิดแบบสูงและไม่จำกัด อย่างไรก็ตามการประกอบการของผู้ประกอบการรับรองเป็นการให้บริการ ผู้ถือใบรับรองและผู้ใช้ใบรับรองถือเป็นผู้บริโภคผู้หนึ่งตามกฎหมายคุ้มครองผู้บริโภค จึงเกิดประเด็นปัญหาขึ้นว่าเป็นการถูกต้องหรือไม่ที่ผู้ประกอบการรับรองจะสามารถจำกัดความรับผิดของตน และถ่ายโอนความรับผิดต่างๆ ไปยังผู้ถือใบรับรองตามสัญญาหรือตามที่กฎหมายเกี่ยวกับลายมือชื่อดิจิตอลกำหนด ตัวอย่างที่สำคัญคือ The Utah Act ได้กำหนดให้ผู้ถือใบรับรองซึ่งเป็นผู้ใช้ลายมือชื่อดิจิตอลมีความเสี่ยงต่อความรับผิด โดยละทิ้งในเรื่องของความสำคัญของนโยบายการคุ้มครองผู้บริโภคไป

หลักการของกฎหมายคุ้มครองผู้บริโภคนั้น ในปัจจุบันไม่คำนึงถึงหลักความสัมพันธ์ในทางสัญญาของคู่กรณี (Privity Rule) เนื่องจากในบางกรณีผู้บริโภคอาจไม่ใช่คู่กรณีในสัญญาเสมอไป รวมทั้งผู้บริโภคซึ่งเป็นคู่กรณีในสัญญาเอง ก็เป็นฝ่ายที่ไม่มีอำนาจต่อรอง (Inequality of bargaining power)ในการทำสัญญา จึงทำให้ตกอยู่ในฐานะที่เป็นผู้เสียเปรียบ รวมไปถึงหลักกฎหมายซื้อขายเดิมที่ว่าผู้ซื้อต้องระวัง (Caveat Emptor) ก็กลับกลายเป็นผู้ขายต้องเป็นฝ่ายใช้ความระมัดระวัง (Caveat Venditor) ตลอดจนภาระการพิสูจน์ความบกพร่องในทางละเมิดของการผลิต ซึ่งโดยปรกติฝ่ายที่กล่าวอ้างซึ่งคือผู้บริโภคต้องเป็นผู้มีหน้าที่นำสืบ ก็กลับให้เป็นภาระการนำสืบของผู้ผลิต หรือใช้การมีบทสันนิษฐานความรับผิดในการผลิตขึ้น[53] รวมไปถึงการใช้หลักความรับผิดเพราะการประกัน (Liability Based on Breach of Warranty) โดยกำหนดให้ผู้ผลิตหรือผู้จำหน่ายมีความรับผิดในคุณภาพของสินค้า หากผู้ผลิตหรือผู้จำหน่ายรับประกันในคุณภาพของสินค้าหรือความเหมาะสมของสินค้า เพื่อวัตถุประสงค์ใดโดยเฉพาะ และกรณีไม่เป็นไปตามที่รับประกัน โดยไม่ต้องพิจารณาถึงความประมาทเลินเล่อของผู้ผลิตหรือผู้จำหน่าย ความรับผิดดังกล่าวครอบคลุมถึงความเสียหายโดยตรง และในบางกรณีอาจรวมถึงความเสียหายซึ่งเกิดขึ้นเนื่องจากสาเหตุดังกล่าวด้วย ถ้าความเสียหายนั้นเกิดขึ้นจากการที่ทรัพย์นั้นขาดคุณสมบัติตามที่ผู้ผลิตรับประกันไว้ หรือการบรรยายสรรพคุณของสินค้าและพฤติการณ์อื่นๆ ที่ถือว่าเป็นการรับประกันคุณภาพของสินค้าโดยปริยาย ซึ่งหากสินค้าหรือผลิตภัณฑ์ขาดคุณภาพเช่นนั้นแล้ว ผู้เสียหายย่อมมีสิทธิเรียกร้องค่าสินไหมทดแทนได้[54]

---

[53] สุษม ศุภนิตย์, คำอธิบายกฎหมายคุ้มครองผู้บริโภค, (กรุงเทพมหานคร: สำนักพิมพ์จุฬาลงกรณ์มหาวิทยาลัย, 2536), หน้า ข.

[54] Bernhard Von Braunschweig, Product Liability: Federal Republic of Germany, p.8 อ้างถึงใน อิทธิพร แก้วทิพย์, "ปัญหาการบังคับใช้พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2522", (วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2538)

ตาม The Electronic Funds Transfer Act (EFTA) ที่เป็นกฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์จากหรือไปสู่บัญชีของผู้บริโภคของประเทศสหรัฐอเมริกา[55] และ Regulation E[56] ซึ่งคือกลุ่มของข้อบังคับซึ่ง The Federal Reserve System เป็นผู้ประกาศเพื่อปฏิบัติให้เป็นไปตาม EFTA[57] ซึ่ง EFTA และ Regulation E ได้กำหนดความรับผิดที่แน่นอนสำหรับสถาบันการเงินในกรณีที่เกิดความผิดพลาดหรือเหตุการณ์ผิดปรกติอื่นใดในการโอนเงินทางอิเล็กทรอนิกส์ และทำการจำกัดความรับผิดสำหรับความผิดพลาดที่เกิดโดยสุจริตและไม่ได้ตั้งใจ EFTA และ

---

55 15 U.S.C. 1693 §§ et seq.

56 12 C.F.R. pt. 205, "Electronic Funds Transfer"

57 Warwick Ford and Michael S. Baum, Id., p. 62

* ตามคำนิยามใน EFTA "Electronic Funds Transfer" คือ การโอนเงินใดใดนอกเหนือไปจากการโอนเงินด้วยเช็ค ดราฟต์ หรือตราสารอื่นที่สามารถโอนทำนองเดียวกัน โดยทางอิเล็กทรอนิกส์ ทางโทรศัพท์ หรือคอมพิวเตอร์ หรือเทปแม่เหล็กตามคำสั่งหรือการอนุญาตให้หักบัญชี หรือเครดิตบัญชีทั้งนี้ ให้รวมถึงคำสั่งโอนเงิน ณ จุดขาย การโอนด้วยเครื่อง ATM การฝากหรือถอนเงินโดยตรงและการโอนทางโทรศัพท์แต่ไม่รวมถึง 1)การรับรองเช็คใดใดหรือการบริการที่ไม่เกี่ยวกับการหักบัญชีหรือให้เครดิตโดยตรงต่อบัญชีของผู้ใช้บริการ 2) การโอนเงินใดใด นอกเหนือจากการดำเนินการโดยสำนักหักบัญชีอัตโนมัติของสถาบันการเงินแก่ผู้ใช้บริการโดยวิธีการโอนเงินของธนาคารกลางหรือสถาบันรับฝากอื่นๆ ที่มิได้มีไว้เพื่อการโอนเงินแก่ผู้ใช้บริการ 3)การโอนเงินใดที่ไม่ใช่เพื่อการซื้อหรือขายหลักทรัพย์หรือเครื่องอุปโภคผ่านตัวแทนที่จะทะเบียนในตลาดหลักทรัพย์ 4) การโอนเงินอัตโนมัติจากบัญชีออมทรัพย์หรือจากบัญชีเผื่อเรียกตามข้อตกลงระหว่างผู้ใช้บริการและสถาบันการเงินเพื่อสินเชื่อในบัญชีของผู้บริโภค หรือ 5) การโอนเงินใดใดโดยทางโทรศัพท์ระหว่างผู้ใช้บริการและเจ้าหน้าที่ หรือโดยพนักงานของสถาบันการเงิน ซึ่งเป็นไปตามแผนอันตกลงกันไว้แล้วและอยู่ภายใต้การโอนเป็นช่วงๆ หรือการโอนที่ไม่มีการไตร่ตรองมาก่อน กับได้ตกลงตามระเบียบของคณะกรรมการ (Electronic Fund Transfer Act 1978 S1693a.) ในเนื้อหาของ EFTA และ Regulation E ได้มีบทบัญญัติในการคุ้มครองผู้บริโภคและจัดสรรความรับผิดในของผู้ส่วนรวมในการพาณิชย์อิเล็กทรอนิกส์ รวมถึงสถาบันการเงินและผู้ถือ physical token เช่น ATM card หรือ Smart card เป็นต้น EFTA และ Regulation E กำหนดกฎเกณฑ์มาตรฐานเมื่อเกิดเหตุผิดปรกติเกี่ยวกับการจ่ายเงินในการพาณิชย์อิเล็กทรอนิกส์ โดยกำหนดให้มีการเปิดเผย (disclosure) และรวบรวม (Documentation) เกี่ยวกับความเสี่ยงเมื่อเกิดเหตุการณ์ผิดปรกติขึ้น รวมทั้งได้จัดทำวิธีการในการระงับข้อพิพาทอีกด้วย

Regulation E ได้กำหนดความรับผิดสำหรับการโอนเงินโดยไม่มีอำนาจ[58](unauthorized transfer) ของผู้บริโภคไว้ที่ $50 หรือผู้บริโภคจะต้องรับผิดเต็มจำนวนทั้งหมด ทั้งนี้ขึ้นอยู่กับเวลาที่ผู้บริโภคใช้ไปในการแจ้งต่อสถาบันการเงินภายหลังที่ access device ดังกล่าวได้ความสูญหายหรือถูกขโมยไป เว้นแต่ผู้บริโภคจะมิได้ 1. ทำการแจ้งโดยทันทีถึงความสูญหายหรือถูกขโมย (give timely notice of loss or theft) และ 2. รายงานถึงการโอนโดยไม่มีอำนาจที่เกิดขึ้นในรายงานสถานะทางการเงินภายในเวลาอันควร (report unauthorized transfers appearing on a periodic statement in a timely manner) โดยได้บัญญัติไว้ในมาตรา 1693g อย่างไรก็ตามหน้าที่ในการแจ้งแก่สถาบันการเงินนี้ EFTA และ Regulation E มิได้กำหนดให้เป็นหน้าที่ของผู้บริโภคในการดูแลรักษา access device แต่อย่างใด ข้อจำกัดความรับผิดดังกล่าว ผู้บริโภคจะไม่ได้รับประโยชน์ ถ้าได้มีการเขียนหรือจารึกหรือทำด้วยประการใดให้ปรากฏซึ่ง PIN หรือ Password บน Access device หรือวัตถุอื่นใดที่อยู่กับ Access device[59] ข้อกำหนดเกี่ยวกับการคุ้มครองผู้บริโภคใน EFTA และ Regulation E นี้มีนัยอย่างสำคัญต่อการพาณิชย์อิเล็กทรอนิกส์ และการใช้ลายมือชื่อดิจิตอล รวมไปถึงเครื่องมืออย่างอื่นเกี่ยวกับอำนาจในการใช้และการตรวจสอบความถูกต้องแท้จริง EFTA และ Regulation E จัดให้มีระเบียบมาตรฐานที่สำคัญที่เกี่ยวกับการเปิดเผยและรวบรวม กลุ่มของความเสี่ยงที่แตกต่างที่เกิดขึ้นในการพาณิชย์อิเล็กทรอนิกส์ ซึ่งต้องการวิธีการจัดสรรความรับผิดที่แตกต่างกัน

จากที่ได้พิจารณาข้างต้นจึงได้มีผู้เสนอให้มีการเปรียบเทียบความรับผิดของผู้ถือใบรับรอง (Subscriber) กับผู้บริโภคใน EFTA และ Regulation E โดยให้ถือว่าผู้ถือใบรับรองก็จัดเป็นผู้บริโภคผู้คนหนึ่ง จึงควรที่จะทำการจำกัดความรับผิดของผู้ถือใบรับรอง โดยใช้แนวความคิดของกฎหมายคุ้มครองผู้บริโภค เช่นเดียวกันกับ EFTA และ Regulation E โดยควรมีการวางข้อกำหนดเกี่ยวกับการจำกัดความรับผิดของผู้ถือใบรับรอง เพื่อเป็นการคุ้มครองผู้ถือใบรับรองในฐานะที่เป็นผู้บริโภคคนหนึ่ง ซึ่งอาจมีการวางเงื่อนไขหรือข้อกำหนดเบื้องต้นเอาไว้ก็ได้

ในส่วนของความรับผิดของผู้ประกอบการรับรองกับผู้ใช้ใบรับรอง (Relying Party) นั้น จากการศึกษาพบว่า กฎหมายเกี่ยวกับลายมือชื่อดิจิตอลได้กำหนดให้ผู้ประกอบการรับรองเป็นผู้รับประกันเนื้อหาในใบรับรองที่ตนออกว่าถูกต้องแท้จริง รวมไปถึงการรับประกันคุณภาพในส่วนอื่นของใบรับรอง ซึ่งจะได้อธิบายต่อไป โดยต้องระบุใน CPS หรือในใบรับรองว่าเนื้อหาส่วนใดของใบรับรองที่ตนให้การรับประกัน และส่วนใดไม่ให้การรับประกัน และในกรณีที่ไม่เป็นไปตามที่ได้ให้การรับประกันไว้ ผู้ประกอบการรับรองก็จะต้องรับผิด โดยไม่คำนึงว่าเป็นความประมาท

---

58 สังเกต ภู่กฤษณา, "ความรับผิดของธนาคารเกี่ยวกับการโอนเงินโดยเครื่องอิเล็กทรอนิกส์", (วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชานิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2540), หน้า 116

59 Warwick Ford and Michael S. Baum, Id., p. 63(footnote 145), 89

เลินเล่อของผู้ประกอบการรับรองหรือไม่ ซึ่งจะเห็นได้ว่าในส่วนนี้ได้มีการนำหลักกฎหมายคุ้มครองผู้บริโภคไปใช้เพื่อมุ่งคุ้มครองผู้ใช้ใบรับรองซึ่งเป็นผู้บริโภคผู้บริโภคผู้หนึ่ง

3.5.4 กฎหมายในเรื่องข้อสัญญาที่ไม่เป็นธรรม

จากการที่ผู้ประกอบการรับรองมีหน้าที่ในการออกใบรับรองเพื่อรับรองว่า ผู้ถือใบรับรองเป็นเจ้าของกุญแจส่วนตัวที่มีความเกี่ยวพันกับกุญแจรหัสสาธารณะที่ปรากฏในใบรับรอง ความสัมพันธ์ของผู้ประกอบการรับรองกับผู้ถือใบรับรองจึงเป็นความสัมพันธ์ในรูปของข้อตกลงหรือสัญญาระหว่างกันเป็นหลัก โดยผู้ประกอบการรับรองอยู่ในฐานะเป็นผู้ประกอบธุรกิจการค้าหรือวิชาชีพหรือผู้ให้บริการออกใบรับรองให้แก่ผู้ถือใบรับรองซึ่งอยู่ในฐานะเป็นผู้บริโภคหรือผู้รับบริการ ซึ่งข้อตกลงหรือสัญญาดังกล่าวนี้ก็จะต้องตกอยู่ภายใต้บทบัญญัติของกฎหมายเกี่ยวกับนิติกรรมสัญญาตามที่ได้บัญญัติไว้ในประมวลกฎหมายแพ่งและพาณิชย์ โดยที่หลักกฎหมายสัญญาที่บัญญัติไว้ในประมวลกฎหมายของทุกประเทศมีพื้นฐานของหลักเจตนาของบุคคลและหลักเสรีภาพในการทำสัญญา (Freedom of contract) ซึ่งเป็นหลักในการอธิบายว่าทำไมคู่สัญญาจึงต้องปฏิบัติตามสัญญา หรือสัญญาต้องเป็นสัญญา (pacta sun servanda)[60] หลักกฎหมายเหล่านี้เกิดขึ้นในคริสต์ศตวรรษที่ 19 ซึ่งเป็นช่วงที่สภาพของสังคมเศรษฐกิจในสมัยนั้น คู่สัญญามีความเสมอภาคเท่าเทียมกันที่จะต่อรองกำหนดเนื้อหาของสัญญาร่วมกัน การแสดงเจตนาของคู่สัญญาสามารถทำได้โดยเสรี[61] ด้วยเหตุนี้คู่สัญญาจะอ้างในภายหลังที่สัญญาเกิดขึ้นโดยความสมัครใจ โดยไม่มีการข่มขู่หรือสำคัญผิด หรือกลฉ้อฉล ว่าสัญญานั้นไม่ยุติธรรม อันตนไม่ควรต้องผูกพันหรือต้องปฏิบัติการชำระหนี้นั้นไม่ได้

อย่างไรก็ตามในปัจจุบัน สัญญาระหว่างผู้ให้บริการและผู้รับบริการได้ถูกพัฒนาแตกต่างไปจากเดิมมาก ทั้งรูปแบบของสัญญาและเนื้อหาในสัญญา ซึ่งสัญญาส่วนใหญ่จะอยู่ในรูปแบบของสัญญาสำเร็จรูป (Adhesion contract) หรือสัญญามาตรฐาน (standard form contract) ที่เกิดขึ้นจากการกำหนดเนื้อหาของสัญญาไว้ล่วงหน้าของผู้ให้บริการแต่เพียงฝ่ายเดียว ซึ่งเป็นคู่สัญญาฝ่ายที่มีอำนาจต่อรองในทางเศรษฐกิจและทางเทคนิคที่เหนือกว่า ความเสมอภาคระหว่างผู้ให้บริการและผู้รับบริการที่จะตกลงเนื้อหาความผูกพันร่วมกันเป็นรายกรณีได้สูญหายไป ความได้เปรียบของผู้ให้บริการจะเป็นตัวทำให้เกิดปัญหาในการกำหนดเนื้อหาของข้อสัญญา ในลักษณะที่เป็นการให้สิทธิยกเว้นหรือจำกัดความรับผิดของตน หรือตัดสิทธิของผู้รับบริการที่จะได้รับความคุ้มครองบางประการตามกฎหมายอย่างไม่เป็นธรรม ซึ่งเป็นผลมาจากการที่ผู้รับบริการที่มีอำนาจต่อรอง

---

[60] ดาราพร ถิระวัฒน์, กฎหมายสัญญา: สถานะใหม่ของสัญญาปัจจุบันและปัญหาข้อสัญญาที่ไม่เป็นธรรม. (กรุงเทพมหานคร: โรงพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2535), หน้า 1.

[61] ดาราพร ถิระวัฒน์. เรื่องเดิม. หน้า 2.

(bargaining power) ที่ด้อยกว่า ดังนั้นหลักของกฎหมายสัญญาที่บัญญัติไว้ในประมวลกฎหมายซึ่งมีลักษณะของปัจเจกชนนิยม* (individualism) ที่มีอิสระมีเสรีภาพในการทำสัญญาและอยู่บนพื้นฐานของหลักความศักดิ์สิทธิ์ของเจตนาจึงเริ่มที่จะเสื่อมคลายลง จากการที่สัญญาสำเร็จรูปหรือสัญญามาตราฐานเปิดโอกาสให้กำหนดข้อสัญญาที่เป็นประโยชน์แก่ผู้ร่างสัญญา (ผู้ให้บริการ) ไว้ล่วงหน้าเพื่อเป็นการบังคับแก่บุคคลที่เข้ามาเป็นคู่สัญญา (ผู้รับบริการ) ในภายหลัง เพราะไม่มีความเป็นอิสระและเจตนาของคู่สัญญาไม่มีความสำคัญ จากการที่ไม่มีการเจรจาต่อรองกันได้อย่างแท้จริงในระหว่างคู่สัญญา[62]

สัญญาสำเร็จรูปหรือสัญญามาตรฐานเป็นสัญญาที่มีลักษณะดังนี้[63]

1. เป็นสัญญาที่มีคู่สัญญาฝ่ายหนึ่งที่มีอำนาจทางเศรษฐกิจ (economic power) หรือมีความรู้ความสามารถทางเทคนิคเหนือกว่าหรือได้เปรียบกว่า ซึ่งอาจจะมีลักษณะของการผูกขาดในทางข้อเท็จจริงหรือในทางกฎหมายก็ได้
2. คู่สัญญาฝ่ายที่มีอำนาจเหนือกว่านี้เป็นผู้กำหนดข้อสัญญาที่เปลี่ยนแปลงไม่ได้และมีลักษณะเป็นเงื่อนไขทั่วไปที่กำหนดเนื้อหาสาระไว้ล่วงหน้า ซึ่งเป็นสัญญาที่ทำไว้จำนวนมาก เพื่อใช้กับบุคคลไม่จำกัดจำนวน และไม่จำกัดตัวผู้เข้าทำสัญญา
3. การกำหนดข้อสัญญาต่างๆ เป็นการทำขึ้นโดยฝ่ายเดียวหรืออาจเกิดจากบุคคลภายนอกเป็นผู้กำหนดให้หรือเป็นผู้ทำสัญญาขึ้น ซึ่งเป็นข้อกำหนดเงื่อนไขที่คู่สัญญาอีกฝ่ายหนึ่งมีหน้าที่เพียงจะต้องยอมรับข้อกำหนดที่ได้วางไว้แล้วนั้น หรือ

---

* ดาราพร ถิระวัฒน์. เรื่องเดิม. หน้า 13.

"หลักปัจเจกชนนิยม คือหลักที่ว่ารัฐจะต้องรับรู้สิทธิส่วนบุคคลให้มากที่สุดเท่าที่จะเป็นไปได้ รัฐจะต้องรับรองเสรีภาพส่วนบุคคลซึ่งมนุษย์ทุกคนมีอยู่ตามธรรมชาติ รัฐจะต้องไม่ทำลายสิทธิพื้นฐานของบุคคล บุคคลทุกคนมีเสรีภาพเว้นแต่ในบางเรื่องที่เป็นกรณีอันสมควร จึงจะมีข้อจำกัดเสรีภาพได้ นอกจากนั้นแล้วเสรีภาพของบุคคลจะถูกจำกัดลงได้ก็ด้วยความสมัครใจของบุคคลเองเท่านั้น ดังนั้นเจตนาของบุคคลจึงมีความศักดิ์สิทธิ์และอิสระ บุคคลจะไม่ถูกผูกพันในหนี้ใดที่เขาไม่ได้ตกลงยินยอมด้วยและในทางกลับกันหนี้ที่เกิดขึ้นจากเจตนาของบุคคลนี้จะผูกมัดบังคับแก่ผู้ที่ตกลงนั้น การมีเสรีภาพคือการที่บุคคลสามารถที่จะถูกบังคับด้วยตัวของตัวเองโดยเฉพาะการผูกมัดตัวเองด้วยสัญญาที่ทำขึ้น เสรีภาพจะไม่มีอยู่ ถ้าบุคคลไม่มีอำนาจเหนือตัวเองที่จะจำกัดตัวของตัวเองได้ เจตนาของบุคคลมีอำนาจที่จะก่อให้เกิดความผูกพันทางหนี้โดยเฉพาะเจาะจงในการเป็นลูกหนี้เจ้าหนี้ขึ้นมาได้"

[62] ดาราพร ถิระวัฒน์, เรื่องเดิม. หน้า 23.

[63] ดาราพร ถิระวัฒน์, เรื่องเดิม. หน้า 36.

ปฏิเสธไม่ต้องการทำสัญญาด้วยเลย เพราะไม่มีสิทธิที่จะแก้ไขเปลี่ยนแปลงข้อกำหนดในสัญญาได้ ซึ่งอาจกล่าวได้ว่าเนื้อหาของสัญญานี้ไม่ได้เกิดจากเจตนาที่แท้จริงของคู่สัญญาทั้งสองฝ่าย ไม่ได้เกิดจากการเจรจาต่อรองหรือตกลงกันอย่างแท้จริง

ซึ่งโดยปรกติแล้วในปัจจุบันสัญญาระหว่างผู้ให้บริการกับผู้รับบริการ หรือผู้ประกอบธุรกิจการค้าวิชาชีพกับผู้บริโภคก็จะเป็นสัญญาสำเร็จรูปหรือสัญญามาตรฐาน เช่น สัญญาระหว่างธนาคารกับผู้ถือบัตรเครดิต หรือสัญญาระหว่างธนาคารกับผู้ใช้บัตรบริการเงินด่วน (A.T.M.) เป็นต้น ในเรื่องดังกล่าวนอกจากกฎหมายคุ้มครองผู้บริโภคที่มีส่วนช่วยในการคุ้มครองและสร้างความเป็นธรรมให้แก่คู่สัญญาที่เป็นผู้บริโภคแล้ว ในแต่ละประเทศยังได้มีการบัญญัติกฎหมายพิเศษเพื่อนำมาปรับใช้สำหรับปัญหาข้อสัญญาที่ไม่เป็นธรรม โดยทำการบัญญัติออกมาเป็นกฎหมายพิเศษเพื่อเสริมกับหลักที่บัญญัติไว้ในกฎหมายแพ่งของตน ทั้งนี้เพื่อเป็นการยืนยันหลักความศักดิ์สิทธิ์ของเจตนา และหลักเสรีภาพในการทำสัญญา ซึ่งหลักทั้งสองในสัญญาสำเร็จรูปหรือสัญญามาตรฐานได้ถูกลดบทบาทลงหรือบางครั้งก็หายไป ดังนี้เจตนารมณ์สำคัญของการบัญญัติกฎหมายเฉพาะในเรื่องข้อสัญญาไม่เป็นธรรม ก็เพื่อจะให้รากฐานของกฎหมายสัญญาที่สำคัญทั้งสองหลักดังกล่าวกลับคืนมามีบทบาทสำคัญอย่างแท้จริง

ในส่วนของต่างประเทศยังมีตัวอย่างที่สำคัญอีกกรณีหนึ่ง คือ กรณีคดี ProCD v. Zeidenberg[64] โดยมีข้อเท็จจริงคือ ProCD คือบริษัทที่ขายผลิตภัณฑ์ CD-ROM* ที่รวบรวมข้อมูลในสมุดโทรศัพท์มากกว่า 3,000 เล่ม โดยเมื่อผู้ซื้อซื้อสินค้าไปจะต้องทำสัญญากับทางบริษัท ProCD จึงจะได้รับใบอนุญาตการใช้สินค้าดังกล่าวจากทาง ProCD โดยสัญญาดังกล่าวจะผูกพันผู้ซื้อทันทีที่กระทำการฉีกหีบห่อหรือพลาสติกที่เคลือบผลิตภัณฑ์ที่ซื้อ ซึ่งลักษณะสัญญาดังกล่าวนี้เรียกว่า "shrinkwrap license" ซึ่งข้อสัญญาในลักษณะนี้ศาลในคดีนี้พิจารณาว่า shrinkwrap license สามารถใช้บังคับได้เว้นแต่ข้อกำหนดในสัญญาดังกล่าวทำให้รู้สึกไม่ยอมรับหรือรับไม่ได้บนพื้นฐานความเป็นไปได้ของสัญญาปรกติ เช่น ขัดกับหลักกฎหมายหรือไร้เหตุผล เป็นต้น ซึ่งในคดีนี้ บริษัท ProCD ได้ทำการบรรจุ shrinkwrap license ไว้ในกล่องของผลิตภัณฑ์ ทำให้ผู้ซื้อไม่สามารถเห็นหรือรับรู้ข้อสัญญาได้ก่อนที่จะตกลงใจเข้าผูกพันในสัญญา เมื่อทำการฉีกพลาสติกหรือหีบห่อของผลิตภัณฑ์ดังกล่าวแล้ว ถือได้ว่าละเมิดข้อห้ามและผู้ซื้อก็ถือว่ายอมรับเข้าผูกพัน shrinkwrap license ทันที ซึ่งทำให้ผู้ซื้อเสียเปรียบและเสียโอกาสในการเลือกซื้อหาผลิตภัณฑ์ที่ตนต้องการ จึงทำให้ข้อสัญญาในลักษณะดังกล่าวใช้บังคับไม่ได้

---

[64] 86 F.3d 1447 (7th Cir. 1996)

* CD-ROM คือ compact disc-read only memory

ในส่วนของประเทศไทย เมื่อปี 2540 รัฐสภาก็ได้ให้ความเห็นชอบกับพระราชบัญญัติว่าด้วยข้อสัญญาที่ไม่เป็นธรรม พ.ศ. 2540 โดยพระราชบัญญัติฉบับนี้ไม่ใช้กับสัญญาทุกประเภท ไม่มีลักษณะเป็นหลักทั่วไปที่จะใช้กับสัญญาโดยทั่วไป แต่จะได้ระบุเฉพาะสัญญาบางประเภทที่จะอยู่ภายใต้กฎหมายฉบับนี้ ทั้งนี้โดยคำนึงถึงลักษณะสัญญาที่จะเป็นมูลเหตุให้เกิดการกำหนดข้อสัญญาที่ไม่เป็นธรรมดังนี้[65]

ก. <u>คำนึงจากประเภทของคู่กรณีที่เข้าเป็นคู่สัญญา</u> ได้แก่ สัญญาที่คู่สัญญาฝ่ายหนึ่งเป็นผู้บริโภค กับคู่สัญญาอีกฝ่ายหนึ่งเป็นผู้ประกอบธุรกิจการค้า หรือวิชาชีพ โดยได้ทำการจำกัดความหมายของคำว่า "ผู้บริโภค" และ "ผู้ประกอบธุรกิจการค้าหรือวิชาชีพ" ไว้ในมาตรา 4* ซึ่งความหมายของคำว่า "ผู้บริโภค" ในพระราชบัญญัติฉบับนี้จะแคบกว่าความหมายของคำว่าผู้บริโภค (consumers) โดยทั่วไป เพราะจะจำกัดเฉพาะบุคคลที่เกี่ยวข้องในนิติกรรมสัญญาบางประเภทเท่านั้น ส่วนความหมายของคำว่า "ผู้ประกอบธุรกิจการค้าหรือวิชาชีพ" ที่กฎหมายใช้คำว่าผู้ประกอบวิชาชีพ ไม่ใช่ผู้ประกอบอาชีพธรรมดา เนื่องจากธุรกิจในปัจจุบันบางประเภทมีลักษณะพิเศษต้องใช้ความรู้ความสามารถทางเทคโนโลยีเข้ามาด้วย ทำให้เกิดความไม่เท่าเทียมในการทำสัญญาธุรกิจขึ้นอันเป็นมูลเหตุทำให้เกิดข้อสัญญาที่ไม่เป็นธรรมกับคู่สัญญาที่เป็นผู้บริโภคอีกฝ่ายหนึ่ง

ข. <u>คำนึงจากลักษณะความไม่เท่าเทียมกันของคู่กรณี</u> ได้แก่ สัญญาที่คู่สัญญาฝ่ายหนึ่งมีอำนาจต่อรองในการทำสัญญาเหนือกว่าคู่สัญญาอีกฝ่ายหนึ่งอย่างมาก

---

[65] ดาราพร ถิระวัฒน์, <u>เรื่องเดิม</u>, หน้า 87-88.

* มาตรา 3 ในพระราชบัญญัตินี้

"**ผู้บริโภค**" หมายความว่า ผู้เข้าทำสัญญาในฐานะผู้ซื้อ ผู้เช่า ผู้เช่าซื้อ ผู้กู้ ผู้เอาประกันหรือผู้เข้าทำสัญญาอื่นใดเพื่อให้ได้มาซึ่งทรัพย์สิน บริการ หรือประโยชน์อื่นใดโดยมีค่าตอบแทน ทั้งนี้ การเข้าทำสัญญานั้นต้องเป็นไปโดยมิใช่เพื่อการค้า ทรัพย์สิน บริการ หรือประโยชน์อื่นใดนั้น และให้หมายความรวมถึงผู้เข้าทำสัญญาในฐานะผู้ค้ำประกันของบุคคลดังกล่าวซึ่งมิได้กระทำเพื่อการค้าด้วย

"**ผู้ประกอบธุรกิจการค้าหรือวิชาชีพ**" หมายความว่า ผู้เข้าทำสัญญาในฐานะผู้ขาย ผู้ให้เช่า ผู้ให้เช่าซื้อ ผู้ให้กู้ ผู้รับประกันภัย หรือผู้เข้าทำสัญญาอื่นใดเพื่อจัดให้ซึ่งทรัพย์สิน บริการ หรือประโยชน์อื่นใด ทั้งนี้ การเข้าทำสัญญานั้นต้องเป็นไปเพื่อการค้า ทรัพย์สิน บริการ หรือประโยชน์อื่นใดนั้นเป็นทางค้าปกติของตน

ค. <u>คำนึงจากรูปแบบของการทำสัญญา</u> ได้แก่ ข้อสัญญามาตรฐานหรือสัญญาสำเร็จรูป ดังมีคำจำกัดความไว้ในมาตรา 3*

และจากการที่ในกฎหมายเกี่ยวกับลายมือชื่อดิจิตอลของหลายๆ ประเทศ และหลายๆ มลรัฐในประเทศสหรัฐอเมริกาได้ยอมรับผู้ประกอบการรับรองสามารถที่จะทำการจำกัดความรับผิดของตนต่อผู้ถือใบรับรองได้ ทำให้ผู้ประกอบการรับรองน่าที่จะได้ทำการร่างข้อสัญญาสำเร็จรูปหรือสัญญามาตรฐานโดยมีข้อจำกัดความรับผิดของตน หรือตกลงให้ผู้ถือใบรับรองต้องรับผิด และ/หรือรับภาระมากกว่าที่กฎหมายกำหนดอยู่ด้วย เป็นต้น ซึ่งเนื้อหาของข้อสัญญาดังกล่าวตามพระราชบัญญัติว่าด้วยข้อสัญญาที่ไม่เป็นธรรม พ.ศ. 2540 ของไทยถือว่าเป็นลักษณะของข้อสัญญาที่ไม่เป็นธรรมตามที่ได้บัญญัติไว้ในมาตรา 4 วรรค 3** ทำให้ข้อตกลงระหว่างผู้ประกอบการรับรองกับผู้ถือใบรับรองต้องตกอยู่ภายใต้มาตรา 4 ของพระราชบัญญัติดังกล่าว ส่งผลให้ข้อสัญญาดังกล่าวไม่สามารถใช้บังคับได้ตามกฎหมายตามมาตรา 6 ส่วนแรก*** หรือใช้บังคับได้เท่าที่เป็นธรรมและพอสมควรแก่กรณีตามดุลพินิจของศาลตามมาตรา 6 ส่วนหลัก มาตรา 7-9 โดยใช้หลักการตามที่ได้บัญญัติไว้ในมาตรา 10 ในการพิจารณา† เว้นแต่ในกรณีที่ข้อจำกัดความรับผิดหรือยกเว้นความรับผิดดังกล่าวอยู่ภายในกรอบของกฎหมายเกี่ยวกับลายมือชื่อดิจิตอลของไทยได้บัญญัติไว้เป็นการเฉพาะว่าให้ผู้ประกอบการรับรองสามารถกระทำได้ ข้อจำกัดหรือยกเว้นความรับผิดในส่วนนั้นก็จะไม่ตกอยู่ภายใต้บังคับของพระราชบัญญัติว่าด้วยข้อสัญญาที่ไม่เป็นธรรม

อย่างไรก็ตามเทคโนโลยีลายมือชื่อดิจิตอลหรือลายมือชื่ออิเล็กทรอนิกส์เป็นเทคโนโลยีใหม่และมีความก้าวหน้าตลอดเวลา การตีความว่าข้อสัญญาใดทำให้ผู้ประกอบการรับรองได้เปรียบผู้ถือใบรับรองนี้น่าจะเป็นเรื่องที่มีความยุ่งยากและอาจจะอยู่นอกเหนือความเข้าใจของประชาชนหรือศาลยุติธรรมได้ จึงควรได้มีการกำหนดขอบเขตของข้อจำกัดหรือยกเว้นความรับผิดของผู้ประกอบการรับรองอย่างชัดเจน โดยคำนึงถึงหลักเสรีภาพในการทำสัญญาและหลักกฎหมายว่าด้วยข้อสัญญาที่ไม่เป็นธรรมให้มีความเหมาะสม เพื่อความชัดเจน และเป็นประโยชน์ต่อความยุติธรรมในการใช้บังคับกฎหมายต่อไป

---

* "สัญญาสำเร็จรูป" หมายความว่า สัญญาที่ทำเป็นลายลักษณ์อักษรโดยมีการกำหนดข้อสัญญาที่เป็นสาระสำคัญไว้ล่วงหน้า ไม่ว่าจะทำในรูปแบบใด ซึ่งคู่สัญญาฝ่ายหนึ่งฝ่ายใดนำมาใช้ในการประกอบกิจการของตน

** โปรดดู มาตรา 4 วรรค 3 ของพระราชบัญญัติว่าด้วยข้อสัญญาที่ไม่เป็นธรรม พ.ศ. 2540

*** โปรดดู มาตรา 6 ส่วนแรก ของพระราชบัญญัติว่าด้วยข้อสัญญาที่ไม่เป็นธรรม พ.ศ. 2540

† โปรดดู มาตรา 6 ส่วนหลัก มาตรา 7-10 ของพระราชบัญญัติว่าด้วยข้อสัญญาที่ไม่เป็นธรรม พ.ศ. 2540