# พัฒนาการทางกฎหมายที่เกี่ยวข้องกับการรับฟังพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ในคดีแพ่ง

# Development of laws about admissibility of electronic data as evidence in civil cases




สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

นิติศาสตรมหาบัณฑิต มหาวิทยาลัยกรุงเทพ

พ.ศ. 2552

# พัฒนาการทางกฎหมายที่เกี่ยวข้องกับการรับฟังพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ในคดีแพ่ง

# Development of laws about admissibility of electronic data as evidence in civil cases

ศศิธร หงษ์ประเสริฐ

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

นิติศาสตรมหาบัณฑิต มหาวิทยาลัยกรุงเทพ

พ.ศ. 2552

บัณฑิตวิทยาลัย

มหาวิทยาลัยกรุงเทพ

สารนิพนธ์

โดย

นางสาวศศิธร หงษ์ประเสริฐ

เรื่อง

พัฒนาการทางกฎหมายที่เกี่ยวข้องกับการรับฟังพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ในคดีแพ่ง

ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

นิติศาสตรมหาบัณฑิต

อาจารย์ที่ปรึกษา [redacted]

(ดร.ศิรภา จำปาทอง)

อาจารย์ที่ปรึกษาร่วม [redacted]

(อาจารย์ชวลิต อัตถศาสตร์)

กรรมการผู้ทรงคุณวุฒิ [redacted]

(อาจารย์สุรางคณา วายุภาพ)

**ชื่องานวิจัย** : พัฒนาการทางกฎหมายที่เกี่ยวข้องกับการรับฟังพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ในคดีแพ่ง
**ชื่อผู้วิจัย** : นางสาว ศศิธร หงษ์ประเสริฐ
**ชื่อคณะและสถาบัน** : คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ
**สาขา** : กฎหมายธุรกิจระหว่างประเทศและธุรกรรมทางอิเล็กทรอนิกส์
**รายชื่อที่ปรึกษา** : ดร.ศิรภา จำปาทอง
**ปีการศึกษา** : 2552
**คำสำคัญ** : พัฒนาการ การรับฟัง พยานหลักฐาน ข้อมูลอิเล็กทรอนิกส์

## บทคัดย่อ

ในปัจจุบันผู้คนส่วนใหญ่ใช้เทคโนโลยีคอมพิวเตอร์กันมากขึ้นทำให้การติดต่อสื่อสารมีความสะดวกรวดเร็ว โดยเฉพาะอย่างยิ่งการติดต่อทำธุรกรรมผ่านสื่ออิเล็กทรอนิกส์ ซึ่งอาจก่อให้เกิดข้อพิพาทระหว่างผู้ซื้อและผู้ขาย ซึ่งเป็นการยากต่อการรวบรวมพยานหลักฐานเพราะพยานหลักฐานเป็นข้อมูลอิเล็กทรอนิกส์เป็นการยากต่อการพิสูจน์เพราะการใช้ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานค่อนข้างมีความยุ่งยาก อาจต้องใช้ผู้เชี่ยวชาญเฉพาะทางในด้านนี้โดยเฉพาะ ในการค้น หรือรื้อเพื่อค้นหาข้อมูลที่ถูกซ่อนหรืออาจลบทิ้งไปแล้วให้กลับมาใหม่ โดยที่ตัวของพยานหลักฐานนั้นยังคงมีความเป็นต้นฉบับหรือมีความน่าเชื่อถือดังเดิมไม่เปลี่ยนแปลง

งานวิจัยฉบับนี้มีวัตถุประสงค์เพื่อศึกษาการพิสูจน์พยานหลักฐานโดยวิธีนิติคอมพิวเตอร์ซึ่งเป็นวิธีการในการตรวจพิสูจน์หลักฐานของข้อมูลอิเล็กทรอนิกส์ นอกจากนี้ยังได้ศึกษาไปถึงกฎหมายของประเทศสหรัฐอเมริกาและสหราชอาณาจักร ที่มีพัฒนาการทางกฎหมายที่ก้าวหน้า รวมทั้งกฎหมายแม่แบบของคณะกรรมาธิการกฎหมายระหว่างประเทศแห่งสหประชาชาติว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ UNCITRAL Model Law On Electronic Commerce 1996 และ UNCITRAL Model Law On Electronic Signatures 2001

**Title** : Development of Laws about Admissibility of Electronic Data as Evidence in Civil Cases

**Author** : Miss Sasithorn Hongprasert

**School** : Law, Bangkok University

**Major** : Law of International Business and Electronic Transactions

**Advisors** : Dr. Sirapa Champathong

**Academic Year** : 2552

**Keywords** : Development, admissibility, Evidence, Electronic data

**Abstract**

In the present, the majority of the population uses computer technology increasingly causing communication to be faster and efficient especially communication through electronic mails. These electronic mails or e-mails may cause dispute between the producers and consumers which would be difficult to gather these information for investigation. Investigating these electronic information are troublesome because these informations are complicated and it may need help from a specialist. This specialists would need to retrieve information that is hidden or erased to be in its original form.

This research objective is for educational purpose. Investigating evidence using computer forensic, which is the investigation of electronic information. It also gives a study on the laws of United States of America and England. Include UNCITRAL Model Law On Electronic Commerce 1996 และ UNCITRAL Model Law On Electronic Signatures 2001.

# กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้ สำเร็จลุล่วงไปได้โดยความอนุเคราะห์เป็นอย่างดียิ่งจากบุคคลต่าง ๆที่กรุณาให้คำปรึกษา ให้ข้อมูล และความช่วยเหลือในด้านต่าง ๆที่เป็นประโยชน์ในการศึกษาและการทำสารนิพนธ์ ข้าพเจ้าขอกล่าวขอบคุณไว้ดังนี้

ท่านอาจารย์ดร. ศิรภา จำปาทอง ที่กรุณารับเป็นที่ปรึกษาให้กับข้าพเจ้าและได้ให้คำชี้แนะต่าง ๆในเรื่องของเนื้อหาที่ควรปรับปรุงและแก้ไขข้อบกพร่องให้สารนิพนธ์ฉบับนี้มีความสมบูรณ์เป็นประโยชน์ต่อผู้ที่อ่าน ผู้เขียนจึงขอกราบขอบพระคุณท่านอาจารย์เป็นอย่างสูงไว้ ณ ที่นี้

ท่านอาจารย์ ชวลิต อัตถศาสตร์ ที่กรุณารับเป็นที่ปรึกษาให้กับข้าพเจ้าและได้สละเวลาอันมีค่ายิ่งในการให้คำแนะนำต่าง ๆ รวมทั้งให้คำชี้แนะในหัวข้อและประเด็นที่สำคัญในการทำสารนิพนธ์ฉบับนี้ ผู้เขียนจึงขอกราบขอบพระคุณท่านอาจารย์เป็นอย่างสูงไว้ ณ ที่นี้

ผู้เขียนขอกราบขอบพระคุณ มหาวิทยาลัยกรุงเทพที่ได้ให้การสนับสนุนทุนการศึกษาในโครงการทุนนักกีฬาทีมชาติแก่ข้าพเจ้าตั้งแต่สมัยที่เรียนระดับปริญญาตรีจนถึงปัจจุบัน ผู้เขียนจึงขอกราบขอบพระคุณไว้ ณ ที่นี้

ท่านอาจารย์ นุกูล นิลวงษานุวัติ อาจารย์ที่ปรึกษาชมรมยิงปืนมหาวิทยาลัยกรุงเทพที่ได้คอยให้กำลังใจและช่วยเหลือให้คำปรึกษาและช่วยติดต่อประสานงานให้แก่ข้าพเจ้าในทุก ๆ เรื่อง ผู้เขียนขอกราบขอบพระคุณท่านอาจารย์เป็นอย่างสูงไว้ ณ ที่นี้

ผู้เขียนขอกราบขอบพระคุณ บิดา มารดาและพี่ ๆในครอบครัวของผู้เขียนทุกคน ซึ่งท่านคอยเป็นกำลังใจและให้การช่วยเหลือสนับสนุนในทุก ๆด้านและขอกราบขอบพระคุณท่านอาจารย์ผู้สอนทุก ๆท่านที่ได้ประสิทธิประสาทวิชาความรู้ต่าง ๆให้กับผู้เขียน

นอกจากนี้ผู้เขียนขอขอบคุณพี่ ๆและเพื่อนนักศึกษามหาวิทยาลัยกรุงเทพ ที่คอยให้ความช่วยเหลือและให้คำปรึกษา แลกเปลี่ยนข้อมูลความรู้ รวมทั้งการติดต่อประสานงานในการศึกษาครั้งนี้ รวมทั้งน้อง ๆที่ให้ความช่วยเหลือในการทำสาระนิพนธ์ฉบับนี้

(ศศิธร หงษ์ประเสริฐ)

**สารบัญ**

**หน้า**

**สารบัญ (ต่อ)**

**บทที่** **หน้า**

**สารบัญ (ต่อ)**

**บทที่** **หน้า**

**สารบัญ (ต่อ)**

**บทที่** **หน้า**

**สารบัญ (ต่อ)**

**บทที่** **หน้า**

# บทที่ 1
# บทนำ

## 1.1 ความเป็นมาและความสำคัญของปัญหา

ในยุคเทคโนโลยีสารสนเทศและการสื่อสารที่ก้าวหน้าไปไม่หยุดยั้งในปัจจุบัน โดยเฉพาะเทคโนโลยีคอมพิวเตอร์และการใช้งานอินเทอร์เน็ตที่สามารถนำไปใช้งานได้หลากหลายรูปแบบ ซึ่งส่งผลกับการใช้ชีวิตประจำวันของผู้คนเป็นจำนวนมากโดยเฉพาะในด้านของการทำธุรกิจ ที่ส่งผลให้การใช้งานอินเทอร์เน็ตทำให้ผู้ประกอบการพาณิชย์กับผู้บริโภคได้รับความสะดวกสบายเพิ่มมากขึ้น

ในอดีตรูปแบบของการพาณิชย์หรือการค้าระหว่างประเทศเป็นยุคของการใช้กระดาษ ส่วนการพาณิชย์อิเล็กทรอนิกส์ในระยะแรกที่รู้จักใช้กันอย่างแพร่หลายคือ โทรพิมพ์ (telex) และโทรสาร (Fax) ซึ่งส่งผลให้กฎหมายพาณิชย์เริ่มมีผลกระทบเพราะในโทรพิมพ์และโทรสารนั้นไม่ปรากฏลายมือชื่อของคู่สัญญาจึงทำให้เกิดผลกระทบในทางการค้าระหว่างประเทศ

เมื่อมาถึงยุคเทคโนโลยีด้านอิเล็กทรอนิกส์ทำให้เกิดการพาณิชย์ที่ติดต่อสื่อสารกันทางสื่ออิเล็กทรอนิกส์หรือเรียกว่าระบบไร้กระดาษ (Paperless) ซึ่งเทคโนโลยีในยุคนี้เรียกว่า การแลกเปลี่ยนข้อมูลด้วยสื่ออิเล็กทรอนิกส์(Electronic Data Interchange-EDI) หลังจากนั้นจึงมีการพัฒนาไปถึงการค้าทางอิเล็กทรอนิกส์หรือที่ เรียกว่า พาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce E-Commerce) ซึ่งการติดต่อทำการค้าที่เห็นได้ชัดในยุคนี้คือ การติดต่อทำการค้าโดยใช้ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) และการโฆษณาขายสินค้าและบริการต่างๆ ผ่านทางเว็บไซด์ ซึ่งเทคโนโลยีที่วิวัฒนาการไปอย่างไม่หยุดยั้งนี้ย่อมส่งผลทำให้เกิดการเปลี่ยนแปลทางด้านกฎหมายเพื่อรองรับต่อผลพวงที่เกิดขึ้น และเพื่อให้สอดคล้องกับเทคโนโลยีสมัยใหม่ การที่เทคโนโลยีมีการเปลี่ยนแปลงไปอย่างรวดเร็วจึงเป็นการยากที่จะสามารถบัญญัติกฎหมายที่สามารถครอบคลุมและบังคับใช้กับเทคโนโลยีใหม่ๆได้ทันและสมบูรณ์ในทุกกรณี และเมื่อเทคโนโลยีก้าวไกลไปจนถึงขั้นที่การรับส่งข้อมูลอิเล็กทรอนิกส์สามารถกระทำได้ภายในเวลาไม่กี่วินาที

แม้คู่กรณีจะอยู่กันคนละทวีปหรือคนละประเทศ เมื่อมีการทำการซื้อขายสินค้าโดยทำคำเสนอ คำสนองโดยผ่านทางไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) ซึ่งสิ่งเหล่านี้ส่งผลในเรื่องของ

การพิสูจน์และเก็บรวบรวมพยานหลักฐานทั้งที่เกี่ยวกับตัวผู้รับและผู้ส่ง ว่าได้มีการส่งข้อมูลกันจริงหรือไม่ วัน เวลาและสถานที่ ที่อาจเกิดเป็นกรณีพิพาทในคดีทางแพ่งในเรื่องของการผิดสัญญา และการลงลายมือชื่อ ซึ่งประเด็นเหล่านี้เป็นการพิจารณาที่เกี่ยวข้องกับการก่อให้เกิดสัญญา (formation of contract) ซึ่งเราต้องตระหนักว่ากฎหมายของประเทศทั้งระบบ civil law และ common law สัญญาจะเกิดขึ้นเมื่อมีคำเสนอและคำสนองซึ่งแต่ละประเทศต่างก็มีทฤษฎีและหลักกฎหมายที่ต่างกัน ซึ่งปัญหาที่พบคือเมื่อระบบเครือข่ายอินเทอร์เน็ตมีการเชื่อมโยงเครือข่ายหลายทอดจะถือเอาเวลาใดเป็นเวลาที่ข้อมูลนั้น “ไปถึง” อีกฝ่ายหนึ่ง และวิธีการในการเก็บรวบรวมพยานหลักฐานต่างๆของข้อมูลอิเล็กทรอนิกส์จะเก็บรักษาอย่างไรให้ข้อมูลนั้นยังคงมีความน่าเชื่อถือ และสามารถนำไปเป็นพยานหลักฐานในศาลได้

จากการศึกษาพบว่าประเทศไทยได้เริ่มเล็งเห็นความสำคัญของการพาณิชย์อิเล็กทรอนิกส์โดยเมื่อปีพ.ศ. 2535 คณะกรรมการส่งเสริมการพัฒนาเทคโนโลยีแห่งชาติได้ตั้งคณะอนุกรรมการเฉพาะกิจเพื่อพัฒนาโครงการทางด้านการค้าระหว่างประเทศเพื่อทำหน้าที่ดูแลตลอดจนกำกับนโยบายและเป้าหมายโดยทำงานภายใต้สังกัดของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) แต่แม้ว่าเราจะมีหน่วยงานที่คอยกำกับดูแลในเรื่องของการพาณิชย์อิเล็กทรอนิกส์อยู่ แต่การทำธุรกรรมผ่านทางสื่ออิเล็กทรอนิกส์ยังพบปัญหาและอุปสรรคสำคัญในเรื่องเกี่ยวกับการฟ้องร้องบังคับคดีโดยเฉพาะในเรื่องของการเก็บรวบรวมและพิสูจน์พยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ในคดีแพ่งต่างๆ เพราะในเรื่องเกี่ยวกับการใช้ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานมีความยุ่งยากอาจต้องใช้ผู้เชี่ยวชาญเฉพาะทางในด้านนี้มาพิสูจน์เกี่ยวกับการค้น หรือรื้อเพื่อค้นหาข้อมูลที่ถูกซ่อนไว้หรืออาจถูลบทิ้งไปแล้วให้กลับมาใหม่ โดยที่ตัวของพยานหลักฐานนั้นยังคงมีความเป็นต้นฉบับหรือมีความน่าเชื่อถือดังเดิมไม่เปลี่ยนแปลง การศึกษาปัญหาดังกล่าวนี้ได้ศึกษาไปถึงวิธีการตรวจพิสูจน์หลักฐานของข้อมูลคอมพิวเตอร์(Computer Forensics) ว่ามีวิธีการอย่างไร และยังได้ศึกษากฎหมายของประเทศสหรัฐอเมริกาและ สหราชอาณาจักร รวมทั้งกฎหมายแม่แบบของ UNCITRAL ที่เรียกว่า UNCITRAL Model Law on Electronic Commerce 1996 และ UNCITRAL Model Law on Electronic Signatures 2001 ซึ่งเป็นกฎหมายแม่แบบที่ UNCITRAL หรือ United Nation Commission For International Trade Law จัดทำขึ้น 2 ฉบับแต่ประเทศไทยนำกฎหมายแม่แบบสองฉบับนี้เป็นตัวอย่างแล้วผนวกรวมเป็นพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และมีการแก้ไขเพิ่มเติมเป็นพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 โดยมีวัตถุประสงค์

เพื่อรองรับการพัฒนาทางเทคโนโลยีที่เกี่ยวกับการติดต่อสื่อสารทาง อิเล็กทรอนิกส์และการทำธุรกรรมทางอิเล็กทรอนิกส์ในปัจจุบัน



## 1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาถึงกฎหมายทั้งภายในประเทศและต่างประเทศเกี่ยวกับการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีแพ่ง
2. เพื่อให้ทราบถึงวิธีการพิสูจน์พยานหลักฐานของข้อมูลอิเล็กทรอนิกส์

## 1.3 ขอบเขตของการวิจัย

ศึกษาถึงการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์หรือนิติคอมพิวเตอร์(Computer-forensics) เพื่อจุดประสงค์ในการค้นหาและวิเคราะห์ข้อมูลที่มีอยู่ หรือที่ถูกลบทิ้ง หรือที่ถูกซ่อน ซึ่งอาจใช้เป็นหลักฐานที่มีประโยชน์ในทางกฎหมายรวมถึงศึกษาถึงการยึดและเก็บรักษาข้อมูลอิเล็กทรอนิกส์ให้อยู่ในสภาพที่เป็นจริงมากที่สุดเพื่อความน่าเชื่อถือของพยานหลักฐาน รวมทั้งศึกษาถึงการรับรองและตรวจพิสูจน์ความถูกต้องแท้จริงของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีแพ่งและศึกษาถึงกฎหมายแม่แบบ UNCITRAL Model Law on Electronic Commerce 1996 และ UNCITRAL Model Law on Electronic Signatures 2001เกี่ยวกับความน่าเชื่อถือของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์และการพิสูจน์ลายมือชื่ออิเล็กทรอนิกส์ตามกฎหมายแม่แบบ UNCITRAL Model Law และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ.2544 รวมทั้งศึกษาถึงมาตรการทางกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานของประเทศสหรัฐอเมริกาและสหราชอาณาจักรในคดีทางแพ่ง

## 1.4 คำถามของการวิจัย

1. การพิสูจน์พยานหลักฐานที่เป็นข้อมูลทางอิเล็กทรอนิกส์ในคดีแพ่งมีวิธีการอย่างไร
2. พัฒนาการทางกฎหมายของต่างประเทศที่เกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานที่มีความก้าวหน้ามากกว่าประเทศไทยเพียงใด

## 1.5 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1. ให้ทราบถึงวิธีการพิสูจน์พยานหลักฐานในคดีทางแพ่งว่ามีวิธีการอย่างไร



2. ทำให้ได้ศึกษาถึงกฎหมายเกี่ยวกับพยานหลักฐานที่เป็นข้อมูลทางอิเล็กทรอนิกส์ของต่างประเทศเพื่ออาจจะสามารถนำมาพัฒนากฎหมายของประเทศเราในอนาคต
3. ให้ประโยชน์กับสังคมในเรื่องการใช้ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานเพื่อให้เกิดประสิทธิภาพในการสู้คดีในศาล

**1.6 นิยามศัพท์**

**ธุรกรรมทางแพ่ง** เช่น การก่อตั้งสิทธิส่วนบุคคล การทำหนังสือมอบอำนาจ การจดทะเบียนทะเบียนสมรส การทำพินัยกรรม แต่พาณิชย์เป็นเรื่องสัญญาต่างๆ เช่น สัญญาเช่า สัญญาซื้อขายเป็นต้น

**ธุรกรรมภาครัฐ** เกี่ยวข้องกับการจดทะเบียนบริษัท จดทะเบียนเครื่องหมายการค้า จดทะเบียนสิทธิบัตร ขอสัมปทานเหมืองแร่ การยื่นคำฟ้องหรือคำให้การต่อศาลหากศาลอนุญาตให้รับคำฟ้องหรือคำให้การทางสื่ออิเล็กทรอนิกส์

**อิเล็กทรอนิกส์** หมายถึง การประยุกต์ใช้วิธีการทางอิเล็กตรอนไฟฟ้า คลื่นวิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีการต่างๆ เช่นว่านั้น

**นิติคอมพิวเตอร์** หมายถึง การใช้เทคโนโลยีคอมพิวเตอร์เพื่อจุดประสงค์ในการค้นหา และวิเคราะห์ข้อมูลที่อาจถูกลบทิ้งหรือถูกซ่อนไว้ เพื่อใช้ประโยชน์ในด้านกฎหมาย

**ธุรกรรมทางอิเล็กทรอนิกส์** หมายถึง ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน

**ข้อมูลอิเล็กทรอนิกส์** หมายถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลโดยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ โทรสาร

**ลายมือชื่ออิเล็กทรอนิกส์** หมายถึง อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใด ที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

**เจ้าของลายมือชื่อ** หมายถึง ผู้ซึ่งถือข้อมูลสำหรับสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นในนามของตนเองหรือแทนบุคคลอื่น



**ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

**การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์** หมายถึง การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

**ผู้ส่งข้อมูล** หมายถึง บุคคลซึ่งเป็นผู้ส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีการที่ผู้นั้นกำหนดโดยบุคคลนั้นอาจจะส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ ทั้งนี้ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

**ผู้รับข้อมูล** หมายถึง บุคคลซึ่งผู้ส่งข้อมูลประสงค์จะส่งข้อมูลอิเล็กทรอนิกส์ให้และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

**ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

**พยานหลักฐานดิจิทัล** คือ สารสนเทศ (Information) หรือข้อมูล(Data) ที่อาจมีประโยชน์ต่อการสืบสวนสอบสวนซึ่งอาจถูกเก็บบันทึกไว้ในอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์คอมพิวเตอร์หรือโทรศัพท์มือถือ

# บทที่ 2
# กฎหมายลักษณะพยาน การนำสืบพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ในทางแพ่ง และวิธีการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์

## 2.1 กฎหมายลักษณะพยาน

กฎหมายลักษณะพยานในโลกนี้ได้มีแนวคิดการแบ่งกฎหมายลักษณะพยานออกเป็น 2 ระบบ คือ ระบบกล่าวหาและระบบไต่สวน โดยเฉพาะในเรื่องการดำเนินการ (la marche) และเนื้อหา (la matiere) ของกระบวนการพิจารณา โดยในการดำเนินกระบวนการพิจารณามีข้อน่าคิดอยู่ว่าศาลหรือคู่ความเป็นผู้ที่มีบทบาทหรือผู้ริเริ่มในส่วนที่เกี่ยวกับเนื้อหาของคดีและขั้นตอนการดำเนินกระบวนการพิจารณา แต่เดิมเราเรียกว่า “ระบบกล่าวหา” ( principe accusatoire) หากคู่กรณีเป็นผู้มีบทบาทในเรื่องดังกล่าว เราเรียกว่า “ระบบไต่สวน” ( principe inquisitoire หรือ inquisitprial ) ซึ่งเรื่องทั้งสองอย่างนี้ได้ถูกแบ่งแยกออกจากกันโดยเด็ดขาด ดังนั้นกระบวนการพิจารณาอาจจะถูกกำหนดโดยศาล ( maxime d’ office) หรือโดยคู่ความ ( maxime de disposition) โดยมีนักวิชาการเป็นจำนวนมากที่เห็นว่า หลักการกำหนดกระบวนการพิจารณาโดยศาลนี้เป็นหลักการเดียวกันกับหลักไต่สวน

## 2.2 พยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความแพ่ง สามารถแบ่งพยานออกได้เป็น 3 ประเภท ดังนี้

### 2.2.1 พยานเอกสาร

ความหมายของพยานเอกสารตามประมวลกฎหมายวิธีพิจารณาความแพ่งไม่ได้กำหนดไว้แต่อย่างใด แต่ตามความเห็นของนักกฎหมายอาจให้ความหมายได้ดังนี้

ศาสตราจารย์โสภณ รัตนากร[1] เห็นว่า

“พยานเอกสาร” หมายถึง สิ่งซึ่งมีการบันทึกตัวอักษร ตัวเลข รูปรอย หรือเครื่องหมาย ซึ่งสามารถแสดงข้อความหรือความหมายอย่างใดอย่างหนึ่งให้ศาลตรวจดูได้

---

[1] โสภณ รัตนากร,**คำอธิบายกฎหมายลักษณะพยาน**.พิมพ์ครั้งที่7,(กรุงเทพมหานคร: สำนักพิมพ์นิติบรรณการ,2544

อาจารย์เข็มชัย ชุติวงศ์[2] เห็นว่า

“พยานเอกสาร” หมายถึง ข้อความใดๆในเอกสารที่มีการอ้างอิงเป็นพยานโดยอาศัยการสื่อความหมายของข้อความนั้นพิสูจน์ความจริง

อาจารย์ปิติกุล จิระมงคลพาณิชย์[3] เห็นว่า

“พยานเอกสาร” หมายความว่า ข้อมูลที่บันทึกไว้ในสื่อชนิดใดก็ตามสามารถพิสูจน์ข้อเท็จจริงที่พิพาทในคดีได้และนำสืบชนิดที่บันทึกข้อมูลดังกล่าวนั้นมาใช้เป็นพยานหลักฐานในศาลก็ให้ถือเป็นพยานเอกสาร และให้รวมถึงสื่อที่บันทึกไว้ในคอมพิวเตอร์หรือสื่อสารสนเทศอื่นๆ[4] ด้วย

จากความหมายของพยานเอกสารทั้งในความเห็นของนักกฎหมายและในทางตำราพยานเอกสารมีลักษณะที่สำคัญ 3 ประการ คือ

(1) สิ่งที่มีการบันทึกไว้ ไม่ว่าจะบันทึกโดย ตัวอักษร ตัวเลข รูปรอย หรือเครื่องหมายใดก็ตาม

(2) การบันทึกนั้นได้กระทำบนสื่อกลาง ไม่ว่าสื่อกลางนั้นจะเป็นวัตถุใดก็ตาม เช่น กระดาษ ฟิล์ม แถบแม่เหล็ก การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์

(3) สิ่งที่บันทึกนั้นสามารถสื่อความหมายให้รับรู้เรื่องราว ข้อมูล หรือข้อเท็จจริงใดๆได้ เช่น บอกเล่าเรื่องราวการทำนิติกรรมสัญญา ประวัติศาสตร์ เหตุการณ์ต่างๆ ที่เกิดขึ้น

ดังนั้น พยานเอกสาร จึงหมายถึง สิ่งที่มีการบันทึกไว้ ไม่ว่าโดยการบันทึกโดยวิธีใดก็ตาม และการบันทึกนั้นกระทำผ่านสื่อกลางใดๆ เช่นทางสื่ออิเล็กทรอนิกส์หรือผ่านทางเครื่องคอมพิวเตอร์[4] ซึ่งสามารถสื่อความหมายให้รับรู้เรื่องราว ข้อมูลหรือข้อเท็จจริงใดๆได้ในภายหลัง

“ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

---

[2] เข็มชัย ชุติวงศ์,**คำอธิบายกฎหมายลักษณะพยาน**,พิมพ์ครั้งที่ 5,(กรุงเทพมหานคร: สำนักพิมพ์นิติบรรณการ,2538),น.195.

[3] ปิติกุล จิระมงคลพาณิชย์,**คำอธิบายกฎหมายลักษณะพยาน:ว่าด้วยพยานเอกสาร** ,พิมพ์ครั้งที่ 2, (กรุงเทพมหานคร:สำนักพิมพ์วิญญูชน,2548),น.11

[4] ดูรายละเอียดได้จากภาคผนวก ก หน้า 90

จะเห็นว่าข้อมูลอิเล็กทรอนิกส์มีลักษณะ 3 ประการที่สำคัญ เช่นเดียวกับพยานเอกสาร กล่าวคือ

(1) ลักษณะของเอกสารต้องมีสิ่งที่มีการบันทึกไว้ ไม่ว่าจะบันทึกโดย ตัวอักษร ตัวเลข รูปรอย หรือเครื่องหมายใด ก็ตาม และกรณีของข้อมูลอิเล็กทรอนิกส์ก็มีเรื่องราว หรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดก็ตาม เช่นเดียวกัน

(2) การบันทึกนั้นได้กระทำบนสื่อกลาง ไม่ว่าสื่อกลางนั้นจะเป็นวัตถุใดก็ตาม และกรณีของข้อมูลอิเล็กทรอนิกส์อาจแสดงออกโดยสภาพของสิ่งของนั้น หรือสื่ออิเล็กทรอนิกส์กล่าวคือ โดยผ่านวิธีการใดๆที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกันและรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็กหรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่างๆเช่นว่านั้น เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

(3) สิ่งที่บันทึกนั้นสามารถสื่อความหมายให้รับรู้เรื่องราว ข้อมูล หรือข้อเท็จจริงใดๆได้ เช่น บอกเล่าเรื่องราวการทำนิติกรรม ประวัติศาสตร์ เหตุการณ์ต่างๆ ที่เกิดขึ้น และกรณีของข้อมูลอิเล็กทรอนิกส์ก็สามารถสื่อความหมายได้เช่นเดียวกัน

เมื่ออ้างอิงข้อมูลอิเล็กทรอนิกส์ในฐานะพยานเอกสารแล้ว ก็ต้องปฏิบัติตามหลักการนำสืบต้นฉบับเอกสารด้วย ซึ่งกรณีของข้อมูลอิเล็กทรอนิกส์นี้ต้นฉบับจะเกิดขึ้นเมื่อมีการจัดทำขึ้นในครั้งแรกเท่านั้น หากต่อมามีการบันทึกต่อไปในสิ่งอื่นใด ข้อมูลอิเล็กทรอนิกส์ที่บันทึกต่อไปนั้นก็เป็นเพียงสำเนาเท่านั้น และเมื่อมีการปิด(Turn off) คอมพิวเตอร์ ต้นฉบับที่เก็บอยู่ในหน่วยความจำสำหรับเก็บข้อมูลและคำสั่ง (RAM: Random Access Memory)ดังกล่าวก็จะถูกทำลายไป ทำให้เกิดปัญหาในการนำต้นฉบับมาสืบ เพราะไม่มีต้นฉบับให้นำสืบอีกต่อไปแล้ว หรือหากเป็นกรณีที่ผู้สร้างข้อมูลอิเล็กทรอนิกส์ต้องการให้ข้อมูลอิเล็กทรอนิกส์ที่เก็บไว้ที่หน่วยความจำสำรองเป็นต้นฉบับแล้ว ข้อมูลอิเล็กทรอนิกส์ดังกล่าวเป็นต้นฉบับได้ แต่หากมีการบันทึกต่อๆกันไปอีกก็อาจจะพิสูจน์กันได้ยากว่าข้อมูลอิเล็กทรอนิกส์ที่อยู่ที่ใดเป็นต้นฉบับกันแน่ เพราะมีความถูกต้องตรงกัน แต่อย่างไรก็ตามสิ่งที่ประมวลผลและปรากฏออกมาทางหน้าจอคอมพิวเตอร์และสิ่งพิมพ์ออก(printouts)ที่พิมพ์ออกมาเป็นเพียงสำเนาเท่านั้น

กรณีของข้อมูลอิเล็กทรอนิกส์จึงอาจเข้าข้อยกเว้นตาม มาตรา 93 (1) มาตรา 93 (2) และมาตรา 93 (4)[5] กล่าวคือ หากคู่ความตกลงกันใช้สำเนาเอกสารนำสืบศาลก็สามารถยอมรับฟังได้ หรือกรณีไม่สามารถนำต้นฉบับมาได้โดยประการอื่นซึ่งตามบทบัญญัติกำหนดให้ศาลมีอำนาจอนุญาตให้นำสำเนาหรือพยานบุคคลมาสืบก็ได้ หรือกรณีไม่มีการคัดค้านเอกสารตามมาตรา 125[6] ก็ไม่ต้องนำต้นฉบับมาแสดง กล่าวคือ มีการนำสืบโดยสำเนาเอกสารได้ ดังเช่นคำพิพากษาฎีกาที่ 5963/2539 ต.9 น.1765 การส่งเอกสารโดยวิธีโทรสารเป็นวิทยาการสมัยใหม่ซึ่งเป็นข้อเท็จจริงที่รู้กันโดยทั่วไปว่าผู้ส่งจะนำต้นฉบับของเอกสารที่จะทำการส่งไปลงในเครื่องโทรสารแล้วจัดการส่งโดยวิธีโทรสารไปยังเครื่องโทรสารของผู้รับ ต้นฉบับผู้ส่งจะเป็นผู้เก็บไว้ โทรสารที่โจทก์ส่งศาลเป็นพยานซึ่งจำเลยยอมความถูกต้องแล้ว จึงรับฟังได้

การที่นำหลักการนำสืบต้นฉบับเอกสารมาใช้กับข้อมูลอิเล็กทรอนิกส์นั้น มีข้อพิจารณาถึงความเหมาะสม กล่าวคือ ไม่ว่าต้นฉบับข้อมูลอิเล็กทรอนิกส์จะยังมีอยู่หรือไม่ก็ตามสิ่งที่ประมวลผลและปรากฏออกมาทางหน้าจอคอมพิวเตอร์และสิ่งพิมพ์ออก(Printouts) ที่พิมพ์ออกมาก็เป็นเพียงสำเนาเท่านั้น ดังนั้น จึงควรที่จะกำหนดให้มีการยอมรับข้อมูลอิเล็กทรอนิกส์แม้ไม่ใช่ต้นฉบับอย่างชัดแจ้ง

---

[5] ประมวลกฎหมายวิธีพิจารณาความแพ่งมาตรา 93 การอ้างเอกสารเป็นพยานหลักฐานให้ยอมรับฟังได้เฉพาะต้นฉบับเอกสารเท่านั้นเว้นแต่

(1) เมื่อคู่ความที่เกี่ยวข้องทุกฝ่ายตกลงกันว่าสำเนาเอกสารนั้นถูกต้องแล้วให้ศาลยอมรับฟังสำเนาเช่นว่านั้นเป็นพยานหลักฐาน

(2) ถ้าต้นฉบับเอกสารนำมาไม่ได้ เพราะถูกทำลายโดยเหตุสุดวิสัย หรือสูญหาย หรือไม่สามารถนำมาได้โดยประการอื่น อันมิใช่เกิดจากพฤติการณ์ที่ผู้อ้างต้องรับผิดชอบ หรือเมื่อศาลเห็นว่าเป็นกรณีจำเป็นและเพื่อประโยชน์แห่งความยุติธรรมที่จะต้องสืบสำเนาเอกสารหรือพยานบุคคลแทนต้นฉบับเอกสารที่นำมาไม่ได้นั้น ศาลจะอนุญาตให้นำสำเนาหรือพยานบุคคลมาสืบก็ได้

(3) เมื่อคู่ความฝ่ายที่ถูกคู่ความอีกฝ่ายหนึ่งอ้างอิงเอกสารมาเป็นพยานหลักฐานยันตนมิได้คัดค้านการนำเอกสารนั้นมาสืบตามมาตรา 125 ให้ศาลรับฟังสำเนาเอกสารเช่นว่านั้นเป็นพยานหลักฐานได้ แต่ทั้งนี้ต้องไม่ตัดอำนาจศาลตามมาตรา 125 วรรคสาม

[6] ประมวลกฎหมายวิธีพิจารณาความแพ่งมาตรา 125 คู่ความฝ่ายที่ถูกอีกฝ่ายหนึ่งอ้างอิงเอกสารมาเป็นพยานหลักฐานยันตน อาจคัดค้านการนำเอกสารนั้นมาสืบโดยเหตุที่ว่าไม่มีต้นฉบับหรือต้นฉบับนั้นปลอมทั้งฉบับหรือบางส่วนหรือสำเนานั้นไม่ถูกต้องกับต้นฉบับ โดยคัดค้านต่อศาลก่อนการสืบพยานเอกสารนั้นเสร็จ

ถ้าคู่ความซึ่งประสงค์จะคัดค้านมีเหตุผลอันสมควรที่ไม่อาจทราบได้ก่อนการสืบพยานเอกสารนั้นเสร็จว่าต้นฉบับเอกสารนั้นไม่มีหรือเอกสารนั้นปลอมหรือสำเนามาถูกต้อง คู่ความนั้นอาจยื่นคำร้องขออนุญาตคัดค้านการอ้างเอกสารมาสืบดังกล่าวข้างต้นต่อศาลไม่ว่าเวลาใดก่อนศาลพิพากษา ถ้าศาลเห็นว่าคู่ความนั้นไม่อาจยกข้อคัดค้านได้ก่อนนั้น และคำขอนั้นมีเหตุผลฟังได้ ก็ให้ศาลมีคำสั่งอนุญาตตามคำขอ

**2.2.2 พยานบอกเล่า**

"พยานบอกเล่า" หมายถึง ถ้อยแถลง ลายลักษณ์อักษรแสดงออกถึงความคิด หรือกิริยาอาการที่แสดงออกแทนถ้อยคำหรือลายลักษณ์อักษรที่แสดงหรือมุ่งพิสูจน์ว่าพยานหลักฐานอื่นที่มิใช่พยานหลักฐานที่มาให้หรือพิสูจน์ต่อศาลเป็นความจริง[7]

ตามประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 95/1 กำหนดห้ามมิให้ศาลรับฟังพยานบอกเล่า แต่ก็มีข้อยกเว้นคือ

(1) ตามสภาพ ลักษณะ แหล่งที่มา และข้อเท็จจริงแวดล้อมของพยานบอกเล่านั้น น่าเชื่อว่าจะพิสูจน์ความจริงได้หรือ

(2) มีเหตุจำเป็นเนื่องจากไม่สามารถนำบุคคลซึ่งเป็นผู้ที่ได้เห็น ได้ยิน หรือทราบข้อความเกี่ยวในเรื่องที่จะให้การเป็นพยานนั้นด้วยตนเองโดยตรงมาเป็นพยานได้ และมีเหตุผลสมควรเพื่อประโยชน์แห่งความยุติธรรมที่จะรับฟังพยานเหล่านั้น

พยานบอกเล่า ได้แก่ ข้อความซึ่งเป็นการบอกเล่าที่พยานบุคคลใดนำมาเบิกความต่อศาลข้อความซึ่งเป็นการบอกเล่าที่บันทึกไว้ในเอกสารหรือวัตถุอื่นใดซึ่งได้อ้างเป็นพยานหลักฐานต่อศาล

สำหรับข้อมูลอิเล็กทรอนิกส์นั้น อาจไม่ใช่พยานบอกเล่าเสมอไป กล่าวคือ กรณีที่ข้อมูลอิเล็กทรอนิกส์จะเป็นพยานบอกเล่าก็ต่อเมื่อเป็นการบันทึกข้อมูลเก็บไว้แล้วนำข้อมูลนั้นมาแสดงใหม่ เช่น การบันทึกโดยมนุษย์ ส่วนข้อมูลอิเล็กทรอนิกส์ที่ไม่เป็นพยานบอกเล่าก็ต่อเมื่อข้อมูลนั้นเกิดจากเครื่องเอง เช่น ข้อมูลบันทึกธุรกรรมต่างๆ อันเป็นนิติกรรมสัญญา เช่น การสั่งขายหุ้นหรือสินค้า การฝากเงิน โอนเงิน หรือถอนเงิน เป็นต้น และข้อมูลที่เกิดจากการประมวลผล เช่น การคำนวณดอกเบี้ย กรณีที่ข้อมูลอิเล็กทรอนิกส์เป็นพยานบอกเล่า ในการนำมาใช้เป็นพยานหลักฐานจึงต้องห้ามมิให้รับฟังด้วยหากจะให้ศาลรับฟังก็ต้องพิสูจน์ให้เข้าข้อยกเว้นตามที่กฎหมายกำหนด

**2.2.3 พยานวัตถุ**

ความหมายของ "พยานวัตถุ"ตามประมวลกฎหมายวิธีพิจารณาความแพ่งไม่ได้กำหนดไว้แต่อย่างใด แต่ตามความเห็นของนักกฎหมายอาจให้ความหมายได้ดังนี้

---

[7] เด่นฟ้า เรืองฤทธิ์เดช, **"ปัญหาข้อกฎหมายเกี่ยวกับการรับฟังเอกสารอิเล็กทรอนิกส์"** ,ดุลพาห 53: 3, (กันยายน-ธันวาคม 2549):น.75

ศาสตราจารย์โสภณ รัตนากร เห็นว่า

“พยานวัตถุ”หมายถึง วัตถุอย่างอื่นนอกจากเอกสารซึ่งนำมาให้ศาลตรวจ

อาจารย์เข็มชัย ชุติวงศ์ เห็นว่า

“พยานวัตถุ”หมายถึงสิ่งของใดๆที่คู่ความอ้างอิงให้ศาลตรวจดูเพื่อประโยชน์แก่คดีของตน

อาจารย์โอสถ โกศิน เห็นว่า

“พยานวัตถุ” หมายความว่า วัตถุอย่างใดๆอันมิใช่เอกสารซึ่งคู่ความนำส่งเพื่อให้ศาลตรวจ

จากความเห็นของนักกฎหมายดังกล่าวเห็นว่าลักษณะของพยานวัตถุมีลักษณะ 2 ประการ คือ

1.เป็นวัตถุหรือสิ่งของอย่างใดๆที่มิใช่เอกสาร

2.มีวัตถุประสงค์ในการอ้างอิงเพื่อให้ศาลตรวจดู

ดังนั้น จึงอาจให้ความหมายของพยานวัตถุได้ว่า

“พยานวัตถุ”หมายถึง วัตถุหรือสิ่งของอย่างใดๆที่มิใช่เอกสารที่อ้างอิงเป็นพยานหลักฐานเพื่อให้ศาลตรวจดู

การตรวจดูของศาลดังกล่าวอาจเป็นการตรวจดูโดยประสาททางตา หรือประสาทสัมผัสทางอื่นก็ได้ เช่น เสียง กลิ่น สัมผัส รสชาติ เป็นต้น

ข้อมูลอิเล็กทรอนิกส์มีการบันทึกอยู่ในวัตถุ สิ่งของ หรือสื่อกลางใดๆจึงสามารถอ้างอิงเป็นพยานหลักฐานในฐานะที่เป็นพยานวัตถุได้ กล่าวคือ อ้างอิงเป็นพยานหลักฐานเพื่อให้ศาลตรวจดูลักษณะข้อมูลอิเล็กทรอนิกส์นั้น

**2.3 การนำสืบพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ในทางแพ่ง**

การแบ่งการรับฟังพยานหลักฐานแตกต่างกันไปในคดีแพ่งและคดีอาญา อันเนื่องมาจากแนวความคิดที่แตกต่างกันในการพิจารณาคดี ในคดีอาญาเป็นเรื่องของการพิสูจน์จนปราศจากข้อสงสัยว่าจำเลยกระทำผิดจริง(proof beyond reasonable doubt)ในขณะที่คดีแพ่งภายใต้ประมวลกฎหมายวิธีพิจารณาความแพ่ง(ป.วิ.พ.)เป็นเรื่องของการชั่งน้ำหนักพยานหลักฐานว่าพยานหลักฐานของฝ่ายใดน่าเชื่อถือกว่ากัน(proof on the balance of probability)ยิ่งไปกว่านั้นจากการที่ประเทศไทยได้รับอิทธิพลเกี่ยวกับการบังคับใช้และตีความกฎหมายพยานหลักฐานมาจากประเทศสหราชอาณาจักรส่งผลให้การรับฟังพยานหลักฐานของประเทศไทยเป็นไปในแนวทางเดียวกับกฎหมายคอมมอนลอว์ของประเทศสหราชอาณาจักรทั้ง

ในส่วนข้อยกเว้นของการรับฟังพยานบอกเล่า เช่น ถ้อยแถลงที่ทำให้เสียประโยชน์ ถ้อยแถลงของผู้ตายที่บอกไว้ก่อนตายและรู้ว่าตนเองใกล้ตาย และหลักเกณฑ์การติดต่อสื่อสารที่ได้รับเอกสิทธิ์ที่จะเก็บไว้เป็นความลับ เช่น ระหว่างทนายกับลูกความ เป็นต้น อย่างไรก็ดียังคงมีความแตกต่างของแนวทางในการพัฒนาระบบกฎหมายและการใช้ระบบผสมระหว่างการที่ประเทศไทยใช้ระบบกฎหมายซีวิลล์ลอว์ แต่มีการใช้แนวทางการตีความและนำกฎหมายมาบังคับใช้ของระบบกฎหมายคอมมอนลอว์ ซึ่งกฎหมายระบบคอมมอนลอว์นี้มีการแบ่งหลักเกณฑ์ของการรับฟังพยานหลักฐานได้ดังนี้

**2.3.1. หลักเกณฑ์การรับฟังพยานหลักฐานที่ดีที่สุด** (The Best Evidence Rule)

ตามป.วิ.พ.มาตรา93[8] ต้นฉบับเอกสารเท่านั้นที่สามารถรับฟัง[9] เว้นแต่จะเข้าข้อยกเว้น เช่น ต้นฉบับเอกสารถูกทำลาย หรือคู่ความทุกฝ่ายตกลงกันว่าสำเนานั้นถูกต้องแล้ว ซึ่งรวมไปถึงกรณีที่คู่ความอีกฝ่ายหนึ่งมิได้โต้แย้งคัดค้านความถูกต้องที่แท้จริงของสำเนาเอกสารซึ่งคู่ความฝ่ายหนึ่งนำสืบหรืออ้างเป็นพยานหลักฐานว่าไม่มีต้นฉบับ หรือสำเนานั้นไม่ถูกต้องตรงกับต้นฉบับ[10]

---

[8] ประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 93 การอ้างเอกสารเป็นพยานหลักฐานนั้นให้ยอมรับฟังได้แต่ต้นฉบับเอกสารเท่านั้นเว้นแต่

(1) เมื่อคู่ความที่เกี่ยวข้องทุกฝ่ายตกลงกันว่าสำเนาเอกสารนั้นถูกต้องแล้ว จึงให้ศาลยอมรับฟังสำนาเช่นว่านั้นเป็นพยานหลักฐานแห่งเอกสารนั้นได้

(2) ถ้าต้นฉบับเอกสารนั้นหาไม่ได้เพราะสูญหายหรือถูกทำลายโดยเหตุสุดวิสัย หรือไม่สามารถนำเอกสารต้นฉบับมาได้โดยประการอื่นศาลจะอนุญาตให้นำสำเนาหรือพยานบุคคลมาสืบก็ได้

(3) ต้นฉบับเอกสารที่อยู่ในความอารักขาหรือในความควบคุมของทางราชการนั้นจะนำมาแสดงได้ก็ต่อเมื่อได้รับอนุญาตของ รัฐมนตรี หัวหน้ากรม กอง หัวหน้าแผนก หรือผู้รักษาการแทนในตำแหน่งนั้นๆ ที่เกี่ยวข้องแล้วแต่กรณีเสียก่อนอนึ่ง นอกจากศาลจะกำหนดให้เป็นอย่างอื่น สำเนาเอกสารหรือข้อความที่คัดจากเอกสารเหล่านั้นซึ่งรัฐมนตรี หัวหน้ากรม กอง หัวหน้าแผนก หรือผู้ที่รักษาการแทนในตำแหน่งนั้นๆได้รับรองถูกต้องแล้ว ให้ถือว่าเป็นอันเพียงพอในการที่จะนำมาแสดง.

[9] คำพิพากษาฎีกาที่ 621/2546 : เมื่อจำเลยโต้แย้งคัดค้านความถูกต้องแท้จริงของสำเนาตารางกรมธรรม์ สำเนาเอกสารดังกล่าวจึงต้องห้ามมิให้รับฟังตามประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา93.

[10] ประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 125/คำพิพากษาฎีกาที่ 2867/2544,คำพิพากษาฎีกาที่ 2295/2543 และคำพิพากษาฎีกาที่ 1041/2537.

**2.3.2 หลักเกณฑ์การรับฟังพยานหลักฐานที่เป็นพยานบอกเล่า** (The Hearsay Rule) ตาม ป.วิ.พ. มาตรา 95(2) ห้ามมิให้ศาลรับฟังพยานบอกเล่า ดังนั้น หากคู่ความประสงค์ที่จะนำพยานบอกเล่ามาสืบศาลย่อมงดสืบพยานปากนั้นได้[11] อย่างไรก็ตาม กรณีที่พยานบอกเล่าปากนั้นมิใช่เป็นผู้ที่รู้เห็นหรือทราบข้อความดังกล่าวมาโดยตรง แต่หากเป็นผู้ที่มีหน้าที่เกี่ยวข้องกับเหตุการณ์หรือข้อความที่คู่ความประสงค์จะนำสืบ ก็ไม่ต้องห้ามมิให้รับฟัง คู่ความที่เกี่ยวข้องสามารถนำพยานปากดังกล่าวเข้าเบิกความรับรองความถูกต้องแท้จริงของข้อความหรือเหตุการณ์ได้[12] ในประเทศอังกฤษมีคดีตัวอย่างที่แสดงว่าการบันทึกด้วยเครื่องคอมพิวเตอร์ดังกล่าว เป็นพยานบอกเล่าคือ คดี R.V. Conventy justices, ex parte Bullard (1992)[13] "ในการบันทึกข้อมูลที่เกี่ยวกับภาษีอากร โดยมนุษย์เป็นผู้บันทึกข้อมูลลงในเครื่องคอมพิวเตอร์ printout ที่ได้จากเครื่องคอมพิวเตอร์ในกรณีนี้เป็นพยานบอกเล่า เพราะข้อมูลที่เกี่ยวข้องซึ่งได้บันทึกลงในเครื่องคอมพิวเตอร์นั้นกระทำโดยมนุษย์"

**2.3.3 หลักเกณฑ์การรับรองความถูกต้องแท้จริงของพยานหลักฐาน**

การรับรองความถูกต้องแท้จริงหมายความว่า การบันทึกมีความหมายเป็นไปตามสิ่งที่ต้องการหรือไม่ การบันทึกดังกล่าวนี้จะต้องการการพิสูจน์(identified) และเชื่อมโยงแหล่งที่มา ตามหลักของกฎหมายคอมมอนลอว์ การรับรองความถูกต้องแท้จริงเป็นพื้นฐานของการนำเสนอพยานเอกสารต่อศาล[14] ในคดีแพ่งจะมีหลักเกณฑ์ในการพิจารณาความถูกต้องแท้จริงของพยานหลักฐานเช่นเดียวกับคดีอาญา แต่จะมีหลักเกณฑ์เพิ่มเติมในการรับฟังพยานเอกสารโดยไม่จำเป็นต้องมีพยานบุคคลมานำสืบรับรองความถูกต้องแท้จริงของพยานเอกสารได้

---

[11] คำพิพากษาฎีกาที่9145/2539.

[12] คำพิพากษาฎีกาที่ 1795/2538: "ข้อที่จำเลยฎีกาว่าพยานบุคคลของโจทก์เป็นพยานบอกเล่ารับฟังไม่ได้นั้น เห็นว่าพยานบุคคลของโจทก์ได้เบิกความรับรองเอกสารว่ามีอยู่จริงและถูกต้อง แม้พยานโจทก์ที่เบิกความมาจะมิได้รู้เห็นขณะพยานทำเอกสาร แต่พยานเหล่านั้นเป็นผู้มีหน้าที่เกี่ยวข้องกับพยานเอกสาร และเมื่อได้ตรวจสอบเอกสารต่างๆแล้วก็สามารถรับรองความถูกต้องแท้จริงได้ ทั้งเอกสารต่างๆที่โจทก์อ้างมาจำเลยก็ได้หาได้นำสืบว่าไม่ถูกต้องหรือไม่สมบูรณ์แต่อย่างใดการที่ศาลชั้นต้นและศาลอุทธรณ์รับฟังพยานบุคคลของโจทย์ดังกล่าวจึงไม่ต้องห้ามตามประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 95(2)"

[13] Christina McAlhone and Michael Stockdale, **Evidence in a Nutshell**,(Londom : Sweet & Maxwell, 1996) , : 54.

[14] พรเพชร วิชิตชลชัย, บทวิเคราะห์เรื่อง **การรับฟังข้อมูลจากสื่ออิเล็กทรอนิกส์เป็นพยานหลักฐานในคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ**,เอกสารประกอบการสัมมนาทางวิชาการเรื่องกฎหมายพาณิชย์อิเล็กทรอนิกส์(E-commerce Laws): นวัตกรรมทางกฎหมายที่จำเป็นและเร่งด่วนแห่งสังคมไทย,หอประชุมมหิศร อาคารไทยพาณิชย์ปาร์ค พลาซ่า กรุงเทพฯ, เมื่อวันที่ 6-7 พฤษภาคม 2542.(อัดสำเนา) น.3

ในคดีที่จำเลยขาดนัดยื่นคำให้การหรือขาดนัดพิจารณาและเป็นคดีที่ฟ้องบังคับให้จำเลยชำระหนี้เป็นเงินจำนวนแน่นอน โจทก์สามารถส่งพยานเอกสารแทนการสืบพยานได้[15] ซึ่งมีคำพิพากษาในบางคดีที่เกี่ยวกับการพิจารณาระบบเทคโนโลยีคอมพิวเตอร์ที่จะต้องมีการพิสูจน์ในเรื่องของการบันทึกข้อมูลโดยเครื่องคอมพิวเตอร์ การเก็บข้อมูล ความปลอดภัยของข้อมูลตั้งแต่เวลานำเข้าจนถึงเวลาที่ได้ข้อมูลอิเล็กทรอนิกส์ออกมาจากหน่วยความจำสำรอง การเคลื่อนย้ายข้อมูล การดูแลรักษาข้อมูลอิเล็กทรอนิกส์จนถึงเวลาที่เสนอต่อศาล เช่นในคดี ปีค.ศ. 1972 คดี R. v. Robson&Harris [1972] 2 All.ER.699 ซึ่งได้มีการคัดค้านความถูกต้องแท้จริงจากเทปที่บันทึก Shaw J. ได้ตัดสินว่า จะต้องมีการชี้ขาดในเบื้องต้นว่า ข้อเท็จจริงที่ได้จากการบันทึกได้มีการรับรองความถูกต้องหรือไม่ วิธีการพิสูจน์อาจจะนำสืบถึงความเป็นมาของการบันทึกเทปนี้ รวมถึงกระบวนการบันทึกจนถึงเวลาส่งเทปนี้ต่อศาล

จะเห็นได้ว่าแนวทางในการรับฟังพยานหลักฐานของประเทศสหรัฐอเมริกา ประเทศสหราชอาณาจักรและประเทศไทยจะมีหลักเกณฑ์ส่วนใหญ่ที่ไม่แตกต่างกัน ทั้งในกรณีของการรับฟังพยานหลักฐานที่ดีที่สุด ข้อห้ามในการรับฟังพยานบอกเล่า และพิจารณาความถูกต้องแท้จริงของพยานหลักฐาน แต่อย่างไรก็ดี ประเทศไทยมีแนวทางที่เคร่งครัดน้อยกว่าในการรับฟังพยานบอกเล่า ไม่ว่าจะเป็นการไม่ต้องห้ามมิให้รับฟังพยานบอกเล่าที่เป็นพยานเอกสารหรือพยานวัตถุทั้งในคดีแพ่งและคดีอาญา และข้อยกเว้นให้รับฟังพยานบอกเล่าได้ในกรณีที่ศาลเห็นว่าสมเหตุสมผลและเป็นพยานหลักฐานที่สามารถพิสูจน์ได้ว่าจำเลยผิดหรือบริสุทธิ์

### 2.4 การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์[16]

การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์หรือนิติคอมพิวเตอร์ (Computer forensics) ในความหมายทั่วไปเป็นการปฏิบัติหรือศึกษาเฉพาะเกี่ยวกับการสืบสวนสื่อคอมพิวเตอร์เพื่อจุดประสงค์ในการค้นหา และวิเคราะห์ข้อมูลที่มีอยู่หรือที่ถูกลบทิ้งหรือที่ถูกซ่อน ซึ่งอาจใช้เป็นหลักฐานที่มีประโยชน์ในทางกฎหมาย

---

[15] ประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 198 ทวิ,มาตรา 206

[16] ไพจิตร สวัสดิสาร,**การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์**,ดุลพาห,เล่ม 1 ปีที่ 53 (มกราคม-เมษายน)น.63-100

สถาบันความปลอดภัยทางอิเล็กทรอนิกส์ (Cyber security Institute) ให้ความหมายการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ว่า “เป็นการเก็บรักษาไว้ การชันสูตร การดึงหรือถอนหลักฐานที่พบออกมา การอธิบายผล และการจัดทำเอกสารของหลักฐานทางคอมพิวเตอร์รวมถึงกฎเกณฑ์พยานหลักฐาน กระบวนการทางกฎหมาย ความน่าเชื่อถือของพยานหลักฐานการรายงานข้อเท็จจริงของข้อมูลที่พบและการเตรียมการเกี่ยวกับความเห็นของผู้เชี่ยวชาญ”[17] ดังนั้น

นิติคอมพิวเตอร์ (Computer Forensics) จึงหมายถึง การแสวงหา, เก็บรักษา,วิเคราะห์, และ การนำเสนอพยานหลักฐานที่เกี่ยวกับคอมพิวเตอร์

กล่าวอีกนัยหนึ่งก็คือ การใช้กระบวนการที่จะระบุ, บ่งชี้, เก็บรักษา, และ กู้คืน บรรดาข้อมูลแบบดิจิทัลที่มีความสำคัญต่อการสืบสวน

ผู้ที่เกี่ยวข้องไม่ว่าจะเป็นพนักงานสอบสวนของสำนักงานตำรวจแห่งชาติ, เจ้าหน้าที่กรมสอบสวนคดีพิเศษ (DSI) ของกระทรวงยุติธรรม, เจ้าหน้าที่ของสถาบันนิติวิทยาศาสตร์, ผู้พิพากษา และอัยการ ตลอดจน ทนายความ มีความจำเป็นที่จะต้องเรียนรู้เรื่องComputer Forensics เพื่อที่จะสามารถดำเนินการไต่สวนคดีอาชญากรรมคอมพิวเตอร์ได้อย่างถูกต้องและมีประสิทธิภาพ ศาสตร์เรื่อง Computer Forensics นับเป็นความรู้ขั้นสูงทางด้าน Information Security การรวบรวมและเก็บพยานหลักฐาน (Evidence) ที่อยู่ในรูปของข้อมูลดิจิทัลจำเป็นต้องกระทำโดยผู้ที่มีความเชี่ยวชาญทางด้าน Computer Forensics โดยเฉพาะ มิฉะนั้นข้อมูลที่มีค่าอาจสูญหายไปด้วยความรู้เท่าไม่ถึงการณ์ข้อมูลที่อยู่ในหน่วยความจำ (RAM) สามารถนำมาใช้พิจารณาทางชั้นศาลได้หากมีการจัดเก็บอย่างถูกต้อง ข้อมูลในฮาร์ดดิสก์ถึงแม้จะถูกลบไปแล้ว หรือ ฮาร์ดดิสก์ถูกฟอร์แมตไปแล้ว ก็ยังสามารถเรียกคืนได้โดยโปรแกรมที่มีความสามารถในการกู้ข้อมูลโดยเฉพาะ เช่น Encase หรือ Forensic Tool Kit (FTK) เป็นต้น การกู้ข้อมูลทำให้พนักงานสอบสวนสามารถค้นพบข้อมูลบางอย่าง เช่น ไฟล์ที่ถูกลบไปแล้ว, รหัสผ่านที่ถูกลบไปแล้ว, พฤติกรรมการเข้าถึงไฟล์ของผู้ใช้คอมพิวเตอร์, วันเวลาที่ถูกต้องของเหตุการณ์จาก Log File, อีเมล์ที่ผู้ต้องสงสัยใช้ในการติดต่อกัน, IP Address ของผู้ต้องสงสัยเพื่อสอบไปถึงเบอร์โทรศัพท์ที่ต่อเข้า ISP ตลอดจนร่องรอยที่ทิ้งไว้ในระบบ โปรแกรมที่ใช้ในการ Backup Image ของฮาร์ดดิสก์ที่มีข้อมูลหลักฐานนั้น มีความสำคัญเช่นเดียวกับโปรแกรมที่ใช้ในการกู้ข้อมูล พนักงานสอบสวนควรมีอุปกรณ์คอมพิวเตอร์ที่ใช้ในการปฏิบัติการComputer

---

[17] http://www.cybersecurityinstitute.biz/Definition of computer Forensics: The preservation, identification, extraction, Interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing export opinion in a court of law or other legal and/ or administrative proceeding as to what was found

Forensics โดยเฉพาะเมื่อจะต้องดำเนินการกับ digital evidence ใดๆแล้ว จะต้องปฏิบัติตามหลักสำคัญ ของ general forensic และ ขั้นตอนการดำเนินงาน อย่างเคร่งครัดการจะยึดหลักฐานทาง digital นั้น จะต้องใช้วิธีการที่ ไม่เปลี่ยนแปลง หลักฐานนั้น ในกรณีที่จำเป็นจะต้องให้บุคคลใด เข้าถึง original digital evidence บุคคลนั้นจะต้องผ่านการฝึกอบรม เพื่อการนั้น โดยเฉพาะในทุกกิจกรรมที่เกี่ยวข้องกับ การยึด, การเข้าถึง, การเก็บรักษา, การเคลื่อนย้ายถ่ายโอน digital evidence นั้น จะต้องมีการลงบันทึกเป็นเอกสาร ไว้ทุกขั้นตอน และสามารถตรวจสอบได้ เจ้าหน้าที่ผู้ดำเนินการ จะต้องไม่ทำให้ digital evidence นั้น เกิดความเสียหาย โดยจะต้อง มีจิตสำนึกและรับผิดชอบ เสมือนว่าเป็น ของๆตน เจ้าหน้าที่ทุกฝ่าย จะต้องรู้จักหน้าที่ใน การยึด, การเข้าถึงข้อมูล, การเก็บรักษา ,การถ่ายโอนข้อมูล ที่เป็น digital evidence โดยจะต้องปฏิบัติตามหลักสำคัญดังกล่าวได้แก่

General Definitions relating to digital evidence

*Digital Evidence*

Information stored or transmitted in binary form that may be relied upon in court.

*Original Digital Evidence*

Physical items and those data objects, which are associated with those items at the time of seizure.

*Duplicate Digital Evidence*

A duplicate is an accurate digital reproduction of all data objects contained on the original physical item.

*Copy*

A copy is an accurate reproduction of information contained in the data objects independent of the original physical item.

แนววิธีการปฏิบัติด้าน computer forensic ต้องอยู่ใต้กฎเกณฑ์ดังต่อไปนี้

- ต้องไม่จัดการ ทำงาน หรือ เก็บรวบรวม พยาน หลักฐานอย่างผิดพลาด ไม่ถูกต้องและไม่ถูกวิธี
- ต้องไม่ทำงานกับพยานหลักฐานตัวจริง [ใช้สำเนา]

◆ ต้องไม่ไว้ใจระบบปฏิบัติการ(operating system OS ) ของผู้ต้องสงสัย

◆ ลงบันทึก ทำรายงาน ทุกเรื่อง ทุกแง่มุม ทุกกิจที่ได้ลงมือทำไปทุกขั้นตอนอย่างละเอียด

หลักฐาน มี 3 แหล่ง คือ

(1) ที่เครื่องและอุปกรณ์ ระหว่างทาง

(2) ที่เครื่องและอุปกรณ์ ที่ถูกกระทำ

(3) ที่เครื่องและอุปกรณ์ ผู้กระทำผิด

(1) หลักฐานที่เครื่องและอุปกรณ์ ระหว่างทาง ได้แก่

- Log File
- Traffic Data

(2) หลักฐานที่เครื่องและอุปกรณ์ ที่ถูกกระทำ ได้แก่

- Log file

(3) หลักฐานที่เครื่องและอุปกรณ์ ของผู้กระทำผิด ได้แก่

- Volatile Data ข้อมูลระเหยง่าย ก่อนปิดเครื่อง
- Log file
- ไฟล์ข้อมูลต่างๆ ที่จัดเก็บไว้
- ไฟล์ข้อมูลที่ถูกลบไปแล้ว ฯลฯ

**วิธีการในการสร้างความน่าเชื่อถือของการยึดของกลางที่มีข้อมูลบันทึกอยู่**

- การห่อหุ้ม ของกลาง เพื่อมิให้สามารถเข้าถึงข้อมูลได้
- ให้ การเคลื่อนย้าย ของกลาง ที่มีข้อมูลบันทึกอยู่
- ใช้ เข็มทิศ ตรวจสอบก่อนเคลื่อนย้าย ว่าเส้นทางนั้น มีสนามแม่เหล็กรุนแรง หรือไม่เพราะอาจทำให้ข้อมูล ที่อยู่ใน Hard disk เสียหายได้

- ผู้ต้องหา, ญาติ, บุคคล ที่น่าเชื่อถือ ร่วมกัน ลงลายมือชื่อ ในวัสดุที่ห่อหุ้ม
- การเก็บรักษา ของกลาง ที่มีข้อมูลบันทึกอยู่
- ไม่เก็บในห้องที่มีอุณหภูมิ ร้อน, อบอ้าว, เปียกชื้น, ไม่อยู่กลางแดด ฝน
- ไม่เก็บในห้องที่ มีสนามแม่เหล็ก รุนแรง เพราะอาจทำให้ข้อมูล ที่อยู่ใน Hard disk เสียหายได้
- มีระบบควบคุม รักษาความปลอดภัย

**วิธีการตรวจพิสูจน์ ของกลาง**

- ก่อนการเปิดวัสดุห่อหุ้ม ต้องให้ ผู้ต้องหา, ญาติ, บุคคลที่น่าเชื่อถือ ที่ได้ลงลายมือชื่อไว้ก่อนหน้านั้น ตรวจพินิจว่า มีการฉีกทำลาย วัสดุห่อหุ้มนั้น หรือไม่
- ควรมีการทำบันทึก และถ่ายภาพไว้เป็นหลักฐาน
- หลังจากนั้น จึงทำการ สำเนา Hard disk
- การทำสำเนา โดยการใช้ คำสั่ง ทางคอมพิวเตอร์ มีความน่าเชื่อถือ น้อยกว่า การใช้เครื่องมือ สำเนา Hard disk
- ในระหว่างการทำสำเนา ต้องทำต่อหน้า ควรมีการทำบันทึก และถ่ายภาพไว้เป็นหลักฐาน
- หลังจากนั้น ต้องมีการ ปิดวัสดุห่อหุ้ม ในลักษณะเดิม โดยให้ ผู้ต้องหา, ญาติ, บุคคลที่น่าเชื่อถือ ลงลายมือชื่อไว้
- ควรมีการทำบันทึก และถ่ายภาพไว้เป็นหลักฐาน
- ไม่ตรวจ โดยใช้ Hard disk ของกลาง
- ต้องสำเนาข้อมูล จาก Hard disk ของกลาง ทั้งหมด ลงใน Hard disk ตัวอื่น ที่มีขนาดเท่ากัน หรือใหญ่กว่า

- ใช้ Hard disk ตัวใหม่ เพื่อการตรวจพิสูจน์
- หากผู้ตรวจ พบหลักฐานใด ให้จดบันทึก ชื่อไฟล์ แหล่ง Path ที่อยู่ของข้อมูลนั้น
- สอบปากคำ เพื่อไปแถลงในศาล
- หากมีการต่อสู้ ศาลอาจจะ แต่งตั้งผู้ชำนาญ เพื่อมาตรวจใน Hard disk ของกลาง ต่อไป

หากดำเนินการ ตามขั้นตอนดังกล่าวแล้ว ก็จะสร้างความน่าเชื่อถือได้ว่า นับแต่การยึดของกลางมา จนถึงการตรวจ และฟ้องศาล จะไม่มีผู้ใด มาเพิ่มเติม แก้ไข ลบ ข้อมูล ใดๆ ได้

- ของกลางนั้น ถูกเก็บรักษาในสภาพเดิม
- ขณะตรวจ ไม่มีการแก้ไขข้อมูล

การรวบรวมหลักฐานจากเครื่องของผู้กระทำผิด

- เตรียมสื่อที่จะใช้จัดเก็บข้อมูล
- เก็บข้อมูลที่ระเหยง่าย Volatile Data
- เก็บข้อมูลจาก Hard disk ด้วยวิธี Image
- นำข้อมูลที่ได้มาวิเคราะห์
- โปรแกรมที่ใช้ในการทำ imaging และวิธีการใช้โปรแกรมนี้ในการสร้างหรือทำ image ของฮาร์ดดิสค์ hard disk drive ของผู้ต้องสงสัย จะเป็นเครื่องกำหนดว่าจะได้ imageในรูปแบบหรือ format ใด เมื่อนำออกมาเขียนลงบน hard disk driveที่สะอาด

การเตรียมสื่อที่จะใช้จัดเก็บข้อมูล ได้แก่

**แผ่นดิสต์**

- ล้างข้อมูลในแผ่นดิสก์ ตามกรรมวิธี เป็นขั้นตอน
- เลือกโปรแกรมที่จำเป็นที่จะบันทึกในแผ่นดิสก์

- จัดทำ MD5 โปรแกรมดังกล่าว ก่อนบันทึก แล้วบันทึกลงในแผ่นดิสก์
- บันทึกโปรแกรมที่จำเป็น ลงในแผ่นดิสก์
- จัดทำ MD5 โปรแกรมดังกล่าว หลังบันทึก แล้วบันทึกลงในแผ่นดิสก์

**Hard Disk**

- Hard Disk ต้องมีขนาดไม่น้อยกว่าเป้าหมาย
- ล้างข้อมูลใน Hard Disk ตามกรรมวิธี เป็นขั้นตอน

เมื่อถึงที่เกิดเหตุ

- ถ้าเครื่องยังไม่ได้ปิด และมีความจำเป็นต้องใช้ ข้อมูลที่ระเหยง่าย Volatile Data ให้นำแผ่นดิสก์ ที่เตรียมไว้ จัดเก็บข้อมูลที่ระเหยได้ก่อน เป็นอันดับแรก ลงในแผ่นดิสก์นั้น
- ทำสำเนาไว้ใช้ภายหลัง แผ่นจริงส่งศาล แผ่นสำเนาใช้วิเคราะห์
- ข้อมูลที่ระเหยง่าย ได้แก่ วันเวลาที่เปิดเครื่อง, รายละเอียดในการใช้งาน, ไฟล์ที่สร้าง, ไฟล์ที่ลบ ฯลฯ
- นำ Hard Disk ที่เตรียมไว้ ใช้โปรแกรมจัดทำ Image
- ห่อหุ้มเครื่องของกลาง ให้พยานลงลายมือชื่อ ในวัสดุที่ห่อหุ้ม
- ถ่ายภาพ วิดีโอ ทำบันทึก ไว้เป็นหลักฐาน

สิ่งที่เกี่ยวข้องกับการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์มีดังนี้

1. การเก็บรักษาไว้ – เมื่อมีการวิเคราะห์การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ จะต้องทำทุกอย่างที่เป็นไปได้ในการเก็บรักษาสื่อและข้อมูลต้นฉบับ โดยปกติแล้วจะเกี่ยวกับรูปจำลองทางการตรวจพิสูจน์หลักฐาน (Forensic image) หรือสำเนาของสื่อต้นฉบับและทำการวิเคราะห์จากทั้งสำเนาและต้นฉบับ

2. การชันสูตร – ในขั้นต้น เป็นการตรวจพิสูจน์สิ่งที่ใช้บรรจุหลักฐานที่เกี่ยวกับคอมพิวเตอร์ เช่น อุปกรณ์เก็บข้อมูล (Hard drive) ฟลอปปี้ดิสก์ และไฟล์ คอมพิวเตอร์หรือ

อุปกรณ์เก็บข้อมูล (Hard drive) เองไม่ใช่หลักฐาน ขั้นตอนต่อไปคือการวิเคราะห์เป็นการตรวจพิสูจน์ข้อมูลที่เกี่ยวข้องกับสถานการณ์ที่มีอยู่ ค้นหาคำสำคัญ และตรวจดูไฟล์ต่าง ๆ

3. การดึงหรือถอนหลักฐานที่พบออกมา – หลักฐานที่พบต้องดึงออกมาจากสื่อนั้นและเก็บไว้ในสื่ออื่นรวมถึงพิมพ์ออกมาเป็นกระดาษ

4. การอธิบายผล – มีเครื่องมือหรือโปรแกรมที่เรียกว่า Graphical User Interface (GUI) ซึ่งเป็นวิธีการใช้งานของผู้ใช้คอมพิวเตอร์ที่เลือกเฟ้น โปรแกรม หรือคำสั่งโดยชี้ไปยังรูปภาพแทนสิ่งเหล่านั้นบนจอภาพแทนการป้อนคำสั่งยาว ๆ ความสามารถค้นหาหลักฐานเป็นสิ่งหนึ่งที่สำคัญ แต่ความสามารถในการอธิบายอย่างถูกต้องเป็นอีกอย่างหนึ่งที่สำคัญเช่นกัน ตัวอย่างเช่นผู้เชี่ยวชาญฝ่ายอัยการในคดีหนึ่งได้ใช้ GUI ที่ใช้สำหรับหากิจกรรมของโปรแกรมการค้นหาข้อมูลในอินเตอร์เน็ต (Internet search engine) พบว่า มีการค้นหานับเป็นร้อย ๆ ครั้ง ซึ่งคาดว่ากระทำโดยจำเลย และจำเลยมีเจตนาเข้าไปดูข้อมูลเฉพาะประเภท การค้นหาจึงสามารถแสดงถึงเจตนาได้ แต่ผู้เชี่ยวชาญฝ่ายจำเลยตรวจสอบพยานหลักฐานเดียวกันพบว่าการค้นหาในแต่ละครั้งเป็นเรื่องการเชื่อมต่อกับเอกสารอื่นหรือ Hyperlink และไม่ใช่เป็นการค้นหาเลย การเชื่อมต่อกับเอกสารอื่นเป็นการกดปุ่มคลิกฐานข้อมูลที่ถูกค้น เพื่อดึงข้อมูลที่เกี่ยวเนื่องกับการเชื่อมโยงนั้น วิธีการในการเชื่อมต่อคือ การที่ GUI เข้าไปในช่องทางซึ่งเป็นขณะเดียวกับการเชื่อมต่อเหล่านั้นทำงานซึ่งคล้ายกับเว็บเพจที่สามารถพบได้ และเป็นเครื่องชี้ให้เห็นว่าเป็นกิจกรรมของโปรแกรมการค้นหาข้อมูลหรือ Search engine ผู้เชี่ยวชาญฝ่ายอัยการทึกทักเอาเองว่า เครื่องมืออัตโนมัติจะเกี่ยวข้องกับตัวแปรทุกตัวและสามารถแสดงการค้นที่แท้จริงได้ จึงเป็นการเข้าใจที่ผิด ผู้เชี่ยวชาญจึงขาดทักษะทางเทคนิคในการอธิบายผลที่แท้จริงและทำตัวพึ่งกับเครื่องมืออัตโนมัติเพียงอย่างเดียว ในคดีนี้ปรากฏต่อไปว่าผู้เชี่ยวชาญฝ่ายจำเลยพบอีเมล์จำนวนมากในขณะที่ผู้เชี่ยวชาญฝ่ายอัยการหาไม่พบ โดยทั้งผู้เชี่ยวชาญฝ่ายจำเลยและผู้เชี่ยวชาญฝ่ายอัยการใช้เครื่องมือในการวิเคราะห์ที่เหมือนกัน แต่ความแตกต่างเกิดจากประสบการณ์และความชำนาญของผู้เชี่ยวชาญ ไม่ใช่เครื่องมือที่ใช้

5. การจัดทำเอกสาร – เอกสารควรเก็บไว้ตั้งแต่เริ่มต้นจนจบเนื่องจากเป็นส่วนหนึ่งของเส้นทางการเก็บรักษาหรือ Chain of custody และเป็นสิ่งที่ต้องนำส่งศาลในที่สุด

6. กฎเกณฑ์พยานหลักฐาน – จะเกี่ยวกับเรื่องการเบิกความของผู้เชี่ยวชาญ การรับฟังพยานหลักฐาน ความเชื่อมั่น และความเกี่ยวข้องกับคดี นอกจากนั้นในบางประเทศ เช่น สหรัฐอเมริกา อาจมีการรับฟังพยานหลักฐานทางวิทยาศาสตร์ที่ต้องผ่านการทดสอบหรือหลักเกณฑ์ที่ได้วางหลักในคดีบรรทัดฐานก่อน เช่น the Frye test และ the Daubert test

7. กระบวนการทางกฎหมาย – เกี่ยวกับการออกหมายค้น การให้การเป็นพยาน การพิจารณาคดี การสอบสวน และการเปิดเผยเรื่องราวสาระ เป็นต้น

8. ความน่าเชื่อถือของพยานหลักฐาน – เป็นเรื่องการควบคุมทุกอย่างที่เกี่ยวกับคดีและสถานการณ์ เป็นเรื่องเส้นทางการเก็บรักษาหรือ Chain of custody และความแน่ใจว่าสื่อต้นฉบับไม่ถูกเปลี่ยนแปลง

9. การรายงานข้อเท็จจริงของข้อมูลที่พบ – ซึ่งควรจะสามารถในการกระทำซ้ำผลที่ได้ด้วย

10. การเตรียมการเกี่ยวกับความเห็นของผู้เชี่ยวชาญ – อาจต้องมีการเบิกความในสิ่งที่พบและความเห็นต่าง ๆ ในศาลหรือที่อื่น

การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์สามารถใช้ประโยชน์ในการนำมาใช้เปิดเผยหลักฐานที่เป็นไปได้ในกรณีต่าง ๆ รวมถึง

- การละเมิดลิขสิทธิ์
- การละเมิดสิทธิคนอื่น
- การล่วงละเมิดทางเพศ
- การฉ้อโกง
- การคอร์รัปชั่น
- การจารกรรมทางอุตสาหกรรม
- การฟอกเงิน
- การทำลายข้อมูล
- การขู่เข็ญเอาเงิน
- การถอดรหัสข้อมูล
- การโจรกรรมทรัพย์สินทางปัญญา
- การใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาต
- สิ่งลามกอนาจารเกี่ยวกับเด็ก
- การทำซ้ำโปรแกรมคอมพิวเตอร์
- การเข้าถึงข้อมูลส่วนตัวโดยไม่ได้รับอนุญาต

การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์เป็นการรวมเทคนิคพิเศษต่าง ๆ โดยใช้โปรแกรมคอมพิวเตอร์ที่ซับซ้อนในการตรวจ[18] และวิเคราะห์ข้อมูลที่ไม่สามารถเข้าถึงได้โดยผู้ใช้

โดยปกติข้อมูลอาจถูกลบทิ้งโดยผู้ใช้เป็นเดือนหรือปีก่อนที่มีการสืบสวน หรืออาจไม่ได้เก็บเอาไว้ แต่อาจยังคงมีอยู่ทั้งหมดหรือบางส่วนในอุปกรณ์เก็บข้อมูล (Hard drive)

ผู้เชี่ยวชาญทางการตรวจพิสูจน์หลักฐานสามารถช่วยเหลือการทำคดี ซึ่งจะเป็นประโยชน์อย่างยิ่งสำหรับทนายความ ลูกความ และคดีต่าง ๆ การช่วยเหลือดังกล่าวสามารถทำได้ในรูปของ

- การสืบหาหรือทำให้แน่ใจว่าคอมพิวเตอร์ที่มีปัญหาจะมีข้อมูลที่เกี่ยวข้องกับคดีหรือไม่
- การช่วยเหลือในการเตรียมและตอบคำซักถามเกี่ยวกับหลักฐานที่ค้นพบ
- การกู้หรือเอาคืนและตรวจสอบข้อมูลที่สามารถเข้าถึงโดยการใช้โปรแกรมหรือวิธีการทางการตรวจพิสูจน์หลักฐาน
- การทำรายงานต่าง ๆ ที่ใช้ในศาล
- การวางแผนและจัดหาการเบิกความของผู้เชี่ยวชาญ

ในการพิจารณาว่าคอมพิวเตอร์มีข้อมูลที่สามารถใช้เป็นหลักฐานได้หรือไม่ ผู้ที่เป็นมืออาชีพจำเป็นต้องสร้างรูปจำลองที่เหมือนกันกับอุปกรณ์เก็บข้อมูล (Image drive)[19] เพื่อป้องกันการเปลี่ยนแปลงสิ่งที่มีอยู่หรือต้นฉบับ รูปจำลองที่สร้างขึ้นดังกล่าวต้องเป็นภาพที่สะท้อนถึงสิ่งที่มีอยู่ ไม่เพียงแต่เป็นสำเนาข้อมูลแบบง่าย ๆ การที่จะได้รับสำเนาที่ถูกต้องนี้ต้องใช้เทคนิคทางการตรวจพิสูจน์หลักฐานเฉพาะ

รูปจำลองที่ใช้นี้เป็นสิ่งที่วิกฤตเพราะในแต่ละครั้งหากมีใครเปิดเครื่องคอมพิวเตอร์จะมีการเปลี่ยนแปลงเกิดขึ้นโดยอัตโนมัติกับไฟล์ต่าง ๆ การเปลี่ยนแปลงนี้ไม่สามารถมองเห็นได้ แต่สามารถเปลี่ยนแปลงแม้กระทั่งลบหลักฐานได้ เช่น วันที่ที่มีการประกอบอาชญากรรม เส้นทางการเก็บรักษาหรือ Chain of custody มีความสำคัญต่อผู้เชี่ยวชาญที่ควบคุมการสร้างรูปจำลอง และประเมินข้อมูลในการนำไปใช้เป็นพยานหลักฐานเช่นเดียวกับในทางนิติเวชศาสตร์ กรณีเช่นนี้ผู้เชี่ยวชาญจะใช้รหัสที่เรียกว่า Hash codes หรือรหัสที่สร้างขึ้นตามวิธีการที่

---

[18] โปรดดูรายละเอียดการทำงานของโปรแกรมคอมพิวเตอร์ที่ภาคผนวก ข หน้า 97

[19] Image หรือ Imaging

เป็นคำที่ใช้เพื่อบรรยายกระบวนการในการทำสำเนาแบบบิทต่อบิท (bit for bit) ของ hard disk drive ที่เป็นพยานหลักฐาน หรือ สำเนาของสื่อแบบอิเล็กทรอนิกส์ ที่ใช้เก็บ/บรรจุข้อมูล(storage media) ภาพ หรือ image นี้ อาจมาในรูปสำเนา ส่วนต่อส่วน ที่ตรงกันทุกอย่าง หรืออาจมาในรูปไฟล์แบบภาพ (image files)

โปรแกรมเก็บข้อมูลตามการคำนวณทางคณิตศาสตร์หรือฟังก์ชันย่อยข้อมูล เพื่อรักษาหรือดูแลเส้นทางการเก็บรักษา Hash codes เป็นเลขมาก ๆ ที่กำหนดเฉพาะไฟล์แต่ละไฟล์และในแต่ละอุปกรณ์เก็บข้อมูล (Drive) โดยการคำนวณทางคณิตศาสตร์ ถ้าหากไฟล์หรืออุปกรณ์เก็บข้อมูล (Drive) ถูกเปลี่ยนไปไม่ว่าจะน้อยมากที่สุดก็ตาม Hash codes จะเปลี่ยนแปลงเช่นกัน Hash codes เหล่านี้จะถูกคำนวณบนต้นฉบับและรูปจำลองในจุดต่าง ๆ ระหว่างการสืบสวนเพื่อที่จะทำให้แน่ใจว่ากระบวนการตรวจสอบไม่ได้มีการปรับแต่งรูปจำลองที่กำลังตรวจสอบอยู่

การวิเคราะห์การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์เป็นสิ่งที่มีประโยชน์ ในกรณีที่ข้อมูลส่วนบุคคลอาจจะถูกเก็บในคอมพิวเตอร์ อาทิ ในคดีหย่าร้างเรื่องหนึ่ง สามีซ่อนเงินที่เป็นสินสมรสในบัญชีลับของธนาคาร ในคดีอื่น ๆ เช่น ลูกจ้างใช้ชื่อโปรแกรมคอมพิวเตอร์ซ้ำกับโปรแกรมที่พัฒนาโดยนายจ้างปัจจุบันเพื่อที่เปิดบริษัทใหม่ของลูกจ้าง หรือกรณีลูกจ้างผู้ชายส่งอีเมล์ที่เชิญชวนไปยังผู้ร่วมงานผู้หญิงเป็นเวลานานนับหลายเดือน แม้ว่าคู่ความดังกล่าวนี้จะลบข้อมูลจากคอมพิวเตอร์ แต่ผู้เชี่ยวชาญทางการตรวจพิสูจน์หลักฐานสามารถกู้เอาหลักฐานจากอุปกรณ์เก็บข้อมูล (Drive) คืนได้

การที่จะกู้เอาหลักฐานที่ลบไปคืนมานั้นสามารถทำได้ ระบบปฏิบัติการคอมพิวเตอร์จะมีไดเรกทอรีที่มีชื่อและที่อยู่ของไฟล์แต่ละไฟล์อุปกรณ์เก็บข้อมูล (Drive) เมื่อไฟล์หรือแฟ้มงานถูกลบไป จะมีเหตุการณ์ต่าง ๆ เกิดขึ้นในคอมพิวเตอร์ จะมีเครื่องชี้บ่งสถานภาพของไฟล์ หรือ File status marker ที่แสดงว่าไฟล์ได้ถูกลบไป และมีเครื่องชี้บ่งสถานภาพของดิสก์หรือ Disk status marker ที่แสดงว่ามีช่องว่างอยู่สำหรับใช้ประโยชน์ได้

ช่องว่างที่มีใหม่นี้เรียกว่า ช่องว่างที่ยังไม่ถูกจัดสรรหรือยังว่างอยู่ (Free or unallocated space) ระหว่างที่ช่องว่างดังกล่าวยังไม่ถูกเขียนทับโดยไฟล์อื่น ผู้เชี่ยวชาญจะสามารถกู้คืนไฟล์ได้ทั้งหมด การเขียนทับจะเกิดจากการกระทำของผู้ใช้ เช่น การเพิ่มโปรแกรมใหม่หรือสร้างเอกสารใหม่โดยเขียนทับลงในช่องว่างที่ไฟล์ที่ถูกลบทิ้งเคยอยู่ เมื่อข้อมูลถูกเขียนทับโดยข้อมูลใหม่ ส่วนหนึ่งหรือทั้งหมดของไฟล์จะไม่สามารถกู้คืนได้โดยใช้เทคนิคทางการตรวจพิสูจน์หลักฐาน

ช่องว่างที่สามารถนำมาใช้ได้ในอุปกรณ์เก็บข้อมูล (Hard drive) ของคอมพิวเตอร์จะแบ่งออกเป็นส่วน ๆ ที่เรียกว่า เซกเตอร์ (Sector) ที่มีขนาดเท่ากัน หากผู้ใช้ต้องการที่จะเก็บข้อมูล ระบบปฏิบัติการของคอมพิวเตอร์จะตรวจสอบโดยอัตโนมัติว่าเซกเตอร์ใดที่จะนำมาใช้ในหลายกรณี ข้อมูลที่จะเก็บจะไม่ใช้ช่องว่างทั้งหมดที่มีอยู่ในเซกเตอร์ที่ถูกกำหนดว่าจะใช้กรณีเช่นนี้ ข้อมูลที่เคยเก็บในอุปกรณ์เก็บบันทึกยังคงมีอยู่ในส่วนของเซกเตอร์ที่ถูกำหนดที่ยังไม่ได้ใช้ ซึ่งเรียกว่า Slack space ซึ่งหมายความแม้ส่วนของอุปกรณ์เก็บข้อมูล (Drive) ถูกเขียนทับด้วยข้อมูลใหม่ โอกาสที่มีคือจะมีหลักฐานที่เกี่ยวข้องยังคงอยู่ในส่วนของเซกเตอร์ที่ถูกกำหนดที่ยังไม่ได้ใช้ ข้อมูลดังกล่าวนี้จะถูกกู้คืนได้โดยใช้เทคนิคทางการตรวจพิสูจน์หลักฐาน

ผู้เชี่ยวชาญการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์จะทราบวิธีการเข้าสู่ช่องว่างที่ยังไม่ถูกจัดสรรหรือยังว่างอยู่ กับส่วนของเซกเตอร์ที่ถูกกำหนดที่ยังไม่ได้ใช้ รวมทั้งช่องอื่น ๆ ของข้อมูลที่ซ่อนอยู่โดยใช้เครื่องมือที่เหมาะสม ทำให้สามารถที่จะกู้ข้อมูลคืนได้ข้อมูลที่ซ่อนอยู่จะมีรายละเอียดเกี่ยวกับสิ่งที่เกิดขึ้นในคอมพิวเตอร์ เช่น เว็บไซต์ที่ผู้ใช้ได้ใช้ อีเมล์ที่ส่งและรับ ธุรกรรมทางอินเตอร์เน็ตที่เกี่ยวกับการเงิน เอกสาร จดหมาย และรูปภาพที่ได้ถูกสร้างขึ้น ถูกแก้ไขหรือถูกเข้าถึง แม้ว่าข้อมูลไม่ได้เก็บไว้ในคอมพิวเตอร์ก็ตาม การทำงานเช่นว่านี้เกิดได้อย่างไร หากต้องการให้ข้อมูลของผู้ใช้มองเห็นจากจอคอมพิวเตอร์ ระบบจะเก็บข้อมูลไว้ในสถานที่ชั่วคราว เมื่อคอมพิวเตอร์ปิดลง ข้อมูลจะยังคงมีอยู่ในสถานที่ชั่วคราวนั้นแม้ว่าผู้ใช้จะไม่เก็บไว้เป็นไฟล์ก็ตาม

เมื่อผู้ใช้เข้าสู่อินเตอร์เน็ต โปรแกรมเบราว์เซอร์ซึ่งเป็นโปรแกรมที่ใช้แสดงข้อมูลบนอินเตอร์เน็ตจะเก็บเรคคอร์ดหรือรายชื่อของเว็บไซต์ที่ผู้ใช้ได้เข้าไปคุ้กกี้[20] ซึ่งเป็นไฟล์ที่เบราว์เซอร์ใช้ในการตามกิจกรรมของผู้ใช้ในอินเตอร์เน็ต ซึ่งจะมีรหัสผ่าน ( Password) และข้อมูลอื่นเกี่ยวกับการปฏิบัติของผู้ใช้อินเตอร์เน็ต[21] โปรแกรมเฉพาะรวมถึง Microsoft Word สามารถเก็บข้อเท็จจริงเอาไว้เกี่ยวกับเอกสารต่าง ๆที่ถูกสร้างขึ้น ถูกปรับปรุง หรือถูกเข้าไปภายในเอกสารเหล่านั้น ข้อเท็จจริงนี้เรียกว่า Metadata[22] ซึ่งบันทึกเหตุการณ์ของเอกสารเป็นลำดับเวลา รวมถึงการแสดงถึงผู้ที่ปรับแก้และเก็บเอกสาร ไดเรกทอรี และเครื่องพิมพ์ที่ใช้พิมพ์ ผู้เชี่ยวชาญทางการตรวจพิสูจน์หลักฐานคอมพิวเตอร์สามารถกู้ Metadata และทราบถึงประวัติของเอกสารได้

ในบางกรณี แม้ผู้ใช้จะมีอุปกรณ์เก็บข้อมูลที่ถูกจัดการพื้นที่แต่ละส่วนของแฟ้มข้อมูลที่อยู่กันอย่างกระจัดกระจายและนำมาใช้เรียงชิดติดกันหรืออุปกรณ์เก็บข้อมูลที่ถูกจัดรูปแบบแล้วหลักฐานยังสามารถกู้คืนได้

### 2.4.1 ปัญหาทางกฎหมายเกี่ยวกับการพิสูจน์พยานหลักฐานของข้อมูลอิเล็กทรอนิกส์

คอมพิวเตอร์เข้ามาเกี่ยวข้องกับการพิจารณาพิพากษาคดี ในการสืบสวนหรือหาพยานหลักฐานทางคอมพิวเตอร์ที่ต้องมีความแท้จริง ถูกต้อง สมบูรณ์ น่าเชื่อถือ และรับฟังเป็นพยานหลักฐานได้ ดังนั้น เพื่อที่จะให้ได้มาซึ่งพยานหลักฐานที่มีคุณสมบัติดังกล่าวการใช้นิติคอมพิวเตอร์จึงควรมีองค์ประกอบดังต่อไปนี้ด้วย

---

[20] ไฟล์เล็ก ๆ ที่เก็บไว้บนคอมพิวเตอร์ซึ่งสร้างขึ้นจากเว็บไซต์ที่ผู้เข้าไปเยี่ยมชม โดยมีจุดมุ่งหมายในการบอกข้อมูลของผู้ใช้ เมื่อมีการเข้าสู่เว็บไซต์นั้น ๆ อีกครั้ง

[21] คุ้กกี้สามารถถูกลบออกโดยผู้ใช้ที่ทราบ และเขียนสถานที่ทับซ้อนลงไป ถ้าไม่ทำเช่นนั้นแล้วการสืบสวนทางการตรวจพิสูจน์หลักฐานสามารถทราบถึงรายชื่อของเว็บไซต์ที่ผู้ใช้ได้เข้าไป

[22] ส่วนของข้อมูลที่ใช้ควบคุมข้อมูล มีลักษณะที่จะบ่งบอกให้รู้ว่าข้อมูลนี้เป็นประเภทอะไร ใครเป็นผู้สร้าง หรือนำข้อมูลใช้เพื่ออะไร

1. เป็นกระบวนการที่อธิบายได้ชัดเพื่อใช้กับงานต่าง ๆ

2. มีความคาดหวังว่า คู่ความอีกฝ่ายจะโต้แย้งว่า ไม่สามารถแสดงให้เห็นความแท้จริง ความเชื่อมั่น ความสมบูรณ์ และความเป็นไปได้ของการเสื่อมสภาพที่เป็นผลตามมาจากการสืบสวน

3. มีความเป็นไปได้ว่าจะเกิดการทดสอบอีก หากมีโดยผู้เชี่ยวชาญที่จ้างโดยคู่ความอีกฝ่ายหนึ่งและ

4. มีความคาดหวังว่าจะเกิดปัญหาในการทดสอบทางกฎหมายที่เป็นเกณฑ์ในเรื่องการรับฟังพยานหลักฐาน

อย่างไรก็ตาม ยังคงมีความแตกต่างในเรื่องการสืบสวนเรื่องดังกล่าวแบบเดิม ๆ นิติคอมพิวเตอร์มีอัตราการเปลี่ยนแปลงของเทคโนโลยีคอมพิวเตอร์อย่างรวดเร็ว เช่น การทดสอบในเรื่องความมีอยู่ของยาเสพติด วัตถุระเบิด ใยผ้า เนื้อเยื่อร่างกาย เป็นต้น ที่คาดหวังว่าหากเวลาผ่านไป การทดสอบดังกล่าวอาจถูกแก้ไขหรือพบว่ามีข้อผิดพลาด แต่จุดประสงค์ที่แท้จริงของการทดสอบและรายละเอียดที่จำเป็นยังคงไม่เปลี่ยนแปลง ซึ่งความใหม่และความล้าสมัยเป็นเรื่องปกติและจะเกิดขึ้นในเทคโนโลยีคอมพิวเตอร์

**2.4.2 กฎหมายที่เกี่ยวกับการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์หรือนิติคอมพิวเตอร์ในต่างประเทศ**

ในประเทศสหรัฐอเมริกาได้มีการออกกฎหมายที่กระทบต่อนิติคอมพิวเตอร์ คือ The Electronic Communication Privacy Act (ECPA) The Wiretap Statue The Pen/Trap Statue และ The USA PATRIOT Act และ The Sarbanes – Oxley Act of 2002

**2.4.2.1 The Electronic Communication Privacy Act (ECPA) 1986**

ECPA เป็นอำนาจทางกฎหมายในการควบคุมในกรณีของไฟล์คอมพิวเตอร์ที่เก็บไว้ (Stored) ที่ถูกส่งไปยังผู้บริหารเครือข่าย (Network administrator) ซึ่งต่างจากการดักฟัง (Interception) ที่การสื่อสารเป็นเวลาในขณะนั้นที่อยู่ภายใต้ the Wiretap statue

ข้อมูลคอมพิวเตอร์ที่เก็บไว้รวมถึง การสื่อสารอินเทอร์เน็ตทั้งหมด เช่น อีเมล์ที่เก็บไว้ในเครื่องแม่ข่ายของผู้ให้บริการ (Internet Service Provider (ISP)) ข้อมูลที่เก็บในเครือข่ายมีระดับการป้องกันความเป็นส่วนบุคคลในระดับต่าง ๆ กัน ขึ้นอยู่กับความสำคัญหรือความไวต่อความรู้สึกของข้อมูล ใน Title 18 , Section 2703 ของ the U.S. Code พระราชบัญญัติ ECPA จึงมีระดับอยู่ 5 ระดับ ซึ่งระดับใดที่มีความไวต่อความรู้สึกมากขึ้นความชอบธรรมที่รัฐบาลต้องแสดงเพื่อให้ได้รับข้อมูลจากบุคคลที่สามก็จะมากขึ้นโดยเฉพาะผู้บริหารระบบ ข้อมูลที่ไวต่อความรู้สึกมากที่สุดประกอบด้วยเนื้อหาการสื่อสารที่ไม่ได้ถูกนำมาใช้อีก เช่น อีเมล์ที่อยู่ในการเก็บข้อมูลทางอิเล็กทรอนิกส์เป็นเวลา 180 วันหรือน้อยกว่า

แต่หลังจาก 180 วัน ข้อมูลดังกล่าวเป็นข้อมูลที่ไม่สดและไม่ได้รับการคุ้มครองในอันดับต้น ๆ และไม่ต้องใช้หมายค้นในการเข้าถึงข้อมูลนั้น ส่วนข้อมูลที่ไวต่อความรู้สึกน้อยที่สุดรวมถึงข้อมูลพื้นฐานเท่านั้น เช่น ชื่อของสมาชิก และใบเสร็จจ่ายอย่างไร การได้รับข้อมูลดังกล่าวนี้ รัฐบาลจำเป็นเพียงออกหมายเรียกทางฝ่ายบริหาร (An administrative subpoena) เท่านั้น หมายเรียกดังกล่าวออกโดยหน่วยงานของรัฐโดยไม่ต้องขออนุญาตศาลก่อน เช่น FBI สามารถออกหมายเรียกในเหตุอันสมควร หากในภายหลังมีการคัดค้านและศาลเห็นว่าไม่มีเหตุสมควร ข้อมูลที่ได้รับภายใต้หมายเรียกก็จะถูกยกเลิกไป

#### 2.4.2.2 The Wiretap Statute (Title III), amended 1986

พระราชบัญญัตินี้จะเกี่ยวข้องกับการดักฟังโดยตรง หรือการดักฟังการสื่อสารทางอิเล็กทรอนิกส์ในเวลานั้นโดยหน่วยงานของรัฐบาล พระราชบัญญัติรู้จักในนามของ Title III เพราะในครั้งแรกออกมาเป็น Title III ของพระราชบัญญัติ The Omnibus Crime Control and Safe Streets ปี 1968[23] ผู้ที่สืบสวนที่จะเข้าถึงเข้าสู่คอมพิวเตอร์ที่เป็นเป้าหมายในขณะที่ข้อมูลข่าวสารกำลังส่งจะต้องใช้กฎหมาย the Wiretap statute ซึ่งส่วนมากจะมีใช้กับการสนทนาทางโทรศัพท์ ก่อนที่รัฐบาลจะต่อสายดักฟังโทรศัพท์ได้จะต้องมีคำสั่งจากศาล ศาลมีคำสั่งตามจำนวนความชอบธรรมที่ต้องแสดงให้เห็นในตอนออกคำสั่งนั้น มาตรา 2518 ของ Wiretap statute ได้กำหนดจำนวนความชอบธรรมที่มีนัยสำคัญ รวมถึงการแสดงเหตุอันควรสงสัยที่จะเชื่อว่าการดักฟังจะทำให้เกิดพยานหลักฐานที่เกี่ยวกับการกระทำผิดโทษหนัก; กระบวนการการสืบสวนตามปกติจะล้มเหลวมีแนวโน้มว่าจะไม่สำเร็จหรืออันตรายเกินไป; คอมพิวเตอร์หรือเครื่องมืออิเล็กทรอนิกส์ที่ใช้ในการกระทำผิด และการสืบสวนจะทำการดักฟังน้อยที่สุดในการสื่อสารที่บริสุทธิ์ ถ้าศาลพอใจว่าข้อกำหนดทั้งหมดมีอยู่ ศาลก็จะเซ็นคำสั่งดังกล่าวให้บุคคลเป้าหมายจะได้รับแจ้งหลังจากคำสั่งดักฟังหมดไป

กรณีดังกล่าวมีความแตกต่างจากคำสั่งศาลสำหรับเครื่องมือที่ใช้ดักการสื่อสาร ที่ออกไปและเข้ามาที่เรียกว่า Pen/Trap ที่ใช้เพียงข้อความของผู้สืบสวนว่าตนเชื่อว่าข้อมูลที่จะได้รับจะเกี่ยวข้องกับการสืบสวนทางอาญา ดังที่จะกล่าวต่อไป

#### 2.4.2.3 The Pen/Trap Statute, amended 2001

The Pen/Trap Statute[24] กำหนดรูปแบบการเข้าไปของรัฐที่ล่วงล้ำน้อยกว่าใน Wiretap statute กฎหมายนี้ให้อำนาจในการติดตั้ง Pen register และ Trap-and-trace โดย Pen register จะบันทึกการหมุนโทรศัพท์ เส้นทาง และแสดงข้อมูลที่เกี่ยวกับการสื่อสาร

---

[23] 18 United States Code Sec. 2510 – 2522, amended in 1986.

[24] 18 United States Code Sec. 3121- 3127.

อิเล็กทรอนิกส์ที่ออกไป (outgoing) การสื่อสารอิเล็กทรอนิกส์หมายถึง โทรศัพท์ คอมพิวเตอร์ โทรเลข และโทรพิมพ์ ส่วนเครื่องมือ trap-and-trace จะบันทึกข้อมูลเช่นเดียวกันแต่เป็นการสื่อสารที่เข้ามา (incoming) แต่ข้อเท็จจริงที่สำคัญคือทั้งสองแบบจะไม่บันทึกเนื้อหาของการสื่อสาร เพียงแต่บันทึกข้อมูลที่เกี่ยวกับเบอร์โทรศัพท์ทั้งที่เป็นการเรียกออกและเรียกเข้า

#### 2.4.2.4 The USA PATRIOT ACT 2001

โดยปกติผู้ที่เป็นเป้าหมายในการค้นจะถูกแจ้งให้ทราบในเวลาที่มีการค้นทางกายภาพ แต่พระราชบัญญัตินี้อนุญาตให้มีการแจ้งให้ทราบภายหลัง (Delayed notification) ซึ่งเป็นบทบัญญัติที่เรียกว่า “แอบมอง”

นอกจากนี้พระราชบัญญัตินี้ทำให้ผู้ที่ใช้กฎหมายสามารถติดตั้งเครื่องมือการลอบติดตามอิเล็กทรอนิกส์ง่ายขึ้น เดิมคำสั่งการดักฟังหรือคำสั่ง Pen register ขอออกได้ในเขตอำนาจที่เครื่องมือนั้นติดตั้ง แต่การสื่อสารทางอินเตอร์เน็ตจะเกี่ยวกับผู้ให้บริการอินเตอร์เน็ตตั้งอยู่ในเขตอำนาจต่าง ๆ กัน มาตรา 216 และ 220 จึงอนุญาตให้มีการติดตั้งเครื่องมือทุกแห่งในสหรัฐอเมริกา

มาตรา 225 มีความสำคัญต่อผู้ที่ทำการสืบสวนทางนิติคอมพิวเตอร์ และผู้ให้ข้อมูลแก่รัฐบาล ทั้งให้ความคุ้มกันในการฟ้องร้องคดีทางแพ่งกับบุคคลใดที่ให้ความช่วยเหลือทางเทคนิคหรืออื่น ๆ ในการได้มาซึ่งข้อมูลทางอิเล็กทรอนิกส์ตามคำสั่งศาล หรือตามที่ร้องขอตามกฎหมายในการให้ความช่วยเหลือฉุกเฉิน

พระราชบัญญัตินี้บัญญัติขยายขอบเขตการสืบสวนออกไป แต่อย่างไรก็ตามยังมีบทบัญญัติการสิ้นสุดหรือ “Sunset” provision ซึ่งบัญญัตินี้จะสิ้นสุดในวันที่ 31 ธันวาคม ค.ศ. 2005 ถ้าสภาคองเกรสไม่ขยายเวลาต่อไป แต่บทบัญญัติการสิ้นสุดนี้ไม่ใช้กับพระราชบัญญัติทั้งฉบับ ส่วนที่สำคัญเช่นการให้อำนาจในการแจ้งการค้นในภายหลังและคำสั่งการดักฟังจะไม่สิ้นสุดโดยอัตโนมัติ

นิติคอมพิวเตอร์ได้รับการรองรับโดยพระราชบัญญัตินี้ตามมาตรา 816 โดยให้งบประมาณจำนวน 50 ล้านเหรียญสหรัฐ ในการสร้างและสนับสนุนห้องปฏิบัติการนิติคอมพิวเตอร์ภูมิภาค ห้องปฏิบัติการนี้จะทำการสืบสวนและฝึกอบรมผู้ที่ทำการสืบสวน

#### 2.4.2.5 The Sarbanes-Oxley Act of 2002[25]

พระราชบัญญัติฉบับนี้ออกมาสืบเนื่องจากเหตุการณ์คดี United States of America v. Arthur Andersen LLP ของศาล United States District Court Southern District

---

[25] John Patzakis, **International Journal of Digital Evidence Spring 2002**, Volume 2 , Issue 1.

of Texas กล่าวคือ วันที่ 15 มิถุนายน ค.ศ.2002 แอนเดอร์เสนถูกตัดสินในข้อหาต่อต้านความยุติธรรมโดยทำลายเอกสารที่เกี่ยวกับการตรวจสอบการเงิน (Audit) ของ เอ็นรอน (Enron) ลูกค้า จึงเป็นผลให้คณะกรรมการหุ้นและหลักทรัพย์ไม่อนุญาตให้แอนเดอร์เสนผู้กระทำผิดทำการตรวจสอบบริษัทอื่น แอนเดอร์เสนจึงยอมถอนใบอนุญาตและสิทธิในการปฏิบัติการตรวจสอบในวันที่ 31 สิงหาคม ในขณะเดียวกันได้มีการตั้งคณะกรรมการการพิจารณาทางบัญชีที่ผิดพลาดของบริษัทมหาชนหรือ Public Company Accounting Oversight Board (“Oversight Board”)

พระราชบัญญัติ Sarbanes-Oxley ฉบับนี้ ได้ออกมาบังคับเรื่องการค้นเอกสารอิเล็กทรอนิกส์ การบังคับลงโทษทางอาญาที่เข้มงวดในกรณีมีการเปลี่ยนแปลงหรือทำลายหลักฐานที่บันทึกไว้ รวมถึงสิ่งที่เก็บในรูปของอิเล็กทรอนิกส์ และบังคับเรื่องผลผลิตของหลักฐานที่บันทึกไว้ในรูปแบบอิเล็กทรอนิกส์ กับเอกสารอื่นเมื่อเรียกโดยคณะกรรมการการพิจารณาทางบัญชีที่ผิดพลาดของบริษัทมหาชน

นอกจากออกเป็นพระราชบัญญัตินี้แล้ว ได้มีหน่วยงานที่ดูแลต่าง ๆ รวมทั้ง National Association of Securities Dealers (NASD) ที่ออกระเบียบใหม่ ๆ และแนวทางที่เพิ่มความต้องการในการเก็บรักษาเอกสารที่มีอยู่ บริษัทมหาชนและผู้ตรวจต้องปฏิบัติตามกฎระเบียบใหม่ ๆ อย่างมีกระบวนการ และข้อตกลงร่วมที่เป็นระบบในการนำพยานหลักฐานที่อาศัยคอมพิวเตอร์ในการตรวจสอบภายในและการสืบสวนที่มากมายคณานับซึ่งพระราชบัญญัติ Sarbanes-Oxley ต้องใช้เป็นแหล่งกำเนิดหรือที่มาอย่างหลีกเลี่ยงไม่ได้ สิ่งที่นำมาใช้เป็นกระบวนการบังคับ คือ นิติคอมพิวเตอร์ที่เป็นการรวบรวม วิเคราะห์ และการนำเสนอพยานหลักฐานที่อาศัยคอมพิวเตอร์ในศาล ถ้าหากพยานหลักฐานคอมพิวเตอร์ที่โดยสภาพแล้วจะมีการเปลี่ยนแปลงอย่างมากทำการรวบรวมและจัดการอย่างไม่เหมาะสมและถูกต้องพอแล้วก็มีแนวโน้มว่าไม่สามารถใช้ในศาลได้

## 2.5 การค้นข้อมูลอิเล็กทรอนิกส์ในคดีแพ่งในต่างประเทศ

### 2.5.1 การค้นโดยไม่มีหมายค้น

ในประเทศสหรัฐอเมริกา ในคดีระหว่าง Illinois V. Andreas ศาลฎีกาวินิจฉัยว่าหมายค้นไม่จำเป็น หากไม่มี “ความคาดหวังอย่างมีเหตุผลในเรื่องส่วนบุคคล (reasonable expectation of privacy)” ในเรื่องที่ทำการค้นนั้น ในคดี U.S. v. Barth ศาลได้วินิจฉัยว่าผู้เป็นเจ้าของคอมพิวเตอร์มีความคาดหวังอย่างมีเหตุผลในเรื่องส่วนบุคคลในข้อมูลที่เก็บไว้ในคอมพิวเตอร์ อย่างไรก็ตาม หากเจ้าของโอนการครอบครองให้บุคคลที่สาม เช่น ส่งคอมพิวเตอร์ไปซ่อม ความคาดหวังดังกล่าวก็หมดไปเพราะบุคคลที่ซ่อมเครื่องสามารถเข้าถึงคอมพิวเตอร์และข้อมูลที่เก็บไว้

ในคดีก่อน ๆ ที่ไม่เกี่ยวกับคอมพิวเตอร์ หากข้อมูลเปิดเผยยังบุคคลที่สาม ความคาดหวังอย่างมีเหตุผลในเรื่องส่วนบุคคลจะหมดไป ในคดี U.S. v. Miller[26] ศาลฎีกาวินิจฉัยว่าความคาดหวังอย่างมีเหตุผลในเรื่องส่วนบุคคลหมดไปเมื่อข้อมูลเกี่ยวกับบัญชีธนาคารเปิดเผยต่อธนาคารแล้ว ในคดี Couch.v.U.S. ศาลฎีกาวินิจฉัยว่า ลูกค้าไม่มีความคาดหวังอย่างมีเหตุผลในเรื่องส่วนบุคคลในข้อมูลที่เปิดเผยต่อพนักงานบัญชี

เมื่อนำมาใช้ปรับกันในเรื่องอินเทอร์เน็ต จะหมายถึงการแสดงข้อมูลบนกระดานข่าว (Internet bulletin board) หรือส่งอีเมล์ไปยังห้องพูดคุย (Chat room) การสูญเสียความคาดหวังอย่างมีเหตุผลในเรื่องส่วนบุคคลเป็นสิ่งที่สำคัญมาก เพราะข้อมูลจำนวนมากได้ถูกส่งในเครือข่ายและอินเทอร์เน็ต ดังนั้น ในประเทศสหรัฐอเมริกาถือว่าเป็นการสูญเสียการป้องกันจาก Fourth Amendment หากสภาพแวดล้อมแสดงว่าผู้ส่งข้อมูลไม่มีความคาดหวังอย่างมีเหตุผลในเรื่องส่วนบุคคล ตำรวจไม่ต้องมีหมายค้นเพื่อให้ได้ข้อมูลมา

ในคดี U.S. v. Simons ลูกจ้างของรัฐทำงานในหน่วย Central Intelligence Agency (CIA) ถูกสงสัยว่าใช้คอมพิวเตอร์ในที่ทำงานของตนถ่ายข้อมูลลามก หน่วยงาน CIA จึงเข้าสู่เครื่องคอมพิวเตอร์นั้นจากที่อื่นโดยไม่มีหมายค้นและพบภาพลามกของเด็ก ในการพิจารณาคดีดังกล่าวจำเลยพยายามที่จะลบภาพเหล่านั้นทิ้ง และอ้างว่ามีการละเมิด Fourth Amendment อย่างไรก็ตาม หน่วยงาน CIA มีนโยบายการใช้อินเทอร์เน็ตโดยที่อนุญาตให้มีการตรวจสอบการเข้าสู่อินเทอร์เน็ตของผู้ใช้เป็นระยะ ๆ ศาลวินิจฉัยตามนโยบายที่เป็นทางการนี้ว่าลูกจ้างไม่มีความคาดหวังอย่างมีเหตุผลในเรื่องส่วนบุคคล ดังนั้นจึงไม่จำเป็นต้องมีหมายในการค้น

ในการค้นไม่จำเป็นต้องมีหมายค้นหากผู้ที่เป็นเป้าหมายยินยอมให้ค้นคอมพิวเตอร์ของตน และในการค้นไม่จำเป็นต้องมีหมายค้นเมื่อบุคคลที่สาม เช่น คู่สมรส บิดามารดา นายจ้าง หรือเพื่อนร่วมงานยินยอมในการค้นตราบใดที่คู่ความฝ่ายที่สามดังกล่าวมีสิทธิควบคุมคอมพิวเตอร์เท่าเทียมกัน

ในการค้นไม่จำเป็นต้องมีหมายค้นเมื่อมีเหตุอันควรสงสัยเกิดขึ้นโดยมีเหตุฉุกเฉิน ไม่มีเวลาหรือโอกาสที่จะได้รับหมายค้น ตัวอย่างในคดี U.S. v. David เมื่อตำรวจสังเกตเห็นบุคคลเป้าหมายกำลังลบไฟล์ทิ้งจึงได้เข้ายึดคอมพิวเตอร์เอาไว้

ในคดีตามพระราชบัญญัติ Electronic Communications Privacy Act (ECPA) เป็นเรื่องอำนาจทางกฎหมายในการควบคุมที่มีมากกว่า Fourth Amendment

---

[26] U.S. Department of Justice (2002). **Searching and Seizing Computers and Obtaining Evidence in Criminal investigations.**

**2.5.2 การค้นในสถานที่ทำงาน**

การใช้คอมพิวเตอร์และเข้าสู่อินเทอร์เน็ตในสถานที่ทำงานมีมากขึ้น อาทิ ในคดี O'Connor v. Ortega คดีนี้ทำให้เห็นความแตกต่างระหว่างสถานที่ทำงานราชการและเอกชน ในกรณีนายจ้างสามารถให้ความยินยอมแก่ตำรวจในการค้นคอมพิวเตอร์ของลูกจ้างได้ อย่างไรก็ตาม ถ้านายจ้างเป็นรัฐบาล หากรัฐบาลให้ความยินยอมโดยตัวเอง ในคดี O'Connor วินิจฉัยว่าการให้ความยินยอมของรัฐบาลเช่นนั้นไม่ชอบด้วยกฎหมาย

ในกรณีของเอกชน ลูกจ้างที่มีอำนาจควบคุมคอมพิวเตอร์เท่า ๆ กัน สามารถให้ความยินยอมในการค้นได้ ถ้าการค้นนั้นมีพยานหลักฐานที่จะกล่าวหาลูกจ้างคนอื่น การค้นโดยไม่มีหมายจะไม่เป็นการละเมิด Fourth Amendment และพยานหลักฐานสามารถรับฟังได้ นายจ้างและหัวหน้างานที่มีอำนาจในคอมพิวเตอร์ของลูกจ้างสามารถให้ความยินยอมในการค้นเช่นกัน นอกจากนั้นจะมีประโยชน์ ถ้านายจ้างมีนโยบายในการจ้างอย่างเป็นทางการที่กำหนดให้นายจ้างสามารถรักษาอำนาจเหนือคอมพิวเตอร์และเครือข่ายนั้น

หากเป็นกรณีที่นายจ้างในส่วนเอกชนทำการค้นโดยการตัดสินใจของตนเองปราศจากตำรวจเข้าเกี่ยวข้องแล้ว เช่น นายจ้างมีเหตุผลที่สงสัยว่าลูกจ้างใช้เวลาในการซื้อและขายบนเว็บไซต์ eBay โดยใช้คอมพิวเตอร์ของสำนักงาน จึงค้นคอมพิวเตอร์พบว่ามีพยานหลักฐานในเรื่องยักยอกฉ้อโกง และได้แจ้งตำรวจ เช่นนี้การค้นไม่เป็นการละเมิด Fourth Amendment[27] เพราะจำกัดเฉพาะการค้นของรัฐบาลไม่ใช่เอกชน พยานหลักฐานที่ได้มาจึงรับฟังได้ในการพิจารณาคดีอาญาลูกจ้างนั้น การค้นของเอกชนเช่นนี้น้อยมากที่จะละเมิด Fourth Amendment

ในกรณีถ้าเป็นรัฐบาล รัฐบาลไม่สามารถให้ความยินยอมในการค้นคอมพิวเตอร์ของลูกจ้าง การค้นจึงต้องอาศัยอำนาจในการค้นจากหน่วยงานอื่นเช่นการออกหมายค้น

## 2.6 ตัวอย่างคดีที่เกิดขึ้นเกี่ยวกับการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์

**Sony Computer Entertainment Australia Pty Ltd v Jakopoevic [2001] FCA 1520**

ในประเทศออสเตรเลียได้มีการละเมิดเครื่องหมายการค้า ผู้อุทธรณ์ได้ผลิตและจำหน่ายซีดีรอมที่มีเครื่องหมายการค้าปลอมของเครื่องหมาย "Sony" เมื่อผู้อุทธรณ์ทราบว่าจะมีการสืบสวนจึงได้ลบเรคคอร์ดทางธุรกิจหลายอย่างออกจากคอมพิวเตอร์ ผู้เชี่ยวชาญนิติคอมพิวเตอร์สามารถค้นพบไฟล์คอมพิวเตอร์ที่ถูกลบทิ้งได้

---

[27] Retrieved from http://www.usdoj.gov/criminal/cybercrime/A.

**V Cable Inc. v. Budnick, 2001 WL 1556323 (2nd Clr. Dec. 3, 2001)** ในการสืบสวนการขายและจำหน่ายอุปกรณ์สายเคเบิล ตำรวจยึดคอมพิวเตอร์ที่เชื่อว่าจะมีพยานหลักฐานที่เกี่ยวข้องกับการกระทำผิด หลังจากนั้นตำรวจได้ส่งคอมพิวเตอร์ไปยังบริษัทซอฟต์แวร์เอกชนเพื่อการวิเคราะห์ มีการอุทธรณ์ว่า ทันทีที่คอมพิวเตอร์หลุดพ้นจากการเก็บรักษาของตำรวจ คอมพิวเตอร์และหลักฐานที่ถูกบันทึกจะถูกแก้ไขหรือเปลี่ยนแปลง จะใช้เป็นพยานหลักฐานไม่ได้ ศาลวินิจฉัยว่าเอกสารดังกล่าวไม่มีความน่าเชื่อถือเพียงพอที่จะรับฟังตาม Rule 803(6) of the Federal Rules of Evidence

**United States v. Lloyd, 269 F. 3d 228 (3rd Clr.2001)** ศาลได้วินิจฉัยว่าผู้ที่กระทำผิดในการฝังโปรแกรมประสงค์ร้ายที่เรียกว่า Time bomb ซึ่งทำให้การปฏิบัติงานในบริษัท New Jersey-based Omega Engineering Corp. หยุดลง ไม่สามารถขอพิจารณาคดีใหม่ในเรื่องความอคติของลูกขุน ศาลยืนตามคำชี้ขาดของคณะลูกขุนว่า จำเลยมีความผิดในความผิดข้อหาก่อวินาศกรรมคอมพิวเตอร์ คดีนี้ผู้เชี่ยวชาญด้านคอมพิวเตอร์มีความจำเป็นที่ขาดไม่ได้และได้นำมาใช้ในการกู้เอาหลักฐานเกี่ยวกับ time bomb คืนมา

**Munshanl v. Signal Lake Venture Fund II, 2001 WL 1526954 (Mass. Super. Oct. 9, 2001)** ในข้อโต้เถียงเรื่องความแท้จริงของข้อมูลอีเมล์ ศาลได้ตั้งผู้เชี่ยวชาญคอมพิวเตอร์คนกลาง จากรายงานและการวิเคราะห์ของผู้เชี่ยวชาญของศาลพบว่าโจทก์ปลอมอีเมล์ที่โต้เถียงนั้น และพยายามที่จะซ่อนเรื่องที่แต่งขึ้นมา ศาลยกฟ้องโจทก์และสั่งให้โจทก์จ่ายค่าผู้เชี่ยวชาญและค่าทนายความแทนจำเลย

**Northwest Airlines v. Local 2000, C.A. No. 00-08 DWF/AJB (D. MInn. Feb. 2, 2002)** ศาลออกคำสั่งให้ผู้เชี่ยวชาญของโจทก์เป็นผู้เชี่ยวชาญฝ่ายที่สามที่เป็นกลาง ผู้เชี่ยวชาญทำในนามศาลได้รวบรวมและทำรูปจำลองอุปกรณ์เก็บข้อมูล (Hard drive) และจัดรายงานให้แก่คู่ความทั้งหมด ศาลได้ออกข้อตกลงในรายละเอียดในการดำเนินการเกี่ยวกับการแสดงทางอิเล็กทรอนิกส์

**Simon Property Group v. MySimon, Inc., 194 F.R.D. 639 (S.D. Ind. 2000)** โจทก์ยื่นคำร้องในการบังคับในคดีเครื่องหมายการค้า ศาลวินิจฉัยว่าโจทก์มีสิทธิที่จะพยายามในการกู้คืนไฟล์คอมพิวเตอร์ที่ถูกลูกจ้างของจำเลยลบทิ้งจากคอมพิวเตอร์ โดยศาลต้องการออกมาตรการป้องกัน รวมถึงการตั้งผู้เชี่ยวชาญของโจทก์ให้เป็นเจ้าพนักงานของศาลและให้ข้อมูลที่กู้คืนมาแก่ทนายจำเลยในการที่ตรวจสอบก่อน

**Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999)** ศาลตั้งผู้เชี่ยวชาญทางคอมพิวเตอร์ที่เชี่ยวชาญในการค้นหาทางอิเล็กทรอนิกส์เพื่อสร้างรูปจำลอง (Mirror image) ของอุปกรณ์เก็บข้อมูล (Hard drive) ของจำเลย ศาลสงวนสิทธิของผู้ร้องที่จะคัดค้านผลอันเกิดหลังจากข้อมูลได้ค้นพบโดยผู้เชี่ยวชาญ และจากการตรวจสอบเอกสารต่าง ๆ

**Advantacare Health Partners, LP v. Access IV, 2004 WL 1837997 (N.D. Cal. Aug. 17, 2004)** โจทก์ฟ้องจำเลยซึ่งเป็นลูกจ้างเดิมของโจทก์ว่า บริษัทของจำเลยที่ตั้งใหม่แข่งขันโดยตรงกับธุรกิจของโจทก์ คดีนี้โจทก์ได้จ้างผู้เชี่ยวชาญการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์เพื่อที่จะตรวจสอบคอมพิวเตอร์ที่มีงานเดิมอยู่ ผู้เชี่ยวชาญพบว่า ก่อนที่จะออกจากบริษัทโจทก์ จำเลยเข้าสู่เครือข่ายคอมพิวเตอร์ของโจทก์และได้ทำสำเนาไฟล์ความลับของบริษัท ต่อจากนั้นได้ลบไฟล์ที่ทำสำเนาในอุปกรณ์เก็บข้อมูล (Hard drive) ของจำเลยเพื่อพยายามปกปิดไฟล์ที่สำเนาไว้ จากพยานหลักฐานนี้ศาลมีคำสั่งอนุญาตตามคำร้องของโจทก์ให้โจทก์สามารถทำสำเนาทางการตรวจพิสูจน์หลักฐานของคอมพิวเตอร์และแม่ข่ายทั้งที่บ้านและธุรกิจของจำเลย ผู้เชี่ยวชายการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์พบว่าหลังจากที่ศาลออกคำสั่งได้มีการค้นหาในคอมพิวเตอร์เพื่อใช้ซอฟต์แวร์ในการลบข้อมูลหลายครั้งและโปรแกรมที่เรียกว่า “BC Wipe” นำมาใช้เพื่อลบไฟล์มากกว่า 13,000 ไฟล์ จากคอมพิวเตอร์และแม่ข่ายทั้งที่บ้านและธุรกิจของจำเลย นอกจากนั้นยังพบว่าไฟล์อีก 100 ไฟล์ ถูกลบทิ้งประมาณไม่กี่ชั่วโมงก่อนที่จำเลยจะมอบอุปกรณ์เก็บข้อมูล (Hard drive) ให้โจทก์เพื่อวิเคราะห์เมื่อได้ข้อเท็จจริงเช่นนี้ ศาลจึงมีคำสั่งให้จำเลยลบไฟล์ทิ้งถาวรและอนุญาตให้โจทก์ทำรูปจำลองของอุปกรณ์เก็บข้อมูล (Hard drive) จากการทำดังกล่าว ผู้เชี่ยวชาญของโจทก์พบไฟล์ความลับหลายพันไฟล์ยังคงอยู่ในอุปกรณ์เก็บข้อมูล (Drive) จำเลยโต้แย้งว่าไม่สามารถรับรองได้ว่าจำเลยได้ลบทิ้งทุกไฟล์ เพราะโจทก์ไม่ได้แสดงให้เห็นไฟล์เหล่านั้นว่ามีชื่ออยู่ในไดเรกทอรีไหนและคอมพิวเตอร์ใด ศาลปฏิเสธข้อโต้แย้งนี้และวินิจฉัยว่า พฤติกรรมของจำเลยตั้งแต่เริ่มต้นคดีนี้ชี้ให้เห็นถึงความจงใจ ความผิดและความไม่สุจริต ศาลพิพากษาให้จำเลยใช้เงิน $20,000 และชี้ว่าข้อโต้แย้งนั้นอาจทำให้ลูกขุนสรุปหรืออนุมานในทางลบเกี่ยวกับไฟล์ที่ถูกลบทิ้งนั้น

**Ohio v. Brian Cook, 149 Ohio App. 3d 422; 2002** ในกรณีที่พยานหลักฐานสามารถรับฟังเป็นพยานหลักฐานแล้ว ขั้นตอนต่อไปคือต้องพิสูจน์ว่าการวิเคราะห์และการเก็บรักษาได้ทำโดยถูกต้อง ซึ่งในทางปฏิบัติจะใช้วิธีรูปจำลองที่ใช้การส่งข้อมูลบิตต่อบิต ไม่ว่าจะใช้ได้หรือใช้ไม่ได้ จากสื่ออุปกรณ์เก็บข้อมูล (Hard drive) ไปยังอุปกรณ์เก็บข้อมูล (Hard drive) แต่เป็นไปได้ที่ใช้ขั้นตอนวิธีตรวจผลรวม (Checksum algorithms) เช่น MD5[28] or SHA1[29] ว่าข้อมูลที่เขียนในอุปกรณ์เก็บข้อมูล (Drive) จะเหมือนกับต้นฉบับหรือไม่ ศาลชี้ว่าถ้าค่าที่ได้จากต้นฉบับและรูปจำลองเหมือนกัน รูปจำลองดังกล่าวมีผลและถือว่าเป็นต้นฉบับได้

---

[28] MD5 เป็นฟังก์ชันทางเดียวของการจัดข้อมูลที่เรียกว่า hash ซึ่งเป็นข้อมูลและเปลี่ยนไปเป็นอนุกรมของตัวเลขและสามารถเปรียบเทียบข้อมูลที่คำนวณที่ถูกย่อยนี้กับข้อมูลที่ย่อยและเข้ารหัสกับกุญแจสาธารณะเพื่อตรวจสอบว่าข้อมูลไม่ได้ถูกเปลี่ยนไป การเปรียบเทียบนี้เรียกว่า “hash check”.

[29] W3.org/PICS/DSig/SHA1_1_0.

**Ohio v. Brian Cook, 149 Ohio App. 3d 422; 2002** จำเลยโต้แย้งหลายปัญหาเรื่องความชอบด้วยกฎหมายของข้อมูลและพยานแวดล้อมที่เกี่ยวกับผู้สร้างไฟล์ จำเลยอ้างว่าไม่ได้มีการรับรองความน่าเชื่อของข้อมูลบนอุปกรณ์เก็บข้อมูล (Hard drive) ตามขั้นตอน เช่น การนำอุปกรณ์เก็บข้อมูล (Drive) ใส่ในถุงสถิต จำเลยโต้แย้งว่าวันที่และเวลาในไฟล์ในระบบไม่ได้มีการทดสอบ CMOS ในเวลาปัจจุบันของระบบหรือไม่ได้ใส่แบตเตอรี่ใน CMOS ตอนที่ใส่พยานหลักฐานเพื่อดูความน่าเชื่อถือของนาฬิการะบบ ผู้เชี่ยวชาญการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ของจำเลยพบนาฬิการะบบถูกปิดประมาณ 5 นาที และจำเลยไม่ได้อยู่ที่บ้านระหว่างเวลาที่ไฟล์ได้สร้างขึ้น อย่างไรก็ตาม ศาลพบว่ามีเหตุผลฟังได้ว่าอาจมีการเข้าสู่ระบบและสร้างไฟล์ที่มีปัญหานั้นจากที่อื่นที่อยู่ไกลได้ ศาลพบว่ามาตรการที่กล่าวมาในเรื่องความน่าเชื่อนั้นไม่มีความจำเป็นเพราะรูปจำลองทำให้เป็นจริงเหมือนกับต้นฉบับได้ในทางตรงกันข้าม ถ้าจำเลยถูกต้องอุปกรณ์เก็บข้อมูล (Hard drive) อาจสูญเสียบิตในการส่งได้ ถ้าพยานหลักฐานเอาไว้หลังรถลาดตระเวนของตำรวจถัดจากอุปกรณ์วิทยุสื่อสารที่มีกำลังส่งมาก ข้อมูลอาจสูญหายและมีการเปลี่ยนแปลงข้อมูล ถึงแม้ว่าจะมีความเป็นไปได้ว่าอาจมีความเสียหายต่ออุปกรณ์เก็บข้อมูล (Drive) อาจเกิดขึ้นได้ ความน่าจะเป็นของบิตที่ถูกจัดใหม่ให้เกิดเป็นภาพลามกของเด็กไม่น่าเป็นไปได้

## 2.7 การใช้ประโยชน์ทางการตรวจพิสูจน์หลักฐานทางโปรแกรมคอมพิวเตอร์

หลักสี่ประการในการวิเคราะห์หาความเป็นเจ้าของที่สามารถนำมาใช้ในรหัสต้นฉบับและในการใช้ประโยชน์ทางการตรวจพิสูจน์หลักฐานโปรแกรมคอมพิวเตอร์มีดังนี้

**2.7.1 การแยกแยะผู้เป็นเจ้าของ (Author discrimination)** เป็นขั้นตอนการตัดสินใจว่าบางส่วนของรหัสเขียนขึ้นโดยเจ้าของคนเดียวหรือโดยเจ้าของหลาย ๆ คนที่แตกต่างกันซึ่งจะรวมถึงการประมาณจำนวนของเจ้าของหลายรายที่มีส่วนร่วมในการเขียนรหัสส่วนเดียว หรือรหัสทั้งหมด[30] และจะรวมถึงการคำนวณความคล้ายคลึงบางอย่างระหว่างรหัสสองชิ้นหรือมากกว่าและความเป็นไปได้โดยการประมาณความไม่คงที่ระหว่างและภายในวัตถุ ตัวอย่างเรื่องนี้สามารถแสดงให้เห็นว่ารหัสสองชิ้นอาจจะเป็นไปได้ว่าเขียนโดยเจ้าของที่แตกต่างกัน[31] โดยปราศจากการชี้ชัดอย่างจริง ๆ ถึงเจ้าของในปัญหานั้น

---

[30] Sallis P., Aakjaer, A., and MacDonnell, S. ( 1996). **Software Forensics;** Old Methods for a New Science. Proceeding of SE:E&P'96 (Software Engineering: Education and Practice). Dunedin. New Zealand. IEEE Computer Society Press. 367-371.

[31] มีความจำเป็นอย่างยิ่งในการแยกระหว่างการชี้ให้เห็นเจ้าของหลายคนสำหรับชุดของโปรแกรมกับความเป็นเจ้าของร่วมในโปรแกรมเดี่ยว ๆ

**2.7.2 การชี้ชัดถึงเจ้าของ (Author Identification)** มีผู้ที่เป็นเป้าหมายเพื่อที่พิจารณาความเหมือนของเจ้าของเฉพาะคนที่ได้เขียนบางชิ้นของรหัสโดยอาศัยตัวอย่างรหัสอื่น ๆ ของโปรแกรมเมอร์คนนั้น ซึ่งสามารถใช้ในกรณีที่มีตัวอย่างรหัสของโปรแกรมเมอร์หลายคนและพิจารณาความคล้ายกันกับของรหัสชิ้นใหม่ที่กำลังเขียนโดยโปรแกรมเมอร์แต่ละคน การประยุกต์ใช้เช่นนี้จะคล้ายคลึงกับความพยายามในการพิจารณาความเป็นเจ้าของของงานนิพนธ์และนำไปใช้กับรหัสต้นฉบับที่สามารถบอกถึงความเป็นเจ้าของในงานรหัสชิ้นใหม่ว่าเป็นเจ้าของรหัสที่ตรงกับลักษณะของรหัสชิ้นอื่นที่เขียนโดยเจ้าของคนนี้ได้ เช่น ไวรัสคอมพิวเตอร์

**2.7.3 คุณลักษณะของเจ้าของ (Author Characterization)** เป็นการพิจารณาคุณลักษณะบางประการของโปรแกรมเมอร์ในการแบ่งแยกรหัสออกเป็นชิ้นเล็กชิ้นน้อย เช่น บุคลิกภาพ และพื้นภูมิการศึกษา โดยอาศัยรูปแบบของการเขียนโปรแกรม ตัวอย่างเรื่องนี้จะใช้พิจารณาว่าส่วนของรหัสมีแนวโน้มว่าจะถูกเขียนโดยบุคคลที่มีพื้นภูมิทางการศึกษาโดยมองจากรูปแบบของการเขียนโปรแกรมและเทคนิคที่ใช้

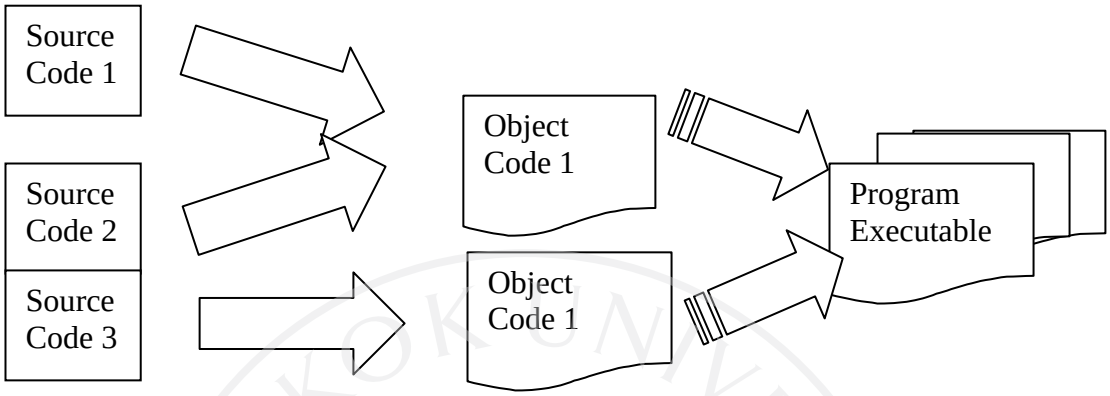
**2.7.4 พิจารณาความตั้งใจของเจ้าของ (Author Intent determination)** อาจเป็นไปได้ถึงการพิจารณาในบางกรณีว่ารหัสที่มีผลที่ไม่ต้องการถูกเขียนขึ้นด้วยจิตใจที่ไม่ดีงามหรือเป็นผลมาจากความผิดพลาดโดยอุบัติเหตุ สืบเนื่องมาจากกระบวนการการพัฒนาโปรแกรมจะต้องมีข้อผิดพลาด[32] และข้อผิดพลาดบางอย่างทำให้เกิดผลเสียหายตามมา จึงทำให้สามารถขยายไปตรวจสอบถึงการกระทำโดยประมาทเลินเล่อ ซึ่งโดยปกติแล้วรหัสที่เกิดผิดพลาดนี้จะถูกสงสัยว่ามีความเข้มงวดน้อยกว่ารหัสปกติของโปรแกรมเมอร์

เทคนิคทางการตรวจพิสูจน์หลักฐานนี้ไม่ได้ถูกจำกัดเฉพาะการวิเคราะห์รหัสต้นฉบับที่เขียนโดยโปรแกรมเมอร์และใช้ในการสร้างโปรแกรม รหัสต้นฉบับโดยปกติแล้วจะถูกแปลง

---

[32] ในทางตรงกันข้ามที่ว่ารหัสเขียนโดยเจ้าของคนเดียวกันสามารถนำมาใช้ทดสอบในเรื่องการลอกเลียนจากเจ้าของคนใดคนหนึ่ง และดู Whale, G. (1990). Software Methods and Plagiarism Detection. Journal of Systems and Software. 13:131-138.

(Complied) เป็นภาษาเครื่องหรือ object code ซึ่งต่อมาจะโยงเป็นโปรแกรมจริง ๆ ที่ทำงานได้ ดังภาพต่อไปนี้




ข้อมูลสามารถถูกสกัดมาจากรหัสภาษาเครื่อง/รหัสโปรแกรมจริงที่ทำงานได้โดยวิธีแปลงกลับ (Decompiled) ไปเป็นรหัสต้นฉบับโดยมีข้อมูลที่หายไป[33] หรือสกัดจากลักษณะที่แน่นอนที่มีอยู่ในโปรแกรมจริงที่ทำงานได้ที่สามารถทำให้เห็นถึงโปรแกรมที่ใช้แปลงรหัสต้นฉบับไปเป็นภาษาเครื่อง (Compiler) และหรือฮาร์ดแวร์ที่มีระบบปฏิบัติการที่ถูกนำมาใช้

ภาษาชั้นสูงบางภาษาแทนที่จะใช้กระบวนการแปลงรหัสดังที่กล่าวมาแล้ว อาจทำงานในระบบโปรแกรมที่อ่านประโยคคำสั่งที่เขียนด้วยภาษาชั้นสูง แล้วแปลงเป็นภาษาเครื่องเพื่อทำตามคำสั่งนั้นทีละบรรทัดทันที (Interpreter) ในกรณีเช่นนี้โปรแกรมจริงที่ทำงานได้ก็เป็นรหัสต้นฉบับในตัวเอง และโปรแกรมจะทำงานภายใต้สภาพแวดล้อมที่แปลงรหัสไปเป็นคำสั่งที่เครื่องจักรสามารถเข้าใจ นี้เป็นสิ่งที่ธรรมดาสำหรับภาษาระดับสูง แต่ยังคงใช้ได้สำหรับภาษาอื่นที่เรียกว่า scripting languages แต่ทั่วไปแล้วคำว่าโปรแกรมจริงที่ทำงานได้จะหมายถึงโปรแกรมที่แปลงรหัสแบบ Compiler

ดังนั้น โดยไม่คำนึงถึงรูปแบบใดของโปรแกรมที่กำลังพิจารณาจะเป็นรหัสต้นฉบับ (Source code) หรือโปรแกรมจริงที่ทำงานได้ (Executable) ที่แปลงมาแล้ว การวัดสามารถนำมาใช้ในวัตถุประสงค์ในการวิเคราะห์ความเป็นเจ้าของได้ ประเภทของข้อมูลที่มีอยู่จะขึ้นอยู่กับรูปแบบของโปรแกรม (รหัสต้นฉบับหรือภาษาเครื่อง) และในกรณีที่แตกต่างกัน รูปแบบหนึ่งอาจดีกว่าอย่างอื่น ๆ แต่โดยทั่วไป รหัสต้นฉบับจะให้ข้อมูลจำนวนมากที่สุด อย่างไรก็ตามข้อมูลบางอย่างที่ไม่คำนึงถึงรูปแบบของโปรแกรมอาจมีประโยชน์เมื่อนำมารวมกับความรู้ที่มีอยู่ที่ไม่เกี่ยวกับโปรแกรม

---

[33] โดยทั่วไป โปรแกรมแปลรหัส (Compilers) ทำให้รหัสได้ผลดีที่สุด แต่สูญเสียโครงสร้างบางอย่างและใช้สัญลักษณ์แทนที่ชื่อต่าง ๆ

ข้อตกลงเบื้องต้นของการตรวจพิสูจน์หลักฐานโปรแกรมคอมพิวเตอร์[34] คือ โปรแกรมเมอร์มีแนวโน้มที่มีรูปแบบการเขียนรหัสที่แตกต่างกัน รูปแบบและรูปร่างดังกล่าวจะสามารถรู้ได้โดยเพื่อน ๆ หรือผู้เชี่ยวชาญในการวิเคราะห์รหัสที่มีตัวอย่างของรหัสนั้น ๆ แต่อย่างไรก็ตาม ปัญหาที่ว่าคุณสมบัติหรือลักษณะเฉพาะของบุคคลสามารถถูกซ่อนหรือเลียนแบบได้ดีนั้นมีความสำคัญอย่างเห็นได้ชัด เมื่อมีการลงความเห็นว่าบุคคลใดเป็นเจ้าของ ได้มีผู้ให้ความเห็นว่าอย่างน้อยยังคงมีหลักฐานแสดงเอกลักษณ์หลงเหลืออยู่หลังจากความพยายามของผู้เป็นเจ้าของที่จะปลอมแปลงเอกลักษณ์ของตน กล่าวคือ บางลักษณะของรูปแบบของโปรแกรมเมอร์ไม่สามารถถูกเปลี่ยนแปลงได้ถ้ามีการเขียนโปรแกรมอย่างมีประสิทธิผล คำถามที่สำคัญอีกประการหนึ่งคือความเป็นเจ้าของสามารถที่จะถูกจำแนกออกอย่างถูกต้องและพอเพียงหรือไม่ในตนเอง และนำไปสู่คำถามพื้นฐานที่ว่าจะมีข้อมูลเพียงพอหรือไม่ในการใช้เทคนิคนี้เพื่อหาหลักฐานหาความเป็นเจ้าของในการใช้ประโยชน์ทางกฎหมาย (Legal context) หรืออีกนัยหนึ่งคำถามที่ว่าเอกลักษณ์หรือลักษณะแสดงความเป็นเจ้าของสามารถแสดงในระดับความแน่นอนที่เพียงพอหรือไม่เพื่อที่จะใช้เป็นข้อโต้แย้งทางกฎหมาย หลักฐานดังกล่าวสามารถเป็นสถิติหรือความเห็นผู้เชี่ยวชาญ การวิเคราะห์ความเป็นเจ้าของรหัสของโปรแกรมใช้ในการต่าง ๆ รวมถึงการวิเคราะห์รหัสที่ประสงค์ร้าย (Malicious code) และการสืบหาการลอกเลียนแบบ (Plagiarism) และรวมถึงการศึกษาทางจิตวิทยาในการเขียนโปรแกรมเพื่อประเมินถึงคุณภาพของรหัส

---

[34] ดูรายละเอียดประเภทของรหัสที่ใช้สำหรับการตรวจพิสูจน์หลักฐานโปรแกรมคอมพิวเตอร์ ที่ผนวก ค หน้า108

# บทที่ 3
# กฎหมายไทยและกฎหมายต่างประเทศที่เกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน

## 3.1 กฎหมายไทยที่เกี่ยวข้องกับการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน

กฎหมายของไทยที่เกี่ยวข้องกับการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานนั้นมีกฎหมายที่สำคัญคือพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. 2544 โดยเจตนารมณ์ของกฎหมายฉบับนี้ คือเพื่อรองรับสถานะของข้อมูลอิเล็กทรอนิกส์ให้เทียบเท่ากับการทำเป็นหนังสือหรือหลักฐานเป็นหนังสือรับรองวิธีการส่งและรับข้อมูลการใช้ลายมือชื่อตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์โดยกำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ทำหน้าที่วางนโยบายเพื่อกำหนดหลักเกณฑ์ต่างๆซึ่งเป็นการส่งเสริมธุรกรรมทางอิเล็กทรอนิกส์ทั้งภายในและระหว่างประเทศ โดยพระราชบัญญัติฉบับนี้ได้นำเอากฎหมายแม่แบบของUNCITRAL คือ UNCITRAL Model Law on Electronic Commerce 1996 และUNCITRAL Model Law on Electronic Signatures 2001ซึ่งเป็นกฎหมายแม่แบบที่UNCITRALหรือUnited Nation Commission For International Trade Law จัดทำขึ้นทั้ง 2 ฉบับ แต่ประเทศไทยได้นำกฎหมายแม่แบบทั้ง 2 ฉบับนี้มาผนวกรวมเป็น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. 2544และมีการแก้ไขเพิ่มเติมเป็นพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551

### 3.1.1 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัติฉบับนี้ใช้กับธุรกรรมในทางแพ่งและทางพาณิชย์ที่ได้ติดต่อสื่อสารและกระทำผ่านสื่ออิเล็กทรอนิกส์ และยังเปิดโอกาสให้นำกฎหมายฉบับนี้มาใช้บังคับกับธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ซึ่งจะเห็นได้ว่ากฎหมายฉบับนี้มีขอบเขตครอบคลุมถึงคดีแพ่งและพาณิชย์ทุกประเภท ไม่ว่าจะเป็นคดีหนี้ หรือคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ และอาจถือได้ว่าเป็นบทบัญญัติที่มีขอบเขตครอบคลุมในคดีแพ่งได้เทียบเท่าประมวลกฎหมายวิธีพิจารณาความแพ่ง แต่ก็ยังมีกรณีที่มีการกำหนดธุรกรรมที่เป็นข้อยกเว้นไว้ ซึ่งการที่กฎหมายให้อำนาจในการตราพระราชกฤษฎีกากำหนดธุรกรรมที่ยกเว้นมิให้นำ

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับนั้น อาจเพราะมีเหตุผลที่ว่าธุรกรรมบางประเภทโดยสภาพไม่อาจทำด้วยวิธีการทางอิเล็กทรอนิกส์ได้ เพราะบางกรณีอาจเป็นสิ่งที่กฎหมายได้คำนึงถึงแล้วว่าที่ต้องการให้มีการยกเว้นเพราะธุรกรรมบางประเภทมีความละเอียดอ่อนที่ต้องการการพิจารณาและการไตร่ตรองอย่างรอบคอบก่อนการดำเนินการ โดยธุรกรรมที่ได้รับการยกเว้นได้แก่ พินัยกรรม ตราสารเปลี่ยนมือได้ หรือการดำเนินการใดๆ เกี่ยวกับการโอนสิทธิในอสังหาริมทรัพย์ เป็นต้น[1] โดยในปัจจุบันมีการประกาศใช้พระราชกฤษฎีกากำหนดมิให้นำบทบัญญัติตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับกับธุรกรรม 2 ประเภท คือ ธุรกรรมที่เกี่ยวกับครอบครัวและธุรกรรมเกี่ยวกับมรดก[2]

นอกจากนี้เดิมยังมีข้อถกเถียงกันในทางวิชาการเกี่ยวกับว่าจะสามารถนำพระราชบัญญัติฉบับนี้ไปใช้ในคดีอาญาได้ด้วยหรือไม่ ซึ่งปัญหาข้อถกเถียงดังกล่าวได้เป็นอันยุติลงเมื่อพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 ได้แก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. 2544 มาตรา 11 โดยกำหนดว่า ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์ และกำหนดให้การชั่งน้ำหนักพยานหลักฐานต้องพิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง โดยให้นำมาใช้บังคับกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย

การกำหนดห้ามมิให้ศาลปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานเป็นการยืนยันให้ศาลต้องรับฟังเสมอ แต่ก็ใช่ว่าจะต้องมีน้ำหนักน่าเชื่อถือเสมอไป เพราะหลักเกณฑ์ในการชั่งน้ำหนักพยานหลักฐานถูกบัญญัติไว้แล้วในมาตรา11วรรคที่สอง

ส่วนการกำหนดให้การรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานตามมาตรานี้ก็ไม่ได้ระบุว่าให้รับฟังในรูปแบบของพยานประเภทใด ซึ่งเมื่อเราพิจารณาจากลักษณะของ

---

[1] ชัยวัฒน์ วงศ์วัฒศานต์,ทวีศักดิ์ กออนันตกูล และ สุรางคณา แก้วจำนง, **คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ.2544** (กรุงเทพมหานคร: สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ,2545) น.14-15

[2] พระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับ พ.ศ.2549

ข้อมูลอิเล็กทรอนิกส์ ซึ่งอาจจะมีลักษณะเป็นได้ทั้งพยานเอกสารและพยานวัตถุ แต่ก็มีลักษณะพิเศษต่างไปจากพยานเอกสารและพยานวัตถุ ดังนั้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์น่าจะเป็นพยานหลักฐานอีกประเภทหนึ่งที่ไม่รวมอยู่ในพยานหลักฐานตามที่กฎหมายลักษณะพยานหลักฐานกำหนดไว้

**ในส่วนของการรับรองลายมือชื่อ**

ตามมาตรา 9 แห่งพระราชบัญญัติฉบับนี้ยอมรับให้ข้อมูลอิเล็กทรอนิกส์ให้มีฐานะเท่าเทียมกับลายมือชื่อธรรมดา โดยมีเงื่อนไขว่าข้อมูลอิเล็กทรอนิกส์นั้นต้อง

(1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อได้ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตนและ

(2) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณีและความน่าเชื่อถือดังกล่าวให้คำนึงถึง

1. ความมั่นคงและรัดกุมของการใช้วิธีการหรืออุปกรณ์ในการระบุตัวบุคคลสภาพพร้อมใช้งานของทางเลือกในการระบุตัวบุคคล กฎเกณฑ์เกี่ยวกับลายมือชื่อที่กำหนดไว้ในกฎหมายระดับความมั่นคงปลอดภัยของการใช้ลายมือชื่ออิเล็กทรอนิกส์ การปฏิบัติตามกระบวนการในการระบุตัวบุคคลผู้เป็นสื่อกลาง ระดับของการยอมรับหรือไม่ยอมรับ วิธีการที่ใช้ในการระบุตัวบุคคลในการทำธุรกรรม วิธีการระบุตัวบุคคล ณ ช่วงเวลาที่มีการทำธุรกรรมและติดต่อสื่อสาร

2. ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ จำนวนครั้งหรือความสม่ำเสมอในการทำธุรกรรม ประเพณีทางการค้าหรือทางปฏิบัติ ความสำคัญ มูลค่าของธุรกรรมที่ทำ หรือ

3. ความรัดกุมของระบบการติดต่อสื่อสาร

นอกจากนี้ยังกำหนดให้การใช้ลายมือชื่ออิเล็กทรอนิกส์สามารถอนุโลมใช้บังคับกับการประทับตราของนิติบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ได้ด้วย

**ในส่วนของการนำเสนอและการเก็บรักษาอย่างเอกสารต้นฉบับ**

มาตรา10 ยอมรับให้กรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ หากได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์โดยใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และสามารถแสดงข้อความนั้นในภายหลังได้ ก็ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมาย ในส่วนของความถูกต้องของข้อความให้

พิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงส่วนใดของข้อความ เว้นแต่การรับรองหรือการบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใดๆที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงข้อความซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้น และการวินิจฉัยความน่าเชื่อถือของวิธีการรักษาความถูกต้องของข้อความให้พิเคราะห์ถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง รวมทั้งวัตถุประสงค์ของการสร้างข้อความนั้น และการใช้แทนต้นฉบับได้นั้น ยังรวมถึงสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ดังกล่าวด้วย หากสิ่งพิมพ์ออกนั้นมีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์ และมีการรับรองสิ่งพิมพ์ออกโดยหน่วยงานที่มีอำนาจตามที่คณะกรรมการประกาศกำหนด

**ในส่วนของการรับรองการเก็บรักษาข้อมูลอย่างเอกสารทั่วไป**

การรับรองการเก็บรักษาข้อมูลอิเล็กทรอนิกส์เทียบเท่าเอกสารธรรมดานี้ เดิมมิได้กำหนดไว้ชัดเจนว่ารวมถึงการแปลเอกสารเก่าให้อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ด้วยหรือไม่ แต่ในปัจจุบันได้มีการแก้ไขกฎหมายในประเด็นนี้โดยให้นำบทบัญญัติในมาตรา10 มาตรา11 มาตรา12 มาใช้บังคับด้วย

มาตรา12 กำหนดให้กรณีที่กฎหมายกำหนดให้การเก็บรักษาเอกสารหรือข้อความใด ถ้าได้เก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ โดยข้อมูลนั้นสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง และได้เก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์นั้น หรืออยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับให้ปรากฏอย่างถูกต้องได้ และได้เก็บรักษาข้อความส่วนที่ระบุถึงแหล่งกำเนิด ต้นทาง ปลายทางของข้อมูลอิเล็กทรอนิกส์ ตลอดจนวันและเวลาที่ส่งหรือได้รับข้อความดังกล่าว(ถ้ามี) ให้ถือว่าได้มีการเก็บรักษาเอกสารหรือข้อความตามที่กฎหมายต้องการแล้ว โดยทั้งนี้จะไม่นำไปใช้บังคับกับข้อความที่ใช้เพียงเพื่อวัตถุประสงค์ในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์ การเก็บรักษาข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลงนั้น น่าจะต้องมีวิธีการเก็บรักษาข้อมูลอิเล็กทรอนิกส์ที่มีมาตรการรักษาความปลอดภัยทางกายภาพ และมาตรการรักษาความปลอดภัยทางเทคนิค เช่นมีการป้องกันการเข้าถึงข้อมูลอิเล็กทรอนิกส์โดยมิชอบทางระบบเครือข่ายคอมพิวเตอร์ ไม่ว่าจะเป็นระบบเครือข่ายในองค์กรหรือระบบเครือข่ายอินเตอร์เน็ต โดยจะต้องมีการแสดงหรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์โดยวิธีการที่น่าเชื่อถือ ซึ่งวิธีการนี้จะต้องสามารถรักษาความถูกต้องของข้อมูลอิเล็กทรอนิกส์ตั้งแต่แรกสร้างข้อมูลนั้นขึ้นเป็นข้อมูลรูปแบบสุดท้าย (final form) ตามกฎหมายแม่แบบของUNCITRAL ให้ถือว่าเป็นการแสดงหรือเก็บรักษาเอกสารต้นฉบับตามกฎหมายแล้ว ส่วนการเก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นต้องกระทำในรูปแบบที่สามารถแสดงว่าข้อมูลอิเล็กทรอนิกส์นั้นมีเนื้อหาตรงกันกับข้อมูลหรือเอกสาร

ที่ต้องเก็บรักษา ตามคำอธิบายประกอบกฎหมายแม่แบบ เป็นข้อกำหนดที่ว่าข้อมูลอิเล็กทรอนิกส์ที่เก็บรักษานั้นต้องมีเนื้อหาตรงกัน (represent accurately) กับข้อมูลหรือเอกสารที่ต้องเก็บรักษานั้นมิได้หมายความว่าข้อมูลอิเล็กทรอนิกส์นั้นต้องไม่มีการเปลี่ยนแปลงจากรูปเดิม ทั้งนี้เพราะการเก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นมักมีการเข้ารหัสข้อมูล การบีบข้อมูล (compression) หรือการเปลี่ยนรูปข้อมูล (conversion) อยู่เป็นปกติ

**ในส่วนของการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน**

ตามมาตรา 11 ได้กำหนดห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์และกำหนดให้การชั่งน้ำหนักพยานหลักฐานต้องพิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง โดยให้นำมาใช้บังคับกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย

การกำหนดให้รับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานตามมาตรานี้แต่เดิมการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานนั้น อยู่ในดุลพินิจของศาลที่จะกำหนดว่าสามารถรับฟังได้หรือไม่ แต่การกำหนดไว้แล้วตามพระราชบัญญัติฉบับนี้เป็นการกำหนดให้ศาลต้องรับฟังเสมอ แต่อย่างไรก็ตามการกำหนดของกฎหมายฉบับนี้ก็มิได้หมายความว่าพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ทุกชิ้นจะต้องมีน้ำหนักน่าเชื่อถือเสมอไป จึงมีการกำหนดหลักเกณฑ์ในการชั่งน้ำหนักพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ไว้ในมาตรา 11 วรรคสอง ดังนี้ คือ “ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง” การกำหนดหลักเกณฑ์เช่นนี้เป็นเรื่องของการใช้ “ต้นฉบับ” เป็นพยานหลักฐาน เพราะกฎหมายของไทยการจะอ้างเอกสารเป็นพยานหลักฐานนั้นอนุญาตให้รับฟังได้แต่ต้นฉบับเอกสาร ตามประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 93 ดังนี้ “การอ้างเอกสารเป็นพยานนั้น ให้ยอมรับฟังได้แต่ต้นฉบับเอกสารเท่านั้น...” แต่ตามมาตรา 10 ของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้บัญญัติไว้สอดคล้องกับกฎหมายแม่แบบว่า เอกสารที่จะใช้เป็นพยานหลักฐานได้นั้นไม่จำเป็นต้องอยู่ในรูปของต้นฉบับแต่สามารถอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ได้ เพราะได้มีการกำหนดวิธีการเก็บรักษาที่ถือว่าเป็นการเก็บรักษาอย่างเอกสารต้นฉบับไว้ในมาตรา 10 ที่มีหลักเกณฑ์สำคัญคือ

(1) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ

(2) สามารถแสดงข้อความนั้นในภายหลังได้

ซึ่งความถูกต้องของข้อความตาม (1) ต้องพิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงใด ๆของข้อความ ซึ่งการกำหนดให้ไม่มีการเปลี่ยนแปลงใด ๆของข้อความอาจหมายถึงการที่เราพิมพ์ข้อความหรือข้อมูลใด ๆลงไปเป็นจำนวนเท่าใด ข้อความหรือข้อมูลที่แสดงออกมาปรากฏทางหน้าจอคอมพิวเตอร์ หรือ print out ก็ต้องมีจำนวนเท่านั้น ยกเว้นแต่การรับรองหรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใด ๆที่อาจเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงข้อความซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้น ซึ่งการกำหนดหลักเกณฑ์เช่นนี้สอดคล้องกับบทบัญญัติของกฎหมายแม่แบบใน Article 8 และ Article 9 ในเรื่องของการเก็บรักษาเอกสารอย่างต้นฉบับ และการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน[3]

ในส่วนของการกำหนดให้รับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานตามมาตรา 11 นั้นก็มิได้กำหนดว่าให้รับฟังในรูปของพยานประเภทใด และโดยวิธีใด ซึ่งจากสถานะของข้อมูลอิเล็กทรอนิกส์อาจสามารถอนุมานได้ว่าข้อมูลอิเล็กทรอนิกส์น่าจะจัดเป็นพยานหลักฐานอีกประเภทหนึ่ง เพราะข้อมูลอิเล็กทรอนิกส์นั้นมีลักษณะที่เป็นได้ทั้งพยานเอกสารและพยานวัตถุ และการยอมรับข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานอีกประเภทหนึ่งนั้นใช่ว่าเพิ่งจะยอมรับเมื่อมีพระราชบัญญัติฉบับนี้ แต่ในศาลชำนัญพิเศษต่าง ๆ เช่น ศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ และศาลล้มละลายก็ได้ยอมรับข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานอีกประเภทหนึ่งมาเป็นเวลานานแล้ว โดยมีการกำหนดให้มีวิธีการนำสืบและการรับฟังเป็นพยานหลักฐานไว้โดยเฉพาะ ดังจะได้กล่าวไว้ในหัวข้อต่อไป

### 3.1.2 ข้อกำหนดของศาลชำนัญพิเศษต่าง ๆ

#### 3.1.2.1 ข้อกำหนดของศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ. 2540

ข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ. 2540 เป็นข้อกำหนดที่ออกโดยอาศัยอำนาจตามความในมาตรา 30 แห่งพระราชบัญญัติจัดตั้งศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ และวิธีพิจารณาคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ. 2539

[3] โปรดดูรายละเอียดได้ที่ภาคผนวก ง หน้า 115

ตามข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ.2540 กำหนดเกี่ยวการรับฟังข้อมูลอิเล็กทรอนิกส์ไว้ในข้อ33-36[4] โดยให้ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานอีกประเภทหนึ่ง โดยมีวิธีการนำสืบ การรับฟังเป็นพยานหลักฐานโดยเฉพาะดังนี้

ข้อมูลอิเล็กทรอนิกส์ ได้แก่ ข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์(ข้อ33) ข้อมูลบันทึกไว้ในหรือได้มาจากไมโครฟิล์ม สื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศประเภทอื่น(ข้อ36)

มีการกำหนดวิธีการนำสืบโดยคู่ความจะต้องปฏิบัติให้ถูกต้องเกี่ยวกับวิธีการนำสืบตามข้อ(34)กล่าวคือ ต้องมีการยื่นบัญชีระบุพยานและยื่นสำเนาสื่อที่บันทึกข้อมูลนั้น มิฉะนั้นศาลจะไม่รับฟังข้อมูลนั้นเป็นพยานหลักฐาน เว้นแต่ศาลเห็นว่าเพื่อประโยชน์แห่งความยุติธรรมจึงจะรับฟังข้อมูลนั้นเป็นพยานหลักฐานประกอบกับพยานหลักฐานอื่นด้วยก็ได้

ในเรื่องของการรับรองถูกต้องตามร่างข้อกำหนดนี้สามารถแบ่งได้ 3วิธี ดังนี้

1. การรับรองความถูกต้องโดยคู่ความฝ่ายที่อ้าง(ข้อ33)
2. การรับรองความถูกต้องเพราะการไม่คัดค้านของคู่ความอีกฝ่าย(ข้อ35)
3. การรับรองความถูกต้องโดยการตรวจสอบของศาล(ข้อ35)

ข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ.2540 ฉบับนี้ แม้จะกำหนดหลักเกณฑ์ในการนำสืบข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในการรับรองความถูกต้องไว้แต่ข้อกำหนดดังกล่าวเป็นเพียงข้อกำหนดของศาลชำนัญพิเศษไม่สามารถนำมาใช้ร่วมกับคดีประเภทอื่นได้หากจะนำไปใช้ก็ต้องกำหนดหรือบัญญัติขึ้นมาต่างหาก เช่น ข้อกำหนดคดีล้มละลาย หรือข้อกำหนดคดีภาษีอากร

### 3.1.2.2 ข้อกำหนดคดีล้มละลาย พ.ศ. 2549

ข้อกำหนดคดีล้มละลาย พ.ศ.2549 ออกโดยอาศัยอำนาจตามความในมาตรา 19 แห่งพระราชบัญญัติจัดตั้งศาลล้มละลายและวิธีพิจารณาคดีล้มละลาย พ.ศ.2542 แก้ไขเพิ่มเติมโดยพระราชบัญญัติจัดตั้งศาลล้มละลายและวิธีพิจารณาคดีล้มละลาย(ฉบับที่3) พ.ศ.2548

---

[4] โปรดดูรายละเอียดได้ที่ภาคผนวก จ หน้า 119

ตามข้อกำหนดคดีล้มละลาย พ.ศ.2549 ได้กำหนดเกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์ไว้ในข้อ 20-23[5] โดยให้ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานอีกประเภทหนึ่ง มีวิธีการนำสืบ การรับฟังเป็นพยานหลักฐานโดยเฉพาะ ซึ่งมีเนื้อหาเช่นเดียวกันกับข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ. 2540 ข้อ 33-36 ทั้งประเภทของข้อมูลอิเล็กทรอนิกส์ การยื่นพยานหลักฐาน และการรับรองความถูกต้องแท้จริง แต่ก็มีข้อแตกต่างบางประการดังนี้

(1) การรับรองของบุคคลที่เกี่ยวข้องหรือดำเนินการตามข้อกำหนดคดีล้มละลาย พ.ศ.2549 ข้อ 20 นั้น จะมีการรับรองว่า

- การบันทึกข้อมูลโดยเครื่องคอมพิวเตอร์ หรือการประมวลโดยเครื่องคอมพิวเตอร์เป็นการกระทำตามปกติในการประกอบกิจการของผู้ใช้คอมพิวเตอร์ และ

- การบันทึกและการประมวลผลข้อมูลเกิดจากการใช้เครื่องคอมพิวเตอร์ปฏิบัติงานตามขั้นตอนการทำงานของเครื่องคอมพิวเตอร์อย่างถูกต้อง และหากมีกรณีการทำงานของเครื่องคอมพิวเตอร์ขัดข้องก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

หรือไม่ก็ได้ แต่ข้อกำหนดของคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศกลางพ.ศ. 2540 ข้อ 33 ต้องมีการรับรองเสมอ

(2) ถ้ามีคำรับรองของบุคคลที่เกี่ยวข้องหรือดำเนินการแล้ว คู่ความก็ไม่ต้องแสดงให้ศาลเห็นถึงการกระทำตามปกติของผู้ใช้และความถูกต้องของการบันทึกและประมวลผลข้อมูลอีก ในขณะที่ข้อกำหนดของคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศกลาง แม้มีการรับรองก็ยังต้องแสดงให้ศาลเห็นเสมอ

(3) ข้อมูลอิเล็กทรอนิกส์ที่มิใช่ข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์ เช่น ไมโครฟิล์ม สื่ออิเล็กทรอนิกส์ สื่อเทคโนโลยีสารสนเทศประเภทอื่น ในข้อกำหนดคดีล้มละลายไม่ต้องแสดงให้เห็นถึงการกระทำตามปกติของผู้ใช้และความถูกต้องของการบันทึกและการประมวลผลข้อมูลแต่อย่างใด ขณะที่ในข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศกลาง ยังต้องมีด้วย

---

[5] โปรดดูรายละเอียดได้ที่ภาคผนวก ฉ หน้า 121

### 3.1.2.3 ข้อกำหนดคดีภาษีอากร พ.ศ. 2544

ข้อกำหนดคดีภาษีอากร พ.ศ.2544 เป็นข้อกำหนดที่ออกโดยอาศัยอำนาจตามความในมาตรา 20 แห่งพระราชบัญญัติจัดตั้งศาลภาษีอากร พ.ศ.2528

ตามข้อกำหนดคดีภาษีอากรนี้ กำหนดเกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์ไว้ในข้อ 30-33[6] โดยให้ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานอีกประเภทหนึ่ง มีวิธีการนำสืบเป็น การรับฟังเป็นพยานหลักฐานโดยเฉพาะ ซึ่งมีเนื้อหาเช่นเดียวกันกับข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศพ.ศ.2540 ข้อ33-36 ทั้งประเภทของข้อมูลอิเล็กทรอนิกส์ การยื่นพยานหลักฐาน และการรับรองความถูกต้องแท้จริง

## 3.2 กฎหมายของต่างประเทศที่เกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน

กฎหมายต่างประเทศที่เกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานที่จะนำมาพิจารณามีอยู่ 3 ฉบับซึ่งจะได้พิจารณาเป็นลำดับดังนี้ ลักษณะทั่วไปของกฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์ หลักเกณฑ์ และผลทางกฎหมายของกฎหมายแม่แบบUNCITRAL ในการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน กฎหมายแม่แบบของ UNCITRAL ว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ และกฎหมายแม่แบบว่าด้วยพยานหลักฐานอิเล็กทรอนิกส์ 2002 (Draft Model Law on Electronic Evidence 2002)

### 3.2.1 กฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์[7]

กฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์เป็นกฎหมายการพาณิชย์ทางอิเล็กทรอนิกส์ฉบับแรกถูกร่างขึ้น โดยคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติ (United Nations Commission on International Trade Law - UNCITRAL) ซึ่งเป็นคณะกรรมาธิการคณะหนึ่งอยู่ภายใต้องค์การสหประชาชาติ

---

[6] โปรดดูรายละเอียดได้ที่ภาคผนวก ช หน้า 123

[7] พินัย ณ นคร , **กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์,** บทบัณฑิตย์ หน้า 3-4 เล่ม 56 ตอน 2, พ.ศ. 2543

คณะกรรมาธิการคณะนี้มีวัตถุประสงค์ในการสร้างกฎเกณฑ์ทางการค้าระหว่างประเทศให้เป็นแบบแผนเดียวกันและมีความสอดคล้องกัน ซึ่งกฎหมายดังกล่าวนี้เรียกว่ากฎหมายแม่แบบว่าด้วยการพาณิชย์ทางอิเล็กทรอนิกส์ (Model Law on Electronic Commerce) ผ่านการยกร่างและพิจารณาร่วมกันของบรรดาประเทศสมาชิกของสหประชาชาติแล้วเสร็จในปี พ.ศ. 2539 โดยสมัชชาใหญ่แห่งสหประชาชาติยังแนะนำให้ทุกประเทศให้ความสำคัญและคำนึงถึงกฎหมายแม่แบบนี้อย่างที่สุดในการตราหรือแก้ไขกฎหมายของตนเพื่อจรรโลงให้กฎหมายการค้าระหว่างประเทศในเรื่องนี้สอดคล้องกันและเป็นอันหนึ่งอันเดียวกัน[8]

### 3.2.2 ลักษณะทั่วไปของกฎหมายแม่แบบของUNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์

#### 3.2.2.1 กฎหมายกำหนดกรอบเบื้องต้น (Framework Law)

กฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์มุ่งหมายเพียงกำหนดหลักเกณฑ์สำคัญ ๆที่ประเทศต่าง ๆนำไปใช้เป็นแนวทางในการตราหรือแก้ไขกฎหมายของตนเพื่อรองรับวิธีการรับส่งหรือเก็บรักษาข้อมูลโดยใช้วิธีการทางอิเล็กทรอนิกส์เพื่อให้กฎหมายของประชาคมโลกเป็นไปในทิศทางเดียวกัน แต่ละประเทศที่นำกฎหมายแม่แบบนี้ไปใช้เป็นแนวทางในการตราหรือแก้ไขกฎหมายของตนสามารถกำหนดรายละเอียดต่าง ๆเพิ่มเติมจากหลักเกณฑ์สำคัญ ที่กำหนดไว้ในกฎหมายแม่แบบ โดยส่วนที่เพิ่มเติมนั้นสอดคล้องกับหลักเกณฑ์สำคัญและเจตนารมณ์ของกฎหมายแม่แบบ ดังนั้นจึงกล่าวกันว่ากฎหมายแม่แบบเป็น กฎหมายกำหนดกรอบเบื้องต้น (Framework Law)

---

[8] อารัมภบทบางตอนของมติสมัชชาใหญ่แห่งสหประชาชาติที่สะท้อนถึงความสำคัญของกฎหมายแม่แบบจึงได้คัดมากล่าว ณ ที่นี้

"Noting that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, "Convinced that the establishment of a model law facilitating the use of electronic commerce that is acceptable to States with different legal, social and economic systems, could contribute significantly to the development of harmonious economic relations,"

**3.2.2.2 หลักการสำคัญของกฎหมายแม่แบบมีหลักการสำคัญดังนี้**

**3.2.2.2.1 หลักการยอมรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ เสมอกับสถานะทางกฎหมายของเอกสารธรรมดา (Functional-equivalent approach)**

หลักความเท่าเทียมกัน (Functional-equivalent approach) หลักการนี้เป็นการยกระดับความเท่าเทียมว่าการทำธุรกรรมทางอิเล็กทรอนิกส์ มีค่าเท่าเทียมกับการทำธุรกรรมที่ปรากฏในรูปของกระดาษตามบทบัญญัติในมาตรา8-12ของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เป็นต้น โดยปกติแล้วกฎหมายของประเทศต่างๆได้วางข้อกำหนดบางเรื่องไว้เช่น การทำเป็นหนังสือ (writing) การมีหลักฐานเป็นหนังสือ (evidence in writing) การมีเอกสารต้นฉบับ (original) ตลอดจนการลงลายมือชื่อ (signature) ข้อกำหนดเหล่านี้เป็นอุปสรรคต่อการค้าโดยใช้ข้อมูลอิเล็กทรอนิกส์ซึ่งการแก้ไขข้อขัดข้องทางกฎหมายเหล่านี้จำเป็นต้องให้การยอมรับ หรือรับรองว่าข้อมูลอิเล็กทรอนิกส์มีสถานะทางกฎหมายเช่นเดียวกับเอกสารธรรมดาการให้ข้อมูลอิเล็กทรอนิกส์มีผลหรือสถานะทางกฎหมายเช่นเดียวกับเอกสารธรรมดาตามหลักFunctional-equivalent approachนั้นมิได้ลบล้างหลักกฎหมายที่ใช้กับเอกสารธรรมดา กฎหมายมิได้ระบุบังคับให้ใช้ข้อมูลอิเล็กทรอนิกส์แทนเอกสารธรรมดา

ดังนั้นบุคคลยังคงสามารถติดต่อทำการค้ากันโดยใช้วิธีแบบเดิมโดยอยู่ภายใต้บังคับของหลักกฎหมายดั้งเดิม(เช่นหลักประมวลกฎหมายแพ่งและพาณิชย์ของไทยว่าด้วยสัญญาที่ต้องมีหลักฐานเป็นหนังสือ) กฎหมายว่าด้วยพาณิชย์ทางอิเล็กทรอนิกส์จึงเป็นเพียงการให้ทางเลือกใหม่แก่บุคคลที่ต้องการทำการค้าโดยผ่านสื่ออิเล็กทรอนิกส์

**3.2.2.2.2 หลักเสรีภาพในการแสดงเจตนา ( Party Autonomy)**

หรือเรียกอีกชื่อหนึ่งว่า หลักความศักดิ์สิทธิ์ในการแสดงเจตนา คือการเคารพในสิทธิเสรีภาพในการแสดงเจตนาของคู่กรณีว่าประสงค์จะให้เป็นอย่างไร หากไม่ขัดต่อความสงบเรียบร้อยหรือบทบัญญัติแห่งกฎหมายไม่ได้บัญญัติห้ามไว้โดยชัดแจ้ง ในลักษณะของบทบัญญัติบังคับห้ามเปลี่ยนแปลง (Mandatory Rules) ก็สามารถตกลงตามที่คู่กรณีต้องการได้

**3.2.2.2.3 หลักความเป็นกลางทางเทคโนโลยีและความเป็นกลางของสื่อ (Technology Neutrality)**

เป็นกรณีที่กฎหมายได้เปิดกว้างให้มีความยืดหยุ่นและยอมรับเทคโนโลยีสารสนเทศต่างๆที่เปลี่ยนแปลงไปอย่างรวดเร็วมีการพัฒนาอย่างต่อเนื่อง กฎหมายจึงต้องเปิดกว้างยืดหยุ่นเพื่อให้ทันกับการเปลี่ยนแปลงของเทคโนโลยี วัตถุประสงค์หลักในการรับรองสถานภาพทางกฎหมายของข้อมูลอิเล็กทรอนิกส์จะพบได้จากบทบัญญัติใน Article 5[9] และ Article 3[10] ของ Model Law on Electronic Commerce จากบทบัญญัติทั้ง 2 มาตราจะเห็นได้ว่ากฎหมายรับรองสถานภาพของข้อมูลอิเล็กทรอนิกส์ เช่นการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์(EDI) ไปรษณีย์อิเล็กทรอนิกส์(E-Mail) โทรเลข (Telegram) โทรพิมพ์ (Telex) โทรสาร (Telecopy)

**หลักเกณฑ์และผลทางกฎหมายของกฎหมายแม่แบบ UNCITRAL ในการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน**

**3.2.2.2.4 หลักเกณฑ์เกี่ยวกับการรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์กฎหมายแม่แบบของUNCITRALว่าด้วยพาณิชย์อิเล็กทรอนิกส์**

ยอมรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ปรากฏอยู่ใน Article 5: Legal recognition of data messages[11] ซึ่งบัญญัติว่า “ข้อมูลจะไม่ถูกปฏิเสธผลทางกฎหมาย หรือปฏิเสธความสมบูรณ์หรือการมีผลบังคับทางกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์” บทบัญญัตินี้นับเป็นหัวใจของกฎหมายแม่แบบฉบับนี้ นอกจากบทบัญญัติมาตรานี้แล้วผู้ร่างกฎหมายแม่แบบได้ตระหนักว่าประเด็นทางกฎหมาย

---

[9] Article 5. Legal recognition of data messages

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

[10] Article 3 (a) “Data message” means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI) , electronic mail, telegram, telex or telecopy;

[11] Ibid

เกี่ยวกับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์มักจะเป็นประเด็นที่เกี่ยวข้องกับการทำสัญญาระหว่างกัน จึงได้มีบทบัญญัติที่กล่าวถึง การรับรองผลทางกฎหมายของคำเสนอ คำสนอง และการแสดงเจตนา

**3.2.2.2.5 หลักเกณฑ์เกี่ยวกับการทำเป็นหนังสือ และต้นฉบับ**

ข้อกำหนดเกี่ยวกับ “หนังสือ” เป็นข้อขัดข้องทางกฎหมายของประเทศต่างๆที่มักกำหนดให้สัญญาบางประเภทหรือบางอย่างต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือจึงจะใช้บังคับได้ กฎหมายแม่แบบจึงกำหนดให้การใช้ข้อมูลอิเล็กทรอนิกส์ถือว่าเป็นการทำเป็นหนังสือหรือมีหลักฐานเป็นหนังสือ และหากข้อมูลอิเล็กทรอนิกส์อยู่ในสภาพที่สามารถเข้าถึงและสามารถนำกลับมาใช้ภายหลังได้(accessible so as to be usable for subsequent reference) โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่ามีความทัดเทียมกับเอกสารที่ทำเป็นหนังสือ หรือมีหลักฐานเป็นหนังสือ ทั้งนี้คำอธิบายประกอบกฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์(Guide to Enactment) ได้อธิบายว่า สภาพที่สามารถเข้าถึงข้อมูลอิเล็กทรอนิกส์นั้น หมายถึงสภาพที่ข้อมูลอิเล็กทรอนิกส์สามารถอ่านและแปลได้ (readable and interpretable)

ส่วนหลักเกณฑ์เกี่ยวกับ “ต้นฉบับ” กฎหมายแม่แบบของUNCITRAL บัญญัติว่า หากมีการแสดงหรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์โดยวิธีการที่น่าเชื่อถือได้ ซึ่งสามารถรักษาความถูกต้องของข้อมูลอิเล็กทรอนิกส์ตั้งแต่แรกสร้างข้อมูลนั้นขึ้นเป็นข้อมูลรูปแบบสุดท้าย (final form)ก็ให้ถือว่าเป็นการแสดงหรือเก็บรักษาต้นฉบับตามกฎหมายนั้นแล้ว

มีข้อน่าสังเกตว่า การแสดงหรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์อย่างเอกสารต้นฉบับเพื่อใช้เป็นพยานหลักฐานนั้น การรักษาความถูกต้องของข้อมูลอิเล็กทรอนิกส์ ต้องพิเคราะห์ว่าข้อมูลอิเล็กทรอนิกส์ยังอยู่ในสภาพที่สมบูรณ์ โดยปราศจากการเปลี่ยนแปลงแก้ไข (complete and unaltered)หรือไม่ ส่วนการพิเคราะห์วิธีการรักษาความถูกต้องของข้อมูลอิเล็กทรอนิกส์ว่าเป็นวิธีการที่น่าเชื่อถือได้หรือไม่ ต้องพิจารณาจากพฤติการณ์ทั้งปวงที่เกี่ยวข้อง และวัตถุประสงค์ของการสร้างข้อมูลนั้น หรือหากเป็นกรณีที่กฎหมายกำหนดให้แสดงเอกสารต้นฉบับ ถ้าบุคคลเลือกที่จะนำข้อมูลอิเล็กทรอนิกส์ที่ไม่มีการเปลี่ยนแปลงแก้ไขมาแสดงแทนการแสดงเอกสารต้นฉบับ ข้อมูลอิเล็กทรอนิกส์นั้นต้องอยู่ในสภาพที่สามารถทำให้ปรากฏแก่บุคคลที่จะเป็นผู้รับข้อมูลนั้นด้วย

**3.2.2.2.6 หลักเกณฑ์การรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน**

กฎหมายแม่แบบUNCITRAL มีบทบัญญัติเกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานไว้ด้วย ส่วนการชั่งน้ำหนักพยานหลักฐานเป็นเรื่องที่ต้องพิจารณาถึงพฤติการณ์ทั้งปวงโดยคำนึงถึง วิธีการสร้าง เก็บ รับ และส่งข้อมูลอิเล็กทรอนิกส์ และวิธีการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์นั้น

**3.2.2.2.7 หลักเกณฑ์ความเป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ เวลาและสถานที่ที่ถือว่าได้ส่ง และได้รับข้อมูล**

**3.2.2.2.7.1 การส่งและรับข้อมูลอิเล็กทรอนิกส์ กฎหมายแม่แบบของ UNCITRAL ได้กำหนดข้อสันนิษฐานที่เกี่ยวข้องไว้ 3 ประการคือ**

ก. หากผู้ส่งได้ส่งข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง กฎหมายถือว่าผู้ส่งเป็นผู้ส่งข้อมูลอิเล็กทรอนิกส์นั้นจะปฏิเสธว่าตนมิได้ส่งไม่ได้[12]

ข. ในระหว่างผู้ส่งและผู้รับข้อมูลอิเล็กทรอนิกส์ ถ้าข้อมูลอิเล็กทรอนิกส์ใดส่งโดยผู้มี อำนาจกระทำแทนผู้ส่งเกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้นกฎหมายถือว่า ข้อมูลอิเล็กทรอนิกส์นั้นเป็นของผู้ส่ง[13]

ค. กรณีที่ข้อมูลอิเล็กทรอนิกส์ได้ส่งไปโดยระบบคอมพิวเตอร์หรือระบบเครือข่ายเองโดยตั้งโปรแกรมรับ-ส่งและประมวลผลอัตโนมัติ กฎหมายถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้มีการส่งออกไปทางระบบอัตโนมัติดังกล่าวเป็นของผู้ที่ปรากฏชื่อว่าเป็นผู้ส่ง[14]

ง. กรณีคู่กรณีได้ตกลงกันเกี่ยวกับวิธีการในการพิสูจน์ตัวบุคคลเมื่อมีการส่งข้อมูลอิเล็กทรอนิกส์ไปยังอีกฝ่ายหนึ่ง ถ้าผู้รับข้อมูลได้ใช้วิธีการตรวจสอบตัวบุคคลตามวิธีการที่ตกลงกันไว้ก่อนแล้วและผลการตรวจสอบปรากฏว่าบุคคลใดเป็นผู้ส่งข้อมูลอิเล็กทรอนิกส์ กฎหมายกำหนดข้อสันนิษฐานเป็นคุณแก่ผู้รับข้อมูลว่า ข้อมูลอิเล็กทรอนิกส์ที่ได้รับนั้นเป็นข้อมูลที่ส่งโดยบุคคลนั้น เมื่อว่าระบบการตรวจสอบระบุว่าเป็นผู้ส่งข้อมูลจะอ้างว่าตนมิได้เป็นผู้ส่งข้อมูลไม่ได้[15] ทั้งนี้เพราะผู้ส่งได้ตกลงให้ผู้รับข้อมูลใช้ระบบตรวจสอบเช่นนั้นเอง จึงต้องผูกพันตามระบบตรวจสอบที่ได้ตกลงไว้ก่อนแล้ว

จ. กรณีการส่งข้อมูลอิเล็กทรอนิกส์เกิดจากการกระทำของผู้มีความสัมพันธ์ใกล้ชิดที่สามารถขนาดเข้าถึง(access) นำวิธีทางเทคนิคของบุคคลนั้นไปใช้ส่ง

---

[12] Article 13 (1)

[13] Article 13 (2) (a)

[14] Article 13 (2) (b)

[15] Article 13 (3)

ข้อมูลอิเล็กทรอนิกส์ไปให้ผู้รับ กฎหมายสันนิษฐานว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นเป็นของบุคคลดังกล่าวแม้ตนจะมิได้เป็นผู้ส่งข้อมูลก็ตาม เพราะกฎหมายประสงค์ให้บุคคลใช้ความระมัดระวังและวิธีการรักษาความปลอดภัยของตนเอง หากตกไปอยู่ในความครอบครองของผู้อื่นที่มีความสัมพันธ์ใกล้ชิดกับตน ก็ต้องรับผิดในข้อมูลที่ส่งออกไปแม้ตนจะมิได้อนุญาตก็ตาม[16]

**3.2.2.2.7.2 เวลาที่ถือว่าได้ส่งและได้รับข้อมูล**

เวลาที่ถือว่าได้ส่งข้อมูลอิเล็กทรอนิกส์กฎหมายแม่แบบ UNCITRAL กำหนดให้มีผลเมื่อข้อมูลนั้นเข้าสู่ระบบข้อมูลที่อยู่นอกเหนือการควบคุมของผู้ส่งหรือของตัวแทนของผู้ส่ง

เวลาที่ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนั้น กฎหมายกำหนดว่าถ้าผู้รับได้กำหนดระบบข้อมูลที่ใช้รับข้อมูลไว้โดยเฉพาะ การรับข้อมูลจะมีผลเมื่อข้อมูลได้เข้าสู่ระบบข้อมูลที่กำหนดไว้ กฎหมายก็จะถือว่าการรับข้อมูลมีผลเมื่อผู้รับได้เรียกข้อมูลนั้นขึ้นมาให้ปรากฏแก่ผู้รับด้วย(retrieved by the addressee) แต่หากมิได้มีการกำหนดระบบข้อมูลใดไว้โดยเฉพาะ การรับข้อมูลจะมีผลตั้งแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์เข้าสู่ระบบข้อมูลของฝ่ายผู้รับข้อมูลนั้น[17]

**3.2.2.2.7.3 สถานที่ที่ถือว่าได้ส่งและรับข้อมูลอิเล็กทรอนิกส์**

กฎหมายแม่แบบUNCITRAL กำหนดหลักเกณฑ์เกี่ยวกับสถานที่ที่ถือว่าการส่งและการรับข้อมูลอิเล็กทรอนิกส์มีผล โดยถือว่าข้อมูลอิเล็กทรอนิกส์ได้ส่ง ณ สถานที่ที่ผู้ส่งข้อมูลอิเล็กทรอนิกส์ประกอบธุรกิจ และได้รับ ณ สถานที่ที่ผู้รับประกอบธุรกิจ หากคู่กรณีมีสถานที่ประกอบธุรกิจหลายแห่งก็ให้ยึดถือเอาสถานที่ที่มีความสัมพันธ์ใกล้ชิดกับธุรกรรมนั้นมากที่สุด หรือหากไม่อาจชี้ได้ว่าสถานที่ใดมีความสัมพันธ์ใกล้ชิดกับธุรกรรมนั้นมากที่สุด ก็ให้ยึดเอาสถานที่ทำการแห่งใหญ่ หากไม่มีสถานที่ทำการแห่งใหญ่ก็ให้ถือเอาถิ่นที่อยู่ปกติของคู่กรณีเป็นสำคัญ[18]

---

[16] Article 13 (3) (b)

[17] Article 15 (2)

[18] Article 15 (4) (a),(b)

**3.2.2.2.8 หลักเกณฑ์เกี่ยวกับ “ลายมือชื่อ”**

กฎหมายแม่แบบของUNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์กำหนดว่า ลายมือชื่ออิเล็กทรอนิกส์ต้องสร้างขึ้นโดยกระบวนการที่สามารถระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อและสามารถบ่งบอกได้ว่าบุคคลนั้นเห็นชอบกับข้อความอิเล็กทรอนิกส์ที่มีลายมือชื่อนั้นกำกับ และวิธีการที่นำมาใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นต้องมีความน่าเชื่อถือ โดยต้องเป็นวิธีการที่เหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ ส่วนความน่าเชื่อถือและเหมาะสมเป็นเรื่องที่ต้องพิเคราะห์พฤติการณ์ทั้งปวงประกอบ ทั้งนี้กฎหมายแม่แบบ UNCITRAL(Guide to Enactment) ได้ให้ตัวอย่างของพฤติการณ์ดังกล่าวไว้ว่า ให้รวมถึงพฤติการณ์ดังต่อไปนี้ ความพร้อม คุณสมบัติหรือประสิทธิภาพของเครื่องมือที่คู่กรณีนำมาใช้ ความสามารถของระบบสื่อสาร ลักษณะของกิจกรรมทางการค้านั้น ความบ่อยครั้งที่คู่กรณีทำธุรกรรมระหว่างกัน ประเภทและธุรกรรมที่ทำระหว่างกัน ความสำคัญและมูลค่าของข้อมูลอิเล็กทรอนิกส์ที่สื่อสารกัน ทางปฏิบัติทางการค้า[19]

**3.3 กฎหมายแม่แบบว่าด้วยพยานหลักฐานอิเล็กทรอนิกส์ 2002 (Draft Model Law on Electronic Evidence 2002)**

**3.3.1 ลักษณะทั่วไป**

กฎหมายแม่แบบว่าด้วยพยานหลักฐานอิเล็กทรอนิกส์เป็นร่างกฎหมายที่กลุ่มประเทศในเครือจักรภพอังกฤษ ได้ตั้งกลุ่มผู้เชี่ยวชาญ (Expert Group) ร่วมกันยกร่างขึ้นมาเพื่อให้มีมาตรการคุ้มครองการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน เนื่องจากข้อมูลอิเล็กทรอนิกส์นั้นมีความแตกต่างจากเอกสารธรรมดา ข้อมูลอิเล็กทรอนิกส์มีความซับซ้อนสูง มีแนวโน้มว่าจะถูกทำลายหรือแก้ไขเปลี่ยนแปลงได้ง่ายกว่าบันทึกในกระดาษ ร่างกฎหมายนี้กลุ่มผู้เชี่ยวชาญร่างขึ้นเพื่อให้เป็นแนวทางหรือมาตรฐานขั้นต่ำในการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน ซึ่งมีเนื้อหาสำคัญเกี่ยวกับบทบัญญัติทั่วไปในการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ขอบเขตของกฎหมาย การรับรองความถูกต้องแท้จริง การใช้หลักพยานหลักฐานที่ดีที่สุด ข้อสันนิษฐานในเรื่องความถูกต้อง มาตรฐาน การพิสูจน์โดยคำให้การพยานการถามค้าน ข้อตกลงในการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน และการรับฟังลายมือชื่ออิเล็กทรอนิกส์

---

[19] พินัย ณ นคร **กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์**, บทบัณฑิตย์ ,เล่ม 56 ตอน 2 , พ.ศ. 2543:น. 4-10

**3.3.2 บทบัญญัติทั่วไปในการรับฟังข้อมูลข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน**

ตามมาตรา3 กำหนดห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานเพียงเพราะว่าอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

**3.3.2.1 หลักกฎหมายที่เกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน**

(1) หลักพยานหลักฐานที่ดีที่สุด

ตามมาตรา 4(1) กำหนดขอบเขตของพระราชบัญญัติฉบับนี้ว่าไม่มีผลกระทบถึงกฎหมายคอมมอนลอว์ใดๆ หรือกฎเกณฑ์ตามพระราชบัญญัติอื่นที่เกี่ยวกับการรับฟังหรือการบันทึกยกเว้นกฎเกณฑ์เกี่ยวกับความน่าเชื่อถือและหลักการรับฟังพยานหลักฐานที่ดีที่สุด และมาตรา6กำหนดให้กระบวนพิจารณาใดๆที่ใช้หลักการรับฟังพยานหลักฐานที่ดีที่สุดที่เกี่ยวกับบันทึกอิเล็กทรอนิกส์ กฎเกณฑ์ดังกล่าวถูกทำให้เป็นที่พอใจได้โดยการพิสูจน์ถึงความถูกต้องแท้จริงของระบบบันทึกอิเล็กทรอนิกส์ซึ่งข้อมูลถูกบันทึกหรือจัดเก็บไว้และในกระบวนการทางกฎหมายใดๆเมื่อบันทึกอิเล็กทรอนิกส์ในรูปสิ่งพิมพ์ออก(Printouts) มีความสอดคล้อง น่าเชื่อถือ หรือถูกใช้เช่นเดียวกับบันทึกของข้อมูลที่ถูกบันทึกหรือจัดเก็บในรูปสิ่งพิมพ์ออก(Printouts) ให้สิ่งพิมพ์ออก(Printouts) นั้นคือบันทึกตามวัตถุประสงค์ของหลักการรับฟังพยานหลักฐานที่ดีที่สุด

(2) การรับฟังพยานบอกเล่า

ตามมาตรา 4(1) กำหนดขอบเขตของพระราชบัญญัติฉบับนี้ว่าไม่กระทบถึงกฎหมายคอมมอนลอว์ใดๆหรือกฎเกณฑ์ตามพระราชบัญญัติอื่นเกี่ยวกับการรับฟังหรือการบันทึก ยกเว้นกฎเกณฑ์ความน่าเชื่อถือและหลักการรับฟังพยานหลักฐานที่ดีที่สุด ซึ่งหลักการรับฟังพยานบอกเล่าก็เป็นส่วนหนึ่งของหลักพยานหลักฐานที่ดีที่สุด จึงได้รับยกเว้นไปด้วย

(3) การรับรองความถูกต้อง

ก.การพิสูจน์โดยผู้อ้าง

ตามมาตรา 5 บุคคลที่อ้างข้อมูลอิเล็กทรอนิกส์ (electronic record) เป็นพยานหลักฐานในกระบวนวิธีพิจารณาทางกฎหมายใดๆ มีภาระการพิสูจน์ถึงความน่าเชื่อถือว่าพยานหลักฐานนั้นสามารถสนับสนุนให้เห็นถึงข้อมูลอิเล็กทรอนิกส์ตามที่กล่าวอ้าง

ข. ข้อสันนิษฐานโดยกฎหมาย

ตามมาตรา 7 กรณีที่ไม่มีพยานหลักฐานอื่นในทางตรงกันข้าม ความถูกต้องแท้จริงของระบบข้อมูลอิเล็กทรอนิกส์ซึ่งข้อมูลอิเล็กทรอนิกส์ถูกบันทึกหรือเก็บรักษา จะถูกสันนิษฐานไว้ก่อนว่าถูกต้อง หากในกระบวนการทางกฎหมายใดๆ ที่

(a) พยานหลักฐานที่ถูกอ้างอิงเพื่อสนับสนุนการค้นหาว่าระบบคอมพิวเตอร์หรือสิ่งอื่นใดในลักษณะเดียวกันในทุกๆครั้ง มีความถูกต้องหรือถ้าไม่เป็นเช่นนั้น กรณีที่ระบบดังกล่าวไม่ถูกต้องหรืออยู่นอกการควบคุม ความถูกต้องที่แท้จริงของบันทึกจะไม่ถูกกระทบจากสถานการณ์เช่นว่านั้น และไม่มีเหตุอันควรสงสัยเป็นอย่างอื่นถึงความถูกต้องแท้จริงของบันทึก หรือ

(b) ข้อมูลอิเล็กทรอนิกส์มีการบันทึกหรือจัดเก็บโดยคู่กรณีฝ่ายตรงข้าม หรือ

(c) ข้อมูลอิเล็กทรอนิกส์มีการบันทึกหรือจัดเก็บตามปกติประเพณีและตามลักษณะของธุรกิจ โดยบุคคลซึ่งไม่ใช่คู่ความในกระบวนพิจารณาและไม่ได้บันทึกหรือจัดเก็บโดยอยู่ภายใต้การควบคุมของคู่ความฝ่ายที่กล่าวอ้างบันทึกอิเล็กทรอนิกส์เป็นพยานหลักฐาน

ค. มาตรฐานทั่วไปในการพิสูจน์

ตามมาตรา 8 กำหนดเกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์ โดยอาจกำหนดต้องนำเสนอเป็นพยานหลักฐานตามมาตรฐานใดๆ กระบวนพิจารณา ประเพณีและการปฏิบัติในการบันทึกหรือเก็บรักษาบันทึกอิเล็กทรอนิกส์ ตามประเภทของธุรกิจในการใช้ การบันทึก หรือเก็บรักษา บันทึกอิเล็กทรอนิกส์ และธรรมชาติและบันทึกของวัตถุประสงค์ของบันทึกอิเล็กทรอนิกส์นั้น

ง. การใช้คำให้การของพยานพิสูจน์ความน่าเชื่อถือ

ตามมาตรา 9 กำหนดสาระสำคัญที่กล่าวถึงในมาตรา 6 มาตรา 7 มาตรา 8 อาจสร้างขึ้นในรูปคำให้การพยาน

จ. การถามค้านของคู่ความ

ตามมาตรา 10(1) กำหนดให้คำให้การที่กล่าวถึงในมาตรา 9 อาจถูกถามค้านได้โดยคู่ความอีกฝ่าย และ (2) คู่ความอาจถามค้านพยานตามมาตรา 7(C) ได้

ฉ. ข้อสัญญาให้รับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานได้

ตามมาตรา 11(1)กำหนดว่ากรณีที่ไม่มีกฎหมายบัญญัติเป็นอย่างอื่น คู่ความอาจตกลงกันในเวลาใดๆ ให้รับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานได้

ช.การรับฟังลายมือชื่ออิเล็กทรอนิกส์เป็นพยานหลักฐาน

ตามมาตรา 12 ยอมรับให้ใช้ลายมือชื่ออิเล็กทรอนิกส์แทนลายมือชื่อธรรมดาได้ และต้องพิสูจน์ถึงความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์นั้นไม่ว่าโดยวิธีใดๆ รวมถึงโดยการแสดงให้เห็นถึงกระบวนการสร้างเท่าที่จำเป็นเพื่อระบุถึงตัวบุคคล ในการทำธุรกรรม และเพื่อเป็นการรับรองว่าข้อมูลอิเล็กทรอนิกส์เป็นของบุคคลนั้น[20]

### 3.4 กฎหมายแม่แบบว่าด้วยลายมือชื่ออิเล็กทรอนิกส์ 2001 (Model Law On Electronic Signatures 2001)

นับตั้งแต่คณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติ(United Nations Commission or International Trade Law – UNCITRAL) ได้สร้างกฎหมายแม่แบบว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ (Model Law on Electronic Commerce) ขึ้น คณะกรรมาธิการก็มีความกังวลในเรื่องของลายมือชื่อทางอิเล็กทรอนิกส์ โดยเฉพาะอย่างยิ่งลายมือชื่อดิจิตอลและหน่วยงานที่ทำการรับรอง (Certification Authorities) จึงได้มีการสำรวจความต้องการและเตรียมการยกร่างกฎเกณฑ์แม่แบบ (Uniform Rules) ให้ครอบคลุมเรื่องต่างๆ อันได้แก่ หลักกฎหมายที่สนับสนุนกระบวนการรับรอง การกำหนดความเสี่ยงและความรับผิดของผู้ใช้ ผู้ให้บริการ และบุคคลที่เกี่ยวข้องในการใช้เทคนิคการรับรอง การออกใบรับรอง เป็นต้น ดังนั้นจึงได้มีการตั้งคณะทำงานเพื่อยกร่างกฎหมายแม่แบบให้ครอบคลุมเรื่องดังกล่าว และกฎเกณฑ์แม่แบบในเรื่องลายมือชื่ออิเล็กทรอนิกส์ก็เสร็จสมบูรณ์ในปี ค.ศ. 2000 โดยใช้ชื่อว่า UNCITRAL Model Law on Electronic Signatures และมีแนวทางการใช้ที่รียกว่า Guide to Enactment ที่เสร็จสมบูรณ์ในปี ค.ศ. 2001 ทั้งนี้เพื่อเป็นการยอมรับว่าลายมือชื่อทางอิเล็กทรอนิกส์มีสถานะทางกฎหมายเช่นเดียวกับลายมือชื่อที่ลงกันไว้ในระบบกระดาษนั่นเอง ทั้งนี้เพื่อเป็นการยอมรับว่าลายมือชื่อทางอิเล็กทรอนิกส์มีสถานะทางกฎหมายเช่นเดียวกับลายมือชื่อที่ลงกันไว้ในระบบกระดาษนั่นเอง นอกจากนี้กฎเกณฑ์แม่แบบยังให้แนวทางในเรื่องระบบโครงสร้างกุญแจสาธารณะ[21] (Public Key Infrastructure – PKI) ซึ่งเป็นระบบที่นิยมใช้กันในปัจจุบัน

---

[20] ดูรายละเอียด Model Law on Electronic Evidence 2002ที่ภาคผนวก ซ หน้า 125

[21] PKI เป็นเทคโนโลยีกุญแจสาธารณะ โดยใช้กุญแจคู่(ชุดตัวเลข-ฐาน16)คือ Public Key และPrivate Key ซึ่งสร้างโดย CPS (Cryptographic Service Provider) ในเครื่องคอมพิวเตอร์หรือ smart cardของผู้ใช้งาน หรือผู้ขอต้องส่ง Public Key ให้ CA หรือเรียกอีกชื่อหนึ่งว่า ผู้ออกใบรับรองอิเล็กทรอนิกส์

### 3.4.1 ที่มา วัตถุประสงค์และความหมายของลายมือชื่ออิเล็กทรอนิกส์

โดยปกติในชีวิตประจำวันผู้คนส่วนใหญ่มักต้องมีการลงนามในเอกสารต่าง ๆ เพื่อเป็นการยืนยันรับรองความถูกต้องแท้จริงของข้อมูลตั้งแต่ในอดีตจนถึงปัจจุบัน แต่ในยุคโลกาภิวัฒน์นี้ความก้าวหน้าทางเทคโนโลยีสารสนเทศทำให้นอกจากจะมีการลงลายมือชื่อโดยปกติทั่วไปในระบบกระดาษแล้วก็ยังมีการใช้ลายมือชื่ออิเล็กทรอนิกส์และลายมือชื่อดิจิตอลกันมากขึ้น แม้กฎหมายจะรับรองให้ข้อมูลอิเล็กทรอนิกส์มีผลทางกฎหมายเสมอกับเอกสารธรรมดา (โดยต้องพิสูจน์ความน่าเชื่อถือของข้อมูลอิเล็กทรอนิกส์ ซึ่งศาลจะชั่งน้ำหนักพยานหลักฐานตามพฤติการณ์แห่งกรณี) และในประมวลกฎหมายแพ่งและพาณิชย์ไม่ได้บัญญัติให้นิยามไว้โดยตรง แต่หากพิจารณาประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 9 วรรคสอง ก็จะพอพบว่า กฎหมายมิได้จำกัดเฉพาะการลงลายมือชื่อด้วยการเขียนเท่านั้นเพราะหากเป็นการพิมพ์ลายนิ้วมือ แกงได ตราประทับ หรือเครื่องหมายอื่นทำนองเช่นว่านั้น ที่ทำลงในเอกสารแทนลายมือชื่อ หากมีพยานลงลายมือรับรองไว้สองคนก็ให้ถือเสมือนลงลายมือชื่อ และหากทำลงในเอกสารต่อหน้าพนักงานเจ้าหน้าที่ ก็ไม่จำเป็นต้องมีพยานลงลายมือชื่อรับรองอีก จึงอาจกล่าวได้ว่ากฎหมายไม่ได้ต้องการการลงลายมือชื่อด้วยการเขียนเสมอไป หากเป็นการทำ “เครื่องหมายอื่นทำนองเช่นว่านั้น” ดังนั้นการลงลายมือชื่อจึงเป็นไปเพื่อวัตถุประสงค์อย่างน้อย 2 ประการเพื่อเป็นหลักฐานแสดงความแท้จริงของเอกสารและเพื่อเป็นหลักฐานแสดงการตกลงและตัดสินใจของผู้ลงชื่อนั่นเอง

#### 3.4.1.1 ลายมือชื่อดิจิทัล

ลายมือชื่อดิจิทัลมีวัตถุประสงค์เพื่อยืนยันข้อเท็จจริงทั้งสองประการดังกล่าวเช่นกัน ลายมือชื่อดิจิทัลไม่ใช่การลงลายมือชื่อในแบบที่เคยชินกันในชีวิตประจำวัน และไม่ใช่การลงลายมือชื่อลงในเอกสารแล้วส่งเอกสารนั้นไปทางอิเล็กทรอนิกส์ เช่น ลงชื่อใน e-mail แต่ลายมือชื่อดิจิทัล เป็นวิธีการรับรองตัวผู้ทำเอกสารและข้อความในเอกสาร โดยอาศัยหลักการในการเข้ารหัส (cryptography) ใช้โปรแกรมแปลงข้อมูลคอมพิวเตอร์เป็นข้อความเข้ารหัส โดยอาศัยกุญแจเข้ารหัส (KEY) ซึ่งเจ้าของเท่านั้นที่รู้เป็นตัวแปลง หากผู้อื่นไม่รู้รหัสดังกล่าวก็จะไม่สามารถอ่านข้อความนั้นได้ เมื่อจะอ่านข้อความก็ต้องใส่กุญแจรหัสกลับเข้าไป ก็จะได้ข้อความเดิมคืนกลับมา

---

เพื่อจะได้เป็นใบรับรองของผู้ใช้งานที่จะต้องเก็บไว้เพื่อใช้ในการลงนามโดยมีรหัสผ่านป้องกัน ส่วน Public Key เอาไว้ยืนยันตัวตนผู้ลงนามและแลกกับบุคคลอื่นเพื่อเข้ารหัสเอกสาร

**3.4.1.2 ลายมือชื่ออิเล็กทรอนิกส์**

ลายมือชื่ออิเล็กทรอนิกส์ ตามความหมายของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 หมายถึง อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์กับบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น[22] โดยในปัจจุบันผู้ที่ทำการติดต่อสื่อสารโดยใช้ข้อมูลอิเล็กทรอนิกส์อาจใช้ลายมือชื่ออิเล็กทรอนิกส์กำกับข้อมูลอิเล็กทรอนิกส์นั้นอีกด้วยเพื่อให้ข้อมูลอิเล็กทรอนิกส์ที่ส่งกันนั้นมีความปลอดภัยยิ่งขึ้น โดยจะเป็นหลักประกันว่าบุคคลที่ใช้ลายมือชื่ออิเล็กทรอนิกส์นั้นเป็นเจ้าของลายมือชื่อนั้นและเห็นชอบกับเนื้อหาสาระของข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อนั้นกำกับ ลักษณะหน้าที่ดังกล่าวนี้ของลายมือชื่ออิเล็กทรอนิกส์เป็นสาระสำคัญที่กฎหมายแม่แบบกำหนดไว้ใน Article 7[23] นั่นเอง กฎหมายของประเทศต่าง ๆ จึงมักกำหนดบทนิยามของ “ลายมือชื่ออิเล็กทรอนิกส์” ให้สอดคล้องกับสาระสำคัญของ Article 7 ของกฎหมายแม่แบบ เช่น Electronic Transactions Act 1998 ของประเทศสิงคโปร์ได้นิยามลายมือชื่ออิเล็กทรอนิกส์ว่าหมายถึง “อักษร อักขระ ตัวเลข หรือสัญลักษณ์อื่นที่อยู่ในรูปดิจิทัล ซึ่งนำมาประกอบกับหรือนำมาใช้ให้มีความสัมพันธ์เชิงตรรกะกับข้อมูลอิเล็กทรอนิกส์

---

[22] สุพิศ ประณีตพลกรัง, **ความรู้เบื้องต้นกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์** ,เนติบัณฑิตยสภา: น.48

[23] “Article 7 Signature

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

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

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

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

(3) The provisions of this article do not apply to the following : (…)

และสร้างขึ้นหรือรับมาใช้เพื่อพิสูจน์ความถูกต้องแท้จริงของข้อมูลอิเล็กทรอนิกส์และความเห็นชอบกับข้อมูลอิเล็กทรอนิกส์"[24]

วิธีการในการสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นมีหลายวิธีซึ่งแต่ละวิธีต้องสามารถระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อนั้นได้และต้องประกันได้ว่าผู้เป็นเจ้าของลายมือชื่อได้เห็นชอบกับเนื้อหาของข้อมูลอิเล็กทรอนิกส์ที่ได้ใช้ลายมือชื่ออิเล็กทรอนิกส์กำกับตัวอย่างของวิธีการ ที่อาจนำมาใช้ เช่น การใช้รหัสประจำตัว (PIN) การใช้ลายพิมพ์นิ้วมือแบบดิจิตอล การสแกนม่านตาของบุคคล หรือการแปลงสัญญาณเสียงพูดเป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งคอมพิวเตอร์จะนำเอาสิ่งเหล่านั้นมาประกอบกับข้อมูลอิเล็กทรอนิกส์ที่ประสงค์จะส่งไปยังคู่กรณีอีกฝ่ายหนึ่ง ขณะนี้หลาย ประเทศได้มีกฎหมายว่าด้วยลายมือชื่ออิเล็กทรอนิกส์เพื่อเสริม Article 7 ของกฎหมายแม่แบบของ UNCITRAL บางประเทศก็ได้ออกเป็นกฎหมายฉบับเดียวกับกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions) โดยมีหมวดที่ว่าด้วยลายมือชื่ออิเล็กทรอนิกส์เป็นการเฉพาะ บางประเทศก็แยกบัญญัติเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์เป็นกฎหมายอีกฉบับหนึ่งต่างหากจากกันแต่มีความสัมพันธ์กัน และในการบัญญัติรับรองผลทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์นั้น บางประเทศบัญญัติรับรองเฉพาะลายมือชื่อดิจิทัลเท่านั้น[25] จึงต้องพิเคราะห์กันว่าลายมือชื่อดิจิทัลมีลักษณะอย่างไรและแตกต่างกับลายมือชื่ออิเล็กทรอนิกส์ทั่วไปหรือไม่

คำว่า "ลายมือชื่ออิเล็กทรอนิกส์" นั้นเป็นคำที่มีความหมายกว้าง ซึ่งครอบคลุมถึงลายมือชื่อที่สร้างโดยวิธีการทางอิเล็กทรอนิกส์ทุกประเภท (การสแกนม่านตา การใช้รหัสประจำตัว การแปลงสัญญาณเสียงพูดเป็นข้อมูลอิเล็กทรอนิกส์ ฯลฯ) ส่วนคำว่า"ลายมือชื่อดิจิทัล" มีความหมายอย่างแคบ ซึ่งหมายถึงลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นโดยใช้เทคโนโลยีกุญแจคู่เท่านั้น ทั้งนี้โดยอาศัยระบบการเข้ารหัสแบบอสมมาตร (asymmetric cryptosystem หรือ asymmetric cryptography) ซึ่งจะได้กล่าวต่อไป

---

[24] Article 2: "In this Act, unless the context otherwise requires – "Electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with intention of authenticating or approving the electronic record."

[25] เช่น The Digital Signature Act ของมลรัฐยูท่าห์ ประเทศสหรัฐอเมริกา; The Digital Signature Act ของประเทศเกาหลีใต้; The Digital Signature Act ของประเทศมาเลเซีย; The Digital Signature Act ของประเทศเยอรมัน (ซึ่งปรากฏเป็น Article 3(อันประกอบด้วยบทบัญญัติ 16 มาตรา) ของ Information and Communication Services Act 1997

การใช้เทคโนโลยีกุญแจคู่นั้นมีการสร้างกุญแจคู่หนึ่ง (Key Pair) ซึ่งประกอบด้วยกุญแจส่วนตัว (Private key) และกุญแจสาธารณะ (Public Key) ซึ่งสร้างขึ้นโดยใช้ระบบคอมพิวเตอร์เพื่อให้กุญแจทั้งสองมีความสัมพันธ์เชิงคณิตศาสตร์ (Algorithm) ซึ่งกันและกันการที่ต้องให้ระบบคอมพิวเตอร์สร้างกุญแจที่มีความสัมพันธ์ทางคณิตศาสตร์ซึ่งกันและกันก็เพื่อให้ผู้ที่ประสงค์จะสร้างลายมือชื่ออิเล็กทรอนิกส์สามารถใช้กุญแจส่วนตัวในการสร้างลายมือชื่ออิเล็กทรอนิกส์และให้บุคคลทั่วไปสามารถใช้กุญแจสาธารณะในการตรวจพิสูจน์ว่าลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นนั้นเป็นลายมือชื่อที่แท้จริงหรือไม่และข้อมูลอิเล็กทรอนิกส์ที่มีการใช้ลายมือชื่ออิเล็กทรอนิกส์กำกับนั้นเป็นข้อมูลที่ถูกเปลี่ยนแปลงแก้ไขหลังจากที่มีการสร้างลายมือชื่อหรือไม่ การที่สามารถตรวจพิสูจน์เช่นว่านั้นได้ก็เป็นเพราะความสัมพันธ์เชิงคณิตศาสตร์ระหว่างกุญแจทั้งสองนั่นเอง ผู้ที่จะสร้างลายมือชื่ออิเล็กทรอนิกส์เพื่อกำกับข้อมูลอิเล็กทรอนิกส์ใดก็จะนำเอาข้อมูลอิเล็กทรอนิกส์นั้นมาเข้ารหัส (encryption) โดยใช้กุญแจส่วนตัวซึ่งไม่มีผู้ใดทราบนอกจากผู้เป็นเจ้าของกุญแจส่วนตัวเอง[26]

ข้อมูลอิเล็กทรอนิกส์ที่เข้าถูกรหัสแล้วจะเรียกว่า ciphertext ส่วนนี้เองที่เป็นลายมือชื่ออิเล็กทรอนิกส์และเป็นส่วนที่นำไปใช้กำกับข้อมูลอิเล็กทรอนิกส์เดิม[27] เมื่อมีการส่งข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่ออิเล็กทรอนิกส์นั้นกำกับอยู่ไปยังผู้รับ ผู้รับก็สามารถใช้กุญแจสาธารณะที่เจ้าของลายมือชื่อเผยแพร่ให้บุคคลทั่วไปทราบนั้นมาตรวจสอบลายมือชื่อดังกล่าว กุญแจสาธารณะจะถอดรหัส (decryption) ของข้อมูลที่ได้เข้ารหัสไว้ด้วยกุญแจส่วนตัว เนื่องจากกุญแจสาธารณะมีความสัมพันธ์ทางคณิตศาสตร์กับกุญแจส่วนตัว ดังนั้นข้อมูลอิเล็กทรอนิกส์ที่ได้รับหลังจากการถอดรหัสด้วยกุญแจสาธารณะจึงต้องตรงกัน และดังที่ได้กล่าวมาแล้วข้อมูลอิเล็กทรอนิกส์ที่นำมาเข้ารหัสด้วยกุญแจส่วนตัวเพื่อเป็นลายมือชื่ออิเล็กทรอนิกส์นั้นก็คือข้อมูล

---

[26] อันที่จริงแล้ว ก่อนที่จะนำข้อมูลอิเล็กทรอนิกส์นั้นมาเข้ารหัสด้วยกุญแจส่วนตัวก็อาจมีการนำข้อมูลนั้นมา ผ่านกระบวนการย่อยข้อมูลอีกด้วย ซึ่งมักจะทำให้ข้อมูลนั้นมีขนาดเล็กลง กระบวนการนี้เรียกว่า Hash Function กฎหมายของบางประเทศกำหนดให้มีการใช้ Hash Function อีกด้วย เช่น Electronic Transaction Act 1998 ของประเทศสิงคโปร์ และ Digital Signature Act 1997

[27] ลายมือชื่ออิเล็กทรอนิกส์มีลักษณะดังตัวอย่างข้างล่างนี้

82:03:9f:35:5a:f6:d5:d6:70:04:74:55:22:f5:d2:42:6f:7e:87:b9:3b:
59:33:68:19:21:85:ab:cb:a2:77:8e:97:f0:2e:52:28:8a:ed:fe:30:91:
52:11:9f:4b:1e:10:d5:96:2e:9f:17:48:3b:62:6b:b6:53:31:3b:a1:e6:
f5:a3:fa:80:bf:01:5c:42:4a:de:bf:b3:12:2f:8b:c0:63:80:13:89:54:
ae:52:b8:0b:f4:86:5d:09:43:bd:39:35:63:60:35:7e:c3:83:20:26:1e:
ac:af:6c:da:98:69:13:31:ba:7b:01:f9:59:57:71:27:1b:59:8a:16:1c:
09:24

เดิมที่ประสงค์จะนำลายมือชื่ออิเล็กทรอนิกส์นั้นไปกำกับอยู่นั่นเอง ด้วยเหตุนี้หากมีการเปลี่ยนแปลงเนื้อหาสาระของข้อมูลอิเล็กทรอนิกส์นี้หลังจากที่ได้ส่งข้อมูลนี้ไปแล้ว เมื่อนำกุญแจสาธารณะมาถอดรหัสกลับเป็นข้อมูลหรือข้อความเดิม ก็จะได้ข้อมูลหรือข้อความที่ไม่เหมือนกัน จึงสามารถทราบได้ว่าข้อมูลอิเล็กทรอนิกส์มีการเปลี่ยนแปลงแก้ไขจากเดิม เทคโนโลยีที่มีการใช้กุญแจสาธารณะตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ที่สร้างโดยอาศัยการนำกุญแจส่วนตัวมาเข้ารหัสนั้นเรียกว่า “เทคโนโลยีกุญแจสาธารณะ” หรือ Public Key Infrastructure หรือเรียกย่อว่า เทคโนโลยี PKI (บางครั้งก็เรียกกันว่า Public Key Cryptography หรือ PKC) และลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นโดยเทคโนโลยีนี้จะเรียกกันว่า “ลายมือชื่อดิจิทัล”

### 3.4.2 หลักการทำงานของเทคโนโลยีลายมือชื่ออิเล็กทรอนิกส์

1.กุญแจรหัสแบบ symmetric cryptography

ในการส่งข้อมูลผ่านระบบอินเตอร์เน็ตนั้นอาจมีผู้ดักข้อความดังกล่าวและสามารถใช้โปรแกรมโดยเฉพาะสามารถถอดข้อความดังกล่าวได้เช่นกัน แม้ว่าจะทำได้ยากและต้องเป็นผู้เชี่ยวชาญก็ตาม เพราะวิธีนี้มีจุดอ่อนที่จะต้องส่งกุญแจไปพร้อมกันกับข้อความ และหากถอดรหัสกุญแจได้ ก็จะสามารถอ่านข้อความทั้งหมดได้ วิธีการเข้ารหัสโดยกุญแจเดี่ยวนี้เรียกว่า “conventional single key” หรือ “symmetric cryptography” วิธีนี้มีจุดอ่อนที่ไม่มีความปลอดภัยเพียงพอ เพราะไม่สามารถยืนยันตัวผู้ทำเอกสารได้ ใครก็ตามที่สามารถถอดรหัสได้ ก็สามารถอ่านข้อความและเขียนข้อความนั้นได้ใหม่ และสามารถยืนยันข้อความในเอกสารว่าถูกต้องหรือไม่ถูกต้องได้อีกด้วย

2.กุญแจรหัสแบบ asymmetric cryptosystem

เพื่อแก้ปัญหาดังกล่าว จึงมีการพัฒนาระบบเข้ารหัสแบบ asymmetric cryptosystem หรือมักนิยมเรียกว่าแบบ public key system ในระบบนี้จะมีกุญแจรหัส 2 ตัว ตัวแรกเรียกว่า private key หรือกุญแจลับ อีกตัวหนึ่งรียกว่า public key หรือกุญแจเปิดเผย ซึ่งโดยหลักการแล้วจะมีเพียงเจ้าของลายมือชื่อดิจิทัลเท่านั้นที่ทราบ ใช้ในการเข้ารหัสข้อความและอยู่ในความรับผิดชอบของเจ้าของที่จะไม่ให้ตกไปถึงมือผู้อื่น ส่วนpublic key เป็นกุญแจ

---

(ที่มา: **หนังสือเผยแพร่ร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. ...** ของสำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยี อิเล็กทรอนิกส์ และคอมพิวเตอร์แห่งชาติ, 2543)

เปิดเผยของเจ้าของลายมือชื่อดิจิทัล มีอยู่ในที่สาธารณะ ซึ่งผู้รับเอกสารสามารถหาพบได้เอง เช่น จาก web site ที่ให้บริการในเรื่องนี้ซึ่งผู้ลงลายมือชื่อดิจิทัลลงทะเบียนไว้เป็นต้น ใช้ในการถอดรหัสข้อความ และกุญแจทั้งสองนี้มีความสัมพันธ์กันในทางคณิตศาสตร์กล่าวคือ เมื่อใช้ private key เข้ารหัสแล้ว จะต้องใช้ public key เท่านั้นในการถอดรหัสหรือกลับกันไม่สามารถใช้กุญแจรหัสเดิมทั้งเข้าและถอดรหัสได้ วิธีการเข้ารหัสแบบนี้ ผู้ลงลายมือชื่อดิจิทัลจะกำหนดขอบเขตข้อมูลที่จะเข้ารหัส เรียกว่ากำหนด message แล้วใช้โปรแกรมเฉพาะซึ่งมี hash function ซึ่งจะทำการคำนวณข้อความใน message ย้อนกลับไปมาหลายครั้งแล้วแปลง message นั้นให้เป็นผลลัพธ์ทางคณิตศาสตร์ เรียกว่า hash result ซึ่งจะมีลักษณะเป็นผลการคำนวณซึ่งสัมพันธ์กับข้อความใน message นั้น หลังจากนั้นใช้ private key ของตนในการเข้ารหัส hash result เป็นลายมือชื่อดิจิทัล แล้วส่งไปยังผู้รับปลายทางพร้อมกับเอกสารส่วนผู้รับปลายทางมีหน้าที่ คือคำนวณหา hash result ของเอกสารที่ส่งมาก่อนตามขอบเขต message ที่กำหนด เพื่อหาผลลัพธ์ หลังจากนั้นจะใช้ public key ของผู้ลงลายมือชื่อดิจิทัล ถอดรหัสข้อมูลลายมือชื่อดิจิทัล หากถอดรหัสได้ และได้ผลลัพธ์ hash result ตรงกับเอกสารที่ส่งมา ก็จะยืนยันข้อเท็จจริง 2 ประการ คือ **ประการแรก** เอกสารนั้นผู้ลงลายมือชื่อดิจิทัลเป็นคนส่งมา (หรือโดยผู้ที่เป็นเจ้าของ private key ยินยอมให้ใช้ได้) เพราะสามารถใช้ public key ถอดออกมาได้ **ประการที่สอง** ข้อความในเอกสารนั้นถูกต้อง ไม่มีการดัดแปลงแก้ไขหรือต่อเติมในระหว่างทางที่ส่งมาเพราะ hash result ที่ถอดรหัสออกมาได้ ได้ผลการคำนวณตรงกับเอกสาร ซึ่งหากมีการแต่งเติมเพียงครั้งเดียว จะมีผลให้การคำนวณนั้นได้ผลลัพธ์ผิดไปจากเดิมอย่างมาก เพราะ hash function จะต้องคำนวณย้อนกลับไปกลับมาหลายครั้ง จึงไม่มีทางที่จะเปลี่ยนแปลงข้อความแล้วทำให้ได้ผลการคำนวณเดิมอีก ด้วยวิธีนี้การส่งเอกสารจึงมีความปลอดภัยเพราะผู้ส่งและผู้รับเอกสารไม่จำเป็นต้องรู้รหัสลับของกันและกัน ถึงแม้หากมีผู้ดักเอกสารได้ระหว่างทาง ก็จะไม่มีกุญแจรหัสส่งไปพร้อมกับเอกสาร และแม้จะทราบว่าเป็นเอกสารของผู้ใด ก็ไม่สามารถแต่งเติมข้อความในเอกสารได้ เพราะไม่มีทางจะทำให้ hash result มีผลลัพธ์เช่นเดิม วิธีการลงลายมือชื่อดิจิทัลเช่นนี้จึงได้รับการยอมรับว่ามีความปลอดภัยเพียงพอการลงลายมือชื่อดิจิทัล แม้จะไม่มีการเขียนลายมือชื่อลงบนกระดาษเป็นหลักฐานเหมือกับการลงลายมือชื่อปกติก็ตาม แต่ก็เห็นได้ว่า ลายมือชื่อดิจิทัลมีวัตถุประสงค์เช่นเดียวกับการลงลายมือชื่อปกติ ส่วนวิธีการลงลายมือชื่อดิจิทัลนั้นเป็นวิธีการที่อาศัยเทคโนโลยีสมัยใหม่ที่เปลี่ยนแปลงไป[28]

---

[28] อาทิตย์ ออกเวหา, **Digital signatures เป็นการลงลายมือชื่อตามกฎหมายหรือไม่**, ดุลพาห, เล่ม 2 ปีที่47, พฤษภาคม-สิงหาคม 2543 : น.29-31

### 3.4.3 การรับรองลายมือชื่ออิเล็กทรอนิกส์ [29]

การใช้กุญแจสาธารณะเพื่อตรวจสอบความถูกต้องแท้จริงของลายมือชื่อดิจิทัลจะไม่เป็นที่น่าเชื่อถือแก่บุคคลทั่วไปถ้าหากไม่มีการรับรองโดยบุคคลที่สามที่น่าเชื่อถือได้ (Trusted Third Party) ทั้งนี้ถ้าไม่มีบุคคลที่สามเป็นผู้รับรองความถูกต้องของกระบวนการสร้างกุญแจคู่แล้ว ก็เท่ากับว่าผู้ที่ประสงค์จะใช้ลายมือชื่อดิจิทัลเป็นผู้รับรองตนเอง บุคคลที่สามที่น่าเชื่อถือได้ที่ทำหน้าที่ในการรับรองเกี่ยวกับลายมือชื่อดิจิทัลนั้นจะเรียกกันว่า Certification Authority หรือ CA (ซึ่งในที่นี้จะเรียกว่า “ผู้ประกอบการรับรอง”) ในการรับรอง ผู้ประกอบการรับรองจะออกใบรับรองให้ผู้ขอ

ในหลายประเทศกำหนดให้ผู้ประกอบการรับรองต้องได้รับอนุญาตให้ประกอบการโดยหน่วยงานของรัฐจะเป็นผู้ออกใบอนุญาต ซึ่งโดยปกติแล้วผู้ประกอบการรับรองจะต้องอยู่ภายใต้การกำกับดูแลของรัฐ โดยรัฐอาจกำหนดหลักเกณฑ์ต่างๆให้ผู้ประกอบการรับรองปฏิบัติ เช่นหลักเกณฑ์เกี่ยวกับวิธีการที่นำมาใช้สร้างกุญแจส่วนตัวและกุญแจสาธารณะโดยต้องเป็นวิธีการที่มีความปลอดภัยเหมาะสมกับความก้าวหน้าทางเทคโนโลยีและสภาพทางธุรกิจ หรือหลักเกณฑ์ว่าด้วยการจัดทำข้อปฏิบัติเกี่ยวกับการประกอบการรับรอง (ที่เรียกกันว่า Certification Pracetice Statements หรือ CPS) ในขณะที่บางประเทศก็มิได้ควบคุมการประกอบการรับรองเกี่ยวกับลายมือชื่อดิจิทัลและถือว่าเป็นเรื่องที่ต้องปล่อยให้เป็นไปตามกลไกลของตลาดสิ่งสำคัญประการแรกที่ผู้ประกอบการรับรองต้องกระทำเพื่อให้ลายมือชื่อดิจิทัลของผู้ขอใบรับรองมีความน่าเชื่อถือก็คือการพิสูจน์ตัวบุคคลของผู้ขอใบรับรอง (ซึ่งมักเรียกกันว่า Subscriber) ในการนี้ผู้ประกอบการรับรองต้องตรวจสอบให้เป็นที่แน่ชัดว่าบุคคลนั้นมีตัวตนจริงและไม่ได้นำชื่อของบุคคลอื่นไปแอบอ้างใช้โดยไม่ได้รับอนุญาต เมื่อตรวจสอบตัวบุคคลแล้วก็ต้องตรวจสอบความปลอดภัยและความถูกต้องของกุญแจส่วนตัวและกุญแจสาธารณะ ทั้งนี้ต้องแน่ใจว่าผู้ที่จะได้รับใบรับรองต้องใช้วิธีการที่น่าเชื่อถือได้ในการสร้างกุญแจคู่ ผู้ประกอบการรับรองบางรายก็กำหนดให้ต้องใช้โปรแกรมคอมพิวเตอร์ของผู้ประกอบการรับรองในการสร้างกุญแจคู่และในการเข้ารหัสข้อมูล แต่ผู้ประกอบการรับรองบางรายก็อาจเปิดโอกาสให้ผู้ขอใบรับรองใช้โปรแกรมของผู้ขอใบรับรองได้ โดยอาจวางข้อกำหนดว่าโปรแกรมนั้นต้องมีลักษณะทางเทคนิคบางประการ (กฎหมายของบางประเทศอาจกำหนดให้ต้องใช้วิธีการหรือเทคโนโลยีที่รัฐกำหนดโดยอาจออกข้อบังคับหรือกฎหมายลำดับรองมากำหนดรายละเอียดอีกทีหนึ่ง)

---

[29] พินัย ณ นคร, **กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์**, บทบัณฑิตย์ เล่ม 56 ตอน 2 พ.ศ. 2543 : น. 27-31

เมื่อออกใบรับรองให้แก่ผู้ขอใบรับรอง ผู้ประกอบการรับรองจะระบุรายละเอียดดังต่อไปนี้ไว้ในใบรับรอง กล่าวคือ ข้อเท็จจริงเกี่ยวกับตัวบุคคลของผู้ได้รับการรับรอง วิธีการทางเทคนิคที่ใช้ในการสร้างกุญแจคู่หรือมาตรฐานที่นำมาใช้ในการเข้ารหัส และกุญแจสาธารณะของผู้ถือใบรับรอง นอกจากข้อเท็จจริงเกี่ยวกับผู้ถือใบรับรองแล้ว ใบรับรองยังระบุรายละเอียดเกี่ยวกับผู้ประกอบการรับรองอีกด้วย ซึ่งนอกจากระบุชื่อและสถานที่ทำการของผู้ประกอบการรับรองและยังต้องระบุกุญแจสาธารณะและลายมือชื่อดิจิทัลของตนเองอีกด้วย เพราะผู้ประกอบการรับรองต้องลงลายมือชื่อดิจิทัลในใบรับรองที่ออกให้แก่ผู้ขอใบรับรองจากตนด้วย การใช้ลายมือชื่ออิเล็กทรอนิกส์ทั่ว ๆไป (กล่าวคือ ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างขึ้นโดยใช้วิธีการที่สามารถระบุตัวบุคคลผู้สร้างลายมือชื่อได้และสามารถแสดงได้ว่าบุคคลนั้นเห็นชอบกับเนื้อหาสาระของข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อนั้นกำกับอยู่นั้น) ก็ได้รับการรับรองให้มีผลทางกฎหมายเช่นเดียวกับลายมือชื่อธรรมดาที่ลงกันในเอกสารอยู่แล้ว ส่วนความถูกต้องแท้จริงกันนั้นเป็นเรื่องที่ต้องพิสูจน์กันในภายหลัง ซึ่งจะต้องมีการสืบพยานและศาลจะเป็นผู้ชั่งน้ำหนักพยานเอง อย่างไรก็ตามถ้าหากได้มีการใช้ลายมือชื่ออิเล็กทรอนิกส์ที่อยู่ในรูปของลายมือชื่อดิจิทัลกฎหมายของหลายประเทศมักจะรับรองผลมากกว่าลายมือชื่ออิเล็กทรอนิกส์ทั่ว ๆไป โดยจะถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย ซึ่งจะได้รับประโยชน์ในแง่ข้อสันนิษฐานทางกฎหมายดังจะกล่าวต่อไป

ในกฎหมายต่างประเทศนั้น คำว่า “ลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย” (Secure electronic signature) จะหมายถึงลายมือชื่อที่สร้างขึ้นโดยวิธีการที่มีลักษณะเฉพาะตัวของบุคคลผู้สร้างลายมือชื่อ (Unique to that person) และวิธีการดังกล่าวจะอยู่ภายใต้การควบคุมของบุคคลนั้นโดยเฉพาะ (Under the sole control of that person) เมื่อวิธีการที่นำมาใช้นั้นมีลักษณะเฉพาะของบุคคลที่ประสงค์จะสร้างลายมือชื่อและเป็นวิธีการที่ไม่มีผู้ใดนอกจากบุคคลนั้นเองควบคุมการสร้างลายมือชื่อนั้นก็ย่อมเป็นที่แน่ชัดว่าลายมือชื่อนั้นเป็นของบุคคลนั้น กฎหมายจึงสร้างข้อสันนิษฐานว่าลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัยเป็นของบุคคลนั้น และข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อแบบปลอดภัยดังกล่าวกำกับอยู่นั้นได้รับความเห็นชอบโดยบุคคลนั้น (กล่าวคือ มิได้มีการเปลี่ยนแปลงแก้ไขเลย) ผลของข้อสันนิษฐานดังกล่าวทำให้ผู้ที่ยืนยันในความถูกต้องแท้จริงของลายมือชื่อนั้นและของข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อนั้นกำกับอยู่ไม่ต้องมีหน้าที่พิสูจน์ แต่บุคคลที่จะโต้แย้งว่าลายมือชื่อหรือข้อมูลนั้นไม่ถูกต้องมีหน้าที่ต้องพิสูจน์ ซึ่งกรณีที่มีการโต้แย้งนั้นอาจมีทั้งกรณีที่บุคคลที่ถูกสันนิษฐานว่าเป็นเจ้าของลายมือชื่อโต้แย้งว่าตนมิได้สร้างลายมือชื่อนั้นหรือโต้แย้งว่าข้อมูลอิเล็กทรอนิกส์ที่ตนใช้ลายมือชื่อกำกับนั้นถูกเปลี่ยนแปลงแก้ไขและกรณีที่บุคคลอื่นซึ่งไม่ประสงค์จะถูกผูกพันโดยนิติกรรมโต้แย้งเพื่อให้หลุดพ้นจากความรับผิดที่มิฉะนั้นแล้วตนจะมีต่อผู้ที่ได้รับการสันนิษฐานว่าเป็นเจ้าของลายมือชื่อทั้งหมดหรือบางส่วนในการกำหนดข้อสันนิษฐานเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์

แบบปลอดภัยนั้น กฎหมายแต่ละประเทศอาจวางข้อกำหนดไว้ต่างกันบ้าง ซึ่งก็เป็นข้อกำหนดเกี่ยวกับวิธีการเพื่อความปลอดภัย (Security Procedure) ที่นำมาใช้ บางประเทศกำหนดว่าวิธีการเพื่อความปลอดภัยจะต้องเป็นวิธีการที่กฎหมายกำหนดหรือที่มีความเหมาะสมในทางธุรกิจตามที่คู่กรณีตกลงกัน (ซึ่งอาจกำหนดหลักเกณฑ์ในการพิเคราะห์ความเหมาะสมในทางธุรกิจไว้ด้วยว่า ให้คำนึงถึงวัตถุประสงค์ของวิธีการรักษาความปลอดภัยที่นำมาใช้ ตลอดจนพฤติการณ์ทางธุรกิจ ซึ่งรวมถึงพฤติการณ์ดังต่อไปนี้ คือ ลักษณะของธุรกรรม ลักษณะและสภาพของคู่กรณี จำนวนของธุรกรรมทำนองเดียวกันวิธีการอื่นที่ใช้รักษาความปลอดภัยมีอยู่หรือไม่และจำนวนค่าใช้จ่ายหากนำวิธีการอื่นมาใช้ตลอดจนวิธีการรักษาความปลอดภัยที่ใช้ในธุรกรรมทำนองเดียวกัน) บางประเทศก็กำหนดถึงขนาดที่ว่าวิธีการรักษาความปลอดภัยต้องเป็นวิธีการที่ได้รับการรับรองจากเจ้าหน้าที่หรือองค์กรของรัฐเท่านั้น

สำหรับลายมือชื่อดิจิทัลนั้น โดยเหตุที่ลายมือชื่อดิจิทัลเป็นลายมือชื่อที่สร้างขึ้นโดยใช้เทคโนโลยีแบบ PKI ซึ่งได้รับการยอมรับกันเป็นการสากลว่าเป็นเทคโนโลยีที่มีความปลอดภัยสูง ดังนั้นกฎหมายจึงถือว่าลายมือชื่อดิจิทัลเป็นลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัย ซึ่งเมื่อถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัยแล้วก็จะทำให้ข้อสันนิษฐานเกี่ยวกับความถูกต้องแท้จริงใช้บังคับทันที อย่างไรก็ตามโดยทั่วไปแล้วกฎหมายของประเทศต่าง ๆได้กำหนดให้ลายมือชื่อดิจิทัลได้รับประโยชน์จากข้อสันนิษฐานเช่นว่านั้นก็เฉพาะเมื่อได้รับการรับรองโดยผู้ประกอบการรับรองเท่านั้น ซึ่งส่วนใหญ่จะกำหนดด้วยว่าต้องได้รับการรับรองโดยผู้ประกอบการรับรองที่ได้รับอนุญาตเท่านั้น (Licensed certification authority) และกฎหมายอาจให้อำนาจรับรองรัฐมนตรีออกระเบียบกำหนดหลักเกณฑ์เพิ่มเติมด้วยว่าลายมือชื่อดิจิทัลที่จะถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์แบบปลอดภัยต้องมีลักษณะใดบ้าง

### 3.4.4 ความเชื่อถือในลายมือชื่อดิจิทัลและหน้าที่และความรับผิดชอบของบุคคลที่เกี่ยวข้อง[30]

#### 3.4.4.1 เหตุแห่งความเชื่อถือ

การสร้างระบบรับรอง (Certification) เกี่ยวกับลายมือชื่อดิจิตอลก็เพื่อให้ผู้ที่ทำการติดต่อกับผู้ที่ได้รับการระบุชื่อในใบรับรองว่าเป็นเจ้าของลายมือชื่อนั้นมีความมั่นใจในความถูกต้องแท้จริงของลายมือชื่อนั้นและของข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อนั้นกำกับ การที่

---

[30] เนื้อหาส่วนใหญ่สรุปจาก Wacharapong Yawai, **การสร้างใบรับรองอิเล็กทรอนิกส์** (e-Certificate) การประยุกต์ใช้งานการเข้ารหัส(Encryption) และลายมือชื่ออิเล็กทรอนิกส์ (e-Singature),เอกสารประกอบการสอน

จะเชื่อถือในความถูกต้องแท้จริงของสิ่งดังกล่าวได้ บุคคลที่เข้าติดต่อก็ต้องเชื่อถือในรายการต่างๆที่ระบุไว้ในใบรับรอง โดยจะเชื่อถือว่าผู้ประกอบการรับรองได้ตรวจสอบรายการเหล่านั้นมาอย่างถูกต้องแล้ว โดยเฉพาะอย่างยิ่ง การตรวจสอบตัวบุคคลและกุญแจคู่ของผู้ถือใบรับรอง

**3.4.4.2 หน้าที่ของผู้ประกอบการรับรองและผู้ขอหรือผู้ถือใบรับรองเพื่อเป็น หลักประกันว่าข้อมูลที่ระบุในใบรับรองจะเป็นข้อมูลที่ถูกต้อง**

กฎหมายว่าด้วยลายมือชื่อดิจิทัลของประเทศต่างๆ จึงมักกำหนดหน้าที่สำคัญๆของผู้ประกอบการรับรองและผู้ขอหรือผู้ถือใบรับรองไว้ โดยในส่วนของผู้ประกอบการรับรองนั้น กฎหมายกำหนดให้ใช้ระบบที่น่าเชื่อถือได้ (Trustworthy system) ในการประกอบการรับรองและตรวจสอบข้อเท็จจริงเกี่ยวกับผู้ขอใบรับรอง (ทั้งข้อเท็จจริงเกี่ยวกับตัวบุคคลของผู้ใบรับรอง ข้อเท็จจริงเกี่ยวกับกุญแจของผู้ขอใบรับรอง และข้อเท็จจริงอื่นๆ) นอกจากนี้ ในกรณีที่มีการระงับหรือเพิกถอนใบรับรองที่ผู้ประกอบการรับรองออกให้แก่บุคคลใดไปแล้วนั้น หรือมีข้อเท็จจริงอันเป็นสาระสำคัญที่มีผลกระทบต่อความน่าเชื่อถือของใบรับรอง (เช่น มีการปลอมแปลงกุญแจส่วนตัว หรือมีการเปลี่ยนแปลงรายการในใบรับรองโดยไม่ได้รับอนุญาตจากผู้ประกอบการรับรอง) ผู้ประกอบการรับรองก็ต้องแจ้งให้สาธารณชนทราบด้วย โดยต้องมีระบบการแจ้ง (repository) ที่มีประสิทธิภาพและทันการณ์ นอกจากนั้นหากตนทราบว่าเหตุเช่นนั้นจะมีผลกระทบต่อบุคคลใดเป็นการเฉพาะก็ต้องแจ้งให้บุคคลนั้นทราบด้วย ซึ่งโดยปกติแล้วผู้ประกอบการรับรองมักจะมีข้อปฏิบัติในการประกอบการรับรอง (CPS) เกี่ยวกับเรื่องเหล่านี้อยู่แล้ว ส่วนผู้ขอหรือผู้ถือใบรับรองนั้นนอกจากต้องใช้วิธีการที่น่าเชื่อถือในการสร้างกุญแจส่วนตัว กฎหมายยังกำหนดให้ต้องใช้ความระมัดระวังในการรักษากุญแจส่วนตัวและไม่เปิดเผยกุญแจ ส่วนตัวให้ผู้ซึ่งมิได้รับอนุญาตทราบ ตลอดจนหน้าที่ที่จะต้องแจ้งให้ผู้ที่เกี่ยวข้องหรือผู้ที่อาจได้รับความเสียหายทราบในกรณีรู้หรือสงสัยว่ามีการปลอมแปลงเกิดขึ้น

**3.4.5 คำรับรองตามกฎหมาย (Representations)**

นอกจากกฎหมายจะกำหนดหน้าที่ที่ผู้ประกอบการรับรองและผู้ขอหรือผู้ถือใบรับรองต้องปฏิบัติแล้ว กฎหมายมักจะมีระบบ “คำรับรอง” (Representations) ทั้งในส่วนของผู้ประกอบการรับรองและผู้ขอหรือผู้ถือใบรับรอง การให้คำรับรองข้อเท็จจริงต่างๆ ทำให้บุคคลทั่วไปเชื่อถือในความถูกต้องแท้จริงของลายมือชื่อดิจิทัลและของข้อมูลอิเล็กทรอนิกส์ที่มีการใช้ลายมือชื่อดิจิทัลกำกับ สำหรับผู้ประกอบการรับรองนั้นกฎหมายมักกำหนดว่าการที่ผู้ประกอบการรับรองออกใบรับรองให้ผู้ใดถือว่าผู้ประกอบการรับรองได้ให้คำรับรองว่าผู้นั้นได้ยอมรับ (accept) ใบรับรองแล้วและได้ถือกุญแจส่วนตัวโดยชอบซึ่งสามารถใช้กุญแจสาธารณะตรวจสอบความถูกต้องแท้จริงของลายมือชื่อดิจิทัลและของข้อมูลอิเล็กทรอนิกส์ได้ นอกจากนี้กฎหมายยังถือว่าผู้ประกอบการรับรองได้รับรองว่าข้อมูลที่ระบุในใบรับรองเป็นข้อมูลที่ถูกต้อง

โดยผู้ประกอบการรับรองมิได้รู้ถึงข้อเท็จจริงอันเป็นสาระสำคัญซึ่งอาจมีผลกระทบต่อความน่าเชื่อถือของใบรับรอง ในด้านผู้ขอหรือผู้ถือใบรับรองนั้น กฎหมายถือว่าผู้ขอหรือผู้ถือใบรับรองได้รับรองว่าข้อมูลอันเป็นสาระสำคัญที่ได้ให้ไว้แก่ผู้ประกอบการรับรองเป็นจริงและตนเป็นผู้ถือกุญแจส่วนตัวโดยชอบ

แม้กฎหมายจะกำหนดหน้าที่ให้ทั้งผู้ประกอบการรับรองและผู้ขอหรือผู้ถือใบรับรองปฏิบัติเพื่อให้ใบรับรองมีความน่าเชื่อถือและเพื่อให้บุคคลทั่วไปเชื่อมั่นว่าข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อดิจิตอลกำกับนั้นเป็นข้อมูลอิเล็กทรอนิกส์ที่ถูกต้อง แต่กฎหมายก็ไม่ประสงค์ให้ผู้ที่เชื่อถือในความถูกต้องแท้จริงนั้นเชื่อถือโดยปราศจากเหตุผลอันสมควร ดังนั้นหากมีพฤติการณ์ที่เห็นได้ว่าบุคคลไม่ควรเชื่อถือว่าใบรับรองหรือข้อมูลอิเล็กทรอนิกส์ที่มีลายมือชื่อดิจิตอลกำกับนั้นถูกต้องแท้จริง บุคคลที่ดำเนินการใดไปโดยเชื่อถือในใบรับรองหรือในข้อมูลอิเล็กทรอนิกส์นั้นก็ไม่อาจเรียกร้องค่าเสียหายอันเกิดจากความเชื่อถืออันไม่สมเหตุสมผลนั้น พฤติการณ์ที่แสดงว่าบุคคลไม่ควรจะเชื่อถือในความถูกต้องแท้จริงนั้นต้องพิเคราะห์กันเป็นกรณีๆไป โดยปกติแล้วต้องคำนึงถึงสิ่งดังต่อไปนี้ด้วย คือ ต้องพิเคราะห์ว่าบุคคลที่เชื่อถือในใบรับรองหรือในข้อมูลอิเล็กทรอนิกส์ได้รู้ถึงข้อเท็จจริงในใบรับรองหรือไม่ มูลค่าหรือความสำคัญของข้อมูลอิเล็กทรอนิกส์ที่มีการใช้ลายมือชื่อดิจิทัลปฏิบัติระหว่างคู่กรณี และทางปฏิบัติทางการค้า เป็นต้น

### 3.4.6 ความรับผิดของผู้ประกอบการรับรองและผู้ขอหรือผู้ถือลายมือชื่อ

การที่กฎหมายกำหนดหน้าที่ของผู้ประกอบการรับรองและของผู้ขอหรือผู้ถือใบรับรองมีผลให้บุคคลดังกล่าวต้องรับผิดต่อผู้ที่ได้รับความเสียหายจากการกระทำผิดหน้าที่ที่กฎหมายกำหนดนั่นเอง เช่น ในกรณีที่ผู้ขอใบรับรองใช้ชื่อปลอมในการขอใบรับรองและผู้ประกอบการรับรองมิได้ใช้ความระมัดระวังอันสมควรในการตรวจสอบตัวบุคคล (Identity) ของผู้ขอใบรับรองจึงออกใบรับรองให้แก่ผู้ขอใบรับรองที่ใช้ชื่อปลอมนั้น ในกรณีดังว่านี้ผู้ประกอบการรับรองจะต้องรับผิดต่อผู้ที่เชื่อถือในใบรับรองนั้น (เว้นแต่จะมีพฤติการณ์ที่แสดงว่าไม่สมควรจะเชื่อถือ ดังกล่าวข้างต้น) ในทำนองเดียวกัน การที่กฎหมายกำหนดคำรับรอง (Representations) ของผู้ประกอบการรับรองและของผู้ถือใบรับรองไว้ก็มีผลให้บุคคลดังกล่าวต้องรับผิดต่อผู้ที่ได้รับความเสียหายจากการที่ข้อเท็จจริงที่ได้ให้คำรับรองนั้นเป็นเท็จ อย่างไรก็ตาม บางประเทศยอมให้ผู้ประกอบการรับรองจำกัดความรับผิดได้ โดยต้องระบุระดับของความรับผิดไว้ในใบรับรอง ซึ่งเมื่อบุคคลทั่วไปได้เห็นระดับของความรับผิดที่ระบุไว้ในใบรับรองแล้วก็จะสามารถตัดสินใจได้ว่าตนควรจะให้ความเชื่อถือในใบรับรองหรือในข้อมูลอิเล็กทรอนิกส์

### 3.4.7 ความจำเป็นในการรับรองลายมือชื่ออิเล็กทรอนิกส์ และระบบความปลอดภัยของธุรกรรมพาณิชย์อิเล็กทรอนิกส์

#### 3.4.7.1 ความจำเป็นในการรับรองลายมือชื่ออิเล็กทรอนิกส์

โดยการรับรองในรับรองดิจิทัลซึ่งแบ่งออกเป็น 3 ประเภท คือ ใบรับรองเครื่องแม่ข่าย ใบรับรองตัวบุคคล ใบรับรองสำหรับองค์กรรับรองความถูกต้อง โดยเฉพาะในภาครัฐเองในขณะนี้ก็มีนโยบายที่จะให้ประชาชนสามารถติดต่อหรือทำธุรกรรมกับหน่วยงานของรัฐผ่านทางอินเตอร์เน็ตได้ด้วย อาทิ กรมสรรพากรเปิดให้ประชาชนและนิติบุคคลสามารถยื่นและชำระภาษีทางออนไลน์ หรือกรมทะเบียนการค้าเปิดให้ประชาชนจองชื่อนิติบุคคลทางออนไลน์ เป็นต้น นอกจากนี้ ภายในหน่วยงานของรัฐเองหลายแห่งเท่าที่มีก็มีแผนจะปรับเปลี่ยนงานสารบรรณจากที่เป็นระบบกระดาษมาสู่ระบบอิเล็กทรอนิกส์เพื่อลดค่าใช้จ่ายและเพิ่มประสิทธิภาพความรวดเร็วในการติดต่อสื่อสาร เนื่องจากสามารถใช้ลายมือชื่ออิเล็กทรอนิกส์กำกับข้อมูลอิเล็กทรอนิกส์ต่าง ๆเพื่อผูกพันเจ้าของลายมือชื่อกับข้อมูลได้สร้างขึ้นให้มีผลทางกฎหมายเช่นเดียวกับการลงลายมือชื่อในเอกสารกระดาษ

อย่างไรก็ตาม ถึงแม้ว่าธุรกรรมทางอิเล็กทรอนิกส์จะมีประโยชน์มากมาย แต่การจะปรับเปลี่ยนระบบจากกระดาษไปสู่อิเล็กทรอนิกส์หรือที่เรียกว่าสำนักงานปราศจากกระดาษ (Paperless Office) ก็ไม่ได้ง่ายอย่างที่คิด บางคนกลับมองว่าเป็นภาระและยุ่งยากมากกว่าเดิมปัญหาหลักไม่ได้อยู่ที่กฎหมายหรือเทคโนโลยี แต่กลับอยู่ที่พฤติกรรมการใช้งานเป็นสำคัญ องค์กรหลายแห่งลงทุนติดตั้งระบบติดต่อสื่อสารภายในองค์กร ไม่ว่าจะเป็นอีเมล์หรือระบบงานสารบรรณอิเล็กทรอนิกส์ (Work flow) แต่ตัวผู้บริหารกลับไม่เคยใช้คอมพิวเตอร์ มีแต่พนักงานระดับปฏิบัติการเท่านั้นที่ใช้ ดังนั้นเอกสารอิเล็กทรอนิกส์ที่ส่งขึ้นมาจากเจ้าหน้าที่ระดับปฏิบัติการขึ้นไปถึงผู้บริหารจะต้องถูกทำเป็นกระดาษเสียก่อนโดยเลขาฯเพื่อให้ผู้บริหารลงนามและหลังจากนั้นเลขาฯก็จะพิมพ์คำสั่งดังกล่าวลงไปบนระบบอิเล็กทรอนิกส์และส่งต่อไปให้พนักงานเพื่อปฏิบัติและถ้ายิ่งองค์กรนั้นมิได้นำเอาลายมือชื่ออิเล็กทรอนิกส์มาใช้เพื่อยืนยันคำสั่งดังกล่าวมาจากผู้บริหารท่านนั้นจริงด้วยแล้วเอกสารฉบับนั้นจะสร้างงานเพิ่มเป็น 2 เท่า คือต้องส่งทางอิเล็กทรอนิกส์ด้วย(เพื่อสะดวกต่อการสืบค้นและเก็บรักษา) และยังต้องส่งเอกสารต้นฉบับที่มีรายมือชื่อผู้บริหารเพื่อยืนยันว่าคำสั่งถูกต้องไปพร้อมกัน

การนำเอาระบบอิเล็กทรอนิกส์มาประยุกต์ใช้กับธุรกรรมเพื่อให้เกิดประสิทธิผลสูงสุดนั้น ทั้งกระบวนการตั้งแต่ต้นทางจนถึงปลายทางควรจะต้องเป็นรูปแบบอิเล็กทรอนิกส์ทั้งหมดโดยเฉพาะเมื่อมีการนำเอาลายมือชื่ออิเล็กทรอนิกส์มาประยุกต์ใช้ด้วยจะสามารถทดแทนระบบกระดาษได้อย่างสมบูรณ์ ยกตัวอย่างเช่น บริษัทแห่งหนึ่งทำเว็บไซต์ B2B ขึ้นมาเพื่อให้ตัวแทนจำหน่ายสามารถสั่งซื้อสินค้าทางออนไลน์ เมื่อลูกค้าส่งคำสั่งซื้อสินค้าเข้ามายังเว็บไซต์ คำสั่งซื้อนั้นอาจจะส่งไปยังฝ่ายขายเพื่อตรวจความถูกต้อง หลังจากฝ่ายขาย

อนุมัติก็จะส่งต่อไปยังฝ่ายบัญชีเพื่อตรวจสอบวงเงินสินเชื่อและหากอนุมัติก็จะทำการออกใบกำกับภาษีหรือใบเสร็จ และสุดท้ายส่งต่อไปยังฝ่ายสต๊อกเพื่อจัดเตรียมสินค้าหากกระบวนการทั้งหมดกระทำโดยอิเล็กทรอนิกส์ทั้งหมดวงจรการขายก็จะมีความรวดเร็วโดยเจ้าหน้าที่ในแต่ละส่วนสามารถตรวจสอบและลงนามอนุมัติตามขั้นตอนบนหน้าจอคอมพิวเตอร์ได้ทันที โดยการใช้ลายมือชื่ออิเล็กทรอนิกส์ในการยืนยันตัวตน จะเห็นได้ว่าในกระบวนการนี้ไม่จำเป็นต้องมีเอกสารใดๆเป็นหลักฐานในการอนุมัติเลยเริ่มตั้งแต่ลูกค้าสามารถส่งคำสั่งซื้อที่มีลายมือชื่ออิเล็กทรอนิกส์ของตนไปจนถึงเจ้าหน้าที่สต๊อกที่ทำการปล่อยสินค้า

### 3.4.7.2 ระบบความปลอดภัยของธุรกรรมพาณิชย์อิเล็กทรอนิกส์

ความปลอดภัยสำหรับการใช้และการทำพาณิชย์อิเล็กทรอนิกส์ เมื่อกล่าวถึงความปลอดภัยโดยทั่วไปแล้วจะครอบคลุมถึงความปลอดภัยทางกายภาพ (Physical Security) ได้แก่ทรัพย์สินหรืออุปกรณ์ต่างๆและความปลอดภัยของข้อมูล(Information Security) ซึ่งในที่นี้จะเน้นถึงความปลอดภัยของข้อมูลเป็นหลักเนื่องจากข้อมูลเป็นสิ่งที่อาจจะถือได้ว่าเป็นหัวใจในการทำธุรกิจก็ว่าได้และง่ายต่อการคุกคามเพราะพาณิชย์อิเล็กทรอนิกส์นั้นจะเป็นการรับส่งหรือการแลกเปลี่ยนข้อมูลกันบนเครือข่าย ข้อมูลที่กล่าวถึงจะอยู่ในทุกๆส่วนของธุรกรรมพาณิชย์อิเล็กทรอนิกส์ไม่ว่าจะเป็น การค้นหาข้อมูล การโฆษณา การสั่งซื้อ การชำระเงิน และการส่งสินค้าหรือบริการตัวอย่างของการคุกคามได้แก่

- การเข้าถึงระบบเครือข่ายจากผู้ที่ไม่มีสิทธิ์
- การเข้ามาทำลาย เปลี่ยนแปลง หรือขโมยข้อมูล
- การนำข้อมูลไปเปิดเผยแก่ผู้อื่นที่ไม่เกี่ยวข้อง
- การทำให้การทำงานของระบบหยุดชะงัก
- การปฏิเสธความรับผิดชอบในการทำธุรกรรม หรือ การอ้างว่าได้รับ

ซึ่งถ้าข้อมูลเหล่านั้นเกี่ยวข้องกับ ข้อมูลทางการเงินเช่น หมายเลขบัตรเครดิต ข้อมูลลับของบริษัท(Corporate Secret) หรือข้อมูลที่เป็นทรัพย์สินทางปัญญา (Intellectual Property)จะก่อให้เกิดความเสียหายอย่างมาก

**หลักการรักษาความปลอดภัยในการสื่อสาร**

- ต้องสามารถระบุตัวตนผู้ส่งสารได้ (Authentication)
- ต้องรักษาความเป็นส่วนตัวได้ (Privacy)
- เนื้อหาถูกต้อง ครบถ้วน (Integrity)
- ผู้ส่งไม่สามารถปฏิเสธความรับผิดชอบภายหลังได้ (Non-repudiation)

**3.5 กฎหมายเกี่ยวกับการรับฟังพยานหลักฐานของประเทศสหรัฐอเมริกา Federal Rule of Evidence Act (FRE)**

ก่อนหน้าที่ประเทศสหรัฐอเมริกาจะมีการยกร่าง Federal Rule of Evidence Act (FRE) ได้มีการร่าง The Federal Business Records Act ในปีค.ศ. 1936 ซึ่งการปรับปรุงดังกล่าวได้กระทำก่อนการประดิษฐ์เครื่องคอมพิวเตอร์ แต่ผู้ปรับปรุงกฎหมายได้ปรับปรุงให้กฎหมายฉบับนี้มีความยืดหยุ่นเป็นอย่างมาก กล่าวคือ ใช้คำว่า การเขียนแบบใดๆหรือการบันทึก (any writing or record) และมีการบันทึกการเขียนนั้นลงในหนังสือหรือสิ่งอื่นๆ ซึ่งมีตัวอย่างของศาลสหรัฐฯในคดี United States v. Fedley 552 F.2d 181,184 (5th Cir 1975) ที่ได้นำกฎหมายฉบับนี้มาใช้โดยการตีความแบบยืดหยุ่นกล่าวคือ เป็นการรับฟัง printout โดยไม่มีการโต้แย้ง แต่ในปัจจุบันกฎหมายฉบับนี้ได้ถูกทดแทนโดย Federal Rule of Evidence แล้ว

Federal Rule of Evidence ได้ยกร่างขึ้นและแล้วเสร็จในปีค.ศ. 1998 เพื่อแก้ปัญหาการรับฟังพยานบอกเล่าที่ได้บัญญัติไว้ในมาตรา 803[31] ดังนี้ “บันทึก รายงาน ประวัติ หรือการรวบรวมข้อมูลไม่ว่าในรูปแบบใดของการกระทำ เหตุการณ์ เงื่อนไข ความเห็น หรือการวินิจฉัยที่ได้กระทำใน หรือใกล้เวลาหรือจากข้อมูลที่ส่งมาโดยบุคคลที่ได้รู้ความนั้น หากการเก็บข้อมูลนั้นเป็นการดำเนินการทางธุรกิจเป็นปกติธุระ และเป็นหลักปฏิบัติของธุรกิจนั้นที่จะต้องทำ บันทึกรายงาน ประวัติ รวบรวมข้อมูล จะต้องนำสืบผู้ครอบครองเอกสารหรือบุคคลที่มีคุณสมบัติใกล้เคียง หากเห็นว่าสารสนเทศ หรือวิธีการหรือสิ่งแวดล้อมในการเตรียมการไม่น่าเชื่อถือ

ซึ่งจะเห็นได้ว่าปัญหาการรับฟังพยานบอกเล่า ศาลสามารถรับฟังเอกสารดังที่กล่าวมาแล้วนั้นเป็นพยานหลักฐานได้ หากศาลเห็นว่าสารสนเทศหรือวิธีการหรือสิ่งแวดล้อมในการเตรียมการมีความน่าเชื่อถือ ซึ่งมีคดีตัวอย่างที่ตัดสินตาม Federal Rule of Evidence เช่น
คดี United State v. Scholle 553 f2d 11090(8thCir.1977)
จำเลยถูกกล่าวหาว่าค้ายาเสพติด มีการนำ printout ของเครื่องคอมพิวเตอร์ที่วิเคราะห์ส่วนประกอบของยาที่ถูกยึดทั่วทั้งสหรัฐฯและมีการบันทึกเวลาและสถานที่ที่แสดงรูปแบบการแจกจ่ายของยาที่จำเลยถูกกล่าวหาว่ามีส่วนอยู่ด้วย ศาลว่าไม่มีเหตุจะสันนิษฐานว่าไม่น่าเชื่อถือ

---

[31] Rule 803 Hearsay Exception: Availability of Declarant Immaterial

The following are not excluded by the hearsay rule, even though the declarant is available as a witness:

(6) Records of regularly conducted activity.

**-หลักเกณฑ์ทั่วไปในคดีแพ่ง**

พยานหลักฐานทางอิเล็กทรอนิกส์ในคดีแพ่งสามารถรับฟังได้หรือไม่นั้นจะใช้หลักเกณฑ์โดยทั่วไปของกฎหมายคอมมอนลอว์และได้รับยกเว้นตามข้อยกเว้นใน FRE เช่นเดียวกับคดีอาญา อย่างไรก็ตาม ยังคงมีส่วนที่เพิ่มเติมในการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ในคดีแพ่งในส่วนที่เกี่ยวกับธุรกรรมทางพาณิชย์อิเล็กทรอนิกส์

พระราชบัญญัติที่เกี่ยวข้องกับการรับฟังพยานหลักฐานทางพาณิชย์อิเล็กทรอนิกส์ของสหรัฐอาจสามารถพิจารณาได้ภายใต้หลักเกณฑ์ของกฎหมาย 3 ฉบับ คือ Electronic Signature in Global and National Commerce Act (2000) (E-Sign) กฎหมายต้นแบบ The Uniform Transactions Act (UETA) และมาตรา 9 ของThe Uniform Commercial (UCC)

E-Sign เป็นกฎหมายซึ่งบังคับใช้ในระดับสหพันธรัฐเพื่อรองรับผลของลายมือชื่ออิเล็กทรอนิกส์และมีผลใช้บังคับกับธุรกรมที่เกิดขึ้นระหว่างมลรัฐหรือระหว่างประเทศ ส่วน UETA เป็นกฎหมายในระดับมลรัฐ โดยเป็นร่างกฎหมายต้นแบบซึ่งร่างโดย The U.S. National Conference of Commissioners on Uniform State Laws (NCCUSL) เพื่อสนับสนุนการพาณิชย์อิเล็กทรอนิกส์เช่นกัน โดยมีนโยบายเพื่อส่งเสริมให้ทุกมลรัฐบังคับใช้กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ไปในทิศทางเดียวกัน แต่ละมลรัฐสามารถนำร่างต้นแบบไปบังคับใช้ทั้งในรูปแบบเดียวกับต้นร่างและการแก้ไขปรับปรุงบางส่วนเพื่อให้สอดคล้องกับบทบัญญัติของกฎหมายในมลรัฐของตน[32]

UETA และ E-Sign จะบังคับใช้ครอบคลุมถึงธุรกรรมทางอิเล็กทรอนิกส์และสัญญาในขณะที่ UCC จะบังคับใช้กับธุรกรรมการซื้อขายสินค้าซึ่งอาจเกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์หรือไม่ก็ได้นอกจากนี้ ยังมีบางมลรัฐที่รับเอาหลักเกณฑ์การรับรองการมีอยู่ของเอกสารอิเล็กทรอนิกส์ดังกล่าวไว้ในหลักเกณฑ์เกี่ยวกับพยานหลักฐาน เช่น มลรัฐวิสคอนซิน โดยบัญญัติ ว่า ต้นฉบับของหนังสือรวมไปถึงข้อมูลที่เก็บไว้ในคอมพิวเตอร์หรือเครื่องมือในลักษณะเดียวกัน

---

A memorandum,report,record,or data compilation, in any form,of acts,events,conditions,opinions,or diagnoses,made at or near the time by,or form information transmitted by,a person with knowledge,if kept in the course of a regulary conducted business activity,and if it was the regular practice of that business activity to make the memorandum,report,records,or data compilation,all as shown by the testimony of the custodian or other qualified witness,unless the source of information at the method or circumstances of preparation indicade lack of trustworthiness….

[32] Stephen E. Blythe,**"Digital Signature Law of The United Nations,European Union,United Kingdom and United States:Promotion of Growth in E-Commerce with Enchanced Security",(**Winter 2005) Richmond Journal of Law and Technology[29].

เช่น print out หรือการประมวลผลใดที่สามารถอ่านได้และแสดงว่ามีความถูกต้อง[33]

UETA และ E-Sign ต่างก็เป็นบทบัญญัติของวิธีสบัญญัติโดยมีจุดประสงค์ให้สัญญาหรือบันทึกซึ่งอยู่ในรูปของอิเล็กทรอนิกส์มีสถานะทางกฎหมายเทียบเท่ากับกระดาษ โดยไม่มีผลกระทบถึงกฎหมายสารบัญญัติโดยส่วนใหญ่ของกฎหมายทั้งสองฉบับจะมีสาระสำคัญเหมือนกัน ไม่ว่าจะเป็นหลักเกณฑ์ทั่วไป เช่น บันทึกหรือลายมือชื่อจะไม่ถูกปฏิเสธถึงความมีผลทางกฎหมายหรือการบังคับใช้เพียงเพราะว่าอยู่ในรูปแบบของอิเล็กทรอนิกส์ สัญญาจะไม่ถูกปฏิเสธถึงความมีผลทางกฎหมายหรือการบังคับใช้เพียงเพราะว่าถูกบันทึกอยู่ในรูปแบบของบันทึกทางอิเล็กทรอนิกส์ ถ้ากฎหมายต้องการให้ทำเป็นหนังสือ บันทึกทางอิเล็กทรอนิกส์ถือว่ามีการทำเป็นหนังสือแล้ว และถ้ากฎหมายต้องการให้มีการลงลายมือชื่อ การลงลายมือชื่ออิเล็กทรอนิกส์ถือว่ามีการลงลายมือชื่อแล้ว ทั้งนี้ บันทึกทางอิเล็กทรอนิกส์ดังกล่าวจะต้องสามารถเก็บรักษาและสามารถทำซ้ำในภายหลังได้อย่างครบถ้วนถูกต้อง และเอกสารในรูปแบบอิเล็กทรอนิกส์สามารถถือเป็นต้นฉบับเอกสารหากการจัดทำเอกสารเป็นไปตามมาตรฐานการจัดเก็บบันทึก นอกจากนี้ การเก็บรักษาเอกสารในรูปแบบอิเล็กทรอนิกส์ซึ่งมีความถูกต้องและผู้ที่มีสิทธิสามารถเข้าถึงข้อมูลเพื่อตรวจสอบหรือทำซ้ำได้ในรูปแบบที่ถูกจัดเก็บ ในภายหลัง เอกสารอิเล็กทรอนิกส์ดังกล่าวถือว่าเป็นการเพียงพอแล้วสำหรับกฎหมายใดที่ต้องการให้มีการเก็บรักษาบันทึกหรือเอกสารสัญญาดังกล่าว

UETA และ E-Sign ต่างก็ระบุนิยามต่างๆ ที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ไว้ในลักษณะเดียวกัน เช่น

อิเล็กทรอนิกส์ หมายถึง เทคโนโลยีซึ่งเกี่ยวข้องกับกระแสไฟฟ้า ดิจิตอล แถบแม่เหล็กไร้สาย สายเคเบิลใยแก้ว แถบแม่เหล็กที่มีประจุไฟฟ้า หรือสิ่งใกล้เคียง[34]

บันทึกทางอิเล็กทรอนิกส์ หมายถึง สัญญาหรือบันทึกอื่นๆ ซึ่งสร้าง ทำให้เกิดขึ้น ส่งสื่อสาร รับ หรือเก็บโดยวิธีทางอิเล็กทรอนิกส์[35]

---

[33] Wis.Stat.section 910.01(3)specifies that an “original” writing includes “data…stored in a computer or similar device,any printout or other output readable by sight,shown to reflect the data accurateiy. …”

[34] The Uniform Electronic Transactions Act § 2 (5) at 266/The Electronic Signature in Global and National Commerce Act: 106 (2).

[35] The Uniform Electronic Transactions Act § 2 (7) at 266/The Electronic Signature in Global and National Commerce Act: 106 (4).

ลายมือชื่ออิเล็กทรอนิกส์ หมายถึง เสียง สัญลักษณ์ กระบวนการทางอิเล็กทรอนิกส์ซึ่งแนบหรือเกี่ยวพันเป็นลำดับขั้นตอนกับสัญญา หรือบันทึกอื่นใดซึ่งได้ถูกใช้หรือรับเอาโดยบุคคลโดยมีเจตนาที่จะลงลายมือชื่อในบันทึกนั้น[36]

ข้อความ หมายถึง ข้อมูล ข้อเขียน รูปภาพ เสียง สัญลักษณ์ โปรแกรมคอมพิวเตอร์ ซอฟต์แวร์ ดาต้าเบส หรือสิ่งทำนองเดียวกัน[37]

บันทึก หมายถึง ข้อความซึ่งอยู่ในสื่อซึ่งจับต้องได้ หรือซึ่งถูกจัดเก็บในอิเล็กทรอนิกส์หรือสื่อกลางอื่นๆที่สามารถเรียกให้ปรากฏในรูปที่สามารถมองเห็นได้[38]

สิ่งที่ศาลสหรัฐฯตีความว่าเป็นการลงลายมือชื่อได้แก่ a long-hand signature,initials,a signed “X”,a hand stamp[39],a letterhead[40],a typewritten signature[41], a facsimile signature[42], audio[43] และ videotape

ในคดี Re CAFETERIA OPERATORS,L.P.,et al.,Debtors.ศาลวินิจฉัยว่า ภายใต้หลักกฎหมาย The Perishable Agricultural Commodities Act (PACA) ซึ่งคู่สัญญาสามารถขยายระยะเวลาการชำระหนี้ออกไปเกินสามสิบวันได้ หากมีการทำข้อตกลงกันไว้เป็นหนังสือซึ่งในกรณีธุรกรรมที่เกี่ยวเนื่องระหว่างรัฐนี้ อีเมล์มีคุณสมบัติของข้อตกลงเป็นหนังสือภายใต้ E-Sign:101

---

[36] The Uniform Electronic Transactions Act § 2 (8) at 266/The Electronic Signature in Global and National Commerce Act: 106 (5).

[37] The Uniform Electronic Transactions Act § 2 at 266/The Electronic Signature in Global and National Commerce Act: 106 (7).

[38] The Uniform Electronic Transactions Act § 2 at 266/The Electronic Signature in Global and National Commerce Act: 106 (9).

[39] จากคำพิพากษาในคดี States of North Carolina v. Watts 289 NC 445,0220SE.2d389(1976) อ้างโดย Michael S.Baum ใน Analysis of Legal Aspects p.124.

[40] จากคำพิพากษาในคดี Cox Engineering Inc.v. Funston Machine& Supply Co., 749 SW. 2d 508(Tex. CT. App. 1988) อ้างโดย Michael S. Baum ใน Analysis of Legal Aspects p. 124

[41] จากคำพิพากษาในคดี Save-on-Carpets of Arizona.Inc.; Jarratt v. Trend Mills, 545 F. 2d 1239(9th Circ. 1976).20 UCC Rep. 1082 อ้างโดย Michael S. Baum ใน Analysis of Legal Aspects p. 124

[42] จากคำพิพากษาในคดี Maricopa Country v. Osborn, 60 Ariz. 290 136 p.2 d 270,(1943) อ้างโดย Michael S. Baum ใน Analysis of Legal Aspects p. 124

[43] จากคำพิพากษาในคดี Ellis Canning Co. v. Bernstein 11 UCC Rep. Serv (Callaghen)443,348 F. Supp. 1212 (d.Colo.1972) อ้างโดย Michael S. Baum ใน Analysis of Legal Aspects p.124

นอกจากนี้ ธุรกรรมบางประเภทที่ UETA และ E-Sign ไม่ใช้บังคับซึ่งสอดคล้องและเป็นในทิศทางเดียวกัน เช่น พินัยกรรมและทรัสต์[44] หรือกรณีที่กฎหมายอื่นของแต่ละมลรัฐระบุไว้เป็นอย่างอื่น เช่น ไม่สามารถใช้บังคับกับกฎหมายเกี่ยวกับครอบครัว การรับบุตรบุญธรรมและการหย่า[45] นอกจากนี้ E-Sign ยังไม่ใช้บังคับกับคำสั่งหรือหมายของศาล ตลอดจนกระบวนพิจารณาและเอกสารใด ๆ ที่เกี่ยวข้องกับการดำเนินคดีในศาล หนังสือบอกกล่าวยกเลิกหรือบอกเลิกการใช้บริการสาธารณูปโภค[46] ประกันสุขภาพ หรือผลประโยชน์จากการประกันชีวิต[47] ตลอดจนไม่สามารถใช้กับเอกสารที่ต้องมีในการขนส่งหรือครอบครองวัตถุอันตราย ยาฆ่าแมลง สารพิษ หรือสารอันตรายอื่นๆ[48]

อย่างไรก็ตาม ยังคงมีความไม่ชัดเจนว่ากฎหมายทั้งสองฉบับดังกล่าวสามารถนำไปใช้ในคดีอาญาด้วยหรือไม่ เนื่องจากไม่มีบทบัญญัติของกฎหมายบัญญัติไว้อย่างชัดเจนให้นำไปบังคับใช้ อีกทั้งกฎหมายทั้งสองฉบับดังกล่าวต่างก็เป็นบทบัญญัติที่มีจุดประสงค์ให้สัญญาหรือบันทึกซึ่งอยู่ในรูปอิเล็กทรอนิกส์มีสถานะทางกฎหมายเทียบเท่ากับกระดาษ โดยมุ่งถึงผลของบันทึกหรือลายมือชื่อในรูปแบบอิเล็กทรอนิกส์ ซึ่งเป็นหลักเกณฑ์ในคดีแพ่งจึงอาจไม่สามารถนำไปบังคับใช้ในคดีอาญาได้ ดังนั้น จึงยังคงต้องรอดูผลการวินิจฉัยของศาลหรือผู้ที่เกี่ยวข้องต่อไป

นอกจากนี้ กฎหมายทั้งสองฉบับยังคงมีความแตกต่างกันในบางส่วน ในข้อแรก UETA มีบทบัญญัติเฉพาะในการพิจารณาว่าบันทึกทางอิเล็กทรอนิกส์สามารถเชื่อมโยงกับบุคคลหรือนิติบุคคลใดโดยชอบด้วยกฎหมายหรือไม่ โดยกำหนดว่าหากบันทึกหรือลายมือชื่ออิเล็กทรอนิกส์เป็นผลมาจากการกระทำของบุคคลใดแล้วถือว่าบุคคลนั้นเกี่ยวข้องด้วย[49] และบันทึกอิเล็กทรอนิกส์สามารถรับฟังได้หากมีลายมือชื่อหรือบันทึกแนบหรือเกี่ยวพันเป็นลำดับขั้นตอนกับบุคคลที่มีอำนาจที่จะลงลายมือชื่อ โดยไม่จำเป็นต้องมีการรับรองลายมือชื่อ[50] หรือต้องมีเทคโนโลยี เช่น PKI[51] สำหรับรับรองความถูกต้องแท้จริงของลายมือชื่ออีก โดยที่ E- Sign ไม่มีบทบัญญัติในส่วนนี้

---

[44] The Uniform Electronic Transactions Act § 3 (b) (1), at 235. /The Electronic Signature in Global and National Commerce Act: 103 (a) (1).

[45] The Uniform Electronic Transactions Act § 3 (b) (4), at 235. /The Electronic Signature in Global and National Commerce Act: 103 (a) (2).

[46] The Electronic Signature in Global and National Commerce Act: 103 (b) (1).

[47] The Electronic Signature in Global and National Commerce Act: 103 (b) (2).

[48] The Electronic Signature in Global and National Commerce Act: 103 (b) (2).

[49] The Electronic Signature in Global and National Commerce Act: 103 (b) (3).

[50] The Uniform Electronic Transactions Act § 9 (a) (4) at 261.

[51] The Uniform Electronic Transactions Act § 11at 266, PKI หรือ Public Key Infrastructure เป็นกระบวนการที่จัดทำขึ้นเพื่อก่อให้เกิดความมั่นใจกับผู้ใช้ระบบการเข้ารหัสข้อความ (encryption) โดยจัดให้มีการรับรองกุญแจสาธารณะ (public key) ของผู้ใช้ โดยผู้ที่ได้รับอนุญาตให้ออกใบรับรอง (certification authorities/CA) ระบบการเข้ารหัสข้อความประกอบด้วยระบบการคำนวณทางคณิตศาสตร์ (mathematical algorithms) จำนวน 2 ชุด ชุดแรก เพื่อเข้ารหัส (encrypt) ข้อความตัวอักษรธรรมดา (plain text) เพื่อป้องกันมิให้บุคคลอื่นทราบหรือเข้าใจข้อความนั้น และชุดที่สองเพื่อถอดรหัส (decrypt) ข้อความที่ถูกเข้ารหัสดังกล่าวออกมาเป็นข้อความธรรมดา ซึ่งระบบการคำนวณทางคณิตศาสตร์ดังกล่าวเปรียบเสมือนกุญแจ กุญแจที่เปิดเผยกับบุคคลทั่วไปจะเรียกว่า กุญแจสาธารณะ ซึ่งอาจเลือกกุญแจเพื่อเข้ารหัสหรือถอดรหัสเป็นกุญแจสาธารณะก็ได้ และกุญแจที่ถูกเก็บไว้กับผู้ใช้ระบบดังกล่าวโดยไม่เปิดเผยกับบุคคลทั่วไปเรียกว่า กุญแจส่วนตัว (private key) : ซึ่งเมื่อเลือกกุญแจสาธารณะเป็นแบบเข้ารหัสหรือถอดรหัสแล้ว กุญแจส่วนตัวก็จะเป็นอีกแบบหนึ่งที่เหลือ โดยเหตุที่ระบบการเข้ารหัสข้อความ ทำให้สามารถยืนยันหรือระบุถึงบุคคลใดบุคคลหนึ่งว่าเป็นผู้ส่งเอกสารดังกล่าวได้จึงถือเป็นลายมือชื่อดิจิตอลอย่างหนึ่งด้วย –Michael Chissick and Alistair Kelman, Electronic Commerce Law and Practice, (2nd ed., 2000) 155-164./ Henry H. Perritt, JR., Law and the Information Super Highway (1996) 394-396.

ข้อสอง E- Sign มีบทบัญญัติคุ้มครองผู้บริโภค โดยบัญญัติว่า หากกฎหมายใดบัญญัติถึงหน้าที่ในการจัดหาข้อมูลเป็นลายลักษณ์อักษรให้กับผู้บริโภคแล้ว ถือว่าการจัดหาข้อมูลนั้นได้มีการดำเนินการแล้ว หากมีการจัดหาบันทึกอิเล็กทรอนิกส์ให้โดยความยินยอมของผู้บริโภคซึ่งเข้าใจอย่างชัดแจ้งถึงความยินยอมแล้ว และผู้บริโภคจะถอนความยินยอมเมื่อใดก็ได้โดยปราศจากค่าใช้จ่าย[52]

ข้อสาม E-Sign มีบทบัญญัติที่จะต้องนำ E-Sign นำมาใช้บังคับในกรณีที่มีกฎหมายมลรัฐใช้บังคับในเรื่องเดียวกัน เว้นเสียแต่ว่ามลรัฐนั้นรับเอา UETA มาบังคับใช้โดยไม่มีการเปลี่ยนแปลงแก้ไข หรือรับเอากระบวนการอื่นใดหรือมาตรการอื่นใดที่เป็นไปในแนวทางเดียวกันกับ E-Sign มาบังคับใช้[53]

ข้อสี่ UETA มีบทบัญญัติที่เป็นทางเลือกสำหรับมลรัฐในส่วนที่ไม่เกี่ยวกับการเป็นคู่สัญญาทางการค้าหรือการพาณิชย์ที่จะให้มีการใช้บันทึกทางอิเล็กทรอนิกส์หรือลายมือชื่ออิเล็กทรอนิกส์เกี่ยวกับหน่วยงานของมลรัฐหรือไม่ เช่น กรณีที่คู่สัญญาตกลงกันที่จะจัดทำโฉนดที่ดินในรูปของอิเล็กทรอนิกส์ ธุรกรรมระหว่างคู่สัญญามีผลตามกฎหมาย และโฉนดที่ดินอิเล็กทรอนิกส์นั้นชอบด้วยกฎหมาย แต่คู่สัญญาดังกล่าวจะไม่สามารถยื่นโฉนดที่ดินอิเล็กทรอนิกส์ต่อหน่วยงานของมลรัฐได้ เว้นเสียแต่ว่าจะมีบทบัญญัติของกฎหมายอนุญาตให้ดำเนินการได้[54]

ส่วน UCC มีบทบัญญัติที่เกี่ยวกับการรับฟังพยานหลักฐานอิเล็กทรอนิกส์บัญญัติอยู่ในมาตรา 9 โดยบทบัญญัติดังกล่าวถูกแก้ไขปรับปรุงจากบทบัญญัติเดิมเป็นการแทนที่แนวความคิดของลายลักษณ์อักษรและลายมือชื่อด้วยการบันทึกและความถูกต้องแท้จริง ดังนั้นบุคคลสามารถรับรองความถูกต้องแท้จริงของบันทึกได้โดยการลงลายมือชื่อ หรือทำให้เป็นผลหรือรับเอาสัญลักษณ์ใด ๆ หรือโดยการใส่รหัส หรือวิธีการอื่นใดไม่ว่าทั้งหมดหรือบางส่วนของบันทึกโดยมีเจตนาที่จะรับรองความถูกต้องแท้จริงที่สามารถยืนยันถึงตัวบุคคลผู้รับหรือยอมรับบันทึกดังกล่าว[55]

นอกจากพระราชบัญญัติทั้งสามฉบับดังกล่าวแล้ว สหรัฐฯยังมีบทบัญญัติเกี่ยวข้องกับพยานหลักฐานทางอิเล็กทรอนิกส์ใน Federal Rule of Civil Procedure ข้อ 34 ซึ่งเป็นบทบัญญัติที่คู่ความจะต้องเปิดเผยพยานเอกสารที่เกี่ยวข้องในประเด็นแห่งคดีที่อยู่ในความครอบครองของตน (Discovery Rule) โดยได้มีการแก้ไขเพิ่มเติมให้เอกสารรวมไปถึงการเก็บ

---

[52] The Electronic Signature in Global and National Commerce Act: 101 (c) (1).

[53] The Electronic Signature in Global and National Commerce Act: 102 (2) (a).

[54] Lorna Brazell, Electronic Signatures Law and Regulation (2004) 153.

[55] American Jurisprudence Legal Forms, Second Edition Database updated November 2003 Chapter 150 B. Internet Transactions.

รวบรวมข้อมูลและข้อมูลอิเล็กทรอนิกส์ในทุกรูปแบบ ซึ่งสอดคล้องกับบทบัญญัตินิยามของเอกสารที่ระบุไว้ใน FRE ข้อ 1001 (1) ดังนั้นคู่ความจะต้องเปิดเผยข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องกับประเด็นในคดีที่อยู่ในความครอบครองของตน แต่ทั้งนี้จะอยู่ภายใต้ Federal Rule of Civil Procedure ข้อ 26 ซึ่งเป็นบทบัญญัติที่ใช้ในการวินิจฉัยแนวโน้มความเกี่ยวข้องของเอกสารที่ถูกขอให้เปิดเผยกับภาระของคู่ความที่ถูกขอเช่นนั้น ซึ่งการเปิดเผยข้อมูลดังกล่าวจะสอดคล้องกับหน้าที่ในการเก็บรักษาเอกสารรวมทั้งข้อมูลอิเล็กทรอนิกส์ภายใต้หลักกฎหมายคอมมอนลอว์คู่ความมีหน้าที่เก็บรักษาเอกสารเมื่อมีการเริ่มคดีโดยเก็บรักษาเอกสารเท่าที่เกี่ยวข้องภายใต้หลักความสุจริตและสามารถทำได้อย่างมีเหตุผล[56] นอกจากนี้ กรณีที่ข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องถูกการทำลายและไม่มีทางเยียวยาและไม่มีบทบัญญัติตอบโต้ใดที่เหมาะสมแล้ว ศาลจะถือว่าการเจตนาทำลายข้อมูลดังกล่าวถือเป็นข้อสันนิษฐานว่าพยานหลักฐานนั้นไม่ชอบ[57] ซึ่งต้องห้ามมิให้รับฟังเป็นพยานหลักฐานหากคู่ความดังกล่าวต้องการอ้างเอกสารนั้นและถือว่าคู่ความนั้นรับข้อเท็จจริงดังกล่าวแล้วหากคู่ความอีกฝ่ายต้องการอ้างอิงหลักฐานนั้น

ในส่วนของ The Uniform Act ได้บัญญัติถึงกรณีของบันทึกซึ่งกฎหมายกำหนดให้ต้องมีการเก็บรักษาไว้นั้น ซึ่งหากมีการทำซ้ำโดยวิธีถ่ายภาพ หรือถ่ายไมโครฟิล์มหรือวิธีการอื่นใดที่เป็นไปตามมาตรฐานที่ผู้จัดเก็บบันทึกเอกสารกำหนด (the Archivist) การจัดเก็บดังกล่าวจึงจะถือได้ว่ามีการจัดเก็บต้นฉบับเอกสารแล้ว และวัตถุจากการทำซ้ำดังกล่าวจะมีสถานะทางกฎหมายเช่นเดียวกับต้นฉบับ สำเนาของวัตถุที่มีการทำซ้ำดังกล่าว หากมีการประทับตราหรือรับรองโดยผู้จัดเก็บบันทึก เอกสารสำเนาดังกล่าวจะสามารถรับฟังเป็นพยานหลักฐานได้เช่นเดียวกับต้นฉบับของวัตถุนั้น ซึ่งสิ่งที่ทำซ้ำดังกล่าวไม่ว่าจะเป็น การบันทึก คัดลอก ทำซ้ำโดยวิธีการอื่นๆ สิ่งที่ทำซ้ำดังกล่าวก็สามารถรับฟังเป็นพยานหลักฐานได้เช่นเดียวกับต้นฉบับของสิ่งนั้น ไม่ว่าต้นฉบับจะยังมีอยู่หรือไม่ก็ตาม และการขยายสิ่งที่ทำซ้ำ โทรสารของสิ่งที่ทำซ้ำสามารถรับฟังเป็นพยานหลักฐานได้หากสิ่งที่ทำซ้ำยังคงมีอยู่และสามารถนำมาตรวจสอบในศาลได้

โดยรวมพยานหลักฐานอิเล็กทรอนิกส์โดยส่วนใหญ่จะไม่ต้องห้ามมิให้รับฟังในประเทศสหรัฐอเมริกา ทั้งหลักเกณฑ์ข้อห้ามในการรับฟังพยานหลักฐานไม่ว่าจะหลักการรับฟังพยานหลักฐานที่ดีที่สุด หลักการห้ามรับฟังพยานบอกเล่าและการรับรองความถูกต้องแท้จริงของเอกสารถูกผ่อนคลายลงโดยไม่นำมาบังคับใช้อย่างเข้มงวดในการรับฟังพยานหลักฐานทาง

---

[56] William J. Robinson, **'An Overview of Electronic Discovery'**, Practicing Law Institute Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series PLI Order No. 6578 September – November, (2005) Patent Litigation 2005[194].

[57] Crescendo Investments v. Brice, 61 S.W.3d 465(Tex.2001).

อิเล็กทรอนิกส์ทั้งนี้อันเนื่องมาจากลักษณะเฉพาะของพยานหลักฐานในรูปแบบของอิเล็กทรอนิกส์

**3.6 กฎหมายเกี่ยวกับการรับฟังพยานหลักฐานของประเทศสหราชอาณาจักร**

**-หลักเกณฑ์ทั่วไปในคดีแพ่ง**

พยานหลักฐานทางอิเล็กทรอนิกส์ในคดีแพ่งสามารถรับฟังได้หรือไม่นั้นจะใช้หลักเกณฑ์การรับฟังเช่นเดียวกับการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญาในส่วนของกฎหมายคอมมอนลอว์ อย่างไรก็ตาม ยังคงมีส่วนที่เพิ่มเติมสำหรับการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ในคดีแพ่งใน The Civil Evidence Act 1995, The Civil Procedure Rules 1998 และในส่วนที่เกี่ยวกับธุรกรรมทางพาณิชย์อิเล็กทรอนิกส์ ดังนี้

รัฐสภาของอังกฤษได้มีการตรากฎหมาย The Civil Evidence Act 1995 ซึ่งมีผลใช้บังคับตั้งแต่วันที่13 มกราคม ค.ศ. 1997 ซึ่งสาเหตุของการตรากฎหมายฉบับดังกล่าวเป็นการแก้ไขปัญหาของการรับฟังพยานหลักฐานโดยเฉพาะพยานสารสนเทศที่ทำให้เกิดปัญหาหลัก 3 ประการคือ 1. หลักเรื่องการห้ามรับฟังพยานบอกเล่า(Hearsay) 2. หลักพยานที่ดีที่สุด(Best Evidence Rule) 3. การรับรองความถูกต้องแท้จริง(Authentication) ซึ่งหลักการต่างๆที่เกี่ยวข้องกับพยานหลักฐานอิเล็กทรอนิกส์จะถูกบัญญัติไว้ในมาตราต่าง ๆ ดังนี้

มาตรา 1 บัญญัติว่า พยานหลักฐานจะไม่ต้องห้ามมิให้รับฟังเพียงเพราะว่าพยานหลักฐานดังกล่าวเป็นพยานบอกเล่า

มาตรา 8 (1) บัญญัติว่าข้อความในเอกสารจะสามารถรับฟังเป็นพยานหลักฐานได้ถ้าสามารถพิสูจน์ได้ถึงวิธีการจัดทำ หรือเอกสารนั้นยังคงมีอยู่โดยการแสดงวิธีการจัดทำสำเนาของเอกสารดังกล่าวหรือส่วนสำคัญของเอกสาร และสามารถรับรองความถูกต้องแท้จริงโดยวิธีที่ศาลเห็นชอบ

มาตรา 8 (2) บัญญัติว่า ความแตกต่างระหว่างสำเนาและต้นฉบับจะไม่ใช่สาระสำคัญในการรับฟังพยานหลักฐาน

มาตรา 9 บัญญัติว่า เอกสารซึ่งเป็นส่วนหนึ่งของบันทึกทางธุรกิจหรือบันทึกของเจ้าหน้าที่ซึ่งทำขึ้นโดยพนักงานหรือเจ้าหน้าที่ที่มีหน้าที่จัดทำสามารถรับฟังเป็นพยานหลักฐานได้โดยไม่ต้องมีการพิสูจน์

มาตรา 12 บัญญัติว่า เอกสาร หมายถึง สิ่งใด ๆ ซึ่งข้อมูลในทุกรูปแบบถูกบันทึกไว้

สำเนา ในส่วนที่เกี่ยวข้องกับเอกสาร หมายถึง สิ่งใด ๆ ที่ข้อมูลได้ถูกบันทึกไว้ได้ถูกคัดลอกไม่ว่าโดยวิธีใด ๆ และไม่ว่าโดยทางตรงหรือทางอ้อม

จากบทบัญญัติดังกล่าว บันทึกทางธุรกิจ หรือบันทึกของเจ้าหน้าที่ซึ่งทำขึ้นโดยพนักงานหรือเจ้าหน้าที่ที่มีหน้าที่จัดทำสามารถรับฟังเป็นพยานหลักฐานได้โดยไม่ต้องมีการพิสูจน์รวมทั้งบันทึกทางธุรกิจหรือบันทึกของเจ้าหน้าที่ที่ทำขึ้นโดยคอมพิวเตอร์แต่ทั้งนี้ไม่ห้ามคู่ความอีกฝ่ายในการที่จะหมายเรียกพยานที่เกี่ยวข้องมาเพื่อพิสูจน์ถึงความถูกต้องแท้จริงของเอกสาร

ในส่วนของ The Civil Procedure Rules 1998 Part 31 คู่ความทุกฝ่ายจะต้องเปิดเผยพยานเอกสารที่เกี่ยวข้องกับข้อกล่าวอ้างของตน (disclosure of documents) ซึ่งเอกสารตาม The Civil Procedure Rules 1998 Part 31.4 หมายถึง สิ่งใด ๆ ซึ่งข้อมูลไม่ว่าในรูปแบบใด ๆ ถูกบันทึกไว้[58] เอกสารจึงไม่จำกัดเฉพาะสิ่งที่เป็นลายลักษณ์หรือกระดาษ แต่จะรวมไปถึงอีเมล์ รูปถ่าย สื่อและสิ่งบันทึกภาพหรือเสียง เช่น วีดีโอ และเทป ตลอดจนข้อมูลที่เกี่ยวข้องที่ถูกจัดเก็บไว้ใน hard drive ของคอมพิวเตอร์หรือดิสก์ บันทึกทางธุรกิจ รวมถึงบันทึกทางบัญชีด้วย The Companies Act 1985 บัญญัติให้บริษัทมหาชนจำกัดต้องเก็บรักษาบันทึกทางบัญชีไว้เป็นระยะเวลา 6 ปี และบริษัทจำกัดต้องเก็บรักษาบันทึกทางบัญชีไว้เป็นระยะเวลา 3 ปี (The Companies Act 1985 s. 222) อย่างไรก็ตาม ยังไม่มีการกล่าวถึงบทบัญญัติเพิ่มเติมในส่วนของนิติบุคคลทุกประเภทว่าจะต้องมีการเก็บรักษาบันทึกทางบัญชีให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ไว้เป็นระยะเวลานานเท่าใด ซึ่งอาจมีเป็นข้อกำหนดของนิติบุคคลในแต่ละที่ๆจะเป็นข้อกำหนดหรือข้อบังคับภายใน ในส่วนของบริษัทมหาชนและบริษัทจำกัดนั้น การเก็บเอกสารดังกล่าวในรูปของสื่อบันทึกข้อมูลหรือการทำซ้ำซึ่งเอกสารดังกล่าวให้อยู่ในรูปของสื่อบันทึกข้อมูล เช่น ซีดีรอม ซึ่งสามารถที่จะทำซ้ำซึ่งเอกสารดังกล่าวได้ ถือเป็นการปฏิบัติตามกฎหมายในการเก็บรักษาเอกสารแล้ว ทั้งนี้ เนื่องจากภายใต้ The Companies Act 1985 มาตรา 722 (1) บัญญัติว่าเอกสารใด ๆ ที่บริษัทต้องเก็บรักษาภายใต้กฎหมายนี้ จะเก็บในรูปแบบของการดำเนินการใน bound book หรือบันทึกเรื่องราวดังกล่าวในรูปแบบอื่น ๆ ก็ได้ Michael Chissick and Alistair Kelman, Electronic Commerce Law and Practice, (2nd ed., 2000) 183. และในคดี Brian S. Grave v Leslie & Godwin Financial Services Limited ศาลวินิจฉัยว่าบริษัทประกันภัยมีหน้าที่ที่จะต้องระวังรักษาเอกสารของผู้เอาประกันภัยและห้ามทำลายเอกสารดังกล่าวเว้นเสียแต่ว่าจะได้รับคำสั่งจากผู้เอาประกันภัย ยิ่งไปกว่านั้นเอกสารการจ่ายเงินไม่ว่าจะเป็นของผู้เอาประกันภัยหรือไม่บริษัทประกันภัยก็ห้ามทำลาย เว้นเสียแต่ว่าจะได้รับความยินยอมจากผู้เอาประกันภัย ดังนั้น คู่ความทุกฝ่ายจะต้องเปิดเผยพยานอิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อกล่าวอ้างของตน (disclosure of documents) ไม่ว่าจะเป็น

---

[58] The Civil Procedure Rules 1998 Part 31.4: The word “document” means anything on which information of any description is recorded.

พยานหลักฐานที่เป็นผลดีหรือผลร้ายกับข้อกล่าวอ้างของตนเองหรือของคู่ความฝ่ายอื่นหลังจากที่มีการยื่นคำฟ้องคำให้การของทุกฝ่ายแล้วโดยใช้หลักการเดียวกันกับการเปิดเผยพยานเอกสารโดยทั่วไป

นอกจากนี้ ภายใต้หลักเกณฑ์ของ The E-commerce directive ที่ระบุแนวทางให้ประเทศสมาชิกอนุญาตให้สัญญาสามารถดำเนินการได้โดยวิธีการทางอิเล็กทรอนิกส์โดยการบัญญัติกฎหมายมารองรับ สหราชอาณาจักรหนึ่งในสมาชิกของ European Union (EU) จึงตรากฎหมาย The U.K. Electronic Communications Act 2000 (“ECA”) เพื่อบังคับใช้กับธุรกรรมทางอิเล็กทรอนิกส์เมื่อวันที่ 25 พฤษภาคม 2538 ECA มาตรา 7 (1) บัญญัติให้ลายมือชื่ออิเล็กทรอนิกส์และการรับรองความถูกต้องของลายมือชื่อดังกล่าวโดยบุคคลใดสามารถรับฟังเป็นพยานหลักฐานเกี่ยวข้องกับความถูกต้องแท้จริงและความสมบูรณ์ของการติดต่อสื่อสารหรือข้อมูลที่มีการลงลายมือชื่อดังกล่าวได้

ความถูกต้องแท้จริง หมายถึง ลักษณะบ่งชี้เฉพาะของผู้ทำเอกสาร ความถูกต้องแท้จริงของวัน เวลา และข้อมูลของเอกสารดังกล่าว ตลอดจนเจตนาให้มีผลทางกฎหมาย

ความสมบูรณ์ของข้อมูล หมายถึง ความเป็นไปได้ของการถูกแทรกแซง แก้ไข หรือเปลี่ยนแปลงข้อมูล

โดยหลักแล้ว ECA จะบังคับใช้กับกิจกรรมของผู้ให้บริการข้อมูลและธุรกิจที่เกี่ยวข้องกับ e – commerce ผู้ให้บริการ (service provider) ที่จดทะเบียนจัดตั้งในประเทศสมาชิกใดจะอยู่ภายใต้กฎหมายของประเทศนั้นโดยไม่คำนึงว่าจะดำเนินกิจกรรมนอกประเทศแต่ภายใจประเทศสมาชิกอื่นหรือไม่ (The country of origin principle)

ต่อมาภายใต้ The Directive on a Community Framerwork for Electronic Signatures (“E – Signatures Directive”) สหราชอาณาจักรซึ่งเป็นหนึ่งในประเทศสมาชิกของ EU ได้อนุวรรตกฎหมายของตนตาม E – Signatures Directive โดยตรา The Electronic Signatures Regulations 2000 ( E – Sign Regulations) ซึ่งมีผลบังคับใช้เมื่อวันที่ 8 มีนาคม พ.ศ. 2545

E – Signatures Directive จะมีการแบ่งแยกระหว่างลายมือชื่ออิเล็กทรอนิกส์ “electronic signatures” และลายมือชื่ออิเล็กทรอนิกส์ขั้นสูง “advanced electronic signatures”[59] ซึ่งลายมือชื่ออิเล็กทรอนิกส์ขั้นสูง คือ ลายมือชื่ออิเล็กทรอนิกส์ที่ได้รับการรับรองโดยผู้รับรองอิสระ (a Certification Service Provider) แล้วว่าลายมือชื่ออิเล็กทรอนิกส์ดังกล่าว

---

[59] Council Directive 1999/93/EC, 2000 OJ. (L 13) 5 article 2.

เป็นลายมือชื่อของบุคคลใดบุคคลหนึ่งจริง[60] และสามารถเชื่อมโยงและระบุบุคคลที่มีการลงลายมือชื่อ ตลอดจนเชื่อมโยงกับข้อมูลในลักษณะที่ผู้รับสามารถที่จะตรวจสอบการเปลี่ยนแปลงแก้ไขใด ๆ ถ้าหากมีในเอกสารต้นฉบับที่ส่งมาด้วยได้[61] ดังนั้น จึงห้ามมิให้มีการปฏิบัติที่แตกต่างสำหรับลายมือชื่ออิเล็กทรอนิกส์ขั้นสูง และสามารถรับฟังเป็นพยานหลักฐานในศาลได้[62]

นอกจากนี้ E – Signatures Directive ยังบัญญัติรับรองให้บุคคลตามกฎหมายสามารถเป็นบุคคลที่ลงลายมือชื่อได้ (Legal persons can be signatories)

อย่างไรก็ตาม E – Signatures Regulations ไม่มีบทบัญญัตินิยามที่ระบุถึงเครื่องมือที่สามารถสร้างลายมือชื่อที่เชื่อถือได้ไว้เป็นการเฉพาะ[63]

ดังนั้น แม้ลายมือชื่ออิเล็กทรอนิกส์ขั้นสูงจะสามารถรับฟังเป็นพยานหลักฐานในศาลได้ แต่น้ำหนักความน่าเชื่อถือของพยานหลักฐานที่มีลายมือชื่ออิเล็กทรอนิกส์ขั้นสูงลงไว้จะมีแค่ไหนเพียงใดก็ยังคงอยู่ในดุลพินิจของผู้พิพากษาที่พิจารณาคดีแต่ละคดี และในบางกรณีอาจต้องห้ามมิให้รับฟัง[64]

นอกจากนี้ กฎหมายของสหราชอาณาจักรยังไม่มีบทบัญญัติการรับรู้ถึงการรับรองลายมือชื่อในต่างประเทศหรือการรับรองโดยผู้รับรองอิสระในต่างประเทศ[65] ดังนั้น การรับรองลายมือชื่อในต่างประเทศอาจต้องห้ามมิให้รับฟังลายมือชื่อนั้นเช่นกัน

---

[60] Council Directive 1999/93/EC, 2000 OJ. (L 13) Annex II.

[61] Council Directive 1999/93/EC, 2000 OJ. (L 13) 5 article 2 (2) (a) – (d). สมาคมผู้ผลิตและให้บริการด้านคอมพิวเตอร์และกลุ่มผู้ดำเนินการด้านอุตสาหกรรมในประเทศสหราชอาณาจักรร่วมมือกันจัดตั้งระบบการรับรองลายมือชื่อหรือระบบ the Scheme ซึ่งภายใต้ระบบดังกล่าวผู้รับรองลายมือชื่ออิสระที่มีการรับรองลายมือชื่อที่เป็นไปตามมาตรฐานที่กำหนดจะได้รับอนุญาตให้สามารถแสดงเครื่องหมายแสดงคุณภาพดังกล่าวได้ โดยการรับรองจะมีการประเมินปีละครั้ง

[62] Council Directive 1999/93/EC, 2000 OJ. (L 13) 7 article 5 (1) (b).

[63] Interdisciplinary Centre for Law & Info. Tech., Katholieke University Leuven, Study for the European Commission: **The Legal and Market Aspects of Electronic Signatures**, 215-16 (2003).

[64] Interdisciplinary Centre for Law & Info. Tech., Katholieke University Leuven, Study for the European Commission: **The Legal and Market Aspects of Electronic Signatures**, 215-16 (2003).

[65] Brazell, above n 119, 133.

โดยรวมการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ในประเทศสหราชอาณาจักรและประเทศสหรัฐมีแนวโน้มผ่อนคลายลงจากหลักเกณฑ์ทั่วไปเช่นเดียวกัน ทั้งไม่มีความเคร่งครัดในการรับฟังต้นฉบับเอกสาร ตลอดจนการรับฟังสัญญาหรือบันทึกซึ่งอยู่ในรูปของอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ ทั้งนี้ เนื่องมาจากตัวพยานอิเล็กทรอนิกส์เองและรูปแบบของการแสดงผลของพยานอิเล็กทรอนิกส์โดยส่วนใหญ่ที่จะทำได้ก็แต่ในรูปของสำเนา เช่น Print out ทั้งในบางกรณียังเป็นการยากหรือไม่สะดวกที่จะนำหรือแสดงต้นฉบับของพยานอิเล็กทรอนิกส์ถึงขนาดที่ให้รับฟัง print out เป็นต้นฉบับในกรณีของสหรัฐ และการไม่ห้ามมิให้รับฟังสำเนาเอกสารของสหราชอาณาจักร รวมไปถึงการส่งเสริมการพาณิชย์อิเล็กทรอนิกส์ ให้สัญญาสามารถดำเนินการได้โดยวิธีการทางอิเล็กทรอนิกส์และการรับรองผลของลายมือชื่ออิเล็กทรอนิกส์ อย่างไรก็ตาม การรับฟังพยานหลักฐานอิเล็กทรอนิกส์ในประเทศสหราชอาณาจักรจะมีความเคร่งครัดมากกว่าในประเทศสหรัฐ เนื่องจากนอกจากผู้จัดทำหรือผู้ที่เกี่ยวข้องกับเอกสารจะต้องสามารถเบิกความยืนยันข้อเท็จจริงในเอกสารแล้ว จะต้องมีผู้ที่มีความคุ้นเคยเกี่ยวกับการทำงานของคอมพิวเตอร์มาเบิกความเป็นพยานต่อศาลด้วย ในขณะที่ประเทศสหรัฐต้องการเพียงแค่ผู้จัดทำหรือผู้ที่เกี่ยวข้องกับเอกสารมาเบิกความยืนยันก็เพียงพอในการที่จะรับฟังเอกสารดังกล่าวแล้ว แต่ทั้งสหรัฐอเมริกาและสหราชอาณาจักรก็ยังไม่มีหน่วยงานที่จะออกมารับรองการทำธุรกรรมทางอิเล็กทรอนิกส์ผ่านทาง e-mail มีเพียงการกำหนดว่าหากมีการฟ้องร้องคดีที่เกี่ยวกับการทำธุรกรรมทางอิเล็กทรอนิกส์สามารถกระทำได้โดยพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์นั้นไม่ต้องห้ามมิให้รับฟัง แต่แต่ละประเทศก็มีการกำหนดวิธีการนำสืบพยานหลักฐานที่แตกต่างกันออกไป และใช้วิธีการกำหนดความหมายของคำว่า “เอกสาร” ให้มีความหมายครอบคลุมมากขึ้น อย่างไรก็ดี การรับฟังพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทยยังคงมีความแตกต่างไปจากทั้งสองประเทศดังกล่าว ทั้งยังมีอุปสรรคที่ต้องปรับปรุงแก้ไขกฎหมายเพื่อก้าวให้ทันการเปลี่ยนแปลงของเทคโนโลยีต่อไป

# บทที่4
# บทวิเคราะห์

จากข้อมูลต่างๆที่ได้กล่าวมาแล้วในบทที่ 2 และบทที่ 3 สามารถพิจารณาได้ว่าการพิสูจน์พยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ในคดีแพ่งของไทยเรานั้นมีเพียงเป็นบทบัญญัติที่เป็นการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน โดยพิจารณาได้จากเมื่อมีการประกาศใช้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. 2544 ตามมาตรา 10 ของพระราชบัญญัติดังกล่าวได้บัญญัติไว้ดังนี้ “ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

(1) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ

(2) สามารถแสดงข้อความนั้นในภายหลังได้

ความถูกต้องของข้อความตาม (1) ให้พิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงใดๆของข้อความ เว้นแต่การรับรองหรือบันทึกเพิ่มเติมซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้นหรือการเปลี่ยนแปลงใดๆที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษาหรือการแสดงข้อความ

ในส่วนของมาตรา 11 ได้บัญญัติห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนกาสรพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใดเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้นให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง ตามพระราชบัญญัติดังกล่าวเท่ากับเป็นการรับรองยืนยันให้รับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน ซึ่งแต่เดิมนั้นศาลมีดุลพินิจที่จะรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานหรือไม่ก็ได้ แต่เมื่อมีพระราชบัญญัติดังกล่าวนี้มาใช้บังคับจึงส่งผลให้มีการยอมรับข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานอีกประเภทหนึ่งที่สามารถสืบพิสูจน์ให้ศาลเห็นในศาลได้ แต่ถึงแม้กฎหมายจะยอมรับให้มีการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในชั้นศาลได้ แต่ก็ต้องมีการนำสืบให้เห็นถึงที่มาของข้อมูลว่ามีการเก็บรักษาอย่างไร มีการประมวลผลอย่างไร มีวิธีการอย่างไร มีความปลอดภัยมากน้อยเพียงใด และมีน้ำหนักน่าเชื่อถือมากน้อยแค่ไหน ซึ่งเป็นเรื่องของวิธีการทางเทคนิคโดยเฉพาะซึ่งวิธีการเหล่านี้ในปัจจุบันได้มีวิธีที่เรียกว่า “วิธีการตรวจพิสูจน์หลักฐานโดยวิธี นิติ

คอมพิวเตอร์” (Computer Forensics) ซึ่งกระบวนการนี้เป็นวิธีการที่เป็นที่ยอมรับในระดับสากล ได้ผ่านการออกแบบเพื่อป้องกันการรั่วไหลของความลับหรือข้อมูล และเป็นการป้องกันมิให้เกิดการเปลี่ยนแปลงใดๆกับข้อมูลที่สามารถใช้เป็นพยานหลักฐานอิเล็กทรอนิกส์ได้ ซึ่งการที่มีวิธีการที่ใช้ในการตรวจพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์นั้นเป็นเรื่องที่ดีที่สามารถสร้างมาตรฐานการพิสูจน์ให้เป็นแบบเดียวกัน และสามารถทำให้ข้อมูลอิเล็กทรอนิกส์ที่นำมาเป็นพยานหลักฐานในศาลนั้นมีความน่าเชื่อถือมากขึ้น แต่วิธีการเหล่านี้ก็ยังเป็นวิธีการที่ยังไม่แพร่หลายนักเพราะยังคงมีการใช้เฉพาะในคดีที่อยู่ในความดูแลของกรมสอบสวนคดีพิเศษ (DSI) หากเราสามารถนำวิธีการในการตรวจพิสูจน์พยานหลักฐานโดยวิธีนิติคอมพิวเตอร์นี้มาเผยแพร่และกำหนดให้เป็นมาตรฐานในการตรวจพิสูจน์พยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ไม่ว่าคดีเหล่านั้นจะอยู่ในความควบคุมดูแลของกรมสอบสวนคดีพิเศษหรือไม่ก็ตาม น่าจะเป็นประโยชน์อย่างกว้างขวางเพราะในปัจจุบันยังมีผู้ที่ไม่รู้เกี่ยวกับกรรมวิธีในการตรวจพิสูจน์พยานหลักฐานของข้อมูลอิเล็กทรอนิกส์อีกเป็นจำนวนมาก หากมีการฟ้องร้องบังคับคดีเกิดขึ้นก็อาจต้องเสียค่าใช้จ่ายเป็นจำนวนมากในการที่จะต้องหาผู้เชี่ยวชาญพิเศษทางด้านนี้มาตรวจพิสูจน์พยานหลักฐาน เพื่อให้พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์นั้นมีความน่าเชื่อถือมากขึ้น ดังนั้นหากเราสร้างบทบัญญัติให้เป็นแม่แบบให้มีมาตรฐานเดียวกันไม่ว่าคดีนั้นจะเป็นคดีอะไรก็ตามไม่ว่าจะเป็นคดีทางแพ่งหรือทางอาญา หากพยานหลักฐานที่ต้องนำสืบหรือนำมาแสดงต่อศาลเป็นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ก็ต้องใช้หลักเกณฑ์และมาตรฐานแบบเดียวกันนี้

ส่วนในเรื่องของการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์นั้น เมื่อศึกษาเปรียบเทียบกับกฎหมายของต่างประเทศทั้งของประเทศสหรัฐอเมริกาและสหราชอาณาจักรแล้วพบว่า บทบัญญัติของกฎหมายต่างประเทศมีแนวทางและวิธีการในการพิสูจน์และรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ที่หลากหลายกว่าประเทศไทย สามารถนำมาเป็นแนวทางในการพัฒนากฎหมายของประเทศไทยในอนาคต รวมถึงวิธีการบางอย่างที่สามารถแก้หรือลดปัญหาการขาดความสามารถในการพิสูจน์ความจริงของคู่ความในคดีที่พิพาทกันได้ เพราะในต่างประเทศทั้งในประเทศสหรัฐอเมริกาและสหราชอาณาจักรได้มีบทบัญญัติแก้ไขหรือเพิ่มเติมบทบัญญัติของกฎหมายฉบับเก่าเพื่อการปรับและนำมาใช้ให้เข้ากับการเปลี่ยนแปลงไปอย่างรวดเร็วของเทคโนโลยีในปัจจุบัน ซึ่งจะสามารถเห็นได้จากบทบัญญัติที่มีเพิ่มเติมเข้ามาเรื่อยๆ และมีการแยกรายละเอียดปลีกย่อยของข้อกฎหมายไม่ว่าจะเป็นการกำหนดหลักเกณฑ์ต่างๆทั้งในเรื่องของ เกณฑ์การรับฟังพยานหลักฐานที่ดีที่สุด เกณฑ์การรับฟังพยานบอกเล่า เกณฑ์การรับรองความถูกต้องแท้จริงของพยานหลักฐาน หรือแม้แต่การออกกฎหมายให้เป็นกฎหมายแม่แบบและให้แต่ละรัฐนำกฎหมายแม่แบบนี้ไปปรับใช้กับรัฐของตนได้ ซึ่งการตราบทบัญญัติเช่นนี้เป็นการตราบทบัญญัติที่ครอบคลุมในรายละเอียดต่างๆ ต่างจากกฎหมายของไทยที่ยังมีปัญหาความไม่แน่นอนของสถานะของพยานหลักฐานอิเล็กทรอนิกส์

เช่น กรณีที่หากถือว่าข้อมูลอิเล็กทรอนิกส์เป็นพยานเอกสาร ก็ต้องนำบทบัญญัติที่เกี่ยวกับพยานเอกสารมาใช้บังคับด้วยเช่น ป.วิ.พ. มาตรา 95 “ห้ามมิให้นำสืบพยานบุคคลแทนหรือแก้ไขเปลี่ยนแปลงพยานเอกสาร ในกรณีที่กฎหมายบังคับให้ต้องมีพยานเอกสารมาแสดง เว้นแต่จะเข้าข้อยกเว้น เช่น ต้นฉบับเอกสารสูญหาย หรือถูกทำลาย หรือถูกปลอมหรือหนี้ตามเอกสารนั้นไม่สมบูรณ์ หรือตีความหมายผิด ซึ่งหากไม่เข้าข้อยกเว้นแล้วจะนำพยานบุคคลมานำสืบประกอบข้อมูลอิเล็กทรอนิกส์นั้นไม่ได้” หรือตามป.วิ.พ. มาตรา 90 เกี่ยวกับการยื่นสำเนาเอกสารต่อศาลและคู่ความอีกฝ่าย ดังนั้น หากข้อมูลอิเล็กทรอนิกส์ถือเป็นพยานเอกสารแล้วคู่ความฝ่ายที่ประสงค์จะอ้างข้อมูลอิเล็กทรอนิกส์ ก็ต้องยื่นสำเนาข้อมูลอิเล็กทรอนิกส์ต่อศาลและคู่ความอีกฝ่ายหนึ่งด้วย

ถึงแม้ว่าพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 8 ของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 บัญญัติว่าภายใต้บังคับบทบัญญัติแห่งมาตรา 9 ในกรณีที่ใช้กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ หรือมีเอกสารมาแสดงแล้วจะถือว่าข้อมูลอิเล็กทรอนิกส์ที่จัดทำขึ้นในรูปแบบที่สามารถเข้าถึงและนำกลับมาใช้ใหม่ได้โดยความหมายไม่เปลี่ยนแปลง จะถือว่าข้อความนั้นได้ทำเป็นหนังสือหรือมีหลักฐานเป็นหนังสือหรือมีเอกสารมาแสดงแล้ว แต่ก็ยังไม่ได้เป็นบทบัญญัติว่าข้อมูลอิเล็กทรอนิกส์ดังกล่าวถือเป็นพยานเอกสารทุกกรณี และตามมาตรา 8 แห่งพระราชบัญญัติฉบับนี้ กำหนดให้การทำหนังสือ หลักฐานเป็นหนังสือ และกรณีที่ต้องมีเอกสารมาแสดง สามารถทำในรูปอิเล็กทรอนิกส์ได้ หากสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ซึ่งคำว่า “สามารถเข้าถึงได้” นั้นหมายความรวมถึงข้อความที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ที่สามารถอ่านออกและอธิบายได้โดยใช้โปรแกรมหรือซอฟต์แวร์และรวมถึงข้อมูลอิเล็กทรอนิกส์ที่จำเป็นต้องแปลงข้อมูลนั้นให้สามารถอ่านเข้าใจได้ด้วย ส่วนคำว่า “นำกลับมาใช้ได้” นั้น หมายถึง มนุษย์เป็นผู้ใช้และยังรวมถึงการใช้โดยการประมวลผลด้วยเครื่องคอมพิวเตอร์ด้วย และคำว่า “โดยความหมายไม่เปลี่ยนแปลง” นั้น หมายถึง ต้องมีลักษณะถาวร ไม่มีการแก้ไขเปลี่ยนแปลง กล่าวคือ ข้อมูลอิเล็กทรอนิกส์นั้นต้องไม่ได้สร้างขึ้นโดยใช้มาตรฐานที่ต่ำเกินไป เหตุผลสำคัญ ที่ต้องกำหนดเงื่อนไขให้สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลงนั้น ก็เพราะว่าเทคโนโลยีที่ใช้ในการสร้างข้อมูลอิเล็กทรอนิกส์กับเทคโนโลยีที่ใช้ในการอ่านหรือใช้ข้อมูลอิเล็กทรอนิกส์นั้น อาจมีความแตกต่างกัน ทำให้ไม่สามารถอ่านหรือแปลงข้อมูลได้ถูกต้องตรงกัน

ส่วนในประเทศสหรัฐอเมริกา บทบัญญัติของFRE ข้อ 1001 กำหนดให้คู่ความต้องเปิดเผยข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องกับประเด็นในคดีที่อยู่ในความครอบครองของตนโดยต้องอยู่ภายใต้ Federal Rule of Civil Procedure ข้อ26 ซึ่งเป็นบทบัญญัติที่ใช้ในการ

วินิจฉัยแนวโน้มความเกี่ยวข้องของเอกสารที่ถูกขอให้เปิดเผยกับภาระของคู่ความที่ถูกขอเช่นนั้น ซึ่งการเปิดเผยข้อมูลดังกล่าวจะสอดคล้องกับหน้าที่ในการเก็บรักษาเอกสารรวมทั้งข้อมูลอิเล็กทรอนิกส์ภายใต้หลักกฎหมายคอมมอนลอว์คู่ความมีหน้าที่เก็บรักษาเอกสารเมื่อมีการเริ่มคดีโดยเก็บรักษาเอกสารเท่าที่เกี่ยวข้องภายใต้หลักความสุจริตและสามารถทำได้อย่างมีเหตุผล นอกจากนี้ยังมีการกำหนดนิยามของคำว่า “เอกสารและบันทึก” ลงใน FRE ให้รวมไปถึงคอมพิวเตอร์ ระบบการถ่ายภาพ และเทคโนโลยีใหม่อื่นๆ จึงส่งผลให้บทบัญญัติเกี่ยวกับพยานเอกสารต่างๆจะสามารถนำไปใช้บังคับกับพยานหลักฐานอิเล็กทรอนิกส์อันเกิดจากคอมพิวเตอร์หรือเทคโนโลยีสมัยใหม่อื่นๆได้ด้วย โดยจะไม่ก่อให้เกิดความไม่แน่นอนของสถานะของข้อมูลอิเล็กทรอนิกส์ หรือแม้แต่ประเทศสหราชอาณาจักรก็ยังกำหนดนิยามที่ชัดเจนเกี่ยวกับพยานเอกสารไว้ใน The Civil Procedure Rules 1998 Part 31.4 ที่บัญญัติว่า เอกสาร หมายถึง สิ่งใดๆซึ่งข้อมูลไม่ว่าในรูปแบบใดๆถูกบันทึกไว้ ดังนั้นเอกสารจึงหมายความรวมถึง e-mail รูปถ่าย สื่อ หรือสิ่งบันทึกภาพหรือเสียง ตลอดจนข้อมูลที่เกี่ยวข้องที่ถูกเก็บไว้ใน hard drive ของคอมพิวเตอร์หรือดิสก์ด้วย ดังนั้นบทบัญญัติของพยานเอกสารจึงนำมาใช้กับพยานอิเล็กทรอนิกส์ได้ด้วย

จากปัญหาดังกล่าวในส่วนของทั้งคดีแพ่งและคดีอาญาภายใต้กฎหมายของไทยจะสามารถแก้ไขได้โดยการเพิ่มให้คำนิยามของคำว่า “เอกสาร” ให้ชัดเจนมากขึ้นเพื่อจะได้ไม่ก่อให้เกิดการตีความว่าพยานอิเล็กทรอนิกส์ถือเป็นพยานเอกสารหรือไม่

ส่วนในเรื่องของ print out หรือดิสก์ หรือ back up ไฟล์จะถือว่าเป็นต้นฉบับหรือสำเนานั้น ตาม พ.ร.บ. ธุรกรรม มาตรา 11 วรรคแรก“ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์” แต่ก็มิได้ห้ามมิให้ปฏิเสธการรับฟังเพราะเหตุอื่น เช่น ข้อมูลอิเล็กทรอนิกส์ดังกล่าวถือเป็นสำเนาเอกสาร แต่ตามป.วิ.พ. มาตรา 93 มีข้อบัญญัติให้การรับฟังเอกสารเป็นพยานหลักฐานนั้น ให้ยอมรับฟังได้แต่ต้นฉบับเอกสารเท่านั้น เว้นแต่จะเข้าข้อยกเว้นทั้ง 3 ประการที่ได้บัญญัติไว้ แต่อย่างไรก็ตามแม้มีข้อยกเว้นทั้ง 3 ประการ แต่เนื่องจากยังคงมีความไม่แน่นอนว่า print out หรือ ดิสก์ หรือ back up ไฟล์ จะถือว่าเป็นพยานหลักฐานที่เป็นต้นฉบับหรือสำเนา จึงทำให้กรณีที่คู่ความอ้าง print out หรือ ดิสก์ หรือ back up ไฟล์ จะถือเป็นกรณีที่หาต้นฉบับไม่ได้หรือไม่ และถือเป็นสำเนามานำสืบหรือไม่ หรือคู่ความอีกฝ่ายสามารถคัดค้านว่า print out หรือ ดิสก์ หรือ back up ไฟล์ ไม่ถูกต้องตรงกับต้นฉบับได้หรือไม่

ซึ่งกรณีเหล่านี้แตกต่างจากบทบัญญัติกฎหมายของประเทศสหรัฐอเมริกาที่ถือว่า print out หรือผลผลิตใดๆจากคอมพิวเตอร์ถือว่าเป็นต้นฉบับเอกสาร หรือในกรณีของสหราชอาณาจักรที่ไม่ห้ามมิให้รับฟังสำเนาเอกสาร จึงไม่ต้องมีกรณีที่ต้องวินิจฉัยว่าเอกสารนี้เป็นต้นฉบับหรือสำเนา

กรณีของการแปลงเอกสารเก่าให้อยู่ในรูปของสื่ออื่นๆที่ทนทานและทำซ้ำได้ เป็นกรณีที่พ.ร.บ. ธุรกรรมมีการจำกัดรูปแบบในการแปลงเอกสาร เนื่องจากมาตรา 10 และมาตรา 12[1]ของพ.ร.บ.ธุรกรรมไม่สามารถครอบคลุมกรณีที่มีการจัดเก็บเอกสารในรูปของสื่ออื่นๆที่ทนทานและทำซ้ำได้ เช่นภาพถ่ายหรือไมโครฟิล์ม เนื่องจากกรณีนี้ไม่ถือเป็นข้อมูลอิเล็กทรอนิกส์ตามความหมายในมาตรา 4 แห่งพ.ร.บ. ธุรกรรม ดังนั้นในกรณีนี้การจัดเก็บเอกสารโดยวิธีนี้จึงไม่ถือว่ามีการจัดเก็บเอกสารตามที่กฎหมายกำหนด แต่อย่างไรก็ตามกรณีของการสแกนเอกสารเก่าและแปลงให้อยู่ในรูปของข้อมูลดิจิทัลในเครื่องคอมพิวเตอร์ อยู่ในนิยามความหมายของมาตรา 10 และมาตรา 12 ของพ.ร.บ. ธุรกรรม แต่การที่กำหนดให้ หากสิ่งพิมพ์ออกนั้นมีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์ และมีการรับรองสิ่งพิมพ์ออกโดยหน่วยงานที่มีอำนาจตามที่คณะกรรมการประกาศกำหนดแล้ว ให้ถือว่าสิ่งพิมพ์ออกดังกล่าวใช้แทนต้นฉบับได้นั้น หากเป็นการโต้ตอบกันทางจดหมายอิเล็กทรอนิกส์ (e-mail) เช่นนี้จะให้หน่วยงานใดมากำกับดูแลและมีอำนาจรับรองข้อความดังกล่าวตามที่กฎหมายกำหนด และในส่วนของมาตรา 12/1 ของพ.ร.บ. ธุรกรรมบัญญัติให้นำ บทบัญญัติในมาตรา 10 มาตรา 11 และมาตรา 12 มาใช้บังคับกับเอกสารหรือข้อความที่ได้มีการจัดทำหรือแปลงให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ในภายหลังด้วยวิธีการทางอิเล็กทรอนิกส์และการเก็บรักษาเอกสารและข้อความดังกล่าวด้วยโดยอนุโลม การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ตามวรรคหนึ่งให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด นั้นวิธีการเก็บรักษาข้อมูลอิเล็กทรอนิกส์ตามกฎหมายไม่ได้ระบุวิธีการตลอดจนวิธีพิสูจน์ทราบความถูกต้องแท้จริงไว้ว่าอย่างไร เรื่องนี้ยังไม่มีความชัดเจน

หรือกรณีที่มีการนำสืบเอกสารที่ทำซ้ำจากสื่อที่แปลงมาจากเอกสารเก่า เอกสารดังกล่าวน่าจะถือว่าเป็นสำเนาของสำเนา ซึ่งอาจต้องห้ามมิให้รับฟังตาม ป.วิ.พ.ตามมาตรา 93 เว้นแต่จะเข้าข้อยกเว้นตามกฎหมาย ซึ่งกรณีนี้อาจไม่เข้าข้อยกเว้น เนื่องจากไม่อาจถือว่าต้นฉบับสูญหายหรือถูกทำลายโดยเหตุสุดวิสัย แต่ก็อาจถือได้ว่าเป็นกรณีที่ไม่สามารถนำต้นฉบับมาสืบได้โดยประการอื่น หรืออาจถือว่าเป็นพยานหลักฐานอันเป็นประเด็นข้อสำคัญในคดีตามป.วิ.พ. มาตรา86 วรรคสามซึ่งศาลเห็นว่าเพื่อประโยชน์แห่งความยุติธรรมแล้วควรนำสืบพยานหลักฐานดังกล่าว แต่หากไม่ใช่แล้วก็ต้องห้ามมิให้รับฟัง และหากก่อให้เกิดข้อได้เปรียบเสียเปรียบกันแล้วศาลก็จะไม่อนุญาตให้รับฟังเอกสารดังกล่าวเช่นกัน

---

[1] ดูรายละเอียดของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้ที่ภาคผนวก ฉ

แต่ในกรณีของประเทศสหรัฐอเมริกา The Uniform Act ได้บัญญัติกรณีของบันทึกที่กฎหมายกำหนดให้ต้องมีการเก็บรักษา หากมีการทำซ้ำโดยวิธีถ่ายภาพ หรือถ่ายไมโครฟิล์มหรือวิธีการอื่นใดที่เป็นไปตามมาตรฐานที่ผู้จัดเก็บบันทึกเอกสารกำหนด การจัดเก็บดังกล่าวถือได้ว่ามีการจัดเก็บอย่างต้นฉบับเอกสารแล้ว และวัตถุจากการทำซ้ำดังกล่าวจะมีสถานะทางกฎหมายเช่นเดียวกับต้นฉบับ สำเนาของวัตถุที่มีการทำซ้ำดังกล่าวหากมีการประทับตราหรือรับรองโดยผู้จัดเก็บบันทึกเอกสารสำเนาดังกล่าวจะสามารถรับฟังเป็นพยานหลักฐานได้เช่นเดียวกับต้นฉบับของวัตถุนั้น

ในกรณีของสหราชอาณาจักรได้บัญญัติให้ผู้กล่าวอ้างต้องนำผู้จัดทำเอกสารมาเบิกความยืนยันข้อเท็จจริงในเอกสาร และนำผู้ที่มีความคุ้นเคยเกี่ยวกับการทำงานของคอมพิวเตอร์หรือเครื่องมือในการแปลงเอกสารมาเบิกความเป็นพยานต่อศาลด้วย โดยผู้กล่าวอ้างต้องสามารถพิสูจน์ได้ถึงวิธีการจัดทำเอกสาร และสามารถรับรองความถูกต้องแท้จริงโดยวิธีที่ศาลเห็นชอบ ตาม The Civil Evidence Act 1995

ส่วนกฎหมายของประเทศไทยแม้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544จะมาจากกฎหมายแม่แบบของ UNCITRAL แต่เมื่อมีการพิจารณาคดีขึ้นสู่ศาลผู้พิพากษาอาจจะต้องมีความรู้เฉพาะทางในด้านการตรวจพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์นี้ด้วย เพราะพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์นี้ยากที่จะพิสูจน์หาความจริง เพราะพยานหลักฐานชนิดนี้เป็นพยานหลักฐานที่อาจถูกเปลี่ยนแปลงแก้ไขข้อมูลอาจถูกลบหรือซ่อนหลักฐานที่มีความสำคัญต่อรูปคดีได้ง่าย หากเรามีบทบัญญัติในเรื่องวิธีการพิสูจน์ การนำสืบและการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานก็จะเป็นประโยชน์อย่างยิ่ง ซึ่งวิธีการที่หลากหลายจะเป็นการให้โอกาสแก่คู่ความในการพิสูจน์ความจริง โดยอาจมีแนวทางได้ดังนี้

(1) การกำหนดหลักเกณฑ์ในการนำสืบความน่าเชื่อถือของข้อมูลอิเล็กทรอนิกส์
(2) การรับรองความถูกต้องโดยการตรวจสอบของศาล
(3) การมีกระบวนการรับรอง
(4) การพิสูจน์หรือการรับรองความถูกต้องโดยคู่ความฝ่ายที่อ้าง
(5) การมีข้อสันนิษฐานโดยกฎหมาย

โดยเฉพาะการมีกระบวนการรับรอง (Approved Process) ต้องเป็นการรับรองโดยบุคคลหรือองค์กรที่ได้รับการแต่งตั้งโดยจะอยู่ในรูปของใบรับรองที่ลงนามโดยบุคคลที่มีตำแหน่งหน้าที่รับผิดชอบที่เกี่ยวกับการปฏิบัติการหรือผู้บริหารของผู้ประกอบการรับรอง (Certifying Authority) และมีวัตถุประสงค์เพื่อให้ความเห็นชอบด้วยกับกระบวนการรับรองดังกล่าว และผลของข้อมูลอิเล็กทรอนิกส์ที่ผ่านกระบวนการรับรองคือ กฎหมายสันนิษฐานไว้ก่อนว่าถูกต้องแท้จริง เว้นแต่จะพิสูจน์ให้เห็นเป็นอย่างอื่น โดยวิธีการรับรองความถูกต้องแท้จริง

ต้องมีกระบวนการเก็บรักษา โดยให้มีขั้นตอนต่าง ๆเพื่อความน่าเชื่อถือและสามารถมั่นใจได้ว่าข้อมูลทั้งหมดมีความถูกต้องแท้จริง โดยอาจมีขั้นตอนต่าง ๆดังนี้ เช่น

- การมีมาตรการการป้องกันการเข้าถึงข้อมูลของบุคคลที่ไม่มีอำนาจ
- การมีอุปกรณ์ที่ได้มาตรฐานในการป้องกันรักษาความปลอดภัยที่เกี่ยวกับการเปลี่ยนแปลงแก้ไขข้อมูลโดยผู้ที่ไม่มีอำนาจ
- การจัดให้มีระบบฐานข้อมูลสำรอง และมีระบบการกู้คืนอย่างมีประสิทธิภาพ
- การเพิ่มเติมในเอกสารต้องไม่แตกต่างไปจากข้อมูลต้นฉบับ
- ข้อมูล (out put) ต้องถูกรักษาความปลอดภัย
- การเก็บรักษาข้อมูลอิเล็กทรอนิกส์ต้องสามารถเก็บรักษาข้อมูลไว้ได้ทั้งหมด เป็นต้น

ดังนั้นในการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานจึงมีความจำเป็นที่ต้องมีบทบัญญัติที่เป็นรายละเอียดต่าง ๆเพิ่มเติม เพื่อจะได้เป็นประโยชน์ในการสู้คดีและการพิจารณาในศาลต่อไป

# บทที่ 5
# บทสรุปและข้อเสนอแนะ

## 5.1 บทสรุป

แม้ในโลกของเทคโนโลยีจะมีการเปลี่ยนแปลงไปตลอดเวลา แต่คนที่คิดหาประโยชน์ในทางมิชอบจากเทคโนโลยีก็มีการพัฒนาวิธีการให้ทันสมัยมากขึ้นตลอด ดังนั้นจึงเป็นเรื่องที่ต้องระวังและเน้นด้านความปลอดภัย เพราะอาจมีการเจาะข้อมูล ทำลายข้อมูล การเข้าไปล่วงรู้รหัสส่วนบุคคล หรือกุญแจลายมือชื่อส่วนบุคคล โดยเฉพาะในส่วนของข้อมูลอิเล็กทรอนิกส์ที่เรามีความจำเป็นต้องเน้นในด้านการรักษาความปลอดภัยและต้องสร้างระบบขึ้นเพื่อป้องกันการเข้าถึงข้อมูล ต้องมีการป้องกันในเชิงกายภาพ มีการป้องกันด้านsoftware มีการออกแบบระบบให้ส่วนใดสามารถเข้าถึงได้ส่วนใดเข้าถึงไม่ได้ ตลอดจนต้องมีการจัดเก็บรวบรวบรวมข้อมูลสำรองไว้ในที่ที่ปลอดภัย หรือมี Back up files ข้อมูลต่างๆ ส่วนในด้านของกฎหมายหากเกิดกรณีพิพาทก็ต้องมีการนำสืบพยานหลักฐาน ตลอดจนต้องพิสูจน์หาข้อเท็จจริงต่างๆที่เป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งอาจต้องหาผู้เชี่ยวชาญเฉพาะทางมาสืบให้ศาลเห็นถึงความเป็นไปของข้อมูลอิเล็กทรอนิกส์นั้น ส่วนในเรื่องของการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานนั้น ประเทศไทยเราก็มีพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. 2544 และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) แก้ไขเพิ่มเติมพ.ศ. 2551 ที่มีต้นแบบมาจากกฎหมายแม่แบบว่าด้วยพาณิชย์อิเล็กทรอนิกส์ของคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติ (United Nations Commission on International Trade Law หรือ UNCITRAL) ที่ได้ผนวกรวมเอากฎหมายแม่แบบทั้ง 2 ฉบับของ UNCITRAL คือ UNCITRAL Model Law On Electronic Commerce 1996 และ UNCITRAL Model Law On Electronic Signatures 2001 ออกมาเป็นพระราชบัญญัติฉบับนี้ แต่จากสถานะที่ไม่แน่นอนของพยานหลักฐานอิเล็กทรอนิกส์และผลผลิตจากพยานหลักฐานอิเล็กทรอนิกส์ภายใต้กฎหมายเกี่ยวกับพยานหลักฐานของประเทศไทย ตลอดจนความแตกต่างในการรับฟังพยานหลักฐานระหว่างเอกสารต้นฉบับที่ถูกแปลงกับเอกสารที่แปลง หรือเอกสารต้นฉบับที่ถูกแปลงกับผลผลิตจากข้อมูลอิเล็กทรอนิกส์หรือผลผลิตจากเอกสารที่แปลงก่อให้เกิดอุปสรรคและความไม่มั่นใจในการพัฒนาและการนำเทคโนโลยีสมัยใหม่มาใช้เพื่อลดต้นทุนในการผลิตและการจัดเก็บข้อมูล ตลอดจนความเชื่อมต่อและความง่ายต่อการจัดเก็บและการสืบค้นข้อมูล ในปัจจุบันไม่ว่าจะเป็นการจัดทำเอกสารให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์หรือการแปลงเอกสารเก่าให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ซึ่งในเรื่องนี้เป็นเรื่องของการตรวจพิสูจน์พยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ เราก็มีวิธีการตรวจพิสูจน์ทางนิติคอมพิวเตอร์(Computer Forensics) ที่เป็นมาตรฐานที่เป็นที่ยอมรับเป็นสากล แต่ก็ยังไม่มีการบัญญัติถึงวิธีการเหล่านี้ลงไปในตัวบทกฎหมาย รวมทั้งในเรื่องของสถานะของพยานหลักฐานของข้อมูลอิเล็กทรอนิกส์หากจัดว่าข้อมูลอิเล็กทรอนิกส์เป็นพยานเอกสาร ต้องมีบทบัญญัติที่แน่นอนในส่วนของนิยามของข้อมูลมูลอิเล็กทรอนิกส์ให้กว้างขวาง

ครอบคลุมมากขึ้นในบทบัญญัติของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งวิธีการเก็บรักษาข้อมูลอิเล็กทรอนิกส์ และหน่วยงานที่จะรับรองความถูกต้องแท้จริงของข้อมูลอิเล็กทรอนิกส์ที่ยังไม่มีความชัดเจน

**5.2 ข้อเสนอแนะ**

แม้ว่าประเทศไทยจะมีพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. 2544 และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) แก้ไขเพิ่มเติม ที่นำมาจากกฎหมายแม่แบบของ UNCITRAL แล้วแต่กฎหมายของเราก็ยังไม่มีความชัดเจนเกี่ยวกับการกำหนดหลักเกณฑ์ในการนำสืบความน่าเชื่อถือของข้อมูลอิเล็กทรอนิกส์ จึงควรกำหนดให้มีกระบวนการดังต่อไปนี้

(1) การรับรองความถูกต้องโดยการตรวจสอบของศาล

(2) การมีกระบวนการรับรอง

(3) การพิสูจน์หรือการรับรองความถูกต้องโดยคู่ความฝ่ายที่อ้าง

(4) การมีข้อสันนิษฐานโดยกฎหมาย

(5) การกำหนดวิธีการนำสืบ

ซึ่งหลักเกณฑ์ต่างๆเหล่านี้มีในกฎหมายของต่างประเทศ รวมทั้งวิธีการพิสูจน์พยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ (Computer Forensics) ที่ควรจะมีเป็นบทบัญญัติเป็นหลักเกณฑ์ที่แน่นอน ที่สามารถใช้พิสูจน์พยานหลักฐานของข้อมูลอิเล็กทรอนิกส์ได้ทั้งในคดีแพ่งและคดีอาญา ซึ่งกระบวนการนี้เป็นวิธีการที่เป็นที่ยอมรับในระดับสากล ได้ผ่านการออกแบบเพื่อป้องกันการรั่วไหลของความลับหรือข้อมูล และเป็นการป้องกันมิให้เกิดการเปลี่ยนแปลงใดๆ กับข้อมูลที่สามารถใช้เป็นพยานหลักฐานอิเล็กทรอนิกส์ได้

นอกจากนี้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ควรกำหนดเพิ่มเติมรวมถึง การโต้ตอบกันทางจดหมายอิเล็กทรอนิกส์ (e-mail) เช่นนี้จะให้หน่วยงานใดมากำกับดูแลและมีอำนาจรับรองข้อความดังกล่าวตามที่กฎหมายกำหนด ซึ่งในส่วนนี้ข้าพเจ้าเห็นควรให้ กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์มากำกับดูแลในเรื่องของสัญญาซื้อขายและการรับรองข้อมูลที่มีการโต้ตอบกันในส่วนของกรณีที่มีการทำพาณิชย์อิเล็กทรอนิกส์หรือการทำธุรกรรมทางอิเล็กทรอนิกส์ เช่นเดียวกับมาตรการในเรื่องของการรับรองลายมือชื่ออิเล็กทรอนิกส์ โดยกรมพัฒนาธุรกิจการค้าอาจเป็นผู้รับรองได้โดยมีวิธีการที่กำหนดให้การทำสัญญาต้องใช้แบบที่ร่างโดยกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ และสามารถเข้ามากรอกใน web site ของกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ โดยในสัญญาฉบับนี้หากผู้ซื้อหรือผู้ขายต้องการที่จะกำหนดรายละเอียดเพิ่มเติมในเรื่องของสัญญา ก็สามารถกรอกหรือระบุรายละเอียดต่างๆเพิ่มเติมลงไปได้ในร่างสัญญา โดยอาจใช้เป็นหมาย

เหตุเพิ่มเติมท้ายข้อสัญญา แล้วให้เจ้าหน้าที่ผู้มีหน้าที่กำกับดูแลเรื่องนี้เป็นผู้ลงนามรับรองความถูกต้องของข้อสัญญาที่ได้จัดทำขึ้น

หรือหากไม่ให้การรับรองโดยกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ทางกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ก็อาจกำหนดให้มีหน่วยงานเอกชนมาเป็นผู้ทำหน้าที่ในการรับรองแทน โดยอาจมีการกำหนดคุณสมบัติการเป็นผู้อนุญาต ให้เป็นหน่วยงานรับรองความถูกต้องแท้จริงของข้อมูลอิเล็กทรอนิกส์ของผู้ประกอบการค้าพาณิชย์ทางอิเล็กทรอนิกส์ ให้หน่วยงานเอกชนนั้นเป็นหน่วยงานที่มีอำนาจรับรองในการทำสัญญา และต้องมีการสร้างแบบร่างของสัญญาให้เป็นมาตรฐานแบบเดียวกัน และมีการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไปจนกว่าจะถึงการสิ้นสุดของสัญญา หรือมีการส่งมอบสินค้าเป็นที่เรียบร้อย และต้องมีการทำสำเนาโดยอาจทำเป็นแผ่น disk หรือ print out ออกมาและให้คู่สัญญาทั้ง 2 ฝ่าย คือฝ่ายผู้ซื้อและผู้ขายเก็บรักษาไว้คนละฉบับ และที่ตัวหน่วยงานเอกชนที่เป็นผู้รับรองความถูกต้องของสัญญาที่เป็นข้อมูลอิเล็กทรอนิกส์อีกหนึ่งฉบับ โดยทั้งนี้ต้องอยู่ภายใต้การกำกับควบคุมดูแลของกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ เพื่อความสะดวกต่อการควบคุมดูแลในการให้ใบอนุญาตหน่วยงานเอกชนที่ให้การรับรองการทำสัญญาทาง e-mail หรือการเพิกถอนใบอนุญาตผู้ประกอบการรับรองที่เป็นหน่วยงานเอกชนนั้น หากขาดคุณสมบัติการเป็นผู้รับรอง โดยมาตรฐานการเป็นผู้รับรองนั้นต้องมีมาตรฐานในการรับรองเป็นแบบเดียวกัน เช่น การมีกระบวนการรับรอง การสร้าง การเก็บรักษาข้อมูลอิเล็กทรอนิกส์ เป็นต้น และกฎหมายก็ควรกำหนดข้อสันนิษฐานให้ถือว่าถูกต้องหากข้อมูลอิเล็กทรอนิกส์ได้ผ่านกระบวนการรับรองจากหน่วยงานผู้มีอำนาจที่เป็นผู้รับรอง เว้นแต่จะพิสูจน์ให้เห็นเป็นอย่างอื่น

การกำหนดให้มีกระบวนการรับรองความถูกต้องแท้จริงของข้อมูลอิเล็กทรอนิกส์นี้ จะทำให้เกิดความสะดวกแก่คู่ความทั้ง 2 ฝ่ายที่ต้องการอ้างข้อมูลอิเล็กทรอนิกส์มาเป็นพยานหลักฐาน เพราะเท่ากับเป็นการทำให้มีบุคคลภายนอกมาตรวจสอบและรับรองความถูกต้องแท้จริงของข้อมูลอิเล็กทรอนิกส์ให้

รวมทั้งวิธีการเก็บรักษาตลอดจนวิธีการพิสูจน์ทราบความถูกต้องแท้จริงของข้อมูลอิเล็กทรอนิกส์ที่จะใช้เป็นพยานหลักฐานก็ควรมีการกำหนดระบุลงไปเป็นบทบัญญัติและวิธีการที่แน่นอนตายตัวว่าควรมีวิธีการอย่างไร เช่นการเก็บรักษาควรเก็บในสื่อ (Media) ที่สามารถรักษาความถูกต้องแท้จริง (Integrity) และสามารถระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้ และควรมีระบบเก็บรักษาความลับของข้อมูลที่จัดเก็บ และมีการกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่นการทำ Data Archiving หรือ การเก็บไว้ใน Centralized log Sever หรือการทำ Data Hashing เว้นแต่ให้ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือ

ผู้บริหารองค์กรกำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย และให้รวมถึงพนักงานเจ้าหน้าที่ของรัฐ

หรือหากมีข้อพิพาทที่เกี่ยวกับการพิสูจน์ความถูกต้องแท้จริงของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ข้าพเจ้าเห็นว่าอาจนำวิธีการของการตรวจพิสูจน์หลักฐานโดยนิติวิธี (computer forensics) มาเป็นมาตรฐานในการใช้ตรวจพิสูจน์หลักฐานให้เป็นมาตรฐานเดียวกัน

ในเรื่องของ print out หรือ ดิสก์ หรือ back up ไฟล์ จะถือเป็นต้นฉบับหรือสำเนายังไม่มีความแน่นอน ต่างจากบทบัญญัติของประเทศสหรัฐอเมริกาและสหราชอาณาจักรที่ระบุไว้ว่าให้ถือว่า print out หรือผลผลิตใดๆจากคอมพิวเตอร์ถือเป็นต้นฉบับเอกสาร ซึ่งสิ่งเหล่านี้อาจแก้ปัญหาด้วยการให้นิยามของข้อมูลอิเล็กทรอนิกส์ให้ครอบคลุมเช่นเดียวกับประเทศสหรัฐอเมริกาและสหราชอาณาจักรที่ได้กำหนดนิยามของ พยานหลักฐานอิเล็กทรอนิกส์ที่ประกอบด้วย ตัวอักษร คำ ตัวเลข ภาพวาด กราฟ แผนภาพ รูปถ่าย บันทึกเสียง หรือสิ่งที่เทียบเท่าที่ทำให้มีขึ้นโดยการเขียน การพิมพ์ดีด การพิมพ์ การถ่ายเอกสาร การถ่ายภาพ การกระตุ้นของแม่เหล็ก การบันทึกด้วยเครื่องมือกล หรือเครื่องไฟฟ้า หรือการรวบรวมข้อมูลในรูปแบบอื่นจะถือเป็นพยานเอกสาร บทบัญญัติเกี่ยวกับพยานเอกสารต่างๆ ก็จะนำไปใช้บังคับกับพยานหลักฐานอิเล็กทรอนิกส์ในกรณีดังกล่าวด้วยจึงไม่ก่อให้เกิดความไม่แน่นอนว่าข้อมูลอิเล็กทรอนิกส์อันเกิดขึ้นจากคอมพิวเตอร์ หรือเทคโนโลยีสมัยใหม่อื่นๆ และควรระบุว่าความแตกต่างระหว่างสำเนาและต้นฉบับจะไม่ใช่สาระสำคัญในการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

นอกจากนี้ควรจัดให้มีผู้เชี่ยวชาญทางการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ โดยผู้เชี่ยวชาญนี้ควรเป็นผู้ที่มีหน่วยงานของรัฐรับรองและต้องเป็นหน่วยงานที่เป็นองค์กรส่วนกลางในการพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งไม่ว่าโจทก์หรือจำเลยหากจะนำพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์มานำสืบพิสูจน์ต่อศาล ต้องให้ผู้เชี่ยวชาญที่เป็นผู้พิสูจน์พยานหลักฐานส่วนกลางเป็นผู้ตรวจพิสูจน์ ซึ่งจะทำให้เกิดความเป็นกลางและได้มาตรฐานในการตรวจพิสูจน์

อย่างไรก็ตามแม้โดยรวมแล้วการปรับปรุงตัวบทกฎหมายที่เกี่ยวข้องจะสามารถแก้ไขปัญหาส่วนใหญ่ที่อาจเกิดขึ้นได้ และการปรับแก้ตัวบทกฎหมายที่เกี่ยวข้องก็จำเป็นต่อการพัฒนาและส่งเสริมการนำเอกสารอิเล็กทรอนิกส์มาใช้แทนเอกสารกระดาษก็ตาม

แต่เนื่องจากเทคโนโลยีโดยส่วนใหญ่จะเปลี่ยนแปลงไปอย่างรวดเร็ว จึงเป็นการยากที่จะสามารถบัญญัติกฎหมายที่จะสามารถครอบคลุมและบังคับใช้กับเทคโนโลยีใหม่ๆ ได้ทันและสมบูรณ์ในทุกกรณีดังจะเห็นได้จากในกรณีของประเทศสหรัฐหรือประเทศสหราชอาณาจักรอันเป็นประเทศที่ส่งเสริมและพัฒนาการใช้ข้อมูลอิเล็กทรอนิกส์อย่างกว้างขวางเองก็ยังคงมีความพยายามที่จะแก้ไขเพิ่มเติมและปรับปรุงตัวบทกฎหมายอยู่เรื่อยๆ เพื่อให้ทันกับความก้าวหน้าทางเทคโนโลยีดังนั้น ลำพังเพียงการแก้ไขตัวบทกฎหมายที่ใช้บังคับอยู่ในปัจจุบันจึงไม่เพียงพอที่จะแก้ไขปัญหาที่เกิดขึ้นหรืออาจเกิดขึ้นทั้งหมดได้ แต่จะต้องมีการปรับเปลี่ยนกฎหมายให้ทันสมัยอยู่เสมอเพื่อแก้ไขปัญหาที่เกิดขึ้นหรืออาจเกิดขึ้นควบคู่ไปกับการส่งเสริมให้เกิดความรู้ความเข้าใจในเทคโนโลยีและกฎหมายที่เกี่ยวข้องต่อไป

ยิ่งไปกว่านั้นปัญหาทางด้านกฎหมายก็มิใช่ปัจจัยหลักแต่เพียงประการเดียวที่เป็นอุปสรรคในการพัฒนาและการส่งเสริมการนำเทคโนโลยีมาใช้ในการจัดเก็บเอกสาร ความน่าเชื่อถือของข้อมูลอิเล็กทรอนิกส์ซึ่งขึ้นอยู่กับปัจจัยทางด้านวิศวกรรมหรือระบบความปลอดภัยของเอกสารหรือการบริหารการจัดเก็บเอกสาร ตลอดจนความพร้อมของผู้ที่เกี่ยวข้องก็ส่งผลต่อการปรับเปลี่ยนนำเทคโนโลยีสมัยใหม่มาใช้ในการจัดเก็บเอกสารเช่นกัน

นอกจากนี้ แม้วิวัฒนาการที่ไม่หยุดยั้งในปัจจุบันทำให้ไม่อาจปฏิเสธความก้าวหน้าทางด้านเทคโนโลยีในทุก ๆ ด้าน แต่เนื่องจากความไม่เท่าเทียมกันของสังคมไม่ว่าจะเป็นทางด้านอำนาจ อายุ จุลทรัพย์ หรือสติปัญญา จึงทำให้เกิดความจำเป็นที่ต้องมีการควบคุมและป้องกันผู้ที่ด้อยกว่าไม่ให้ถูกเอาเปรียบหรือได้รับความไม่เป็นธรรม และก็เป็นความจำเป็นที่ผู้ที่เกี่ยวข้องจะต้องเล็งเห็นถึงปัญหาและเครื่องมือหนึ่งที่สามารถใช้ในการควบคุมและป้องกันก็คือกฎหมาย ดังนั้น แม้การเปลี่ยนแปลงของเทคโนโลยีอาจเป็นเหตุให้ต้องมีการเปลี่ยนแปลงกฎหมายให้เท่าทันและครอบคลุม แต่ในทางกลับกันการเปลี่ยนแปลงกฎหมายก็สามารถควบคุมเทคโนโลยีให้เป็นไปในทิศทางที่กำหนดได้เช่นกัน ดังนั้น การปรับปรุงแก้ไขกฎหมายไม่ว่าในกรณีใด นอกจากผู้ที่เกี่ยวข้องจะต้องคำนึงถึงข้อดีและข้อเสียของการแก้ไขกฎหมายนั้น ๆ อันเป็นวัตถุประสงค์หลักแล้ว ยังจะต้องคำนึงถึงผู้ที่จะได้รับผลกระทบจากการปรับแก้กฎหมายดังกล่าวด้วย

# บรรณานุกรม

## หนังสือภาษาไทย


เข็มชัย ชุติวงศ์,**คำอธิบายกฎหมายลักษณะพยาน**,พิมพ์ครั้งที่ 5,กรุงเทพมหานคร:สำนักพิมพ์นิติบรรณการ,2538

ชัยวัฒน์ วงศ์วัฒศานต์,ทวีศักดิ์ กออนันตกูล และ สุรางคณา แก้วจำนง, **คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ.2544** กรุงเทพมหานคร: สำนักงานเลขานุการคณะกรรมการ เทคโนโลยีสารสนเทศแห่งชาติ,2545

เด่นฟ้า เรืองฤทธิ์เดช, **"ปัญหาข้อกฎหมายเกี่ยวกับการรับฟังเอกสารอิเล็กทรอนิกส์"** ,ดุลพาห 53: 3,กันยายน-ธันวาคม 2549

ปิติกุล จิระมงคลพาณิชย์,**คำอธิบายกฎหมายลักษณะพยาน:ว่าด้วยพยานเอกสาร**,พิมพ์ครั้งที่ 2, กรุงเทพมหานคร:สำนักพิมพ์วิญญูชน,2548,น.11

ประเสริฐ คันธมานนท์,สมชัย จันทรมัสการ, **"พยานหลักฐานดิจิตอล",** บทบัณฑิตย์ 62:1 (มีนาคม 2549) : 45-46

พินัย ณ นคร , **กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์**, บทบัณฑิตย์เล่ม 56 ตอน 2, พ.ศ. 2543 :น.27-31

ไพจิตร สวัสดิสาร,**การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์,**ดุลพาห,เล่ม 1 ปีที่ 53 (มกราคม-เมษายน)

วัชรพงษ์ ยาวัย, **เอกสารประกอบการสอน ลายมือชื่ออิเล็กทรอนิกส์**

สุพิศ ประณีตพลกรัง, **ความรู้เบื้องต้นกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์** ,เนติบัณฑิตยสภา: น. 48

โสภณ รัตนากร,**คำอธิบายกฎหมายลักษณะพยาน.**พิมพ์ครั้งที่7,กรุงเทพมหานคร:สำนักพิมพ์นิติบรรณการ,2544

อาทิตย์ ออกเวหา, **Digital signatures เป็นการลงลายมือชื่อตามกฎหมายหรือไม่**, ดุลพาห , เล่ม 2 ปีที่47, พฤษภาคม-สิงหาคม 2543

โอภาส เอี่ยมสิริวงศ์,**เครือข่ายคอมพิวเตอร์และการสื่อสาร**,(กรุงเทพมหานคร:บริษัท ซีเอ็ดยูเคชั่น,2548),น.20-24

หนังสือเผยแพร่ร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. ... ของสำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยี อิเล็กทรอนิกส์ และคอมพิวเตอร์แห่งชาติ, 2543

**ภาษาอังกฤษ**

Christina McAlhone and Michael Stockdale, **Evidence in a Nutshell**,(Londom : Sweet & Maxwell, 1996) , : 54.

John Patzakis, **International Journal of Digital Evidence Spring 2002**, Volume 2 , Issue 1. U.S. Department of Justice (2002). Searching and Seizing Computers and Obtaining Evidence in Criminal investigations

Stephen E. Blythe,"**Digital Signature Law of The United Nations,European Union,UnitedKingdom and United States:Promotion of Growth in E-Commerce with Enchanced Security"**,(Winter 2005) Richmond Journal of Law and Technology[29].

**บทความ**

พรเพชร วิชิตชลชัย, บทวิเคราะห์เรื่อง **การรับฟังข้อมูลจากสื่ออิเล็กทรอนิกส์เป็นพยานหลักฐานในคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ**,เอกสารประกอบการสัมมนาทางวิชาการเรื่อง กฎหมายพาณิชย์อิเล็กทรอนิกส์(E-commerce Laws): นวัตกรรมทางกฎหมายที่จำเป็นและเร่งด่วนแห่งสังคมไทย,หอประชุมมหิศรอาคารไทยพาณิชย์ปาร์ค พลาซ่า กรุงเทพฯ, เมื่อวันที่ 6-7 พฤษภาคม 2542.(อัดสำเนา)น.3 สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, **กฎหมายธุรกรรมทางอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์**, (กรุงเทพมหานคร:สำนักงาน),น.24

อนันต์ จันทรโอภากร,**คอมพิวเตอร์กับกฎหมายลักษณะพยาน**,(กรุงเทพมหานคร คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์,2533),น.20-21

อารัมภบทบางตอนของมติสมัชชาใหญ่แห่งสหประชาชาติในเรื่องของ **ความสำคัญของกฎหมายแม่แบบ**

## บทความภาษาอังกฤษ

Interdisciplinary Center for Law & Info. Tech., Katholieke University Leuven, Study for the European Commission: **The Legal and Market Aspects of Electronic Signatures,** 215-16 (2003).

Sallis P., Aakjaer, A., and MacDonnell, S. ( 1996). **Software Forensics**; Old Methods for a New.

William J. Robinson, " **An Overview of Electronic Discovery**", Practicing Law Institute Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series PLI Order No. 6578 September-November, (2005) Patent Litigation 2005 (194).

# ผนวก ก
# ประเภทของข้อมูลอิเล็กทรอนิกส์

ประเภทของข้อมูลอิเล็กทรอนิกส์สามารถแบ่งออกได้เป็นหลายประเภทดังนี้

**1. แบ่งตามลักษณะการสร้าง**

ข้อมูลอิเล็กทรอนิกส์ที่บันทึกในเครื่องคอมพิวเตอร์อาจแบ่งประเภทตามลักษณะการสร้างได้ ดังนี้[1]

ก. ข้อมูลอิเล็กทรอนิกส์ที่สร้างโดยมนุษย์

ข้อมูลที่เพียงจัดเก็บไว้ในระบบคอมพิวเตอร์ซึ่งมนุษย์เป็นผู้สร้างขึ้น เช่น แฟ้มไปรษณีย์เสียง แฟ้มอีเมล์ สารสนเทศในรูป ข้อความ ภาพ เสียง

ข. ข้อมูลอิเล็กทรอนิกส์ที่สร้างโดยอัตโนมัติ

ข้อมูลที่สร้างขึ้นโดยระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ เช่น แฟ้มโปรแกรม แฟ้มข้อมูลชั่วคราว แฟ้มประวัติระบบ แฟ้มลงบันทึกเข้าออกเว็บไซน์ แฟ้มแคชและคุ๊กกี้

ค. ข้อมูลอิเล็กทรอนิกส์ที่สร้างโดยมนุษย์และโดยอัตโนมัติประกอบกัน

ข้อมูลที่ประกอบด้วยข้อมูลที่จัดเก็บไว้ในระบบคอมพิวเตอร์และที่สร้างขึ้นโดยระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ทั้ง 2 ประเภท เช่น แผนภูมิ (Chart) ซึ่งเป็นผลลัพธ์ที่ได้จากการทำงานของโปรแกรมตารางการทำงานหรือคำนวณ

การแบ่งประเภทของข้อมูลอิเล็กทรอนิกส์ตามลักษณะการสร้างนี้จะมีผลต่อการรับฟังพยานหลักฐานในเรื่องของหลักการรับฟังพยานบอกเล่า

**2. แบ่งตามลักษณะความซับซ้อน**

การแบ่งประเภทของข้อมูลอิเล็กทรอนิกส์ตามลักษณะความซับซ้อนนี้ จะมีผลต่อการรับฟังพยานหลักฐานในเรื่องของการรับรองความถูกต้องแท้จริงของข้อมูลอิเล็กทรอนิกส์ ยิ่งข้อมูลมีความซับซ้อนมากขึ้นก็ยิ่งต้องมีวิธีการในการรับรองความถูกต้องแท้จริงที่น่าเชื่อถือมากขึ้นและอาจต้องมีบุคคลและอุปกรณ์ต่างๆ เข้ามาเกี่ยวข้องหลายอย่าง

**3. ข้อมูลอิเล็กทรอนิกส์ในระบบเครือข่าย**

ข้อมูลอิเล็กทรอนิกส์ที่อยู่ในระบบเครือข่ายนี้จะมีการรับส่งกันไปมาได้ง่ายและอาจเก็บรักษาอยู่ในฐานข้อมูลหลายแห่งขึ้นอยู่กับประเภทของระบบเครือข่ายนั้นๆซึ่งก็อาจจะทำให้มีข้อมูลอิเล็กทรอนิกส์เดียวกันอยู่ในหลายแห่ง ตัวอย่างเช่น

---

[1] ประเสริฐ คันธมานนท์, สมชัย จันทรมัสการ, “**พยานหลักฐานดิจิตอล**”, บทบัณฑิตย์ 62:1 (มีนาคม 2549): 45-46

-ข้อมูลอิเล็กทรอนิกส์ในระบบการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์(EDI)ก็จะมีข้อมูลอิเล็กทรอนิกส์เก็บอยู่ที่ผู้ส่งและศูนย์บริการ EDI (VAN) และอาจมีเก็บรักษาอยู่ที่ผู้รับหากมีการสำเนาข้อมูลที่เก็บอยู่ที่ศูนย์บริการ EDI (VAN) ไปยังเครื่องของตน

-ข้อมูลอิเล็กทรอนิกส์ในระบบอินเตอร์เน็ตหากมีการส่งหรือรับข้อมูลกันก็จะมีข้อมูลอิเล็กทรอนิกส์เก็บอยู่ที่เครื่องคอมพิวเตอร์ของผู้ส่งและเครื่องคอมพิวเตอร์ของผู้ให้บริการอินเตอร์เน็ตนั้นทั้งผู้ให้บริการอินเตอร์เน็ตของผู้รับและผู้ส่ง

**4. ข้อมูลอิเล็กทรอนิกส์ที่ไม่อยู่ในระบบเครือข่าย**

ข้อมูลอิเล็กทรอนิกส์ที่ไม่อยู่ในระบบเครือข่ายนี้อาจเป็นข้อมูลที่เก็บไว้ในเครื่องคอมพิวเตอร์ หรือสื่อบันทึกข้อมูลใดๆ ที่ไม่ได้เชื่อมต่อกับระบบเครือข่าย ซึ่งก็จะมีขอบเขตที่จะค้นหาน้อยกว่าข้อมูลในระบบเครือข่ายซึ่งก็เป็นผลดีในแง่ของการค้นหาทำได้ง่ายแต่ก็มีข้อเสียเพราะหากข้อมูลสูญหายไปอาจหาไม่ได้อีก ในขณะที่ในระบบเครือข่ายอาจมีการรับส่งและเก็บไว้ที่คอมพิวเตอร์หลายเครื่อง

นอกจากนี้ข้อมูลอิเล็กทรอนิกส์ที่มีการส่งและรับฝ่ายเดียว เช่น โทรทัศน์ การกระจายเสียง ก็อาจค้นหาข้อมูลได้จำกัด เฉพาะผู้ที่ส่งเท่านั้น ในส่วนเครือมือและอุปกรณ์ยองผู้รับ เช่น โทรทัศน์ วิทยุ หากไม่มีการสำเนาข้อมูลไว้ต่างหากก็จะไม่มีข้อมูลอิเล็กทรอนิกส์นั้นเหลืออยู่ แบ่งตามลักษณะการใช้เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

**5. ข้อมูลอิเล็กทรอนิกส์ในเครื่องมือและอุปกรณ์ที่ใช้กันเป็นปกติ**

กรณีของข้อมูลอิเล็กทรอนิกส์ที่เกิดขึ้นจากเครื่องมืออุปกรณ์นี้หากเป็นการใช้งานเครื่องมือและอุปกรณ์ตามปกติไม่ว่าจะเป็นการใช้งานตามปกติของภาคราชการหรือของภาคเอกชน ก็สามารถสันนิษฐานได้ว่าข้อมูลอิเล็กทรอนิกส์ที่เกิดขึ้นนั้น มีความถูกต้องปกตินี้หมายความว่า[2]

(1) Hardware นั้นๆ ได้ใช่อยู่เป็นปกติ ไม่ใช่สั่ง Hardware เพื่อนำมาใช้เฉพาะกิจ คือเพื่อเตรียมพยานหลักฐานต่อศาล

(2) Software หรือ Program ที่ใช้อยู่เป็นตัวผลิต Output หรือเอกสารที่อ้างเป็นพยานก็เป็นโปรแกรมที่ใช้อยู่เป็นปกติ และ

(3) ได้มีการจัดทำและเก็บรักษา Computer file (ข้อมูลอิเล็กทรอนิกส์) เหล่านั้นเป็นปกติธุระในทางธุรกิจของตนเช่นกัน

---

[2] อนันต์ จันทรโอภากร,**คอมพิวเตอร์กับกฎหมายลักษณะพยาน**,(กรุงเทพมหานคร คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์,2533),น.20-21

**6. ข้อมูลอิเล็กทรอนิกส์จากอุปกรณ์อื่น**[3]

ต่อไปนี้เป็นตัวอย่างของข้อมูลอิเล็กทรอนิกส์จากอุปกรณ์อื่นๆที่ไม่ใช่คอมพิวเตอร์

**1 โทรเลข (Telegraphy)**

หลักการทำงานของระบบโทรเลข จะใช้วิธีการแปลตัวอักษรหรืออักขระ ตัวเลข ให้เป็นรหัสจากนั้นก็จะทำการแปลรหัสดังกล่าวให้เป็นสัญญาณไฟฟ้าส่งผ่านตัวกลาง เช่น สายทองแดง เพื่อไปยังปลายทาง เมื่อปลายทางได้รับก็จะทำการถอดรหัสให้เป็นข้อความ

**2 โทรพิมพ์ (Telex)**

เป็นรูปแบบของการบริการโทรเลขชนิดหนึ่งแต่ผู้ใช้งานสามารถติดต่อโต้ตอบกันได้โดยเครื่องโทรพิมพ์จะมีลักษณะคล้ายเครื่องพิมพ์ดีดที่เป็นได้ทั้งเครื่องรับส่งข้อมูลในตัวเดียวกันโทรพิมพ์สื่อสารกันได้โดยอาศัยตัวนำหรือช่องสัญญาณและชุมสายที่มีการเชื่อมต่อกับเครื่องโทรพิมพ์ต่าง ๆเข้าไว้ด้วยกันตามต้องการผู้ใช้งานทั้งสองฝั่งสามารถติดต่อโต้ตอบกันได้โดยเครื่องโทรพิมพ์จะมีลักษณะคล้ายเครื่องพิมพ์ดีดที่เป็นได้ทั้งเครื่องรับส่งข้อมูลในตัวเดียวกันโทรพิมพ์สื่อสารกันได้โดยอาศัยตัวนำหรือช่องสัญญาณและชุมสายที่มีการเชื่อมต่อกับเครื่องโทรพิมพ์ต่าง ๆเข้าไว้ด้วยกันตามต้องการผู้ใช้งานทั้งสองฝั่งสามารถติดต่อสื่อสารกันได้ด้วยการพิมพ์โต้ตอบระหว่างกันโดยข้อความที่ส่งถึงกันจะทำได้ด้วยการพิมพ์ข้อความลงบนกระดาษพิมพ์ของทั้งสองฝ่าย และถึงแม้ว่าฝ่ายผู้รับจะไม่มีพนักงานคอยรับข้อความ เครื่องก็จะสามารถทำงานและหยุดเองโดยอัตโนมัติ

**3 โทรสาร (Facsimile)**

เครื่องโทรสารมักเรียกสั้นๆ ว่า แฟกซ์ (Fax) ใช้เทคนิคของแสงสแกนลงบนเอกสารต้นฉบับที่สามารถเป็นได้ทั้งข้อความและภาพจากนั้นก็จะเปลี่ยนเป็นสัญญาณไฟฟ้าเพื่อส่งต่อไปตามสายโทรศัพท์ เมื่อเครื่องฝ่ายผู้รับได้รับข้อมูลที่ส่งมาก็จะนำข้อมูลที่เป็นสัญญาณไฟฟ้านั้นมาเปลี่ยนเป็นข้อมูลที่เหมือนกับต้นฉบับ

ข้อมูลที่อาจพบได้ในเครื่องโทรสาร เช่น หมายเลขในการโทรด่วน ข้อมูลการส่งแฟกซ์ (ข้อมูลการรับเข้าและการส่งออก) รายการส่งแฟกซ์ (การรับเข้าและการส่งออก) หัวข้อการส่งแฟกซ์ (header line) การตั้งเวลาเป็นต้น

---

[3] เนื้อหาส่วนใหญ่คัดลอกจาก โอภาส เอี่ยมสิริวงศ์,**เครือข่ายคอมพิวเตอร์และการสื่อสาร**, (กรุงเทพมหานคร:บริษัท ซีเอ็ดยูเคชั่น,2548),น.20-24โดยเฉพาะข้อมูลที่อยู่ในรูปแบบของสื่อประสมหรือมัลติมีเดีย อีกทั้งในขณะที่ใช้งานก็ยังสามารถใช้โทรศัพท์ได้ด้วย เนื่องจากช่องความถี่ที่แตกต่างกันในการสื่อสาร ในขณะที่รูปแบบเดิมหรือแอนะล็อกนั้น เมื่อใช้งานอินเตอร์เน็ตนั้นก็จะไม่สามารถใช้งานโทรศัพท์ได้

**4 โทรศัพท์ (Telephone)**

เป็นอุปกรณ์ที่นิยมใช้เป็นอย่างสูง ซึ่งมักมีการใช้งานตามบ้านเรือนเกือบทุกครัวเรือนในปัจจุบันชุมสายโทรศัพท์ได้มีการพัฒนาและเปลี่ยนมาเป็นรูปแบบของสัญญาณดิจิตอลในบางพื้นที่มากขึ้นตามลำดับเพื่อรับรองการสื่อสารข้อมูลความเร็วสูง การใช้ชุมสายโทรศัพท์ในการสื่อสารนั้นมีราคาถูกและเป็นที่นิยม ตัวอย่างเช่น การใช้งานอินเตอร์เน็ตตามบ้านเรือนต่างๆด้วยการใช้คอมพิวเตอร์เชื่อมต่อกับโมเด็ม ซึ่งบางบริษัทที่บริการอินเตอร์เน็ต (ISP) ก็ยังคงมีรูปแบบการบริการแบบแอนะล็อกกับแบบดิจิตอลความเร็วสูง เช่น ISDN หรือ ADL เป็นต้น โดยระบบดิจิตอลจะมีช่องสัญญาณหรือแบนด์วิดธ์ที่กว้างกว่า ทำให้มีการรับส่งข้อมูลที่รวดเร็ว
อย่างไรก็ตามข้อจำกัดของโทรศัพท์แบบมีสาย ทำให้เกิดการใช้งานที่ไม่คล่องตัว จึงมีการพัฒนาระบบเคลื่อนที่แบบไร้สายขึ้น โดยระบบดังกล่าวจะมีการแบ่งเขตรับส่งสัญญาณวิทยุออกเป็นพื้นที่ตามส่วนต่างๆ ที่เรียกว่า เซลล์ (Cell) ในแต่ละเซลล์ก็จะมีเสาอากาศตามประเภทของคลื่นนั้นๆไว้สำหรับส่งสัญญาณหลายๆสัญญาณพร้อมกัน ทำให้สามารถใช้โทรศัพท์ติดต่อกันได้ ไม่ว่าผู้ใช้โทรศัพท์เคลื่อนที่จะอยู่บริเวณใดก็ตามและยังสามารถสื่อสารระหว่างโทรศัพท์เคลื่อนที่ด้วยกัน หรือกับโทรศัพท์ตามบ้านที่มีสาย

ข้อมูลที่อาจพบได้ในโทรศัพท์ เช่น หมาเลขโทรออก ชื่อและที่อยู่ หมายเลขโทรเข้า ข้อมูลอื่นๆ ที่อาจอยู่ในหน่วยความจำ หมายเลขโทรศัพท์/เพจเจอร์ ชื่อและที่อยู่หมายเลข PIN (PIN number) หมายเลขโทรศัพท์ที่ฝากข้อความเสียงไว้ รหัสการเข้าฟังข้อความเสียงหมายเลขบัตรเดบิต (Debit card number) หมายเลขบัตรโทรศัพท์ (Calling card number) ข้อมูลการเชื่อมต่ออินเตอร์เน็ต/อีเมล์ ข้อมูลของบริษัทผู้ให้บริการ ข้อมูลบนจอภาพที่อาจเป็นประโยชน์ต่อการสืบสวน ข้อมูลอื่นๆ ที่อาจจะพบได้ในเครื่อง PDA ข้อมูลอื่นๆ ที่เกี่ยวกับการทำธุรกรรมทางการเงิน

**5 โทรทัศน์ (Television)**

เป็นระบบที่มีการแพร่ภาพกระจายไปยังคลื่นความถี่สูง เช่น ย่านความถี่สูง VHF (Very High Frequency) หรือย่านความถี่สูง UHF (Ultra High Frequency) ซึ่งเป็นย่านความถี่ที่ใช้สำหรับกิจการทางโทรทัศน์ ในอดีตการแพร่ภาพทางโทรทัศน์มักจะประสบปัญหากับพื้นที่รับสัญญาณ เช่น ตามจังหวัดที่ห่างไกล แต่ในปัจจุบันได้มีการตั้งสถานีทวนสัญญาณโทรทัศน์ตามพื้นที่ต่างๆทั่วประเทศ เพื่อให้ประชาชนตามจังหวัดต่างๆ สามารถรับชมการแพร่ภาพทางโทรทัศน์ได้ ปัจจุบันการส่งสัญญาณทางโทรทัศน์ในประเทศไทยมี 2 ระบบด้วยกัน คือ ระบบออกอากาศทั่วไป (Broadcast) และอีกระบบหนึ่งคือ ระบบเคเบิลทีวี (Cable Television) สำหรับระบบนี้จำเป็นต้องสมัครสมาชิกและต้องเสียค่าบริการรายเดือน โดยจะมีเสารับสัญญาณที่แตกต่างกับเสาอากาศของโทรทัศน์ทั่วไป นอกจากนี้ยังมีเทคโนโลยีหนึ่งที่เรียกว่า “Video on Demand” ซึ่งเป็นระบบโทรทัศน์ที่ผู้ชมสามารถเป็นผู้เลือกชมรายการได้ด้วยตนเอง

**6 วิทยุกระจายเสียง (Radio)**

เป็นการสื่อสารที่อาศัยคลื่นวิทยุด้วยการส่งคลื่นไปยังอากาศเพื่อเข้าไปยังเครื่องรับวิทยุ โดยใช้เทคนิคการกล้ำสัญญาณ หรือว่าการมอดูเลต (Modulate) ด้วยการรวมกับคลื่นเสียงที่เป็นคลื่นไฟฟ้าความถี่เสียงรวมกัน ทำให้การสื่อสารด้วยวิทยุกระจายเสียงนั้นไม่จำเป็นต้องใช้สาย อีกทั้งยังสามารถส่งคลื่นได้ในระยะเวลาที่ไกลออกไปได้ตามประเภทของคลื่นนั้น ๆ ข้อมูลต่าง ๆ จึงอาจอยู่ในรูปคลื่นวิทยุได้

**7 ดาวเทียม (Satellite)**

เนื่องจากคลื่นไมโครเวฟมีข้อจำกัดเรื่องของลักษณะภูมิประเทศที่มีผลต่อการบดบังคลื่น ดังนั้นจึงได้มีการพัฒนาดาวเทียม โดยความเป็นจริงแล้ว ดาวเทียมก็คือสถานีไมโครเวฟนั่นเอง แต่เป็นสถานีไมโครเวฟที่ลอยอยู่บนเหนือพื้นผิวโลก มีลักษณะเป็นจานขนาดใหญ่โคจรห่างจากพื้นโลกประมาณ 22,300 ไมล์ ทำให้สามารถติดต่อสถานีภาคพื้นดินที่อยู่บนโลกได้

เราสามารถส่งดาวเทียมที่เรียกว่า Geostationary ซึ่งเป็นดาวเทียมหมุนโคจรด้วยความเร็วเท่ากับโลก ทำให้ดูเหมือนกับไม่มีความเคลื่อนไหว และด้วยการนำดาวเทียมดังกล่าวขึ้นไปโคจรบนพื้นผิวโลกเพียง 3 ดวงก็สามารถครอบคลุมการสื่อสารได้ทุกมุมโลก โดยดาวเทียมดวงหนึ่งส่งสัญญาณในบริเวณกว้างเท่ากับ 1 ใน 3 ของโลก (120 องศา) ดังนั้นดาวเทียม 3 ดวงก็ครอบคลุมบริเวณพื้นโลกทั้งหมด (360 องศา) ส่วนการสื่อสารสามารถส่งสัญญาณแบบขาขึ้น (Uplink) ซึ่งเป็นการส่งสัญญาณจากดาวเทียมจากสถานีภาคพื้นดินไปยังดาวเทียม และการส่งสัญญาณแบบขาลง (Downlink) ซึ่งเป็นการส่งสัญญาณจากดาวเทียมมายังสถานีภาคพื้นดิน และด้วยเทคโนโลยีดาวเทียมในอนาคตก็จะสามารถสื่อสารได้ทั้งสองทาง ไม่ว่าจะเป็นแบบขาขึ้นหรือขาลงในขณะเดียวกัน

**8 สแกนเนอร์ (Scanners)**

สแกนเนอร์ใช้สร้างเอกสารภาพจากรูปภาพหรือเอกสารที่เป็นกระดาษหรือสิ่งของโดยวางลงบนฐานของเครื่องสแกนเนอร์ และทำการเก็บไว้ในเครื่องคอมพิวเตอร์ในรูปของไฟล์คอมพิวเตอร์ เครื่องสแกนเนอร์สามารถเก็บข้อมูลไว้ในเครื่องได้

**9 เครื่องปริ้นเตอร์ (Printers)**

เครื่องปริ้นเตอร์ใช้พิมพ์ข้อมูลจากเครื่องคอมพิวเตอร์ลงบนกระดาษ ซึ่งมีหลายชนิดด้วยกันคือ เครื่องพิมพ์เลเซอร์ (laser) เครื่องพิมพ์แบบพ่นหมึก (ink jet) เครื่องพิมพ์แบบแผ่นฟิล์มความร้อน (thermal dye) และเครื่องพิมพ์แบบหัวเข็ม (dot matrix) เครื่องปริ้นเตอร์สามารถเก็บข้อมูลไว้ในเครื่องได้

**10 เครื่องถ่ายสำเนา (Copiers)**

เครื่องถ่ายสำเนาใช้ในการทำสำเนาสิ่งต่าง ๆ โดยวางต้นฉบับของสิ่งที่ต้องการสำเนาลงบนฐานของเครื่องถ่ายสำเนา

ข้อมูลที่สามารถพบได้ในเครื่องถ่ายเอกสาร เช่น รายการสำหรับการโทรด่วน สำเนาต่าง ๆ ที่เครื่องทำการเก็บไว้ ทั้งข้อมูลที่เป็นการป้อนเข้ามาในเครื่องและข้อมูลที่พิมพ์ออกมาจากเครื่อง แฟ้มข้อมูล (รูปภาพ หรือเอกสารจากเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่าย) หัวข้อ ( Header Line) การตั้งเวลา

**11 เครื่องทำสำเนาแผ่นซีดีและเครื่องพิมพ์ฉลาก (Compact Disk Duplicators and Labelers)**

เครื่องทำสำเนาแผ่นซีดีหรือเครื่องปั๊มแผ่นซีดีใช้ในการสร้างแผ่นซีดีจำนวนมาก ๆ หากมีการใช้งานเของเครื่องที่ไม่เหมาะสมอาจเป็นการกระทำผิดกฎหมายละเมิดลิขสิทธิ์ได้

สิ่งที่เครื่องปั๊มแผ่นซีดีและเครื่องพิมพ์ฉลากสามารถเก็บไว้ในเครื่องได้ คือ ข้อมูลต่าง ๆ เกี่ยวกับการใช้งานของเครื่อง

**12 กล้องดิจิตอล กล้องวีดีโอ และเครื่องเสียง (Digital Cameras/Video/Audio)**

เครื่องวีดีโอและสื่อบันทึกเสียงนั้นสามารถเก็บบันทึกได้ทั้งในรูปแบบอนาล็อก (analog) และแบบดิจิตอล (Digital) ซึ่งจะพบสื่อบันทึกในลักษณะต่าง ๆ ที่หลากหลายกันได้ทั้งใน 2 รูปแบบข้างต้น อุปกรณ์เหล่านี้สามารถที่จะใช้ได้ในตัวมันเอง ใช้เชื่อมต่อกับเครือข่าย ใช้เป็นส่วนตัว ใช้เป็นสื่อบันเทิงภายในบ้าน หรือใช้ในการประกอบธุรกิจก็ได้ เช่น ข้อความ ภาพนิ่ง ภาพกราฟฟิก แสดงวันเวลา ชื่อผู้บันทึก หรือระบบที่ใช้ก็ได้ อุปกรณ์บางชนิดอาจมีฟังก์ชั่นพื้นฐานของเครื่องคอมพิวเตอร์ประกอบอยู่ หรืออาจจะเป็นอุปกรณ์คอมพิวเตอร์โดยตัวมันเองเลยก็ได้

อุปกรณ์ชนิดนี้อาจพบได้ทั้งในรูปแบบที่สามารถพกพาได้หรืออาจเป็นรูปแบบที่ใช้อยู่เฉพาะที่แต่ก็อาจสามารถเคลื่อนย้ายได้โดยง่าย การเก็บข้อมูลของอุปกรณ์เหล่านี้นั้นอาจสามารถเก็บข้อมูลลงไปในหน่วยความจำภายในเครื่องได้โดยตรง หรืออาจบันทึกข้อมูลลงในสื่อบันทึกที่สามารถเคลื่อนย้ายได้ (removable media) ก็ได้

# ผนวก ข
# การทำงานของคอมพิวเตอร์

จากเรื่องพื้นฐานทางด้านเทคนิคของระบบคอมพิวเตอร์ การประมวลผลข้อมูลการเก็บและเรียกข้อมูล ทำให้เราทราบว่าสื่อที่สำคัญที่ใช้ในการเก็บและเรียกข้อมูล ก็คือจานบันทึกอ่อน (Floppy Disk) และจานบันทึกแข็ง (Hard Disk)

ลักษณะการบันทึกข้อมูลลงในแผ่นดิสก์ (Disk) ที่มีลักษณะเป็นแผ่นกลมๆจะบันทึกบันทึกข้อมูลเป็นวงแหวนซ้อนๆ กันเหมือนแผ่นเสียง วงแหวนแต่ละวงเรียกว่าแทร็ก (Track) สำหรับ Floppy Disk หรือไซลินเดอร์ (Cylinder) สำหรับ Hard Disk แต่ละวงแบ่งออกเป็นส่วนๆ เรียกว่าเซ็กเตอร์(Sector) (Floppy Disk ขนาด 3.5 นิ้ว แบ่งเป็น 17 Sectors และ Hard disk ส่วนใหญ่แบ่งเป็น 63 Sectors ต่อ Cylinder)
ในหน่วยขับ (Drive) แต่ละตัวอาจมีแผ่นดิสก์ที่ใช้บันทึกข้อมูลหลายหน้า แต่ละหน้าจะมีหัวอ่าน 1 หัว ใน Floppy Disk Drive มีหัวอ่านสองหัว แต่ใน Hard Disk Drive อาจมีหัวอ่านตั้งแต่ 2-16 หัว

หน่วยที่เล็กที่สุดที่ใช้ในการบันทึกข้อมูลเรียกว่า คัสเตอร์ (Cluster) และใน 1 Cluster อาจจะประกอบด้วย 2-6 Sectors ขึ้นอยู่กับขนาดของความจุของแผ่นดิสก์ ซึ่งระบบปฏิบัติการจะเป็นตัวจัดการในเรื่องนี้

เมื่อกล่าวถึงเครื่องคอมพิวเตอร์ สิ่งที่ขาดไม่ได้ก็คือระบบปฏิบัติการ หรือ OS (Operating System) ซึ่งเป็นระบบการจัดการที่มีประสิทธิภาพสูง ถูกต้อง แม่นยำและรวดเร็วในการ

- บันทึกข้อมูลไว้ในแผ่นดิสก์
- อ่านข้อมูลที่บันทึกไว้ออกมาใช้งาน
- แก้ไขข้อมูลที่บันทึกไว้ให้ถูกต้องเป็นปัจจุบัน
- ลบหรือยกเลิกข้อมูลที่เตรียมไว้

OS ที่ใช้อยู่ในเครื่องคอมพิวเตอร์ที่อยู่มากมายหลายค่าย แต่ละค่ายมีการพัฒนา OS ของตนเอง ตามเทคโนโลยีที่เปลี่ยนไปอย่างสม่ำเสมอ เช่น PC-DOS หรือ MS-DOS ที่ใช้กับเครื่อง IBM PC Compatible เริ่มออกสู่ตลาดตั้งแต่ปี ค.ศ.1981 (Version 1.0)พัฒนาเป็น Version 2 ในปี ค.ศ.1982 และพัฒนาไปเรื่อยๆ จนกระทั่งถึง Version 6 ในปี ค.ศ. 1992 ซึ่งแต่ละค่ายได้มีการคิดค้นและพัฒนากันตลอดเวลาเพื่อชิงความได้เปรียบกันในทางธุรกิจ

OSแต่ละตัวมีวิธีการจัดการในการเก็บและเรียกข้อมูลแตกต่างกันแต่มีหลักการใกล้เคียงกันคือจัดแบ่งพื้นที่ของแผ่นดิสก์เพื่อจัดระบบในการเก็บรายละเอียดและส่วนสำคัญของไฟล์ อาจแยกพื้นที่ต่างๆได้ดังนี้

- Boot Sector
- FAT (File Allocation Table)
- Data Area
- Directory Area

การบันทึกไฟล์ของ MS-DOS จะมีการแยกเก็บรายละเอียด ดังนี้

- ข้อมูลของไฟล์ทั้งหมดเก็บไว้ที่ Data Area
- ชื่อไฟล์ วันเดือนปีและเวลาที่บันทึก ขนาดไฟล์ ชนิดของไฟล์ และหมายเลข Cluster แรกที่ใช้เป็นพื้นที่ในการเก็บไฟล์ (Data Area) เก็บไว้ที่ส่วนของ Directory Area
- หมายเลขของ Cluster ต่างๆ ที่ใช้ในการบันทึกไฟล์นี้ จนถึง Cluster สุดท้าย แสดงไว้ในส่วนที่เรียกว่า FAT

การลบไฟล์ใน MS-DOS ไม่มีการลบข้อมูลของไฟล์ในส่วนที่บันทึกไว้ใน Data Area เพียงแต่ทำเครื่องหมายไว้ที่ชื่อไฟล์ใน ของ Directory Area และใน FAT เพื่อให้ OS ทราบว่าไฟล์นี้ไม่ใช้งานแล้วสามารถเขียนหรือบันทึกข้อมูลไฟล์อื่นทับได้ ดังนั้นหากยังไม่มีการเขียนหรือบันทึกข้อมูลทับข้อมูลของไฟล์ที่ถูกสั่งลบก่อนหน้านั้นยังคงอยู่โดยครบถ้วนสมบูรณ์ สามารถกู้คืนได้

ในการเขียนข้อมูลหรือไฟล์ใหม่ทับไฟล์เดิมที่ถูกลบไปก็เช่นเดียวกัน OS ไม่ได้ลบข้อมูลหรือไฟล์เก่า เพียงแต่เขียนหรือบันทึกไฟล์ใหม่ทับพื้นที่ที่ใช้เก็บไฟล์ที่ถูกลบ ดังนั้นหากไฟล์ที่บันทึกใหม่มีขนาดเล็กกว่าไฟล์เดิมที่ถูกลบย่อมมีข้อมูลบางสวนของไฟล์หลงเหลืออยู่ในสื่อหรือแผ่นดิสก์ ซึ่งอาจเป็นข้อมูลหรือข้อความที่เป็นประโยชน์ต่อรูปคดี

โดยปกติแล้วระบบปฏิบัติการต่างๆจะมีคำสั่งให้ผู้ใช้งานใช้ในการขอดูชื่อไฟล์ที่เก็บบันทึกไว้พร้อมรายละเอียดต่างๆ ที่เกี่ยวข้อง เช่น ขนาดของไฟล์ วันเดือนปีและเวลาที่บันทึก ชนิดของไฟล์ นอกจากนั้นยังมีโปรแกรมอรรถประโยชน์ (Utility Software) ที่มาพร้อมกับระบบปฏิบัติการ เพื่ออำนวยความสะดวกแก่ผู้ใช้งานในการจัดการกับไฟล์และสื่อที่ใช้ในการบันทึกข้อมูล เช่น ซ่อนไฟล์ (Hidden Filed),เปลี่ยนชื่อไฟล์ ฯลฯ แต่มีประสิทธิภาพสู้โปรแกรมอรรถประโยชน์ (Utility Software) โดยตรงเช่น PC Tools หรือ Norton Utility ซึ่งสามารถเข้าไปดูและแก้ไขดิสก์ได้ทุกตารางนิ้วไม่ได้

ในการใช้งานเครื่องคอมพิวเตอร์ ย่อมมีการบันทึก แก้ไขและลบข้อมูล ในการดำเนินการเหล่านั้นย่อมมีร่องรอยการใช้งานแต่ละครั้งหลงเหลืออยู่ในสื่อที่ใช้บันทึกเนื่องจากในการลบแต่ละครั้งระบบปฏิบัติการไม่ได้ลบข้อมูลจริง ดังกล่าวข้างต้น หากเราใช้โปรแกรมอรรถประโยชน์ที่เหมาะสมก็จะสามารถกู้ไฟล์หรือข้อมูลที่ถูกลบทิ้งคืนมา นอกจากนั้นยังสามารถเข้าไปดูข้อมูล

ข้อความที่เคยถูกบันทึกไว้และยังถูกเขียนหรือบันทึกทับไม่หมดหรืออาจตรวจหาข้อมูลที่ผู้ใช้งานจงใจพิมพ์ซ่อนไว้ได้

**การทำงานของคอมพิวเตอร์**

1. **โครงสร้างการทำงานและฟังก์ชั่นภายในคอมพิวเตอร์**

(1) ฟังก์ชั่นพื้นฐานทางคอมพิวเตอร์

แบ่งออกเป็น 4 แบบคือ

1.การประมวลผลข้อมูล (Data processing)

การประมวลผลข้อมูลเป็นฟังก์ชั่นที่สำคัญของคอมพิวเตอร์ ที่มีรูปแบบแตกต่างกันไป

2.การจัดเก็บข้อมูล (Data Storage)

เมื่อคอมพิวเตอร์ทำการประมวลผลข้อมูล เช่น ได้รับข้อมูลจากส่วนต่าง ๆเข้ามาหรืออาจอ่านข้อมูลจากสื่อบันทึกข้อมูลต่าง ๆไม่ว่าจะเป็นดิสก์ หรือซีดีรอม ก็จะส่งต่อไปยังหน่วยความจำและซีพียูก็จะนำข้อมูลจากหน่วยความจำมาทำการประมวลผลเพื่อให้เป็นผลลัพธ์ต่อไป จากการทำงานดังกล่าวข้างต้นคอมพิวเตอร์ก็จะต้องสามารถจัดเก็บส่วนข้อมูลดังกล่าวไว้ชั่วคราวเพื่อรอประมวลผลหรือเพื่อนำไปใช้งานและทำการประมวลผลต่อไป และสามารถจัดเก็บข้อมูลแบบ Long-term storage ซึ่งหมายถึงการจัดเก็บข้อมูลลงในสื่อบันทึกข้อมูลต่าง ๆ โดยที่ข้อมูลที่บันทึกนั้นจะต้องสามารถทำการเรียกข้อมูลเหล่านั้นขึ้นมาเพื่อทำการปรับปรุงได้

3.การเคลื่อนย้ายข้อมูล (Data Movement)

การเคลื่อนย้ายข้อมูลเป็นสิ่งที่สำคัญประการหนึ่งคอมพิวเตอร์จะต้องสามารถเคลื่อนย้ายข้อมูลทั้งข้อมูลภายในและข้อมูลภายนอกการปฏิบัติการของคอมพิวเตอร์ประกอบด้วยอุปกรณ์ที่คอยให้บริการแหล่งข้อมูลต้นทางและข้อมูลปลายทาง เมื่อข้อมูลจากอุปกรณ์ส่งมาเพื่อติดต่อกับคอมพิวเตอร์เพื่อทำการประมวลผลหรือแสดงผลลัทธ์ในรูปแบบต่าง ๆกระบวนการนี้จะทำให้ทราบถึงอินพุตท์และเอาท์พุต

4.การควบคุม(Control)

คอมพิวเตอร์จะต้องสามารถควบคุมฟังก์ชั่นการทำงานเหล่านี้ได้ รวมทั้งการตอบสนองและการปฏิบัติตามคำสั่งที่ได้รับคำสั่งมา

(2) โครงสร้างคอมพิวเตอร์

ประกอบด้วย 3 องค์ประกอบ คือ หน่วยประมวลผลกลาง หน่วยความจำหลัก และอินพุต/เอาท์พุต

หน่วยประมวลผลกลางทำหน้าที่ควบคุมการปฏิบัติหน่วยประมวลผลกลางทำหน้าที่ควบคุมการปฏิบัติงานของคอมพิวเตอร์ และการประมวลผลข้อมูล ซึ่งอาจเรียกอีกอย่างหนึ่งว่าโปรเซสเซอร์หรือซีพียู ประกอบไปด้วยส่วนสำคัญ 3 ส่วนคือ หน่วยควบคุม หน่วยคำนวณและตรรกะ และรีจีสเตอร์

หน่วยความจำหลักเป็นพื้นที่สำหรับจัดเก็บข้อมูลสำคัญต่างๆเพื่อส่งให้หน่วยประมวลผลกลางประมวลผลมีหน้าที่สำคัญคือ จัดเก็บชุดคำสั่ง จัดเก็บข้อมูลเพื่อรอการประมวลผล และจัดเก็บข้อมูลหรือสารสนเทศที่ได้จากการประมวลผล จากนั้นก็นำสารสนเทศเหล่านั้นส่งไปยังเอาท์พุตที่ต้องการ หรือจัดเก็บลงในหน่วยความจำสำรองต่อไป หน่วยความจำสำหรับจัดเก็บ ข้อมูลและคำสั่ง (RAM: Random Access Memory)นั้น เป็นหน่วยความจำที่สามารถเก็บข้อมูลและคำสั่งจากหน่วยรับข้อมูล แต่ข้อมูลและคำสั่งเหล่านั้นสามารถหายไปได้เมื่อมีการรับข้อมูลและคำสั่งใหม่ หรือปิดเครื่อง หรือกระแสไฟฟ้าขัดข้อง[1] จึงต้องส่งไปยังเอาท์พุตที่ต้องการ หรือจัดเก็บลงในหน่วยความจำสำรองต่อไป

อินพุต/เอาต์พุตเป็นส่วนที่ใช้สำหรับเคลื่อนย้ายข้อมูลระหว่างคอมพิวเตอร์กับอุปกรณ์ทั้งภายในและภายนอก

ในการประมวลผลของซีพียูมีขั้นตอนต่างๆดังต่อไปนี้

1.การเฟตช์(Fetch)เป็นกระบวนการที่หน่วยควบคุมไปนำคำสั่งที่ต้องการจากหน่วยความจำมาเก็บไว้ในรีจีสเตอร์

2.การแปลความหมาย(Decode)เป็นกระบวนการถอดรหัสหรือแปลความหมายคำสั่งต่างๆเพื่อส่งไปยังหน่วยคำนวณและตรรกะจัดการต่อไป

3.การเอ็กส์คิวต์(Excute)เป็นกระบวนการประมวลผลคำสั่งโดยหน่วยคำนวณและตรรกะซึ่งจะประมวลผลทีละคำสั่ง

4.การจัดเก็บ(Store) เป็นกระบวนการจัดเก็บผลลัพธ์ที่ได้จากการประมวลผลและจัดเก็บไว้ในหน่วยความจำหรือรีจีสเตอร์

อุปกรณ์นำข้อมูลเข้าและและอุปกรณ์แสดงผลข้อมูล

(1) อุปกรณ์นำข้อมูลเข้า (Input Devices)

อินพุต คือ ข้อมูลต่างๆหรือชุดคำสั่งที่เราป้อนเข้าสู่หน่วยความจำในคอมพิวเตอร์เมื่อผู้ใช้มีความประสงค์ที่จะป้อนข้อมูลเข้าไปยังคอมพิวเตอร์ จำเป็นต้องใช้อุปกรณ์อินพุตเพื่อนำข้อมูลหรือชุดคำสั่งเหล่านั้นไปเก็บไว้ในหน่วยความจำคอมพิวเตอร์ เพื่อเตรียมการประมวลผลต่อไป

---

[1] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ,กฎหมายธุรกรรมทางอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์,(กรุงเทพมหานคร:สำนักงาน,2544),น.24

อุปกรณ์อินพุตสามารถแบ่งได้เป็น 2 ประเภทคือ

ก.อุปกรณ์อินพุตมาตรฐาน (Standard Methods of Input) ได้แก่ คีย์บอร์ด เมาส์

ข.อุปกรณ์อินพุตอื่นๆ(Alternative Methods Input) เช่น ปากกาหรือสไตลัส ปากกาแสง จอภาพแบบสัมผัส จอยสติ๊ก สแกนเนอร์ ไมโครโฟน กล้องดิจิตอล เป็นต้น

(2) อุปกรณ์แสดงผลข้อมูล (Output Devices)

เอาต์พุตคือข้อมูลที่ได้ประมวลผลมาแล้วโดยผลลัพธ์ที่ได้จากการประมวลผลนั้นสามารถนำไปใช้ให้เกิดประโยชน์ได้ คอมพิวเตอร์จะนำข้อมูลที่อินพุตเข้ามาทำการประมวลผลออกเป็นเอาต์พุตโดยใช้อุปกรณ์เอาต์พุต โดยสามารถแสดงได้หลายรูปแบบด้วยกันขึ้นอยู่กับฮาร์ดแวร์หรือซอฟแวร์ที่ใช้งานอุปกรณ์เอาต์พุต เช่น จอภาพ เครื่องพิมพ์ เป็นต้น

เทคโนโลยีมัลติมีเดียและสื่อจัดเก็บข้อมูล

มัลติมีเดีย (Multimedia) หรือสื่อประสม เป็นการนำสื่อหลายๆประเภทมาผสมผสานใช้งานร่วมกันซึ่งอาจประกอบไปด้วยข้อความ ภาพกราฟฟิก เสียงพูด เสียงดนตรี ภาพวีดีโอหรือภาพเคลื่อนไหว การนำเสนอข้อมูลในรูปแบบมัลติมีเดียจะช่วยสร้างความสนใจแก่ผู้ดู น่าติดตามไม่น่าเบื่อ สามารถโต้ตอบการใช้งานได้ง่ายขึ้น และมีความบันเทิง

ส่วนสื่อจัดเก็บข้อมูลเป็นสื่อ(Media) ที่ใช้สำหรับจัดเก็บข้อมูล ชุดคำสั่ง และจัดเก็บสารสนเทศอื่นๆซึ่งถือเป็นหน่วยความจำสำรองกล่าวคือหน่วยความจำหลักของคอมพิวเตอร์นั้นจะเป็นหน่วยความจำแบบชั่วคราว ข้อมูลจะสูญหายหมดหากปราศจากกระแสไฟเลี้ยง ดังนั้นข้อมูลสำคัญต่างๆจึงจำเป็นต้องมีการจัดเก็บไว้บนหน่วยความจำถาวรก่อนที่จะทำการปิดเครื่องเพื่อที่จะได้ข้อมูลที่เก็บลงในสื่อนั้นไปใช้งานในวันข้างหน้าได้ โดยสื่อต่างๆที่ใช้สำหรับที่จัดเก็บข้อมูลนั้นต้องใช้ควบคู่กับอุปกรณ์ขับที่ใช้กับสื่อนั้น

สื่อจัดเก็บข้อมูลอาจแบ่งได้เป็น 2 ชนิด คือ สื่อจัดเก็บข้อมูลที่ใช้เทคโนโลยีแบบแม่เหล็ก (Magnetic Storage) และสื่อจัดเก็บข้อมูลที่ใช้เทคโนโลยีแบบแสง (Optical Storage)สื่อจัดเก็บข้อมูลที่ใช้เทคโนโลยีแบบแม่เหล็ก เช่น ฟลอปปีดิสก์ ดิสก์ความจุสูง ฮาร์ดดิสก์ เทป เป็นต้น สื่อจัดเก็บข้อมูลที่ใช้เทคโนโลยีแบบแสง เช่น ซีดีรอม ดีวีดีรอม ซีดีอาร์และซีดีอาร์ดับบลิว เป็นต้น

ซอฟท์แวร์และการจัดการข้อมูล

ซอฟท์แวร์ คือ กลุ่มชุดของคำสั่ง (Instruction) ที่สั่งให้คอมพิวเตอร์ทำงานเพื่อประมวลผลตาที่ต้องการ แบ่งได้เป็น 2 ประเภท คือ ซอฟท์แวร์ระบบ (System Software) และซอฟต์แวร์ประยุกต์ (Application Software)

(1) ซอฟท์แวร์ระบบ (System Software)

ซอฟท์แวร์ระบบ คือ โปรแกรมที่ทำหน้าที่ในการควบคุมการทำงานของเครื่องคอมพิวเตอร์รวมถึงอุปกรณ์ต่างๆซึ่งรวมถึงทำหน้าที่เป็นตัวกลางระหว่างผู้ใช้งานกับคอมพิวเตอร์โดยซอฟต์แวร์ระบบยังสามารถแบ่งออกเป็นระบบปฏิบัติการ(Operating System) และโปรแกรมอรรถประโยชน์

ระบบปฏิบัติการเป็นโปรแกรมที่มีความสำคัญมาก ประกอบด้วยชุดโปรแกรมที่ทำหน้าที่ควบคุมดูแลการดำเนินการต่างๆ ภายในระบบคอมพิวเตอร์และเป็นตัวกลางในการประสานการทำงานของฮาร์ดแวร์และซอฟต์แวร์ต่างๆเช่น พีซีคอมแพทเทเบิล(PC- Compateble) บนวินโลว์แพลตฟอร์ม พีซีแมคอินทอชและแมคโอเอสแพลตฟอร์ม ลีนุกต์แพลตฟอร์ม

โปรแกรมอรรถประโยชน์เป็นโปรแกรมที่ใช้งานเฉพาะอย่าง เช่น โปรแกรม Scan Disk,Disk Defragmenter,System Restore และ Back up เป็นต้น

(2) ซอฟต์แวร์ประยุกต์ (Application Softeare)

ซอฟต์แวร์ประยุกต์เป็นซอฟต์แวร์ที่นำมาใช้สำหรับงานเฉพาะด้าน ได้แก่ ชุดซอฟต์แวร์ต่างๆ ที่ใช้กับระบบงานทางธุรกิจหรือระบบงานอื่นๆที่เกี่ยวข้อง เช่น ซอฟต์แวร์ที่ใช้กับการจัดการวัตถุดิบ บัญชี สินค้าคงคลัง ซอฟต์แวร์โรคผู้ป่วยที่ใช้กับวงการแพทย์

สำหรับการจัดการข้อมูลในคอมพิวเตอร์นั้นก่อนอื่นต้องทำความเข้าใจพื้นฐานถึงแฟ้มข้อมูลก่อน

โครงสร้างแฟ้มข้อมูลประกอบด้วยโครงสร้างพื้นฐานที่ลำดับจากหน่วยที่เล็กที่สุดไปยังหน่วยที่ใหญ่ขึ้นตามลำดับคือ บิต ไบต์ ฟิลด์ เรคคอร์ด และ ไฟล์ แฟ้มข้อมูลพื้นฐานมี4 ประเภท คือ แฟ้มข้อมูลหลัก (Master File) แฟ้มข้อมูลรายงานความเปลี่ยนแปลง (Transaction File) แฟ้มรายงาน (Report File) แฟ้มข้อมูลชั่วคราว (Temporary File)

การจัดการแฟ้มข้อมูลอาจแบ่งได้เป็น 2 วิธี คือ ระบบแฟ้มข้อมูล (File-base System) และระบบฐานข้อมูล (Database File)

ระบบแฟ้มข้อมูล(File-base System) เป็นการจัดการข้อมูลโดยที่แต่ละหน่วยงานจะมีข้อมูลเป็นของตนเอง ซึ่งมีข้อเสียคือข้อมูลบางอย่างย่อมมีความเกี่ยวข้องกับเช่น แผนกบุคคลกับแผนกขาย ซึ่งข้อมูลของพนักงานในพนักงานขายก็เป็นพนักงานคนหนึ่งในแผนกบุคคล ข้อมูลจึงมีการจัดเก็บซ้ำซ้อน

ระบบฐานข้อมูล (Database File) มีฐานข้อมูลเป็นแหล่งรวมของแฟ้มข้อมูลจากส่วนงานต่างๆ มีกระบวนการจัดหมวดหมู่อย่างเป็นระเบียบแบบแผน ผู้ใช่งานจากส่วนงานต่างๆมารถเข้าถึงฐานข้อมูลส่วนกลางเพื่อนำไปใช้งานหรือประมวลผลร่วมกันได้ทำให้แก้ปัญหาความซ้ำซ้อนของการจัดเก็บข้อมูลได้

**ตัวอย่างรายละเอียดการตรวจพิสูจน์หลักฐานโปรแกรมคอมพิวเตอร์ (Software Forensics) ซึ่งเป็นส่วนหนึ่งของการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ และเป็นเทคนิคในการวิเคราะห์ความเป็นเจ้าของของโปรแกรมคอมพิวเตอร์**

การตรวจพิสูจน์หลักฐานโปรแกรมคอมพิวเตอร์ คือการนำความรู้ทางวิทยาศาสตร์มาประยุกต์ใช้ เพื่อพิสูจน์ข้อเท็จจริงในคดีความที่เกี่ยวกับโปรแกรมคอมพิวเตอร์ เพื่อผลในการบังคับใช้กฎหมายและการลงโทษ ดังนั้นเมื่อเกิดกรณีการละเมิดลิขสิทธิ์ว่ามีการกระทำซ้ำ มีการลอกเลียน หรือดัดแปลง หรือกรณีที่มีการกระทำผิดทางอาญาที่เกี่ยวกับโปรแกรมคอมพิวเตอร์ เช่น มีการปล่อยไวรัสทำให้ระบบคอมพิวเตอร์เสียหาย เป็นต้น การนำการตรวจพิสูจน์หลักฐานโปรแกรมคอมพิวเตอร์มาใช้เพื่อพิสูจน์ข้อเท็จจริงว่าโปรแกรมดังกล่าวเหมือนหรือคล้ายกันกับโปรแกรมต้นฉบับหรือไม่ ใครเป็นเจ้าของไวรัสหรือโปรแกรมที่ประสงค์ร้ายจึงมีความสำคัญที่จะพิสูจน์ให้ทราบข้อเท็จจริงและนำผลไปใช้ในทางกฎหมายต่อไปได้

โปรแกรมคอมพิวเตอร์โดยทั่วไปจะเขียนในรูปที่เรียกว่ารหัสต้นฉบับ (Source Code) ซึ่ง Source Code เป็นรูปแบบข้อความหรือชุดคำสั่งของโปรแกรมคอมพิวเตอร์ที่เขียนโดยโปรแกรมเมอร์ ในบางกรณี Source Code ได้มาโดยโปรแกรมอื่น Source Code เขียนอยู่บนพื้นฐานของคำสั่งที่มีระดับสูงกว่า (โดยปกติจะเขียนเป็นแบบสั้น (Abstract) หรือใช้สภาพแวดล้อมการออกแบบด้วยภาพ (Visual Design Environment) ดังนั้น Source Code ทุกระดับจะเขียนด้วยภาษาโปรแกรมระดับสูง ยกเว้นที่เขียนด้วยภาพ

ภาษาโปรแกรมคอมพิวเตอร์ถือว่าเป็นรูปแบบของภาษาในทางภาษาศาสตร์ หรือเป็นเป็นชุดของภาษาที่เป็นประเภทเฉพาะ ภาษาที่ใช้เขียนโปรแกรมคอมพิวเตอร์จะแตกต่างกันใแง่ของเวลาหรือยุคที่เรียกว่า Generation (เวลาที่โปรแกรมได้สร้างขึ้นและสะท้อนถึงระดับของแนวคิด) ประเภท (Type) เช่น ภาษากระบวนคำสั่ง ภาษาไม่เป็นกระบวนการคำสั่ง ภาษาเชิงอ็อบเจกต์ และภาษาเชิงหน้าที่ ดังนั้นโปรแกรมดังกล่าวสามารถตรวจสอบจากการตรวจพิสูจน์หลักฐานเช่นเดียวกับข้อความที่เป็นการเขียน

```
// Factorial takes an integer as an returns
// the factorial of the input
// This routine does not deal with negative valuest
Int Factorial (int Input)
{
        Int Counter;
        Int Fact;
        Fact = 1; // Initializes Fact to 1 since factorial 0
is 1
        For (Counter=Input; Counter>1;
Counter=Counter-1
        {
                Fact = Fact*Counter;
        }
        Return Fact;
}
```

**รูปภาพที่เป็นส่วนของโปรแกรมภาษา C++**

จากรูปภาพที่ ๑ แสดงให้เห็นถึงรหัสสองส่วนที่เขียนโดยภาษา C++ โดยโปรแกรมเมอร์สองคนที่แตกต่างกัน โปรแกรมเมอร์ทั้งสองจะเขียนเพื่อให้ทำงานตามหน้าที่ที่เหมือนกันคือ การคำนวณทางคณิตศาสตร์แฟกทอเรียล (Factorial (n)) ที่ปกติจะเขียน n! กล่าวคือ สิ่งที่นำเข้าที่เหมือนกันทำให้เกิดผลเหมือนกัน

```
Int  f(int x)  {
Int a, y = 1;
If (lx) return 1; else return x*f(x-1); }
```

โปรแกรมเมอร์แต่ละคนจะมีขั้นตอนวิธี หรือลำดับขั้นตอนที่แน่นอนซึ่งใช้ในการแก้ไขปัญหาเดียวกันแตกต่างจากโปรแกรมเมอร์คนอื่นซึ่งเรียกว่า อัลกอริทึม (Algorithm)[2] และมี

วิธีการเขียน (Style) ที่แตกต่างกันในการเขียนรหัส ขั้นตอนวิธีที่ 1 คือการวนซ้ำ (Loop)[3] จากค่าที่เริ่มจาก 1 หลังจากนั้นมีข้อมูลนำเข้า ส่วนขั้นตอนวิธีที่ 2 ซับซ้อนมากขึ้น กล่าวคือ เป็นการเรียกซ้ำหรือ Recursion[4] ความแตกต่างของการเขียนจะรวมถึงการเขียนหมายเหตุ (Comment) ชื่อตัวแปร (Variable names) การเว้นบรรทัด (Space) การจัดย่อหน้า (Indentation)[5] และระดับของความสามารถในแต่ละหน้าที่หรือฟังก์ชัน

ส่วนของรหัสข้างต้นนี้สั้นเกินไปหรือไม่มีนัยสำคัญ อย่างไรก็ตาม ทำให้เห็นภาพความสามารถของโปรแกรมเมอร์ในการเขียนโปรแกรมที่มีลำดับขั้นตอนที่ต่างจากโปรแกรมเมอร์คนอื่นโดยปราศจากการแนะนำให้ทำอย่างนั้น ฟังก์ชันหรือหน้าที่ต่าง ๆ ในโปรแกรมมีวิธีการเขียนอย่างเป็นธรรมชาติของผู้สร้างสรรค์ และสะท้อนถึงความแตกต่างที่ชัดแจ้งระหว่างโปรแกรมเหล่านั้นได้

รหัสต้นฉบับที่เขียนโดยภาษาต่าง ๆ[6] เป็นชุดของข้อความที่เป็นคำสั่งให้เครื่องคอมพิวเตอร์ทำงาน ในกรณีตัวอย่างข้างต้นเป็นเพียงคำสั่งที่กำหนดหน้าที่ให้คอมพิวเตอร์ทำงานแบบง่ายและสั้นที่สามารถถูกเรียกใช้จากส่วนอื่นของโปรแกรมได้ โปรแกรมเหล่านี้จะถูกเขียนมาโดยมีส่วนที่แตกต่างกันและลำดับขั้นตอนของการปฏิบัติงานทั่วไป โดยขั้นตอนจะรวมถึงลำดับที่เป็นเงื่อนไข เช่น เงื่อนไขแบบมีเหตุผลอาจทำให้เกิดการทำซ้ำ การเพิ่ม หรือการละเว้นคำสั่งบางอย่างที่มีอยู่ในรหัสนั้น

แม้รหัสต้นฉบับเป็นภาษาที่เป็นพิธีการและเข้มงวดมากกว่าภาษาพูด หรือภาษาเขียน โปรแกรมเมอร์ยังคงมีระดับของความยืดหยุ่นอยู่มาก เมื่อมีการเขียนโปรแกรมในการให้คอมพิวเตอร์ปฏิบัติงาน ความยืดหยุ่นนี้จะรวมถึงลักษณะที่งานจะถูกทำให้สำเร็จ (ขั้นตอนวิธีที่ใช้ในการแก้ปัญหา) วิธีที่รหัสต้นฉบับได้ถูกแสดงออกในรูปของการออกแบบ (การเว้นบรรทัด การย่อหน้า ตัวอักษรที่ใช้เป็นในการเริ่มต้นส่วนต่าง ๆ ของรหัส เป็นต้น) และลักษณะที่เกี่ยวกับรูปแบบที่ขั้นตอนวิธีจะถูกทำขึ้น (เช่น การเลือกข้อความ หรือชื่อของตัวแปรต่างๆ)

---

[2] ชุดของคำสั่งที่บอกเป็นขั้นเป็นตอน ปกติมักใช้เพื่ออธิบายคำสั่งที่เขียนด้วยภาษาโปรแกรม เช่น ภาษาซี ซึ่งเป็นคำสั่งงานแบบเป็นทางการที่สามารถติดตามการทำงานได้ในแต่ละขั้น เช่น สูตรคณิตศาสตร์หรือชุดคำสั่งในโปรแกรมคอมพิวเตอร์

[3] การเขียนโปรแกรมให้ปฏิบัติการซ้ำๆ จนกว่าจะเป็นไปตามเงื่อนไขที่กำหนด

[4] กระบวนการที่เกิดขึ้นเมื่อซอร์ฟแวร์รูทีนหรือโพรซีเยอร์เรียกตัวเองขณะทำงาน

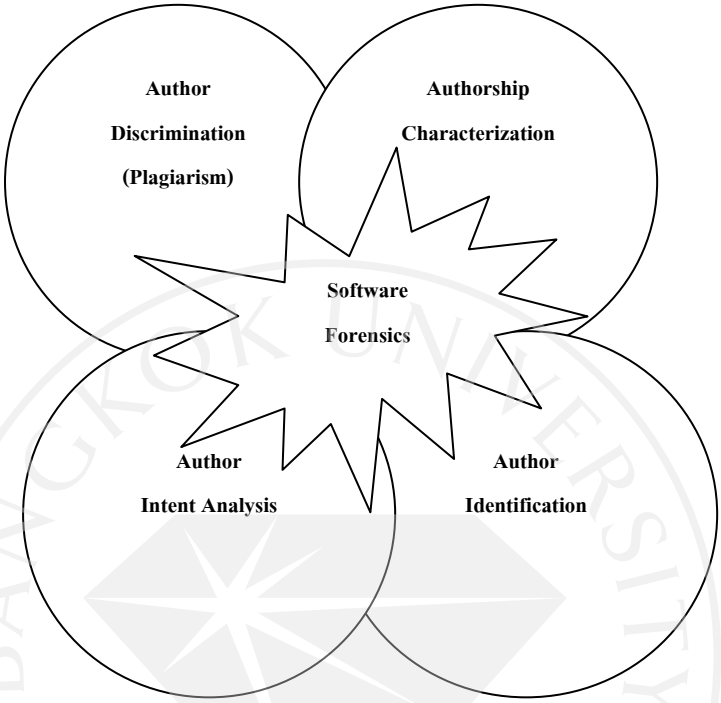
[5] การจัดย่อหน้าภายในหน้ากระดาษ บรรทัดแรกของทุก ๆ ย่อหน้าจะเลื่อนเยื้องเข้าไปเพื่อทำให้ข้อความอ่านได้ง่ายขึ้น

[6] ซึ่งในขณะนี้เป็นภาษายุคที่สามที่รวมภาษาโปรแกรมต่าง ๆเอาไว้

ทางเลือกอื่น ๆ ที่โปรแกรมเมอร์มี เช่น การเลือกฮาร์ดแวร์ที่มีระบบปฏิบัติการ ภาษาที่ใช้เขียน ตัวแปรคำสั่ง และโปรแกรมที่ใช้พิมพ์งานที่นำมาใช้ การที่โปรแกรมเมอร์สามารถมีการ

ตัดสินใจได้มากขึ้นทำให้เพิ่มความเข้มข้นของเสรีภาพและการแสดงออก ลักษณะต่าง ๆ ของโปรแกรมคอมพิวเตอร์ เช่น ขั้นตอนวิธี การออกแบบ รูปแบบและสภาพแวดล้อมสามารถเป็นการเฉพาะต่อโปรแกรมเมอร์แต่ละรายหรือแต่ละประเภทของโปรแกรมเมอร์ ซึ่งเป็นความแตกต่างระหว่างโปรแกรมเมอร์ และเป็นความจริงหากการรวมกันของลักษณะต่าง ๆ และสำนวนการเขียนโปรแกรมจะทำให้เกิดข้อความหรือคำที่ใช้แก้ปัญหาของโปรแกรมเมอร์นั้น ๆ ดังนั้นจึงดูเหมือนว่าโปรแกรมคอมพิวเตอร์สามารถมีข้อมูลที่เป็นพยานหลักฐานที่ใช้ชี้ระบุตัวและลักษณะของผู้เป็นเจ้าของ ดังนั้นหากมีการแยกแยะว่ารหัสต้นฉบับของโปรแกรมตามความเป็นจริงแล้วเป็นภาษาประเภทหนึ่งที่เหมาะสำหรับการวิเคราะห์ความเป็นเจ้าของแล้วการประยุกต์ใช้และเทคนิคต่างก็จะเกิดขึ้นมากมาย ส่วนสัดของงานที่ใช้ในภาษาศาสตร์ในการคำนวณสำหรับการวิเคราะห์หาผู้เป็นเจ้าของข้อความ จึงเทียบเท่ากับรหัสต้นฉบับของโปรแกรมคอมพิวเตอร์ ในลักษณะที่คล้ายคลึงกัน เทคนิคที่ใช้ในการตรวจพิสูจน์หลักฐานสำหรับการตรวจลายมือและภาษาจึงสามารถนำมาใช้เป็นการตรวจพิสูจน์หลักฐานโปรแกรมคอมพิวเตอร์ ดังนั้นคำว่าการตรวจพิสูจน์หลักฐานโปรแกรมคอมพิวเตอร์จึงหมายถึงการใช้มาตรวัดจากรหัสต้นฉบับหรือรหัสภาษาเครื่องในจุดมุ่งหมายทางกฎหมายหรือเป็นทางการ

# ผนวก ค
# ประเภทของรหัสที่ใช้สำหรับการวิเคราะห์การตรวจพิสูจน์พยานหลักฐานโปรแกรมคอมพิวเตอร์




**การตรวจพิสูจน์หลักฐานโปรแกรมคอมพิวเตอร์**

**ประเภทของรหัสที่ใช้สำหรับการวิเคราะห์ (Types of code available for analysis)**

รหัสที่ใช้ในการวิเคราะห์มีทั้งที่เป็นโปรแกรมจริงที่ทำงานได้ (The executable) และรหัสต้นฉบับ (Source code)

**ก. โปรแกรมจริงที่ทำงานได้ (Executable code)**

ประเภทของโปรแกรมจริงที่ทำงานได้ที่ใช้โจมตีระบบมีดังนี้

**ไวรัส** (Viruses) ไวรัสเป็นโปรแกรมที่ติดตนเองอยู่กับโปรแกรมอื่นเพื่อที่จะทำซ้ำตนเอง

**เวิร์ม** (Worms) เป็นโปรแกรมเดี่ยวที่เพิ่มทวีโดยการทำซ้ำตนเอง คล้ายกับไวรัสแต่ปราศจากโปรแกรมอื่นที่เป็นหลัก

**โทรจานฮอร์ส** (Trojan horse) เป็นโปรแกรมที่ส่งให้เกิดผลที่ไม่ประสงค์โดยเสแสร้งว่าเป็นโปรแกรมที่มีประโยชน์ ซึ่งสามารถเป็นทั้งโปรแกรมที่เขียนขึ้นและเป็นผลมาจากการปรับแต่งโปรแกรมที่มีอยู่เดิม

**โลจิกบอมบ์** (Logic bomb) เป็นส่วนของโปรแกรมที่เขียนขึ้นเพื่อทำให้เกิดการกระทำที่ไม่ประสงค์เมื่อมีเหตุการณ์ใดเหตุการณ์หนึ่งเป็นสิ่งกระตุ้นให้เกิดขึ้น

โดยปกติแล้วไวรัสจะทิ้งรหัสของตนไว้ในโปรแกรมที่ถูกทำลาย อย่างไรก็ตาม รหัสที่ถูกแปลงแล้ว หลักฐานส่วนมากจะสูญหายไปรวมถึงชื่อตัวแปร การออกแบบ และหมายเหตุ แต่สิ่งที่ยังคงหลงเหลืออยู่คือ

- โครงสร้างข้อมูลและขั้นตอนวิธี (Data structures and algorithms) สามารถชี้ให้เห็นภูมิหลังของโปรแกรมเมอร์ เนื่องจากส่วนมากแล้วโปรแกรมเมอร์จะใช้ขั้นตอนวิธีเฉพาะที่ได้เรียนมาหรือแสดงออก และมีความสบายใจในการใช้ การไม่มีทางเลือกที่ดีที่สุดอาจจะชี้ให้เห็นถึงการขาดความรู้หรือโปรแกรมเมอร์นั้นใช้รูปแบบการเขียนโปรแกรมของผู้อื่นหรืออาจมองถึงความชอบหรือเป็นภาษาที่นิยมใช้มากที่สุด
- คอมไพเลอร์และข้อมูลระบบ (Compiler and system information) รหัสโปรแกรมจริงที่ทำงานได้ประกอบไปด้วยเครื่องหมายที่อาจชี้ให้ถึงคอมไพเลอร์ที่ใช้
- รหัสของทักษะการเขียนโปรแกรมและขอบเขตของความรู้ (Level of programming skill and areas of knowledge) ความเข้มข้นของความซับซ้อนและความง่ายสามารถชี้ให้เห็นถึงผู้ที่เป็นเจ้าของ ความแตกต่างในความซับซ้อนภายในโปรแกรมชี้ให้เห็นถึงการผสมผสานของเจ้าของหลายคนหรือเจ้าของคนเดียวที่เชี่ยวชาญในเฉพาะทาง
- ทางเลือกของการเรียกใช้ระบบ (Choice of System Calls) กล่าวคือ หน้าที่หรือ Functions ที่ใช้ในการสนับสนุนในรหัสอาจชี้ให้เห็นบางอย่างเกี่ยวกับพื้นภูมิหลังของโปรแกรมเมอร์ ข้อผิดพลาด (Errors) ที่ปรากฏในรหัส รหัสเกือบทั้งหมดจะมีข้อผิดพลาด และระบบที่ซับซ้อนจะมีจุดบกพร่องอย่างแน่นอน โปรแกรมเมอร์จะมีข้อผิดพลาดที่เหมือนๆกันเสมอ ๆ
- **ข.รหัสต้นฉบับ (Source code)**

สิ่งที่สามารถนำมาใช้ในการวิเคราะห์รหัสต้นฉบับของโปรแกรมที่ประสงค์ร้าย (Malicious programs) มีหลายอย่าง เช่นภาษาที่ใช้เขียนโปรแกรม (Programming language)

ภาษาสามารถชี้ให้เห็นพื้นภูมิหลังของเจ้าของเนื่องจากโปรแกรมเมอร์จะไม่ใช้ภาษาที่ไม่คุ้นเคย รวมถึงความชอบทางจิตวิทยาที่โปรแกรมเมอร์อาจรู้สึกต่อภาษาใดภาษาหนึ่ง

**ค. การจัดรูปแบบของรหัส (Formatting of code)** วิธีที่รหัสต้นฉบับได้ถูกจัดรูปแบบ สามารถชี้ให้เห็นทั้งข้อมูลของเจ้าของและทางจิตวิทยาที่เกี่ยวกับเจ้าของ Pretty-printers จะใช้ในการจัดรูปแบบรหัสต้นฉบับอัตโนมัติซึ่งจะทำให้ไม่ทราบข้อมูลเฉพาะเจ้าของแต่จะทราบว่า Pretty – printers แบบใดที่นำมาใช้ลักษณะเฉพาะ (Special features) เช่น Macros[1] อาจใช้ในการชี้ว่าเป็นคอมไพเลอร์หรือ Library แบบใด

**ง. วิธีการเขียนหมายเหตุ (Commenting style)** สามารถทำให้เห็นความแตกต่างของวิธีการของโปรแกรมเมอร์ หากหมายเหตุมากพอจะทำให้สามารถใช้การวิเคราะห์ภาษาศาสตร์ของข้อความ (Textual linguistic analysis)

**จ. การตั้งชื่อตัวแปร (Variable naming)** เป็นการแสดงความแตกต่างของรูปแบบของเจ้าของ การใช้ชื่อที่มีความหมายหรือไม่มีความหมาย การใช้มาตรฐาน และการใช้ตัวอักษรใหญ่ในชื่อตัวแปร

**ฉ. การสะกดและไวยากรณ์ (Spelling and grammar)** การตรวจการสะกดและไวยากรณ์สามารถใช้ชี้ความเป็นเจ้าของได้ ความผิดพลาดในการสะกดอาจมีได้ในชื่อตัวแปรและในโปรแกรมย่อย

**ช. แบบของการใช้ภาษา (Use of language features)** โปรแกรมเมอร์บางคนชอบที่จะใช้แบบเฉพาะของภาษามากว่าคนอื่น

**ซ. ขนาด (Size)** ขนาดของรูทีนหรือโปรแกรมย่อยสามารถชี้ให้เห็นความเข้มข้นความสามารถในการใช้สมองหรือพุทธิพิสัยของโปรแกรมเมอร์

**ฌ. ข้อผิดพลาด (Errors)** โปรแกรมเมอร์จะมีข้อผิดพลาดที่เหมือนหรือคล้าย ๆ กัน

**ญ. การนำรหัสมาใช้อีกครั้ง (Reuse of code)** ถ้ารหัสเดิมที่มีการชี้ชัดถึงผู้เป็นเจ้าของได้ถูกนำมาใช้ ก็สามารถชี้ให้เห็นเจ้าของหรือความเชื่อโยงได้

[1] เครื่องมือที่เขียนด้วยโปรแกรมระดับสูงที่ใช้เพื่อจัดการงานหรือกระบวนงานอัตโนมัติภายในโปรแกรมแมคโครทำงานเฉพาะภายในโปรแกรมเฉพาะเท่านั้น

**การวิเคราะห์รหัสที่ประสงค์ร้าย (Analysis of malicious code)**

สิ่งที่ต้องตอบคำถามให้ได้ในเบื้องต้นคือ

- รหัสดังกล่าวทำอะไร เป็นคำถามที่ตอบโดยวิศวกรหรือ Software Engineers
- ใครเขียนรหัสดังกล่าว เป็นคำถามที่เกี่ยวกับความเป็นเจ้าของรหัสนั้น
- รหัสดังกล่าวเขียนเมื่อใด เนื่องจากหากระยะเวลาผ่านไป โปรแกรมเมอร์อาจมีการเปลี่ยนแปลงรูปแบบของตน หรืออาจมีการเขียนเพิ่มเติมโปรแกรมในภายหลัง

ความตั้งใจของรหัส ซึ่งอาจเกิดขึ้นโดยผิดพลาดหรือโดยตั้งใจ ซึ่งเป็นปัญหามากเพราะไม่สามารถที่พิสูจน์ถึงเจตนาหรือความประมาท ตัวอย่างกรณีเช่นการโจมตีแบบโลจิกบอมบ์ที่ทำขึ้นเนื่องจากมีการเอาลูกจ้างฝ่ายการจ่ายเงินเดือนขององค์กรออก เป็นการตั้งใจ อย่างไรก็ตามอาจมีกรณีที่เป็นทั้งตั้งใจหรือไม่สามารถหลีกเลี่ยงความบกพร่องของรหัส

**กรณีศึกษาที่เกี่ยวข้อง**

กรณีศึกษา 2 กรณี ที่มีการวิเคราะห์เกี่ยวกับรหัสที่ประสงค์ร้ายต้นฉบับ คือ เวิร์ม WANK และ OilZ กับเวิร์มอินเทอร์เน็ต (The Internet Worm)

1.The Internet Worm

สแปมฟอร์ดได้วิเคราะห์เวิร์มอินเทอร์เน็ตที่เขียนโดยโรเบิร์ต มอร์ริส ซึ่งได้ปล่อยในอินเทอร์เน็ตเมื่อเดือนพฤศจิกายน 2531 เป็นการวิเคราะห์ทางเทคนิคและการหาความเป็นเจ้าของ โดยอาศัยพื้นฐานจาก 3 รุ่นหรือเวอร์ชั่นของโปรแกรมเวิร์มที่ได้กระทำโดยกระบวนวิศวกรรมย้อนรอยซึ่งได้สร้างขึ้นเป็นเอกเทศและสะท้อนถึงรหัสต้นฉบับ บทสรุปมีดังนี้

- รหัสเขียนไม่ดีและมีข้อผิดพลาดกับไม่มีประสิทธิภาพ
- รหัสไม่สามารถแปลงไปใช้กับระบบปฏิบัติการอื่น
- รหัสบางทีอาจไม่ได้ตรวจสอบโดยใช้โปรแกรมที่อำนวยความสะดวกในการตรวจสอบ
- รหัสมีการรองรับข้อบกพร่องน้อยมาก ทำให้มองเห็นว่าเจ้าของเป็นคนที่ลวกๆและมีการรองรับข้อบกพร่องน้อยมาก สิ่งที่เป็นไปได้อีกคือเวิร์มที่ปล่อยออกมายังไม่สมบูรณ์พอ
- รหัสชี้ว่าเวอร์ชั่นสุดท้ายน่าจะครอบคลุมมากกว่า
- โครงสร้างข้อมูลที่ใช้เป็นลิงค์ลิสต์ (Linked lists)[2] ทั้งหมดที่ไม่มีประสิทธิภาพและชี้ให้เห็นการขาดความสามารถหรือการอบรมในการเขียนโปรแกรม
- รหัสประกอบด้วยความซ้ำซ้อนของกระบวนการ

- ส่วนที่ใช้ในการแปลงข้อมูลเพื่อเป็นรหัสมีประสิทธิภาพอย่างมากและเป็นฟังก์ชันที่ไม่ใช้โดยเวิร์มอื่น ๆ
- รหัสดูเหมือนว่าจะมีการเขียนที่ใช้เวลานาน

ข้อสังเกตข้างต้นชี้ให้เห็นถึงจำนวนองค์ความรู้ที่ได้มาจากรหัสต้นฉบับ จุดสำคัญคือการขาดความสามารถของเจ้าของ เวิร์มที่ปล่อยออกมายังไม่สมบูรณ์พอ ความเป็นเจ้าของคู่และรหัสใช้เวลาในการเขียนนาน

เมื่อเปรียบเทียบกับรหัสของ โรเบิร์ต มอร์ริสแล้ว ข้อสังเกตข้างต้นกับเมทริกซ์อื่นในรายละเอียดจะนำไปสู่การชี้เอกลักษณ์ของมอร์ริสว่าเป็นเจ้าของรหัส

**2. The WANK and OILZ worms**

ลองสต๊าฟและชูลซ์นักโปรแกรมเมอร์ได้ศึกษาเกี่ยวกับเวิร์มชื่อ WANK และ OILZ ซึ่งได้ถูกปล่อยออกมาในปี 2532 เพื่อจู่โจมระบบของนาซ่า (NASA) และระบบของ DOE เวิร์มทั้งสองตัวนี้เขียนในภาษา DCL ซึ่งเป็นภาษาลายมือ (A scripting language) โดย WANK เริ่มหลัง OILZ ประมาณ 2 อาทิตย์

---

[2] โครงสร้างข้อมูลมีวิธีการเชื่อมโยงข้อมูลตัวหนึ่งกับข้อมูลอีกตัวหนึ่งโยงกันไปเรื่อย ๆ ลิงค์ลิสต์ประกอบด้วย 2 ส่วนคือ ข้อมูลและตัวชี้ (Pointer)

ข้อเท็จจริงที่ว่าเวิร์มทั้งสองเขียนด้วยภาษา DCL เป็นภาษาที่ไม่ต้องแปลงและให้ข้อมูลมากกว่าโปรแกรมที่แปลงแล้ว WANK เขียนด้วยคำสั่งทั้งหมด 785 บรรทัด และออกแบบเป็นรหัสที่มีโครงสร้าง ลองสต๊าฟและชูลซ์ได้ตั้งข้อสังเกตดังนี้

- มีเจ้าของสามคนที่เขียนระบบนี้
- เจ้าของคนที่ 1
    - มีรูปแบบเชิงวิชาการในการเขียน
    - มีลักษณะพรรณนาและชื่อตัวแปรเป็นตัวพิมพ์เล็ก
    - การไหลอยู่บนพื้นฐานของตัวแปร คำสั่ง gotos และโปรแกรมย่อย subroutines และซับซ้อน
    - มีระดับความเข้าใจที่สูง
    - เป็นการทดลองมากกว่ามีความตั้งใจที่ประสงค์ร้าย
- เจ้าของคนที่ 2
    - เป็นรหัสที่ประสงค์ร้ายโดยตั้งใจที่มีเจตนาร้าย
    - ใช้ความหยาบคาย
    - ใช้อักษรตัวพิมพ์ใหญ่
    - รูปแบบการเขียนที่ง่าย ๆ
- เจ้าของคนที่ 3
    - นำเอารหัสคนอื่นมาประกอบ
    - ใช้ตัวพิมพ์ทั้งตัวใหญ่และเล็ก
    - ชื่อตัวแปรไม่มีพรรณนา
    - เขียนรหัสง่าย ๆ คล้ายภาษา BASIC
    - มีความพยายามแก้ไข Bug ในรหัส โดย OILZ แก้ไข Bugs บางอย่างใน WANK

ชิ้นส่วนของพยานหลักฐานนี้มีค่าในการสืบสวนการจู่โจม จุดหลักคือมีเจ้าของหลายคนและความแตกต่างในระหว่างเจ้าของนั้น ข้อมูลดังกล่าวนี้อาจจะไม่นำไปสู่การชี้ชัดว่าใครเป็นผู้เกี่ยวเนื่องบ้าง แต่ทำให้เกิดพยานหลักฐานที่อาจเพียงพอในความแน่ชัดอยู่ในระดับที่น่าพอใจ

ดังนั้น การตรวจพิสูจน์หลักฐานโปรแกรมคอมพิวเตอร์ จึงมีความสำคัญมากขึ้นในกระบวนการทั้งทางอาญาและทางแพ่ง รวมทั้งบางสิ่ง เช่น การค้นหาการลอกเลียนแบบทางวิชาการ (Academic plagiarism detection) ได้มีการประดิษฐ์เครื่องมือหรือโปรแกรม ตัวอย่างเช่น

1. IDENTIFIED (Intergrated Dictionary-based Extraction of Non-language-dependent Token Information for Forensics Identification, Examination, and Discrimination)[3] เพื่อช่วยศึกษาปัญหาในทางกฎหมาย โปรแกรมนี้ประกอบด้วยการให้เหตุผลโดยเทียบกับคดีก่อน (Case – based Reasoning) การวิเคราะห์โดยใช้ Discriminant analysis และเทคนิคอื่น ๆ รวมถึงโมเดลทางสถิติในเรื่อง certainty
2. The Access Data Forensics Toolkit® (FTK ™) ที่ให้เจ้าหน้าที่ในกระบวนการยุติธรรมและเจ้าหน้าที่ด้านความปลอดภัยในการใช้ตรวจพิสูจน์คอมพิวเตอร์ โดยกลั่นกรองค้นหาฟังก์ชัน ค้นหาไฟล์เพื่อพบพยานหลักฐานที่ต้องการ รวมทั้งใช้วิเคราะห์อีเมล์

---

[3] Gray, A.R., Sallis, P.J., and MacDonnell, S.G. (1998). IDENTIFIED (Intergrated Dictionary-based Extraction of Non-language-dependent Token Information for Forensics Identification, Examination, and Discrimination): **A dictionary-based system for extracting source code metrics for software forensics**. Submitted to SE:E&P'98 Software Engineering: Education & Practice. Dunedin. New Zeland.

**ผนวก ง**

**พระราชบัญญัติ**

**ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2)**

**พ.ศ. 2551**

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ 6 กุมภาพันธ์ พ.ศ. 2551

เป็นปีที่ 63ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา 1 พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551”

มาตรา 2 พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา 3 ให้เพิ่มความต่อไปนี้เป็นวรรคสองของมาตรา 8 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

“ในกรณีที่กฎหมายกำหนดให้ต้องมีการปิดอากรแสตมป์ หากได้มีการชำระเงินแทนหรือดำเนินการอื่นใดด้วยวิธีการทางอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่หน่วยงานของรัฐซึ่งเกี่ยวข้องประกาศกำหนด ให้ถือว่าหนังสือ หลักฐานเป็นหนังสือ หรือเอกสาร ซึ่งมีลักษณะเป็นตราสารนั้นได้มีการปิดอากรแสตมป์และขีดฆ่าตามกฎหมายนั้นแล้ว ในการนี้ในการกำหนดหลักเกณฑ์และวิธีการของหน่วยงานของรัฐดังกล่าว คณะกรรมการจะกำหนดกรอบและแนวทางเพื่อเป็นมาตรฐานทั่วไปไว้ด้วยก็ได้”

มาตรา 4 ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา 9 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

“วิธีการที่เชื่อถือได้ตาม (2) ให้คำนึงถึง

ก. ความมั่นคงและรัดกุมของการใช้วิธีการหรืออุปกรณ์ในการระบุตัวบุคคล สภาพพร้อมใช้งานของทางเลือกในการระบุตัวบุคคล กฎเกณฑ์เกี่ยวกับลายมือชื่อที่กำหนดไว้ในกฎหมาย ระดับความมั่นคงปลอดภัยของการใช้ลายมือชื่ออิเล็กทรอนิกส์ การปฏิบัติตามกระบวนการในการระบุตัวบุคคลผู้เป็นสื่อกลาง ระดับของการยอมรับหรือไม่ยอมรับ วิธีการที่ใช้ในการระบุตัวบุคคลในการทำธุรกรรม วิธีการระบุตัวบุคคล ณ ช่วงเวลาที่มีการทำธุรกรรมและติดต่อสื่อสาร

ข. ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ จำนวนครั้งหรือความสม่ำเสมอในการทำธุรกรรม ประเพณีทางการค้าหรือทางปฏิบัติ ความสำคัญ มูลค่าของธุรกรรมที่ทำ หรือ

ค. ความรัดกุมของระบบการติดต่อสื่อสาร

ให้นำความในวรรคหนึ่งมาใช้บังคับกับการประทับตราของนิติบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ ด้วยโดยอนุโลม”

มาตรา 5 ให้เพิ่มความต่อไปนี้เป็นวรรคสี่ของมาตรา 10 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

“ในกรณีที่มีการทำสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ตามวรรคหนึ่งสำหรับใช้อ้างอิงข้อความของข้อมูลอิเล็กทรอนิกส์ หากสิ่งพิมพ์ออกนั้นมีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์และมีการรับรองสิ่งพิมพ์ออกโดยหน่วยงานที่มีอำนาจตามที่คณะกรรมการประกาศกำหนดแล้ว ให้ถือว่าสิ่งพิมพ์ออกดังกล่าวใช้แทนต้นฉบับได้”

มาตรา 6 ให้ยกเลิกความในมาตรา 11 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และให้ใช้ความต่อไปนี้แทน

“มาตรา 11 ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้นให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวงให้นำความในวรรคหนึ่งมาใช้บังคับกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย”

มาตรา 7 ให้เพิ่มความต่อไปนี้เป็นมาตรา 12/1 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

“มาตรา 12/1 ให้นำบทบัญญัติในมาตรา 10 มาตรา 11 และมาตรา 12 มาใช้บังคับกับเอกสารหรือข้อความที่ได้มีการจัดทำหรือแปลงให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ในภายหลังด้วยวิธีการทางอิเล็กทรอนิกส์ และการเก็บรักษาเอกสารและข้อความดังกล่าวด้วยโดยอนุโลม การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ตามวรรคหนึ่งให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด”

มาตรา 8 ให้ยกเลิกความในวรรคหนึ่งของมาตรา 36 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และให้ใช้ความต่อไปนี้แทน

“มาตรา 36 ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์”

ประกอบด้วย รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นประธานกรรมการ

ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นรองประธานกรรมการ และกรรมการอื่นอีกจำนวนสิบสองคนซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้ทรงคุณวุฒิด้านการเงิน ด้านการพาณิชย์อิเล็กทรอนิกส์ ด้านนิติศาสตร์ ด้านวิทยาการคอมพิวเตอร์ ด้านวิทยาศาสตร์หรือวิศวกรรมศาสตร์และด้านสังคมศาสตร์ ที่ได้รับการสรรหาด้านละสองคน ทั้งนี้ ผู้ทรงคุณวุฒิคนหนึ่งของแต่ละด้านต้องมาจากภาคเอกชน และให้หัวหน้าสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นกรรมการและเลขานุการ”

มาตรา 9 ให้เพิ่มความต่อไปนี้เป็นมาตรา 42/1 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

“มาตรา 42/1 ให้คณะกรรมการได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนดคณะอนุกรรมการที่คณะกรรมการแต่งตั้งตามมาตรา 42 ให้ได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะกรรมการกำหนด”

มาตรา 10 ให้ยกเลิกความในมาตรา 43 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และให้ใช้ความต่อไปนี้แทน

“มาตรา 43 ให้จัดตั้งสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นส่วนราชการในสำนักงานปลัดกระทรวง กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ทำหน้าที่เป็นหน่วยงานธุรการของคณะกรรมการ”

มาตรา 11 ในระหว่างที่จัดตั้งสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตามมาตรา 43 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ยังไม่แล้วเสร็จ ให้สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรับผิดชอบทำหน้าที่หน่วยงานธุรการของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ไปพลางก่อนให้ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแต่งตั้งข้าราชการซึ่งดำรงตำแหน่ง ไม่ต่ำกว่าระดับแปดหรือเทียบเท่าในสังกัดสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารทำหน้าที่เป็นหัวหน้าสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ไปพลางก่อนจนกว่าการจัดตั้งสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จะแล้วเสร็จเพื่อประโยชน์ในการปฏิบัติงานตามวรรคหนึ่ง รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจะสั่งให้ข้าราชการในสังกัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมาปฏิบัติงานชั่วคราวในสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารตามความจำเป็นก็ได้

มาตรา 12 ให้นายกรัฐมนตรีและรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้

ผู้รับสนองพระบรมราชโองการ

พลเอก สุรยุทธ์ จุลานนท์

นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากปัจจุบันกฎหมายว่าด้วยธุรกรรม ทางอิเล็กทรอนิกส์ยังไม่มีบทบัญญัติรองรับในเรื่องตราประทับอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่สามารถระบุถึงตัวผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ได้เช่นเดียวกับลายมือชื่ออิเล็กทรอนิกส์ ทำให้เป็นอุปสรรคต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ที่ต้องมีการประทับตราในหนังสือเป็นสำคัญ รวมทั้งยังไม่มีบทบัญญัติที่กำหนดให้สามารถนำเอกสารซึ่งเป็นสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์มาใช้แทนต้นฉบับหรือให้เป็นพยานหลักฐานในศาลได้และโดยที่ได้มีการปรับปรุงโครงสร้างระบบราชการตามพระราชบัญญัติปรับปรุง กระทรวง ทบวง กรม พ.ศ. 2545 และกำหนดให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นหน่วยงานที่มีอำนาจหน้าที่เกี่ยวกับการวางแผน ส่งเสริม พัฒนา และดำเนินกิจการเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารประกอบกับปัจจุบันธุรกรรมทางอิเล็กทรอนิกส์ได้มีการใช้อย่างแพร่หลาย จำเป็นที่จะต้องมีหน่วยงานธุรการเพื่อทำหน้าที่กำกับดูแลเพื่อให้เป็นไปตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และเป็นฝ่ายเลขานุการของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ โดยสมควรจัดตั้งสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สังกัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารขึ้นทำหน้าที่แทนศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ อันจะเป็นการส่งเสริมความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์และเสริมสร้างศักยภาพการแข่งขันในเวทีการค้าระหว่างประเทศสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์เพื่อให้สอดคล้องกับหลักการดังกล่าวจึงจำเป็นต้องตราพระราชบัญญัตินี้

## ผนวก จ

## ข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ. 2540

**“...**

ข้อ 33 ศาลอาจรับฟังข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์เป็นพยานหลักฐานในคดีได้ หาก

(1)การบันทึกข้อมูลโดยเครื่องคอมพิวเตอร์ หรือการประมวลโดยเครื่องคอมพิวเตอร์เป็นการกระทำตามปกติในการประกอบกิจการของผู้ใช้เครื่องคอมพิวเตอร์ และ

(2)การบันทึกและการประมวลผลข้อมูลเกิดจากการใช้เครื่องคอมพิวเตอร์ปฏิบัติงานตามขั้นตอนการทำงานของเครื่องคอมพิวเตอร์อย่างถูกต้อง และแม้หากมีกรณีการทำงานของเครื่องคอมพิวเตอร์ขัดข้องก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

การกระทำตามปกติของผู้ใช้ตาม (1) และความถูกต้องของการบันทึกและการประมวลผลข้อมูลตาม (2) ต้องมีคำรับรองของบุคคลที่เกี่ยวข้องหรือดำเนินการนั้น

ข้อ 34 คู่ความที่ประสงค์จะเสนอข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์จะต้องระบุข้อมูลที่จะอ้างไว้ในบัญชีระบุพยานตามมาตรา 88 แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง พร้อมยื่นคำแถลงแสดงความจำนงเช่นว่านั้น และคำรับรองตามข้อ 33 วรรคสองกับสำเนาสื่อที่บันทึกข้อมูลนั้นในจำนวนที่เพียงพอเพื่อให้คู่ความอีกฝ่ายหนึ่งมารับไปจากเจ้าพนักงานศาล เว้นแต่

(1)สื่อที่บันทึกข้อมูลนั้นอยู่ในความครอบครองของคู่ความฝ่ายอื่น หรือของบุคคลภายนอก ให้คู่ความฝ่ายที่อ้างอิงข้อมูลยื่นคำขอโดยทำเป็นคำร้องต่อศาล ขออนุญาตงดส่งคำรับรองตามข้อ 33 วรรคสอง และสำเนาสื่อที่บันทึกข้อมูล และขอให้ศาลมีคำสั่งเรียกสื่อที่บันทึกข้อมูลนั้นมาจากผู้ครอบครอง โดยให้คู่ความฝ่ายที่อ้างนั้นมีหน้าที่ติดตามเพื่อให้ได้สื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลในวันสืบพยาน หรือในวันอื่นตามที่ศาลเห็นสมควรกำหนด

(2)ถ้าการทำสำเนาสื่อที่บันทึกข้อมูลนั้น จะทำให้กระบวนพิจารณาล่าช้าหรือเป็นที่เสื่อมเสียแก่คู่ความซึ่งอ้างอิงข้อมูลนั้น หรือมีเหตุผลแสดงว่าไม่อาจส่งสำเนาสื่อบันทึกข้อมูลนั้นให้แล้วเสร็จภายในเวลาตามที่กำหนดได้ ให้คู่ความฝ่ายที่อ้างอิงข้อมูลยื่นคำขอโดยทำเป็นคำร้องต่อศาลขออนุญาตงดส่งสำเนาสื่อที่บันทึกข้อมูลและขอนำสื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลในวันสืบพยานหรือในวันอื่นตามที่ศาลเห็นสมควรกำหนด

ถ้าคู่ความฝ่ายที่อ้างอิงไม่สามารถนำสื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลได้ภายในเวลาตามวรรคหนึ่ง ศาลจะกำหนดให้ทำการตรวจข้อมูลดังกล่าว ณ สถานที่ เวลา และภายในเงื่อนไขตามที่ศาลเห็นสมควรแล้วแต่สภาพแห่งข้อมูลนั้น ๆ ก็ได้

ถ้าคู่ความที่ประสงค์จะอ้างอิงข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์มิได้ปฏิบัติให้ถูกต้องตามความในวรรคหนึ่งหรือวรรคสอง ห้ามมิให้ศาลรับฟังข้อมูลนั้นเป็นพยานหลักฐาน แต่ถ้าศาลเห็นว่าเพื่อประโยชน์แห่งความยุติธรรมจะรับฟังข้อมูลเช่นว่านั้นเป็นพยานหลักฐานประกอบพยานหลักฐานอื่นด้วยก็ได้

ข้อ 35 คู่ความฝ่ายที่ถูกอีกฝ่ายหนึ่งอ้างอิงข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์มาเป็นพยานหลักฐานยันตนอาจยื่นคำแถลงต่อศาลก่อนการสืบข้อมูลนั้นเสร็จ คัดค้านการอ้างข้อมูลนั้น โดยเหตุที่ว่าข้อมูลดังกล่าวไม่เข้าเงื่อนไขของการรับฟังตามข้อ 33 หรือสื่อที่บันทึกข้อมูลนั้นปลอม หรือสำเนาสื่อบันทึกข้อมูลนั้นไม่ถูกต้องทั้งหมดหรือบางส่วน เว้นแต่จะแสดงให้เป็นที่พอใจแก่ศาลว่ามีเหตุอันสมควรที่ไม่อาจทราบเหตุแก่งการคัดค้านได้ก่อนเวลาดังกล่าว คู่ความฝ่ายนั้นอาจยื่นคำร้องขออนุญาตคัดค้านการอ้างข้อมูลหรือสื่อหรือสำเนาสื่อที่บันทึกข้อมูลเช่นว่านั้นต่อศาลไม่ว่าเวลาใด ๆ ก่อนพิพากษาคดี และถ้าศาลเห็นว่าคู่ความฝ่ายนั้นไม่อาจยกข้อคัดค้านได้ก่อนนั้นและคำร้องนั้นมีเหตุผลฟังได้ก็ให้ศาลอนุญาตตามคำร้อง ในกรณีที่มีการคัดค้านดังว่ามานี้ ให้นำมาตรา 126 แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง มาใช้บังคับโดยอนุโลม

ถ้าคู่ความซึ่งประสงค์จะคัดค้านไม่คัดค้านการอ้างข้อมูลดังกล่าวเสียก่อนการสืบข้อมูลนั้นเสร็จ หรือศาลไม่อนุญาตให้คัดค้านภายหลัง ห้ามมิให้คู่ความฝ่ายนั้นคัดค้านการอ้างอิงข้อมูลนั้นเป็นพยานหลักฐาน แต่ทั้งนี้ไม่ตัดอำนาจของศาลในการที่จะไต่สวนและชี้ขาดในเรื่องเงื่อนไขของการรับฟังข้อมูลนั้นตามข้อ 33 หรือในเรื่องความแท้จริงหรือถูกต้องของสื่อหรือสำเนาสื่อที่บันทึกข้อมูลเช่นว่านั้น ในเมื่อศาลเห็นสมควรเพื่อประโยชน์แห่งความยุติธรรม

ข้อ 36 ให้นำข้อกำหนดข้อ 33 ถึงข้อ 35 มาใช้บังคับแก่การรับฟังข้อมูลที่บันทึกไว้ในหรือได้มาจากไมโครฟิล์ม สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศประเภทอื่นโดยอนุโลม”

## ผนวก ฉ

## ข้อกำหนดคดีล้มละลาย พ.ศ. 2540

**“...**

ข้อ 20 ศาลอาจรับฟังข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์ เป็นพยานหลักฐานในคดีได้ หาก

(1)การบันทึกข้อมูลโดยเครื่องคอมพิวเตอร์หรือการประมวลผลโดยเครื่องคอมพิวเตอร์เป็นการกระทำตามปกติในการประกอบธุรกิจของผู้ใช้เครื่องคอมพิวเตอร์ และ

(2)การบันทึกและการประมวลผลข้อมูลเกิดจากการใช้เครื่องคอมพิวเตอร์ปฏิบัติงานตามขั้นตอนการทำงานของเครื่องคอมพิวเตอร์อย่างถูกต้อง และแม้หากมีกรณีการทำงานของเครื่องคอมพิวเตอร์ขัดข้อง ก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

การพิสูจน์ถึงการกระทำตามปกติของผู้ใช้ตาม (1) และความถูกต้องของการบันทึกและการประมวลผลข้อมูลตาม (2) อาจใช้คำรับรองของบุคคลที่เกี่ยวข้องหรือการดำเนินการนั้นก็ได้

ข้อ 21 คู่ความที่ประสงค์จะเสนอข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์จะต้องระบุข้อมูลที่จะอ้างไว้ในบัญชีระบุพยานตามมาตรา 88 แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง พร้อมยื่นคำแถลงแสดงความจำนงเช่นว่านั้น กับสำเนาสื่อที่บันทึกข้อมูลนั้นในจำนวนที่เพียงพอเพื่อให้คู่ความอีกฝ่ายหนึ่งมารับไปจากเจ้าพนักงานศาล เว้นแต่

(1)สื่อที่บันทึกข้อมูลนั้นอยู่ในความครอบครองของคู่ความฝ่ายอื่น หรือของบุคคลภายนอก ให้คู่ความฝ่ายที่อ้างอิงข้อมูลยื่นคำขอโดยทำเป็นคำร้องต่อศาลขออนุญาตงดส่งสำเนาสื่อบันทึกข้อมูลและขอให้ศาลมีคำสั่งเรียกสื่อที่บันทึกข้อมูลนั้นมาจากผู้ครอบครองโดยให้คู่ความฝ่ายที่อ้างนั้นมีหน้าที่ติดตามเพื่อให้ได้สื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลในวันสืบพยานหรือในวันอื่นตามที่ศาลเห็นสมควรกำหนด

(2)ถ้าการทำสำเนาสื่อที่บันทึกข้อมูลนั้น จะทำให้กระบวนพิจารณาล่าช้าหรือเป็นที่เสื่อมเสียแก่คู่ความซึ่งอ้างอิงข้อมูลนั้น หรือมีเหตุผลแสดงว่าไม่อาจส่งสำเนาสื่อที่บันทึกข้อมูลนั้นให้แล้วเสร็จภายในเวลาตามที่กำหนดได้ ให้คู่ความฝ่ายที่อ้างอิงข้อมูลยื่นคำขอโดยทำเป็นคำร้องต่อศาลขออนุญาตงดส่งสำเนาสื่อที่บันทึกข้อมูลและขอนำสื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลในวันสืบพยาน หรือในวันอื่นตามที่ศาลเห็นสมควรกำหนด

ถ้าคู่ความฝ่ายที่อ้างอิงไม่สามารถนำสื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลได้ภายในเวลาตามวรรคหนึ่ง ศาลจะกำหนดให้ทำการตรวจข้อมูลดังกล่าว ณ สถานที่ เวลา และภายในเงื่อนไขตามที่ศาลเห็นสมควร แล้วแต่สภาพแห่งข้อมูลนั้น ๆ ก็ได้

ถ้าคู่ความที่ประสงค์จะอ้างอิงข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์มิได้ปฏิบัติให้ถูกต้องตามความในวรรคหนึ่งหรือวรรคสอง ห้ามมิให้ศาลรับฟังข้อมูลนั้นเป็นพยานหลักฐาน แต่ถ้าศาลเห็นว่าเพื่อประโยชน์แห่งความยุติธรรมจะรับฟังข้อมูลเช่นว่านั้นเป็นพยานหลักฐานประกอบพยานหลักฐานอื่นด้วยก็ได้

ข้อ 22 คู่ความฝ่ายที่ถูกอีกฝ่ายหนึ่งอ้างอิงข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์มาเป็นพยานหลักฐานยันตน อาจยื่นคำแถลงคัดค้านการอ้างข้อมูลนั้นต่อศาลก่อนการสืบข้อมูลนั้นเสร็จ โดยเหตุที่ว่าข้อมูลดังกล่าวไม่เข้าเงื่อนไขของการรับฟังตามข้อ 20 หรือสื่อที่บันทึกข้อมูลนั้นปลอม หรือสำเนาสื่อที่บันทึกข้อมูลนั้นไม่ถูกต้องทั้งหมดหรือบางส่วน เว้นแต่จะแสดงให้เป็นที่พอใจแก่ศาลว่ามีเหตุอันสมควรที่ไม่อาจทราบเหตุแห่งการคัดค้านได้ก่อนเวลาดังกล่าว คู่ความฝ่ายนั้นอาจยื่นคำร้องขออนุญาตคัดค้านการอ้างข้อมูลหรือสื่อหรือสำเนาสื่อที่บันทึกข้อมูลนั้นไม่ถูกต้องทั้งหมดหรือบางส่วน เว้นแต่จะแสดงให้เป็นที่พอใจแก่ศาลว่ามีเหตุอันสมควรที่ไม่อาจทราบเหตุแห่งการคัดค้านได้ก่อนเวลาดังกล่าว คู่ความฝ่ายนั้นอาจยื่นคำร้องขออนุญาตคัดค้านการอ้างข้อมูลหรือสื่อหรือสำเนาสื่อที่บันทึกข้อมูลเช่นว่านั้นต่อศาลไม่ว่าเวลาใด ๆ ก่อนพิพากษาคดี และถ้าศาลเห็นว่าคู่ความฝ่ายนั้นไม่อาจยกข้อคัดค้านได้ก่อนนั้นและคำร้องนั้นมีเหตุผลฟังได้ ก็ให้ศาลอนุญาตตามคำร้อง ในกรณีที่มีการคัดค้านดังว่ามานี้ ให้นำมาตรา 126 แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง มาใช้บังคับโดยอนุโลม

ถ้าคู่ความซึ่งประสงค์จะคัดค้านไม่คัดค้านการอ้างข้อมูลดังกล่าวเสียก่อนการสืบข้อมูลนั้นเสร็จ หรือศาลไม่อนุญาตให้คัดค้านภายหลัง ห้ามมิให้คู่ความฝ่ายนั้นคัดค้านการอ้างอิงข้อมูลนั้นเป็นพยานหลักฐาน แต่ทั้งนี้ไม่ตัดอำนาจของศาลในการที่จะไต่สวนและชี้ขาดในเรื่องเงื่อนไขของการรับฟังข้อมูลนั้น ตามข้อ 20 หรือในเรื่องความแท้จริงหรือถูกต้องของสื่อหรือสำเนาสื่อที่บันทึกข้อมูลเช่นนั้น ในเมื่อศาลเห็นสมควรเพื่อประโยชน์แห่งความยุติธรรม

ข้อ 23 ให้นำความใน 21 ถึงข้อ 22 มาใช้บังคับแก่การรับฟังข้อมูลที่บันทึกไว้ในหรือได้มาจากไมโครฟิล์ม สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศประเภทอื่นโดยอนุโลม”

## ผนวก ช

## ข้อกำหนดคดีภาษีอากร พ.ศ.2544

**“...**

ข้อ 30 ศาลอาจรับฟังข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์เป็นพยานหลักฐานในคดีได้ หาก

(1)การบันทึกข้อมูลโดยเครื่องคอมพิวเตอร์ หรือการประมวลผลโดยเครื่องคอมพิวเตอร์เป็นการกระทำตามปกติในการประกอบกิจการของผู้ใช้เครื่องคอมพิวเตอร์ และ

(2)การบันทึกและการประมวลผลข้อมูลเกิดจากการใช้เครื่องคอมพิวเตอร์ปฏิบัติงานตามขั้นตอนการทำงานของเครื่องคอมพิวเตอร์อย่างถูกต้อง และแม้หากมีกรณีการทำงานของเครื่องคอมพิวเตอร์ขัดข้องก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

การกระทำตามปกติของผู้ใช้ตาม (1) และความถูกต้องของการบันทึกและการประมวลผลข้อมูลตาม (2) ต้องมีคำรับรองของบุคคลที่เกี่ยวข้องหรือดำเนินการนั้น

ข้อ 31 คู่ความที่ประสงค์จะเสนอข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์จะต้องระบุข้อมูลที่จะอ้างไว้ในบัญชีระบุพยานตามข้อ 15 พร้อมยื่นคำแถลงแสดงความจำนงเช่นว่านั้น และคำรับรองตามข้อ 30 วรรคสอง กับสำเนาสื่อที่บันทึกข้อมูลนั้นในจำนวนที่เพียงพอเพื่อให้คู่ความอีกฝ่ายหนึ่งมารับไปจากเจ้าพนักงานศาลเว้นแต่

(1)สื่อที่บันทึกข้อมูลนั้นอยู่ในความครอบครองของคู่ความฝ่ายอื่น หรือของบุคคลภายนอก ให้คู่ความฝ่ายที่อ้างอิงข้อมูลยื่นคำขอโดยทำเป็นคำร้องต่อศาลขออนุญาตงดส่งคำรับรองตามข้อ 30 วรรคสอง และสำเนาสื่อบันทึกข้อมูล และขอให้ศาลมีคำสั่งเรียกสื่อที่บันทึกข้อมูลนั้นมาจากผู้ครอบครองให้คู่ความฝ่ายที่อ้างนั้นมีหน้าที่ติดตามเพื่อให้ได้สื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลในวันสืบพยานหรือในวันอื่นตามที่ศาลเห็นสมควรกำหนด

(2)ถ้าการทำสำเนาสื่อที่บันทึกข้อมูลนั้น จะทำให้กระบวนพิจารณาล่าช้าหรือเป็นที่เสื่อมเสียแก่คู่ความซึ่งอ้างอิงข้อมูลนั้น หรือมีเหตุผลแสดงว่าไม่อาจส่งสำเนาสื่อที่บันทึกข้อมูลนั้นให้แล้วเสร็จภายในเวลาตามที่กำหนดได้ ให้คู่ความฝ่ายที่อ้างอิงข้อมูลยื่นคำขอโดยทำเป็นคำร้องต่อศาลขออนุญาตงดส่งสำเนาสื่อที่บันทึกข้อมูลและขอนำสื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลในวันสืบพยาน หรือในวันอื่นตามที่ศาลเห็นสมควรกำหนด

ถ้าคู่ความฝ่ายที่อ้างอิงไม่สามารถนำสื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลได้ภายในเวลาตามวรรคหนึ่ง ศาลจะกำหนดให้ทำการตรวจข้อมูลดังกล่าว ณ สถานที่ เวลา และภายในเงื่อนไขตามที่ศาลเห็นสมควรแล้วแต่สภาพแห่งข้อมูลนั้น ๆ ก็ได้

ถ้าคู่ความที่ประสงค์จะอ้างอิงข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์มิได้ปฏิบัติให้ถูกต้องตามความในวรรคหนึ่งหรือวรรคสอง ห้ามมิให้ศาลรับฟังข้อมูลนั้นเป็นพยานหลักฐาน แต่ถ้าศาลเห็นว่าเพื่อประโยชน์แห่งความยุติธรรมจะรับฟังข้อมูลเช่นว่านั้นเป็นพยานหลักฐานประกอบพยานหลักฐานอื่นด้วยก็ได้

ข้อ 32 คู่ความฝ่ายที่ถูกอีกฝ่ายหนึ่งอ้างอิงข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์มาเป็นพยานหลักฐานยันตน อาจยื่นคำแถลงต่อศาลก่อนการสืบข้อมูลนั้นเสร็จ คัดค้านการอ้างข้อมูลนั้นโดยเหตุที่ว่าข้อมูลดังกล่าวไม่เข้าเงื่อนไขของการรับฟังตามข้อ 30 หรือสื่อที่บันทึกข้อมูลนั้นปลอม หรือสำเนาสื่อที่บันทึกข้อมูลนั้นไม่ถูกต้องทั้งหมดหรือบางส่วน เว้นแต่จะแสดงให้เป็นที่พอใจแก่ศาลว่ามีเหตุอันสมควรที่ไม่อาจทราบเหตุแห่งการคัดค้านได้ก่อนเวลาดังกล่าว คู่ความฝ่ายนั้นอาจยื่นคำร้องขออนุญาตคัดค้านการอ้างข้อมูลหรือสื่อหรือสำเนาสื่อที่บันทึกข้อมูลเช่นว่านั้นต่อศาลไม่ว่าเวลาใด ๆ ก่อนพิพากษาคดี และถ้าศาลเห็นว่าคู่ความฝ่ายนั้นไม่อาจยกข้อคัดค้านได้ก่อนนั้นและคำร้องนั้นมีเหตุผลฟังได้ก็ให้ศาลอนุญาตตามคำร้อง ในกรณีที่มีการคัดค้านดังว่ามานี้ ให้นำประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 126 มาใช้บังคับโดยอนุโลม

ถ้าคู่ความซึ่งประสงค์จะคัดค้านไม่คัดค้านการอ้างข้อมูลดังกล่าวเสียก่อนการสืบข้อมูลนั้นเสร็จ หรือศาลไม่อนุญาตให้คัดค้านภายหลัง ห้ามมิให้คู่ความฝ่ายนั้นคัดค้านการอ้างอิงข้อมูลนั้นเป็นพยานหลักฐาน แต่ทั้งนี้ไม่ตัดอำนาจของศาลในการที่จะไต่สวนและชี้ขาดในเรื่องเงื่อนไขของการรับฟังข้อมูลนั้นตามข้อ 30 หรือในเรื่องความแท้จริงหรือถูกต้องของสื่อหรือสำเนาสื่อที่บันทึกข้อมูลเช่นว่านั้น ในเมื่อศาลเห็นสมควรเพื่อประโยชน์แห่งความยุติธรรม

ข้อ 33 ให้นำข้อกำหนด ข้อ 30 ถึงข้อ 32 มาใช้บังคับแก่การรับฟังข้อมูลที่บันทึกไว้ในหรือได้มาจากไมโครฟิล์ม สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศประเภทอื่นโดยอนุโลม”

## ผนวก ซ

# ELECTRONIC EVIDENCE MODEL LAW

AN ACT to make provision for the legal recognition of electronic records and to facilitate the admission of such records into evidence in legal proceedings.

BE IT ENACTED by the Parliament *[name of legislature]* of ..... *[name of country]* as follows:

Short Title 1. This Act may be cited as the Electronic Evidence Act, 2002

Interpretation 2. In this Act,

"data" means representations, in any form, of information or concepts;

"electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print out or other output of that data.

"electronic records system" includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and preservation of electronic records.

"legal proceeding" means a civil, criminal or administrative proceeding in a court or before a tribunal, board or commission.

General Admissibility

3. Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record.

4. (1) This Act does not modify any common law or statutory rule relating to the admissibility or records, except the rules relating to authentication and best evidence.

Scope of Act (2) A court may have regard to evidence adduced under this Act in applying any common law or statutory rule relating to the admissibility of records.

Authentication 5. The person seeking to introduce an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

Application of Best Evidence Rule

6. (1) In any legal proceeding, subject to subsection (b), where the best evidence rule is applicable in respect of electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.

(2) In any legal proceeding, where an electronic record in the form of printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purposes of the best evidence rule.

Presumption of Integrity

7. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed in any legal proceeding:

(a) where evidence is adduced that supports a finding that at all material times the computer system or other similar device was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the integrity of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the integrity of the record.

(b) where it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

Standards 8. For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or preserved, having regard to the type of business or endeavour that used, recorded or preserved the electronic record and the nature and purpose of the electronic record.

Proof by Affidavit

9. The matters referred to in sections 6, 7, and 8 may be established by an affidavit given to the best of the deponent's knowledge or belief.

Cross Examination

10. (1) A deponent of an affidavit referred to in section 9 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

(2) Any party to the proceedings may, with leave of the court,cross examine a person referred to in subsection 7(c).

Agreement on Admissibility of Electronic Records

11. (1) Unless otherwise provided in any other statute, an electronic record is admissible, subject to the discretion of the court, if the parties to the proceedings have expressly agreed at any time that its admissibility may not be disputed.

(2) Notwithstanding subsection (1), an agreement between the parties on admissibility of an electronic record does not render the record admissible in a criminal proceeding on behalf of the prosecution if at the time the agreement was made, the accused person or any of the persons accused in the proceeding was not represented by a solicitor.

Admissibility of Electronic Signature

12. (1) Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.

(2) An electronic signature may be proved in any manner, including bys howing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

## ผนวก ฌ

## UNCITRAL Model Law on Electronic Commerce 1996

### Part one. Electronic commerce in general

CHAPTER I. GENERAL PROVISIONS

Article 1. Sphere of application*

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

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

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

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

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

"This Law applies to any kind of information in the form of a data message, except in the following situations: [...]."

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

Article 2. Definitions

For the purposes of this Law:

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

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

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

(d) “Addressee” of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;

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

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

Article 3. Interpretation

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

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

Article 4. Variation by agreement

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

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

CHAPTER II. APPLICATION OF LEGAL REQUIREMENTS TO DATA MESSAGES

Article 5. Legal recognition of data messages

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

Article 5 bis. Incorporation by reference

(as adopted by the Commission at its thirty-first session, in June 1998)

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

Article 6. Writing

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

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

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

Article 7. Signature

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

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

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

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

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

Article 8. Original

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

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

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

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

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

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

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

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

Article 9. Admissibility and evidential weight of data messages

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

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

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

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

Article 10. Retention of data messages

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

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

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

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

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

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

## CHAPTER III. COMMUNICATION OF DATA MESSAGES

### Article 11. Formation and validity of contracts

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

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

### Article 12. Recognition by parties of data messages

(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

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

### Article 13. Attribution of data messages

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

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

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

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

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

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

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

(4) Paragraph (3) does not apply:

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

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

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

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

Article 14. Acknowledgement of receipt

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

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

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

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

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

## Part two. Electronic commerce in specific areas

### CHAPTER I. CARRIAGE OF GOODS

#### Article 16. Actions related to contracts of carriage of goods

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

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

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

(iii) issuing a receipt for goods;

(iv) confirming that goods have been loaded;

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

(ii) giving instructions to a carrier;

(c) (i) claiming delivery of goods;

(ii) authorizing release of goods;

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

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

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

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

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

#### Article 17. Transport documents

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

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

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation

must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

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

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

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

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

# ประวัติผู้เขียน

ชื่อ-สกุล : นางสาว ศศิธร หงษ์ประเสริฐ

วัน เดือน ปี : 13 มิถุนายน พ.ศ. 2527

วุฒิการศึกษา :

ปี 2550 ปริญญาตรี นิติศาสตร์บัณฑิต

ประสบการณ์การทำงาน :

รับราชการ เริ่มปี 2550-ปัจจุบัน สังกัดมณฑลทหารบกที่ 11

ปัจจุบันเป็นนักกีฬายิงปืนทีมชาติไทย