

(ร่าง)

รายงานการศึกษาวิจัย

เรื่อง

กฎหมายพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce Law)

กฤษณะ ช่างกล่อม

สวทช.
NSTDA



จัดทำโดย :

โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ
สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม

ศวทช.

ศอ.1

148

2542

ฉ.1

(ร่าง)

รายงานการศึกษาวิจัย

เรื่อง

กฎหมายพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce Law)

กฤษณะ ช่างกล่อม

สวทช.
NSTDA



(ร่าง)

กฎหมายพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce Law)

กฤษฎีกา ช่างกล่อม

ISBN 974-7578-61-1

พิมพ์ครั้งที่ 1

จำนวน 1,500 เล่ม

เมษายน 2542

สงวนลิขสิทธิ์ ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2521/2537

โดย สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

ไม่อนุญาตให้คัดลอกส่วนใดส่วนหนึ่งของเล่มนี้ นอกจากจะได้รับอนุญาต

เป็นลายลักษณ์อักษรจากเจ้าของลิขสิทธิ์เท่านั้น

Copyright © 1998 by

National Information Technology Committee Secretariat

National Electronics and Computer Technology Center

National Science, Technology and Environment,

73/1 NSTDA Building, Rama VI Road, Ratchathewi

Bangkok 10400 Thailand

Tel : (662) 644-8150..9 Fax : (662) 644-6653

จัดทำโดย

โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม

73/1 ชั้น 6 อาคาร สวทช. ถนนพระรามที่ 6 เขตราชเทวี กรุงเทพฯ 10400

โทรศัพท์ 644-8150..9 โทรสาร : 644-6653

E-mail : nitc-sec@nwg.nectec.or.th

Web Site : <http://www.nitc.go.th>

2542
118.1
148
1542
2.1

คำนำ

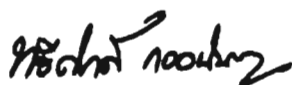
ตามที่คณะรัฐมนตรีได้มีมติตามหนังสือที่ นร 0205/16727 ลงวันที่ 15 ธันวาคม พ.ศ. 2541 ให้ความเห็นชอบต่อโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศที่จัดขึ้นโดยคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ อันประกอบด้วยการศึกษาและยกร่างกฎหมายทั้ง 6 ฉบับอันได้แก่

1. กฎหมายการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์
2. กฎหมายการโอนเงินอิเล็กทรอนิกส์
3. กฎหมายลายมือชื่ออิเล็กทรอนิกส์
4. กฎหมายอาชญากรรมทางคอมพิวเตอร์
5. กฎหมายคุ้มครองข้อมูลส่วนบุคคล และ
6. กฎหมายลำดับรองของรัฐธรรมนูญมาตรา 78

โดยให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติเป็นศูนย์กลางในการดำเนินการและประสานงานระหว่างหน่วยงานต่างๆ ที่กำลังดำเนินการจัดทำกฎหมายเทคโนโลยีสารสนเทศและกฎหมายอื่นๆ ที่เกี่ยวข้อง

รายงานการศึกษาวิจัยเรื่อง กฎหมายพาณิชย์อิเล็กทรอนิกส์ หรือกฎหมายแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ ฉบับนี้ จึงถือเป็นส่วนหนึ่งของโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ ดังที่ได้กล่าวมาข้างต้น โดยมีวัตถุประสงค์เพื่อเป็นการสร้าง "องค์ความรู้" เพื่อให้สามารถพัฒนาความรู้ทั้งทางกฎหมาย และทางเทคนิคในด้านนี้ต่อไป รวมทั้งจะทำให้กระบวนการในการยกร่างกฎหมายพาณิชย์อิเล็กทรอนิกส์สามารถทำได้อย่างมีประสิทธิภาพ

เนื่องจากเป็นความจำเป็นเร่งด่วนและสามารถใช้ประโยชน์จากงานดังกล่าวนี้ ทางผู้จัดทำจึงเห็นควรให้พิมพ์รายงานการวิจัยฉบับนี้เป็นฉบับ "ร่าง" ไปก่อนโดยจะได้ตีพิมพ์เป็นฉบับสมบูรณ์ต่อไป



(ดร. วิศักดิ์ กอนันตกุล)

ผู้อำนวยการ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

บทนำ

ร่างรายงานการวิจัยฉบับนี้ทำขึ้นภายใต้ข้อจำกัดของเวลาที่เร่งด่วนเพื่อที่จะสามารถนำมาเป็นพื้นฐานเบื้องต้นในการทำความเข้าใจกฎหมายพาณิชย์อิเล็กทรอนิกส์ต่อไป ผู้จัดทำตระหนักเป็นอย่างดีว่ารายงานฉบับนี้คงจะไม่มีคุณสมบัติมากนักรวมทั้งอาจมีข้อบกพร่องมากมาย แต่อย่างไรก็ดีผู้จัดทำก็น้อมรับความผิดพลาดทั้งปวงอย่างดุษฎี

ร่างรายงานการวิจัยฉบับนี้จะแบ่งออกเป็นเจ็ดบท โดยในบทแรกจะกล่าวถึงประวัติความเป็นมาของกฎหมายไทยและระบบกฎหมาย ในบทที่สองจะกล่าวถึงความสัมพันธ์ระหว่างเทคโนโลยีและกฎหมาย บทที่สามจะอธิบายถึงเทคโนโลยีพาณิชย์อิเล็กทรอนิกส์ บทที่สี่จะกล่าวถึงสัญญาทางอิเล็กทรอนิกส์ ในบทที่ห้าจะอธิบายถึงความรับผิดชอบและการกระจายความรับผิดชอบ (Attribution Issues) ส่วนในบทที่ 6 จะได้กล่าวถึงพยานหลักฐานทางอิเล็กทรอนิกส์ บทที่ 7 จะเป็นตัวอย่างโครงการจัดทำใบตราส่งให้เป็นอิเล็กทรอนิกส์ และบทสุดท้ายจะเป็นบทสรุป

ผู้จัดทำหวังเป็นอย่างยิ่งว่ารายงานการวิจัยฉบับนี้จะต้องมีการปรับปรุงให้มีความสมบูรณ์ยิ่งขึ้นอย่างแน่นอน

สารบัญ

หน้า

คำนำ

บทนำ

บทที่ 1 บทนำทางประวัติศาสตร์	6
1. ประวัติศาสตร์กฎหมายไทย	6
2. ระบบกฎหมาย	8
2.1 ระบบ Common Law	
2.2 ระบบ Civil Law	
3. ตัวอย่างของระบบกฎหมายที่มีการแยกกฎหมายแพ่ง ออกจากกฎหมายพาณิชย์	9
3.1 กฎหมายของประเทศฝรั่งเศส	
3.2 กฎหมายของประเทศเยอรมัน	
4. สรุป	12
บทที่ 2 เทคโนโลยีพาณิชย์อิเล็กทรอนิกส์	14
1. เทคโนโลยีพาณิชย์อิเล็กทรอนิกส์	14
1.1 เทเล็กซ์	
1.2 โทรสาร	
1.3 ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail)	
1.4 การแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ (Electronic Data Interchange)	
2. เทคโนโลยีพาณิชย์อิเล็กทรอนิกส์ : องค์ประกอบของระบบ	19

2.1 องค์ประกอบเบื้องต้นของระบบ EDI	19
2.1.1 คอมพิวเตอร์ฮาร์ดแวร์และซอฟต์แวร์	
2.1.2 บาร์โค้ด	
2.1.3 โปรแกรมคอมพิวเตอร์	
2.1.4 มาตรฐาน EDI	
2.1.5 เครือข่ายโทรคมนาคม	
2.2 ระบบการจัดเก็บข้อมูล	22
2.3 โปรโตคอลการสื่อสาร EDI	25
บทที่ 3 ความสัมพันธ์ระหว่างกฎหมายและเทคโนโลยีสารสนเทศ	42
1. ความสัมพันธ์ระหว่างกฎหมายและสังคม	42
2. สังคมสารสนเทศ	44
3. ผลของความก้าวหน้าทางเทคโนโลยีพาณิชย์อิเล็กทรอนิกส์	48
ต่อการเปลี่ยนแปลงของกฎหมาย	
3.1 รูปแบบของการมีส่วนร่วมของมนุษย์	
3.2 สื่อที่ใช้ในการแสดงเจตนา	
3.3 การเกิดของทรัพย์สินชนิดใหม่	
3.4 สถานที่และเวลาที่เปลี่ยนไป	
3.5 ความเสี่ยงที่เกิดขึ้นใหม่	
บทที่ 4 ธุรกรรมอิเล็กทรอนิกส์ (Electronic Transaction)	59
1. ความทั่วไป	59
2. การเจรจาสัญญา	65
3. เจตนา	65
4. คำเสนอ	67
5. คำสนอง	69
6. การรับคำเสนอและคำสนอง	73

7. การถอนคำเสนอ	74
8. การเกิดของสัญญา (Formation Of Contract)	76
9. แบบของสัญญา	80
10. การตีความสัญญา	87
11. กฎหมายที่จะใช้บังคับ (Choice of Law)	88
บทที่ 5 ความรับผิดและการกระจายความรับผิด (Attribution Issues)	90
1. ความรับผิด	90
1.1 ความรับผิดของผู้ให้บริการการสื่อสาร	
1.2 ความรับผิดของผู้ส่งข้อมูล	
1.3 ความรับผิดของผู้รับข้อมูล	
1.4 ความปลอดภัย (Securities) และไวรัสคอมพิวเตอร์	
2. การกระจายความรับผิด (Attribution Issues)	92
บทที่ 6 พยานหลักฐานอิเล็กทรอนิกส์	94
1. ความทั่วไป	94
2. ตัวอย่างของกฎหมายพยานหลักฐานของต่างประเทศ	97
2.1 กลุ่มประเทศ Common Law	
2.1.1 สหรัฐฯ	
2.1.2 สหราชอาณาจักร	
2.1.3 ออสเตรเลีย	
2.2 กลุ่มประเทศ Civil Law	
2.2.1 เยอรมัน	
2.2.2 ฝรั่งเศสและเบลเยียม	
2.2.3 ลักเซมเบิร์ก	
2.3 พยานอิเล็กทรอนิกส์ตามกฎหมายไทย	
3. แนวทางในการพิจารณาพยานอิเล็กทรอนิกส์	118

- 3.1 การตรวจสอบความถูกต้องแท้จริง (Authenticity)
- 3.2 การให้น้ำหนักพยาน

บทที่ 7 ตัวอย่างโครงการจัดทำใบตราส่งให้เป็นอิเล็กทรอนิกส์	138
บทสรุป	143
บรรณานุกรม	
ภาคผนวก ตารางการเปรียบเทียบกฎหมายพาณิชย์อิเล็กทรอนิกส์ ของประเทศไทย	

บทที่ 1

บทนำทางประวัติศาสตร์กฎหมายไทย

และระบบกฎหมาย

1. บทนำทางประวัติศาสตร์กฎหมายไทย¹

หากพิจารณาถึงประวัติศาสตร์ของการนิติบัญญัติไทยแบบสมัยใหม่นั้นเริ่มตั้งแต่สมัยรัชการที่ 4-5 เป็นต้นมา โดยการเปลี่ยนแปลงในสมัยนี้ อาจกล่าวได้ว่าการตัดสินใจที่สำคัญ 3 ครั้งคือ²

1.1 ครั้งแรก มีการรับเอากฎหมายอังกฤษเข้ามาใช้ (เพื่อเพิ่มเติมกฎหมายเดิมให้มีความสมบูรณ์ขึ้น) ซึ่งเข้ามา 2 ทาง คือ

- (ก) เป็นการรับเข้ามาเป็นเรื่องๆ หรือที่เรียกว่า piece meal โดยศาลจะนำหลักกฎหมายของอังกฤษเข้ามาเป็นส่วนประกอบกฎหมายไทยที่บกพร่องให้สมบูรณ์ขึ้น
- (ข) เป็นการรับเข้ามาโดยทางโรงเรียนสอนกฎหมาย กล่าวคือ ไทยได้ส่งนักกฎหมายไปศึกษาต่อที่ประเทศอังกฤษ

สำหรับสาเหตุที่ไทยต้องรับเอากฎหมายอังกฤษเข้ามาใช้ก็เพราะว่า ไทยได้มีการติดต่อกับต่างชาติมากขึ้น กฎหมายเดิมที่มีอยู่ไม่เพียงพอ แต่เนื่องจากมีความจำเป็นที่จะต้องใช้อย่างรีบด่วน การนำกฎหมายอังกฤษเข้ามาใช้นับเป็นวิธีทางที่สะดวกที่สุดในระยะเวลานั้น

¹ โปรดดู ร. แลงการ์ด, ประวัติศาสตร์กฎหมายไทย (กฎหมายเอกชน: ข้อความเบื้องต้น, ละเมิด, สัญญา, กฎหมายที่ดิน), มหาวิทยาลัยธรรมศาสตร์และการเมือง, 2478-2483 (พิมพ์ซ้ำโดยมูลนิธิโครงการตำรา 2526)

² โปรดดู ศาสตราจารย์ ดร. ปรีดี เกษมทรัพย์, นิติปรัชญา, พิมพ์ครั้งที่ 4, โครงการตำราและเอกสารประกอบการสอนคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2541, หน้า 49-51

1.2 ครั้งที่สอง มีการตัดสินใจที่จะทำประมวลกฎหมายและจะทำแบบประมวลกฎหมายของฝรั่งเศส

สาเหตุที่มีการตัดสินใจครั้งที่สองนี้ สืบเนื่องมาจากปัญหาเรื่องสิทธิสภาพนอกอาณาเขต กล่าวคือ เมื่อไทยติดต่อกับชาติใด ก็อนุญาตให้ชาตินั้นใช้ขนบธรรมเนียมของเขาในการตัดสินข้อพิพาทได้ เช่นเมื่อไทยติดต่อกับฝรั่งเศส และฝรั่งเศสใช้ขนบธรรมเนียมของเขาในการตัดสินข้อพิพาท ไทยจึงอนุญาตเพราะในเวลานั้น ไทยถือหลักบุคคล มิได้ถือหลักดินแดน จึงมีความคิดว่าคนชาติใดก็ควรใช้ขนบธรรมเนียมของคนชาตินั้น

เรื่องสิทธิสภาพนอกอาณาเขตนี้ก่อให้เกิดปัญหากับไทยเป็นอย่างมาก เพราะว่าบุคคลในบังคับของชาติตะวันตกต่างก็อ้างสิทธิสภาพนอกอาณาเขต ทำให้ประชาชนชาวไทยได้รับความเดือดร้อนไม่เป็นธรรม เพราะศาลไทยไม่สามารถตัดสินคดีได้อย่างเต็มที่ ไทยจึงขอยกเลิกสิทธิสภาพนอกอาณาเขต ซึ่งฝรั่งเศสก็ยินยอมโดยมีเงื่อนไขว่าไทยต้องเปลี่ยนแปลงระบบกฎหมายให้เหมือนอารยประเทศ

ในที่สุด ในปลายสมัยรัชกาลที่ 5 เราตัดสินใจว่า ต้องทำประมวลกฎหมายแทนที่จะรับกฎหมายอังกฤษทั้งหมด เพราะกฎหมายอังกฤษนั้นเป็นกฎหมายของระบบ Common Law ซึ่งมีแต่คำพิพากษาฎีกาเป็นส่วนใหญ่ ไม่สะดวกในการที่จะรับเข้ามาและเราก็ไม่มีงบประมาณเพียงพอด้วย การตัดสินใจที่จะทำประมวลกฎหมายจึงเกิดขึ้น โดยในขณะนั้นคิดว่าการเลียนแบบชาติอื่นจะสะดวกที่สุด จึงตัดสินใจที่จะเลียนแบบฝรั่งเศส ซึ่งในครั้งนั้นได้มีการทดลองร่างประมวลกฎหมายแพ่งและพาณิชย์ บรรพ 1-2 ออกมาเมื่อ พ.ศ. 2466 และได้มีการประกาศใช้เพื่อให้ผู้พิพากษาพิจารณา

1.3 ครั้งที่สาม มีการตัดสินใจที่จะทำประมวลกฎหมายโดยเลียนแบบเยอรมันแทนการทำประมวลกฎหมายโดยเลียนแบบฝรั่งเศส

สาเหตุที่มีการตัดสินใจครั้งที่สาม เนื่องมาจากมีปัญหาในการทำประมวลกฎหมายเลียนแบบฝรั่งเศส เพราะชาวผู้ร่างที่มีความรู้ความเชี่ยวชาญทางด้านนี้ แม้แต่นักกฎหมายฝรั่งเศสที่เชิญเข้ามาก็เช่นกัน ทำให้พระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัวทรงเกรงว่าการร่างประมวลกฎหมายจะสำเร็จนั้นเข้าไป จึง

ทรงมีพระกระแสรับสั่งให้พระยามานวราชเสวีซึ่งเป็นเลขานุการคณะกรรมการร่างประมวลกฎหมายในสมัยนั้นรับกระทำโดยเร็ว พระยามานวราชเสวีได้ถวายความคิดเห็นว่า ควรออกแบบของประมวลกฎหมายเยอรมันซึ่งญี่ปุ่นนำมาดัดแปลงไว้แล้ว โดยเราลอกต่อจากญี่ปุ่นอีกทอดหนึ่งจึงจะกระทำได้รวดเร็ว พระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัวจึงโปรดเกล้าฯ ให้ดำเนินการตามนั้น

ในที่สุด การร่างประมวลกฎหมายเลียนแบบเยอรมันได้สำเร็จลุล่วงไปด้วยดีภายในระยะเวลาอันรวดเร็ว และมีการประกาศใช้ประมวลกฎหมายแพ่งและพาณิชย์ในต้นรัชกาลที่ 7 ในราว พ.ศ. 2468 และได้มีการประกาศใช้ครบ 6 บรรพ ราวปี พ.ศ. 2475

2. ระบบกฎหมาย

เป็นที่ยอมรับในวงการนิติศาสตร์โดยทั่วไปว่าการแยกระบบกฎหมายโดยมองในแง่ของนิติวิธี ในปัจจุบันอาจแยกได้เป็นสองระบบคือระบบ Common Law และระบบ Civil Law³

2.1 ระบบ Common Law

เป็นระบบที่เกิดขึ้นในประเทศอังกฤษ หลักกฎหมายที่มีอยู่จะไม่ใช่เป็นลายลักษณ์อักษร กฎหมายเกิดจากคำพิพากษาของศาล ส่วนกฎหมายลายลักษณ์อักษรที่ตราออกมานั้นถือเป็นกฎหมายเฉพาะเรื่องเฉพาะราว ดังนั้นกฎหมายลายลักษณ์อักษรจึงเป็นกฎหมายที่ออกมาเพื่อแก้ไขเพิ่มเติม หรือเปลี่ยนแปลงยกเลิกกฎหมายที่มีอยู่แล้วเท่านั้น⁴

2.2 ระบบ Civil Law

³ โปรดดู Albert A. Ehrenzweig Book review Communist and their law by John H. Hargard 58 Cal L. Re, June 1970, p. 1010

⁴ โปรดดู Sir William Buckland and Loid MacNair, Roman Law and Common Law,

มีประวัติความเป็นมาจากกฎหมายโรมันซึ่งเป็นระบบกฎหมายใหญ่ที่มีประวัติความเป็นมายาวนานเกินกว่าสองพันปี และเจริญรุ่งเรืองก่อนสมัยคริสตศักราชที่ 5-6 โดยจักรพรรดิจัดตั้งเนยนาได้มีบัญชาในปี AD 528 ให้รวบรวมประมวลกฎหมายใหม่ และได้จัดทำประมวลกฎหมายดังกล่าวมาตั้งแต่ AD 529 ถึง AD 555 และเรียกประมวลกฎหมายฉบับนี้ว่า "Corpus Iuris Civilis (the Corpus)" ซึ่งประกอบไปด้วย the Digest, the Institutes, the Code and the Novels มีผู้กล่าวว่านอกจากคัมภีร์ไบเบิลแล้วประมวลกฎหมายดังกล่าวมีความสำคัญอย่างมากต่อชีวิตของชาวยุโรปเป็นอย่างมาก⁵

พัฒนาการของกฎหมายโรมันโดยชาวโรมันกินเวลาถึงราว 1000 ปี จากราว 450 ก่อนคริสตศักราช ถึง AD 550 ต่อมาได้รับการพัฒนาในสมัยกลางโดยนำมาผสมผสานกับกฎหมายของศาสนจักร (Cannon Law) และกฎหมายจารีตประเพณี กลายเป็นกฎหมายที่เรียกว่า Ius Commune ในภาคพื้นยุโรป และยังคงมีอยู่ในกลุ่มประเทศคอมมอนลอว์ และเป็น Gemeines Recht ในประเทศเยอรมัน จนกระทั่งได้มีการบัญญัติกฎหมายขึ้นในศตวรรษที่ 19⁶

ลักษณะสำคัญประการหนึ่งของกฎหมายโรมันคือแยกกฎหมายพาณิชย์ (Commercial Code) ออกจากกฎหมายแพ่ง (Civil Code)⁷ เนื่องจากกฎหมายพาณิชย์นั้นมีความเกี่ยวข้องกับการค้าระหว่างประเทศและพ่อค้า ซึ่งมีทางปฏิบัติและจารีตประเพณีของตนเป็นการเฉพาะ เช่นเดียวกันกับที่กฎหมายของทั้งฝรั่งเศสและเยอรมันก็ได้แยกกฎหมายพาณิชย์ออกจากกฎหมายแพ่งเช่นเดียวกัน

3. ตัวอย่างของระบบกฎหมายที่มีการแยกกฎหมายแพ่งออกจากกฎหมายพาณิชย์

3.1 กฎหมายของประเทศฝรั่งเศส

⁵ โปรดดู Vinogradoff, Roman Law, re-printed 1968, Cambridge; Buckland, A Textbook of Roman Law, Cambridge University Press, 1966; Watson, The Evolution of Law, Blackwell, 1985; Simpson Innovations in Nineteenth Century Contract Law in Legal Theory and Legal History, Hambledon Press, 1987

⁶ Robinson et al, An Introduction to European Legal History, Professional Books Ltd., 1985, Chapter VII

⁷ Fritz Schulz, Roman Legal Science,

จากแนวความคิดของสำนัก Natural Law School⁸ ผสมกับความคิด Enlightenment ที่ต้องการเปลี่ยนแปลงสังคม ทำให้ประเทศฝรั่งเศสมีการปฏิวัติใหญ่ในปี 1789 และหลังจากนั้น นโปเลียน จึงได้จัดตั้งคณะกรรมการเพื่อจัดทำประมวลกฎหมายขึ้น จนในที่สุดประมวลกฎหมายแพ่งของฝรั่งเศส สามารถประกาศใช้ในปี ค.ศ. 1804 โดยยึดหลักการของการปฏิวัติฝรั่งเศส คือ ยึดหลักเสรีภาพ เสมอภาค และภราดรภาพ ความศักดิ์สิทธิ์แห่งการแสดงเจตนาในการทำสัญญา และความศักดิ์สิทธิ์ของทรัพย์สินเอกชน นอกจากนี้ Code Civil ฝรั่งเศสยังมีประมวลกฎหมายอื่นๆ เช่น Code de Commerce และ Code Penale เป็นต้น

อย่างไรก็ดี กฎหมายฝรั่งเศสได้มีการแยกประเภทของกฎหมายดังนี้ 1. กฎหมายระหว่างกฎหมายมหาชนและกฎหมายเอกชน และ 2. กฎหมายแพ่ง (Civil Law) และกฎหมายพาณิชย์ (Civil Law and Commercial Law-France)

ตามกฎหมายของฝรั่งเศส Code de Commerce คือกฎหมายที่เกี่ยวข้องกับสิทธิในทางทรัพย์สินอุตสาหกรรม (Industrial Property Right) หุ้่นส่วนบริษัท ตราสารเปลี่ยนมือและล้มละลาย เช่นในกรณีที่เป็นการซื้อขายระหว่างพ่อค้า Une Acte de Commerce กำหนดไว้ในมาตรา 632 ว่าให้ศาลใช้ทางปฏิบัติและจารีตประเพณีทางการค้ากับกรณีดังกล่าว

คดีที่เกี่ยวกับทางการพาณิชย์จะต้องขึ้นศาลที่เรียกว่า Tribunal de Commerce ซึ่งมีอยู่ราว 230 แห่งในประเทศฝรั่งเศส มีผู้พิพากษาที่เรียกว่า Juges Consulaires ซึ่งไม่ใช่ผู้พิพากษาอาชีพแต่มีประสบการณ์ทางธุรกิจ เป็นบุคคลที่ได้รับเลือกจากกลุ่มธุรกิจและสมาชิกสภาหอการค้า

วิธีพิจารณาคดีพาณิชย์ใน Tribunal de Commerce ต่างกับวิธีพิจารณาในคดีแพ่งของ Tribunal de grande instance คือจะมีความยืดหยุ่นมากกว่ายอมรับการพิสูจน์หลักฐานโดยปากเปล่า (Oral Proof)

3.2 กฎหมายของประเทศเยอรมัน

⁸ โปรดดู Finnis, J., Natural Law and Natural Rights, Oxford : Clarendon Press, 1980

การจัดทำประมวลกฎหมายแพ่งฝรั่งเศส ได้มีอิทธิพลเข้าไปในประเทศเยอรมันในต้นทศวรรษที่ 19 จนมีการโต้เถียงทางวิชาการว่าเยอรมันควรที่จะดำเนินรอยตามฝรั่งเศสในการจัดทำประมวลกฎหมายขึ้นหรือไม่ โดยนักปราชญ์กฎหมายเยอรมันในสมัยนั้นผู้มีชื่อว่า Prof. Von Savigny (ค.ศ. 1779-1861) แห่งมหาวิทยาลัยเบอร์ลิน ได้กล่าวไว้ในบทความที่มีชื่อว่า **“ภารกิจทางนิติบัญญัติและทางนิติศาสตร์ในปัจจุบัน”** มีใจความว่ากฎหมายไม่ใช่สิ่งที่มนุษย์จะสร้างขึ้นตามใจชอบ แต่เป็นสิ่งที่เกิดขึ้นในประวัติศาสตร์จากสิ่งที่เรียกว่า Volksgeist ซึ่งหมายถึงความคิดและจิตใจประชาชาติและจะเจริญงอกงามวิวัฒนาการไปตามวิถีในตัวของมันเองเหมือนต้นไม้หรือภาษาประจำชาติ ซึ่งจะค่อยๆ เปลี่ยนแปลงวิวัฒนาการไปเพราะเป็นผลผลิตของชาติ กฎหมายของชนชาติโดยอมเป็นไปตามความคิดของชนชาตินั้น เขาอธิบายว่าชนชาติแต่ละชนชาติมีประวัติศาสตร์ที่แตกต่างกัน ความรู้สึกนึกคิดหรือจิตใจย่อมจะแตกต่างกัน กฎหมายย่อมจะต้องมีความสอดคล้องกับเรื่องดังกล่าว

ดังนั้นกฎหมายเยอรมันนอกจากจะมีอิทธิพลจากกฎหมายโรมันแล้วยังมีองค์ประกอบอีกสองประการที่มีผลต่อการพัฒนาการของกฎหมายเยอรมันคือ

1. กฎหมายธรรมชาติ แนวความคิดที่ถือว่ากฎหมายมาจากเหตุผลที่เริ่มจากหลักกฎหมายทั่วไปและได้จากกฎเกณฑ์ต่างๆ ในรายละเอียดเฉพาะเรื่อง Grotius ถือเป็นผู้บุคคลที่ยึดถือแนวความคิดนี้คนหนึ่ง เนื่องจากแนวความคิดนี้ถือเหตุผลเป็นหลักจึงอาจส่งผลให้กฎหมายมีลักษณะเป็นนามธรรมมากเกินไปและไม่สอดคล้องกับความเป็นจริงของสังคม
2. สำนักกฎหมายประวัติศาสตร์ ภายใต้การนำของ Savigny เห็นว่าการใช้กฎหมายที่ถือแบบตัวบทเป็นหลักจะส่งผลให้กฎหมายมีลักษณะไม่ยืดหยุ่นและแข็งทื่อ กฎหมายควรที่จะมีความสอดคล้องกับชีวิตของสังคม กฎหมายควรที่จะได้มาจากจารีตประเพณีและประวัติศาสตร์ของสังคมนั้นๆ ด้วย

ในประเทศเยอรมันกฎหมายแพ่งมีชื่อเรียกว่า BGB และกฎหมายพาณิชย์มีชื่อเรียกว่า Handelsgesetzbuch (HGB)

กฎหมายพาณิชย์ของเยอรมันจะมีความยืดหยุ่นมากกว่ากฎหมายแพ่ง เช่นศาลจะยอมรับทางปฏิบัติและจารีตประเพณีในทางการค้า และรูปแบบของสัญญาบางอย่างไม่จำเป็นต้องมี เป็นต้น

จริงอยู่ในประเทศเยอรมันคดีทั้งทางแพ่งและทางพาณิชย์ต้องขึ้นศาล Landgericht เช่นเดียวกัน แต่วิธีพิจารณาความในคดีพาณิชย์จะมีความแตกต่างกันออกไปเช่น องค์คณะผู้พิพากษาจะประกอบไปด้วยผู้พิพากษาอาชีพ 1 คน และผู้มีประสบการณ์ทางธุรกิจอีก 2 คน คล้ายกับ Juges Consulaires ของฝรั่งเศส

4. สรุป

1. เนื่องจากระบบกฎหมายไทยเป็นระบบที่อยู่ในกลุ่มของระบบ Civil Law แต่ประเทศไทยก็ได้มีการแบ่งแยกระหว่างกฎหมายแพ่งและกฎหมายพาณิชย์ออกจากกันเหมือนประเทศต้นแบบอย่างเยอรมันหรือฝรั่งเศส ซึ่งการแยกดังกล่าวนี้จะก่อให้เกิดความยืดหยุ่นโดยเฉพาะการปรับใช้กฎหมายที่เกี่ยวข้องกับเรื่องทางการค้า กฎหมายพาณิชย์อิเล็กทรอนิกส์ก็เช่นกัน นอกจากนี้จะเป็นเรื่องเฉพาะทางที่จำเป็นต้องใช้ผู้ใช้และตีความกฎหมายที่จะต้องมีความเชี่ยวชาญในเรื่องทางเทคโนโลยีแล้ว ระบบการให้ความยุติธรรมก็จำเป็นที่จะต้องมีความเชี่ยวชาญและสอดคล้องกับลักษณะพื้นฐานของพาณิชย์อิเล็กทรอนิกส์เช่นกัน
2. จากที่ได้กล่าวมาข้างต้นจะเห็นได้ว่ากฎหมายนั้นเปรียบเสมือนสายน้ำมีต้นกำเนิด มีแหล่งที่มา กฎหมายมิใช่เป็นเพียงตัวหนังสือที่จะลอกเลียนมาใช้โดยไม่คำนึงถึงสภาพของสังคมหรือความจำเป็นของสังคม หรือจะละเลยแม้แต่ความเข้าใจในหลักกฎหมายที่มีอยู่เบื้องหลังกฎหมายดังกล่าว กฎหมายพาณิชย์อิเล็กทรอนิกส์ก็เช่นเดียวกันเป็นกฎหมายที่มีทั้งส่วนประกอบในแง่ของความรู้ทางเทคนิคและทางกฎหมาย กล่าวคือแม้ว่ามีความจำเป็นที่จะต้องมีความรู้ทางเทคโนโลยีอย่างถ่องแท้เพื่อจะสามารถบัญญัติและใช้กฎหมายให้สามารถบรรลุ

วัตถุประสงค์ของกฎหมายนั้นก็คือความยุติธรรม กฎหมายพาณิชย์อิเล็กทรอนิกส์ก็ยังมีรากฐานทางความคิดทางด้านนิติศาสตร์ที่นักวิชาการและสังคมไทยยังจะต้องขบคิดและปรับให้มีความเหมาะสมกับระบบกฎหมายของไทย กฎหมายพาณิชย์มิใช่เป็นตัวแทนสื่อหรืออารมณ์อันรุกรานที่เราหรือสังคมไทยอยากมีอยากได้ก็เพียงแต่ไปลอกเลียนแบบมาโดยมิได้มีการไตร่ตรองพินิจถึงปัญหาทางวิชาการและเทคนิครวมทั้งความสอดคล้องกับสภาพการณ์ ซึ่งเป็นรากฐานที่จะก่อให้เกิดความยุติธรรมเมื่อนำกฎหมายนั้นมาใช้ในที่สุด

บทที่ 2

เทคโนโลยีพาณิชย์อิเล็กทรอนิกส์

เนื่องจากมนุษย์นั้นถือเป็นสัตว์สังคม จึงมีความจำเป็นที่จะต้องติดต่อสื่อสารแลกเปลี่ยนความรู้และความนึกคิดกันอยู่เสมอ ดังนั้นเทคโนโลยีทางการสื่อสารจึงได้รับการพัฒนาอย่างต่อเนื่อง อันส่งผลให้มนุษย์สามารถพัฒนารูปแบบการค้าที่มีความหลากหลายปราศจากข้อจำกัดของเวลาและสถานที่ที่จะทำการค้าได้ เทคโนโลยีที่เกี่ยวกับการค้าโดยการติดต่อสื่อสารทางอิเล็กทรอนิกส์เราจึงเรียกว่า "เทคโนโลยีพาณิชย์อิเล็กทรอนิกส์"

1. เทคโนโลยีของพาณิชย์อิเล็กทรอนิกส์⁹

ตัวอย่างของเทคโนโลยีพาณิชย์อิเล็กทรอนิกส์

1.1 เทเลกซ์

ในปี ค.ศ. 1844 Samuel Morse ได้ค้นพบเทคโนโลยีโทรเลขเป็นคนแรก จึงถือได้ว่าเป็นการเปิดยุคแห่งการพาณิชย์อิเล็กทรอนิกส์ โดยเทเลกซ์ถือเป็นบริการโทรเลขแบบหนึ่งที่ใช้กันอย่างกว้างขวางในวงการธุรกิจในราวกลางศตวรรษนี้ เครื่องเทเลกซ์จะมีระบบที่เรียกว่า "answerback" ซึ่งเป็นรหัสอักษรเลข (Alphanumeric code) ที่เครื่องเทอร์มินอล ซึ่งจะส่งไปโดยอัตโนมัติหรือตามที่ร้องขอไปยังเครื่องเทอร์มินอลอื่น โดยปกติแล้วการตอบกลับ (Answerback) ของเครื่องเทอร์มินอลจะสามารถสังเกตเห็นได้อย่างชัดเจน สัญญาณการตอบกลับ (Answerback signal) ที่พิมพ์บนใบเทเลกซ์จะเป็นทั้งหลักฐานว่าเครื่องได้ส่งเอกสารนั้นแล้วและเอกสารนั้นได้รับแล้ว แต่อย่างไรก็ดี อาจเป็นไปได้ที่สัญญาณ Answerback ดังกล่าวอาจถูกปลอมแปลงได้

⁹ โปรดดู Benjamin Wright and Jane K. Winn, The Law of Electronic Commerce, Aspen Law & Business, New York, 1997, pp. 2-1 – 2-9

ข้อมูลที่ส่งโดยเทเล็กซ์จะมีเลขสำหรับการตรวจสอบ (Audit number) ที่ผู้ให้บริการ (Carrier) ใส่งไปโดยอัตโนมัติ ซึ่งจะช่วยให้การตรวจสอบว่าเทเล็กซ์ที่พิมพ์ออกมาเหมือนกับตัวต้นฉบับจริงหรือไม่ หรือมีความถูกต้องแท้จริง (Authenticity) หรือไม่

โดยทั่วไปแล้ว เทเล็กซ์เป็นการติดต่อสื่อสารแบบ “Real-time” ซึ่งหมายความว่า การรับและการส่งโดยเครื่องเทอร์มินอลสามารถทำได้โดยตรงและทันที (เหมือนกับกรณีของโทรศัพท์) เมื่อไม่นานมานี้ มีการคิดค้นให้เทเล็กซ์สามารถทำงานได้เหมือนไปรษณีย์อิเล็กทรอนิกส์ (E-mail) โดยผู้ให้บริการเทเล็กซ์ (Telex carrier) ได้ใช้เทคนิคที่เรียกว่า “Store and forward” และใช้เครื่องคอมพิวเตอร์มาแทนเครื่องเทเล็กซ์แบบเดิม ซึ่งข้อมูลที่ส่งเข้ามาสามารถเก็บไว้ใน “Electronic Mailbox” หรือบนจานบันทึกของเครื่องคอมพิวเตอร์ (Computer Disk) ไว้ก่อนโดยไม่จำเป็นต้องพิมพ์ออกมาโดยทันที อย่างไรก็ตาม เครื่องเทเล็กซ์ก็ยังถือว่ามีประสิทธิภาพในการทำงานค่อนข้างล่าช้าและมีราคาแพงเมื่อเปรียบเทียบกับ การส่งข้อมูลโดยไปรษณีย์อิเล็กทรอนิกส์ (E-mail) ด้วยเหตุนี้ความนิยมจึงลดลง

1.2 โทรสาร (Facimile)

โทรสาร (Facimile) หรือบางที่เรียกว่า Telecopy เป็นรูปแบบหนึ่งของการส่งข้อมูลทางอิเล็กทรอนิกส์ ซึ่งต้องเป็นไปตามมาตรฐานที่กำหนดโดยสหภาพโทรคมนาคมสากล (International Telecommunication Union : International Telegraph and Telephone Consultative Committee) เครื่องโทรสารเริ่มมีใช้กันมานานแล้ว แต่เพิ่งจะได้รับความนิยมใช้กันอย่างแพร่หลายในทศวรรษ 1980

เครื่องโทรสารที่เป็นที่นิยมส่วนใหญ่เป็นเครื่องโทรสารแบบตั้งโต๊ะ (Stand-alone machine) ที่สามารถเชื่อมต่อเข้ากับระบบโทรศัพท์ เครื่องโทรสารแบบเก่าจะใช้กระดาษเทอร์มอล (Thermal Paper) แต่ในปัจจุบันบางรุ่นจะใช้กระดาษธรรมดาได้ นอกจากนั้นยังสามารถติดตั้งระบบให้คอมพิวเตอร์เป็นเครื่อง Fax/modems เพื่อส่งและรับโทรสารได้เช่นกัน

ข้อมูลโทรสารที่เข้ามาไม่จำเป็นที่จะต้องถูกพิมพ์โดยทันทีบนกระดาษ เครื่องโทรสารที่มีฟังก์ชันการทำงานซับซ้อนจะสามารถเก็บข้อมูลไว้ได้ชั่วคราวจนกว่าผู้ใช้จะมีคำสั่งให้พิมพ์เอกสารดังกล่าวออกมา โทรสารที่รับโดยเครื่องคอมพิวเตอร์สามารถเก็บข้อมูลไว้ในจานบันทึกข้อมูล (Disk) แต่อย่างไรก็ดีการเก็บ

ข้อมูลดังกล่าวนี้จะเก็บไว้ในรูปแบบของโทรสาร (Fax format) ข้อมูลที่เก็บในรูปแบบของโทรสารจะไม่เก็บไว้ในรูปของตัวอักษรเลข (Alphanumeric) แต่จะเก็บในลักษณะของรูปภาพที่มนุษย์สามารถอ่านได้ (Human readable images)

1.3 ไปรษณีย์อิเล็กทรอนิกส์ (E-mail)

ไปรษณีย์อิเล็กทรอนิกส์ (E-mail) คือระบบที่ให้ผู้ใช้งานเครื่องคอมพิวเตอร์สามารถแลกเปลี่ยนข้อมูลกับผู้ใช้งานเครื่องคอมพิวเตอร์เครื่องอื่น (หรือกลุ่มผู้ใช้อื่น) บนเครือข่ายการติดต่อสื่อสาร E-mail ถือเป็นรูปแบบการประยุกต์ใช้งานที่ได้รับความนิยมอย่างมากของอินเทอร์เน็ต แม้ว่าไปรษณีย์อิเล็กทรอนิกส์ (E-mail) จะสามารถส่งได้บนเครือข่ายคอมพิวเตอร์อื่นๆนอกเหนือจากอินเทอร์เน็ตก็ตาม ข้อความของไปรษณีย์อิเล็กทรอนิกส์ (E-mail) บนอินเทอร์เน็ตจะประกอบไปด้วยส่วนหัวของข้อความที่ระบุว่าเป็นเอกสารส่งมาจากไหน ส่งให้ใคร เมื่อไร และตัวเนื้อหาของข้อความ ข้อความ E-mail จะเกิดขึ้นโดยใช้โปรแกรมบนเครื่องหรือระบบของผู้ใช้และส่งไปยังบุคคลอื่นโดยโปรแกรมในการส่งที่มีมาตรฐานในการส่ง (Transfer protocol or standard) ข้อความ E-mail อาจเก็บเป็นเอกสารอิเล็กทรอนิกส์ (Electronic record) หรือพิมพ์ออกมา ซึ่งข้อมูลเหล่านี้สามารถทำซ้ำและส่งต่อไปอีกได้

E-mail addresses บนอินเทอร์เน็ตจะประกอบไปด้วย Local name และ Domain name ซึ่งจะแยกกันโดยเครื่องหมาย @ โดย Local name จะระบุชื่อบุคคลที่ส่งหรือรับข้อมูล ส่วน Domain name จะระบุระบบคอมพิวเตอร์ที่ส่งข้อมูล ตัวอย่างเช่น E-mail address ของ Freda Bloggs คือ fbloggs@law.cyberuni.edu. Local name ของ Bloggs คือ fbloggs ซึ่งเธออาจส่ง e-mail จากคณะนิติศาสตร์ของมหาวิทยาลัยของเธอ ซึ่งกำหนดเป็น Domain name ว่า law.cyberuni.edu. ซึ่ง Domain name ดังกล่าวจะเป็นตัวบอกว่าเธออยู่ในคณะนิติศาสตร์ที่มหาวิทยาลัย Cyberia ซึ่งเป็นสถาบันการศึกษา ตามที่ใช้คำว่า edu หลังชื่อของ Local system ที่ Freda ได้รับ E-mail Address ของเธอ

1.4 การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic Data Interchange : EDI)

การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ หรือ EDI เป็นความก้าวหน้าทางการส่งข้อมูลทางธุรกิจ เช่น คำสั่งซื้อจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่ง โดยทางเทคนิคแล้วข้อความ EDI (EDI message) จะถูกส่งด้วยวิธีเดียวกันกับ E-mail ข้อความ EDI สามารถบันทึกบนสื่อ

อิเล็กทรอนิกส์หรือบนกระดาษได้ เช่นเดียวกับที่ E-mail สามารถทำได้ เทคโนโลยี EDI ได้รับการพัฒนาขึ้นในราวทศวรรษที่ 1970 เพื่อใช้ในอุตสาหกรรมการขนส่ง และได้รับความนิยมแพร่หลายในทศวรรษที่ 1980 เมื่อสามารถนำมาพัฒนาปรับใช้ได้กับอุตสาหกรรมการผลิตและการค้าปลีก ระบบ EDI สามารถใช้ให้เป็นประโยชน์กับระบบคลังสินค้าที่เรียกว่า Just-in-time , Streamlined acquisition และ ระบบการจัดจำหน่าย (Distribution System) ซึ่งจะเป็นประโยชน์กับกระบวนการ Re-engineering ของบริษัท

EDI เป็นคำย่อมาจากคำว่า “การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์” (Electronic Data Interchange) สาเหตุที่ EDI เป็นเรื่องทาง “อิเล็กทรอนิกส์” เนื่องจากเป็นขั้นตอนและกระบวนการที่เกี่ยวข้องกับการทำงานของระบบคอมพิวเตอร์ การใช้คำว่า “ข้อมูล” (Data) ก็เนื่องมาจากว่าเป็นข้อมูลสารสนเทศโดยทั่วไปทุกประเภท และเกี่ยวกับการแลกเปลี่ยน (Interchange หรือ Exchange หรือ Communications) ก็เนื่องจากการแลกเปลี่ยนข้อมูลระหว่างบุคคล ความเคลื่อนไหวของข้อมูลระหว่างบุคคลที่ใช้ EDI จะเรียกโดยรวมว่า Transaction ข้อความ (Transaction) และสัญญาณ (Signal) ต่างๆ ที่ประกอบเป็น EDI Transaction จะเรียกรวมกันว่า “Transaction Set”

EDI นั้นมีประโยชน์ทางธุรกิจหลายอย่าง โดยทั่วไปแล้วสามารถเป็นวิธีทางอิเล็กทรอนิกส์สำหรับการเจรจาและก่อให้เกิดสัญญาระหว่างคู่ค้าที่ใช้ EDI อย่างเช่น วิธีใช้ EDI ในรูปแบบเดิมนั้น มักจะทำการระหว่างคู่ค้าที่มีความใกล้ชิดในระบบปิดที่มีความสัมพันธ์ทางธุรกิจมายาวนานและมีความต่อเนื่อง การใช้ EDI จะเกิดประสิทธิภาพก็ต่อเมื่อคู่ค้าจำเป็นที่จะต้องทำการติดต่อกันในรูปแบบที่คล้ายกันซ้ำกันอย่างต่อเนื่อง ซึ่งจะช่วยลดความล่าช้าและสามารถทำการสื่อสารตอบโต้กันได้อย่างทันที (เช่น ระบบการผลิตแบบ Just-in-time manufacturing)

นอกจากนั้น EDI ยังเป็นการสื่อสารทางธุรกิจที่จำเป็นต้องมีข้อมูลที่มีรูปแบบ (Format) ที่ชัดเจน ข้อมูลทางธุรกิจจะได้รับการจัดเตรียมและวางรูปแบบตามโปรโตคอลหรือมาตรฐานที่ตกลงกันไว้ล่วงหน้าระหว่างคู่ค้า

การที่ EDI จำเป็นต้องทำให้เป็นรูปแบบ (Format) ก็เนื่องจาก 1. ลดความคลุมเครือของการติดต่อสื่อสารที่จะต้องทำเป็นประจำ ดังนั้นมาตรฐาน EDI จะต้องมีรายละเอียดระบุถึงความหมายของคำที่ใช้ในการส่งข้อมูลอย่างชัดเจน และ 2. การที่จะต้องจัดเก็บเอกสารเพื่อใช้อ้างอิงในภายหลานั้น ระบบการจัดเก็บ

เอกสารและการรักษาความปลอดภัยควรจะได้รับการจัดทำอย่างระมัดระวังให้มีเนื้อหาตรงตามที่ต้องการในเวลาต่อมา

ข้อความ EDI จะประกอบไปด้วยกลุ่มของข้อมูลที่เป็นรูปแบบ (Set of formatted data) ระหว่างคู่ค้า การส่ง การรับ และการยืนยันชุดของข้อมูลดังกล่าวจะเรียกว่า EDI "Transaction" โดยปกติแล้ว การสื่อสารสองทางจะเกิดขึ้นใน EDI Transaction กล่าวคือ ผู้ส่งส่งข้อมูล สื่อ (Carrier) (ในกรณีที่เป็นสื่ออิสระ (Independent Carrier)) ยอมรับและยืนยันความถูกต้องของข้อมูล ต่อจากนั้นสื่อจะทำการส่งข้อมูลไปยังผู้รับ โดยผู้รับจะรับและทำการยืนยันความถูกต้องของข้อมูลที่ได้รับ กระบวนการดังกล่าวนี้มีความรวดเร็วกว่าวิธีการที่ใช้กระดาษในรูปแบบเดิมอย่างมาก

EDI สามารถส่งระหว่างผู้รับและผู้ส่งผ่านทางเครื่องคอมพิวเตอร์ทั้งของผู้รับและผู้ส่ง (point-to-point) หรือส่งในรูปของดิสเก็ตที่มีข้อมูล EDI อยู่ก็ได้ (Tape-to-tape exchange) หรือเชื่อมต่อผ่านสายโทรศัพท์หรือเครือข่ายโทรคมนาคมอื่นๆ ก็ได้ นอกจากนั้น EDI ยังสามารถส่งผ่านเครือข่ายคอมพิวเตอร์ (Intermediary computer network) ที่เรียกว่าเครือข่ายเสริม (Value-added network) เครือข่ายบุคคลที่สาม (Third Party Network) หรือผู้ให้บริการ EDI (EDI Service Provider) ผู้ให้บริการ EDI จะให้บริการในการเก็บและส่งข้อมูลต่อ ตรวจสอบสถานะของข้อมูล เก็บข้อมูลไว้เพื่อการตรวจสอบ ตรวจสอบข้อมูลว่าตรงตามมาตรฐานหรือไม่ แปลข้อมูลจากมาตรฐานหนึ่งไปเป็นอีกมาตรฐานหนึ่ง เช่น มาตรฐานในระบบปิดไปเป็นมาตรฐานในระบบเปิด หรือให้บริการที่เกี่ยวข้องอื่นๆ ในขณะที่การบริการ E-mail เป็นที่แพร่หลายในปัจจุบันมีส่วนทำให้บทบาทของ EDI ลดลง ในปัจจุบัน EDI ก็ได้รับการพัฒนาให้ใช้บนเครือข่ายอินเทอร์เน็ต ซึ่งจะทำให้การใช้งานประหยัด สะดวกและรวดเร็วมากขึ้นกว่าเดิมมาก¹⁰

จะเห็นได้ว่า สิ่งที่ทำให้ EDI มีความแตกต่างจากรูปแบบการสื่อสารทางอิเล็กทรอนิกส์อื่นๆ คือ โครงสร้างและระบบของข้อมูลที่ถ่ายโอนกัน และวิธีการที่ข้อมูลถูกบันทึกและได้รับการคุ้มครอง

¹⁰ Eric J. Adams, Second Coming for Electronic Data Interchange, World Trade, Nov. 1997, p. 36

2. เทคโนโลยีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ :องค์ประกอบของระบบ

การติดตั้งระบบ EDI องค์ประกอบทุกองค์ประกอบจะต้องสามารถทำงานได้อย่างเหมาะสมทั้งโดยตัวของมันเองและโดยการเชื่อมต่อกับระบบหรืออุปกรณ์อื่นๆ ระบบ EDI ไม่ใช่จะเกี่ยวข้องกับเพียงแต่เครื่องคอมพิวเตอร์ฮาร์ดแวร์หรือซอฟต์แวร์เพียงเท่านั้น แต่ยังรวมถึงบุคลากรที่มีประสบการณ์และได้รับการอบรมในการใช้ระบบดังกล่าวอย่างมีประสิทธิภาพ นอกจากนั้นยังรวมถึงสัญญาระหว่างคู่ค้าในการใช้ EDI ที่จะต้องกำหนดหน้าที่และความผูกพันระหว่างกันอย่างเหมาะสม

2.1 องค์ประกอบเบื้องต้นของระบบ EDI

2.1.1 คอมพิวเตอร์ฮาร์ดแวร์และซอฟต์แวร์

คอมพิวเตอร์ที่สามารถนำมาใช้กับระบบ EDI นั้นมีทั้งคอมพิวเตอร์ขนาดใหญ่เช่นคอมพิวเตอร์เมนเฟรมไปจนถึงคอมพิวเตอร์ขนาดเล็กอย่างคอมพิวเตอร์ส่วนบุคคลต่างๆ การเลือกใช้ดังกล่าวจะขึ้นอยู่กับความจำเป็นทางธุรกิจ ความสอดคล้องกับเครื่องคอมพิวเตอร์ของคู่ค้า เป็นต้น

2.1.2 บาร์โค้ด

ระบบ EDI ที่ซับซ้อนในปัจจุบันจะมีเครื่องอ่าน Bar Code เป็นส่วนหนึ่งของระบบ EDI โดยที่เครื่องอ่านบาร์โค้ดเหล่านี้สามารถนำไปติดตั้งที่โรงงาน คลังสินค้า และหน่วยจัดส่งและรับสินค้า เพื่อที่จะสามารถติดตามสินค้าที่มี Bar Code ติดอยู่ ว่ามีสินค้าเข้าหรือออกจากคลังสินค้าเท่าไร รวมทั้งทราบว่าสินค้าในคลังสินค้ามีเหลืออยู่เท่าไร ซึ่งความจริงแล้วระบบการควบคุมสินค้าในคลังสินค้าแบบ Just-in-time นั้นจะไม่สามารถเกิดขึ้นได้หากไม่มีรหัสบาร์โค้ดที่สามารถป้อนข้อมูลเข้าไปในระบบ EDI

ตัวอย่างเช่น ด้วยข้อมูลที่ได้จากการติดตาม Bar Code คู่ค้าสามารถตอบรับได้อย่างถูกต้องกับคำสั่งทาง EDI ที่เกี่ยวกับสถานะของปริมาณสินค้าที่มีอยู่ หรือมีคำสั่งล่วงหน้าไปยังคู่ค้าอื่นเพื่อที่จะให้มีความล่าช้าที่เกิดจากการส่งสินค้าน้อยที่สุด¹¹

2.1.3 โปรแกรมคอมพิวเตอร์

¹¹ โปรดดู Meyers and Canis, EDI & Bar Coding Working Together, EDI world, June 1992, p. 29

เครื่องคอมพิวเตอร์ฮาร์ดแวร์เพียงอย่างเดียวไม่สามารถทำงานได้หากปราศจากโปรแกรมคอมพิวเตอร์ที่มีคำสั่งให้เครื่องคอมพิวเตอร์สามารถทำงานได้ตามที่ต้องการ

2.1.4 มาตรฐาน EDI

มาตรฐาน EDI ก็เช่นเดียวกับภาษาที่มีกฎไวยากรณ์และคำศัพท์ ข้อความ EDI จะถูกจัดโครงสร้างตามวากยสัมพันธ์ (Syntax) ที่กำหนด และส่วนต่างๆ (Contain Segment) รวมทั้งองค์ประกอบของข้อมูล (Data Element) ซึ่งองค์ประกอบข้อมูลบางองค์ประกอบเป็นเงื่อนไขบังคับ บางองค์ประกอบเป็นตัวเลือกเท่านั้น

ตัวอย่าง

EDI Message
ST*850*Blue Co.*111** RX@**7742MKB*...

(รหัส 850 หมายถึงข้อความนี้เป็นข้อความสั่งซื้อสินค้า)

ความแตกต่างในประเภทของ EDI อยู่ที่ข้อมูลถูกจัดโครงสร้างและเข้ารหัสตามมาตรฐานที่ได้ตกลงโดยผู้รับและผู้ส่ง

ข้อดีของข้อมูลที่ถูกจัดโครงสร้างและเข้ารหัส คือ เครื่องคอมพิวเตอร์ที่รับข้อมูล EDI สามารถโอนข้อมูลดังกล่าวเข้าไปในโปรแกรมการประยุกต์ใช้งาน อย่างเช่น โปรแกรมการจัดการคลังสินค้า (Inventory management software) ได้โดยอัตโนมัติ ส่วนข้อมูลที่ปรากฏบนกระดาษ โทรสาร เทเลกซ์ หรือ E-mail โดยปกติแล้วจะสามารถอ่านโดยมนุษย์เท่านั้น และจะต้องใช้คนบันทึกข้อมูลใหม่สำหรับโปรแกรมการประยุกต์ใช้งาน ซึ่งต่างจากเครื่องคอมพิวเตอร์ที่รับข้อมูลคำสั่งซื้อในรูปแบบ EDI เครื่องจะสามารถเข้าใจว่าข้อมูลนั้นคือคำสั่งซื้อสินค้าโดยไม่ต้องมีมนุษย์เข้ามาแทรกแซงการทำงาน และสามารถ Log คำสั่งซื้อดังกล่าวในรายการรับคำสั่งซื้อของผู้รับ ทำคำสั่งการส่งสินค้า และส่งข้อมูลเข้าโปรแกรมการทำบัญชี (Accounting Program) ทำให้คำสั่งซื้อดังกล่าวนั้น สามารถถูกตรวจสอบ ส่งและจองได้

ที่สำคัญอย่างยิ่ง การที่ไม่มีมนุษย์เข้ามาแทรกแซงกระบวนการทำงานของ EDI จะช่วยลดความผิดพลาดจากการป้อนข้อมูล ซึ่งก่อให้เกิดระบบการติดต่อสื่อสารที่มีความน่าเชื่อถือมากกว่ากระดาษในการสื่อสารแบบเดิมเสียอีก

มาตรฐาน EDI สามารถตกลงกันอย่างเป็นความลับ (Proprietary) หรือเปิดเผยได้ อย่างแรกเป็นการออกแบบโดยบริษัทหรือกลุ่มบริษัท ซึ่งมาตรฐานแบบปิด (Proprietary) ยังคงมีใช้อยู่ในปัจจุบัน

ในอุตสาหกรรมใหญ่ๆ จะมีการจัดทำมาตรฐานที่เปิดเผยต่อสาธารณะ มาตรฐานที่เป็นที่รู้จักเช่น ANSI X12 (พัฒนาโดย American National Standards Institute, Accredited Standards Committee X12) และ EDIFACT (EDI for Administration, Commerce, and Transport) ที่องค์การสหประชาชาติเป็นผู้พัฒนามาตรฐานดังกล่าว

2.1.5 เครือข่ายโทรคมนาคม

ข้อดีของระบบ EDI อยู่ที่ระบบดังกล่าวใช้ระบบโทรคมนาคมอิเล็กทรอนิกส์ ไม่ได้ใช้ระบบการติดต่อสื่อสารที่ชักช้า อย่างเช่น ไปรษณีย์ การสื่อสารต่อบุคคล (Personal Meeting) หรือการสื่อสารทางโทรศัพท์ ข้อดีของระบบ EDI คือความรวดเร็วในการส่งและรับข้อมูล EDI นอกจากนั้น ด้วยความก้าวหน้าทางเทคโนโลยีการสื่อสารยังส่งผลให้ข้อมูลมีความน่าเชื่อถือ สามารถเก็บข้อมูลไว้ใช้ในอนาคต รวมทั้งสะดวกสำหรับการค้นข้อมูลดังกล่าว

การเชื่อมต่อระบบ EDI เข้ากับระบบโทรคมนาคมเพื่อให้สามารถส่งข้อมูลกันได้สามารถทำได้หลายทางดังต่อไปนี้ 1. เชื่อมต่อระบบคอมพิวเตอร์เข้าด้วยกันทางสาย (Wiring the computer together) 2. ใช้ระบบ Private Telecommunications Capacities (เช่นระบบไมโครเวฟ เป็นต้น) 3. ใช้เครือข่ายโทรคมนาคมสาธารณะ (Public Common Carrier Telecommunication Networks) (อย่างเช่นระบบโทรศัพท์ เป็นต้น) และ 4. ใช้สื่อบุคคลที่สามที่ซับซ้อน (Dedicated EDI Third Party Carriers)

ระบบโทรคมนาคมแบบ EDI มีการบริการที่มีความสมบูรณ์และซับซ้อนมากกว่าเพียงแค่การส่งข้อมูลเพียงเท่านั้น สัญญาระหว่างคู่ค้าควรจะกำหนดให้ชัดเจนถึงการกำหนดหน้าที่และความรับผิดชอบของผู้ให้บริการ EDI และคู่ค้าที่ใช้ EDI ส่วนแ่งมุมที่สำคัญของระบบโทรคมนาคมที่นำมาใช้กับระบบ EDI จะต้องมีความน่าเชื่อถือ (Reliability) ความถูกต้องของข้อมูล (Accuracy) การบันทึกกระบวนการทำงาน

(Transaction Log Capabilities) การจัดเก็บข้อมูล (Message archive capabilities) ระบบรักษาความปลอดภัยทั้งภายในและภายนอก รวมทั้งระบบรักษาความเป็นส่วนตัว (Privacy Features) Temporary transaction holding capabilities และต้นทุน

2.2 ระบบจัดทำเอกสารและระบบจัดเก็บข้อมูล (Message (Transaction) Storage Facilities and Archives)

ระบบ EDI นั้นควรจะมีประสิทธิภาพเทียบเคียงกับระบบเอกสารแบบกระดาษ เอกสาร EDI ควรที่จะต้องมีความถูกต้องและสามารถใช้อ้างอิงและตรวจสอบโดยผู้ที่เกี่ยวข้องได้ ต่อไปนี้เป็นการอธิบายถึงประเภทการจัดเก็บข้อมูล

2.2.1 เอกสารที่บันทึกกระบวนการและข้อความในการรับส่ง EDI (Transaction Log)

“Transaction Log” คือแฟ้มข้อมูลที่บรรจุการสื่อสารของข้อมูล EDI จากผู้ส่งไปยังผู้รับ บุคคลที่เกี่ยวข้องกับการส่งข้อมูล EDI ควรที่จะเก็บ Transaction Logs ของตนเอง

นอกจากนี้ยังมีระบบการทำงานที่มีลักษณะคล้าย Log ที่ใช้กับ Electronic Envelope คือจะให้นี้เนื้อที่สำหรับข้อมูลบริหารของผู้ให้บริการ EDI (Carrier's administrative information) ซึ่งข้อมูลดังกล่าวที่อยู่ในซองจดหมายอิเล็กทรอนิกส์และการยกเลิกนั้น จะทำซ้ำกับข้อมูลที่อยู่ใน Transaction Log ซึ่งการทำซ้ำดังกล่าวจะช่วยป้องกันหรืออย่างน้อยป้องกันการเข้าไปยุ่งเกี่ยว (Tampering) กับข้อมูลหรือปลอมแปลงข้อมูล ขณะเดียวกันยังสามารถเตรียมพร้อมสำหรับการนำข้อมูลที่เก็บไว้มาใช้อย่างรวดเร็วอีกด้วย

2.2.2 ระบบการเก็บเอกสารอิเล็กทรอนิกส์ชั่วคราว – ตู้ไปรษณีย์อิเล็กทรอนิกส์สำหรับ EDI (Temporary Transaction Stores-“Electronic Mailboxes” for EDI)

ระบบ EDI ทุกๆ ระบบจะมีระบบเก็บข้อมูลชั่วคราว แนวความคิดในเรื่องของ EDI boxes ได้มาจากมาตรฐานในทางปฏิบัติในการใช้ Electronic Mailboxes ของอุตสาหกรรมไปรษณีย์อิเล็กทรอนิกส์ (Electronic Mail) อย่างไรก็ดี EDI Mailboxes มีหน้าที่ที่แตกต่างอยู่สองประการ 1. EDI Mailboxes จะต้องมีการรักษาความปลอดภัยในการเก็บข้อมูลและการรักษาความเป็นส่วนตัว (Privacy) 2. ผู้ใช้ EDI จะต้องตรวจสอบข้อมูลและการประมวลผลใน EDI Mailboxes เป็นระยะๆ อย่างสม่ำเสมอ

2.2.3 แฟ้มข้อมูลปัจจุบัน-“แฟ้มการทำงาน” สำหรับข้อมูล EDI ทางธุรกิจ (Current Transaction Files – “Working Files” for Business EDI Data)

เมื่อข้อมูล EDI ส่งไปยังผู้รับ ข้อมูลดังกล่าวจะถูกแปล (Interpret) และเตรียมให้พร้อมสำหรับผู้ที่ต้องการ ข้อมูลจะต้องมีพร้อมไว้จนกว่าข้อมูลดังกล่าวจะถือว่าไม่มีผลต่อการดำเนินการทางธุรกิจแล้ว

การแปล (Interpret) ข้อมูล EDI ที่เข้ารหัสและทำให้สั้น (Condensed and encoded) จะเป็นโอกาสที่ดีในการใช้ระบบรักษาความปลอดภัยในการป้องกันไวรัสคอมพิวเตอร์และผู้นุกรุกเข้ามาในเครือข่ายที่ไม่เชี่ยวชาญมากนัก โดยเฉพาะอย่างยิ่งในระบบโทรคมนาคมที่ให้บริการกับสาธารณชนรวมทั้งคู่แข่ง

2.2.4 การเก็บแฟ้มข้อมูล EDI ระยะยาว และผู้เก็บข้อมูลที่เป็นกลาง (Long-Term (Archive) EDI Files and “Trusted” Recordkeepers)

เนื่องจากการยากที่จะเลือกว่าข้อมูลใดควรที่จะมีการจัดเก็บไว้หรือไม่ ข้อมูล EDI ทั้งหมดควรที่จะถูกเก็บไว้เป็นแฟ้มข้อมูล

ก. วัตถุประสงค์ของการจัดเก็บแฟ้มข้อมูล (Archives)

แฟ้มข้อมูลที่จัดเก็บ (Archive files) มีหน้าที่หลายอย่าง ประการแรกแฟ้มดังกล่าว จะทำหน้าที่เป็นแฟ้มสำรอง (Backup file) สำหรับข้อมูลทางธุรกิจประจำวัน ที่สามารถเรียกใช้ได้โดยบุคคลที่ต้องการ ข้อมูลดังกล่าว ระดับของความจำเป็นของความน่าเชื่อถือและความปลอดภัย (Reliability and security) ในแฟ้มข้อมูลคอมพิวเตอร์ในลำดับขั้นนี้เป็นเรื่องของ การเสนอข้อมูลที่เกี่ยวข้องกับการตัดสินใจในทางธุรกิจ (A matter of Informed Business Judgement)

ประการที่สอง แฟ้มข้อมูลที่จัดเก็บ (Archives) จะสามารถใช้อ้างอิงทั้งการตรวจสอบภายนอกหรือภายในและยังสามารถใช้เพื่อวัตถุประสงค์ในการอ้างอิงประวัติความเป็นมาของเรื่องต่างๆ การทบทวนแฟ้มเอกสารดังกล่าวจะไม่มีผลกระทบต่อการดำเนินธุรกิจประจำวันของบริษัท แต่จะเพิ่มขึ้นเพื่อยืนยันว่าธุรกิจได้ดำเนินไปอย่างมีประสิทธิภาพและเหมาะสมในระยะเวลาที่ผ่านมา ระดับของความปลอดภัยและความสมบูรณ์ (Security and integrity) ในระดับนี้จะทำให้เป็นที่พอใจกับผู้ตรวจสอบและผู้ที่ต้องการทราบประวัติความเป็นมาของเอกสาร โดยทั่วไปแล้วผู้ตรวจสอบที่เป็นอิสระภายนอกต้องการตัวชี้ที่มั่นคง

และนำเชื่อถือในระบบควบคุม การรักษาความปลอดภัย และความสมบูรณ์ของเอกสารมากกว่าผู้ตรวจสอบที่อยู่ภายในหน่วยงาน อย่างไรก็ตามผู้ตรวจสอบมักมีความปรารถนาที่จะช่วยจัดทำ ออกแบบ หรือให้คำปรึกษาวิธีการจัดเก็บเอกสาร

ประการที่สาม แฟ้มข้อมูลที่จัดเก็บจะมีบทบาทหลักในการใช้เป็นพยานหลักฐานในเวลาที่มีข้อพิพาท ระดับของความน่าเชื่อถือที่จำเป็นต่อการสนับสนุนให้เอกสารเป็นพยานหลักฐานที่มีความน่าเชื่อถือจะขึ้นอยู่กับหน้าที่ที่เอกสารนั้นถูกนำไปใช้ การพิสูจน์ในทางแพ่งมักจะเพียงพอถ้าเป็นไปตามมาตรฐานของการชั่งน้ำหนักพยาน ปัญหามักจะอยู่ที่การค้นหาระดับการพิสูจน์ที่น่าเชื่อถือและชัดเจน

เนื่องจากแฟ้มข้อมูลที่จัดเก็บ (Archive) จะเป็นที่ค้นพบพยานหลักฐานในเวลาที่มีข้อพิพาท ดังนั้นแฟ้มข้อมูลที่จัดเก็บดังกล่าวจะต้องถูกจัดทำดัชนีและสามารถตรวจสอบข้ามระบบ (Cross-referenced) เพื่อที่จะให้สามารถใช้แฟ้มข้อมูลดังกล่าวได้อย่างสะดวก

ข. การจัดเก็บแฟ้มข้อมูลโดยผู้จัดเก็บหรือโดยบุคคลที่สามที่เป็นกลาง ("Trusted" Third Party Carriers and Archivists)

ข้อเสนอแนะของผู้เชี่ยวชาญหลายท่าน¹² คือ อย่างน้อยเอกสารชุดหนึ่งควรที่จะถูกจัดเก็บโดยหน่วยงานหรือองค์กรที่เป็นกลาง เพื่อที่จะเพิ่มความน่าเชื่อถือหรือความไว้วางใจในการรับเอกสาร EDI เป็นพยานหลักฐาน หน่วยงานที่จะสามารถทำการจัดเก็บเอกสารจะต้องเป็นผู้ที่สามารถไว้วางใจ (Trust) สำหรับบุคคลทุกฝ่ายได้ ซึ่งจะต้องมีเกณฑ์อันเป็นมาตรฐานดังต่อไปนี้

1. ใช้เทคโนโลยีในการจัดเก็บเอกสารที่ดี
2. ไม่มีเหตุผลใดที่จะเข้าไปแก้ไขข้อมูลที่ตนจัดเก็บ
3. ไม่มีผลประโยชน์ที่จะให้บุคคลอื่นเข้าแก้ไขเปลี่ยนแปลงเอกสารที่จัดเก็บ

¹² Wright, Authenticating EDI: The location of a trusted Record Keeper, 6 Computer Law & Practice 80 (Jan.-Feb., 1990)

4. มีมาตรการและขั้นตอนในการรักษาความปลอดภัยอยู่ในระดับที่ได้มาตรฐานที่จำเป็นสำหรับความถูกต้องและความสมบูรณ์ของข้อมูลที่จัดเก็บ

คู่ค้าที่ใช้ EDI โดยปกติแล้วจะมีทางเลือก 3 ประการในการจัดเก็บข้อมูลดังนี้

1. คู่ค้าที่ใช้ EDI จัดเก็บข้อมูลของตนเอง ซึ่งจำเป็นต้องอาศัยกระบวนการภายในเพื่อสนับสนุนความน่าเชื่อถือของเอกสารในเวลาที่มีข้อพิพาทเกิดขึ้น

2. คู่ค้าใช้หน่วยงานภายในที่จัดไว้อย่างเป็นระบบในการจัดเก็บเอกสาร ถ้าหน่วยงานดังกล่าวมีหน้าที่ในการเก็บรักษาข้อมูล EDI ที่มีผลทางกฎหมายหรือเป็นการตกลงในรูปของสัญญา ซึ่งจะส่งผลให้เอกสารมีความน่าเชื่อถือ เนื่องจากหน่วยงานดังกล่าวมีความน่าเชื่อถือกว่าที่คู่ค้าจัดเก็บเอง

3. คู่ค้าใช้บุคคลหรือหน่วยงานที่จัดเก็บแฟ้มข้อมูลที่เป็นอิสระ ผู้เก็บเอกสารดังกล่าวนี้จะไม่มีหน้าที่อื่นนอกจากจัดแฟ้มเอกสาร (Archive) ทำดัชนีเอกสาร (Index) และรักษาเอกสาร เพื่อที่จะให้หน้าที่ดังกล่าวบรรลุผล ผู้เก็บเอกสารจะต้องสามารถเข้าถึงข้อมูลหรือคู่ค้า EDI จะต้องตกลงที่จะเสนอกลุ่มของข้อมูลที่จะทำการจัดเก็บเพื่อนำมาใช้ในระยะยาวต่อไป ทางเลือกในรูปแบบนี้มักจะมีค่าบริการที่แพงกว่าการจัดเก็บเองภายในหน่วยงาน แต่อย่างไรก็ดีการจัดเก็บโดยบุคคลที่สามจะเป็นวิธีที่ดีที่สุดที่จะทำให้หลีกเลี่ยงความเชื่อมั่นในพยานหลักฐานทางอิเล็กทรอนิกส์ที่นำเสนอได้

2.3 โปรโตคอลการสื่อสารโดยใช้ EDI

ตัวอย่าง การติดต่อสื่อสารโดยใช้ EDI ระหว่างบริษัท ABC และ บริษัท กขค

2.3.1 กลไกในการติดต่อสื่อสารโดยใช้ EDI (The Mechanics of a Typical EDI Transaction)

กระบวนการในการใช้ EDI จะเริ่มต้นขึ้นเมื่อระบบควบคุมคลังสินค้าของบริษัท ABC มีสัญญาณว่าสินค้าในคลังสินค้าลดลงในระดับที่ได้กำหนดไว้ ระบบคลังสินค้าจะส่งข้อความไปที่ผู้จัดการคลังสินค้า ผู้ที่จะรับรู้คำสั่งดังกล่าวก็ต่อเมื่อได้ “Log on” ที่ Workstation โดยเขาจะได้รับประมาณการสินค้าที่ต้องการ (โดยข้อมูลดังกล่าวจะเก็บไว้ในฐานข้อมูลฝ่ายการผลิตและฝ่ายการตลาด) และทำการเลือกบริษัทที่จะสั่งซื้อสินค้าหลังจากที่ตรวจสอบแล้วว่าราคาและคุณภาพดีที่สุดใน

หลังจากนั้นผู้จัดการคลังสินค้าจะเปิดระบบ EDI Transaction Editing Interface (EDI-TEI) ที่จำเป็นที่จะต้องมียรหัสผ่าน (Passcode) เพื่อเหตุผลในการรักษาความปลอดภัย โดยผู้จัดการคลังสินค้าจะแจ้งให้กับผู้ดูแลคอมพิวเตอร์ให้กับบริษัท กขค. ว่ากำลังจัดเตรียมข้อความ EDI ผู้ควบคุมระบบ (System monitor) ก็จะบันทึกข้อมูลใน Special Log

เมื่อผู้จัดการคลังสินค้านำเข้าบริษัท กขค. จะเป็นบริษัทที่ได้รับคำสั่งซื้อสินค้า EDI-TEI จะเลือกโปรโตคอล EDI ที่ได้ออกไว้แล้วทั้งสองฝ่าย นอกจากนั้นยังต้องมีการยืนยันว่าไม่มีปัญหาที่รุนแรงเกิดขึ้นในอดีตที่ผ่านมา ต่อมา EDI-TEI จะเปิดเมนูของประเภทรายการข้อมูลที่มีตามโปรโตคอล EDI ที่เหมาะสม ในกรณีนี้ผู้จัดการฝ่ายคลังสินค้าจะเลือก "inventory order – routine" ตามประเภทรายการข้อมูลที่เหมาะสม (Appropriate transaction type)

ต่อมา EDI-TEI จะเปิดการเชื่อมต่อเอกสาร (Document Interface) ซึ่งจะได้รับการออกแบบให้มีการตรวจสอบ ตรวจข้อผิดพลาดและแก้ไขข้อมูลภายใต้โปรโตคอลที่เหมาะสม ขณะที่การเชื่อมต่อเอกสาร (Document Interface) พร้อมแล้ว ผู้จัดการจะทำการบันทึกข้อมูล รายการข้อมูลที่สำคัญ (เช่นจำนวนสินค้าที่สั่ง) จะถูกบันทึกเป็นสองแบบ (แบบตัวเลขและเขียนอย่างสมบูรณ์ (Numerically and written out) ระบบเชื่อมต่อ (Interface) จะตรวจข้อผิดพลาดในการพิมพ์ อย่างไรก็ตามโดยพื้นฐานแล้วเอกสารจะถูกแก้ไขให้ตรงตามแบบและเนื้อหาที่ถูกต้อง

สมมติว่าในระหว่างการทำคำสั่ง ผู้จัดการคลังสินค้านำเข้าสินค้าในคลังสินค้านั้นอย่างมากจำเป็นที่จะต้องสั่งสินค้าบริษัท กขค. อย่างเร่งด่วนเพื่อให้แน่ใจว่าบริษัท กขค. จะสามารถผลิตสินค้าได้ทันเวลา ผู้จัดการคลังสินค้านำเข้าจะเปิดแบบของข้อความพิเศษ "priority administrative message-rush delivery" ขณะที่ยังอยู่ในการเชื่อมต่อเอกสาร "inventory order – routine" EDI-TEI จะส่งสัญญาณให้ผู้จัดการคลังสินค้านำเข้ายืนยัน new administrative message ที่เกี่ยวกับคำสั่งสินค้าที่ได้เปิดไว้แล้ว เมื่อมีการยืนยัน EDI-TEI จะทำการสร้างจดหมายอิเล็กทรอนิกส์เพื่อส่งข้อมูลเป็น "ชุด" ในขั้นตอนสุดท้ายของการส่ง EDI EDI-TEI จะยืนยันว่าผู้จัดการคลังสินค้าใช้ Workstation ที่มีอำนาจในการส่งข้อมูลประเภทนี้ และต่อมาก็จะเปิดการเชื่อมต่อเอกสารอีกอันหนึ่งเพื่อสร้างและตรวจสอบคำสั่งส่งเอกสารด่วน (Rush Delivery Notice)

เมื่อข้อมูลได้รับการแก้ไขเสร็จสมบูรณ์แล้ว ผู้จัดการคลังสินค้านำเข้าจะเลือกฟังก์ชัน "Process transaction set" ฟังก์ชันนี้จะเข้ารหัสและทำให้เล็กลง (Encodes and Condenses) ในส่วนที่สามารถ

เลือกได้ของข้อมูลตาม EDI โปรโตคอล จากนั้น EDI-TEI จะทำการตรวจสอบข้อมูลกับค่า parameter ที่ตั้งไว้และค่าสถิติต่างๆ ในกรณีนี้จะให้ค่า (Flag) สำหรับรายการข้อมูลนี้ว่าไม่ปกติเนื่องจากในข้อสมมุติฐานนี้ นี่เป็นครั้งที่สี่ที่มี "คำสั่งเร่งด่วน" (Rush Order) สำหรับการสั่งซื้อสินค้าในช่วงสิบสองเดือน จึงควรมีการส่งตรวจสอบอื่นๆ

ณ จุดนี้ระบบ EDI-TEI จะทำการจัดรูปแบบ (format) โดยอัตโนมัติและเข้ารหัสคำสั่ง ใส่ข้อมูลตาม EDI โปรโตคอลและทำรายการใน Internal Logs เมื่อเสร็จสมบูรณ์แล้ว EDI-TEI จะส่งคำขอ (request) และได้รับอำนาจให้ออนข้อมูลไปยังบริษัท กขค

2.3.2 การโอนข้อมูลไปยังระบบของผู้ให้บริการ EDI (Transfer to the EDI Carrier's System)

ภายใต้สมมุติฐานเดิม EDI-TEI กำหนดให้ข้อมูลที่ถูกต้องส่งไปยังระบบเชื่อมโยงผู้ให้บริการ EDI (EDI Carrier Link System (EDI-CLS)) ที่ทำหน้าที่รับข้อมูลแล้วส่งต่อ (Holding and routing) รายการข้อมูล EDI ของบริษัท ABC จะทำการ Log record เมื่อของจดหมายอิเล็กทรอนิกส์ของผู้จัดการคลังสินค้าเข้าไปในระบบ EDI-CLS รายการข้อมูล EDI จะ Log ข้อมูลดังต่อไปนี้ 1. บันทึกข้อมูลผู้เขียนและที่มาของข้อมูล 2. ให้เลขลำดับเอกสาร (Serial Number) 3. บันทึกข้อมูลวันที่และเวลาที่ยอมรับการส่งข้อมูล 4. บันทึกขนาดของชุดรายการข้อมูล (Transaction Set) (ตามหน่วยความจำของเครื่องคอมพิวเตอร์ (บิต)) 5. บันทึกโปรโตคอลตามที่ได้เข้ารหัส และ 6. บันทึกประเภทของรายการข้อมูลที่อยู่ในของจดหมายอิเล็กทรอนิกส์

EDI-CLS จะจัดของจดหมายอิเล็กทรอนิกส์ในรูปแบบของลำดับการมาก่อนหลัง (First in, first out: FIFO) เพื่อจัดส่งต่อไป เมื่อชุดรายการข้อมูลของผู้จัดการคลังสินค้า (บันทึกตามลำดับและเร่งด่วน (Order and rush memo) ได้รับการยอมรับเพื่อการประมวลผล EDI-CLS จะทำการตรวจสอบผู้รับเป้าหมาย (ในที่นี้คือบริษัท กขค) และโปรโตคอลตามชุดรายการข้อมูลได้เข้ารหัส (รวมทั้งโปรโตคอลของจดหมายอิเล็กทรอนิกส์) เพื่อเลือก Carrier ในการส่ง EDI ที่เพียงพอ ในกรณีนี้ EDI-CLS จะกำหนดว่า EDIPhone เป็น Carrier ที่เหมาะสม

ต่อมา EDI-CLS จะเปิดการเชื่อมต่อทางโทรคมนาคม (Telecommunication Link) กับ EDIPhone ซอฟต์แวร์ที่มีชื่อว่า Incoming Transaction Software (ITS) ของ EDIPhone จะตรวจสอบและ

รับรหัส (Identification) ของ 1. ผู้ส่งรายการข้อมูล (บริษัท ABC) 2. ผู้รับรายการข้อมูล (บริษัท กขค) 3. โปรโตคอล EDI ที่ใช้สำหรับรายการข้อมูล และ 4. ขนาดของชุดรายการข้อมูล

ITS จะบันทึกข้อมูลทันทีใน Transaction Log ที่เข้ามาของ EDIPhone และเปิดหน่วยความจำชั่วคราว ของเครื่องคอมพิวเตอร์(Computer memory buffer) ให้เพียงพอสำหรับชุดรายการข้อมูล EDI-CLS ของบริษัท ABC จะส่งข้อมูล ส่วน ITS ของ EDIPhone จะประมวลผลและกรอง (Filter) เพื่อค้นหาข้อมูลที่ไม่สมบูรณ์และคอมพิวเตอร์ไวรัสอื่นๆ เมื่อการรับข้อมูลเสร็จและเก็บ ในหน่วยเก็บข้อมูล EDI ชั่วคราว ITS จะส่ง "Hash total check" ไปยัง EDI-CLS เพื่อที่จะทำการยืนยันว่าได้รับข้อมูลถูกต้องแล้ว โดยถือว่า Hash Total นั้นถูกต้อง สิ่งที่ EDI-CLS จะทำโดยทันที คือ 1. ส่งสัญญาณการยืนยัน และ 2. บันทึกเวลาและวันที่ที่ชุดรายการข้อมูล (Transaction Set) ได้รับอย่างถูกต้องโดย EDIPhone ITS ของ EDIPhone จะบันทึกเวลาและวันที่ที่ได้รับสัญญาณยืนยัน (ซึ่งจะเป็นตัวชี้ให้เห็นถึงขั้นตอนการส่งผ่านข้อมูลได้เสร็จสมบูรณ์แล้ว) ต่อมา ITS ก็จะวางหน่วยควบคุมของชุดรายการข้อมูลไว้ใน "Transaction Processing Software" (TPS) ของ EDIPhone

2.3.3 การประมวลผลข้อมูลและการเก็บรักษาข้อมูลโดยผู้ให้บริการ EDI (Transaction Processing and Recordkeeping)

อันดับแรก TPS จะสร้าง Administrative Record สำหรับชุดรายการข้อมูล รายการข้อมูลดังกล่าวจะรวมถึงวันที่และเวลาที่ Carrier ได้รับการยืนยันความถูกต้องจากบริษัท ABC และต่อมา TPS จะส่งสำเนาของชุดรายการข้อมูลที่ได้รับมาไปยัง Archive Creation System (ACS) โดย ACS จะประกอบไปด้วย Entry Log แยกต่างหากและระบบบันทึกการจัดเก็บข้อมูล (Archive Recording System) ที่ใช้อุปกรณ์เก็บข้อมูลถาวร (Long-term storage device) ที่เรียกว่า WORM (ย่อมาจาก "write once, read many" ระบบการบันทึกข้อมูลที่ไม่สามารถเขียนทับได้คือให้อ่านได้เพียงอย่างเดียว) ความถูกต้องของชุดรายการข้อมูลที่เก็บเข้าแฟ้มเอกสารจะได้รับการยืนยันโดยการแลกเปลี่ยนข้อมูลระหว่าง ACS และ TPS เมื่อมีการยืนยันความถูกต้องแล้ว สัญญาณ ACS ที่ส่งไปยัง TPS ที่ในทิศทางกลับกันจะบันทึกข้อมูลนี้และอ้างอิงถึงเลขลำดับเอกสารของแฟ้มข้อมูลที่จัดเก็บในแฟ้มข้อมูล Administrative Record ต่อมา TPS จะเชื่อมต่อเข้าไปในฐานข้อมูล Special Directives (This database allows an EDI partner to establish a list of people from whom not to accept business.) ที่มีชุดรายการข้อมูลของผู้รับ คือบริษัท กขค

Special Directives ของบริษัท กขค. จะรวมถึง การตรวจสอบว่ารายการข้อมูลของผู้ส่ง ตรงกับรายชื่อคู่ค้า EDI ที่มีอำนาจ (Authorized EDI trading Partners) หรือไม่ บริษัท ABC อยู่ในรายชื่อของบริษัท กขค. และไม่มี Special Directive อื่นจากบริษัท กขค. ที่จะใช้กับรายการข้อมูลนี้ ความจริงที่ว่า Special Directive ของบริษัท กขค. ที่ได้รับการทดสอบและยืนยันจะถูกบันทึกในแฟ้ม Administrative Record สำหรับชุดรายการข้อมูล ณ จุดนี้ TPS จะโอนการควบคุมไปยัง “Outgoing Transaction Software (OTS)”

OTS จะกำหนดจากแฟ้มข้อมูลให้ผู้ให้บริการ EDI (EDI Carrier) ซึ่งในที่นี้คือ EDIPhone ซึ่งจะสามารถติดต่อกับบริษัท กขค. ได้โดยตรง (กล่าวคือผู้ให้บริการ EDI ไม่จำเป็นต้องรอให้บริษัท กขค. ตรวจสอบข้อมูลก่อน) ข้อเท็จจริงอันนี้จะถูกบันทึกไว้ในแฟ้มข้อมูล Administrative สำหรับชุดรายการข้อมูล ต่อมา OTS จะจัดชุดรายการข้อมูลในรูปแบบของลำดับการมาก่อนหลัง (First in, first out: FIFO) เมื่อชุดรายการข้อมูลของบริษัท ABC มาถึง OTS จะเปิดการเชื่อมต่อระบบโทรคมนาคมกับระบบ EDI ของบริษัท กขค. ถ้าในการพยายามครั้งแรก ไม่สามารถเชื่อมต่อระบบโทรคมนาคมได้ (เช่นสายไม่ว่าง) OTS จะบันทึกความพยายามในการเชื่อมต่อการสื่อสารดังกล่าวรวมทั้งเหตุผลที่ไม่สามารถเชื่อมต่อได้ใน Administrative File โดยชุดรายการข้อมูลจะถูกจัดวางไว้ในตอนท้ายของคิวเอกสาร ก่อนที่ OTS จะทำการพยายามครั้งที่สองในการส่งรายการข้อมูล ระบบ EDI-TEI ของบริษัท กขค.จะถาม EDIPhone สำหรับรายการข้อมูลใดๆ ที่ส่งมา หลังจากที่ได้ค้นคิวเอกสารส่งออก OTS จะแยกรายการข้อมูล EDI ต่างๆ สำหรับบริษัท กขค. และส่งไปตามลำดับ เมื่อชุดรายการข้อมูลจากบริษัท ABC ปรากฏขึ้น OTS จะลงบันทึกใน Administrative File สำหรับรายการข้อมูลที่ได้ติดต่อกับบริษัท กขค. แล้วว่า (ลงบันทึกว่า) บริษัท กขค. ได้เริ่มติดต่อ รวมทั้งวันและเวลาของการส่งผ่านชุดข้อมูลของบริษัท ABC

EDI-TEI ของบริษัท กขค. จะบันทึกใน Transaction Log ของตนเองว่า 1. EDIPhone ได้กำลังทวนสัญญาณ (Relaying) ข้อมูลที่ส่งเข้ามาจากบริษัท ABC 2. ชนิดของรายการข้อมูลที่เกี่ยวข้อง 3. โปรโตคอล EDI ที่ใช้ 4. ขนาดของแฟ้มข้อมูล และ 5. รายการข้อมูลของผู้รับภายในบริษัท กขค. ต่อมาก็จะรับข้อมูลที่ส่งผ่านมาจาก EDIPhone ไว้ในหน่วยเก็บความจำชั่วคราว EDI-TEI ของบริษัท กขค. จะคำนวณค่า Hash Total เพื่อตรวจสอบความถูกต้องของการส่งผ่านข้อมูลจาก EDIPhone OTS ของ EDIPhone จะยืนยันการตรวจสอบค่า Hash ต่อมา EDI-TEI จะทำการตรวจสอบ Administrative File ของบริษัท EDIPhone บนชุดรายการข้อมูลของบริษัท ABC เพื่อที่จะค้นหาว่าเมื่อไรที่ได้รับข้อมูลจากบริษัท ABC

และเลขลำดับเอกสาร (Serial Number) ข้อมูลดังกล่าวนี้จะถูกบันทึกใน Transaction Log ของบริษัท กขค ด้วย

OTS ของ EDIPhone จะบันทึกวันที่และเวลาที่ EDI-TEI ของบริษัท กขค ส่งสัญญาณเพื่อ ยืนยันการตรวจสอบ Hash ใน Transaction Log และใน Administrative File สำหรับชุดรายการข้อมูลของบริษัท ABC ต่อมา OTS ก็จะทำการประมวลผล Administrative File เพื่อทำดัชนีรายการข้อมูลที่เหมาะสมสำหรับ Transaction Log และในที่สุดก็จะส่งสำเนาของ Administrative File ไปที่ ACS สำหรับการ จัดเก็บแฟ้มข้อมูลต่อไป

2.3.4 การเริ่มประมวลผลโดยผู้รับข้อมูล EDI

EDI-TEI ของบริษัท กขค จะปิดการเชื่อมต่อกับ EDIPhone และทำการกรองข้อมูล (Filter) ชุดรายการข้อมูลเพื่อตรวจสอบไวรัสคอมพิวเตอร์ ข้อมูลที่ไม่สมบูรณ์ (Garbled data) และสัญญาณพิเศษอื่นๆ (เช่นคำสั่งเร่งด่วน (Rush Order เป็นต้น) และยืนยันว่าผู้ส่งเป็นบริษัท ABC จริง ต่อมาจะสร้างการรับรู้ (acknowledgement) ว่ามีการรับรายการข้อมูลและทำการส่งคำยืนยันชุดรายการข้อมูลที่ได้รับที่ระบุโดย เลขลำดับเอกสาร และระบุทั้งเวลาที่ EDIPhone ได้รับชุดรายการข้อมูลแต่แรกและเวลาและวันที่ที่บริษัท กขค ได้รับรายการข้อมูลดังกล่าว

ต่อมา EDI-TEI ของบริษัท กขค จะเคลื่อนย้ายชุดรายการข้อมูลไปยังส่วนเก็บข้อมูลชั่วคราว (Buffer) ที่สามารถเข้าถึงได้จากเครื่องคอมพิวเตอร์ Workstation ภายในบริษัท กขค โดยชุดรายการข้อมูล จากบริษัท ABC จะถูกจัดทำเครื่องหมาย (Flag) ว่าเป็น "คำสั่งเร่งด่วน" (Rush Order) และจะได้รับการ ถือว่ามีความสำคัญเร่งด่วน (Priority) ในกรณีนี้ "การจัดลำดับความสำคัญ" หมายถึงคอมพิวเตอร์ Workstation ที่ซึ่งผู้จัดการฝ่ายประมวลผลการจัดลำดับ (Order Processing Manager) ทำงานอยู่ ได้ส่ง สัญญาณเตือน (Override Signal) "Beep" ว่ามีข้อมูลที่มีความจำเป็นเร่งด่วนในหน่วยเก็บข้อมูล

2.3.5 การตีความรายการข้อมูล EDI

ผู้จัดการการประมวลผลการจัดลำดับเอกสาร (Order Processing Manager) ของบริษัท กขค จะทำการเก็บรักษา (Save) ข้อมูลที่ได้มาและเปิด EDI-Transaction Interpreting Interface (EDI-TII) ที่ จะยืนยันโดยรหัสผ่านของผู้จัดการ การเตือน “ลำดับความสำคัญของเอกสาร” (Priority Message) จะ แสดงขึ้นอีกครั้งหนึ่งเพื่อที่จะเตือนผู้จัดการการประมวลผลการจัดลำดับความสำคัญถึงการมาถึงของ “คำสั่งเร่งด่วน” จากบริษัท ABC โดยผู้จัดการจะทำการเลือกฟังก์ชัน “เปิดรายการข้อมูล” (Open transaction) จากเมนูและเลือก “คำสั่งเร่งด่วน” (Rush Order) เพื่อให้พิจารณาอย่างทันทีทันใด

EDI-TII จะตรวจสอบโปรโตคอล EDI ตามที่มีคำสั่งเร่งด่วนเข้ามา (Incoming rush order) จะถูก แปลความหมายและใช้โปรแกรม “แปลความหมาย” (Translation) ที่เหมาะสมในการถอดรหัสและรื้อฟื้น (Reconstitute) ข้อความ “Priority administrative message-rush delivery” ผู้จัดการการประมวลผลการ จัดลำดับเอกสารจะต้องอ่านข้อมูลนี้และทำการเลือกรายการข้อมูล “Inventory order – routine” เพื่อทำ การแปลความหมายต่อไป

EDI-TII จะเก็บรักษาสำเนาของข้อความและชุดรายการเอกสารพิเศษ (Special Transaction set) ของ “Priority administrative message-rush delivery” ในหน่วยจัดเก็บข้อมูลชั่วคราวที่กำลังทำงานของ Workstation ของผู้จัดการ หลังจากนั้นจะยืนยันว่าโปรโตคอล EDI ที่ใช้ในรายการข้อมูล “Inventory order-routine” เหมือนกับในรายการข้อมูล “Rush delivery” และเข้าไปในโปรแกรมการแปลข้อมูลที่เหมาะสม

โปรแกรมการแปลข้อมูลจะรื้อฟื้น (Reconstitute) ข้อมูล “Inventory order-routine” และเปิดชุด Statistical Filters และโปรแกรมการแยกแยะข้อมูล (Classification Software) เพื่อจัดประเภทของข้อมูล โดยเฉพาะอย่างยิ่ง จะยืนยันดังต่อไปนี้

บริษัท ABC ได้สั่งซื้อสินค้าก่อน

จำนวนสินค้าที่สั่งตรงกับที่บริษัท ABC เคยสั่ง

ผู้จัดการคลังสินค้าของบริษัท ABC ที่จัดเตรียมรายการข้อมูลดังกล่าวเป็นผู้มีอำนาจที่จะทำคำสั่ง ดังกล่าว (ตรวจสอบกับฐานข้อมูลของบริษัท ABC)

ผู้จัดการคลังสินค้าได้เคยทำคำสั่งที่เหมือนกันในอดีต (ตรวจสอบกับฐานข้อมูลการจำหน่ายสินค้าของบริษัท กขค)

ฝ่ายการตลาดของบริษัท กขค และฝ่ายจัดส่งสินค้า (Shipment Department) ไม่ได้ทำการเปลี่ยนแปลงโครงสร้างราคาสินค้าและวิธีการส่งมอบสินค้าใหม่เร็วๆ นี้ (เงื่อนไขจะกำหนดโดยผู้จัดการของฝ่ายที่เกี่ยวข้อง) และ

ความสัมพันธ์ทางธุรกิจกับบริษัท ABC ไม่มีการเปลี่ยนแปลงในระยะเวลาที่ผ่านมา (เงื่อนไขจะกำหนดโดยผู้บริหารของบริษัท กขค)

EDI-TII จะทำแฟ้มข้อมูลเอกสารภายใน (Internal Archive) ของชุดรายการข้อมูล "Priority administrative message-rush delivery" และ "Inventory order-routine" ที่ได้รับและการแปลความหมายของข้อมูลดังกล่าว รายการข้อมูลเหล่านี้จะถูกทำดัชนีและทำการอ้างอิงข้ามระบบ (Cross-reference) (โดยเลขลำดับเอกสาร (Serial Number) เวลาที่รับรายการข้อมูล สินค้าที่เกี่ยวข้อง และเอกสารบอกกล่าวคำสั่งเร่งด่วน) เพื่อวัตถุประสงค์ในการอ้างอิงภายใน ต่อมา EDI-TII จะแสดงเนื้อหาของคำสั่งไปยังผู้จัดการการประมวลผล (Order processing manager) พร้อมกับข้อมูลที่ไม่ปกติหรือข้อมูลทางสถิติที่ต้องการให้ตัดออก ถ้ามีคำถามใดๆ ที่เกี่ยวกับความหมายของข้อมูลที่แสดง ผู้จัดการสามารถอ้างอิงถึงแนวทางการแปลความหมาย EDI (EDI Interpretation Guidelines) ที่แนบเป็นภาคผนวกของข้อตกลงแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic Data Interchange Agreement)

ในทางทฤษฎี คู่ค้าหรือคู่สัญญาแต่ละฝ่ายควรที่จะสามารถจัดทำเอกสารให้เพียงพอกับวัตถุประสงค์ที่ตนต้องการ ในกรณีที่มีข้อพิพาท เอกสารของบุคคลสามฝ่าย (ผู้ส่ง ผู้ให้บริการส่ง (Carrier) และผู้รับ) จะสามารถตรวจสอบเปรียบเทียบกันได้ หากเพียงสองฉบับถูกต้องตรงกันก็อาจทำให้เชื่อถือได้ว่าเอกสารนั้นถูกต้อง ถ้าไม่มีเอกสารที่ถูกต้องตรงกันเลย จะถือว่าเอกสารที่เก็บโดยบุคคลที่มีผลประโยชน์เกี่ยวข้องน้อยที่สุด (โดยปกติจะเป็นผู้ให้บริการ (Carrier) ที่เป็นบุคคลที่สาม) จะถือเป็นพยานหลักฐานที่มีน้ำหนักมากที่สุด

นอกจากนั้นระบบการจัดเก็บข้อมูลในแต่ละกรณี ก็จะเป็นตัวที่มีความสำคัญ ปัญหาจะขึ้นอยู่กับใช้เอกสาร (Record) อะไรกับข้อเท็จจริงอย่างไรมากกว่า

ก. เอกสารของผู้ส่ง (Sender's Records)

เอกสารของผู้ส่งข้อมูลควรมีเพียงพอที่จะคุ้มครองผลประโยชน์ของผู้ส่ง ผลประโยชน์เหล่านี้ นับตั้งแต่การพบและการแก้ไขปัญหาภายในไปจนถึงการรักษาความเป็นส่วนตัวและความปลอดภัยจนถึงขั้นทำข้อตกลงโดยใช้การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ในฐานะที่เป็นสัญญา

1. "System Monitor Log" ของผู้ส่ง

โดยปกติแล้ว System Monitor Log จะทำหน้าที่สนองตอบต่อวัตถุประสงค์ภายในหลายประการ เช่นทำให้เกิดการวัดผลที่มีประสิทธิผลและมีประสิทธิภาพ สนับสนุนระบบการรักษาความปลอดภัยภายใน และช่วยตรวจจับผู้บุกรุกที่เข้ามายังระบบ โดยปกติแล้ว System Monitor Log จะประกอบไปด้วยข้อมูลดังต่อไปนี้

- วันที่และเวลาของการจัดทำข้อมูลต้นฉบับ
- เครื่องคอมพิวเตอร์ Workstation เครื่องไหนที่จัดทำเอกสารดังกล่าว
 - Computer software package ที่ใช้ประมวลผลรายการข้อมูล
 - เจ้าหน้าที่ที่ทำคำสั่ง
- ชนิดของรายการข้อมูลที่รวมอยู่
- EDI โปโตคอลที่ใช้จัดทำ Format รายการข้อมูล
- วันและวันที่ที่รายการข้อมูลได้รับอำนาจให้จัดส่ง
- คู่ค้าใดที่รายการข้อมูลต้องส่งไปถึง
- "รหัส" (Flag) พิเศษที่แสดงถึงความผิดปกติของชุดรายการข้อมูล

2. "Outgoing Transaction Log" ของผู้ส่ง

Outgoing Transaction Log ของผู้ส่งจะประกอบไปด้วยชุดรายการข้อมูลที่ติดตาม (Trace Transaction Set) การติดตาม (Tracing) ควรจะทำทั้งส่งต่อ (Forward) ไปที่ผู้ให้บริการ EDI (Carrier) หรือส่งกลับ (Backward) ไปที่ต้นกำเนิดรายการข้อมูล EDI เอกสารที่กล่าวถึงในเบื้องต้นจะรวมถึง

- เมื่อไรที่ชุดรายการข้อมูลถูกได้รับจากผู้จัดการคลังสินค้าเพื่อการส่งผ่านข้อมูล
- ใครคือผู้จัดการคลังสินค้าที่จัดทำชุดรายการข้อมูล
- Workstation ไหนที่ใช้ทำชุดรายการข้อมูล
- ขนาดของชุดรายการข้อมูล (ไบต์)
- โปรโตคอล EDI ที่ใช้ Format รายการข้อมูล
- ประเภทของรายการข้อมูลในจดหมายอิเล็กทรอนิกส์
- เลขลำดับเอกสารของผู้ส่งสำหรับชุดรายการข้อมูล
- รหัส (Identity) ของผู้ให้บริการข้อมูล (Carrier) ที่ได้รับเลือกให้ส่งผ่านชุดรายการข้อมูล
- รหัส (Identity) (หรือที่อยู่ทางอิเล็กทรอนิกส์) ของผู้รับรายการข้อมูล และ
- วันและเวลาที่ผู้ให้บริการข้อมูล (Carrier) ยืนยันการรับการส่งผ่านที่ถูกต้องของชุดรายการข้อมูล

มูล

3. "Incoming Transaction Log" ของผู้ส่ง

ข้อมูล Log Record นี้จะเกี่ยวกับข้อมูล EDI (EDI Message) ที่ได้รับจากผู้รับรายการข้อมูล ใช้เพื่อที่จะเป็นส่วนเสริมและ

ให้ Outgoing Transaction Log มีความสมบูรณ์ในการติดตามรายการข้อมูล Log นี้จะประมวลผล "Functional Acknowledgment" ที่ส่งโดยผู้รับรายการข้อมูลต้นฉบับ เอกสารที่เกี่ยวกับ "Functional acknowledgement" อย่างน้อยควรจะระบุรายการข้อมูลที่เกี่ยวข้องเนื่องกับการยอมรับ (Acknowledgement) Log ดังกล่าวควรที่จะมีรายการข้อมูลดังต่อไปนี้

- เวลาและวันที่ที่ "Functional Acknowledgement" ถูกส่งไปแต่แรกโดยผู้รับ (Addressee) รายการข้อมูลต้นฉบับ
- วันและเวลาที่ "Functional Acknowledgement" ได้รับ
- เลขลำดับเอกสาร (Serial Number) ของชุดรายการข้อมูลต้นฉบับที่ออกโดย ผู้ส่ง ผู้รับ และผู้ให้บริการ EDI
- เลขลำดับเอกสารของแฟ้มเอกสาร (Archive) "Functional Acknowledgement" ของผู้ให้บริการ EDI
- ชุดของรหัสตรวจสอบ (Check Flag) ของ "Hash total" และขนาดของข้อมูลที่ใช้ยืนยันความถูกต้องของชุดรายการข้อมูลที่ได้รับโดยบริษัท กขค

ข. เอกสารของผู้ให้บริการ EDI (Carrier's Record)

ผู้ให้บริการ EDI (Carrier) ควรจะปกป้องประโยชน์ของตนเองที่เกี่ยวกับเอกสาร ผู้ให้บริการ EDI จะสนใจในการกระจายความรับผิดชอบ (Attributing Responsibility) สำหรับความผิดพลาดของบุคคลอื่นๆ อาจมีหน้าที่ตามสัญญาในส่วนที่เกี่ยวกับ "ผู้เก็บรักษาข้อมูลได้รับความไว้วางใจ" (Trusted Recordkeeper) (19) โดยปกติแล้วหน้าที่ในการเก็บรักษาข้อมูลจะกำหนดไว้ในข้อตกลงการให้บริการเครือข่าย (Network Agreement) (20) ผู้ให้บริการ EDI จะเป็นผู้เก็บแฟ้มข้อมูล (Archivist) และเอกสารที่จัดเก็บจะต้องเป็นไปตามข้อกำหนดที่ทุกฝ่ายหรือแม้แต่บุคคลภายนอกยอมรับ (21)

1. "Incoming Transaction Log" ของผู้ให้บริการ EDI (Carrier)

ใน Transaction Log ที่เข้ามา (Incoming) จะบันทึกข้อมูลที่เกี่ยวข้องกับรายการข้อมูล EDI ที่ได้รับจากลูกค้า ผู้ให้บริการ EDI (Carrier) จะเป็นคนกลาง (Middleman) ที่สำคัญ และมีหน้าที่เทียบได้กับการเป็นผู้ส่งและผู้รับ (Addressee) รายการข้อมูล เอกสาร EDI ควรที่จะแสดงว่าข้อมูลได้รับ จัดเก็บ และส่งต่ออย่างเหมาะสม และสามารถติดตามรายการข้อมูลใดๆ ทั้งกับผู้รับและผู้ส่ง โดยที่ผู้บริการ EDI จะต้องบันทึกข้อมูลดังต่อไปนี้

- รหัสของผู้ส่งรายการข้อมูล
- รหัสของผู้รับรายการข้อมูล (Addressee)
- โปรโตคอล EDI ตามที่รายการข้อมูลที่ได้รับถูกฟอร์แมต (22)
- ขนาดของชุดรายการข้อมูล (ไบต์)
- เลขลำดับเอกสาร (Serial Number) ของผู้ส่งและผู้ให้บริการ EDI สำหรับชุดรายการข้อมูล
- วันและเวลาที่ผู้ส่งยืนยันว่าผู้ให้บริการ EDI ได้รับการส่งผ่านรายการข้อมูลที่ต้องการ

2. “Administrative File” ของผู้ให้บริการ EDI สำหรับชุดรายการข้อมูล

Administrative File นั้นมีวัตถุประสงค์ในการใช้เปิดเผยว่าผู้ให้บริการ EDI ได้ควบคุมดูแลรายการข้อมูลอย่างไร โดยที่แฟ้มข้อมูลดังกล่าวจะบันทึกข้อมูลต่างๆ ที่เกี่ยวกับการรับ การประมวลผล และการส่งรายการข้อมูล แฟ้มข้อมูลของผู้ให้บริการ EDI จะประกอบไปด้วย

- สถานที่ที่ “Incoming Transaction Log” บันทึกชุดรายการข้อมูล
- วันและเวลาที่ชุดรายการข้อมูลถูกได้รับอย่างถูกต้องจากผู้ส่ง
- รหัส (Identity) ของผู้ส่งชุดรายการข้อมูล

- รหัสของผู้รับชุดรายการข้อมูล
- โปรโตคอล EDI ตามที่ชุดรายการข้อมูลที่ได้รับ
- โปรโตคอล EDI ตามที่ชุดรายการข้อมูลถูกส่งไป
- ตัวบ่งชี้ (Flag) ว่ารายการข้อมูลได้ผ่านการตรวจสอบไวรัสคอมพิวเตอร์และข้อมูลที่ไม่สมบูรณ์ (Garbled Data) เมื่อได้รับจากผู้ส่ง
- เลขลำดับเอกสารตามให้ผู้ให้บริการ EDI (Carrier) ได้จัดชุดรายการข้อมูลเข้าเอกสาร (Archive)
- การยืนยันว่าผู้รับ (Addressee) ได้ทำธุรกิจกับผู้ส่งและไม่มี "Special Directives" ที่ไม่เป็นปกติในส่วนที่เกี่ยวกับผู้ส่งหรือประเภทรายการข้อมูล
- หมายเหตุที่แสดงว่ามีวิธีการส่งชุดรายการข้อมูลหลายวิธีที่อาจส่งไปยังผู้รับ (Addressee) (บริษัท กขค)
- บันทึกที่เกี่ยวกับวิธีการ วันและเวลาของความพยายามที่จะทำการส่งและเหตุผลที่ไม่สามารถทำการส่งได้
- ข้อมูลที่เกี่ยวกับวิธีการ วันและเวลาที่สามารถส่งข้อมูลได้สำเร็จ

3. เอกสาร "Functional Acknowledgment"

เอกสาร "Functional Acknowledgement" จะเป็นเอกสารที่เป็นรูปแบบ (Uniform) ค่อนข้างมาก แต่จะเป็นประเภทรายการข้อมูลที่ค่อนข้างธรรมดา วัตถุประสงค์ที่สำคัญคือจะบอกผู้ส่งข้อมูลว่า "เรา (ผู้รับ) ได้รับการส่งข้อมูลของท่านแล้ว" โดยปกติแล้วโปรโตคอล EDI และมาตรฐานทั้งหมดจะไม่อนุญาตให้ตอบไปยัง "Functional Acknowledgement"

ผู้ให้บริการ EDI จะเก็บสำเนาแฟ้มเอกสาร "Functional Acknowledgement" กระบวนการในการสร้าง "Functional Acknowledgement" สามารถทำโดยอัตโนมัติ และอาจมีความสำคัญในแง่ของการใช้เป็นพยานหลักฐานสำหรับข้อมูลต้นฉบับของผู้ส่งหรือข้อมูลต้นฉบับของผู้รับ

ค. เอกสารของผู้รับ (Addressee's Record)

ผู้รับชุดรายการข้อมูล EDI ควรจะกำหนดเอกสารให้มีความเพียงพอต่อการสนับสนุนและปกป้องผลประโยชน์ของตนเอง อาจมีหน้าที่อื่นๆที่กำหนดไว้ตามสัญญาตามข้อตกลงการใช้การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic Data Interchange Agreement) หรือข้อตกลงการให้บริการเครือข่าย (Network Agreement)

1. "Incoming Transaction Log" ของผู้รับข้อมูล

วัตถุประสงค์หลักของ "Incoming Transaction Log" คือรับ ยืนยันและแจกจ่ายรายการข้อมูล EDI ที่ส่งโดยบุคคลอื่น เช่น Incoming Transaction Log ของบริษัท กขค จะประกอบไปด้วย

- วันและเวลาที่ชุดรายการข้อมูลได้รับอย่างถูกต้องโดยบริษัท EDIPhone
- เลขลำดับเอกสารของชุดรายการข้อมูลของผู้ส่ง (บริษัท ABC) แฟ้มเอกสารของผู้ให้บริการ (Carrier Archive) ซึ่งในที่นี้คือ EDIPhone และผู้รับ (Addressee) ในที่นี้คือบริษัท กขค
- รหัส (Identification) แสดงรายการข้อมูลของผู้ส่ง
- โปรโตคอล EDI ที่ชุดรายการข้อมูลได้รับ
- ประเภทของรายการข้อมูลในชุดรายการข้อมูล
- ขนาดของชุดรายการข้อมูล (ไบต์)

- ตัวบ่งชี้ (Flag) แสดงว่าชุดรายการข้อมูลได้ผ่านการตรวจสอบ (Filter) ไวรัสคอมพิวเตอร์ หรือ ข้อมูลที่ไม่สมบูรณ์ (Garbled Data)

- รหัส (Identity) ของผู้รับชุดรายการข้อมูลเฉพาะ (Addressee) ภายในบริษัท กขค
- วันและเวลาที่ชุดรายการข้อมูลต้นฉบับถูกส่งไปยังผู้ให้บริการ EDI (EDIPhone) และ
- ข้อสังเกตว่าเมื่อไรที่ Functional Acknowledgement เกี่ยวกับรายการข้อมูลถูกส่งไป

2. "Incoming Transaction Archive" ของผู้รับ (Addressee)

รายการข้อมูล EDI ที่เข้ามาทั้งหมดควรจะถูกจัดเข้าแฟ้มข้อมูลภายในในรูปแบบเช่นเดียวกับที่ได้รับมา ซึ่งจะช่วยระบุปัญหาในการประมวลผลภายใน ในเบื้องต้น เอกสารของผู้รับควรมีรายการดังต่อไปนี้

- วันและเวลาที่มีการยืนยันการรับรายการข้อมูลอย่างถูกต้องจากผู้ให้บริการข้อมูล
- ขนาดของชุดรายการข้อมูล (ไบต์)
- เลขลำดับเอกสารของผู้รับ (บริษัท กขค) ตามแฟ้มรายการข้อมูลที่จัดเก็บ
- รหัส (Identity) ของผู้ให้บริการ (Carrier) ที่นำส่งรายการข้อมูล
- ตัวบ่งชี้ (Flag) ที่แสดงว่าข้อมูลในรายการข้อมูลได้ผ่านการตรวจสอบไวรัสคอมพิวเตอร์และข้อมูลที่ไม่สมบูรณ์แล้วหรือไม่ และ
- ลำเนารายการข้อมูลที่ได้รับ

3. "System Monitor Log" ของผู้รับ (Addressee)

System Monitor Log ของผู้รับจะทำการมิลเลอร์ฟังก์ชัน System Monitor Log ของผู้ส่ง โดยจะสามารถติดตาม (Trace) การดำเนินงานภายในของรายการเอกสาร ในเบื้องต้น System Monitor Log ของผู้รับจะประกอบไปด้วยรายการดังต่อไปนี้

- รายการการดำเนินการพิเศษและสัญญาณการประมวลผลที่เกี่ยวกับชุดรายการข้อมูล
- วันที่และเวลาที่รายการข้อมูลมีขึ้นสำหรับส่งครั้งสุดท้ายภายในบริษัท กษค (ผู้รับ)
- ข้อมูลที่เกี่ยวกับเส้นทางการส่งข้อมูลภายใน (Internal Routing Information) จากหน่วยเก็บรายการข้อมูลที่เข้ามาชั่วคราวไปยังผู้รับที่มีหน้าที่
- วันและเวลาที่ผู้รับดำเนินการหลังจากที่ได้เปิดรายการข้อมูลดูแล้ว
- ผู้ที่เปิดรายการข้อมูล
- Workstation ที่ใช้เปิดรายการข้อมูล
- ซอฟต์แวร์ที่ใช้เปิดรายการข้อมูล
- ตัวบ่งชี้ (Flag) ที่แสดงว่าผู้จัดการได้เปิดชุดรายการข้อมูลมีอำนาจที่จะทำการเปิดข้อมูลดังกล่าว
- เลขลำดับสำเนาเอกสารที่จัดเก็บของข้อมูล EDI ที่ทำสำเนาใหม่ (Reconstituted EDI) และ
- การอ้างอิงข้ามระบบ (Cross-reference) (โดยปกติจะใช้เลขลำดับเอกสาร) ของบันทึก (Memoranda) ที่ทำขึ้นเพื่ออ้างอิงถึงการเปิดชุดรายการข้อมูล

ง. ประโยชน์ของการเก็บข้อมูลสำรอง (Utility of Redundant Recordkeeping)

การทำสำเนาเอกสารเพื่อสำรองไว้อาจดูว่าเป็นการไม่ประหยัดต้นทุน อย่างไรก็ตามการคิดดังกล่าวนี้ถือเป็นความคิดที่ค่อนข้างแคบและอาจทำให้เกิดความผิดพลาดได้ซึ่งถือเป็นความเสี่ยงของการทำธุรกิจที่สำคัญ อย่างไรก็ตามการจัดการกับความเสี่ยงและการลดต้นทุนเป็นดุลยพินิจในทางธุรกิจ

เอกสารที่ทำสำเนาควรที่จะต้องเก็บรักษาไว้ด้วยเหตุผลหลายประการ ประการแรกคือผู้ที่เก็บรักษาแต่ละฝ่ายต่างมีวัตถุประสงค์และมูลเหตุจูงใจที่แตกต่างกัน และเมื่อผลประโยชน์มีการขัดกันแต่ละฝ่ายจะต้องสามารถใช้เอกสารในการปกป้องผลประโยชน์ของตนเองได้ นี่คือน้ำหนักของเอกสารที่ทำสำเนาไว้ โดยทั่วไปแล้วเอกสารที่ทำสำเนาเก็บไว้ของแต่ละฝ่ายควรมีความสมบูรณ์และเพียงพอตามวัตถุประสงค์ที่คาดไว้

ประการที่สอง ต้นทุนในการจัดเก็บเอกสารโดยระบบคอมพิวเตอร์มีราคาค่อนข้างต่ำ ต้นทุนที่เก็บโดยแผ่นแม่เหล็ก (Magnetic Media) นั้นมีราคาที่ต่ำกว่าการเก็บสำเนาเอกสารไว้ในรูปของกระดาษ ยิ่งกว่านั้นการค้นและการเลือกใช้เอกสารคอมพิวเตอร์มีความสะดวกและรวดเร็วกว่าการเก็บในรูปของกระดาษ Microfiche หรือเทคโนโลยีการเก็บข้อมูลแบบอื่นก็ตาม

ประการที่สาม การทำสำเนาเอกสารเก็บไว้จะช่วยให้ข้อมูลไม่สูญหายเมื่อเอกสารที่ใช้อยู่ถูกทำลายในกรณีที่มีอุบัติเหตุ และสามารถสร้างใหม่ได้อย่างทันที่

บทที่ 3

ความสัมพันธ์ระหว่างกฎหมายและ เทคโนโลยีสารสนเทศ

1. ความสัมพันธ์ระหว่างกฎหมายและสังคม

หลายคนมักกล่าวว่า “กฎหมายนั้นเป็นสิ่งที่มีชีวิต” กล่าวคือกฎหมายนั้นมีพัฒนาการที่สอดคล้องกับความเปลี่ยนแปลงของชีวิตในสังคมอยู่เสมอ กฎหมายและสังคมจึงไม่อาจแยกออกจากกันได้ดังภาษิตกฎหมายที่ว่า “Ubi Societas Ibi Jus” (ที่ใดมีสังคมที่นั่นมีกฎหมาย) ตัวอย่างที่เห็นได้อย่างเด่นชัดในพัฒนาการของกฎหมายที่มีความสอดคล้องกับความเปลี่ยนแปลงทางสังคมคือพัฒนาการของหลักในเรื่องเสรีภาพในการทำสัญญา ซึ่งจะกล่าวในรายละเอียดต่อ

ในอดีตเดิมสัญญาถือเป็นเรื่องของความสัมพันธ์เกี่ยวกับสิทธิและหน้าที่ ไม่ได้มีการเน้นถึงอิสระในการแสดงเจตนามากนัก โดยเฉพาะในสมัยกลาง (Middle Age) ที่มีรากฐานทางความคิดในเรื่องความสัมพันธ์ทางเศรษฐกิจและสังคมอยู่บนพื้นฐานดังต่อไปนี้ 1. ความสัมพันธ์ของคนโดยทั่วไปในสังคมมักถูกกำหนดโดยจารีตประเพณี 2. แนวความคิดทางเศรษฐกิจและศาสนามีความเกี่ยวเนื่องกันอย่างใกล้ชิดโดยถือว่ามนุษย์มิได้เป็นเจ้าของที่ดิน หากแต่เป็นเพียงผู้ถือครองเท่านั้น และ 3. การใช้เสรีภาพของมนุษย์จะต้องมีความสอดคล้องกับหน้าที่ในฐานะที่มนุษย์เป็นสาวกของพระเจ้าผู้เป็นเจ้าของ

ในสมัยนี้เชื่อว่ามนุษย์ต้องการทรัพย์สินและเสรีภาพที่เกี่ยวข้องกับทรัพย์สินไม่ใช่เพราะตัวของเขาเอง แต่เพื่อครอบครัวเพื่อตั้งรกรากบนที่ดินของเขาเอง

ต่อมาในศตวรรษที่ 18 ความมั่งคั่งของมนุษย์เนื่องจากมีทรัพย์สินอยู่ในความครอบครองมากขึ้นโดยเฉพาะที่ดิน ส่งผลให้กฎหมายว่าด้วยเรื่องทรัพย์สินได้รับการพัฒนาและมีส่วนสนับสนุนให้กฎหมายว่าด้วยสัญญาได้รับการพัฒนาด้วยเช่นกัน กระบวนการการเปลี่ยนแปลงดังกล่าวเกิดขึ้นอย่างค่อยเป็นค่อยไป ดัง

เห็นได้จากในศตวรรษที่ 18 คดีต่างๆ ที่เกี่ยวกับกฎหมายว่าด้วยสัญญาจะเป็นสัญญาที่เกี่ยวกับที่ดินแทบทั้งสิ้น ในความคิดเห็นของ Blackstone ใน Blackstone's Commentaries ก็ได้กล่าวไว้อย่างชัดเจนว่า กฎหมายว่าด้วยสัญญามีบทบาทอย่างมากเกี่ยวเนื่องกับกฎหมายเรื่องทรัพย์สิน เขาเห็นว่า สัญญาเป็นวิธีหนึ่งที่จะได้มาซึ่งกรรมสิทธิในทรัพย์สิน

เช่นเดียวกับที่ John Joseph Powell ในปี 1790 ได้เขียนหนังสือเรื่อง Essay upon the Law of Contract and Agreement ก็ยืนยันเช่นเดียวกันว่า "สัญญานั้นมีส่วนเกี่ยวข้องกับการทำธุรกิจ และกฎหมายสัญญาที่เกิดขึ้นเป็นผลสืบเนื่องมาจากการพัฒนาความคิดในเรื่องทรัพย์สิน"

ในทางหนึ่ง การเปลี่ยนแปลงจากกฎหมายว่าด้วยเรื่องทรัพย์สินไปยังกฎหมายว่าด้วยสัญญาที่เกี่ยวข้องกับทรัพย์สินจะแสดงได้จากความสำคัญของทรัพย์สินที่เปลี่ยนจากคุณค่าในการใช้ (Use Value) ไปเป็นคุณค่าในการแลกเปลี่ยน (Exchange Value) ความเปลี่ยนแปลงดังกล่าวนี้สอดคล้องกับแนวความคิดเศรษฐกิจแบบทุนนิยม (Capitalist Economy) และแนวความคิดเสรีประชาธิปไตยในศตวรรษที่ 19

ในยุคนี้หลักเสรีภาพในการทำสัญญาจึงได้รับการพัฒนาจนถึงจุดสูงสุด ดังจะเห็นได้ว่าหลักที่ว่า "สัญญาต้องเป็นสัญญา" (Pacta sunt servanda) มีใช้กันอย่างแพร่หลายทั้งกฎหมายภายในและกฎหมายระหว่างประเทศ

แต่อย่างไรก็ดีคงเห็นได้ว่าในปัจจุบันคงเห็นได้ว่าหลักเสรีภาพในการทำสัญญา มักถูกจำกัดโดยหลักในเรื่องของการคุ้มครองผู้บริโภค (Consumer Protection) ดังเห็นได้จากบทบัญญัติกฎหมายที่เกี่ยวข้องกับเรื่องข้อสัญญาไม่เป็นธรรมหรือเรื่องของการคุ้มครองผู้บริโภคเป็นต้น ในยุคนี้ความสำคัญของหลักเสรีภาพในการทำสัญญาจึงถูกลดบทบาทโดยหลักกฎหมายอื่นที่เกิดขึ้นจากความจำเป็นของสังคม (Social Necessity)¹³

¹³ Atiya, Patrick Selim, The Rise and Fall of Freedom of Contract, Oxford University Press, 1979

จากที่กล่าวมาจึงเห็นได้ว่ากฎหมายโดยเฉพาะอย่างยิ่ง ในเรื่องหลักเสรีภาพในการทำสัญญานั้น มีพัฒนาการปรับเปลี่ยนให้มีความสอดคล้องกับสภาพการณ์และความจำเป็นของสังคมที่เปลี่ยนไปเสมอ

2. สังคมแห่งสารสนเทศ (Information Society)

ในปี 1992 ธนาคารโลกได้รายงานว่าเงินประมาณ 11-12 พันล้านล้านเหรียญสหรัฐ ตามมูลค่าของหุ้นกู้ (Bonds) ในแต่ละปีที่ส่งให้กับประเทศกำลังพัฒนา¹⁴ ครึ่งหนึ่งทำในรูปของอิเล็กทรอนิกส์ เพื่อที่จะให้เกิดความมั่นคงในการทำธุรกรรมที่เกี่ยวกับการเงินดังกล่าวแต่ละประเทศควรที่จะพัฒนากฎหมายของตนให้สามารถใช้บังคับได้

ปรากฏการณ์ดังกล่าวเป็นผลจากความก้าวหน้าของเทคโนโลยีดิจิทัล ซึ่งคำว่า "ดิจิทัล" นั้นมาจากภาษาละตินที่ว่า "Digitus" ที่แปลว่านิ้วมือ ซึ่งเป็นการอ้างถึงหนึ่งในเครื่องมือที่เก่าแก่ที่สุดของมนุษย์ในการคำนวณ เมื่อข้อมูลถูกเก็บรักษา ส่งผ่านหรือส่งต่อไปในรูปแบบของดิจิทัล ข้อมูลดังกล่าวจะถูกเปลี่ยนเป็นตัวเลข 0 และ 1 การเปลี่ยนแปลงข้อมูลดังกล่าวสามารถทำได้อย่างรวดเร็วมาก โพรเซสเซอร์สามารถคำนวณได้ถึง 1 พันล้านล้านครั้งในหนึ่งวินาที ซึ่งก็สามารถอธิบายได้ว่าทำไมหนังสือ เพลง ภาพเคลื่อนไหว หรือการให้บริการบางประเภทสามารถเกิดขึ้นได้บนเครือข่ายอินเทอร์เน็ต ที่ทุกคนสามารถใช้บริการได้พร้อมกันทุกเวลาและทุกสถานที่ (Anywhere and Anytime)

การติดต่อระหว่างคอมพิวเตอร์และคอมพิวเตอร์ไม่เพียงแต่จะสามารถทดแทนการใช้กระดาษได้ แต่ยังช่วย Reorganization การทำงานภายในบริษัทรวมทั้งยังช่วยปรับปรุงความสัมพันธ์ระหว่างคู่ค้าอีกด้วย

ในกรณีของแนวความคิดเรื่อง Just-in-time (JIT) คอมพิวเตอร์ของผู้ผลิตอาจวางแผนให้สามารถตรวจดูรายการสินค้าที่มีความจำเป็นในระหว่างกระบวนการผลิตและจะทำการออกคำสั่งซื้อทางอิเล็กทรอนิกส์เมื่อรายการสินค้าลดลงในระดับที่กำหนดไว้ คำสั่งซื้อสินค้าทางอิเล็กทรอนิกส์นี้จะถูกส่งไป

¹⁴ World Bank Reports Profit in Fiscal, July 30, 1992

ยังชีพพลายเออร์ทางอิเล็กทรอนิกส์ ซึ่งเครื่องคอมพิวเตอร์ของชีพพลายเออร์ก็จะส่งคำสั่งในการส่งของ (Shipping Order) ไปยังคลังสินค้าของชีพพลายเออร์ โดยไม่มีความจำเป็นที่จะต้องใช้คนในการควบคุมดูแล (Monitor) หรืออนุมัติธุรกรรมดังกล่าว สัญญาถูกทำขึ้นและใช้โดยเครื่องคอมพิวเตอร์ นอกจากนั้นยังมีบางกรณีที่เรียกว่า "Quick Response"¹⁵ ที่คอมพิวเตอร์ของชีพพลายเออร์สามารถวางแผนโปรแกรมให้สามารถตรวจสอบรายการสินค้า (Inventory) ของลูกค้าและสามารถทำคำสั่งส่งสินค้าทางอิเล็กทรอนิกส์ (Electronic Shipping Order) เพื่อทำการส่งสินค้าได้อย่างทันทีเมื่อรายการสินค้าลดลงตามปริมาณที่กำหนดไว้ จะเห็นได้ว่าไม่มีการเจรจาทำสัญญาซื้อขายสินค้าแต่อย่างใด จริงๆแล้วในหลายกรณีเส้นแบ่งระหว่างระบบคอมพิวเตอร์ของชีพพลายเออร์และของลูกค้าจะไม่มีมีความเกี่ยวข้องกับการดำเนินงานของลูกค้าและชีพพลายเออร์เมื่อมีการรวมตัวกันทางอิเล็กทรอนิกส์ ดังนั้นการนำมาซึ่งเทคโนโลยีการสื่อสารทางอิเล็กทรอนิกส์ในการทำธุรกรรมทางการค้าส่งผลให้เกิดการเปลี่ยนแปลงอย่างมากในกระบวนการทำธุรกิจของบริษัท และอาจก่อให้เกิดคำถามทางปัญหาข้อกฎหมายในการวิเคราะห์การเกิดและลักษณะการบังคับใช้ธุรกรรมทางการค้า

การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI) จึงหมายถึงการติดต่อระหว่างเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์เพื่อแลกเปลี่ยนข้อมูลตามรูปแบบ (Format)¹⁶ ที่กำหนดไว้เพื่อใช้ในธุรกรรมรายวันภายในประเทศหรือระหว่างประเทศ และเป็นที่ยอมรับกันอย่างแพร่หลายในวงการอุตสาหกรรมต่างๆ ตัวอย่างเช่น อุตสาหกรรมรถยนต์ของสหรัฐฯ ประกาศว่าจะไม่ทำธุรกิจกับบริษัทที่ไม่ใช้ EDI¹⁷

การนำเอาเทคโนโลยีคอมพิวเตอร์มาใช้นั้นอาจส่งผลดีในแง่ของช่วยลดกระบวนการผลิตและต้นทุนทางด้านการตลาดแต่อย่างไรก็ดีประโยชน์ดังกล่าวจำเป็นต้องนำมาซึ่งน้ำหนักกับต้นทุนทางด้านความปลอดภัยของระบบข้อมูลที่น่ามาใช้

¹⁵ Electronic Messaging Services Taskforce, The Commercial Use of Electronic Data Interchange- A Report and Model Trading Partner Agreement, 45 Bus. Law. 1645, 1649 (1989)

¹⁶ TEDIS Final Report, The Legal Position of the Member States with Respect to Electronic Data Interchange, (Comm'n of the European Communities, Brussels, Belg.), Sept. 1989, pp. 27-28

¹⁷ โปรดดู Magaret A. Emmelhainz, Electronic Data Interchange: A Total Management Guide 53 (1990)

การเติบโตของการใช้เทคโนโลยีอิเล็กทรอนิกส์ในทางการค้าจะเป็นสิ่งหนึ่งที่สะท้อนการเกิดขึ้นของ “เศรษฐกิจที่อยู่บนพื้นฐานของข้อมูลข่าวสาร” (Information Technology) ธุรกิจที่สามารถขยายตลาดและลดต้นทุนในการผลิตโดยการนำเอาเทคโนโลยีสารสนเทศมาใช้จะทำให้ธุรกิจนั้นสามารถก้าวเข้าสู่ยุคแห่งข้อมูลข่าวสารได้อย่างมั่นคง

อย่างไรก็ดีเทคโนโลยีใหม่จะให้ประโยชน์ก็ต่อเมื่อธุรกิจสามารถเชื่อมั่นได้อย่างมีประสิทธิภาพความปลอดภัยของระบบการสื่อสารทางธุรกิจอาจทำให้ต้องเพิ่มค่าใช้จ่ายแต่ก็สามารถช่วยให้ลดความเสี่ยงที่เกิดขึ้นจากเรื่องดังกล่าวได้ เรื่องดังกล่าวเป็นความจริงไม่ว่าระบบการสื่อสารจะอยู่บนพื้นฐานของกระดาษ เครื่องโทรสาร เทเล็กซ์ หรือ E-mail ตัวอย่างเช่น ผู้กระทำความผิดได้ส่งเทเล็กซ์ปลอมไปที่ธนาคาร Chase Manhattan ที่กรุงลอนดอน เพื่อขอให้โอนเงิน 13.5 ล้านดอลลาร์ของกองทุนรัฐบาลโคลอมเบีย เทเล็กซ์ได้ตรวจสอบกลับ (answerback) ไปยังธนาคารกลางของโคลอมเบียแต่ไม่ได้ทำการเข้ารหัสข้อมูลดังกล่าว และธนาคาร Chase Manhattan ก็ไม่ได้ใช้การเข้ารหัสดังกล่าว แม้ว่าตามหลักแล้วควรจะต้องใช้ ก็ตาม ผู้กระทำความผิดก็สามารถได้เงินไปเนื่องจากไม่มีระบบรักษาความปลอดภัย จากหลักฐานในการสอบสวนพบว่า กลไกในการรักษาความปลอดภัยที่เรียกว่า Answerback สามารถปลอมได้¹⁸ หากธนาคารยอมลงทุนในการติดตั้งกลไกในการรักษาความปลอดภัยที่เหมาะสม เหตุการณ์ดังกล่าวคงไม่เกิดขึ้น

เหตุการณ์เช่นเดียวกันเกิดขึ้นกับ บริษัทสวิสในการขายสินค้าให้กับบริษัทเนเธอร์แลนด์ โดยใช้เบงค์การันตีเป็นหลักฐานซึ่งเบงค์การันตีดังกล่าวส่งผ่านโดยเทเล็กซ์ที่ไม่ได้รับการตรวจสอบ (untested telex) เมื่อบริษัทสวิสพยายามที่เรียกเก็บเงินตามเบงค์การันตี ธนาคารปฏิเสธที่จะชำระเงินตามเทเล็กซ์ ผู้เชี่ยวชาญได้สอบสวนแล้วพบว่ากระบวนการรับเทเล็กซ์ไม่มีกลไกในการตรวจสอบว่าใครเป็นผู้ส่ง ศาลจึงสรุปว่า ตามหลักฐานที่ปรากฏไม่น่าจะถือว่าธนาคารได้เป็นผู้ออกเทเล็กซ์ดังกล่าว¹⁹

¹⁸ Prudent Banking Practice Meets the Forged Telex, Int'l Fin. L. Rev. 24-25 (Dec. 1987)

¹⁹ van Dort, Netherlands: Bank Guarantee by Telex, 14 Int'l Bus. Law. 173 (June 1986)

จากเหตุการณ์ทั้งสองเรื่องดังกล่าวมานี้แสดงให้เห็นว่าไม่ใช่ว่าเทคโนโลยีจะไม่จำเป็นสำหรับการทำธุรกรรม แต่ในขณะที่ธุรกรรมมีมูลค่าสูงขึ้นและใช้เทคโนโลยีแพร่หลายมากขึ้นกระบวนการรักษาความปลอดภัยยิ่งมีความจำเป็นมากขึ้นเช่นกัน²⁰

ความมีประสิทธิภาพที่ทำให้ความเสี่ยงทางกฎหมายถูกมองข้ามในทางปฏิบัติ

ธุรกรรมทางการค้าใดๆ ล้วนแต่มีความเสี่ยงเกิดขึ้นไม่มากก็น้อย อย่างไรก็ตามความเสี่ยงที่เกิดขึ้นควรที่จะเป็นความเสี่ยงที่สามารถคาดการณ์ได้ ระดับของการคาดการณ์ได้นั้นเป็นเรื่องที่มีความสำคัญกับกฎหมายทางการค้าเพื่อที่จะให้คู่สัญญาสามารถคาดการณ์ถึงผลของความเสี่ยงที่เกี่ยวข้องกับการทำธุรกรรมได้ อย่างไรก็ตามกฎหมายไม่สามารถทำให้เกิดความแน่นอนอย่างสมบูรณ์ในการประเมินความเสี่ยงที่เกิดจากความรับผิดที่อาจเกิดในการปฏิบัติตามข้อกำหนดของสัญญา ในขณะที่กฎหมายพาณิชย์อิเล็กทรอนิกส์อาจไม่มีความชัดเจนในบางเรื่อง ความไม่แน่นอนเหล่านี้ไม่ได้เป็นเรื่องเดียวกับพาณิชย์อิเล็กทรอนิกส์ แต่เกิดขึ้นจากองค์ประกอบของความเสี่ยงทางธุรกิจที่จะต้องทำการวิเคราะห์ไปพร้อมกับความเสี่ยงอื่นๆ ที่อาจเกิดขึ้นได้

ตัวอย่างเช่น United Parcel Service (UPS) ได้ติดตั้งอุปกรณ์คอมพิวเตอร์มือถือให้กับพนักงานส่งเอกสารของบริษัท เพื่อให้สามารถบันทึกข้อมูลจากหีบห่อที่รับส่ง โดยข้อมูลดิจิทัลดังกล่าวจะถูกเก็บรวบรวมไว้ที่เครื่องคอมพิวเตอร์เมนเฟรมส่วนกลาง ที่ผ่านมา UPS จะได้รับหลักฐานการส่งมอบโดยบอกให้ผู้รับลงนามในใบรับของ เหตุผลสำหรับการที่ UPS เปลี่ยนจากระบบกระดาษมาใช้ระบบเอกสารดิจิทัลก็เนื่องจากลดต้นทุนในการจัดเก็บเอกสารและการเรียกเอกสารมาตรวจสอบ

ก่อนที่ UPS จะใช้ระบบใหม่ ทาง UPS ได้ทำการวิจัยและวิเคราะห์ผลทางกฎหมาย โดยทาง UPS ได้ระบุว่าระบบใหม่ได้ติดตั้งเครื่องควบคุมจำนวนเพื่อให้ความมั่นใจว่าเอกสารที่จัดเก็บจะมีความน่าเชื่อถือ เครื่องควบคุมดังกล่าวซึ่งได้รับการออกแบบและทดสอบมาอย่างดี มีการฝึกอบรมการใช้อุปกรณ์ดังกล่าว และวางระบบป้องกันผู้ที่ไม่ได้รับอนุญาตในการเข้าถึงข้อมูลดังกล่าว ในงานวิจัยดังกล่าวยังได้ระบุว่าภาครัฐก็กำลังอนุญาตให้สามารถใช้เอกสารทางอิเล็กทรอนิกส์แทนเอกสารที่เป็นกระดาษได้

²⁰ Telex Contracts-A Comparative Study, Int'l Fin. L. Rev. 22-29 (May 1982)

อย่างไรก็ดี เนื่องจาความใหม่ของระบบดังกล่าว UPS จึงยากที่จะคาดเดาได้ว่าศาลจะยอมรับฟังเอกสารดิจิทัลหรือไม่ แต่อย่างไรก็ดีลายมือชื่อแบบเดิมก็มักจะถูกลบปลอมแปลง และศาลก็มักจะไม่นับฟังเอกสารที่ปลอมดังกล่าว ดังนั้นทาง UPS จึงสรุปว่าแม้ว่าการเปลี่ยนจากการบันทึกแบบใช้กระดาษมาเป็นการบันทึกโดยใช้ระบบดิจิทัลจะก่อให้เกิดความเสี่ยงทางกฎหมาย แม้ว่าจะมีความเสี่ยงทางกฎหมายก็ตามแต่ก็ยังไม่มากเท่าความเสี่ยงที่เกิดจากการใช้กระดาษในรูปแบบเดิม UPS จึงตัดสินใจว่าเพื่อเหตุผลทางธุรกิจถือว่าคุ้มค่าที่จะเปลี่ยนแปลงดังกล่าว²¹

จากที่กล่าวมาจะเห็นได้ว่าวงการธุรกิจนั้นมีทางปฏิบัติของตนเองที่มักจะคำนึงถึงประสิทธิภาพเป็นเบื้องต้น แม้ว่าจะมีความเสี่ยงทางกฎหมายจากการนำเอาเทคโนโลยีมาใช้ก็ตาม ซึ่งเป็นสัญญาณที่แสดงให้เห็นว่าตัวบทกฎหมายที่มีอยู่เริ่มที่จะมีความไม่สอดคล้องกับความจำเป็นหรือความต้องการของสังคมแล้ว

3. ผลของความก้าวหน้าของเทคโนโลยีสารสนเทศต่อความเปลี่ยนแปลงของกฎหมาย

Prof Negroponte แห่ง MIT's MediaLab ได้เคยกล่าวไว้ในหนังสือ Being Digital (1995) ในเรื่องของการพัฒนาจากระบบอนาล็อกไปสู่ระบบดิจิทัลว่า "อะตอม ได้ถูกแทนที่โดยบิต" ซึ่งมีนัยมากมายจากการเปลี่ยนแปลงดังกล่าว

เมื่อวัตถุที่จับต้องได้กลายเป็นวัตถุที่ไม่สามารถจับต้องได้ มิใช่จะส่งผลเปลี่ยนแปลงถึงแนวความคิดทางเศรษฐศาสตร์ รัฐศาสตร์ หรือสังคมศาสตร์อื่นๆเพียงเท่านั้น หากแต่ยังส่งผลกระทบต่อนิติศาสตร์ด้วยเช่นกัน เช่นเกิดปัญหาว่าประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยการซื้อขาย สามารถนำมาปรับใช้กับ "ผลิตภัณฑ์" ในรูปคลื่นแม่เหล็กไฟฟ้าที่สามารถทำสำเนาจากเครื่องคอมพิวเตอร์ของนาย ก ไปยัง

²¹ โปรดดู Benjamin Wright and Jane K. Winn, The Law of Electronic Commerce, Aspen Law & Business, New York, 1997, p. 1-5

เครื่องคอมพิวเตอร์ของนาย ข ปัญหาที่ตามมาคือเมื่อไรจึงจะถือว่า "ผลิตภัณฑ์" ดังกล่าวได้ถูกส่งมอบแล้ว เป็นต้น

กฎหมายกับการเปลี่ยนแปลงรูปแบบทางความคิด

ตามที่นักปรัชญาที่ชื่อว่า Thomas Kuhn²² อธิบายว่ารูปแบบทางความคิด (Paradigm) จะเป็นรากฐานในการอธิบายปรากฏการณ์ทางวิทยาศาสตร์ รูปแบบทางความคิดใหม่ที่ไม่ถูกต้องและสอดคล้องกับความเป็นจริงอาจก่อให้เกิดแนวความคิดหรือรูปแบบทางทฤษฎีที่ไม่ถูกต้องก็ได้ นักดาราศาสตร์ครั้งหนึ่งเคยใช้รูปแบบทางความคิดที่อยู่บนพื้นฐานว่าโลกเป็นศูนย์กลางของจักรวาล บนรูปแบบทางความคิดดังกล่าวก็จะก่อให้เกิดความคิดหรือทฤษฎีในรายละเอียดที่ไม่ตรงกับความเป็นจริง ต่อมาแนวความคิดเปลี่ยนไป มนุษย์ค้นพบว่าดวงอาทิตย์ต่างหากที่เป็นศูนย์กลางของจักรวาล ความคิดทฤษฎีรวมทั้งมุมมองต่าง ๆ ก็เปลี่ยนไปด้วยเช่นกัน

เช่นเดียวกับกรณีของกฎหมายพาณิชย์ เมื่อสังคมเป็นสังคมสารสนเทศ (Information Society) เศรษฐกิจเป็นเศรษฐกิจที่อยู่บนพื้นฐานของข้อมูลสารสนเทศ (Information Data) รูปแบบทางความคิดที่เดิมเคยอยู่บนทรัพย์สินที่สามารถจับต้องได้ (Tangible object) จุดเน้นได้เปลี่ยนไปเป็นเพิ่มบทบาทและความสำคัญให้กับทรัพย์สินที่จับต้องไม่ได้ (Intangible object) ซึ่งก็คือข้อมูลข่าวสาร (Information) นั่นเอง เมื่อรูปแบบความคิดทางสังคมและเศรษฐกิจเปลี่ยนไป รูปแบบทางความคิดทางกฎหมายก็ต้องเปลี่ยนไปเช่นกัน เกิดกฎหมายเทคโนโลยีสารสนเทศ กฎหมายที่มุ่งแรงโน้มถ่วงไปที่ข้อมูล (Information)²³

นักกฎหมายได้หาวิธีอธิบายว่าทำไม อย่างไร และในสถานการณ์ไหนที่กฎหมายต้องเปลี่ยนแปลง อันเป็นการสนองตอบของการเปลี่ยนแปลงของสังคม กฎหมายแพ่งไม่ได้หล่นลงมาจากสวรรค์ในรูปของ

²² Thomas Kuhn, The Structure of Scientific Revolution 89 (2d ed. 1970)

²³ Michael L. Rustad, "Commercial Law Infrastructure for the Age of Information", Journal of Computer & Information Law, Vol. XV 1997, p. 264

แผ่นหินจารึก²⁴ ประมวลกฎหมายพาณิชย์เป็นผลของทางปฏิบัติและความเปลี่ยนแปลงทางสังคม เนื่องจากสังคมจำเป็นต้องเปลี่ยนแปลง กฎหมายก็จำเป็นต้องเปลี่ยนแปลงเช่นเดียวกัน²⁵

คำว่า "พาณิชย์อิเล็กทรอนิกส์" เป็นคำที่มีความหมายกว้างมากเนื่องจากเป็นคำที่สามารถปรับใช้ได้กับทุกๆ เรื่องในปัจจุบัน โดยทั่วไปแล้วพาณิชย์อิเล็กทรอนิกส์หมายถึงการค้าในทุกประเภทไม่ว่าจะเป็นการค้าระหว่างภาคธุรกิจกับภาคธุรกิจ (Business-to-Business) ภาคธุรกิจกับผู้บริโภค (Business-to-Consumer) ภาคธุรกิจกับหน่วยงานของรัฐ (Business-to-Government) ที่ใช้เทคโนโลยีทางคอมพิวเตอร์หรือทางดิจิทัล โดยไม่คำนึงถึงว่าเทคโนโลยีดังกล่าวจะเป็นสื่อ (Medium) ในการเชื่อมโยงระหว่างคู่สัญญา (การเกิดขึ้นของสัญญา (Formation by computers) หรือเป็นพาหนะ (Vehicle) ทำให้ธุรกรรมนั้นสมบูรณ์ (สัญญาสำหรับข้อมูลดิจิทัล) หรือในฐานะเป็นวัตถุแห่งสัญญา (Object of performance)

ดังที่นักกฎหมายชาวสหรัฐฯ ได้เปรียบเทียบว่ากฎหมายพาณิชย์ของสหรัฐฯ นั้นได้พัฒนามาตั้งแต่สมัยจูราสสิกพาร์คของแนวคำพิพากษาของอเมริกา (Jurassic Park of American jurisprudence)²⁶ โครงสร้างพื้นฐานทางกฎหมายใหม่จำเป็นที่จะต้องได้รับการพัฒนาให้สามารถรองรับความเปลี่ยนแปลงและรูปแบบทางเศรษฐกิจแบบใหม่ของประเทศ

กฎหมายที่เกี่ยวกับสัญญาซื้อขายเดิมนั้นส่วนใหญ่ได้รับการพัฒนาในยุคที่สินค้าที่จับต้องได้มีบทบาทหลักและสำคัญต่อเศรษฐกิจสหรัฐเป็นอย่างมาก ในปัจจุบันบทบาทดังกล่าวได้เปลี่ยนไปแล้ว²⁷ ระบบเศรษฐกิจก็ได้เปลี่ยนจากการพึ่งพาสินค้าที่มีรูปร่างไปสู่สินค้าที่ไม่มีรูปร่าง การสื่อสารผ่านดาวเทียมส่งผล

²⁴ โปรดดู Felix S. Cohen, Transcendental Nonsense and the Functional Approach, 35 Colum. L. Rev. 809 (1935); Oliver Wendell Holmes Jr., The Path of the Law, (1897), reprinted in B.U.L. Rev. 24, 34 (1965)

²⁵ Karl Llewellyn, Some Realism About Realism-Responding to Dean Pound, 44 Harv. L. Rev. 1222-23 (1931)

²⁶ Michael L. Rustad, "Commercial Law Infrastructure for the Age of Information", Journal of Computer & Information Law, Vol. XV 1997, p. 262

²⁷ Michael L. Rustad, "Commercial Law Infrastructure for the Age of Information", Journal of Computer & Information Law, Vol. XV 1997, p. 257

ให้ผู้ให้บริการสามารถส่งข้อมูล เสียง ภาพเคลื่อนไหว เทลิกซ์ แฟกซ์ อีเมล หรือบริการอินเทอร์เน็ตได้อย่างประหยัดและรวดเร็ว²⁸

อุตสาหกรรมสารสนเทศและการพาณิชย์อิเล็กทรอนิกส์มีความสำคัญกับเศรษฐกิจเป็นอย่างมาก เป็นอนาคตของธุรกิจและเป็นอนาคตของประเทศเมื่อเศรษฐกิจเน้นที่ความสำคัญของข้อมูลข่าวสาร กฎหมายก็จำเป็นที่จะต้องปรับให้เข้ากับความเป็นจริงของสังคม

ธุรกรรมที่เกี่ยวกับข้อมูลข่าวสารไม่เหมือนกับธุรกรรมที่เกี่ยวกับสินค้าที่จับต้องได้ สัญญาเพื่อการค้าได้มาของข้อมูลต่างกับสัญญาซื้อขายเครื่องปั้นดินเผา เช่นเดียวกับเศรษฐกิจแห่งข้อมูลข่าวสาร (Information Economy) จะไม่เหมือนกับเศรษฐกิจที่อยู่บนพื้นฐานการผลิตและการค้าขายสินค้า เศรษฐกิจแห่งข้อมูลข่าวสารเอื้อให้เกิดประโยชน์มากมาย ในขณะเดียวกันก็ก่อให้เกิดความเสี่ยงใหม่ๆ และก่อให้เกิดตัวแสดงใหม่ๆ ที่ต่างจากเศรษฐกิจที่อยู่บนพื้นฐานของสินค้า สภาพการณ์ดังกล่าวต้องการแนวความคิดใหม่ของสัญญาด้วยเช่นกัน

ระบบกฎหมายที่สนับสนุนเศรษฐกิจแห่งข้อมูลข่าวสาร (Information Economy) จะต้องเข้าใจความแตกต่างดังกล่าวนี้ ข้อกำหนดของสัญญาโดยเฉพาะอย่างยิ่งข้อกำหนดที่เกี่ยวกับขอบเขตของการให้สิทธิมีความสำคัญอย่างมากในเศรษฐกิจแห่งข้อมูลข่าวสารมากกว่าเศรษฐกิจที่อยู่บนพื้นฐานของสินค้าที่สามารถจับต้องได้

โดยต่อไปนี้จะได้กล่าวถึงองค์ประกอบพื้นฐานสำคัญของกฎหมายที่จำเป็นต้องมีการเปลี่ยนแปลง

3.1 รูปแบบของการมีส่วนร่วมของมนุษย์

หลักกฎหมายพื้นฐานที่สำคัญของกฎหมายสัญญาคืออยู่บนพื้นฐานที่ว่าสัญญาจำต้องทำขึ้นโดยการตัดสินใจของการกระทำของมนุษย์ ทั้งทำในนามของตนเองและในนามของผู้อื่น จากรูปแบบทางความ

²⁸ Richard P. Appelbaum & William J. Chambliss, Sociology, (1997) pp. 433-34

คิดที่มีมนุษย์เข้ามามีส่วนร่วมในการทำสัญญา (Humanistic Model) ซึ่งมีจุดเน้นอยู่ที่ข้อสันนิษฐาน ข้อจำกัดและวิธีการความคิด (Idea) ในการทำสัญญา²⁹

อย่างไรก็ดีจากแนวความคิดตามทฤษฎีกฎหมายกำหนดให้มนุษย์ต้องทำการยอมรับหรือปฏิเสธในการมีนิติสัมพันธ์ซึ่งกันและกัน ซึ่งถือเป็นแนวความคิดที่เป็นรากฐานของกฎหมายสัญญา บุคคลมีสิทธิเลือกที่จะตัดสินใจหรือมีเจตนาอย่างไร ผู้ซื้อสามารถรับคำเสนอ คู่สัญญาอาจมีความผิดพลาดในการแสดงเจตนาตามเงื่อนไขข้อตกลงที่ตนได้เสนอหรือยอมรับไป

สิ่งต่างๆ ที่กล่าวมานี้ถือเป็นเบื้องต้นว่ามนุษย์จะต้องเข้ามาเกี่ยวข้องกับเสมอ

เมื่อคอมพิวเตอร์ถูกนำมาใช้ในการสร้างนิติสัมพันธ์ โดยสามารถแยกออกได้อย่างชัดเจนระหว่าง "เจตนา" และ "การรับรู้" (Knowledge) ของเจ้าของคอมพิวเตอร์³⁰ (ซึ่งจะเป็นผู้ที่จะต้องรับผิดชอบ) ความไม่แน่นอนและปัญหาอาจปรากฏชัดเจนขึ้นกับข้อความคิดทางกฎหมายอย่างเช่นเรื่องของการ "แสดงเจตนา" ในอันที่จะสามารถนำมาปรับใช้กับปรากฏการณ์ใหม่ที่เกิดขึ้นได้ ความยากลำบากอาจเกิดขึ้นในกรณีที่มีข้อผิดพลาดส่งผลให้สิ่งที่คอมพิวเตอร์ "พูด" ไม่ใช่สิ่งเดียวกับที่เจ้าของคอมพิวเตอร์ "ต้องการ" ในกรณีดังกล่าวจะถือได้หรือไม่ว่าคำเสนอหรือคำสนองที่คอมพิวเตอร์ทำขึ้นเป็นคำเสนอหรือคำสนองที่ทำขึ้นโดยตัวแทน (Agent) หรือไม่ จะถือได้หรือไม่ว่าเป็น "การแสดงเจตนา" อย่างแท้จริงของเจ้าของคอมพิวเตอร์หรือไม่ หรือควรที่จะต้องมีหลักเกณฑ์ทางกฎหมายเฉพาะที่เกี่ยวกับการทำนิติกรรมสัญญาทางอิเล็กทรอนิกส์ที่คำนึงถึงประเด็นทางเทคนิคของระบบคอมพิวเตอร์เป็นองค์ประกอบที่สำคัญของกฎหมาย

²⁹ Raymond T. Nimmer, "Electronic Contracting: Legal Issues", Journal of Computer & Information Law, Vol. XIV, 1996, pp. 212-213

³⁰ โปรดดู Mads Bryde Andersen, Electronic Commerce: A Challenge to Private Law?, CENTRO DI STUDI E RICERCHE DI DIRITTO COMPARATO E STRANIERO, Roma, Maggio 1998

องค์ประกอบในเรื่องคนทำให้เกิดปัญหาทางความคิดและทฤษฎีเมื่อนำมาปรับใช้กับเหตุการณ์และข้อเท็จจริงในปัจจุบัน เมื่อคอมพิวเตอร์สองเครื่องสามารถทำสัญญากันได้โดยที่ไม่มีมนุษย์เข้ามาเกี่ยวข้องด้วยเลย กฎหมายเดิม หรือแนวความคิดเดิมเพียงพอหรือไม่กับการนำมาปรับใช้

ตัวอย่างเช่นมาตรา 2B ของประมวลกฎหมายสหรัฐได้กำหนดบทบัญญัติเกี่ยวกับการทำสัญญาทางอิเล็กทรอนิกส์และธุรกรรมทางการค้าที่เกิดจากเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์ “ธุรกรรมทางอิเล็กทรอนิกส์” คือ สัญญาที่มนุษย์อาจไม่ได้ทำการทบทวนข้อมูลที่เกี่ยวข้องกับสัญญา³¹ และ “ตัวแทนทางอิเล็กทรอนิกส์” หมายถึง “โปรแกรมคอมพิวเตอร์ หรือวิธีการอิเล็กทรอนิกส์หรืออัตโนมัติอื่น ๆ ที่ใช้เลือก หรือโปรแกรมโดยคู่สัญญาที่เสนอหรือสนองรับข้อมูลทางอิเล็กทรอนิกส์ หรือการปฏิบัติตามสัญญาทั้งหมดหรือแต่บางส่วน โดยที่มนุษย์ไม่ได้เข้าไปพิจารณาทบทวน”³²

3.2 สื่อที่ใช้ในการแสดงเจตนา

ในกระบวนการค้าระหว่างประเทศ ในแต่ละปีมีความจำเป็นที่ล้านล้านแผ่น กระดาษเหล่านี้คิดเป็นมูลค่าถึง 140 พันล้านเหรียญสหรัฐ แม้ว่ากระดาษจะใช้กันมานานแต่มีราคาแพง ไม่ก่อให้เกิดความคล่องตัวและต้องใช้ที่ในการเก็บมากมาย การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI: Electronic Data Interchange) ส่งผลให้เครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์แลกเปลี่ยนเอกสารต่างได้เช่น คำสั่งซื้อ ในใบเสร็จรับเงิน เป็นต้น นอกจากนั้น EDI ยังใช้ส่งข้อมูลทางการเงินและชำระเงินในรูปแบบทางอิเล็กทรอนิกส์ ผลของ EDI คือใช้แทนเอกสารที่เป็นกระดาษด้วยการส่งข้อมูลทางอิเล็กทรอนิกส์ผ่านวงจรการทำธุรกรรมของบริษัท EDI ก่อให้เกิดการปฏิบัติในวงการธุรกิจ 78% ของ Fortune 1000 companies ปัจจุบันใช้ EDI และอัตราการเจริญเติบโตในการใช้มีสูงถึง 147%³³

³¹ U.C.C. 2B-102(a)(18) (Proposed Draft, Sept. 25, 1997)

³² U.C.C. 2B-102(a)(16) (proposed Draft, Sept. 25, 1997)

³³ Margaret A. Emmelhainz, Electronic Data Interchange: A Total Management Guide 209 (1990), p.210

ในขณะที่ EDI เริ่มทำให้กระดาษหมดความนิยมลง แต่กฎเกณฑ์ทางกฎหมายที่มีอยู่ยังเป็นกฎเกณฑ์ทางกฎหมายที่ยังใช้กับการทำธุรกิจที่ใช้กระดาษอยู่ ในปัจจุบัน EDI จึงอยู่ท่ามกลางความไม่แน่นอนทางกฎหมาย ไม่เป็นที่แน่ชัดว่ากฎเกณฑ์ที่มีอยู่จะสามารถนำมาปรับใช้กับธุรกิจที่เปลี่ยนแปลงไปได้หรือไม่ หรือกฎเกณฑ์เดิมที่มีอยู่อาจจำเป็นต้องแทนที่ด้วยกฎเกณฑ์ใหม่หรือไม่บรรทัดฐานทางกฎหมายเดิมไม่สามารถตอบคำถามทุกคำถามที่ EDI หยิบยกขึ้นได้ จึงถือเป็นความจำเป็นเร่งด่วนที่แต่ละประเทศและระหว่างประเทศจะต้องมาพัฒนามาตรฐานกฎเกณฑ์ทางกฎหมายที่ใช้กับ EDI

การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic Data Interchange : EDI) หมายถึง เทคโนโลยีหรือวิธีการที่สามารถทำให้คู่สัญญาฝ่ายหนึ่งสามารถส่งข้อมูลที่มีผลผูกพันทางกฎหมายไปยังคู่สัญญาอีกฝ่ายหนึ่ง เทคโนโลยีดังกล่าวจะใช้รูปแบบทางอิเล็กทรอนิกส์ที่เป็นมาตรฐาน (Standard Electronic Format) ซึ่งสามารถใช้แทนเอกสารที่เป็นกระดาษเช่น ใบเรียกเก็บเงิน (Invoice) หรือคำสั่งซื้อ (Purchase Order) รูปแบบที่เป็นมาตรฐานจะรวมถึงองค์ประกอบของข้อมูล (Data Element) ที่สามารถอ่านและใช้โดยเครื่องคอมพิวเตอร์ที่รับข้อมูลมา โดยทั่วไปแล้วสิ่งที่เรียกว่า Free Text Element จะไม่สามารถประมวลผลได้โดยตรง แต่สามารถแสดง พิมพ์ และทบทวนโดยบุคคลที่สำนักงานของผู้รับ การใช้ EDI สามารถทำได้ในหลายวัตถุประสงค์ เช่น ใช้แทนเอกสารที่เป็นกระดาษ รวมถึงวิธีการสื่อสารข้อมูลที่เป็นใบตราส่ง (Bill of Lading) การโอนหุ้น (Transferring Securities) และใช้แทน Letter of credit³⁴

โดยต่อไปนี้จะเป็นการวิเคราะห์ถึงบทบาทของกระดาษในฐานะที่เป็นองค์ประกอบที่สำคัญของบทบาทปฏิบัติของกฎหมายที่มีอยู่เดิม

กระดาษจะช่วยแก้ไขปัญหามีข้อพิพาทดังต่อไปนี้

1. พิสูจน์เจตนา เอกสารที่เป็นกระดาษจะช่วยยืนยันถึงข้อผูกพันที่กำหนดไว้ในสัญญาซึ่งผู้ลงนามตามสัญญาดังกล่าวจะต้องถือปฏิบัติ

³⁴ โปรดดู Charles Mooney, Jr., Beyond Negitability: A New Model for Transfer and Pledge of Interest in Securities Controlled by Intermediaries, 12 Cardozo L. Rev. 305, 307 (1990)

2. พิสูจน์ว่าได้ปฏิบัติตามสัญญาแล้ว เอกสารที่เป็นกระดาษหากได้ลงลายมือชื่ออาจแสดงถึงว่าผู้ลงนามดังกล่าวได้ชำระหนี้ตามสัญญาแล้ว
3. การพิสูจน์ความถูกต้อง (Authenticity) เอกสารหากมีการลงลายมือชื่อถือเป็นข้อสันนิษฐานเบื้องต้นว่าเป็นเอกสารที่แสดงเจตนาตามที่กำหนดไว้ในเอกสารดังกล่าวจริง และจะมีผลอย่างมากในการพิสูจน์ความถูกต้องในกรณีของการรับฟังเอกสารใดเป็นพยานหลักฐานหรือไม่

ข้อจำกัดของเอกสารที่เป็นกระดาษ

1. แม้ว่าลายมือชื่อแบบเดิมมักจะได้รับความเชื่อถือเป็นวิธีที่จะช่วยพิสูจน์ความถูกต้องของเอกสาร (Authenticity) แต่ก็ไม่ได้หมายความว่าลายมือชื่อดังกล่าวจะมีความปลอดภัยร้อยเปอร์เซ็นต์ ลายมือชื่ออาจถูกปลอมได้ โดยเฉพาะอย่างยิ่งในกรณีที่ผู้รับไม่คุ้นเคยกับลายมือชื่อของผู้ส่ง
2. เอกสารกระดาษต้องการพื้นที่เก็บเอกสารมากเพื่อเก็บรักษาความลับของเอกสารดังกล่าว

ปัญหาข้อกฎหมายอันเกิดจากการนำเอาเอกสารทางอิเล็กทรอนิกส์มาใช้

1. เอกสารอิเล็กทรอนิกส์สามารถใช้เป็นพยานหลักฐานในศาลหรือไม่
2. กฎหมายของหลายประเทศกำหนดให้ต้องมีการลงลายมือชื่อเพื่อพิสูจน์ว่าเจ้าของลายมือชื่อได้ทำเอกสารดังกล่าวจริง ซึ่งเอกสารทางอิเล็กทรอนิกส์ไม่อาจที่จะลงนามได้เหมือนเอกสารโดยทั่วไป
3. เพื่อที่จะได้รับประโยชน์จากระบบที่ไม่ใช้กระดาษหรือระบบอิเล็กทรอนิกส์ จำเป็นที่จะต้องมีการส่งเอกสารเป็นหลักฐานต่อหน่วยราชการ เช่น เรื่องของภาษีมูลค่าเพิ่มหรือเรื่องของการศุลกากร
4. ในกรณีที่มีการแก้ไขเปลี่ยนแปลงข้อมูลอิเล็กทรอนิกส์ในระหว่างการส่งข้อมูล

3.3 การเกิดขึ้นของทรัพย์สินชนิดใหม่ (New Species of Property)

ผลกระทบที่สำคัญของการมาถึงและความเจริญเติบโตในการใช้สื่ออิเล็กทรอนิกส์คือการเกิดขึ้นของทรัพย์สินประเภทใหม่ที่มีค่าทางการค้า ในอดีต ประเภทของธุรกรรมทางการค้าระหว่างประเทศจะเกี่ยวข้องกับการซื้อขาย ไฟแนนซ์ การขนส่ง และการชำระเงินสำหรับสินค้าและบริการ ในทศวรรษที่ผ่านมาเราได้เห็นการลดบทบาทของ สัญญาที่อยู่บนพื้นฐานของสินค้า (Goods-based contract) ในการค้าระหว่างประเทศและการเกิดขึ้นและเพิ่มระดับความสำคัญของสัญญาที่อยู่บนพื้นฐานของการบริการ (Service contract) นอกจากนั้นแล้วในปัจจุบันเรากำลังมองเห็นการเปลี่ยนแปลง วิวัฒนาการของการทำธุรกรรม วิวัฒนาการที่ไม่ได้อยู่บนพื้นฐานของสินค้าหรือการบริการหากแต่อยู่บนข้อมูลข่าวสาร นั่นคือเราได้เข้าสู่ยุคแห่งข้อมูลข่าวสาร ในปัจจุบันข้อมูลข่าวสารเป็นสิ่งที่มีความสำคัญมากกับการทำธุรกิจข้อมูลดังกล่าวถูกประมวลผล เก็บ และส่งผ่าน

เนื่องจากข้อมูลได้กลายเป็นสิ่งที่มีราคาและเป็นสิ่งที่มีค่าในการทำธุรกิจในยุคแห่งสารสนเทศ การทบทวนถึงข้อความคิดในเรื่องของทรัพย์สินและการใช้ข้อความคิดดังกล่าวกับทรัพย์สินประเภทใหม่เป็นเรื่องที่พึงต้องกระทำอย่างเร่งด่วน

กฎหมายเทคโนโลยีสารสนเทศโดยเฉพาะในส่วนที่เกี่ยวกับการพาณิชย์ได้เกิดขึ้นเพื่อสนองต่อสภาพเศรษฐกิจในปัจจุบัน เป็นยุคหลังจากยุคอุตสาหกรรมเป็นยุคเศรษฐกิจแห่งข้อมูลข่าวสาร (Information Economy)

สัญญาในปัจจุบันเป็นสัญญาที่ไม่เกี่ยวข้องเนื่องกับการโอนทรัพย์สินที่มีรูปร่าง (Res Corporales) กล่าวคือจะอยู่ในรูปของสื่อทางกายภาพอย่างเช่นแผ่นดิสเก็ตหรือแผ่นซีดี ที่บรรจุข้อมูลที่ไม่สามารถจับต้องได้ อย่างไรก็ตามคุณค่าของโปรแกรมไม่ได้อยู่ที่ตัวแผ่นดิสเก็ตแต่อยู่ที่ตัวข้อมูลที่ไม่สามารถจับต้องได้ที่อยู่บนแผ่นดิสเก็ตดังกล่าวหาก

ในส่วนที่เกี่ยวกับสินค้า โดยทั่วไปแล้วผู้ซื้อต้องการครอบครองสินค้าและผู้ขายต้องโอนกรรมสิทธิ์หรือความครอบครองในสินค้า ต่างกับการโอนข้อมูล (Information) วัตถุประสงค์ของผู้รับโอนคือได้ข้อมูลข่าวสารและสิทธิตามสัญญาที่เหมาะสมในการใช้ข้อมูลดังกล่าว วัตถุประสงค์ของผู้ให้บริการข้อมูลคือ

จัดหาข้อมูลและให้สิทธิในการใช้ข้อมูลดังกล่าว ในขณะที่ผู้ให้บริการข้อมูลยังมีสิทธิที่จะใช้ข้อมูลดังกล่าวในอนาคต ซึ่งก็มีความแตกต่างระหว่างสิทธิที่ให้และสิทธิที่ตนเองมีอยู่³⁵

อย่างไรก็ดีจุดสำคัญอยู่ที่ว่าจุดมุ่งหมายผู้รับโอนอยู่ที่สิทธิมากกว่าการครอบครองหรือการควบคุมทางกายภาพ เหมือนกับผู้โอน การโอนสินค้าจะอยู่บนพื้นฐานของการคืนกำไรจากสินค้าดังกล่าว ในขณะที่การโอนสิทธิในข้อมูลผู้โอนจะไม่ยกเลิกความเป็นเจ้าของข้อมูลที่ให้สิทธิไป ตัวอย่างเช่น ข้อเท็จจริงที่ว่าผมเปิดเผยข้อมูลหรือโอนความลับไปให้คุณไม่ได้หมายความว่าผมไม่เคยรู้ข้อมูลดังกล่าว สำหรับสินค้า ธุรกรรมจะถูกพันโดยค่านึงถึงจะเน้นของสิ่งที่จับต้องได้ สำหรับข้อมูลลักษณะของการโอนข้อมูลจะไม่อยู่บนสิ่งที่ส่งมอบทางกายภาพแต่จะอยู่ที่สิทธิที่ให้หรือที่ถือไว้ตามสัญญา

โดยธุรกรรมการซื้อขายสินค้าจะถือว่าการชำระหนี้จะทำการส่งมอบสินค้า ในทางกลับกัน สำหรับธุรกรรมที่เกี่ยวกับข้อมูลข่าวสาร การส่งมอบอาจไม่ใช่สาระสำคัญ ข้อมูลสามารถโอนได้หลายทาง เช่น ทางโทรศัพท์ ทางกาส่งข้อความทางอิเล็กทรอนิกส์ หรือโดยแผ่นดิสเก็ต ในบางธุรกรรมอาจไม่มีการโอนเลยก็ได้ เนื่องจากการทำธุรกรรมดังกล่าวจะเกี่ยวเนื่องกับการให้สิทธิในการใช้ข้อมูลเท่านั้น

ระบบกฎหมายที่สนับสนุนเศรษฐกิจแห่งข้อมูลข่าวสาร (Information Economy) จะต้องเข้าใจความแตกต่างดังกล่าวนี้ ข้อกำหนดของสัญญาโดยเฉพาะอย่างยิ่งข้อกำหนดที่เกี่ยวกับขอบเขตของการให้สิทธิมีความสำคัญอย่างมากในเศรษฐกิจแห่งข้อมูลข่าวสารมากกว่าเศรษฐกิจที่อยู่บนพื้นฐานของสินค้าที่สามารถจับต้องได้

การให้สิทธิไม่ใช่การเช่าหรือการขายสินค้า ทั้งการเช่าและการขายสินค้าจะใช้กับสินค้าเท่านั้น ไม่ใช้กับสิทธิในข้อมูลข่าวสาร ในกรณีการเช่าและการขาย วัตถุประสงค์หลักของผู้รับโอนต้องการสินค้า แต่ในกรณีของการให้สิทธิ ผู้รับโอนต้องการการใช้ข้อมูล

3.4 สถานที่และเวลาที่เปลี่ยนแปลงไป

³⁵ Raymond T. Nimmer, "Article 2B: An Introduction", Journal of Computer & Information Law, Vol. XV, 1997, pp. 212-213

ในการติดต่อกันบนเครือข่ายในระบบเปิดอย่างเช่นอินเทอร์เน็ตนั้น เราสามารถติดต่อกับบุคคลได้ทั่วทุกมุมโลกไม่ว่าเวลาใดก็ได้ แม้ว่าเราจะไม่เคยรู้จักบุคคลดังกล่าวเลยก็ตามที่ บนเครือข่ายหรือบนไซเบอร์สเปซนั้นไม่มีพรมแดน ไม่อาจบอกได้ว่าสัญญาทางอิเล็กทรอนิกส์ที่ทำขึ้นนั้นเกิดขึ้นในประเทศไหนอย่างแน่นอน หรือบุคคลที่เราติดต่อด้วยก็ไม่สามารถระบุได้อย่างชัดเจนว่ามีสัญชาติอะไร ปัญหาในเรื่องของขอบเขตทางภูมิศาสตร์ของข้อตกลงซึ่งในเรื่องนี้ยังเป็นคำถาม และปัญหาระหว่างประเทศที่จะต้องแก้ไขโดยเร่งด่วน กฎหมายของประเทศใดจะถูกนำมาใช้บังคับ และประเทศไหนจะมีอำนาจศาลเหนือข้อพิพาทที่จะเกิดขึ้น

3.5 ความเสี่ยงที่เกิดขึ้นใหม่

เนื่องจากการทำธุรกรรมที่เกี่ยวกับพาณิชย์อิเล็กทรอนิกส์นั้น จำเป็นที่จะต้องพึ่งพาเทคโนโลยีและเครื่องมืออุปกรณ์ทางคอมพิวเตอร์อย่างมาก จึงจำเป็นที่จะต้องมีการกลไกที่จะป้องกันความเสี่ยงที่เรียกว่า "ระบบรักษาความปลอดภัย" (Security) ที่จะกำหนดถึงความพร้อมของระบบในการป้องกันการเข้ามา แกะไขหรือทำลายโดยไม่ได้รับอนุญาต ส่วนคำว่า "Authentication" จะกล่าวถึงวิธีการที่จะทำอย่างไรให้ผู้ใช้งานเกิดความมั่นใจว่าข้อมูลที่ได้รับเป็นข้อมูลที่แท้จริงของผู้ส่ง

ปัญหาข้อกฎหมายที่เกี่ยวกับเรื่องดังกล่าวจะพิจารณาถึงหน้าที่ในการดูแลรักษา (Duty of care) ในการรักษาความปลอดภัย และปัญหาในเรื่องของการกระจายความรับผิดชอบ (Attribution of responsibility) ในกรณีที่ข้อมูลถูกปลอมแปลงหรือแก้ไข การกำหนดว่าใครมีหน้าที่รับผิดชอบในการป้องกันความเสี่ยงดังกล่าว และใครมีหน้าที่รับผิดชอบในค่าเสียหายในกรณีที่ระบบรักษาความปลอดภัยและระบบตรวจสอบความถูกต้อง (Authenticate) ล้มเหลว ปัญหาดังกล่าวเหล่านี้จะเป็นตัวก่อรูปมิติทางกฎหมายของความเสี่ยงการรักษาความปลอดภัย และการพิสูจน์ความถูกต้อง (Authentication) ในการทำสัญญาทางอิเล็กทรอนิกส์

บทที่ 4

ธุรกรรมอิเล็กทรอนิกส์ (Electronic Transaction)

1. ความทั่วไป

วิวัฒนาการทางเทคโนโลยีคอมพิวเตอร์ เป็นสัญญาณเตือนถึงผลกระทบในเรื่องของแนวความคิดเสรีภาพในการทำสัญญา โดยเฉพาะในเรื่องของ EDI ที่ถือว่าสามารถทำงานได้เหมือนมนุษย์ (Anthropomorphosis)

แนวความคิดที่ว่าสัญญาจำเป็นต้องมีความเห็นพ้องต้องกันทางเจตนา "Meeting of the minds" เริ่มปรากฏชัดในราวศตวรรษที่ 18³⁶ ซึ่งก็เป็นแนวความคิดหนึ่งที่ตรงกับเรื่องของเสรีภาพในการทำสัญญาซึ่งเป็นแนวความคิดที่เป็นที่นิยมในราวกลางศตวรรษที่ 19 แต่แนวความคิดดังกล่าวก็ต้องเปลี่ยนแปลงไปตามกาลเวลา³⁷

ตัวอย่างเช่นคดี Corinthian Pharmaceutical Systems Inc. v. Lederle Laboratories³⁸ ซึ่งโจทก์พยายามที่จะซื้อสินค้าก่อนที่จะราคาสินค้าจะขึ้น โดยเขาได้โทรศัพท์สั่งซื้อสินค้าผ่านระบบสั่งซื้อสินค้าทางโทรศัพท์ที่ควบคุมโดยเครื่องคอมพิวเตอร์ของจำเลย เครื่องคอมพิวเตอร์ได้ออก Tracking Number เพื่อการสั่งซื้อแต่ศาลตัดสินว่า "การทำการแทนแบบอัตโนมัติไม่สามารถถือว่าเป็นการยอมรับได้" (an automated, ministerial act cannot constitute an acceptance.)

³⁶ Powell, "Essay upon the Law of Contracts", Pothier, Law of Obligations

³⁷ Atiya, The Rise and Fall of Freedom of Contract, Clarendon Press, Oxford, 1979, p.407-8

³⁸ 724 F. Supp. 605 (S.D. Ind., 1989)

อีกคดีหนึ่งเป็นคดีที่เกิดขึ้นที่ประเทศนิวซีแลนด์ชื่อว่าคดี Databank Systems Ltd v Commissioner of Inland Revenue³⁹ พิจารณาถึงระบบการโอนเงิน ณ จุดขาย (Electronic funds transfer at point of sale) ซึ่ง Lord Templeman อธิบายว่า

"...ผู้ซื้อน้ำมันจากปั้มน้ำมันโดยใช้บัตรเครดิตของธนาคารเป็นวิธีการทำสัญญาระหว่างผู้ซื้อน้ำมันและผู้ขายน้ำมัน บัตรเครดิตและรายละเอียดต่างๆ ที่เกี่ยวกับน้ำมันได้ถูกป้อนเข้าเครื่องคอมพิวเตอร์ซึ่งทำหน้าที่คล้ายเช็คตามที่กฎหมายได้บัญญัติไว้ หากคอมพิวเตอร์ได้รับคำสั่งจากธนาคารว่าแบ่งคีย์ยอมรับเช็คดังกล่าว คอมพิวเตอร์จะทำการเดบิตราคาน้ำมันยังบัญชีธนาคารของผู้ซื้อน้ำมันและเครดิตราคาน้ำมันที่บัญชีธนาคารของปั้มน้ำมัน ดังนั้นจึงถือว่าสัญญาซื้อขายน้ำมันระหว่างผู้ซื้อและผู้ขายเสร็จสมบูรณ์ ดังนั้นเครื่องคอมพิวเตอร์จะทำการออกใบเสร็จรับเงินและบันทึกรายการจำหน่ายน้ำมันไว้รวมทั้งมีคำสั่งให้ทำการสต็อกน้ำมันไว้จำหน่ายต่อไป"

โดยศาลในคดีดังกล่าวพบว่าในกรณีดังกล่าวมีสัญญาที่ทำระหว่างคอมพิวเตอร์และคอมพิวเตอร์ถึงสามฉบับ คือสัญญาระหว่างผู้ซื้อและผู้ขายน้ำมัน สัญญาระหว่างผู้ซื้อและธนาคารผู้ออกบัตรเครดิต และสัญญาระหว่างธนาคารผู้ออกบัตรเครดิตและผู้จำหน่ายน้ำมัน

ในปัจจุบันสถิติในการใช้คอมพิวเตอร์เพื่อทำสัญญามีเพิ่มขึ้นอย่างมาก⁴⁰ เทคโนโลยีในรูปของคอมพิวเตอร์ ดาวเทียมหรือเครื่องมือการสื่อสารสามารถช่วยให้เราตรวจสอบขบวนการขนส่งทั่วโลกนาที่ต่อนาที่ไม่ว่าจะอยู่ที่ไหนทั่วโลก⁴¹ หรือแม้แต่ในปัจจุบัน Municipal Court ของ Long Beach California คอมพิวเตอร์ก็ทำหน้าที่เป็นเจ้าหน้าที่ศาลที่ทำหน้าที่สั่งผู้ขับขี่ยวดยานที่ทำผิดกฎหมายว่าจะต้องจ่ายค่า

³⁹ [1990] 3 N.Z.I.R.385

⁴⁰ Wein , "The Responsibility of Intelligent Artifacts: Toward an Automation Jurisprudence.W (1992) 6 Harv.J.Law and Tec. 103

⁴¹ Yanacek , "Hitching to the Stars; Satellites for Shipping Tracking" , (1998) 29 Transportation and Distribution 16.

ประการใด ให้คำแนะนำการฟ้องร้องคดีที่เกี่ยวกับเงินจำนวนน้อย (Small Claims Prosecutions)⁴² รวมทั้งบริการอื่นๆ ที่เกี่ยวกับการดำเนินคดี เป็นต้น

คอมพิวเตอร์ตามที่ได้ยกตัวอย่างมานี้ไม่ใช่เป็นแต่เพียงเครื่องอำนวยความสะดวกเท่านั้น กล่าวคือทำหน้าที่มากกว่าเป็นเครื่องมือฝากเงินของธนาคารหรือเป็นเพียงเครื่องจำหน่ายตัว เครื่องคอมพิวเตอร์มีบทบาทสำคัญในภาคการธนาคาร การค้าระหว่างประเทศ ตลาดการค้าโภคภัณฑ์ และตลาดหลักทรัพย์ รวมทั้งในธุรกิจประกันภัย

โดยเฉพาะอย่างยิ่งเมื่อนำเอาระบบ EDI มาใช้กับการจัดการแบบ Just in time ซึ่งหมายถึงการจัดเก็บสินค้าให้อยู่ในระดับที่สามารถเรียกใช้เพื่อทำการผลิตได้ไม่ให้มีสินค้าค้างสต็อกมากเกินไป ซึ่งจะทำให้มีรายจ่ายมากขึ้น ระบบ EDI จะช่วยให้การส่งสินค้าสามารถทำได้อย่างรวดเร็วส่งผลให้สินค้ามีอยู่ในสต็อกในระดับที่พอดีอยู่เสมอ

โดยเครื่องคอมพิวเตอร์ของผู้ซื้อจะเช็คสต็อกสินค้าว่าอยู่ในระดับที่กำหนดไว้หรือไม่หากขาดไปเครื่องคอมพิวเตอร์จะสามารถตัดสินใจสั่งสินค้า เครื่องคอมพิวเตอร์ดังกล่าวที่ได้รับการวางโปรแกรมไว้จะทำการจัดทำคำสั่งและส่งไปยังคอมพิวเตอร์ของผู้ขายภายในระยะเวลาอันรวดเร็ว และสำหรับเครื่องคอมพิวเตอร์ของผู้ขายหากคำสั่งซื้อดังกล่าวตรงตามที่ได้วางโปรแกรมไว้ก็จะทำคำสั่งเพื่อส่งสินค้าไปยังผู้สั่งซื้อ และก็จะทำการลงบัญชีของบริษัทและฐานข้อมูลคลังสินค้าของบริษัทโดยอัตโนมัติ สินค้าจะถูกส่งและการตรวจสอบการส่งสินค้าไม่ว่าจะอยู่ ณ มุมไหนของโลกจะทำการตรวจสอบทางอิเล็กทรอนิกส์โดยใช้ระบบดาวเทียม กระบวนการดังกล่าวจะทำโดยอัตโนมัติในทุกๆ ขั้นตอน การที่จะมีมนุษย์เข้ามาแทรกแซงในขั้นตอนใดขั้นตอนหนึ่งจึงทำให้ประสิทธิภาพการดำเนินงานลดลงและสิ้นเปลืองทรัพยากรหรืออาจมีความเสี่ยงเพิ่มมากขึ้น

ระบบ JIT และ EDI สามารถทำให้เกิดการต่อรอยระหว่างเครื่องคอมพิวเตอร์ได้ และสามารถทำให้เกิดสัญญาณได้โดยที่ผู้ซื้อและผู้ขายไม่ได้รับรู้ จึงทำให้เห็นว่าแนวความคิดที่มีอยู่ไม่สามารถปรับใช้กับ

⁴² Moss and Hansen, "Autoclerk" (1992) 78 A.B.A.J. 34

การที่เครื่องคอมพิวเตอร์สามารถทำคำเสนอและคำสนองเหมือนกับเป็นคู่สัญญากัน ซึ่งแนวความคิดเดิมของกฎหมายการทำสัญญาจะต้องอยู่ภายใต้การรับรู้ ความเชื่อถือและความคาดหวังของบุคคล

อย่างไรก็ดีหลักเบื้องต้นของกฎหมายว่าด้วยเรื่องสัญญา คือ วางข้อสันนิษฐานว่าสัญญาอยู่บนพื้นฐานของการตัดสินใจของบุคคลไม่ว่าจะทำเองหรือโดยตัวแทน ซึ่งหลักดังกล่าวในอดีตก็ไม่ค่อยจะมีปัญหามากนักเนื่องจากโดยส่วนใหญ่แล้วสัญญาเกิดจากการเจรจา และตกลงโดยคู่สัญญา จากรูปแบบของข้อสมมติฐานที่ต้องมีคนเข้ามาเกี่ยวข้องในกระบวนการทำสัญญา (Humanistic Model) นั้นมีผลถึงหลักการ รายละเอียดและข้อจำกัดของกฎเกณฑ์ทางกฎหมายในการทำสัญญา

การมาถึงซึ่งคอมพิวเตอร์และพาณิชย์อิเล็กทรอนิกส์ถือเป็นส่วนสำคัญของการประกอบธุรกิจในปัจจุบันที่ส่งผลกระทบต่อหลักการและแนวความคิดที่วางอยู่บนพื้นฐานของการมีมนุษย์เข้ามามีส่วนร่วมในการทำธุรกรรม (Humanistic Principle) ในขณะที่เครื่องคอมพิวเตอร์ไม่มีความคิดหรือมีวิวัฒนาการโดยตัวของมันเอง แต่จะสามารถทำงานหากถูกวางโปรแกรมให้ทำงานตามคำสั่ง สิ่งนี้จะเป็นตัวแสดงให้เห็นความแตกต่างในรากฐานทางความคิดระหว่างการทำสัญญา โดยอิเล็กทรอนิกส์และกฎหมายสัญญาและทางปฏิบัติแบบเดิม ที่สำคัญอย่างยิ่ง เครื่องคอมพิวเตอร์ที่ได้รับการวางโปรแกรมสามารถเลือกและตอบสนอง โดยมีมนุษย์หรือไม่มีมนุษย์เข้ามาเกี่ยวข้องได้ คำถามคือว่าภายใต้สถานการณ์อะไรที่ตัวเลือก และการตอบสนองมีผลผูกพันคู่สัญญา

มนุษย์สามารถมีบทบาทหรือเกี่ยวพันกับการทำสัญญาทางอิเล็กทรอนิกส์และทางธุรกิจโดยทั่วไป เพื่อวัตถุประสงค์ในการพิจารณาเราสามารถที่จะแบ่งออกเป็นสี่ขั้นตอนดังต่อไปนี้

- มนุษย์ต่อมนุษย์ : มนุษย์จะเป็นผู้ตัดสินใจทำหรือไม่ทำสัญญา เครื่องมือทางอิเล็กทรอนิกส์จะเป็นเพียงเครื่องมือในการช่วยส่งข้อมูลที่เกี่ยวข้องกับการตัดสินใจทำสัญญาหรือไม่ ตัวอย่างเช่น นาย ก ส่ง E-mail ไปยัง ข เพื่อเสนอทำสัญญา หลังจากที่ได้พิจารณาคำเสนอแล้ว ข ก็ตอบตกลงรับทำสัญญา

- มนุษย์กับเครื่องคอมพิวเตอร์ (หรือกลับกัน) : มนุษย์จะเป็นฝ่ายเดียวของคู่สัญญาแต่อีกฝ่ายหนึ่งจะเป็นเครื่องคอมพิวเตอร์ อิเล็กทรอนิกส์จะทำการสื่อสารข้อมูลและทำการตัดสินใจโดยคู่สัญญาฝ่ายเดียว ตัวอย่างเช่น ก ติดต่อกับเครื่องคอมพิวเตอร์เพื่อทำการซื้อสินค้า ก ได้สั่งซื้อแผ่น ซีดีชุดล่าสุด 10 แผ่น และเครื่องคอมพิวเตอร์ของเครือข่ายเพื่อการสั่งซื้อสินค้า "รับ" คำสั่งซื้อดังกล่าวและมี "คำสั่ง" ให้โปรแกรมบัญชีคลังสินค้า (Inventory program) เพื่อส่งแผ่น ซีดี จำนวน 10 แผ่นตามราคาที่ได้ตกลงกันได้
- คอมพิวเตอร์กับเครื่องคอมพิวเตอร์ (ตกลงกันได้ก่อน) : ธุรกรรมบางอย่างได้ถูกกำหนดขึ้นและสามารถดำเนินการโดยเครื่องคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์โดยที่มนุษย์ไม่มีความจำเป็นที่จะต้องเข้ามาทบทวนการทำธุรกรรมดังกล่าวอีก แต่ธุรกรรมดังกล่าวสามารถทำขึ้นภายใต้ขอบเขตที่กำหนดโดยสัญญา(Trading Agreement) ที่ทำขึ้นไว้ก่อนระหว่างคู่สัญญา ตัวอย่างเช่น คอมพิวเตอร์ของบริษัทฟอร์ด ได้ส่งวิทยุจากบริษัท XYZ จำนวน 1,000 เครื่องโดยให้จัดส่งให้ทันทีที่คำสั่งดังกล่าวได้รับการยอมรับและบันทึกโดยเครื่องคอมพิวเตอร์ของบริษัท XYZ ที่ได้วางโปรแกรมไว้ล่วงหน้าตามสัญญาที่กำหนดไว้เป็นลายลักษณ์อักษรระหว่างบริษัทฟอร์ด และบริษัท XYZ
- คอมพิวเตอร์กับเครื่องคอมพิวเตอร์ (ไม่ได้ทำความตกลงไว้ล่วงหน้า) : ธุรกรรมสามารถเกิดขึ้นโดยปราศจากการทบทวนของมนุษย์และโดยไม่มีข้อตกลงที่เป็นลายลักษณ์อักษรไว้ล่วงหน้าระหว่างคู่สัญญา ตัวอย่างเช่น ดำ โปรแกรมเครื่องคอมพิวเตอร์ของเขาให้ทำการค้นข้อมูลในอินเทอร์เน็ตรายวัน หรือในเครือข่ายอื่นเพื่อหาข้อมูลเกี่ยวกับราคาทองคำ โปรแกรมค้นและพบว่ามียางานราคา 10,000 บาท จากบริษัทให้บริการข้อมูลแดง คอมพิวเตอร์ของทั้งสองฝ่ายสามารถและก่อให้เกิดการซื้อขายและโอนข้อมูลไปยังเครื่องคอมพิวเตอร์ของดำได้

อย่างไรก็ดีปัญหาอาจมีความซับซ้อนมากขึ้น หากพิจารณาประกอบกับเนื้อหาของการติดต่อสื่อสารซึ่งมีรูปแบบที่ความสำคัญทางกฎหมายที่แตกต่างกันดังต่อไปนี้⁴³

- การติดต่อสื่อสารทางการค้าที่ไม่มีผลทางสัญญา: การสื่อสารในรูปแบบนี้คือการสื่อสารที่ทำกันโดยทั่วไป เช่นข้อมูลทางสถิติต่างๆ แง่มุมทางกฎหมายของการสื่อสารแบบนี้มีเพียงแต่ผู้ส่งอาจรับผิดชอบสำหรับความถูกต้องของข้อมูล⁴⁴
- การสื่อสารที่มีผลทางสัญญา : การสื่อสารในรูปแบบนี้จะใช้เป็นหลักฐานในการก่อให้เกิดสัญญา เช่นคำสั่งซื้อ ในโลกของกระดาษเช่นเอกสารมักจะรวมถึงข้อมูลที่เกี่ยวข้องกับสัญญา เช่นข้อกำหนดมาตรฐานต่างๆ และเงื่อนไขต่างๆของผู้ส่ง
- การสื่อสารซึ่งมีผลให้เกิดการโอนกรรมสิทธิหรือสิทธิตามกฎหมาย: เช่นกรณีของรับรองบางอย่าง ใบตราส่ง (Bill of Lading) หรือตั๋วแลกเงิน (Bill of Exchange) โดยเฉพาะสำหรับใบตราส่งนั้นการโอนการถือครองเอกสารจะแสดงถึงการโอนสิทธิทางกฎหมายในสินค้า สำหรับกรณีตั๋วแลกเงินสามารถโอนสิทธิการรับเงินตามตั๋วแลกเงินดังกล่าวได้
- การสื่อสารที่ทำตามข้อกำหนดทางราชการ : การสื่อสารดังกล่าวรวมถึงข้อมูลที่เกี่ยวข้องภาษีอากร เช่นคณะกรรมการภาษีมูลค่าเพิ่มและหน่วยงานทางด้านศุลกากร สำหรับการค้าระหว่างประเทศ นอกจากนั้นยังเพิ่มความสำคัญ ในเรื่องของการยื่นข้อมูลต่อสหภาพยุโรป

⁴³ โปรดดู Goode R. & Bergsten E., "Legal questions and problems to be overcome", pp. 131-133, in Thomsen, H. B., & B. S. Wheble, Yrading with EDI: The legal Issues, IBC Financial Books 1989; and Reed, C., "EDI-contractual and liability issues", pp. 36-41, Computer Law & Practice, Vol.6, No.2, 1989; and Speipel, P. (ed.), From Data Protection to Knowledge Machines, No.5 Computer2Law Series, Kluwer/The Netherlands 1990

⁴⁴ Hedley Byrne & Co. Ltd. V. Heller & Partners Ltd. [1964] A.C. 465, H.L.

- การสื่อสารที่ต้องการอำนาจทางกฎหมายหรือได้รับอนุญาต : ตัวอย่างเช่นกฎหมายคุ้มครองข้อมูลส่วนบุคคลต้องการให้ผู้ใช้ข้อมูลได้รับการอนุญาตจากหน่วยงานที่มีอำนาจก่อนที่จะส่งข้อมูลออกนอกประเทศ ในขณะที่ในบางประเทศการส่งข้อมูลที่เข้ารหัสจะต้องได้รับอนุญาตก่อน

จะเห็นได้ว่าการมีส่วนร่วมในกระบวนการทำสัญญาของคอมพิวเตอร์ และรูปแบบการติดต่อสื่อสารที่ได้กล่าวมาข้างต้นล้วนแต่ยืนยันให้เห็นว่าในเรื่องของสัญญาทางอิเล็กทรอนิกส์ ปัญหาที่เกิดขึ้นจะหมุนวนอยู่กับเรื่องที่ว่าข้อความอิเล็กทรอนิกส์ (Electronic Message) สามารถก่อให้เกิดคำเสนอหรือคำสนองได้หรือไม่แม้ว่าจะไม่มีการตัดสินใจของมนุษย์เข้ามาเกี่ยวข้อง และนอกจากนั้นยังมีปัญหาว่าเมื่อไรคำเสนอ คำสนอง และการปฏิเสธคำเสนอจะมีผลเมื่อใด รวมทั้งปัญหาในเรื่องของแบบจะเป็นอย่างไร

2. การเจรจาสัญญา

การเจรจาคือกระบวนการต่อรองของคู่เจรจา เมื่อสองร้อยปีที่ผ่านมาการเจรจามักจะทำกันเฉพาะหน้าเพื่อให้แต่ละฝ่ายสามารถสังเกตท่าทีของอีกฝ่ายหนึ่ง แต่ด้วยการมาถึงของเทคโนโลยีสมัยใหม่ส่งผลให้การเจรจาสามารถทำกันโดยห่างซึ่งระยะทางได้ โดยใช้วิธี โทรศัพท์หรือทางไปรษณีย์

และเนื่องจากการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือระบบ EDI นั้นเป็นการติดต่อสื่อสารผ่านทางคลื่นแม่เหล็กไฟฟ้า (Electro Magnetic) ปัญหาจึงเป็นว่ารูปแบบดังกล่าวจะถือเป็นการเจรจาหรือไม่ และหากถือว่าเป็นการเจรจา กฎเกณฑ์ในการเจรจาแบบไหนที่จะนำมาใช้ กล่าวคือจะถือเป็นการเจรจาเฉพาะหน้าหรือห่างโดยระยะทาง

3. เจตนา

ตามที่ได้กล่าวมาแล้วข้างต้นจะเห็นได้ว่าแนวความคิดพื้นฐานของกฎหมายเอกชน (Private Law) ถูกท้าทายจากการเกิดขึ้นของพาณิชย์อิเล็กทรอนิกส์ที่ว่าระบบคอมพิวเตอร์สามารถถูกวางโปรแกรมให้

สามารถทำสัญญาได้เหมือนกับที่มนุษย์ทำได้ การทำทายดังกล่าวมีผลกระทบแนวความคิดสองประการ คือ

1. แนวความคิดที่เป็นองค์ประกอบภายใน (Subjective state of mind) ของคู่สัญญา อันได้แก่เรื่องของเจตนาและการรับรู้ (Knowledge and intent)
2. แนวความคิดในเรื่องขององค์ประกอบภายนอก (Objective situation) เช่นกระบวนการที่ข้อมูล (Message) ถูกรับ ส่ง เข้ารหัส หรือ ถอดรหัส เป็นต้น ซึ่งจะสามารถปรับใช้กับหลักในเรื่องของการทำคำเสนอและคำสนอง

โดยเฉพาะปัญหาองค์ประกอบภายใน (Subjective Concepts) ซึ่งโดยทั่วไปแล้วหลักกฎหมายวางหลักว่า "เจตนา" เป็นองค์ประกอบสำคัญในการก่อนิติสัมพันธ์ ดังนั้นหลักกฎหมายดังกล่าวจึงมีความสำคัญอย่างมากและเป็นพื้นฐานในการพิจารณาถึงความผูกพันที่เกิดขึ้นจากการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ นอกจากนั้นแล้วกฎหมายของบางประเทศยังกำหนดให้คู่สัญญาต้อง "รู้" (Knowledge) ในผลทางกฎหมายที่ตนจะต้องผูกพัน เช่นในกรณีการถอนคำเสนอ เป็นต้น (เป็นตัวอย่างของกฎหมายว่าด้วยสัญญาของประเทศนอร์เวย์)

ตามกฎหมายว่าด้วยสัญญาของประเทศนอร์เวย์ คำเสนออาจถอนได้จนกว่าผู้ได้รับคำเสนอจะได้รับรู้คำเสนอนั้น เช่น ถ้าคอมพิวเตอร์ของนาย ก ได้ส่งคำเสนอในรูปแบบของการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI) ไปยังคอมพิวเตอร์ของ ข และต่อมา ก ต้องการถอนคำเสนอของตนเอง ก ก็ยังสามารถถอนคำเสนอของตนได้จนกว่า ข จะได้รับรู้ถึงคำเสนอนั้น ในกรณีของการใช้ระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์แบบเต็มรูปแบบ ข ไม่อาจรู้ได้ว่าการทำคำเสนอคำสั่ง (order) นั้นทำเสร็จสมบูรณ์แล้ว ณ เวลาใดที่จะถือว่า ข เสียหายอย่างรุนแรงจากการทำธุรกรรมดังกล่าว

อย่างไรก็ดีเจตนาดังกล่าวสามารถดูได้จากข้อตกลงพื้นฐานก่อนเพื่อกำหนดว่าได้กำหนดไว้อย่างไร และหากไม่สามารถหยั่งรู้ถึงเจตนาได้จากข้อตกลงให้ดูถึงพฤติการณ์แวดล้อมกรณีตัวอย่างเช่น การ

เจรจาตกลงกันของคู่สัญญา วิธีปฏิบัติของคู่สัญญา พฤติกรรมของคู่สัญญาอันนำไปสู่การตกลงทำสัญญากัน สารสำคัญและวัตถุประสงค์ของสัญญา หรือประเพณีปฏิบัติโดยทั่วไป เป็นต้น

4. คำเสนอ

4.1 เจตนาที่จะผูกนิติสัมพันธ์ตามกฎหมายอังกฤษ

คำเสนอคือการแสดงเจตนาที่จะผูกนิติสัมพันธ์ตามข้อความที่ได้เสนอไปและเมื่อมีคำสนองรับ ในกฎหมายอังกฤษการส่งจดหมายเวียนแจ้งรายการราคาสินค้า รายการสินค้าหรือการโฆษณาขายสินค้า หรือโดยแสดงสินค้าในตู้หรือบนห้างวางสินค้าไม่ถือเป็นคำเสนอ ถือเป็นเพียงคำเชิญชวนให้เข้าทำสัญญา (Invitation to treat) เท่านั้นและผู้ทำคำเสนอจะเป็นลูกค้า ตัวอย่างเช่นในร้านค้าลูกค้าจะนำสินค้าไปชำระเงินที่ผู้เก็บเงิน ซึ่งเจ้าของร้านมีสิทธิที่จะขายหรือไม่ก็ได้

ความสมบูรณ์ของคำเสนอ

ข้อกำหนดของกฎหมายทั้งสามระบบในเรื่องของคำเสนอคือคำเสนอจะต้องมีความสมบูรณ์เพียงพอที่จะทำคำสนอง ศาลอังกฤษจะพิจารณาจากความชัดเจนของการแสดงเจตนาว่ามีความสมบูรณ์พอที่จะเป็นคำเสนอหรือไม่ (หน้า 44)

4.2 เจตนาที่จะผูกนิติสัมพันธ์ตามกฎหมายฝรั่งเศส

ในทางตรงกันข้ามกฎหมายฝรั่งเศสตัวอย่างที่กล่าวมาข้างต้นนั้นถือว่าเป็นคำเสนอที่สามารถทำคำสนองทั้งสิ้นหากมีการกำหนดราคาไว้อย่างชัดเจน ตัวอย่างเช่นในกรณีของร้านสรรพสินค้าได้ยื่นฟ้องต่อศาล Cour de Cassation ว่าสัญญาที่สร้างขึ้นเมื่อลูกค้าได้หยิบสินค้าของร้านซึ่งมีราคาติดอยู่อย่างชัดเจนลงในตะกร้าที่ทางร้านจัดหาไว้ให้ ดังนั้นเมื่อความเสียหายเกิดขึ้นต่อลูกค้าจากการระเบิดของขวดน้ำผลไม้ในตะกร้าเนื่องจากการบรรจุขวดทำอย่างไม่เหมาะสมเมื่อโดนความร้อนจึงเกิดระเบิดขึ้น ร้านค้าดังกล่าวถูก

ตัดสินว่าจะต้องรับผิดชอบต่อลูกค้าในความเสียหายที่เกิดจากการละเมิดสัญญาตามมาตรา 1147 ของ Code Civil

ความสมบูรณ์ของคำเสนอ

กฎหมายฝรั่งเศสกำหนดให้การแสดงเจตนาจะถือเป็นคำเสนอก็ต่อเมื่อมีความสมบูรณ์และชัดเจนเพียงพอ คำเสนอควรที่จะมีข้อกำหนดที่สำคัญของสัญญาดังนั้นเพียงแต่การที่ผู้สนองตอบเพียงว่า "ผมยอมรับ" (I agree) ก็ถือว่าสัญญาเกิดขึ้นแล้ว แต่หากไม่ได้กำหนดราคาสินค้าไว้ชัดเจนยังไม่ถือว่าเป็นคำเสนอถือเป็นเพียง "Une offre d'entre en pourparlers"

4.3 เจตนาที่จะผูกนิติสัมพันธ์ตามกฎหมายเยอรมัน

กฎหมายเยอรมันคล้ายกับกฎหมายอังกฤษที่แยกระหว่างคำเสนอกับคำชี้ชวน โดยทั่วไปแล้วรายการสินค้า (Catalogue) หรือการโฆษณาสินค้า หรือการวางสินค้าบนห้างถือเป็นเพียงการชี้ชวนมากกว่าเป็นคำเสนอ อย่างไรก็ตามได้มีการวิพากวิจารณ์ในทางวิชาการในกรณีของการวางของในห้างสรรพสินค้าว่าเป็นคำเสนอของทางร้านและการสนองรับคือการนำสินค้าไปชำระเงินหรือเป็นเพียงคำชี้ชวนและการนำสินค้าไปชำระเงินถือเป็นคำเสนอเมื่อทางร้านรับชำระเงินถือว่าร้านมีคำสนองรับสัญญาจึงเกิด

ความสมบูรณ์ของคำเสนอตามกฎหมายเยอรมัน

หลักพื้นฐานของกฎหมายเยอรมันกำหนดไว้ว่า "คำเสนอจะต้องมีความชัดเจนและแข็งแกร่ง

4.4 คำเสนอตามกฎหมายไทย

ตามกฎหมายไทยได้กำหนดลักษณะของคำเสนอในเบื้องต้นไว้ดังต่อไปนี้

1. เป็นการแสดงเจตนาขอทำสัญญา

- ก. หากเป็นการแสดงเจตนาทำคำเสนอต่อบุคคลที่อยู่เฉพาะหน้า คำเสนอนั้นจะมีผลก็ต่อเมื่อผู้รับการแสดงเจตนาได้ “ทราบ” การแสดงเจตนาทำคำเสนอนั้น (มาตรา 168)
 - ข. หากเป็นการทำคำเสนอต่อบุคคลซึ่งมิได้อยู่เฉพาะหน้าหรือบุคคลผู้อยู่ห่างโดยระยะทาง คำเสนอนั้นจะมีผลเป็นคำเสนอก็คือเมื่อการแสดงเจตนาทำคำเสนอได้ไป “ถึง” ผู้รับการแสดงเจตนา (มาตรา 169 วรรค 1)
2. คำเสนอต้องเป็นการแสดงเจตนาที่ชัดเจน ไม่ว่าจะเป็นการแสดงเจตนาด้วยวาจา หรือลายลักษณ์อักษรหรือกริยาอาการก็ตาม
 3. คำเสนอต้องมีข้อความชัดเจนแน่นอนพอที่จะทำให้สัญญาเกิดได้หากผู้รับคำเสนอตอบรับกลับมา

อย่างไรก็ดีแม้ว่าในเรื่องของคำเสนอของแต่ละระบบกฎหมายจะมีความแตกต่างกันแต่ก็สามารถสรุปได้ว่าในแต่ละระบบมีองค์ประกอบของคำเสนออยู่สองประการคือ 1. ผู้ทำคำเสนอจะต้องมีเจตนาที่จะผูกนิติสัมพันธ์ และ 2. คำเสนอจะต้องมีความสมบูรณ์พอเพียงที่จะทำคำสนองได้

ซึ่งจะเห็นได้ว่ากฎหมายสัญญาเดิมจะสันนิษฐานว่าการตัดสินใจทำคำเสนอและการยอมรับคำเสนอหรือไม่ยอมรับคำเสนอจะเกิดขึ้นผ่านมนุษย์ โดยมนุษย์จะใช้การพิจารณาเลือกที่จะตัดสินใจตอบรับหรือไม่ แต่เนื่องจากธุรกรรมทางพาณิชย์อิเล็กทรอนิกส์นั้นอาจเป็นระบบอิเล็กทรอนิกส์อย่างสมบูรณ์ซึ่งเครื่องคอมพิวเตอร์จะทำงานแทนมนุษย์โดยสิ้นเชิง ตัวอย่างเช่นโดยการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ (Electronic Record) สัญญาสามารถทำขึ้นระหว่างเครื่องคอมพิวเตอร์โดยที่มนุษย์มิได้รับทราบการทำคำเสนอดังกล่าวเลยก็เป็นได้

5. คำสนอง

5.1 คำสนองตามกฎหมายอังกฤษ

คำสนองตามกฎหมายอังกฤษจะต้องเป็นการยอมรับตามคำเสนอ อาจเป็นคำพูด หรือลายลักษณ์อักษรหรือโดยการกระทำที่แสดงออกว่ายอมรับคำเสนอ หลักโดยทั่วไปแล้วการทำคำสนองไม่สามารถพิจารณาได้จากการนิ่งเฉยนอกจากเป็นเหตุการณ์ที่เป็นข้อยกเว้นจริงๆ

เวลาที่คำสนองมีผล : เพื่อให้คำสนองมีผลจะต้องมีการสื่อสารคำสนองไปยังผู้ทำคำเสนอโดยทั่วไปจะเป็นการทำหนังสือออกกล่าว แต่หากเป็นการเจรจาเฉพาะหน้าหรือทางโทรศัพท์ถือว่าคำสนองมีผลก็ต่อเมื่อบอกกล่าวให้ผู้เสนอได้ยิน หรือพิจารณาตามทางปฏิบัติอันเป็นปกติของผู้เสนอ เช่นมีการรวบรวมเอกสารที่ส่งมาโดยเครื่องเทเล็กซ์หรือเครื่องแฟกซ์ในระหว่างเวลาทำงานโดยปกติทั่วไป

หลักทั่วไปดังกล่าวไม่สามารถนำมาใช้ได้ในกรณีที่ใช้การส่งคำสนองทางไปรษณีย์ ซึ่งในกรณีดังกล่าวถือว่าคำสนองมีผลก็ต่อเมื่อจดหมายที่ติดแสตมป์และจำนวนซองอย่างเหมาะสมได้ส่งลงตู้ไปรษณีย์แล้วถ้าไม่ได้ตกลงกันไว้เป็นอย่างอื่น

5.2 คำสนองตามกฎหมายฝรั่งเศส

ตามหลักทั่วไปของกฎหมายฝรั่งเศสสัญญาจะเกิดขึ้นก็ต่อเมื่อคำเสนอและคำสนองถูกต้องตรงกัน ในส่วนที่เกี่ยวกับผลของการนิ่งเฉยตามกฎหมายของฝรั่งเศสคล้ายกับของอังกฤษ ตามหลักทั่วไปที่กล่าวว่า “He who says nothing does not consent” อย่างไรก็ดีศาล Cour de cassation ได้ถือว่าเป็นปัญหาข้อเท็จจริงที่จะต้องดูจากข้อเท็จจริงอันเป็นประเด็น (Les juges de fond) ในแต่ละคดี โดยจะต้องพิจารณาจากทางปฏิบัติและประเพณีทางการค้าประกอบ ในทางปฏิบัติทางการค้าศาลฝรั่งเศสมักจะยืนยันประเพณีทางการค้าที่ว่า การนิ่งเฉยก่อให้เกิดการยอมรับมากกว่าศาลอังกฤษ ดังที่มีนักกฎหมายท่านหนึ่งกล่าวว่า “ประเพณีปฏิบัติทำให้เห็นว่าการนิ่งเฉยอาจมีความสำคัญเหมือนกับภาษาที่ต้องการสื่อสารความหมายอย่างใดอย่างหนึ่ง”

การทำคำสนองจะต้องมีการสื่อสาร ถ้าต่อมาคู่เจรจาได้ยืนยันเป็นลายลักษณ์อักษรในข้อตกลงที่ได้ตกลงกันโดยปากเปล่า การยืนยันเป็นลายลักษณ์อักษรจะถือว่าเป็นหลักฐานในการตกลงกันและ

สัญญาจะเกิดขึ้นเมื่อมีการเจรจาทางโทรศัพท์และในการเจรจาดังกล่าวคำเสนอได้รับการสนองรับทางโทรศัพท์ ต่างกับกฎหมายอังกฤษที่ถือว่าสถานที่ที่สัญญาโทรศัพท์เพื่อการสนองรับเกิด

สำหรับการสื่อสารกันทางไปรษณีย์นั้นมีการโต้เถียงกันระหว่างสองทฤษฎีคือทฤษฎี Reception และทฤษฎี Expedition ตามทฤษฎี Reception จะถือว่าสัญญาเกิดเมื่อได้รับจดหมาย ส่วนทฤษฎี Expedition จะถือว่าสัญญาเกิดเมื่อจดหมายที่ระบุคำสนองได้ส่งไป

สำหรับสัญญาที่เกิดขึ้นโดยเทเล็กซ์หรือแฟกซ์ ถือว่าสัญญาเกิดเมื่อมีการส่งเทเล็กซ์หรือแฟกซ์และสถานที่ที่สัญญาทำขึ้นคือที่ซึ่งสัญญานแฟกซ์หรือเทเล็กซ์ที่ทำการสนองรับเกิดขึ้น ซึ่งต่างจากกฎหมายอังกฤษที่ต้องการให้มีการรับคำสนองและสถานที่สัญญาเกิดคือสถานที่รับคำสนองดังกล่าว

5.3 คำสนองตามกฎหมายเยอรมัน

คำสนองก็เช่นเดียวกับนิติกรรม Rechtsgeschäft (juristic transaction) โดยทั่วไปแล้วจะมีผลก็ต่อเมื่อสื่อสารไปยังผู้ทำคำเสนอและการสื่อสารดังกล่าวเข้าไปอยู่ใน "เขตแห่งการควบคุม" (Zone of control) ของผู้รับ เช่นคำสนองถูกได้รับตามที่อยู่ในเวลาทำงานปกติ เป็นต้น

ผลของการนิ่งเฉย แม้ว่าหลักทั่วไปการนิ่งเฉยจะมีใช้การแสดงเจตนาแต่ก็มีข้อยกเว้นในกรณีของการยื่นหนังสือยืนยันทางการค้า (Kaufmannische Bestätigungsschreiben) ระหว่างผู้ทำการค้า ส่วนเวลาที่ถือว่าคำสนองมีผล ตามหลักทั่วไปคำสนองจะมีผลก็ต่อเมื่อได้แสดงเจตนาเข้าไปในเขตแห่งการควบคุมของผู้รับ (Art 130 BGB)

5.4 คำสนองตามกฎหมายไทย

ตามกฎหมายไทยกำหนดหลักเกณฑ์ที่เกี่ยวกับคำสนองไว้ดังต่อไปนี้

1. **ความหมาย** คำสนองคือการแสดงเจตนาตอบรับคำเสนอเพื่อที่จะเข้าทำสัญญากับผู้เสนอ

2. เป็นการแสดงเจตนาขอทำสัญญา

- ค. หากเป็นการแสดงเจตนาทำคำสนองต่อบุคคลที่อยู่เฉพาะหน้า คำสนอนนั้นจะมีผลก็ต่อเมื่อผู้รับการแสดงเจตนาได้ "ทราบ" การแสดงเจตนาทำคำสนอนนั้น (มาตรา 168)
- ง. หากเป็นการทำคำสนองต่อบุคคลซึ่งมิได้อยู่เฉพาะหน้าหรือบุคคลผู้อยู่ห่างโดยระยะทาง คำสนอนนั้นจะมีผลเป็นคำสนองก็ต่อเมื่อการแสดงเจตนาทำคำสนอนได้ไป "ถึง" ผู้รับการแสดงเจตนา (มาตรา 169 วรรค 1)

3. การแสดงเจตนาทำคำสนอนนั้น อาจเป็นการขัดแย้งหรือโดยปริยายก็ได้
4. ในคำสนอนนั้นต้องมีความชัดเจน แน่นนอน และไม่มีเงื่อนไข
5. คำสนอนนั้นจะต้องตอบภายในระยะเวลาที่ระบุในคำเสนอ
6. คำสนอนจะต้องกระทำต่อบุคคลที่เจาะจงตัว

จากที่ได้กล่าวมาข้างต้นจะเห็นได้ว่าระบบกฎหมายต่างๆ นั้นยังมีความแตกต่างในรายละเอียดเกี่ยวกับการทำคำเสนอ โดยเฉพาะการนิ่งเฉยจะถือว่าเป็นการทำคำสนองหรือไม่หลายประเทศยังมีความเห็นไม่ตรงกัน และเช่นเดียวกับการทำคำเสนอ ที่กฎหมายสัญญาเดิมจะสันนิษฐานว่าการตัดสินใจทำคำสนองหรือไม่ทำคำสนองจะเกิดขึ้นผ่านมนุษย์ โดยมนุษย์จะทำการพิจารณาเลือกที่จะตัดสินใจตอบรับหรือไม่ แต่เนื่องจากธุรกรรมทางพาณิชย์อิเล็กทรอนิกส์นั้นอาจเป็นระบบอิเล็กทรอนิกส์อย่างสมบูรณ์ซึ่งเครื่องคอมพิวเตอร์จะทำงานแทนมนุษย์โดยสิ้นเชิง ตัวอย่างเช่นโดยการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ (Electronic Record) สัญญาสามารถทำขึ้นระหว่างเครื่องคอมพิวเตอร์โดยที่มนุษย์มิได้รับทราบการทำคำสนองดังกล่าวเลยก็เป็นได้

ตัวอย่างเช่นในคดี Corinthian Pharmaceutical v Lederle Laboratories - "เมื่อ Corinthian ส่งคำสั่ง Corinthian ได้รับเพียง Tracking Number จากเครื่องคอมพิวเตอร์ของบริษัท Telco เพียงแค่ Tracking Number เท่านั้นยังไม่ถือว่าเป็นการสนองรับ

6. "การรับ" (Receipt)

ตามกฎหมายไทยในเรื่องของการทำคำเสนอและคำสนองนั้นจะถือว่าเมื่อคำเสนอและคำสนอง "ถึง" บุคคลที่ต้องการ หรือบุคคลที่อยู่เฉพาะหน้าได้ "ทราบ" ในคำเสนอหรือคำสนองนั้น

โดยหลักเกณฑ์ดังกล่าวไม่สามารถนำมาใช้กับข้อความอิเล็กทรอนิกส์ซึ่งมีความแตกต่างจากข้อความที่ปรากฏบนกระดาษ ข้อความดิจิทัลจะไม่ส่งไปทางการภาพไปยังผู้จุดหมายได้ เมื่อข้อมูลถูกส่งโดยเครื่องคอมพิวเตอร์ของ ก ขั้นแรกจะมีการประมวลผลที่หน่วยความจำ RAM ของเครื่องคอมพิวเตอร์ของ ก และต่อมาจะไปที่ Server ที่เชื่อมต่อกับเครื่องคอมพิวเตอร์ของ ก และต่อมาจะส่งไปยัง Router และ Servers ของเครือข่ายอินเทอร์เน็ต จนกระทั่งระบบคอมพิวเตอร์ของ ข ได้รับ เป็นขั้นตอนเช่นเดียวกับที่ ก ส่งมาหากแต่กลับขั้นตอนกัน

การสื่อสารในรูปแบบนี้ก่อให้เกิดปัญหาดังต่อไปนี้

1. *อะไรคือที่อยู่* ที่อยู่ทางอิเล็กทรอนิกส์นั้นมีความหมายกว้างกว่าที่อยู่ตามความหมายโดยทั่วไป เช่นบุคคลอาจมีที่อยู่ E-mail address ที่แตกต่างกันเพื่อใช้ในวัตถุประสงค์ที่ต่างกันได้ในหน่วยงานราชการหรือหน่วยงานทางธุรกิจ ที่อยู่ของหน่วยงาน ซึ่งอาจต่างกับที่อยู่จริงก็ได้ ปัญหาว่าที่อยู่ใดที่จะก่อให้เกิดผลทางกฎหมายในการทำหนังสือบอกกล่าว
2. *ฟอร์แมทไหน* เมื่อข้อมูลถูกส่งจาก ก ไปยัง ข มันจะถูกทำขึ้นภายใต้การเปลี่ยนแปลงทางเทคนิค Internet Protocol จะแยกข้อความออกเป็นกลุ่ม (Packages) ย่อยๆ ที่ส่งแยกออกจากกันจาก ก ไป ข ยิ่งไปกว่านั้นข้อความอาจถูกเข้ารหัสเพื่อเก็บรักษาความลับ ปัญหาคือว่าข้อความฟอร์แมทไหนที่จะปรากฏและจะถือว่า "ถึง" ผู้รับแล้วหรือถือว่าผู้รับ "ทราบ" แล้ว
3. *ระบบอะไร (What system?)* ณ จุดไหนจึงจะถือว่าข้อความอิเล็กทรอนิกส์จาก ก ส่งไปยัง ข ไม่สามารถบอกได้ชัดเจนมากนักในทางเทคนิคจาก ณ จุดใดจึงจะถือว่าผู้รับข้อมูลได้รับข้อมูลแล้ว ในกรณีของ Electronic Mail การรับจะประกอบไปด้วยขั้นตอนดังต่อไปนี้ 1. ข้อความ

อิเล็กทรอนิกส์ถูกส่งไปยัง Mail Server ที่ผู้รับสามารถเข้าถึงได้ 2. คำสั่งของผู้รับที่จะเข้าถึงข้อความใน Mail Server ในขั้นตอนนี้จะแสดงนัยว่าข้อความถูกทำสำเนาไปยังระบบของผู้รับ เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล แต่ก็ไม่น่าจะแน่นอนเสมอไป 3. ผู้รับแปลงข้อมูลให้สามารถอ่านได้ เช่น โดยแสดงบนจอภาพหรือโดยพิมพ์ออกมา

อย่างไรก็ดีมีผู้เสนอว่าเพียงแต่รับข้อความที่ Mail Server จะถือว่ารับแล้ว โดยไม่คำนึงว่าผู้รับจะเชื่อมต่อเข้าไปยัง Server หรือไม่ หรือไม่ต้องคำนึงว่าการเชื่อมต่อเข้าไปได้จะสามารถทำได้หรือไม่ เช่นเนื่องจากมีปัญหาทางเทคนิคหรือเกิดจากการกระทำของผู้ให้บริการสื่อสารข้อมูล (Service Provider) ความเห็นนี้คล้ายกับหลัก Mailbox Rule

7. การถอนคำเสนอ

7.1 การถอนคำเสนอตามกฎหมายอังกฤษ

ตามกฎหมายอังกฤษ ถ้าคำสัญญาทำขึ้นเพื่อเปิดให้ทำค่านองภายในระยะเวลาที่กำหนด อาจถอนคำเสนอได้ก่อนที่จะมีการทำค่านอง โดยการถอนคำเสนออาจไม่เป็นผลจนกว่าการถอนคำเสนอนั้นจะถึงผู้รับ ในทางธุรกิจการถอนคำเสนอควรที่จะมีผลเมื่อจดหมายบอกถอนคำเสนอถูกเปิดอ่านในที่ทำงานของผู้รับคำเสนอหรือเปิดในทางปกติของธุรกิจหรือในกรณีที่ เป็นเทเล็กซ์หรือโทรสารจะได้รับที่เครื่องในระหว่างเวลาที่เป็นปกติในการประกอบธุรกิจ ไม่เป็นการเพียงพอที่ผู้ถอนคำเสนอจะมีเจตนาที่จะถอนคำเสนอเท่านั้น การถอนจะต้องสื่อสารถึงผู้รับคำเสนอด้วย

7.2 การถอนคำเสนอตามกฎหมายฝรั่งเศส

ตามหลักกฎหมายฝรั่งเศสถือว่าคำเสนอสามารถถอนเวลาใดก็ได้จนกว่าจะมีคำสนองรับ ดังคำกล่าวที่ว่า “คำเสนอก่อนที่จะมีคำสนองไม่มีผลผูกพัน” แต่อย่างไรก็ตามในปัจจุบันศาลก็ได้วางหลักที่เป็นข้อยกเว้นในทางปฏิบัติ ดังต่อไปนี้ 1. หากผู้เสนอได้กำหนดเวลาถึงความสมบูรณ์ของคำเสนอไว้ชัดเจน เขาก็มีหน้าที่ที่กำหนดตามระยะเวลาดังกล่าว เว้นแต่มีการยกเลิกระยะเวลา 2. ถ้าผู้เสนอไม่ได้กำหนดเวลาไว้แต่ได้ถามให้มีการทำค่านองอย่างทันที ศาลจะกำหนดเวลาที่จะต้องยื่นตามคำเสนอให้มีระยะเวลา

เพียงพอที่จะสามารถทำคำสนองได้ 3. ถ้าผู้เสนอไม่ได้กำหนดระยะเวลาไว้แต่ประการใดคำเสนอต้องรักษาไว้ภายในระยะเวลาที่สมควรซึ่งจะกำหนดตามพฤติการณ์รวมทั้งคำนึงถึงประเพณีปฏิบัติในทางการค้า

7.3 การถอนคำเสนอตามกฎหมายเยอรมัน

ตามมาตรา 145-148 ของ BGB คำเสนอที่มีผลผูกพันผู้เสนอและไม่สามารถถอนในระหว่างเวลาที่มีคำเสนอหรือถ้าไม่ได้บอกระยะเวลาให้ทำคำสนองไว้ถือว่าเวลาที่เหมาะสมว่าจะมีคำสนองเกิดขึ้น หลักข้อนี้ได้รับมาจากกฎหมายเก่าของเยอรมัน ข้อยกเว้นมีแต่เพียงว่าหากผู้ทำคำเสนอได้ระบุว่าคำเสนอของตนเป็น "Freibleibend" หมายความว่า "ไม่ผูกพัน" (Without engagement) หรือมีลักษณะคล้ายกับเพียงว่าเป็นคำชี้ชวน (Invitation to treat) เท่านั้น ในอดีตที่ประเทศเยอรมันประสบปัญหาทางเศรษฐกิจและมีสภาวะเงินเฟ้ออย่างรุนแรงหลังสงครามโลกครั้งที่สองข้อยกเว้นดังกล่าวนี้ถือว่ามีความสำคัญและใช้กันอย่างแพร่หลายแต่อย่างไรก็ดีเมื่อในปัจจุบันที่เศรษฐกิจของประเทศเยอรมันมั่นคงขึ้นข้อยกเว้นดังกล่าวนี้ดูเหมือนจะลดความสำคัญลงไป

หลักในเรื่องความรับผิดชอบก่อนเกิดสัญญาที่มาจากหลัก Culpa in contrahendo ซึ่งเริ่มจากงานเขียนอันโด่งดังของ Prof. Ihering ที่ตีพิมพ์ในปี 1861 ในตอนต้นหลักดังกล่าวจะเกี่ยวกับการชดเชยความเสียหายเนื่องจากสัญญาไม่เกิดขึ้นหรืออาจเป็นโมฆะเนื่องจากความสำคัญผิดที่อีกฝ่ายหนึ่งจะต้องรับผิดชอบ ข้อสำคัญความรับผิดชอบดังกล่าวจะอยู่บนพื้นฐานของความไว้วางใจร่วมกัน (Mutual Trust) และความน่าเชื่อถือซึ่ง Prof. Ihering เห็นว่าหน้าที่ดังกล่าวมีมาตั้งแต่ก่อนที่สัญญาจะมีผลใช้บังคับเสียอีก

7.4 การถอนคำเสนอตามกฎหมายไทย

ตามกฎหมายไทยคำเสนอไม่อาจถอนได้ในกรณีดังต่อไปนี้

1. บอกถอนไม่ได้โดยชัดแจ้ง ตามมาตรา 354 ซึ่งบัญญัติว่า "คำเสนอจะทำสัญญาอันบังระยะเวลาให้ทำค้ำนองนั้น ท่านว่าไม่อาจถอนได้ภายในระยะเวลาที่บ่งไว้"
2. บอกถอนไม่ได้โดยปริยาย ตามมาตรา 355 ซึ่งบัญญัติว่า "บุคคลทำคำเสนอไปยังบุคคลอื่นซึ่งอยู่ห่างกันโดยระยะทางและมีได้บ่งระยะเวลาให้ทำค้ำนอง จะถอนคำเสนอของตนเสียภายในระยะเวลาอันควรคาดหมายว่าจะได้รับคำบอกกล่าวค้ำนองนั้น ท่านว่าหาอาจถอนได้ไม่"

อย่างไรก็ดี หลักกฎหมายตามที่ได้กล่าวมาข้างต้นของประเทศต่างๆ นี้ไม่สามารถนำมาใช้ได้กับสัญญาทางอิเล็กทรอนิกส์ได้อย่างชัดเจนนัก เนื่องจากการทำสัญญาทางอิเล็กทรอนิกส์นั้นสามารถเป็นได้ทั้งการติดต่อกันโดยผู้อยู่ห่างระยะทางและเป็นการสื่อสารกันเฉพาะหน้า ฝ่ายที่เห็นด้วยกับการสื่อสารเฉพาะหน้าเห็นว่าระบบ EDI เน้นที่การทำคำเสนอและการทำค้ำนองอย่างทันที เหตุผลดังกล่าวนี้ว่ามีน้ำหนักในกรณีที่เป็นระบบอัตโนมัติแบบสมบูรณ์ที่เครื่องคอมพิวเตอร์สามารถทำงานได้คล้ายกับคนสองคนทำสัญญากัน การเทียบเคียงกับการติดต่อกันทางโทรศัพท์ที่ไม่สามารถทำได้เนื่องจากการรับรู้ในการส่งข้อมูลจะไม่ถึงผู้รับจนกระทั่งข้อมูลได้รับโดยเครื่องคอมพิวเตอร์และแสดงให้เห็นปรากฏบนจอภาพหรือพิมพ์ออกมาจากเครื่องคอมพิวเตอร์

อย่างไรก็ดี ระบบคอมพิวเตอร์รวมทั้งระบบ EDI สามารถออกแบบให้ตรวจสอบปัญหาที่ว่าไม่มีผู้ได้รับรู้ การติดต่อสื่อสารมีปัญหา การออกแบบดังกล่าวสามารถตรวจสอบความถูกต้อง (Verification) การรับข้อมูล ถ้าความสามารถดังกล่าวถูกออกแบบในระบบ อาจสามารถใช้หลักของการติดต่อกันระหว่างบุคคลที่อยู่เฉพาะหน้าได้ ในกรณีที่มีระบบตรวจสอบการรับข้อมูล (Receipt Verification) เป็นส่วนหนึ่งของระบบ ผู้ส่งจะทราบว่ามีการรับหรือไม่รับโดยทันที ขึ้นอยู่กับรูปแบบของการตรวจสอบ ผู้ส่งจะแน่ใจได้ว่าข้อมูลที่ส่งไปสมบูรณ์หรือไม่ ในกรณีดังกล่าวผู้ส่งสามารถแก้ไขความไม่ถูกต้องหรือทำให้ชัดเจนได้อย่างทันที ดังนั้นศาลควรที่จะใช้การติดต่อกับบุคคลที่อยู่เฉพาะหน้า

8. การเกิดของสัญญา (Contract Formation)

ด้วยเหตุผลหลายประการที่มีความจำเป็นที่จะต้องกำหนดให้ได้ว่าสัญญาเกิดขึ้นที่ไหนและเมื่อไร ตัวอย่างเช่น ภาระความรับผิดชอบในค่าเสียหายที่เกิดจากการละเมิดสัญญาอาจขึ้นอยู่กับเวลาที่เกี่ยวพันกับการเกิดสัญญา สถานที่ที่สัญญาได้ทำขึ้นอาจเกี่ยวกับการกำหนดว่ากฎหมายไหนจะใช้บังคับกับสัญญา นอกจากนั้นการพิจารณาในด้าน Logistical และด้านเวลาอาจมีผลสำคัญในแต่ละขั้นตอนของการเกิดสัญญา คำเสนออาจประกาศโดยทั่วไปในช่วงระยะเวลาที่จำกัดอย่างไรก็ดีอาจไปทับซ้อนหลังจากเวลาที่เหมาะสมก็ได้⁴⁵ ในกรณีที่ไม่ได้กำหนดเงื่อนไขในการทำคำเสนออาจจำเป็นที่จะต้องมีการกำหนดว่าเมื่อไรคำเสนอจึงจะมีผลผูกพัน หากพิจารณาถึงคำสนองและการบอกเลิกคำเสนอ เวลาอาจมีส่วนสำคัญเมื่อคำเสนอถึงตัวผู้รับแล้วและไม่สามารถถอนคำเสนอได้

อย่างไรก็ตามมีหลายทฤษฎีที่กำหนดว่าสัญญาเกิดขึ้นเมื่อไรดังต่อไปนี้

1. Declaration Rule ถือว่าสัญญาเกิดขึ้นในขณะหรือสถานที่ที่มีคำสนองรับ
2. Expedition Rule ถือว่าสัญญาเกิดขึ้นในขณะหรือสถานที่ที่คำสนองถูกส่งไป
3. Reception Rule ถือว่าสัญญาเกิดในขณะหรือสถานที่ที่คำสนองถึงที่หมายปลายทาง
4. Information Rule ถือว่าสัญญาเกิดในขณะหรือสถานที่ที่ผู้เสนอได้รับคำสนอง⁴⁶

⁴⁵ โปรดดู Chitty on Contract, Vol.1, (London: Sweet & Maxwell, 1983) paras. 94-96

⁴⁶ Elias, Lieve, "Data security and formation of contracts," paper presented at "Data Security in Computer Networks and the Legal Problems" Conference, Hanover, September 23-24, 1991

นานนับศตวรรษที่ศาลคอมมอนลอว์ได้พัฒนาหลักที่เกี่ยวกับการทำคำสนองต่อคำเสนอโดยทางไปรษณีย์ซึ่งเป็นการสื่อสารโดยอยู่ห่างระยะทาง ในปี 1880 ศาลในคดี *Byrn v Van Tienhoven* กล่าวว่า "ปัจจุบันเป็นที่ยุติว่า คำเสนอที่ได้ทำขึ้นและได้รับการสนองรับทางจดหมายส่งไปโดยบริการไปรษณีย์ สัญญาจะเกิดขึ้นอย่างสมบูรณ์ก็ต่อเมื่อจดหมายที่เป็นคำสนองส่งไปยังไปรษณีย์ ถึงแม้ว่าจะไม่ถึงปลายทางที่หมายเลยก็ตาม"⁴⁷

อย่างไรก็ดีเมื่อพิจารณาถึงการติดต่อสื่อสารทางอิเล็กทรอนิกส์ในระบบเปิดอย่างเช่นอินเทอร์เน็ต นั้นการที่จะระบุสถานที่รับหรือส่งคำสนอง นั้นไม่สามารถทำได้ง่าย กล่าวคือจะใช้สถานที่ใดเป็นตัวกำหนด ไม่ว่าจะเป็นสถานที่ของเครื่อง สถานที่ของคน สถานที่ของหน่วยงาน หรือสถานที่ที่กำหนดตาม E-mail Address ซึ่งสถานที่เหล่านี้อาจมีความแตกต่างกันโดยสิ้นเชิงก็เป็นได้ ประกอบกับหากพิจารณาถึงหลัก Mail Box Rule ในทางอิเล็กทรอนิกส์คำว่า Mail Box ก็มีให้เห็นเด่นชัดเหมือนกับในการบริการไปรษณีย์ ดังนั้นการปรับใช้ทฤษฎีดังที่ได้กล่าวมาข้างต้นจึงไม่ใช่เรื่องที่ย่ายนักสำหรับการสำลัญญาทางอิเล็กทรอนิกส์

นอกจากนั้นเพื่อที่จะให้สัญญาเกิด มีความจำเป็นอย่างยิ่งที่บุคคลที่เกี่ยวข้องจะต้องมีอำนาจที่จะทำข้อผูกพันบริษัทตามสัญญาดังกล่าว ซึ่งอาจก่อให้เกิดปัญหาข้อกฎหมายในกรณีของการใช้ระบบการสื่อสารแบบ EDI แบบสมบูรณ์ที่คำสั่งซื้อสินค้า (คำเสนอ) อาจเกิดขึ้นโดยระบบคอมพิวเตอร์ของบริษัทเมื่อสินค้าในคลังสินค้าของบริษัทลดลงในระดับที่กำหนดไว้ บริษัทดังกล่าวสามารถปฏิเสธในเวลาต่อมาได้หรือไม่ว่าระบบดังกล่าวไม่มีอำนาจทำคำเสนอ

ในบางกรณีคู่สัญญาใช้ระบบการติดต่อสื่อสารแบบ EDI ก็จริงแต่ก็ยังใช้เอกสารในระบบกระดาษแบบเดิมอยู่เพื่อความมั่นใจ หากกรณีเป็นว่าเมื่อคำเสนอทางอิเล็กทรอนิกส์นั้นได้รับแต่ไม่ได้รับเอกสารที่เป็นกระดาษ ในกรณีดังกล่าวการแสดงเจตนาที่ทำกันทางอิเล็กทรอนิกส์จะมีสถานะทางกฎหมายอย่างไร

⁴⁷ (1880) 5 CPD 344 at 348, per Lindey J.

อย่างไรก็ดีหลักกฎหมายในเรื่องของการเกิดของสัญญาที่กำหนดให้คู่สัญญาจะต้องแสดงเจตนาที่จะก่อนิติสัมพันธ์⁴⁸ ปัญหาคือการที่ระบบดังกล่าวมีคำสั่งซื้อสินค้าอัตโนมัติจะถือได้หรือไม่ว่าเป็นการแสดงเจตนาผูกนิติสัมพันธ์หรือไม่

และหากจะพิจารณาถึงประเภทของสัญญาซึ่งอาจแบ่งออกได้เป็นสามประเภทดังต่อไปนี้

1. สัญญาที่ต้องทำอย่างเป็นทางการ (Solemnized Contracts) ที่ต้องการรูปแบบที่เฉพาะเจาะจงถึงจะถือได้ว่าสัญญาดังกล่าวเสร็จและมีความสมบูรณ์ ตัวอย่างเช่นสัญญาซื้อขายที่ดิน
2. สัญญาที่ก่อให้เกิดการโอนกรรมสิทธิ (Real Contract) สัญญาที่จะต้องมี การส่งมอบวัตถุแห่งสัญญา เช่นสัญญาจำนอง

สัญญาที่เกิดขึ้นจากการยินยอมโดยทั่วไป (Consensual Contracts) สัญญาดังกล่าวนี้นี้จะถือว่าสมบูรณ์เพียงเมื่อคู่สัญญาได้ตกลงกัน⁴⁹

ดังนั้นหากไม่มีกฎหมายที่กำหนดถึงสัญญาทางอิเล็กทรอนิกส์โดยตรงสัญญาในแบบสุดท้ายเท่านั้นที่จะสามารถทำได้

ตามกฎหมายอังกฤษมีคดีที่เกี่ยวกับการสื่อสารทางอิเล็กทรอนิกส์ เช่นเทเล็กซ์ ในคดี Entores Ltd. v. Miles Far East Corporation⁵⁰ ที่ตัดสินว่าเนื่องจากลักษณะที่เป็นการสื่อสารที่สามารถตอบโต้ได้อย่างทันที (Instantaneous Nature of Electronic Communications) ให้ถือว่าสัญญาเกิดก็ต่อเมื่อคำสนองส่งถึงผู้เสนอ (Reception Rule)

อย่างไรก็ดีในปัจจุบันศาลอังกฤษยังไม่ได้ตัดสินว่าระบบการสื่อสารแบบ EDI ควรจะถือว่าสัญญาเกิดขึ้นเมื่อคำสนองส่งถึงผู้รับ หรือ Postal Rule หรือ Expedient Rule หรือไม่ ซึ่งคำสนองจะเกิดขึ้นเมื่อ

⁴⁸ Kleinwort Benson Ltd. v. Malaysia Mining Co. [1989] 1 W.L.R. 379, C.A.

⁴⁹ Amory, B. and Mark Schauss, "EDI as a way to perform and conclude contracts," paper presented at COMPAT'88, Feb. 29 Mar. 2, The Hague, Holland

⁵⁰ 2Q.B.327(1955)

ข้อความดังกล่าวเสนอไปยังผู้ให้บริการสื่อสาร (Communication Provider) ได้แนะนำว่าประเด็นดังกล่าวควรที่จะตามเกณฑ์สามประการดังต่อไปนี้ 1. ระดับของการตอบโต้กันอย่างรวดเร็วทันที่ทันใด (Instantaneous) 2. คุณภาพของการโต้ตอบ และ 3. ความปลอดภัยของการติดต่อสื่อสาร⁵¹

9. แบบของสัญญา

ปปพ. มาตรา 456 ระบุให้ “การซื้อขายสังหาริมทรัพย์ถ้ามิได้ทำเป็นหนังสือ และจดทะเบียน ต่อพนักงานเจ้าหน้าที่ท่านว่าเป็นโมฆะ...

อนึ่งสัญญาจะซื้อจะขายหรือจะซื้อทรัพย์สินอย่างใดดังว่ามานี้ก็ดี คำมั่นในการซื้อขาย ทรัพย์สิน เช่นว่านั้นก็ดี ถ้ามิได้มีหลักฐานเป็นหนังสืออย่างใดอย่างหนึ่งลงลายมือชื่อฝ่ายผู้ต้องรับผิดชอบหรือได้วางประจำไว้ หรือได้ชำระหนี้บางส่วนแล้วท่านว่าจะฟ้องร้องบังคับคดีหาได้ไม่

บทบัญญัติที่กล่าวมาในวรรคก่อนนี้ท่านให้ใช้บังคับถึงสัญญาซื้อขายสังหาริมทรัพย์ ที่ตกลงกันเป็นราคาห้าร้อยบาท หรือน้อยกว่านั้นขึ้นไปด้วย”

สำหรับการลงลายมือชื่อและการทำเป็นหนังสือนั้นได้บัญญัติไว้ในประมวลกฎหมายแพ่งและพาณิชย์ของไทย ในมาตรา 9 ว่า

“เมื่อมีกิจการอันใดซึ่งกฎหมายบังคับให้ทำเป็นหนังสือบุคคลผู้จะต้องทำเป็นหนังสือไม่จำเป็นต้องเขียนเอง แต่หนังสือนั้นต้องลงลายมือชื่อของบุคคลนั้น

ลายพิมพ์นิ้วมือ แง่ใด ตราประทับ หรือเครื่องหมายอื่น ท่านองเช่นว่านั้นที่ทำลงในเอกสารแทนการลงลายมือชื่อ หากมีพยานลงลายมือชื่อ รับรองไว้ด้วยสองคนแล้วให้ถือเสมือนกับลงลายมือชื่อ

ความในวรรคสองไม่ใช้บังคับแก่ การลงลายพิมพ์นิ้วมือ แง่ใด ตราประทับ หรือเครื่องหมายอื่น ท่านองเช่นว่านั้น ซึ่งทำลงในเอกสารที่ทำต่อพนักงานเจ้าหน้าที่”

⁵¹ Amory, B. and Mark Schauss, “EDI as a way to perform and conclude contracts,” paper presented at COMPAT’88, Feb. 29 Mar. 2, The Hague , Holland

จะเห็นได้ว่าตัวบททั้งสองมาตราดังกล่าว กล่าวถึง “หนังสือ” และ “เอกสาร” อีกทั้ง “การลงลายมือชื่อที่ทำลงในหนังสือหรือเอกสาร”

นอกจากนั้นคำศัพท์ที่บัญญัติที่ปรากฏอยู่ในพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2525 ให้ความหมายของเอกสารไว้ว่า “เอกสาร” เป็นคำนามหมายความว่า หนังสือที่เป็นหลักฐานและคำว่า “หนังสือ” หมายความว่า เครื่องหมายที่ขีดเขียนแทนเสียงหรือคำพูด ลายลักษณ์อักษร จดหมายที่มีไปมา เอกสาร บทประพันธ์ และได้ปรากฏความหมายอยู่ในประมวลกฎหมายอาญา พ.ศ. 2499 มาตรา 1(7) โดยได้มีบทนิยาม ความหมายของคำว่า “เอกสาร” ว่า “กระดาษ” หรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือรูปแบบอย่างอื่นจะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น”

โดยแบบที่กำหนดตามประมวลกฎหมายแพ่ง แบ่งได้ 4 ประเภทดังนี้

1. ต้องทำนิติกรรมเป็นหนังสือและจดทะเบียนต่อพนักงานเจ้าหน้าที่ เช่นซื้อขาย อสังหาริมทรัพย์ (มาตรา 456 วรรค 1) ขายฝาก (ซึ่งปรับตามมาตรา 456 วรรค 1) แลกเปลี่ยน (มาตรา 519 ปรับเข้ากับมาตรา 456 วรรค 1) ให้่อสังหาริมทรัพย์ (มาตรา 525) จำนอง (มาตรา 714) หนังสือบริคณส์สนธิ (มาตรา 1024) การได้มาซึ่งอสังหาริมทรัพย์ทางนิติกรรม (มาตรา 1299)
2. ต้องจดทะเบียนต่อพนักงานเจ้าหน้าที่ แต่ไม่ต้องทำเป็นหนังสือ เช่น การจดทะเบียนหุ้นส่วนสามัญและหุ้นส่วนจำกัด (มาตรา 1064, 1078) การจดทะเบียนบริษัทจำกัด (มาตรา 1111) การจดทะเบียนฐานะในครอบครัว (ปพพ.บรรพ 5)
3. ต้องทำเป็นหนังสือต่อพนักงานเจ้าหน้าที่แต่ไม่ต้องจดทะเบียน เช่นการทำพินัยกรรมตาม มาตรา 1600

4. ต้องทำเป็นหนังสือ เช่นเรื่องการโอนหนี้ (มาตรา 306), สัญญาเช่าซื้อ (มาตรา 572), ข้อตกลงคดดอกเบี้ยยทบต้น (มาตรา 655), การโอนหุ้น (มาตรา 1129) เป็นต้น หรือพินัยกรรมตามแบบ

จากเรื่องแบบที่กฎหมายกำหนดเห็นว่าพอจะสรุปถึงเอกสารประเภทที่กฎหมายต้องการกำหนดคุ้มครองดังนี้

1. เรื่องเกี่ยวกับอสังหาริมทรัพย์ ไม่ว่าจะเป็นการซื้อขาย แลกเปลี่ยน ให้ ขายฝาก การได้มาซึ่งอสังหาริมทรัพย์ โดยทางนิติกรรม การที่กำหนดห้ามโอนอสังหาริมทรัพย์ หรือ
2. เกี่ยวกับฐานะของบุคคลหรือนิติบุคคล ในเรื่องหุ้นส่วนบริษัท การจดทะเบียนฐานะครอบครัว หรือ
3. เกี่ยวกับเอกสารที่มีมูลค่า เช่นเรื่องการค้ำค้ำเอกสาร ในมาตรา 960-962 หรือเรื่องตัวเงิน หรือการทำพินัยกรรมเอกสารฝ่ายเมือง หรือพินัยกรรมลับ ในมาตรา 1658-1660 เป็นต้น ซึ่งเป็นการยากจะพิสูจน์ถึงเจตนาของผู้ทำเพราะบุคคลผู้มีส่วนได้เสียนั้นจะเกิดขึ้น เมื่อพินัยกรรมมีผลคือผู้ทำได้ตายไปแล้ว
4. เกี่ยวกับผลซึ่งกระทบกับคนหมู่มากการทำเป็นหนังสือ เช่นเรื่องการเช่าซื้อ การตกลงคดดอกเบี้ยยทบต้น เรื่องตัวเงินต่างๆ

จากที่ได้กล่าวมาข้างต้นนั้นจะเห็นได้ว่าเรื่องแบบเป็นเรื่องทางนโยบายมหาชน ที่มีพัฒนาการมายาวนาน ต่อไปนี้จะเป็นการเปรียบเทียบให้เห็นว่าเอกสารอิเล็กทรอนิกส์นั้น สามารถสนองต่อนโยบายมหาชนเหล่านี้ได้หรือไม่ โดยจะพิจารณาถึงนโยบายต่อนโยบายของเอกสารที่เป็นกระดาษและเอกสารทางอิเล็กทรอนิกส์อย่างเปรียบเทียบ

ก. เอกสารที่เป็นกระดาษแบบเดิม

เอกสารที่เป็นกระดาษ : โดยทั่วไปสังคมมักคุ้นเคยกับการยอมรับและการใช้สัญญาที่เขียนขึ้นบนกระดาษ

เอกสารทางอิเล็กทรอนิกส์ : เช่นเดียวกับทุกๆ สิ่งในชีวิต วิธีการดำเนินชีวิตแบบเดิมมักจะถูกแทนที่โดยวิถีชีวิตแบบใหม่ที่สะดวกและประหยัดกว่า การใช้กระดาษจะส่งผลให้ไม่ประหยัดต้นทุนหากเทียบกับการใช้เอกสารทางอิเล็กทรอนิกส์ นโยบายทางมหาชนโดยทั่วไปจำเป็นต้องพิจารณาถึงความได้เปรียบในเชิงการแข่งขันในการนำเอาเอกสารอิเล็กทรอนิกส์มาใช้ เนื่องจากสามารถทำให้การดำเนินธุรกิจเป็นไปอย่างรวดเร็ว ถูกต้อง มีประสิทธิภาพและประหยัด

การทำเป็นลายลักษณ์อักษร (Writing) จะเป็นการพิสูจน์เจตนาของคู่สัญญา

เอกสารที่เป็นกระดาษ : เอกสารที่เป็นกระดาษจะแสดงให้เห็นว่าผู้เป็นฝ่ายในสัญญาามีเจตนาที่จะทำสัญญา

เอกสารทางอิเล็กทรอนิกส์ : เนื่องจากเอกสารทางอิเล็กทรอนิกส์จะต้องทำขึ้นโดยบุคคลที่มีความเกี่ยวข้องกันในช่วงเวลาใดเวลาหนึ่ง จึงสามารถใช้เป็นหลักฐานยืนยันการแสดงเจตนาได้เช่นเดียวกับที่กระดาษสามารถทำได้

“การทำเป็นลายลักษณ์อักษร” เป็นพยานหลักฐานในการมีอยู่ถึงข้อผูกพันตามสัญญา

เอกสารที่เป็นกระดาษ : เอกสารที่เป็นกระดาษสามารถมีอยู่แยกต่างหากจากความรู้สึกของคู่สัญญา และสามารถใช้เป็นวิธีพิสูจน์อย่างเป็นรูปธรรม (Objective Means) ในการกำหนดเงื่อนไขและข้อกำหนดของข้อตกลงที่พิพาทกัน ดังนั้นการที่ผู้ค้นหาคำจริงสามารถตรวจสอบและตีความข้อกำหนดของสัญญาดังกล่าวอย่างเป็นเอกเทศจะถือว่ามีส่วนช่วยที่มีค่าสำหรับการตีความสัญญา

เอกสารทางอิเล็กทรอนิกส์ : ในขณะที่เอกสาร EDI มีข้อจำกัดในรูปแบบและเนื้อหามากกว่ากระดาษ แต่เอกสาร EDI ก็ยังสามารถแสดงเนื้อหาของเงื่อนไขและข้อกำหนดของสัญญา คู่ความจะไม่ยุ่งยากมากนักในการพิสูจน์ถึงเงื่อนไขและข้อผูกพันตามสัญญาที่ปรากฏในเอกสารอิเล็กทรอนิกส์แต่อย่างใด อย่างไรก็ตามรูปแบบในการเสนอข้อมูลของเอกสารอิเล็กทรอนิกส์อาจไม่เป็นที่คุ้นเคยนัก แต่ก็ไม่ได้

เป็นสาระสำคัญนักหากสามารถสื่อให้เข้าใจความหมายได้ เอกสารที่เป็นกระดาษบางอย่างก็มีรูปแบบการเขียนที่คนโดยทั่วไปไม่สามารถเข้าใจได้ง่ายนัก เช่นเอกสารที่เกี่ยวกับบัญชีและการเงิน เป็นต้น

“ลายลักษณ์อักษร” ในฐานะที่ใช้ป้องกันการฉ้อโกง การเบิกความเท็จ และการสมรู้ร่วมคิด

เอกสารที่เป็นกระดาษ : เอกสารที่เป็นกระดาษสามารถทดสอบให้เป็นที่มั่นใจได้ว่าเอกสารที่เป็นปัญหานั้นไม่ได้ถูกแก้ไขเปลี่ยนแปลงและมีความเกี่ยวข้องกับคู่พิพาทที่เป็นฝ่ายในสัญญา ตัวอย่างเช่น “ลายลักษณ์อักษร” “กระดาษ” “น้ำหมึก” และ “ลายมือชื่อ” เป็นต้น สามารถถูกตรวจสอบความถูกต้องแท้จริงได้

เอกสารที่เป็นอิเล็กทรอนิกส์ : หากมีระบบรักษาความปลอดภัยที่เหมาะสมจะสามารถแสดงให้เห็นได้ว่าการตรวจสอบความถูกต้องแท้จริงจะทำได้ดีกว่าเอกสารที่เป็นกระดาษเสียอีก

ความสะดวกในการพิจารณาคดี (Judicial Economy)

เอกสารที่เป็นกระดาษ : ศาลยินดีที่จะใช้กระดาษมากกว่าเนื่องจากค่อนข้างง่ายที่จะพิสูจน์และอธิบาย มากกว่าเทคโนโลยีใหม่ (เช่น EDI) เนื่องจากศาลอาจใช้เวลาไม่มากนักในการตรวจสอบ

เอกสารอิเล็กทรอนิกส์ : ในกรณีนี้ที่เอกสารมีจำนวนมาก เอกสารทางอิเล็กทรอนิกส์จะประหยัดมากกว่าในการทำซ้ำหรือจัดการมากกว่าเอกสารที่เก็บในรูปของกระดาษ ตัวอย่างเช่น แผ่นดิสก์ (Compact disk) หนึ่งแผ่นที่สามารถเก็บเอกสารได้ถึง 100,000 ฉบับสามารถค้นและจัดการได้อย่างทันที หากเทียบกับเอกสารที่เป็นกระดาษจำนวน 100,000 ฉบับ

การเก็บรักษาเอกสาร

เอกสารที่เป็นกระดาษ : เอกสารที่เป็นกระดาษหากเก็บรักษาไว้อย่างดีจะสามารถอยู่ได้ถึง 100 ปี

เอกสารอิเล็กทรอนิกส์ : เอกสารอิเล็กทรอนิกส์ที่เก็บในแถบแม่เหล็กอย่างเหมาะสมสามารถอยู่ได้ถึง 10 ปี แม้ว่าระยะเวลาจะไม่นานเท่ากระดาษก็ยาวนานพอเพียงที่จะใช้งาน อย่างไรก็ตาม ใ้คงมี

เอกสารอิเล็กทรอนิกส์ใช้พื้นที่ในการเก็บน้อยมากและง่ายต่อการค้นหา ใช้เงินไม่มากนักและง่ายต่อการทำสำเนา

จากที่ได้กล่าวมาข้างต้นจะเห็นได้ว่าแม้ว่าเอกสารอิเล็กทรอนิกส์จะสามารถสนองตอบต่อนโยบายมหาชนในด้านต่างๆ ได้ไม่แพ้เอกสารที่เป็นกระดาษ แต่กฎหมายที่ใช้บังคับอยู่ก็ถือเป็นอุปสรรคในการนำเอาเอกสารอิเล็กทรอนิกส์มาใช้เช่นเดียวกันกับกรณีของลายมือชื่อที่กำหนดไว้ตามกฎหมายก็มีได้เปิดช่องให้นำเอาลายมือชื่ออิเล็กทรอนิกส์มาใช้ได้แต่อย่างไร

โดยต่อไปนี้เป็นตัวอย่างการลงลายมือชื่อหรือการแสดงการยอมรับในรูปของข้อความทางอิเล็กทรอนิกส์⁵²

From Line ข้อความที่ส่งโดย e-mail โดยปกติมักจะมีบรรทัดที่ว่า “จาก” ในตอนต้นของเอกสารที่แสดงว่าผู้ส่งข้อความระบุว่าใครเป็นผู้ส่งข้อความมา โดยปกติแล้วผู้ส่งมักจะวางระบบให้บันทึกชื่อผู้ส่งโดยอัตโนมัติ ผู้ส่งจะมีเจตนาให้ From line เป็นลายมือชื่อหรือไม่ขึ้นอยู่กับพฤติการณ์แวดล้อมกรณีว่าเขาต้องการเช่นนั้นหรือไม่

Mouse Clicks การติดต่อแบบสามารถโต้ตอบกันอย่างทันทีทันใด (Real-time, interactive environment) อย่างเช่น อินเทอร์เน็ต ผู้ที่ท่องไปบนไซเบอร์สเปซ (Cyberspace Traveller) อาจแสดงการยอมรับผูกพัน โดยการกดปุ่มใดปุ่มหนึ่งที่เป็นสัญลักษณ์ว่า “ตกลง” ตัวอย่างเช่น ก่อนการเข้าไปในเว็บไซต์ที่ให้เข้าถึงงานอันมีลิขสิทธิ์ ในเว็บไซต์ดังกล่าวจะมีข้อความว่า “ถ้าคุณตกลงตามเงื่อนไขของสัญญาให้สิทธินี้ กรุณาคลิกที่นี่”

DUNS Number การส่งข้อความในรูปแบบของ EDI โดยปกติแล้วจะระบุตัวผู้ส่งโดยใช้หมายเลข DUNS ซึ่งก็หมายถึงหมายเลขที่ใช้โดยทั่วไป (เช่นหมายเลขประจำตัวประกันสังคม) ภายใต้สถานะการณ

⁵² โปรดดู Benjamin Wright and Jane K. Winn, The Law of Electronic Commerce, Aspen Law & Business, New York, 1997, pp. 14-3 – 14-5

ดังกล่าวความสัมพันธ์ของคู่ค้าที่ใช้ EDI หมายเลขดังกล่าวนี้อาจทำให้ผู้รับรู้ว่าใครเป็นผู้ส่งข้อความมา นอกจากนั้นยังมีวิธีการอื่นๆ ที่ป้องกันให้ผู้ที่ไม่สุจริตมาใช้หมายเลขดังกล่าวในการส่งข้อมูล EDI เช่นการและเปลี่ยนคำยืนยันหรือการส่งข้อมูลกลับคืน (Feedback) เพื่อยืนยันอื่นๆ หมายเลข DUNS ดังกล่าวนี้อาจสามารถใช้เป็นลายมือชื่อของผู้ส่งได้ถ้าหากผู้ส่งมีเจตนาให้เป็นเช่นนั้น เช่นตกลงไว้ในสัญญาแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์

E-mail Closing บางกรณีผู้ส่งข้อความ E-mail มักจะลงท้ายข้อความด้วยคำที่มีความหมายชัดเจนว่า “ลงนาม : สมบัติ แสงสว่าง” หรือระบุชัดว่า “ชื่อของข้าพเจ้าตอนท้ายข้อความนี้คือลายมือชื่อของข้าพเจ้าและแสดงถึงว่าข้าพเจ้าได้ตกลงตามนั้น-สมบัติ แสงสว่าง”

ลายมือชื่อดิจิตอล ในรูปของรหัสหรือกุญแจคู่ที่เรียกว่ากุญแจลับหรือกุญแจสาธารณะ ที่มีความเกี่ยวเนื่องกันทางคณิตศาสตร์ แต่ก็ไม่สามารถทำลอกเลียนแบบซึ่งกันและกันได้ ในปัจจุบันถือเป็นเทคโนโลยีทางด้านลายมือชื่อที่มีความปลอดภัยเป็นอย่างมาก

Biometrics ผู้ส่งข้อความสามารถแนบท้ายข้อความด้วยข้อมูลที่เป็นสัญลักษณ์ของผู้ส่ง เช่นลายพิมพ์นิ้วมือ หรือลายพิมพ์เยื่อบุตา (Retina Scanning) เป็นต้น

ในเรื่องแบบดังที่ได้กล่าวมานี้ถือได้ว่าเป็นอุปสรรคอย่างมากในการทำสัญญาทางอิเล็กทรอนิกส์ซึ่งเป็นกระบวนการที่มีความสำคัญอย่างยิ่งของพาณิชย์อิเล็กทรอนิกส์

ในกฎหมายของประเทศฝรั่งเศส (รวมทั้งเบลเยียม) ตามมาตรา 1341 ของประมวลกฎหมายแพ่ง นิติกรรมจะต้องทำเป็นลายลักษณ์อักษรและลงลายมือชื่อ ในสหรัฐฯ The Statute of Frauds กำหนดให้สัญญาซื้อขายที่มีมูลค่ากว่า 500 เหรียญ จะต้องทำเป็นลายลักษณ์อักษรในอังกฤษสัญญาซื้อขายที่ดินจะไม่สามารถบังคับหากไม่ได้ทำเป็นลายลักษณ์อักษรและลงนามโดยคู่สัญญา (35)

ข้อกำหนดดังกล่าวส่งผลให้เกิดปัญหาดังต่อไปนี้

1. ข้อกำหนดในการทำเป็นลายลักษณ์อักษรสามารถทำได้โดยการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI) ในกรณีที่ข้อมูลถูกส่งโดยเทเลเมติกส์และการติดต่อดังกล่าวถูกบันทึกในรูปแบบข้อมูล คอมพิวเตอร์ที่สามารถอ่านได้หรือไม่

2. วิธีการทางอิเล็กทรอนิกส์สามารถใช้ลงนามตามข้อกำหนดของกฎหมายได้หรือไม่
3. คู่สัญญาสามารถตกลงให้ใช้วิธีการทางอิเล็กทรอนิกส์แทนคำว่า "ลายลักษณ์อักษร" และ "ลงลายมือชื่อ" หรือไม่
4. การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์สามารถใช้แทนเอกสารทางธุรกิจบางอย่าง เช่น ใบตราส่ง (Bill of Lading) ได้หรือไม่

เอกสารคอมพิวเตอร์ในฐานะที่เป็นลายลักษณ์อักษร (Writing)

ตามประมวลแห่งของฝรั่งเศส มาตรา 1341 กำหนดให้นิติกรรมต้องทำเป็นลายลักษณ์อักษร ดังนั้น เอกสารที่ทำโดย EDI ดูเหมือนว่าจะไม่สามารถใช้บังคับได้ อย่างไรก็ตามข้อยกเว้นที่ดูเหมือนจะไม่เป็นปัญหาในการยอมรับ EDI ในฐานะเป็นลายลักษณ์อักษรดังต่อไปนี้

1. หากมูลค่าตามสัญญาต่ำกว่า 5000 ฟรังก์ในฝรั่งเศสและ 3000 ฟรังก์ในเบลเยียมก็สามารถจะทำได้โดยวิธีใดก็ได้
2. มาตรา 1341 ใช้เฉพาะกรณีตามประมวลกฎหมายแพ่งเท่านั้น ไม่รวมถึงเรื่องทางพาณิชย์ซึ่งส่วนใหญ่ EDI จะเป็นเรื่องทางพาณิชย์จึงมีผลสมบูรณ์
3. มาตรา 1341 อาจได้รับการยกเว้นหากทำเป็นข้อตกลงยกเว้น
4. ข้อกำหนดในการให้ลงนามและทำเป็นลายลักษณ์อักษรอาจได้รับการยกเว้นในกรณีที่มีการหาพยาน หลักฐานที่เป็นลายลักษณ์อักษรเป็นการ "พ้นวิสัย" (Material impossibility)

จึงเห็นว่า⁵³ ข้อยกเว้นที่กล่าวมาข้างต้นสามารถใช้ในการติดต่อสื่อสารกันทาง EDI ได้ทั้งหมด ส่งผลให้ Amory และ Poullert สรุปว่า "หลักการลงลายมือชื่อและทำเป็นลายลักษณ์อักษรมีข้อยกเว้นมากมายจนไม่ทำให้ EDI มีปัญหา"

10. การตีความสัญญา

⁵³ Chamoux, "La Loi du 12 Juillet 1980: une ouverture sur de nouveaux moyens de preuve" JCP 1980 II 1391

แม้ว่าหลักการตีความข้อความอิเล็กทรอนิกส์จะไม่ต่างจากการตีความกฎหมายโดยทั่วไป แต่จากลักษณะทางเทคโนโลยีที่มีลักษณะเฉพาะอาจต้องมีวิธีการที่แตกต่างกัน เนื่องจากขาด เจตนาเบื้องต้น ข้อความ อย่างไรก็ดีเนื่องจากเนื้อหาของข้อความอิเล็กทรอนิกส์นั้นมีน้อยส่วนใหญ่จึงมักจะอ้างถึงข้อความอื่นๆ ที่มีได้ระบุไว้ในสัญญา (Incorporation by reference) เมื่อข้อความอ้างถึงข้อความอื่นที่ไม่ได้นิยามไว้ในสัญญา ปัญหาทางกฎหมายเกิดขึ้นว่าข้อความหรือคำนิยามไหนจะถือว่าเป็นส่วนหนึ่งของข้อตกลงในโลกของข้อตกลงที่ใช้กระดาษมักจะมีการอ้างถึง INCOTERMS ซึ่งก็เป็นที่ยอมรับกันโดยทั่วไป สำหรับกรณีของพาณิชย์อิเล็กทรอนิกส์ มีข้อสังเกตดังต่อไปนี้ 1. ไม่มีข้อความมาตรฐานที่เป็นที่ยอมรับกันโดยทั่วไปในกรณีของข้อความทางอิเล็กทรอนิกส์ 2. ข้อจำกัดทางอิเล็กทรอนิกส์ในกรณีของ EDI ที่สามารถบรรจุตัวอักษรได้สูงสุด 64 ตัว

11. กฎหมายที่จะใช้บังคับ (Choice of Law)

จากที่ได้กล่าวมาข้างต้นจะเห็นได้ว่าการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยเฉพาะในส่วนที่เกี่ยวข้องกับพาณิชย์อิเล็กทรอนิกส์ที่ทำบนเครือข่ายแบบเปิดนั้น โดยพื้นฐานแล้วจะเป็นการทำธุรกรรมที่ไม่สามารถกำหนดได้ชัดว่าธุรกรรมดังกล่าวจะต้องเกิดบนแผ่นดินไทยเท่านั้น เนื่องจากเป็นระบบเปิดการทำธุรกรรมจึงอาจเกิดขึ้นได้จากทั่วทุกมุมโลก ซึ่งมักมีผู้กล่าวว่าบนไซเบอร์สเปซนั้นไม่มีพรมแดน ในขณะเดียวกันบุคคลที่เราทำการติดต่อก็ไม่สามารถระบุตัวได้อย่างชัดเจนว่าเป็นใครและมีสัญชาติอะไร รวมทั้งถิ่นที่อยู่หรือภูมิลำเนาที่ถาวรก็ไม่สามารถทราบได้แน่ชัด เนื่องจากจะทราบได้ก็แต่เพียง E-Mail Address ที่ไม่สามารถยืนยันข้อเท็จจริงที่กล่าวมาได้อย่างสมบูรณ์

ประกอบกับการทำสัญญาที่เกี่ยวข้องกับข้อมูลนั้นในบางกรณีการส่งมอบสินค้าหรือการปฏิบัติตามสัญญาหรือการชำระหนี้ก็สามารถทำได้บนเครือข่ายซึ่งก็ไม่สามารถทราบได้อย่างแน่ชัดว่าการปฏิบัติตามสัญญานั้นเกิดขึ้น ณ. ที่ใด

เมื่อองค์ประกอบพื้นฐานไม่ว่าจะเป็นเรื่องของ สัญชาติ สถานที่ที่ทำนิติกรรม สถานที่ที่ปฏิบัติตามสัญญา ภูมิลำเนาหรือถิ่นที่อยู่ หรือดินแดน เป็นต้น ไม่สามารถระบุได้อย่างชัดเจน ปัญหาดังต่อไปนี้

1. ศาลจะมีเขตอำนาจศาลหรือไม่

2. กฎหมายที่จะใช้บังคับ (Choice of Law)
3. การบังคับตามคำพิพากษา (Enforcement of Foreign Judgement) จะทำอย่างไร

กลไกสองประการที่น่าจะทำได้คือการกำหนดกฎหมายที่ใช้บังคับให้ชัดเจนในสัญญา และประเทศต่างๆควรที่จะต้องร่วมมือกันในการลงโทษผู้กระทำความผิดที่เกี่ยวกับพาณิชย์อิเล็กทรอนิกส์

บทที่ 5

ความรับผิดชอบและการกระจายความรับผิดชอบ

(Attribution Issue)

1. ความรับผิดชอบ

ผู้ที่จะต้องรับผิดชอบในกระบวนการการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์จะมีดังต่อไปนี้

1. ผู้ทำข้อความเสนอทางอิเล็กทรอนิกส์ (Originator of the message)
2. ผู้ให้บริการการสื่อสาร (Provider of the communications facility)
3. ผู้รับข้อมูล

1.1 ความรับผิดชอบของผู้ให้บริการการสื่อสาร

ระดับของความรับผิดชอบของผู้ให้บริการการสื่อสารจะแตกต่างกันไปตามแต่กรณีที่เกิดขึ้น ความรับผิดชอบของผู้ให้บริการการสื่อสารมี เช่น

1. นำส่งข้อมูลในรูปแบบ (Format) และโปรโตคอล ที่ถูกต้อง
2. ดูแลไม่ให้ข้อมูลต้องเสียหาย
3. รักษาความปลอดภัยว่าข้อมูลจะส่งถึงมือผู้รับ
4. รักษาความลับและความปลอดภัยของข้อมูล

ความล้มเหลวในการปฏิบัติตามหน้าที่ของผู้ให้บริการการสื่อสารข้อมูลตามที่กำหนดไว้ข้างต้นอาจก่อให้เกิดความเสียหายกับผู้ส่งข้อมูลหรือผู้รับข้อมูลและอาจก่อให้เกิดความรับผิดชอบในส่วนของผู้ให้บริการข้อมูล อย่างไรก็ตามผู้ให้บริการการสื่อสารมักจะยกเว้นความรับผิดชอบมากที่สุดเท่าที่จะทำได้ กฎหมายคงต้องเข้ามาดูแลการยกเว้นความรับผิดชอบดังกล่าว ตัวอย่างเช่น ในกรณีที่ข้อความสั่งซื้อสินค้าถูกส่งให้กับผู้รับ หากการส่งเกิดมีปัญหาก็อาจส่งผลให้เกิดความเสียหายได้ทั้งผู้ส่งข้อมูลและผู้รับข้อมูล ผู้ส่งข้อมูลอาจไม่

สามารถทำการขายสินค้าเนื่องจากไม่สามารถได้รับสินค้าเพื่อที่จะนำมาขายต่อได้ ผู้รับอาจได้รับความเสียหายอย่างทันทีเนื่องจากไม่สามารถขายสินค้าได้ การพิจารณาดังกล่าว สามารถนำมาใช้กับข้อมูลที่มีปัญหาหรือข้อมูลที่ไม่ถูกต้อง

การรักษาความลับของข้อมูลก็เป็นหน้าที่สำคัญของผู้ให้บริการการสื่อสารเช่นกันซึ่งอาจก่อให้เกิดความรับผิดได้ นอกจากนั้นอาจเกิดจากการที่ส่งข้อมูลผิด ซึ่งส่วนใหญ่ความสัมพันธ์ระหว่างผู้ให้บริการการสื่อสารกับผู้รับหรือผู้ส่งข้อมูลมักกำหนดไว้เป็นข้อตกลง

1.2 ความรับผิดชอบของผู้ส่งข้อมูล

โดยทั่วไปแล้วหน้าที่ความรับผิดชอบของผู้ส่งข้อมูลมักเป็นไปตามข้อกำหนดของสัญญา แต่อย่างไรก็ดีความรับผิดชอบโดยทั่วไปมีดังนี้

1. การนำส่งข้อมูลในรูปแบบ (Format) และโปรโตคอลที่ถูกต้อง
2. รักษาไม่ให้ข้อมูลต้องมีปัญหา (Corrupt)
3. ป้องกันไม่ให้ข้อมูลสามารถส่งไปยังผู้รับได้
4. ประกันว่าข้อมูลทำขึ้นโดยมีอำนาจ (Message if properly authorised)
5. ประกันว่าข้อมูลเป็นไปตามที่ได้ตกลงกันได้
6. ดูแลเรื่องลิขสิทธิ์
7. เก็บรักษา Data Log
8. รักษาความลับและความปลอดภัยของข้อมูลที่ได้รับ

ภาระของผู้ส่งข้อมูลจะต้องประกันเรื่องความปลอดภัยของข้อมูลให้มีการป้องกันการรั่วไหลของข้อมูลโดยไม่ได้รับอนุญาต ซึ่งอาจเกี่ยวกับการเปลี่ยนรหัสผ่าน (Password) บ่อย ๆ การทำประกันความรับผิดดังกล่าวก็อาจเป็นสิ่งที่จำเป็น

1.3 ความรับผิดชอบของผู้รับ

โดยทั่วไปแล้วความรับผิดชอบของผู้รับมีดังต่อไปนี้

1. แน่ใจว่าข้อมูลดังกล่าวส่งถึงผู้รับจริง
2. รับและพิสูจน์ความถูกต้องของข้อมูล
3. รักษาความลับและความปลอดภัยของข้อมูล

1.4 ความปลอดภัย (Security) และไวรัสคอมพิวเตอร์

กฎหมายว่าด้วยสัญญาในปัจจุบันไม่ได้กำหนดว่าผู้ใดจะมีหน้าที่รับผิดชอบเกี่ยวกับการบุกรุกทางอิเล็กทรอนิกส์ (Electronic intrusion) การกำหนดไว้ในสัญญาจะช่วยแก้ปัญหาได้ว่าใครมีหน้าที่และความรับผิดชอบเกี่ยวกับความไม่ปลอดภัย (Insecurities) และการทำลายของไวรัสคอมพิวเตอร์ ในกรณีที่ข้อสัญญาไม่ได้กำหนดไว้ ควรที่จะแยกออกเป็นสองกรณี กรณีแรกเป็นเรื่องที่เกี่ยวกับการส่งมอบผลิตภัณฑ์หรือข้อมูลดิจิทัลจากคู่สัญญาฝ่ายหนึ่งไปยังคู่สัญญาอีกฝ่ายหนึ่งที่มีวัตถุที่เป็นอันตรายทางอิเล็กทรอนิกส์ (Harmful electronic material) ส่วนกรณีที่สองเป็นการทำลายโดยไวรัสคอมพิวเตอร์ที่มาทางเครือข่ายจากภายนอก

2. การกระจายความรับผิด (Attribution Issues)

ในการทำธุรกรรมทางอิเล็กทรอนิกส์ ความคิดในเรื่องของการทำคำเสนอและคำสนองจำเป็นต้องพิจารณาถึงความเสี่ยงที่อาจเกิดขึ้นได้จากบุคคลภายนอกหรือจากระบบคอมพิวเตอร์เอง

โดยทั่วไปแล้วพัฒนาการทางกฎหมายและแนวคำพิพากษาได้ถูกพัฒนาขึ้นเพื่อรองรับกับกรณีที่มีการฉ้อโกงหรือ ลักลอบผิด ที่อยู่บนพื้นฐานว่าใครมีหน้าที่หรือโอกาสในการป้องกันความเสียหายตามกระบวนการที่กำหนดไว้

ในกรณีที่การทำธุรกรรมทางอิเล็กทรอนิกส์เกี่ยวข้องกับผู้บริโภค การกระจายความเสี่ยง (allocation of Risk) ที่เกิดจากความผิดพลาด การฉ้อโกง หรือ การปลอมแปลง (False attribution) ได้รับการพัฒนาในการที่ตอบสนองกับการป้องกันความเสี่ยงของ System Operator ที่จะป้องกันความเสียหายได้ดีกว่าความสามารถของผู้บริโภค สิ่งนี้เกิดขึ้นกับระบบการโอนเงินทางอิเล็กทรอนิกส์ภายใต้กฎหมายของสหรัฐ ตัวอย่างเช่น เครดิตหรือบัตรที่มีลักษณะเช่นเดียวกัน จำนวนเงินที่ผู้บริโภคจะต้องรับผิดชอบจะมีจำกัดและโอกาสที่ผู้บริโภคจะต้องรับผิดชอบก็จะต้องมีอยู่อย่างจำกัดในกรณีที่ผู้บริโภคพยายามที่จะป้องกันความเสียหายแน่นอนในกรณีดังกล่าวความเสี่ยงของผู้บริโภคจะมาพร้อมกับระบบการบอกกล่าว (ไม่ว่าจะเป็นลายลักษณ์อักษรหรือทางอิเล็กทรอนิกส์) ซึ่งจะทำให้สามารถค้นพบความผิดพลาดได้ทันเวลา

โดยทั่วไปแล้วโครงสร้างระบบเปิดอาจมีปัญหาคู่ครองผู้บริโภคและมีประเด็นปัญหาในทางนโยบายอีกหลายประการที่จะต้องวิเคราะห์ดังต่อไปนี้

1. จะกระจายความเสี่ยงที่เกิดขึ้นอย่างไร?

การกระจายความเสี่ยงจะต้องทำอย่างระมัดระวัง ที่จะไม่ให้เกิดความเป็นธรรมกับผู้ที่ต้องรับภาระดังกล่าวมากเกินไป

2. บทบัญญัติอย่างไรควรที่จะมีสำหรับการคุ้มครองผู้บริโภค?

ความเสี่ยงที่เกิดขึ้นจากพาณิชย์อิเล็กทรอนิกส์นั้นควรที่จะให้ความสำคัญกับผู้บริโภคที่จะไม่ตกเป็นเครื่องมือของบุคคลที่ไม่สุจริตหรือความเสี่ยงที่อาจเกิดขึ้น ควรวางกลไกที่เหมาะสมในการคุ้มครองผู้บริโภคในเรื่องดังกล่าว

3. ในกรณีที่เกี่ยวกับ Hacker จะทำอย่างไร?

ทางเลือกคือ ให้ความเสียหายตกอยู่กับผู้ที่ถือว่าเป็นผู้ส่งข้อมูล หากมีส่วนในความผิดที่ปล่อยให้ Hacker เข้ามาใช้ข้อมูล

บทที่ 6

พยานหลักฐานอิเล็กทรอนิกส์ (Electronic Evidence)

1. ความทั่วไป

เอกสารมีวัตถุประสงค์หลายประการ วัตถุประสงค์ที่ธรรมดามากที่สุดคือใช้เอกสารหลักฐานภายในหน่วยงานซึ่งจะมีประโยชน์สำหรับการตรวจสอบสต็อกสินค้าและกระบวนการทางการเงินและการคลังของบริษัท นอกจากนั้นเอกสารยังจะบันทึกและแสดงหลักฐานในการทำธุรกรรม โดยเฉพาะอย่างยิ่งเป็นเอกสารสัญญาที่มีการลงนาม กฎหมายถือว่าการลงนามดังกล่าวมีผลให้เอกสารดังกล่าวมีผลผูกพันทางสัญญา เอกสารยังสามารถใช้เป็นพยานหลักฐานในกรณีที่มีข้อพิพาทที่เกี่ยวกับการปฏิบัติตามสัญญา ซึ่งจะทำให้คู่สัญญามีความรู้สึกมั่นใจที่จะมีหลักฐานใช้ยืนยัน นอกจากนั้น เอกสารยังช่วยให้ความมั่นใจกับบุคคลที่สาม ยกตัวอย่างเช่นในกรณีที่พ่อค้าซื้อสินค้าในราคา CIF (cost, insurance, freight) และต่อมาเขาอาจขายสินค้าที่ซื้อมันในขณะที่ยังอยู่ในทะเลและผู้ซื้ออีกสามารถใช้ใบตราส่งสำหรับเป็นพยานหลักฐานของการมีอยู่และเงื่อนไขของสินค้าที่ได้ซื้อไว้ เอกสารยังมีความจำเป็นในการยื่นหรือเก็บรักษาไว้เพื่อให้เป็นไปตามกฎข้อบังคับของหน่วยงานของรัฐบาลในเรื่องต่าง ๆ เช่น การศุลกากรและการตรวจสอบบัญชี เป็นต้น การนำเอาการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI) มาใช้แทนกระดาษจำเป็นที่จะต้องสนองวัตถุประสงค์ที่ได้กล่าวมาข้างต้น

ปัญหาที่เกี่ยวกับเรื่องของพยานหลักฐานที่การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อาจก่อให้เกิดขึ้นสามารถแบ่งออกได้เป็นสองประการดังต่อไปนี้

1. ปัญหาที่เกี่ยวกับการยอมรับฟังพยานหลักฐาน (Admissibility Question) เป็นปัญหา โดยทั่วไปในการดำเนินการพิจารณาดีว่าศาลจะยอมรับฟังเอกสารคอมพิวเตอร์เป็นพยานหรือไม่

2. ปัญหาที่เกี่ยวกับการพิสูจน์ความถูกต้อง (Authentication Question) เป็นที่เกี่ยวกับทางปฏิบัติในการพิสูจน์ความถูกต้องของเอกสารคอมพิวเตอร์

ตัวอย่างเช่น

ก ได้สั่งซื้อสินค้าจาก ข โดยใช้การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI) ข้อมูลการสั่งซื้อของ ก ได้ส่งไปยังระบบคอมพิวเตอร์ของ ข ระบบคอมพิวเตอร์ของ ข ได้ทำการบันทึกการสั่งซื้อ และระบุว่าคำสั่งดังกล่าวมาจาก ก รวมทั้งบันทึกเวลาที่คำสั่งมาถึง ระบบคอมพิวเตอร์ของ ข ทำการตรวจสอบสินค้าในคลังสินค้าโดยอัตโนมัติและยอมรับคำสั่งดังกล่าว เมื่อสินค้าถูกส่งไป ก กลับปฏิเสธการสั่งซื้อสินค้าของตน รวมทั้งปฏิเสธการชำระเงิน⁵⁴

ในกรณีดังกล่าว ข จะต้องพิสูจน์ว่า

1. คำสั่งซื้อได้ถูกส่งมาจริง และ
2. ส่งมาโดย ก

เราสามารถใช้บันทึกข้อมูลในการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์เป็นหลักฐานหรือไม่ ศาลจะรับฟังเอกสารดังกล่าวเป็นพยานหรือไม่ (Admissibility question) และถ้าศาลรับฟังจะพิสูจน์อย่างไรว่าคำสั่งซื้อสินค้านี้เป็นของ ก จริง (Authentication question)

เหตุการณ์อาจมีความซับซ้อนมากขึ้น หากไม่มีคนเข้ามาเกี่ยวข้องกับการทำธุรกรรมดังกล่าวเลย ตัวอย่างเช่นหากเกิดว่าในช่วงนั้นราคาสินค้ามีความผันผวน เวลาในการมีคำสั่งซื้อสินค้าจะเป็นเรื่องที่มีความสำคัญเป็นอย่างมาก เวลาในการทำคำสั่งซื้อของ ก จะได้รับการบันทึกไว้โดยระบบคอมพิวเตอร์ ปัญหาคือการบันทึกดังกล่าวสามารถใช้เป็นหลักฐานยื่นต่อศาลได้หรือไม่ ถือได้หรือไม่ว่าเวลาที่ทำการสั่งซื้อดังกล่าวเชื่อถือได้หรือไม่ การทำธุรกรรมทั้งหมดอาจทำโดยเครื่องคอมพิวเตอร์ โดยไม่มีมนุษย์เข้า

⁵⁴ โปรดดู Rob Bradgate, "Evidential issues of EDI", in Ian Walden (ed.), EDI and The Law, Blenheim Online, London, 1989

มาเกี่ยวข้อง เช่น ระบบคอมพิวเตอร์ของ ก สามารถได้รับการวางโปรแกรมให้ทำการสั่งซื้อสินค้าโดยอัตโนมัติเมื่อสินค้าในสต็อกลดลงในระดับที่กำหนดไว้

พยานหลักฐานคือทุกสิ่งที่สามารถแสดง อธิบาย หรือชี้ให้เห็นข้อเท็จจริงหรือจุดที่เป็นประเด็นปัญหา ผู้ที่แสดงพยานหลักฐานในการพิสูจน์อาจยืนยันพยานหลักฐานต่างๆ ได้หลายประเภทไม่ว่าจะเป็น เอกสาร วัตถุ พยานบุคคล (Witness Testimony) หรือผลของการทดลองหรือกระบวนการทางวิทยาศาสตร์ เพื่อที่จะให้เป็นประโยชน์พยานหลักฐานต้องสามารถเชื่อถือได้ แต่ทราบได้ที่พยานหลักฐานดังกล่าวสามารถเข้าใจได้ พยานหลักฐานนั้นก็ไม่จำเป็นต้องใช้การสื่อสารในรูปแบบอื่นหรือสื่ออื่นที่เป็นที่ยอมรับตามกฎหมายพยานหลักฐานหรือเพื่อทำให้น่าเชื่อถือ พยานหลักฐานจะเป็นสิ่งที่ถูกต้องแท้จริง (Authentic) ก็ต่อเมื่อพยานหลักฐานนั้นเป็นในสิ่งเดียวกับที่ยืนยัน⁵⁵

พยานหลักฐานอาจได้รับการยอมรับฟัง (admissibility) หากแสดงถึงข้อเท็จจริงอย่างชัดเจน ตัวอย่างเช่นในคดี *Roberts v. United States*⁵⁶ จำเลยถูกฟ้องว่าขโมยจากเครื่องเอทีเอ็ม ศาลตัดสินว่าเอกสารทางอิเล็กทรอนิกส์ (Electronic Record) จากเครื่องเอทีเอ็มสามารถรับฟังได้หากใช้แสดงว่าธุรกรรมที่เป็นปัญหาได้เกิดขึ้นจริง

การถกเถียงกันในเรื่องของพยานหลักฐานอิเล็กทรอนิกส์นั้นเริ่มมีความเข้มข้นมากขึ้น โดยเฉพาะในเรื่องของการพิสูจน์ความแท้จริงของเอกสาร (Authenticity) (เช่นในเรื่องของที่มา (origin) และเรื่องความสมบูรณ์ (Integrity)) ของข้อความทางอิเล็กทรอนิกส์ (Electronic Message) ที่เกิดขึ้นจากระบบภายนอก นอกจากนั้นในช่วงเปลี่ยนแปลงจากการใช้เครื่องคอมพิวเตอร์เมนเฟรมไปใช้เครื่องคอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายอย่างเช่น เครือข่ายอินเทอร์เน็ตทำให้เกิดปัญหาเรื่องความปลอดภัยจากแหล่งภายนอกตัวอย่างเช่น แสกเกอร์หรือไวรัสคอมพิวเตอร์ เป็นต้น

⁵⁵ Kevin J. Kotch, "Addressing the Legal Problems of International Electronic Data Interchange: The Use of computer Records as Evidence in Different Legal Systems", 6 Temple Int'l & Comp. L.J. 451 (1992)

⁵⁶ 508 A.2d 110 (D.C. App. 1986) .

2. ตัวอย่างกฎหมายพยานหลักฐานของต่างประเทศ

การใช้เอกสารคอมพิวเตอร์ (Computer Record) เป็นพยานหลักฐานมีปัญหาที่แตกต่างกันระหว่างกลุ่มประเทศที่ใช้ระบบคอมพิวเตอร์และระบบที่ใช้ประมวลกฎหมาย แต่อย่างไรก็ดีทั้งสองระบบมีสิ่งหนึ่งที่เหมือนกันคือ ความสามารถในการใช้เอกสารคอมพิวเตอร์ (Computer Record) เป็นพยานหลักฐานยังไม่เคยได้รับการพิสูจน์ในศาล

2.1 กลุ่มประเทศคอมมอนลอว์

ในระบบคอมมอนลอว์ การยอมรับฟังพยานหลักฐาน (Admissibility) นำหนักในการรับฟังพยานจะถูกกำหนดโดยข้อเท็จจริงซึ่งอาจทำโดยผู้พิพากษาและลูกขุน อุปสรรคที่สำคัญของการยอมรับฟังพยานที่เป็นเอกสารคอมพิวเตอร์คือหลัก Hearsay และหลัก Best Evidence Rule ซึ่งจะได้ทำการกล่าวถึงต่อไป

2.1.1 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐไม่มีกฎหมายเฉพาะว่าด้วยการยอมรับเอกสารคอมพิวเตอร์ (Computer Record) กฎเกณฑ์ที่เกี่ยวกับพยานหลักฐานมีความแตกต่างกันในแต่ละมลรัฐ ในระดับสหรัฐ เอกสารคอมพิวเตอร์ (Computer Record) จะได้รับการยอมรับในศาลในฐานะที่เป็นเอกสารทางธุรกิจซึ่งถือว่าเป็นข้อยกเว้นของหลัก Hearsay Rule ศาลมักจะรับฟังพยานโดยตรงมากกว่าพยานที่มาบอกเล่า ข้อยกเว้นของหลัก Hearsay คือศาลจะรับฟังพยานหลักฐานเฉพาะที่เป็นเอกสารทางธุรกิจ (Business Record) หรือเอกสารมหาชน (Public Records) ภายใต้เหตุผลที่ว่าเอกสารดังกล่าวสะท้อนเหตุผลและความต้องการของหน่วยงานมากกว่าเจตนาของผู้จัดทำเอกสาร เอกสารคอมพิวเตอร์ (Computer Record) ถือว่าไม่ได้ถูกจัดทำและเก็บไว้ในความจำของคนอาจได้รับฟังเป็นพยานหลักฐานซึ่งผู้กล่าวอ้างต้องแสดงว่า

" การรวบรวมข้อมูล ไม่ว่าในรูปแบบใด จะเป็นเรื่องของการกระทำ เหตุการณ์ สภาพการณ์ ความคิดเห็น หรือการวิเคราะห์ ที่ทำขึ้นในเวลาใกล้เคียงกับเหตุการณ์มากที่สุด รวมทั้งได้เก็บไว้ตามทางปฏิบัติอันเป็นปกติทางธุรกิจ และเป็นทางปฏิบัติโดยปกติที่จะต้องทำโดยการรวบรวมข้อมูลดังกล่าว โดยได้รับ

การยืนยันจากพยานบุคคลผู้ทำการเก็บรักษาหรือโดยพยานผู้เชี่ยวชาญ เว้นแต่ว่าแหล่งที่มาของข้อมูลหรือวิธีการหรือสภาพการณ์ในการจัดเตรียมข้อมูลดังกล่าวขาดความน่าเชื่อถือ⁵⁷

Advisory Committee ได้ช่วยให้สภา Congress ในการพัฒนากฎเกณฑ์ของสหรัฐฯ โดยเฉพาะในส่วนที่เกี่ยวกับคำว่า " การรวบรวมข้อมูล " (Data Compilations) เพื่อให้สามารถใช้กฎเกณฑ์ดังกล่าวกับเอกสารคอมพิวเตอร์ (Computer Records) ได้⁵⁸

การพัฒนาหลักการพื้นฐานดังกล่าวนี้ได้อธิบายไว้ว่าพอเพียงที่จะทำให้เอกสารคอมพิวเตอร์ (Computer Records)⁵⁹ สามารถรับฟังได้ การเก็บรักษาเอกสารคอมพิวเตอร์โดยผู้เก็บเอกสารที่มีความเป็นกลางจะช่วยให้การยอมรับฟังพยานหลักฐานที่เป็นเอกสารคอมพิวเตอร์สามารถทำได้ไม่ยากนัก ในขณะที่ก่อนหน้านี้ศาลต้องการเหตุผลสนับสนุนความน่าเชื่อถือของเอกสารคอมพิวเตอร์อย่างกว้างขวาง ในปัจจุบันแนวโน้มในการยอมรับฟังพยานหลักฐานที่เป็นเอกสารคอมพิวเตอร์จะไม่ค่อยมีปัญหามากนัก ส่วนใหญ่จะพิจารณาถึงความเชื่อมโยงของเหตุการณ์ที่ถูบันทึกและข้อความที่บันทึก⁶⁰ อย่างไรก็ตาม ฎีกาฎเกณฑ์ที่สร้างขึ้นใหม่นี้มักต้องอาศัยการพิสูจน์ของพยานผู้เชี่ยวชาญ และสำหรับในกรณีของเอกสารมหาชน (Public Records) ซึ่งเป็นข้อยกเว้นของหลัก Hearsay จะช่วยส่งผลให้เอกสารคอมพิวเตอร์ของหน่วยงานของหน่วยงานของรัฐ (Public Institutions) รับฟังได้โดยไม่ต้องแสดงให้เห็นว่าเอกสารดังกล่าวทำขึ้นตามทางปฏิบัติโดยปกติทางธุรกิจ

นอกจากนี้หลัก Best Evident Rule กำหนดให้ต้องยื่นเอกสารต้นฉบับในกรณีของพยานเอกสารตามหลักกฎหมายพยานของสหรัฐฯ ความถูกต้องของเอกสารที่พิมพ์ผ่านเครื่องคอมพิวเตอร์ (Printout) จะ

⁵⁷ Fed. R. Evid. 803(6)

⁵⁸ Glenn Weissenberger, Federal Rules of Evidence, (1987) p 818

⁵⁹ James V. Vergari & Virginia V. Shue, Fundamentals of Computer-High Technology Law, (1991), p. 338

⁶⁰ Benjamin Wright, The Law of Commerce: EDI, Fax, and E-mail: Technology, Proof, and Liability, (1991), p.

ถือว่าเป็นเอกสารต้นฉบับ ดังนั้นหลัก Best Evident Rule จึงมิได้สร้างปัญหาในการยอมรับฟังพยานหลักฐานที่เป็นเอกสารคอมพิวเตอร์แต่อย่างใด⁶¹

2.1.2 สหราชอาณาจักร

รัฐสภาอังกฤษได้ใช้ความพยายามอย่างมากในการขยายขอบเขตการยอมรับฟังพยานหลักฐานที่เกี่ยวกับเทคโนโลยีสมัยใหม่⁶² โดยการตราพระราชบัญญัติพยานหลักฐานทางแพ่ง ค.ศ. 1968⁶³ กฎหมายฉบับนี้ส่งผลให้เอกสารคอมพิวเตอร์สามารถรับฟังได้ในกระบวนการพิจารณาคดีแพ่ง รวมทั้งสำเนาและต้นฉบับเอกสารคอมพิวเตอร์จะได้รับการรับฟังรวมถึง Oral testimony ก็จะได้รับยอมรับเช่นเดียวกัน เพื่อให้ให้เอกสารคอมพิวเตอร์สามารถฟังได้ ผู้ยื่นพยานดังกล่าวจะต้องแสดงให้เห็นว่าคอมพิวเตอร์ได้ถูกใช้ในธุรกิจอันปกติ และข้อมูลดังกล่าวได้รับการประมวลผลโดยคอมพิวเตอร์อย่างเป็นปกติธุระเช่นกัน รวมทั้งไม่มีความบกพร่องเกิดขึ้นกับคอมพิวเตอร์ระหว่างการประมวลผล บุคคลที่มีหน้าที่รับผิดชอบเกี่ยวกับอุปกรณ์หรือข้อมูลดังกล่าวอาจให้การรับรองถึงความสมบูรณ์ (Identity) ของเอกสาร วิธีการจัดทำเอกสาร รวมทั้งระบุนุอุปกรณ์ที่เกี่ยวข้องกับการจัดทำเอกสาร การที่ศาลจะพิจารณาว่าเอกสารคอมพิวเตอร์จะได้รับการยอมรับหรือไม่ ศาลจะพิจารณาจากพฤติการณ์ต่างๆ ที่กล่าวอ้าง นำหนักของพยานที่เป็นเอกสารคอมพิวเตอร์จะขึ้นอยู่กับพฤติการณ์แวดล้อมของคดี ขณะที่ Phipson on Evidence รายงานว่ายังไม่มีคดีตามมาตรา 5 เกิดขึ้นเลย อย่างไรก็ตามได้มีการมีรายงานว่ามีคดีอาญาที่เกี่ยวข้องกับพยานคอมพิวเตอร์ ซึ่งศาลเห็นว่าพยานคอมพิวเตอร์ศาลอาจรับฟังได้⁶⁴ ซึ่งก็สามารถปรับใช้ในคดีแพ่งได้เช่นกัน

มีปัญหาเกิดขึ้นใหม่ในราวต้นปี 1992 เมื่อรัฐบาลเริ่มจัดทำเอกสารคอมพิวเตอร์เพื่อพิสูจน์ว่าผู้ใดไม่ได้ชำระ(Pool Tax)⁶⁵ อย่างไรก็ตามก็ติดเนื่องจากคดีดังกล่าวตัดสินโดย Magistrate Courts ซึ่งใช้ Civil

⁶¹ Fed. R. Evid. 1001(3)

⁶² Michael Kean, Civil Evidence Act of 1968, 1969, pp. 16-17

⁶³ Civil Evidence Act of 1968

⁶⁴ M.N. Howard et al., Phipson on Evidence (1990) p. 589

⁶⁵ Geoffrey Holgate, Community Charge Enforcement: The Admissibility of Computer Records and the Legislative Dilemma, 156 Loc. Gov't Rev. (1992), pp. 401-402; Clifford Miller, Electronic Evidence- Can You Prove the Transaction Took Place?, 9(5) Computer L. Wkly. 21 (1992)

Evidence Act of 1938 มากกว่าที่จะใช้ Civil Evidence Act of 1968 ซึ่ง พรบ. ดังกล่าวไม่มีบทบัญญัติว่าด้วยการรับฟังพยานที่เป็นเอกสารคอมพิวเตอร์⁶⁶ ด้วยเหตุนี้ศาลดังกล่าวจึงตัดสินว่าเอกสารคอมพิวเตอร์ไม่สามารถรับฟังได้ตามหลัก Hearsay นับแต่นั้นต่อมาสหราชอาณาจักรจึงต้องตราพระราชบัญญัติเพื่อให้ Magistrate Court สามารถรับฟังพยานหลักฐานที่เป็นเอกสารคอมพิวเตอร์ได้

เงื่อนไขตามมาตรา 5 (Computer Evidence Act 1968) กำหนดให้

1. เอกสารถูกจัดเตรียมในระหว่างเวลาที่คอมพิวเตอร์ใช้งานเป็นปกติในการประมวลผลข้อมูล เพื่อวัตถุประสงค์ในการทำธุรกรรมที่เป็นปกติในช่วงเวลาดังกล่าว
2. ข้อมูลที่ปรากฏในรูปของเอกสาร หรือได้รับมาในช่วงเวลาที่ปกติในการส่งมายังเครื่องคอมพิวเตอร์ในการทำธุรกรรมอันเป็นปกติธุระ
3. ในระยะเวลาที่คอมพิวเตอร์ได้ทำงานเป็นปกติอย่างเหมาะสม หากมีความชำรุดบกพร่องหรือระบบเสียหายจะต้องไม่มีผลเสียหายต่อความถูกต้องของเอกสารดังกล่าว
4. ข้อมูลในเอกสารได้ถูกทำขึ้นใหม่หรือได้รับจากข้อมูลที่ส่งให้เครื่องคอมพิวเตอร์ในกิจอันเป็นธุระตามปกติ

ศาลจะต้องพิจารณาว่าเงื่อนไขดังที่ได้กล่าวมาสมบูรณ์หรือไม่ทั้งโดย การสืบพยานบุคคล หรือโดยการรับรองจากบุคคล “ที่มีหน้าที่รับผิดชอบเกี่ยวกับการจัดการเพื่อวัตถุประสงค์ในการใช้งานโดยเครื่องคอมพิวเตอร์” ณ เวลาที่เอกสารได้จัดทำขึ้น (ไม่ใช่เวลาที่เอกสารได้รับการบันทึก (Recorded))

ในมาตรา 2 และ 4 กำหนดให้บุคคล “ที่มีอำนาจ” จะต้องมิหน้าที่ดังต่อไปนี้

⁶⁶ Clifford Miller, Electronic Evidence- Can You Prove the Transaction Took Place?, 9(5) Computer L. Wkly. 102 (1992)

1. จัดการเกี่ยวกับระบบคอมพิวเตอร์ที่ใช้
2. นำข้อมูลเข้าไปยังเครื่องคอมพิวเตอร์
3. การปฏิบัติการของเครื่องคอมพิวเตอร์

อย่างไรก็ดีข้อกำหนดตามมาตรา 5 มักได้รับการวิพากษ์วิจารณ์จากทั้งนักกฎหมายและผู้เชี่ยวชาญทางคอมพิวเตอร์ ซึ่งข้อกำหนดของมาตรา 5 นี้ได้ทิ้งปัญหาทางเทคนิคไว้มากมาย ทำให้สถานะของเอกสารที่ได้จากเครื่องคอมพิวเตอร์มีความไม่ชัดเจน ยิ่งกว่านั้นข้อกำหนดดังกล่าวก็ไม่ได้กล่าวถึงปัญหาที่สำคัญที่สุดของเรื่องดังกล่าวซึ่งนอกจากการยอมรับฟัง (Admissibility) แล้วควรที่จะกล่าวถึงการซึ่งนำหลักฐานหลักฐานทางอิเล็กทรอนิกส์ด้วย ประเด็นต่าง ๆ มีดังต่อไปนี้⁶⁷

1. เงื่อนไขที่กำหนดให้เครื่องคอมพิวเตอร์ต้องถูกใช้อย่างเป็นปกติ (Regularly Used) สำหรับกิจกรรมที่ดำเนินการอย่างเป็นประจำ (Regularly carried on) คำว่า “โดยปกติ” (Regularly) ไม่ได้มีการให้คำ นิยามไว้ และดูเหมือนว่าจะไม่มีเหตุผลเลยที่เอกสารที่ออกมาจากเครื่องคอมพิวเตอร์ที่ใช้เพื่อกิจการเพียงกิจการเดียว (One off task) จะไม่ได้รับการยอมรับหากระบบสามารถแสดงให้เห็นว่าทำงานได้อย่าง ถูกต้องในเวลาดังกล่าวได้
2. ข้อกำหนดไม่ได้กล่าวถึงปรากฏการณ์ที่เรียกว่า GIGO (garbage in, out) ข้อกำหนดตามมาตรา 5 ไม่ได้กล่าวถึงความถูกต้องของข้อมูลที่ป้อนเข้าเครื่องคอมพิวเตอร์ (ปัจจัยบางอย่างเกี่ยวกับการป้อนข้อมูลเข้าไปในระบบจะถูกระบุไว้ในมาตรา 6 เพื่อเป็นองค์ประกอบในการพิจารณาโดยศาลในการตัดสินว่าพยานหลักฐานมีน้ำหนักมากเพียงใด ศาลถูกกำหนดให้พิจารณาพฤติการณ์ทั้งหมด โดยเฉพาะอย่างยิ่ง การประมวลผลข้อมูลและเหตุการณ์และแรงจูงใจของบุคคลในการปกปิดข้อเท็จจริงที่ได้บันทึกไป)

⁶⁷ Rob Bradgate, “Evidential issues of EDI”, in Ian Walden (ed.), EDI and The Law, Blenheim Online, London, 1989 p. 18

3. ข้อกำหนดดังกล่าวไม่ได้กล่าวถึงปัญหาทางด้านความปลอดภัย (Security) ของระบบซึ่งถือว่ามีความสำคัญเป็นอย่างมาก
4. ข้อกำหนดที่ 4 ที่กำหนดให้ข้อมูลที่ทำขึ้นอีกครั้งหนึ่งหรือได้รับมาจากข้อมูลที่ป้อนเข้าไปยังเครื่องคอมพิวเตอร์ ยกเว้นหลักฐานที่รู้โดยเครื่องคอมพิวเตอร์ เช่นจาก Real Time Clock หรือในกรณีที่ระบบกำหนดให้สนองต่อการติดต่อสื่อสารจากระบบคอมพิวเตอร์อื่นเอง กรณีดังกล่าว นั้นมักเป็นกรณีที่ข้อความที่แลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI Message) ถูกส่งและรับโดย อัตโนมัติโดยระบบที่รับข้อมูลดังกล่าว
5. ข้อเท็จจริงที่กำหนดให้ต้องมีการรับรอง โดยบุคคลที่มีหน้าที่รับผิดชอบเกี่ยวกับการบริหารระบบคอมพิวเตอร์ ณ เวลาที่เอกสารได้รับการจัดทำขึ้น ปัญหาคือต้นฉบับของเอกสารนี้คือเอกสารที่อยู่ในเครื่องคอมพิวเตอร์หรือที่พิมพ์ออกมาจากเครื่องคอมพิวเตอร์ (Printout) อาจมีข้อโต้เถียงว่าการรับรองดังกล่าวไม่มีความเหมาะสม ในกรณีที่เอกสาร (Document) ถูกทำขึ้นหลักจากที่ได้ป้อนข้อมูลต้นฉบับลงไป บุคคลที่จะให้คำรับรองอาจไม่มีความรู้เกี่ยวกับการทำงานของระบบ ณ เวลาที่ทำการป้อนข้อมูลก็ได้ คำรับรองที่ให้โดยผู้รับรองอาจเป็นไปตามข้อกำหนดของกฎหมาย แต่ในกรณีที่เป็นที่โต้แย้งผู้ให้การรับรองอาจถูกคาดหวังว่าจะสามารถทำการตรวจสอบระหว่างระบบการทำงานของคอมพิวเตอร์ ณ เวลาที่กำหนดได้ จึงเป็นประโยชน์สำหรับผู้ใช้ในการฟ้องร้องใน อนาคตที่จะเก็บรักษา log ที่เหมาะสมของการทำงานของระบบคอมพิวเตอร์เพื่อให้สามารถทำการรับรองตามมาตรา 5 ได้
6. ข้อกำหนดที่เกี่ยวกับการทำงานที่เหมาะสม (Proper Requirement) อาจสร้างปัญหาก็ได้ สมมติว่า ก ส่งสินค้าให้ ข ตามคำสั่งคำสั่งซื้อโดย EDI ข ปฏิเสธการส่งซึ่งรวมทั้งปฏิเสธการชำระเงิน ก ใช้ข้อความจากคอมพิวเตอร์ ข มาเป็นหลักฐานอ้างว่าข้อความที่ส่งไปนั้นเกิดจากเครื่องคอมพิวเตอร์ทำงานผิดพลาด ผลจะเป็นว่าข้อความไม่สามารถรับฟังเป็นพยานได้เลย เพื่อหลีกเลี่ยงปัญหาดัง กล่าวข้อตกลง EDI ควรที่จะกำหนดล่วงหน้าว่าใครจะเป็นผู้รับผิดชอบในกรณีที่ระบบคอมพิวเตอร์มีปัญหา

ประเด็นปัญหาบางประการที่ควรจะนำเสนออย่างน้อยเพื่อชี้แจงให้นักพยานเอกสาร คอมพิวเตอร์ คือกระบวนการที่ข้อมูลได้รับการบันทึก Automatic read-in systems จะถือว่ามีความถูกต้องมากกว่า ระบบที่ต้องการให้ข้อมูลถูก Re-keyed ไม่ว่าจะจากเอกสารต้นฉบับหรือจากเอกสารที่พิมพ์ ออกมาจาก เครื่องคอมพิวเตอร์ (Printout) ดังนั้น ระบบการบันทึกแบบ EDI ควรที่จะมีความถูกต้องมากกว่าการบันทึก ของข้อมูลคอมพิวเตอร์ที่ทำตามแบบเดิม ข้อกำหนดตาม ข้อกำหนดของกฎหมายไม่ได้เสนอแนะ ประเด็น ปัญหานี้ แต่ก็เป็นการเหมาะสมที่จะเป็นประเด็นที่คู่กรณีจะหยิบยกขึ้นมาเพื่อพิสูจน์ว่าเอกสาร คอมพิวเตอร์ (Computer Record) มีความถูกต้อง (Accuracy) หรือไม่ นอกจากนั้น เนื่องจากข้อมูล จำนวนมากได้รับการประมวลผลโดยบุคคลที่สามหรือโดย บริการเครือข่ายเสริม (VANS) จึงอาจทำให้ พยานคอมพิวเตอร์จำนวนมากถูกละเลยไป

หลัก Best Evidence Rule

โดยทั่วไปแล้วกฎเกณฑ์ทางกฎหมายต้องการเอกสารที่เป็นต้นฉบับมากกว่าสำเนา ดังนั้นการถ่าย สำเนาเอกสารอาจได้รับการยอมรับเป็นพยานหลักฐานและมีคำตัดสินว่า กฎเกณฑ์ไม่สามารถป้องกันการ ยอมรับสำเนาของฟิล์มหรือแถบบันทึกเสียงในฐานะเป็นพยานได้ ถ้าสำเนาดังกล่าวมีความถูกต้องแท้จริง ของพยานหลักฐานดังกล่าว บางคนได้เถียงว่ากฎเกณฑ์ดังกล่าวก็ควรที่จะนำมาใช้กับเอกสารที่ได้จาก คอมพิวเตอร์ด้วยเช่นกัน นอกจากนั้น Amory และ Poulet⁶⁸ ได้ชี้ให้เห็นว่ากฎเกณฑ์ทางกฎหมายอาจไม่ สามารถนำมาใช้บังคับได้ในกรณีที่ข้อมูลได้รับการประมวลผลอย่างซับซ้อนบนพื้นฐานที่ข้อมูลต้นฉบับได้ ถูกแก้ไขเปลี่ยนแปลง

2.1.3 ประเทศออสเตรเลีย

โดยทั่วไปแล้วศาลในประเทศออสเตรเลียมักจะยอมรับฟังพยานหลักฐานที่เป็นคอมพิวเตอร์ แต่ภายใต้แนวความคิดในการตีความที่แตกต่างกันสองวิธี⁶⁹ แนวความคิดแรกเห็นว่าเอกสารคอมพิวเตอร์

⁶⁸ Amory and Poulet, "Computers in the Law of Evidence-A Comparative Approach in Civil and Common Law Systems", (1987) Computer Law and Practice, p. 114

⁶⁹ R.A. Brown, Computer-Produced Evidence in Australia, 8 U. Tas. L. Rev. 46, (1984)

เป็นเพียงเอกสารธุรกิจอย่างหนึ่ง ตัวอย่างเช่นใน South Australia ที่ศาลยืนยันว่าเอกสารคอมพิวเตอร์เป็นเอกสารทางธุรกิจ⁷⁰ อย่างไรก็ตามก็มีข้อยกเว้นในการรับฟังดังนี้ จะรับฟังได้ต่อเมื่อผู้จัดทำเอกสารคอมพิวเตอร์ดังกล่าวอยู่นำหนักของพยานหลักฐานที่เป็นเอกสารคอมพิวเตอร์จะต้องไม่ได้รับการพิจารณาอย่างมีอคติหรือกระทำในทางที่ขัดกับความยุติธรรม วิธีการนี้ได้รับการยอมรับจากรัฐอื่นๆ เช่น Commonwealth, New South Wales, Tasmania, Victoria, Queensland และ The Australian Capital Territory⁷¹

วิธีการที่สองคือการบัญญัติกฎหมายเฉพาะเพื่อให้สามารถรับฟังเอกสารคอมพิวเตอร์ได้ กฎหมาย Computer Evidence Act ของ South Australia ได้รับทั้งคำยกย่องและวิพากวิจารณ์⁷² ภายใต้กฎหมายฉบับนี้เอกสารทางคอมพิวเตอร์ศาลสามารถรับฟังได้หาก 1) เครื่องคอมพิวเตอร์ได้จัดโปรแกรมได้อย่างถูกต้องและใช้บันทึกข้อมูลตามปกติ 2) ข้อมูลที่ได้รับการจัดเตรียมอย่างเป็นระบบและสามารถเป็นที่ยอมรับได้ 3) ไม่มีข้อสงสัยว่าจะมีข้อผิดพลาดเกิดขึ้น 4) เครื่องคอมพิวเตอร์ไม่มีปัญหาหรือถูกแก้ไขจนทำให้ส่งผลถึงความถูกต้องของพยานหลักฐาน 5) เอกสารได้รับการเก็บรักษาไว้โดยบุคคลที่มีอำนาจรับผิดชอบ 6) ไม่มีข้อสงสัยเกี่ยวกับความถูกต้องและความสมบูรณ์ของข้อมูลซึ่งข้อมูลดังกล่าวมานี้อาจได้รับการรับรองโดยบุคคลที่มีอำนาจรับผิดชอบ อย่างไรก็ตามศาลอาจเรียกให้ผู้เชี่ยวชาญมาอธิบายเกี่ยวกับเอกสารคอมพิวเตอร์ที่ให้การรับรองไขครายที่มีอยู่สองคดีขึ้นสู่ศาลแต่อย่างไรก็ดีพยานดังกล่าวไม่เป็นไปตามที่ข้อกำหนดของกฎหมายดังกล่าว⁷³ การบัญญัติกฎหมายเฉพาะสำหรับเอกสารคอมพิวเตอร์ได้ทำโดยหลายรัฐ เช่น Australian Capital Territory, Victoria และ Queensland

บางรัฐอย่างเช่น South Australia ใช้ทั้งวิธีถือว่าเอกสารคอมพิวเตอร์เป็นเอกสารทางธุรกิจ (Business Record) และการออกกฎหมายเฉพาะเพื่อการยอมรับเอกสารคอมพิวเตอร์ซึ่งก็ส่งผลให้เมื่อเอกสารคอมพิวเตอร์ไม่สามารถเข้าข้อกำหนดของกฎหมายเฉพาะได้ เอกสารคอมพิวเตอร์ดังกล่าวสามารถใช้หลัก Common Law มาปรับใช้ได้

⁷⁰ โปรดดู Queen v. Weatherall, 27 S.A. St. R. 238, 240 (S. Aust. 1981)

⁷¹ R.A. Brown, Computer-Produced Evidence in Australia, 8 U. Tas. L. Rev. 46, (1984)

⁷² โปรดดู Colin Tapper, Evidence from Computers, 8 Ga. L. Rev. 562, 612 (1974)

⁷³ Queen v. Weatherall, 27 S.A. St. R. 238, 239 (S. Aust. 1981); Mehesz v. Redman, 21 S.A. St. R. 569, 574-75 (S. Austl. 1979)

2.2 กลุ่มประเทศ Civil Law

ในกลุ่มประเทศที่ใช้ประมวลหรือประเทศ Civil Law นี้เอกสารคอมพิวเตอร์สามารถรับฟังได้ในศาลก็ต่อเมื่อมีกฎหมายบัญญัติไว้เท่านั้น ศาลมีหน้าที่พิจารณานำน้ำหนักของพยานที่เป็นเอกสารคอมพิวเตอร์ในขณะที่เอกสารสามารถได้รับการยอมรับจากศาลแต่คุณค่าในฐานะพยานหลักฐานจะขึ้นอยู่กับความมั่นใจของศาลต่อความน่าเชื่อถือของเอกสารคอมพิวเตอร์

2.2.1 ประเทศเยอรมันนี

มีสองวิธีในการพิสูจน์ตามกฎหมายพยานของเยอรมัน Freibeweis (การพิสูจน์โดยใช้ดุลยพินิจ(Discretionary proof) และ Strengbeweis (การพิสูจน์อย่างเคร่งครัด (Strict proof)Strengbeweis หรือ การพิสูจน์อย่างเคร่งครัดมีอยู่ 5 วิธี⁷⁴ (Inspection, Testimony, expert testimony, evidential document and Examination of parties) โดยทั่วไปแล้วเอกสารคอมพิวเตอร์จะไม่ได้ได้รับการยอมรับในฐานะพยานเอกสารหรือโดยคำให้การของบุคคลที่เกี่ยวข้อง เอกสารคอมพิวเตอร์อาจได้รับการยอมรับเป็นพยานเพื่อพิสูจน์ความมีอยู่ของสัญญาโดยวิธีการ Inspection ตามมาตรา 261 ของประมวลกฎหมายพาณิชย์ของเยอรมัน โดย Inspection คือ “ การเข้าใจโดยทันที(Immediate apprehension) ถึงการมีอยู่และลักษณะ(Characteristics) ของบุคคล สิ่งของ หรือปรากฏการณ์” ในขณะที่เอกสารคอมพิวเตอร์อาจถูกเก็บไว้บนไมโครฟิล์มหรือสื่อข้อมูลคอมพิวเตอร์ (Computer Data Carrier) เอกสารคอมพิวเตอร์เหล่านี้จะได้รับการยอมรับจากศาลก็ต่อเมื่อคู่พิพาทมีหน้าที่นำสืบ ดังนั้นศาลจึงมีอิสระที่กำหนดว่าจะไต่สวนข้อเท็จจริงที่จะใช้ประกอบการพิจารณาคดี

⁷⁴ โปรดดู Klaus-Albrecht Gerstenmaier, World Litigation Law & Practice: West Germany (Ronald E. Myrick ed., 1990); Commission of the European Communities: TEDIS-The Legal Position of the Member States with Respect to Electronic Data Interchange, 1989, p. 64

ยิ่งไปกว่านั้นเอกสารคอมพิวเตอร์ควรมีสถานภาพเดียวกับพยานเอกสารเนื่องจากกฎหมายอนุญาตให้เก็บทางอิเล็กทรอนิกส์ (Electronic Storage) อย่างไรก็ตามน้ำหนักที่ให้กับพยานเอกสารจะขึ้นอยู่กับดุลพินิจของศาลและจะขึ้นอยู่กับความเชื่อมั่นของศาลต่อพยานเอกสารคอมพิวเตอร์ดังกล่าว อย่างไรก็ตามในทางปฏิบัติยังคงมีอุปสรรคอยู่อีกเช่นกันสำหรับการยอมรับฟังพยานเอกสารคอมพิวเตอร์ต่างๆ ที่ศาลสามารถใช้วิธี Inspection ตามประมวลกฎหมายพยานคดีของเยอรมัน น้ำหนักของเอกสารคอมพิวเตอร์จะขึ้นอยู่กับความเชื่อมั่นของศาลต่อเอกสารดังกล่าว ซึ่งก็ควรที่จะมีกฎเกณฑ์เฉพาะที่ควรได้รับการบัญญัติในอนาคต

2.2.2 ประเทศเบลเยียมและฝรั่งเศส

เอกสารคอมพิวเตอร์โดยส่วนใหญ่แล้วจะไม่ได้รับการยอมรับจากศาลเนื่องจากหลัก Best Evidence Rule ของทั้งฝรั่งเศสและเบลเยียม แต่อย่างไรก็ตามในทางปฏิบัติแล้วการใช้เอกสารทางคอมพิวเตอร์จะได้รับการยอมรับในฐานะเป็นข้อยกเว้นจากหลักทั่วไป⁷⁵ ตามประมวลกฎหมายแพ่งของทั้งฝรั่งเศสและเบลเยียม มาตรา 1348 เอกสารทางคอมพิวเตอร์ศาลจะสามารถรับฟังได้เนื่องจากเหตุผลสุดวิสัยที่ไม่สามารถหาเอกสารที่เป็นลายลักษณ์อักษร (Writing) มายืนยันได้ ประมวลกฎหมายแพ่งของทั้งสองประเทศอนุญาตให้สามารถทำการพิสูจน์โดยวิธีใดก็ได้ในกรณีเอกสารได้ถูกทำลายไปโดยอุบัติเหตุหรือโดย Act of God⁷⁶ โดยผู้ที่ยื่นพยานหลักฐานดังกล่าวจะต้องสามารถแสดงให้เห็นว่าธุรกรรมดังกล่าวไม่จำเป็นต้องใช้พยานหลักฐานที่เป็นลายลักษณ์อักษรตามประเพณีปฏิบัติในวงการค้า ตามมาตรา 1348 ของกฎหมายแพ่งของฝรั่งเศส สำเนาเอกสารที่ถูกต้องและทนนาน (Authentic and durable copy) จะสามารถแทนที่เอกสารต้นฉบับและมีน้ำหนักทางพยานเหมือนกันประเทศฝรั่งเศสก็เช่นเดียวกันไม่เหมือนกับประเทศเบลเยียมตรงที่ยอมรับไมโครฟิล์มที่เกิดจากคอมพิวเตอร์ (computer output microfilm:COM)

⁷⁵ โปรดดู Jean-Marie Nelissen Grade & Johan Verbist, World Litigation Law & Practice: Belgium (Ronald E. Myrick, ed., 1989)

⁷⁶ TEDIS-The Legal Position of the Member States with Respect to Electronic Data Interchange, 1989, p. 261

ในฐานะที่เป็นสำเนาเอกสารที่จริงและน่าเชื่อถือ⁷⁷ เอกสารคอมพิวเตอร์อาจถือได้ในเบื้องต้นว่าเป็นหลักฐานของข้อตกลงมาตรา 1325 และ มาตรา 1326 ตามประมวลกฎหมายแพ่งฝรั่งเศส ดังนั้นจึงสมควรที่จะถือว่าเอกสารคอมพิวเตอร์เป็นพยานหลักฐานภายใต้กฎหมายของเบลเยียมและฝรั่งเศส

นอกจากนั้นตามมาตรา 1341 ของประมวลกฎหมายแพ่งฝรั่งเศสและเบลเยียมกำหนดให้สัญญาที่มีมูลค่าตามกำหนดต้องทำเป็นลายลักษณ์อักษร เอกสารคอมพิวเตอร์ไม่ถือว่าเป็นเอกสารที่ทำเป็นลายลักษณ์อักษรตามประมวลกฎหมายแพ่งฝรั่งเศสและเบลเยียมเนื่องจากขาดองค์ประกอบที่สำคัญคือลายมือชื่อ อย่างไรก็ตามมาตรา 1341 จะไม่นำมาใช้กับข้อตกลงที่เป็นการพาณิชย์ (Commercial) อุปสรรคที่สำคัญของเอกสารคอมพิวเตอร์ในฐานะพยานหลักฐานคือการให้น้ำหนักความน่าเชื่อถือของเอกสารคอมพิวเตอร์ ศาลยังคงขาดความมั่นใจในเชื่อถือของเอกสารคอมพิวเตอร์

2.2.3 ประเทศลักเซมเบิร์ก

กฎหมายพยานหลักฐานของลักเซมเบิร์กมีโครงสร้างคล้ายกับของเบลเยียม อย่างไรก็ตามข้อกำหนดที่ถือว่าล้าหน้าอยู่ในระดับหนึ่ง กฎหมายพยานหลักฐานของลักเซมเบิร์กยอมให้รับฟัง Micrographic และนำไปเก็บในเครื่องคอมพิวเตอร์ที่ทำจากต้นฉบับเมื่อการเก็บรักษาต้นฉบับไม่สามารถทำได้ ลักเซมเบิร์กได้ออกกฎหมายใหม่เพื่อรองรับความก้าวหน้าทางเทคโนโลยี⁷⁸

มีข้อยกเว้นของประมวลกฎหมายแพ่งของลักเซมเบิร์กมาตรา 1348 กำหนดว่า“เมื่อคู่กรณีหรือผู้เก็บรักษาไม่สามารถเก็บรักษาเอกสารต้นฉบับและใช้การเก็บแบบ Micrographic และนำไปเก็บในเครื่องคอมพิวเตอร์โดยเอกสารที่เก็บใหม่นี้ทำมาจากเอกสารต้นฉบับโดยบุคคลใดก็ตามที่มีหน้าที่เก็บรักษา การ

⁷⁷ TEDIS-The Legal Position of the Member States with Respect to Electronic Data Interchange, 1989, p. 265

⁷⁸ TEDIS-The Legal Position of the Member States with Respect to Electronic Data Interchange, 1989, p. 179

ทำซ้ำเอกสารขึ้นมาใหม่และการบันทึกลงบนเครื่องคอมพิวเตอร์ ถือว่ามีน้ำหนักเช่นเดียวกับข้อตกลงที่ทำขึ้นเป็นลายลักษณ์อักษร เว้นแต่จะสามารถพิสูจน์เป็นอย่างอื่น"

เพื่อให้ข้อยกเว้นนี้สามารถบังคับใช้ได้คู่กรณีจะต้องปฏิบัติตามมาตรา 1348 ของประมวลกฎหมายแพ่งมาตรา 11 ของประมวลกฎหมายพาณิชย์ และ Grand Ducal Regulation of December 22, 1986 ข้อมูลที่เกิดโดยเครื่องคอมพิวเตอร์จะต้องมีความน่าเชื่อถือและถาวร (Durable) เช่นเดียวกับต้นฉบับ ต้องถูกบันทึกอย่างเป็นระบบ การบันทึกต้องทำในเวลาใกล้เคียงกับการที่เอกสารดังกล่าวได้ทำขึ้น และจะต้องได้รับการดูแลอย่างระมัดระวังในการเก็บรักษาและป้องกันการแก้ไขเปลี่ยนแปลง คู่มือของโปรแกรมคอมพิวเตอร์และคำสั่งใดจะต้องสามารถอ่านเข้าใจได้และจะต้องได้รับการปรับปรุงโดยคนที่มีหน้าที่ดูแลรักษาอุปกรณ์ดังกล่าว ในกรณีที่ข้อมูลที่ถูกบันทึกถูกส่งไปยังเครื่องคอมพิวเตอร์เครื่องอื่น พนักงานที่มีอำนาจจะต้องสามารถแสดงให้เห็นว่าข้อมูลทั้งสองเหมือนกัน ระบบคอมพิวเตอร์จะต้องมีระบบรักษาความปลอดภัย (Security System) ในการป้องกันการแก้ไขเปลี่ยนแปลงและจะต้องอนุญาตให้สามารถเปลี่ยนข้อมูลที่สามารถอ่านเข้าใจได้ตลอดเวลา

2.3 พยานหลักฐานตามกฎหมายไทย⁷⁹

ประมวลวิธีพิจารณาความแ่งและวิธีพิจารณาความอาญาแบ่งตามวิธีการนำพยานเข้าสืบออกเป็น

1. พยานบุคคล 2. พยานเอกสาร 3. พยานวัตถุ

1. พยานบุคคล หมายถึง ถ้อยคำของบุคคลธรรมดาที่มาให้การต่อหน้าศาลเพื่อคำจูนข้อความหรือข้อต่อสู้ของตน
2. พยานเอกสาร หมายถึง ข้อความหรือเครื่องหมายใดๆ ที่อยู่บนกระดาษ หนังสือหรือวัตถุอื่นใด โดยทำให้ปรากฏความหมายด้วย ตัวอักษร ตัวเลข ผังหรือแผนอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นใด ซึ่งคู่ความเสนอต่อศาลเพื่อใช้ความหมายของข้อความ หรือเครื่องหมายนั้นพิสูจน์ความจริง

⁷⁹ โปรดดูเล็คชัน ปานเลิศ, การใช้เอกสารคอมพิวเตอร์เป็นพยานในศาล, วิทยานิพนธ์ปริญญานิติศาสตรบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย, พ.ศ. 2531

3. พยานวัตถุ หมายถึง วัตถุ สิ่งของที่คู่ความอ้างเป็นพยาน และส่งศาลเพื่อให้ศาลตรวจดูเป็นหลักฐานเพื่อพิสูจน์คำจนข้ออ้างหรือข้อต่อสู้ของตน

2.3.1 พยานบอกเล่า (Hearsay Rule)

สืบเนื่องจากกฎหมายไทยเป็นกฎหมายที่มีลักษณะพิเศษ คือมีรูปแบบกฎหมายเป็นระบบประมวลกฎหมาย แต่มีระบบการพิจารณาคดีค่อนข้างไปทางระบบกล่าวหาตามแบบอังกฤษ ดังนั้นจึงเป็นปัญหาว่า "บทตัดพยานบอกเล่า" (Rule against hearsay) นั้นเป็นส่วนหนึ่งของกฎหมายลักษณะพยานหรือไม่ และจากปัญหานี้เองจึงก่อให้เกิดปัญหาที่ยังไม่ยุติ ในกฎหมายลักษณะพยานของไทยจนถึงทุกวันนี้ และปัญหาความไม่แน่นอนของกฎหมายว่าด้วยหลักพยานบอกเล่าที่รับฟังได้หรือไม่ เนื่องจากกฎหมายไทยยังไม่มีบทบัญญัติจำกัดความหมายของพยานบอกเล่าไว้หากแต่ปล่อยให้เป็न्दุลยพินิจของศาลที่จะวินิจฉัยว่า พยานชนิดใดเป็นพยานบอกเล่า และพยานบอกเล่าชนิดใดควรรับฟังได้ ซึ่งศาลฎีกายึดถือตามหลักกฎหมายอังกฤษทำให้เกิดผลเสีย คือไม่มีความแน่นอนของกฎหมาย เนื่องมาจากปัญหาในทางทฤษฎีจะต้องสามารถวิเคราะห์ได้ว่าพยานบอกเล่าในกฎหมายไทยนั้นมีความหมายอย่างไร พยานบอกเล่าในกฎหมายไทยนั้น หมายถึงเฉพาะพยานบุคคลเท่านั้นหรือจะมีความหมายรวมถึงพยานเอกสารด้วย

กรณีเอกสารจากเครื่องคอมพิวเตอร์ คู่ความสามารถนำเสนอเข้ามาเป็นพยานหลักฐานได้โดยไม่ติดปัญหาเรื่องหลักพยานบอกเล่า เนื่องจากเหตุผลดังต่อไปนี้

1. กฎหมายลักษณะพยานของไทย ตั้งแต่เมื่อมีการประกาศใช้กฎหมายวิธีพิจารณาความแพ่งและประมวลกฎหมายวิธีพิจารณาความอาญาแล้ว พระราชบัญญัติให้ใช้กฎหมายวิธีพิจารณาความแพ่งและประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 4 ได้บัญญัติ "ให้ยกเลิกบรรดากฎหมาย กฎและข้อยกเว้นอื่นๆ ในส่วนที่มีไว้แล้วในประมวลกฎหมายนี้ หรือซึ่งขัดแย้งกับประมวลกฎหมายนี้" เป็นผลให้หลักกฎหมายเกี่ยวกับการตัดบทพยานบอกเล่าที่เคยมีอยู่ขัดแย้งแต่เดิมต้องลางเลือนไป เพราะตามกฎหมายใหม่นั้นห้ามมิบทบัญญัติห้ามรับฟังพยานบอกเล่าไว้ชัดเจนไม่มีเพียงมาตรา 95(2) แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง

ซึ่งบัญญัติว่า “ห้ามมิให้รับฟังพยานบุคคลใดเว้นแต่บุคคลนั้น... (2) เป็นผู้ได้ยินหรือทราบข้อความเกี่ยวในเรื่องที่จะให้การเป็นพยานนั้นมาด้วยตนเองโดยตรง...” ดังนั้นเมื่อบทบัญญัติในการรับฟังพยานบอกเล่าไม่ขัดแย้ง โดยให้อยู่ในดุลพินิจของศาล ผู้เขียนจึงเห็นว่ากฎหมายไทยนั้นมีทางออกที่จะรับฟังเป็นพยานหลักฐานในศาลได้

2. เนื่องจากกฎหมายไทยไม่มีบทบัญญัติห้ามรับฟังพยานบอกเล่าที่เป็นพยานเอกสาร ประมวลกฎหมายวิธีพิจารณาความแพ่งมาตรา 95 ระบุให้ใช้บังคับเฉพาะพยานบุคคล และหลักเกณฑ์ในการตรวจสอบความถูกต้องแท้จริงของพยานเอกสารนั้นมีหลักเกณฑ์ในกฎหมายเขียนไว้โดยเฉพาะ ดังนั้นเอกสารจากระบบคอมพิวเตอร์ที่เป็นพยานบอกเล่าสามารถรับฟังเป็นพยานหลักฐานได้

2.3.2 หลักการรับฟังเอกสารต้นฉบับ

หลักเกณฑ์การรับฟังต้นฉบับเอกสารนั้น มีที่มาจากหลักพยานที่ดีที่สุด (Best Evidence Rule) ซึ่งหมายความว่าคู่ความจะต้องนำพยานหลักฐานที่มีคุณภาพสูงสุดมาพิสูจน์ เช่น กรณีที่มีต้นฉบับเอกสารกับสำเนาเอกสาร ก็ต้องนำต้นฉบับเอกสารมาพิสูจน์หรือกรณีที่มิพยานโดยตรงและพยานแวดล้อมก็ต้องนำพยานโดยตรงเข้ามาสืบ ดังนั้นกรณีพยานไม่อาจมาศาลได้เพราะตายหรือสูญหายหรือถูกทำลาย ก็อาจนำพยานที่ด้อยกว่ามาสืบแทนได้ แต่ต้องเป็นพยานที่ดีที่สุดที่สามารถนำสืบได้ เช่น รายงานหรือบันทึกที่เป็นพยานบอกเล่าหรือสำเนาเอกสาร

ตามปกติพยานหลักฐานที่ทำไว้เป็นเอกสาร ซึ่งอาจอ้างเป็นพยานได้นั้นมี 2 อย่างคือ ต้นฉบับเอกสารอย่างหนึ่งและสำเนาของเอกสารนั้นอย่างหนึ่ง คู่ความจะอ้างต้นฉบับหรือสำเนาต้องระบุนำให้ชัดเจนในบัญชีระบุพยาน แต่ตามปกติต้นฉบับเป็นพยานชั้นที่ 1 เป็นพยานที่ดีที่สุด จึงนำสืบได้เสมอ ส่วนสำเนาของเอกสารเป็นสิ่งที่คัดลอก หรือถ่ายไปจากต้นฉบับอีกทีหนึ่งจึงไม่ใช่ของแท้จริง อาจผิดพลาดได้ ถ้านำมาอ้างอิงเป็นพยานปกติศาลจะไม่ยอมรับฟัง เว้นแต่กรณีจะเข้าข้อยกเว้นตามมาตรา 93 ซึ่งผู้อ้างจะต้องแสดงเหตุให้ปรากฏต่อศาลโดยชัดเจนหรือปรากฏว่าคู่ความฝ่ายตรงข้ามยอมรับเอกสารนั้นแล้ว โดยมีหลักดังนี้คือ

1. เมื่อคู่ความทุกฝ่ายรับรองต้องกันว่า สำเนาที่ยื่นนั้นถูกต้องกับต้นฉบับดังนั้นนำสืบสำเนาแทนต้นฉบับได้ (ปวิพ. มาตรา 93)
2. การอ้างหนังสือราชการหรือหนังสือที่อยู่ในความยึดถือของทางราชการเมื่อทางราชการ คือ รัฐมนตรี หัวหน้ากรม กอง หัวหน้าแผนก หรือผู้รักษาการแทนในตำแหน่งนั้นแล้วแต่กรณีอนุญาตให้อ่านนำสืบได้ แล้วศาลยอมรับสำเนาซึ่งรัฐมนตรี หรือหัวหน้ากรม กอง หัวหน้าแผนก หรือผู้รักษาการแทนในตำแหน่งนั้นๆ ได้รับรองถูกต้องแทนตัวหนังสือได้
3. เอกสารมหาชนซึ่งเจ้าหน้าที่ได้ทำขึ้นรับรองนั้น ถ้าจะต้องส่งต้นฉบับมาไว้ยังศาลแล้ว อาจเป็นการขัดข้องแก่งานของราชการ และบางเรื่องไม่สะดวกแก่ประชาชนด้วย เช่น สมุดทะเบียนต่างๆ ซึ่งต้องใช้คงลงและประชาชนอาจจะตรวจดูได้อยู่เสมอเป็นต้น ดังนั้นจากกฎหมายศาลจึงยอมรับสำเนาที่เจ้าหน้าที่ได้รับรองถูกต้องแล้วแทน มีค่าเท่ากับต้นฉบับ เพื่อจะได้รักษาต้นฉบับไว้เป็นของกลาง (ปวิพ. มาตรา 127)
4. เมื่อปรากฏว่าต้นฉบับสูญหายไป โดยหายหรือถูกทำลาย โดยเหตุสุดวิสัยที่ดีหรือเมื่อปรากฏว่ามีเหตุอย่างใดอย่างหนึ่งซึ่งผู้อ้างไม่สามารถจะนำต้นฉบับมาศาลได้ เช่น หนังสือที่อยู่ในความยึดถือของคู่ความอีกฝ่ายหนึ่งหรือคนภายนอก ศาลยอมรับสำเนาไว้แทนต้นฉบับได้ (ปวิพ. มาตรา 122)

2.3.3 วิธีการนำสืบพยานเอกสาร

การนำสืบพยานเอกสารอยู่ภายใต้บังคับของ ประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 88 เช่นเดียวกับพยานประเภทอื่น คือ ต้องอ้างอิงเอกสารนั้นเป็นพยานในบัญชีพยานต่อศาลก่อนวันสืบพยานไม่น้อยกว่า 3 วัน ถ้าจะอ้างเพิ่มเติมต้องอ้างเสียก่อนที่จะเสร็จการสืบพยานของคู่ความฝ่ายที่มีหน้าที่ต้องสืบก่อน ถ้าภายหลังจากนั้นต้องแสดงให้ศาลเป็นที่พอใจว่าตนไม่ทราบว่ามีพยานนี้อยู่ หรือไม่ สามารถจะอ้างมาสืบก่อนนั้นได้ จึงจะนำสืบได้และในการส่งเอกสารเป็นพยานผู้อ้างจะต้องคัดสำเนาเอกสารนั้นให้แก่คู่ความอีกฝ่ายหนึ่งก่อนวันสืบพยานไม่น้อยกว่า 3 วัน เว้นแต่จะเข้าข้อยกเว้นตามประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 90 เช่น เอกสารอยู่กับคนภายนอกหรือคู่ความอีกฝ่ายหนึ่งรับต้น

ฉบับเอกสารที่ส่งศาลแล้ว โจทก์นำสำเนาเอกสารติดท้ายฟ้องไปแล้ว ไม่ต้องส่งสำเนาเวลาสืบพยานอีก เป็นต้น

พยานเอกสารมีลักษณะพิเศษ คือเกิดขึ้นเองไม่ได้ ต้องมีคนทำ แต่เมื่อเกิดแล้วเป็นอย่างไรก็เป็นอยู่อย่างนั้นแม้ว่าเวลาจะผ่านไปนานๆ เว้นแต่จะมีใครแก้ไขเปลี่ยนแปลงภายหลัง สาระสำคัญที่พยานเอกสารต่างจากพยานบุคคลคือ เอกสารพูดไม่ได้ แต่มีข้อเท็จจริงให้คร่ำครวญเข้าใจได้ ดังนั้นการสืบพยานเอกสารมีปัญหาสำคัญ 2 ประการคือ

- ก. ความถูกต้องแท้จริงของเอกสาร หมายความว่าเอกสารนั้นทำขึ้นโดยบุคคลที่ถูกกล่าวอ้าง ไม่ใช่มีการปลอมขึ้นหรือมีแก้ไขเพิ่มเติมภายหลังโดยบุคคลอื่น ความถูกต้องแท้จริงของเอกสารเป็นองค์ประกอบขั้นแรกที่จะทำให้เอกสารนั้นน่าเชื่อถือเพราะถ้าเอกสารนั้นไม่ใช่ของแท้จริงเสียแล้ว ก็ยากที่จะเชื่อได้ว่าข้อความในเอกสารนั้นจะถูกต้องตามความจริง
- ข. ความถูกต้องตามความเป็นจริงของข้อความ หมายความว่าข้อความในเอกสารนั้นตรงกับข้อเท็จจริงที่เกิดขึ้นหรือไม่ ข้อนี้ขึ้นอยู่กับดุลพินิจของศาล โดยเฉพาะว่าศาลจะเชื่อพยานเอกสารนั้นหรือไม่ ถ้าคู่ความฝ่ายหนึ่งมีพยานเอกสารมาแสดง แต่อีกฝ่ายหนึ่งไม่มีพยานมาหักล้างหรือไม่สามารถนำพยานบุคคลมาสืบเปลี่ยนแปลงแก้ไขข้อความในเอกสาร ตามประมวลกฎหมายวิธีพิจารณาความแพ่งมาตรา 94 ศาลก็ต้องรับฟังข้อเท็จจริงตามเอกสารนั้น

2.3.4 วิธีการพิสูจน์ความถูกต้องแท้จริงของเอกสาร

- ก. วิธีการที่ถือว่าฝ่ายตรงข้ามรับ ในการมีอยู่และความแท้จริงถูกต้องแห่งเอกสาร เพราะไม่มีการคัดค้านเอกสารนั้น

ในการสืบพยานเอกสารนั้น ฝ่ายที่อ้างจะต้องนำสืบถึงความถูกต้องแท้จริงแห่งเอกสารก็เฉพาะแต่ในกรณีที่ฝ่ายตรงข้ามคัดค้านเท่านั้น จะเห็นได้ว่าเพื่อให้ฝ่ายตรงข้ามมีโอกาสคัดค้าน ประมวลกฎหมายวิธีพิจารณาความแพ่งมาตรา 90 จึงบังคับให้ฝ่ายที่จะอ้างพยานเอกสารต้องส่งสำเนาเอกสารนั้น

ให้แก่ศาล และคู่ความอีกฝ่ายหนึ่งก่อนวันสืบพยานไม่น้อยกว่าสามวัน ทั้งนี้เพื่อให้อีกฝ่ายมีเวลาตรวจสอบความถูกต้องของเอกสารนั้น ถ้าพบว่าเอกสารนั้นเป็นของปลอมหรือไม่ถูกต้อง ไม่ตรงกับต้นฉบับ ก็จะได้คัดค้านเสีย

กฎหมายวิธีพิจารณาความแพ่งมาตรา 125 วางหลักเกี่ยวกับการคัดค้านพยานเอกสารได้ดังนี้

1. คู่ความทุกฝ่ายที่ถูกอ้างเอกสารมายังตน อาจคัดค้านการนำเอกสารนั้นมานำสืบได้ด้วยสาเหตุ 3 ประการคือ ก. ไม่มีต้นฉบับเอกสาร ข. ต้นฉบับปลอมทั้งฉบับหรือแต่บางส่วน ค. สำเนาไม่ถูกต้องกับต้นฉบับ

การคัดค้านดังกล่าวนี้ แสดงว่าอีกฝ่ายหนึ่งไม่รับรู้เรื่องราวของเอกสารที่อ้างเลย หรือยืนยันว่าสำเนาเอกสารที่ผู้อ้างได้ส่งให้ก่อนวันสืบพยานนั้นไม่ถูกต้องกับของที่เขาถืออยู่ ทำให้มีความสงสัยว่าเอกสารนั้นจะเป็นของปลอม หรือไม่ถูกต้อง ซึ่งผู้คัดค้านจำเป็นต้องดูต้นฉบับเอกสารนั้น ซึ่งฝ่ายที่อ้างจำเป็นจะต้องยื่นต้นฉบับต่อศาล ตามประมวลกฎหมายวิธีพิจารณาความแพ่งมาตรา 122, 125

2. การคัดค้านความถูกต้องแท้จริงนี้ จะต้องคัดค้านเสียก่อนวันสืบพยานคือ วันที่ศาลเริ่มต้นทำการสืบพยานในคดีนั้น ทั้งนี้เพื่อคู่ความฝ่ายที่อ้างจะได้นำต้นฉบับมาส่งศาลทั้งอาจนำพยานบุคคลมาสืบสนับสนุนข้ออ้างของตนในวันพิจารณา คำคัดค้านนี้กฎหมายมิได้บังคับให้ทำเป็นคำร้อง ฉะนั้นอาจทำเป็นคำขอก็ได้ แต่จะต้องบอกกล่าวไปยังคู่ความอีกฝ่ายหนึ่งด้วย

แต่ถ้าคู่ความฝ่ายที่จะคัดค้านมีเหตุอันสมควร ที่ไม่อาจทราบได้ก่อนวันสืบพยานว่าต้นฉบับไม่มีหรือเอกสารนั้นปลอม หรือสำเนาไม่ถูกต้องก็สามารถคัดค้านในเวลาใดๆ ก่อนศาลพิพากษาได้ แต่จะต้องทำเป็นคำร้องขอต่อศาลขออนุญาต คัดค้านการอ้างเอกสารนั้นศาลจะต้องไต่สวนคำร้อง ถ้าศาลเห็นว่าคู่ความฝ่ายนั้นไม่อาจคัดค้านได้ก่อนนั้น และคำขอนั้นมีเหตุผลฟังได้ ก็ให้ศาลอนุญาตตามคำขอ

3. ผลของการไม่คัดค้านการอ้างเอกสารก่อนวันสืบพยาน หรือศาลไม่อนุญาตให้คัดค้านภายหลังวันนั้นก็คือ ห้ามไม่ให้คู่ความฝ่ายนั้นคัดค้านการมีอยู่ และความถูกต้องแท้จริงของเอกสารนั้น หรือความถูกต้องแท้จริงของสำเนาเอกสาร ดังนั้นเอกสารนั้นเป็นอันรับฟังได้ว่าเป็นของแท้หรือสำเนาถูกต้อง ฝ่ายที่อ้างไม่จำเป็นต้องส่งต้นฉบับหรือไม่ต้องนำพยานบุคคลมาสืบประกอบในประเด็นนี้ต่อไป

แต่การไม่คัดค้านแม้จะตัดสินพิพากษาตรงข้ามมิให้โต้แย้งเรื่องความถูกต้องแท้จริงของเอกสาร ก็ไม่ได้ตัดสินพิพากษานั่นในอันที่จะทำสิ่งต่อไปนี้ 1. อ้างว่าสัญญาหรือหนี้ที่ระบุไว้ในเอกสารนั้นไม่สมบูรณ์ 2. อ้างว่าคู่ความอีกฝ่ายหนึ่งมีความผิด ดังนั้นพยานเอกสารที่คู่ความผู้อ้างส่งไว้ต่อศาล แม้อีกฝ่ายหนึ่งไม่ได้โต้แย้งคัดค้านเสียก่อนวันสืบพยาน ก็เพียงแต่ต้องห้ามมิให้คัดค้านการมีอยู่และความแท้จริงของเอกสาร แต่ศาลไม่จำเป็นต้องเชื่อว่าข้อความในเอกสารนั้นเป็นความจริงเสมอไป

4. การคัดค้านเอกสารตามประมวลกฎหมายวิธีพิจารณาความแพ่งมาตรา 125 นี้ เป็นวิธีการที่กฎหมายกำหนดขึ้นในกรณีที่มีการอ้างพยานเอกสารทุกชนิด ไม่ว่าจะเป็นเอกสารอันเป็นฐานที่ตั้งแห่งการโต้แย้งสิทธิในคดีนั้นหรือไม่ เช่น สัญญากู้ สัญญาซื้อขาย และการคัดค้านตามมาตรา นี้ ทำให้เกิดเป็นประเด็นข้อพิพาทแตกต่างกันนอกเหนือจากคำฟ้องขึ้นมาว่าเอกสารนั้นเป็นของแท้จริงถูกต้องหรือไม่ ซึ่งคู่ความฝ่ายที่อ้างต้องนำสืบก่อน เว้นแต่จะมีข้อสันนิษฐานของกฎหมายว่า เอกสารนั้นแท้จริงหรือถูกต้อง เช่นเอกสารมหาชน หรือเอกสารเอกชนที่มีคำพิพากษารับรอง แต่ถ้าเอกสารนั้นเป็นสัญญากู้มาทำยืมฟ้องในกรณีนั้น จำเลยอาจคัดค้านความถูกต้องแท้จริงไว้ในคำให้การก็ได้ และถือว่าเป็นประเด็นข้อพิพาทอันหนึ่ง โดยไม่ต้องคัดค้านตามประมวลกฎหมายวิธีพิจารณาความแพ่งมาตรา 125 อีก

ข. วิธีการที่ศาลชี้ขาดความถูกต้องและแท้จริง

ถ้าคู่ความโต้แย้งกันในเรื่องความถูกต้องแท้จริงของเอกสาร ประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 126 ให้อำนาจศาลที่จะจัดข้อเท็จจริงอันนี้ได้ถ้าศาลเห็นสมควรโดยศาลอาจชี้ขาดโต้แย้งนั้นได้ในทันทีในเมื่อเห็นว่าไม่จำเป็นต้องสืบพยานต่อไป หรือชี้ขาดเมื่อได้สืบพยานตามวิธีต่อไปนี้ทั้งหมด หรือโดยวิธีใดวิธีหนึ่งคือ

1. ตรวจสอบบรรดาเอกสารที่มีได้ถูกคัดค้าน แล้วจดลงไว้ซึ่งการมีอยู่หรือข้อความแห่งเอกสารที่ถูกคัดค้าน
2. ซักถามพยานที่ทราบการมีอยู่ หรือข้อความแห่งเอกสารที่ถูกคัดค้านหรือพยานผู้ที่สามารถเบิกความในข้อความแท้จริงทางเอกสาร หรือความถูกต้องแห่งสำเนา
3. ให้ผู้เชี่ยวชาญตรวจสอบเอกสารที่ถูกคัดค้านนั้น แต่ผู้เชี่ยวชาญก็มีฐานะเป็นพยานบุคคลคนหนึ่งเท่านั้น ดังนั้นแม้โจทก์จำเลยมิได้ตกลงทำกัน ให้ถือเอาความเห็นของผู้เชี่ยวชาญเป็นข้อ

แพ้ชนะแล้ว ความเดิมของผู้เชี่ยวชาญก็เป็นเพียงพยานหลักฐานอันหนึ่งในบรรดาพยานหลักฐานทั้งหลายที่โจทก์อาจสืบ เพื่อแสดงว่าพินัยกรรมปลอม ลำพังเพียงความเห็นของผู้เชี่ยวชาญยังไม่มีเหตุเพียงพอที่จะชี้ขาดความแท้จริง หรือถูกต้องตามประมวลกฎหมายพิจารณาความแพ่งมาตรา 126

ในระหว่างที่ยังมิได้ชี้ขาดตัดสินคดี ให้ศาลยึดเอกสารที่สงสัยว่าปลอมหรือไม่ถูกต้อง แต่ความข้อนี้ไม่บังคับถึงเอกสารราชการซึ่งราชการเรียกคืนไป

ค. ข้อสันนิษฐานของกฎหมายว่าเอกสารเป็นของแท้จริงและถูกต้อง

ประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 127 ให้สันนิษฐานว่า เอกสารมหาชนหรือเอกสารเอกชนที่มีคำพิพากษารับรองเป็นของแท้จริงและถูกต้อง ดังนั้นแม้ความฝ่ายที่อุทธรณ์เอกสารมาขึ้นจะคัดค้านฝ่ายที่อ้างเอกสารก็ไม่ต้องมีหน้าที่นำสืบ เป็นหน้าที่ของฝ่ายคัดค้านที่จะต้องหาพยานมาสืบหักล้างข้อสันนิษฐานของกฎหมาย

การอ้างเอกสารมหาชนมิได้ผูกพันศาลว่าจะต้องเชื่อตามข้อความในเอกสารมหาชนเสมอไป เนื่องจาก ปพพ. 127 กำหนดข้อสันนิษฐานเป็นคุณเฉพาะเรื่องความถูกต้องแท้จริงของเอกสารเท่านั้น

เอกสารโบราณกฎหมายให้ข้อสันนิษฐานว่าเป็นของแท้จริงและถูกต้องโดยไม่ต้องนำพยานบุคคลมาสืบประกอบถึงความถูกต้องแท้จริงอย่างการนำสืบเอกสารธรรมดา แต่จากต้นฉบับเพื่อให้ศาลตรวจว่าเป็นเอกสารโบราณจริง เอกสารที่จะถือเป็นเอกสารโบราณจะต้องประกอบด้วยหลักเกณฑ์ดังต่อไปนี้ คือ

1. เอกสารนั้นจะต้องมีอายุเก่าแก่มาก ทั้งนี้โดยอาจดูจากวันที่ที่ลงไว้ในเอกสารหลักลักษณะของวัสดุที่ใช้ทำเอกสาร โดยจะต้องมีอายุไม่น้อยกว่า 20 ปี
2. ต้องปรากฏว่าเอกสารนั้นถูกต้องเก็บอยู่ในที่ที่สมควรเก็บ หรือได้มาจากบุคคลซึ่งสมควรจะมีเอกสารนั้นไว้ในครอบครอง

3. ถ้าในเอกสารไม่ปรากฏข้อเท็จจริงที่เห็นได้ชัดว่า ผู้ทำเอกสารโบราณนั้นเป็นบุคคลที่มีตัวตนอยู่จริง ก็จะต้องมีพยานมาสืบปรากฏว่า บุคคลผู้นั้นมีตัวตนอยู่จริงแต่ได้ตายไปแล้ว

ง. ในกรณีที่คู่ความฝ่ายหนึ่งอ้างพยานเอกสาร และอีกฝ่ายหนึ่งคัดค้านความมีอยู่หรือความแท้จริงของต้นฉบับ หรือความถูกต้องของสำเนา และไม่มีข้อสันนิษฐานของกฎหมายว่าเอกสารนั้นเป็นของแท้จริงและถูกต้อง ฝ่ายที่อ้างก็จำเป็นต้องนำพยานมาสืบว่าเอกสารนั้นเป็นของแท้จริงและถูกต้อง วิธีการพิสูจน์ความถูกต้องแท้จริงนี้ฝ่ายอ้างเอกสารจะต้องดำเนินการ 2 อย่าง คือ 1. ส่งต้นฉบับเอกสารนั้นต่อศาล 2. นำพยานบุคคลมาสืบประกอบ

การนำต้นฉบับมาส่งศาลนั้น มี ปวิพ. 122 บัญญัติไว้ว่าเมื่อคู่ความฝ่ายใดอ้างอิงเอกสารฉบับใดเป็นพยานหลักฐาน และคู่ความอีกฝ่ายหนึ่งคัดค้านเอกสารนั้นตามที่บัญญัติไว้ในมาตรา 125 ถ้าต้นฉบับเอกสารอยู่ในความครอบครองของคู่ความฝ่ายที่อ้างเอกสาร ให้คู่ความฝ่ายนั้นนำต้นฉบับเอกสารมาแสดงต่อศาลในวันสืบพยานไม่ว่าเวลาใดๆ ก่อนที่จะมีคำพิพากษา ถ้าศาลได้กำหนดให้คู่ความฝ่ายที่อ้างเอกสารส่งต้นฉบับเอกสารต่อศาล โดยที่ศาลเห็นสมควรหรือโดยที่คู่ความอีกฝ่ายหนึ่งยื่นคำขอ ให้คู่ความฝ่ายนั้นส่งต้นฉบับเอกสารต่อศาล เพื่อศาลหรือคู่ความอีกฝ่ายหนึ่งจะได้ตรวจดูตามเงื่อนไข ซึ่งจะได้กำหนดไว้ในกฎกระทรวงว่าด้วยการนั้น หรือตามที่ศาลจะได้กำหนด แต่ถ้า 1. ไม่สามารถจะนำมาหรือยื่นต้นฉบับเอกสารดังกล่าวข้างต้น คู่ความฝ่ายนั้นอาจยื่นคำขอโดยทำเป็นคำร้องต่อศาลในวันที่ทำงานให้นำมา หรือให้ยื่นต้นฉบับเอกสารนั้นแถลงให้ทราบถึงความไม่สามารถที่จะปฏิบัติตามได้พร้อมทั้งเหตุผล ถ้าศาลเห็นว่าผู้ยื่นคำขอไม่สามารถที่จะนำมาหรือยื่นต้นฉบับเอกสารได้ ศาลจะมีคำสั่งอนุญาตให้นำต้นฉบับเอกสารมาในวันต่อไปหรือจะสั่งเป็นอย่างอื่นตามที่เห็นสมควรเพื่อประโยชน์แห่งความยุติธรรมก็ได้ ในกรณีที่ผู้ยื่นคำขอมีความประสงค์ให้ศาลขยายระยะเวลาที่ตนจะต้องนำมาหรือยื่นต้นฉบับเอกสารนั้น คำขอนั้นจะเป็นคำขอฝ่ายเดียวก็ได้ 2. ถ้าการที่จะนำมาหรือยื่นต้นฉบับเอกสารต่อศาลนั้น จะเป็นเหตุให้เกิดการสูญหายหรือบุบสลาย หรือมีข้อขัดข้อง โดยอุปสรรคสำคัญหรือความลำบากยากยิ่งใดๆ คู่ความฝ่ายที่อ้างอิงเอกสารอาจยื่นคำขอฝ่ายเดียวโดยทำเป็นคำร้องต่อศาลในวัน หรือก่อนวันสืบพยาน แถลงให้ทราบถึงเหตุเสียหาย อุปสรรค หรือความลำบากเช่นนั้น ถ้าศาลเห็นว่าต้นฉบับเอกสารนั้นไม่อาจนำมา หรือยื่นต่อศาลได้ ศาลจะมีคำสั่งให้ยื่นต้นฉบับเอกสารนั้น ณ สถานที่ใดต่อเจ้าพนักงานคนใด และภายในเงื่อนไขใดๆ

ตามที่เห็นสมควรก็ได้ หรือจะมีคำสั่งให้คัดสำเนาที่รับรองว่าถูกต้องทั้งฉบับ หรือเฉพาะส่วนที่เกี่ยวข้องเรื่องมายื่นแทนต้นฉบับก็ได้

ถ้าคู่ความฝ่ายที่อ้างเอกสารไม่ยอมยื่นต้นฉบับเอกสาร ตามปกติศาลก็จะไม่ยอมรับฟังเอกสารนั้นเป็นพยาน แต่ถ้าปรากฏว่าคู่ความอีกฝ่ายหนึ่งได้อ้างอิงเอกสารนั้นเป็นพยานด้วย และการที่คู่ความฝ่ายที่อ้างไม่ยอมส่งต้นฉบับเอกสารนั้น ก็เพื่อจะกีดกันไม่ให้อีกฝ่ายหนึ่งอ้างเอกสารเป็นพยาน ตาม ปวิพ. มาตรา 124 ให้ถือว่าข้อเท็จจริงแห่งข้ออ้างที่คู่ความอีกฝ่ายหนึ่งจะต้องนำสืบโดยเอกสารนั้นคู่ความฝ่ายที่ไม่นำมาหรือยื่นเอกสารดังกล่าวข้างต้นนี้ได้นยอมรับแล้ว

ในกรณีมีคู่ความฝ่ายที่อ้างเอกสารไม่สามารถจะนำต้นฉบับเอกสารมาส่งศาลได้เพราะต้นฉบับเอกสารนั้นอยู่ในความครอบครองของบุคคลที่สาม ตาม ปวิพ. มาตรา 123 ให้คู่ความฝ่ายที่อ้าง จะต้องยื่นคำขอโดยทำเป็นคำร้องต่อศาลขอให้ส่งคู่ความอีกฝ่ายหนึ่งส่งต้นฉบับเอกสารแทนการที่ตนจะต้องส่งสำเนาเอกสารนั้นได้ ถ้าศาลมีคำสั่งให้คู่ความอีกฝ่ายหนึ่งยื่นต้นฉบับเอกสารต่อศาลภายในเวลาอันสมควรแล้วศาลจะกำหนด ถ้าคู่ความอีกฝ่ายหนึ่งมีต้นฉบับเอกสารในความครอบครองไม่ปฏิบัติตามคำสั่งเช่นนั้น ให้ถือว่าข้อเท็จจริงแห่งข้ออ้างที่ผู้ขอจะต้องนำสืบโดยเอกสารนั้นคู่ความอีกฝ่ายหนึ่งได้ยอมรับแล้ว

แต่ถ้าต้นฉบับเอกสารอยู่ในความครอบครองของบุคคลภายนอก หรือในความครอบครองของทางราชการ หรือของเจ้าหน้าที่ซึ่งคู่ความที่อ้างไม่อาจขอร้องโดยตรงให้ส่งเอกสารนั้นมาได้ ปวิพ. มาตรา 123 บัญญัติว่าให้นำบทบัญญัติในวรรคก่อนว่าด้วยการที่คู่ความฝ่ายที่อ้างเอกสารยื่นคำขอและการที่ศาลมีคำสั่งล่วงหน้าอย่างน้อย 7 วัน ถ้าไม่ได้เอกสารนั้นมาสืบตามกำหนดที่ศาลเห็นสมควร ก็ให้สืบพยานต่อไปตามที่บัญญัติไว้ในมาตรา 93(2)

ในคดีอาญา หลักเกณฑ์การสืบพยานเอกสารเช่นเดียวกับคดีแพ่ง คือต้นฉบับเอกสารเท่านั้นที่อ้างเป็นพยานได้ แต่ถ้าหาต้นฉบับไม่ได้ สำเนาที่รับรองว่าถูกต้องหรือพยานบุคคลที่รู้ข้อความก็อ้างเป็นพยานได้ แต่ผู้อ้างจะต้องนำเอกสารต้นฉบับมาสืบเสมอ เพราะคดีอาญาไม่มีหลักเกณฑ์เรื่องการสันนิษฐานความถูกต้องแท้จริง โดยการที่อีกฝ่ายหนึ่งไม่คัดค้านตาม ปวิพ. มาตรา 125 แต่ถ้าคู่ความอ้างหนังสือราช

การเป็นพยาน แม้จะมีต้นฉบับอยู่จะส่งสำเนาที่เจ้าหน้าที่รับรองว่าถูกต้องก็ได้ เว้นแต่ในหมายเรียกจะบ่งไว้เป็นอย่างอื่น (ปวิอ. มาตรา 238 วรรค 2) (22)

จากที่ได้กล่าวมาข้างต้นนี้จะเห็นได้ว่าหลักเกณฑ์ในเรื่องการรับฟังเอกสารต้นฉบับนั้นเป็นอุปสรรคสำคัญในการรับฟังพยานหลักฐานจากเครื่องคอมพิวเตอร์ จากเหตุผลดังกล่าวนี้หลักเกณฑ์ในการใช้เอกสารจากคอมพิวเตอร์เป็นพยานหลักฐานในศาลนั้น ควรที่จะมีวิธีการแตกต่างไปจากเอกสารอื่นๆ โดยมุ่งเน้นที่กระบวนการในการชั่งน้ำหนักพยานและการพิสูจน์ความถูกต้องแท้จริง (Authentication)

3. แนวทางในการพิจารณาพยานหลักฐานอิเล็กทรอนิกส์ (Electronic/Computer Record)

3.1 การตรวจสอบความถูกต้องแท้จริง (Authentication)

การพิสูจน์ความถูกต้องแท้จริงของพยานอิเล็กทรอนิกส์ (Authentication of Electronic Evidence)

แม้ว่า “ลายมือชื่อ” จะเป็นประโยชน์ แต่ก็อาจไม่ใช่สิ่งที่จำเป็นมากนัก พยานหลักฐานที่ใช้เพื่อการพิสูจน์ความถูกต้องแท้จริง (Authenticity) ของข้อความหรือเอกสารคอมพิวเตอร์ (Message or computer record) อาจเป็นพยานบุคคลที่แสดงให้เห็นถึงพฤติการณ์แวดล้อมกรณีของข้อความอิเล็กทรอนิกส์ดังกล่าว ลักษณะภายในของข้อความอิเล็กทรอนิกส์ดังกล่าว หรือการแสดงให้เห็นถึงกระบวนการทำงานในการจัดทำข้อความอิเล็กทรอนิกส์ดังกล่าว ในหลายกรณีอาจรวมถึงการแลกเปลี่ยนความเข้าใจระหว่างคู่สัญญาจะช่วยสำหรับการพิสูจน์ความถูกต้องแท้จริงก็ได้ และความถูกต้อง (Conscientious) การสร้างอย่างเป็นระบบ และการเก็บรักษาข้อมูลอาจช่วยในการพิสูจน์ความถูกต้องแท้จริง เทคนิคการเก็บรักษาข้อมูลที่ควรรวมถึงความชัดเจนและเส้นทางการจัดเก็บเอกสาร (Documented chain) ในกรณีที่เอกสารอยู่ในมือของบุคคลที่มีเจตนาหรือไม่มีเจตนาในทางที่มิชอบ วิธีหนึ่งในการพิสูจน์ความถูกต้องแท้จริงของเอกสารคือการใช้ลายมือชื่อดิจิทัลซึ่งถือว่าเป็นเครื่องมือที่มีประสิทธิภาพ

3.1.1 อะไรที่ก่อให้เกิดการพิสูจน์ความถูกต้องแท้จริง

การพิสูจน์ความถูกต้องแท้จริง (Authentication) คือหน้าที่ตามข้อกำหนดของกฎหมาย พยานหลักฐาน ผู้ที่ยื่นพยานหลักฐานจะต้องพิสูจน์ว่าพยานหลักฐานที่ยื่นถูกต้องตรงกับสิ่งที่ผู้ยื่นยืนยัน⁸⁰

อย่างไรก็ดี โดยปกติหลังจากที่ศาลได้อนุญาตที่จะรับฟังพยานหลักฐาน ข้อเท็จจริงแห่ง คดี (Trier of fact) ยังคงเปิดเสรีให้เชื่อหรือไม่เชื่อความถูกต้องแท้จริงของพยานหลักฐาน ดังนั้นหาก เอกสารจากเครื่องแฟกซ์ (Fax Printout) ก่อให้เกิดความถูกต้องแท้จริงในการยอมรับฟังเป็นพยานหลักฐาน คู่กรณีอีกฝ่ายหนึ่งยังสามารถเสนอพยานเพื่อยืนยันข้อเท็จจริง (Trier of Fact) ว่าเอกสารจากเครื่อง แฟกซ์ดังกล่าวเป็นเอกสารปลอม

แต่สำหรับการพิสูจน์ความถูกต้องแท้จริง (Authentication) ของข้อความอิเล็กทรอนิกส์อาจ ก่อให้เกิดปัญหาที่แตกต่าง สำหรับเอกสารที่เป็นกระดาษข้อความและเอกสาร (record) จะเป็นสิ่งเดียวกัน และเป็นสื่อที่มีความคงทน (Durable Medium) ดังนั้นการพิสูจน์ความถูกต้องแท้จริงจะทำกับข้อความและ เอกสารพร้อมกัน แต่สำหรับข้อความอิเล็กทรอนิกส์จะเกี่ยวพันกับสองปัญหาดังกล่าวคือ (1) อะไรคือข้อ ความที่แท้จริง และ (2) เอกสาร (Record) นั้นเป็นเอกสารที่แท้จริงของข้อความนั้นหรือไม่

3.1.2 ความถูกต้องแท้จริงเป็นปัญหาทางปฏิบัติ

เมื่อข้อพิพาททางธุรกิจเกิดขึ้น ปัญหาในเรื่องการพิสูจน์ความถูกต้องแท้จริงของข้อความ (Message) และเอกสาร (Record) จะไม่ใช่ปัญหาใหญ่นัก ข้อพิพาทที่เกิดขึ้นมักจะเป็นปัญหาการตีความ และเนื้อหาของเนื้อหาข้อความ (Message Contents) มากกว่า ผู้ที่คัดค้านพยานหลักฐานสามารถยืนยันจากเอกสารของเขาเพื่อการพิสูจน์ความถูกต้องแท้จริงของข้อความและเอกสารที่เสนอโดยผู้ยื่นพยาน หลักฐานดังกล่าว

ศาลจะไม่เชื่อถือการทดสอบยืนยันที่ไม่มี ความหมาย และการทดสอบพยานมักต้องใช้ เวลาและเงินจำนวนมากสำหรับคู่ความทั้งสองฝ่าย

3.1.3 การพิสูจน์ความถูกต้องแท้จริงของเนื้อหาเอกสารทางอิเล็กทรอนิกส์

⁸⁰ โปรดดู Fed. R. Evid. 901(a)

การรับฟังเนื้อหาของข้อความอิเล็กทรอนิกส์ (Electronic-message contents) เป็นพยานหลักฐานหรือ เพื่อพิสูจน์ความถูกต้องแท้จริงของข้อเท็จจริง ผู้ที่แสดงพยานหลักฐานดังกล่าวจะต้องแสดงต้นตอ (ใครหรืออะไรที่ก่อให้เกิดข้อมูล) และความสมบูรณ์ (integrity) (ไม่ว่าเนื้อหาจะมีความสมบูรณ์หรือปรากฏตามแบบที่ต้องการหรือไม่ หรือมีข้อผิดพลาดหรือมีการปลอมแปลงหรือไม่) ผู้จัดการธุรกิจ (Business Manager) นักเทคนิค และผู้ตรวจสอบ (Auditors) ล้วนแต่มีความคุ้นเคยกับปัญหาดังกล่าวนี้นอกจากนั้นพวกเขายังกังวลความถูกต้องแท้จริงของข้อความ สำหรับในกรณีของข้อมูลที่ปลอมและความไม่ปลอดภัย ผู้จัดการและนักเทคนิคน่าจะมีการควบคุมทางเทคนิคที่เหมาะสมเพื่อป้องกันการเกิด การยอมรับ หรือ การประมวลผลข้อมูลที่ปลอมและไม่ถูกต้อง

ในการพิจารณาคดีที่มีการโต้แย้งในเรื่องของความถูกต้องแท้จริง การผู้เสนอพยานหลักฐานดังกล่าวต้องการแสดงพยานหลักฐานที่น่าเชื่อถือกว่าข้อความดังกล่าวเป็นข้อความจริง พยานหลักฐานอิเล็กทรอนิกส์ผู้ยื่นซึ่งเป็นผู้รับเอกสารอิเล็กทรอนิกส์จะต้องเสนอพยานประกอบดังต่อไปนี้ (1) คำให้การ (Testimony) และกระบวนการการจัดทำเอกสาร นโยบายของผู้รับในการเลือกข้อความ (Policies for screening messages) และการตอบกลับว่าได้รับข้อความดังกล่าวแล้ว (Returning Acknowledgments) (2) Log ที่แสดงว่าได้มีการตอบกลับการยอมรับข้อความที่เป็นปัญหาหรือไม่และเมื่อไร (3) พยานหลักฐานที่เนื้อหาและพฤติกรรมแวดล้อมกรณีของข้อความตรงกับสิ่งที่คาดหวังจากผู้ส่งหรือไม่ และ (4) หลักฐานในเรื่องของที่น่าเชื่อถือของระบบสื่อสารที่ส่งผลให้ข้อความดังกล่าวมีความสมบูรณ์

พยานหลักฐานแวดล้อมกรณีสามารถใช้พิสูจน์ความถูกต้องแท้จริงได้ ตัวอย่างเช่น ข้อมูลที่เกี่ยวกับพยานแวดล้อมกรณีของเอกสารอิเล็กทรอนิกส์ (Electronic Record) อาจไม่ครอบคลุมการใช้อุปกรณ์ซอฟต์แวร์ใหม่ (Software tools) ที่เรียกว่า “data-mining” ที่สามารถกรองข้อมูลจำนวนมากและเลือกเฉพาะรูปแบบและความสัมพันธ์ที่มีความหมาย ผู้ออกบัตรเครดิตใช้เครือข่ายคอมพิวเตอร์ที่มีซอฟต์แวร์ดังกล่าวที่ทำการประเมินพยานแวดล้อมกรณีที่เกี่ยวข้องกับการอนุมัติตามรายการที่ร้องขอและตรวจสอบการฉ้อโกงที่อาจเกิดขึ้น ตัวอย่างเช่น ถ้าบัตรที่ออกให้กับลูกค้าผู้ขายที่ยังเป็นโสดในชิคาโก ถูกนำไปใช้

เพื่อซื้อชุดคลุมท้อง (Maternity Clothes) และนำไปถอนเงินในท้องที่ห่างไกล บัตรเครดิตดังกล่าวอาจได้รับการปฏิเสธหรือผู้ขายสินค้าอาจขอหลักฐานเพิ่มเติม⁸¹

พยานแวดล้อมกรณีของข้อความอิเล็กทรอนิกส์อาจเกี่ยวข้องกับการตรวจสอบความถูกต้องแท้จริงและสามารถใช้เป็นหลักฐานในการแสดงความสมบูรณ์ (Integrity) ของข้อมูลได้ ซึ่งอาจใช้ "ลายมือชื่อทางดิจิทัล" (Digital Signature) ประกอบการนำสืบก็ได้

ผู้ที่ทำการโต้แย้งพยานหรือข้อความทางอิเล็กทรอนิกส์ที่ส่งมาอาจใช้เทคนิคเช่นเดียวกันในการปฏิเสธข้อความอิเล็กทรอนิกส์ดังกล่าว ในคดีทะเลาะวิวาทระหว่าง Dutch-Swiss ในเวลา 6.30 น. นโยบายที่ถูกต้องตรงกันเมื่อออกของธนาคาร Dutch เมื่อออก Telex Guarantee ที่ส่งจากสาขาหลักเพียงเท่านั้น และที่ใช้ Test Keys หรือ Mail Confirmation ในทางกลับกันฝ่าย Swiss Bank ซึ่งเป็นผู้รับถือว่าทะเลาะวิวาทที่ไม่ปลอดภัย (Insecure telex) มีความถูกต้องแท้จริง การที่ไม่ต้องการ Test Key หรือการยืนยันการรับทะเลาะวิวาท Dutch Bank ซึ่งถือครองการควบคุมที่ดีกว่าและพยานหลักฐานที่ดีกว่าเมื่อมีข้อพิพาทเกิดขึ้น ลายมือชื่อดิจิทัลเกี่ยวกับเทคโนโลยีที่เกี่ยวข้องกับการใช้เพื่อทดสอบทะเลาะวิวาท และเมื่อใช้พร้อมกับขั้นตอนในการรักษาความปลอดภัยที่เหมาะสมในการรักษารหัส (Key) ที่ใช้เพื่อทำให้เกิดลายมือชื่อดิจิทัล ควรที่จะมีความน่าเชื่อถือเช่นเดียวกันในการตรวจสอบความถูกต้องแท้จริงของข้อมูลอิเล็กทรอนิกส์⁸²

ปัญหาที่เกี่ยวกับการตรวจสอบความถูกต้องแท้จริงของข้อความคอมพิวเตอร์ (Computer Message) คือการตรวจสอบความถูกต้องแท้จริงของข้อมูลนำเข้าในเครื่องคอมพิวเตอร์ ตัวอย่างเช่นในคดี Victory Memorial Hospital v. Rice⁸³ โรงพยาบาลทดลองที่จะยอมรับเอกสารคอมพิวเตอร์ (Computer Record) ของบริการทางการแพทย์ที่ให้กับผู้ป่วย การบันทึกข้อมูลดังกล่าวได้มาจากข้อมูลที่ปรากฏบนเอกสารที่เป็นกระดาษ (เช่นผลตรวจสอบของห้องทดลอง (Laboratory test report) จะถูกบันทึกเข้าเครื่องคอมพิวเตอร์โดยพนักงาน ในการทดลองดังกล่าว คนไข้ได้ตั้งคำถามเกี่ยวกับความน่าเชื่อถือของข้อมูล

⁸¹ Wallace, Neural Network Computers are Monitoring Your Credit Purchases, N.Y. Times on the Web (Dec. 25, 1996)

⁸² โปรดดู Benjamin Wright and Jane K. Winn, The Law of Electronic Commerce, Aspen Law & Business, New York, 1997, pp. 6-6

⁸³ 493 N.E.2d 117 (Ill. App. 2d Dist. 1986)

ก่อนที่จะมีการนำเข้าบันทึกในเครื่องคอมพิวเตอร์ เพื่อที่จะพิสูจน์ความถูกต้องแท้จริงของข้อมูล โรงพยาบาลจะต้อง (1) ทำตัวอย่างของแบบต้นฉบับและเปรียบเทียบให้เห็นว่าตรงกับข้อมูลที่บันทึกในเครื่องคอมพิวเตอร์ (2) ให้การ (Testimony) ถึงความน่าเชื่อถือของขั้นตอนและกระบวนการของโรงพยาบาลที่เกี่ยวข้องกับการรวบรวมข้อมูลและการบันทึกข้อมูล ศาลได้ตัดสินว่าโรงพยาบาลได้วางรากฐานที่เพียงพอสำหรับการทำให้เอกสารทางอิเล็กทรอนิกส์สามารถรับฟังได้ และตั้งข้อสังเกตว่าคนไข้ยังคงสามารถโต้แย้งต่อลูกขุน (ตามข้อเท็จจริง (Trier of Fact) ว่าเอกสารอิเล็กทรอนิกส์นั้นมีข้อบกพร่องและไม่น่าหนักเพียงพอที่จะรับฟัง

3.1.4 การตรวจสอบความถูกต้องแท้จริงของเอกสารอิเล็กทรอนิกส์

การพิสูจน์ความถูกต้องแท้จริงของเอกสารคอมพิวเตอร์ (Computer Record) สามารถใช้พยานบุคคลสืบพยานในเรื่องดังต่อไปนี้ (1) ขั้นตอนที่ใช้ในการสร้างและการเก็บรักษาเอกสาร และ (2) เส้นทางเดินของการจัดเก็บเอกสารหลังจากที่จัดสร้าง

คดีที่เกี่ยวข้องกับเอกสารคอมพิวเตอร์ (Computer Record) ส่วนใหญ่จะเป็นเรื่องที่ผสมผสานระหว่างปัญหาในการพิสูจน์ความถูกต้องแท้จริงและการวิเคราะห์ในเรื่องของหลัก Hearsay Rule หรือ ข้อยกเว้นสำหรับเอกสารทางธุรกิจ United v. Jones ศาลกล่าวว่าเอกสารคอมพิวเตอร์ที่จะได้คุณภาพตามข้อยกเว้นพยานบุคคลจะต้องสามารถชี้ให้เห็นว่าเอกสารเป็นเอกสารที่ถูกต้องแท้จริงและจะต้องระบุว่าเอกสารดังกล่าวจะต้องทำและเก็บรักษาไว้ตามทางปฏิบัติอันเป็นปกติธุระทางธุรกิจ⁸⁴

ในเรื่องของข้อความทางอิเล็กทรอนิกส์ (Electronic Message) พยานจะต้องสามารถอธิบายถึงสภาพการณ์แวดล้อมของการสร้าง Message Record และเส้นทางการเดินของการเก็บ Record ดังกล่าวโดยทั่วไปแล้ว พยานบุคคลดังกล่าวจะไม่จำเป็นที่จะต้องมีความรู้ว่ามีข้อมูลอย่างไรใน Record หรือได้มีส่วนร่วมในการสร้าง อย่างไรก็ตาม เขาก็จำเป็นต้องรู้กระบวนการเก็บรักษาเอกสาร (Recordkeeping Process)⁸⁵ ผู้ที่เหมาะสมที่จะเป็นผู้ที่เป็นพยานนำสืบดังกล่าวควรที่จะเป็นผู้จัดการ (Manager) ที่ทำหน้าที่

⁸⁴ 554 F.2d 251, 252 (5th Cir.), cert. Denied, 434 U.S. 866 (1977)

⁸⁵ McCormick on Evidence, Cleary ed., 2d ed. 1984, 881

เกี่ยวกับการประมวลผลข้อมูลและระบบการสื่อสาร ในการพิจารณาคดี พยานบุคคลจะต้องชี้ให้เห็นถึงระบบและการทำงานโดยทั่วไปและอาจต้องอธิบายถึงขั้นตอนในการทำดัชนีและการเก็บเอกสาร

การปฏิเสธเอกสารอิเล็กทรอนิกส์ อาจเกิดจากผู้เก็บเอกสารสามารถเข้าไปทำการแก้ไขเพิ่มเติม (หรือได้รับอนุญาตที่จะเข้าไปแก้ไขเพิ่มเติม) ศาลอาจให้เหตุผลว่าการพิสูจน์ความถูกต้องแท้จริงของเอกสารนั้นไม่น่าเชื่อถือถ้าเห็นว่าความสามารถและผู้เก็บรักษาเอกสาร (Recordkeeper) มีมูลเหตุจูงใจที่จะปลอมแปลงเอกสารดังกล่าว การจ้างผู้เก็บรักษาเอกสารที่ไว้วางใจได้สามารถช่วยในการพิสูจน์ความถูกต้องแท้จริงของเอกสาร เช่นในคดี *United States v. Poindexter*⁸⁶ ดูเหมือนว่าจะเป็นไปได้ที่เอกสารของข้อความอิเล็กทรอนิกส์ (Record of the electronic message) ที่เป็นปัญหาเป็นเอกสารที่ถูกต้องแท้จริงเนื่องจากเอกสารดังกล่าวได้รับการเก็บรักษาโดยบุคคลที่เป็นกลาง ซึ่งในที่นี้ก็คือ ผู้ให้บริการระบบไปรษณีย์อิเล็กทรอนิกส์ (E-mail System Operator)⁸⁷

ในคดี *United States v. Briscoe*⁸⁸ รัฐบาลสหรัฐได้ยื่นเอกสารคอมพิวเตอร์ (Computer Record) เป็นพยานหลักฐานซึ่งเอกสารดังกล่าวเก็บรักษาไว้โดยบริษัทโทรศัพท์ท้องถิ่น เหตุผลของการยอมรับฟังพยานเอกสารคอมพิวเตอร์ดังกล่าว คือผู้เก็บรักษาเอกสารดังกล่าวของบริษัทโทรศัพท์ที่ได้ให้การว่าเป็นการกระทำโดยทั่วไปอันเป็นปกติในทางธุรกิจ จำเลยอุทธรณ์คัดค้านเหตุผลดังกล่าวในเหตุผลที่ว่าข้ออ้างดังกล่าวไม่เพียงพอเนื่องจากไม่ได้แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ที่เป็นปัญหามักจะถูกทดสอบอยู่เสมอว่ามีความผิดพลาดในการทำโปรแกรม (Programming Error) ศาลอุทธรณ์ยกฟ้องโดยให้เหตุผลว่า “ตราบไคที่รัฐบาลให้ข้อเท็จจริงเพียงพอที่จะประกันได้ว่าการค้นพบเอกสารดังกล่าวไม่น่าเชื่อถือและฝ่ายที่คัดค้านมีโอกาสที่จะแสวงหาความถูกต้องและวิธีที่เอกสารดังกล่าวถูกจัดเก็บและจัดทำ

พยานบุคคลที่จะมานำสืบเกี่ยวกับเอกสารคอมพิวเตอร์นั้นไม่จำเป็นที่จะต้องเป็นผู้เชี่ยวชาญทางคอมพิวเตอร์ เช่นในคดี *United States v. Linn*⁸⁹ ผู้อำนวยการฝ่ายการสื่อสาร (Director of communications) สำหรับโรงแรมที่จะพิสูจน์ความถูกต้องแท้จริงของเอกสารที่พิมพ์ออกมาจากเครื่อง

⁸⁶ Transcript of Trial, at 17-22-1769, *United States v. Poindexter* (Crim. No. 88-0080-1)ZD.D.C. 1990)

⁸⁷ โปรดดู Manual for Complex Litigation 123 (5th ed. 1982)

⁸⁸ 896 F.2d 1476 (7th Cir.), cert. Denied sub nom. *United States v. Usman*, 498 U.S. 863 (1990)

⁸⁹ 880 F.2d 209 (9th Cir. 1989)

คอมพิวเตอร์ (Computer Printout) ที่แสดงว่าหมายเลขโทรศัพท์ที่เรียกจากห้องและเวลาที่ใช้โทรศัพท์ แม้ว่าพยานดังกล่าวจะไม่ได้อธิบายถึงกระบวนการทางเทคนิคว่าเอกสารดังกล่าวทำขึ้นมาอย่างไร ความรู้ของพยานบุคคลเกี่ยวกับที่มาของเอกสารและความสามารถที่จะแสดงให้เห็นว่าเอกสารดังกล่าวเป็นเอกสารทางธุรกิจ ศาลกพอใจแล้ว

ในคดี American Oil Co. v. Valenti⁹⁰ เอกสารที่พิมพ์ออกมาจากเครื่องคอมพิวเตอร์ (Computer Printout) ระบุรายการในบัญชีโดยสรุประหว่างผู้ขายและลูกค้าสามารถใช้ผู้จัดการฝ่ายขาย (Sales Manager) ผู้ดูแลบัญชีดังกล่าวเป็นผู้นำสืบได้ เนื่องจากเขารู้เกี่ยวกับการทำงานของเครื่องคอมพิวเตอร์จากการรับรายงานประจำเดือนที่ได้จากเครื่องคอมพิวเตอร์และจากงานของเขาที่ทำร่วมกับ Computer Operator แต่เขาไม่มีประสบการณ์โดยตรงกับเครื่องคอมพิวเตอร์

3.1.5 แฟกซ์ในฐานะที่เป็นพยานหลักฐาน

ในคดี People v. Hagan⁹¹ ศาลได้ใช้มาตรฐานเดียวกับการรับฟังพยานหลักฐานที่เป็นเอกสารคอมพิวเตอร์ นำมาใช้กับแฟกซ์

ข้อเท็จจริง คดี Hagan เป็นคดีอาญา Hagan เป็นจำเลยที่ถูกกล่าวหาว่าปลอมเอกสารทางการเงินแล้วส่งแฟกซ์ไปยังตัวแทนบริษัทให้เขาพื้นที่ซึ่งตัวแทนดังกล่าวจะเป็นผู้พิจารณาว่าจะให้เขาพื้นที่กับ Hagan หรือไม่ เอกสารที่ปลอมดังกล่าวจะมีจดหมายจากธนาคารรับรองว่า Hagan มีเงินอยู่ในบัญชีจริง แฟกซ์แสดงให้เห็นว่าถูกส่งจาก Mailboxes, Etc.store ศูนย์ไปรษณีย์ย่อยที่ให้บริการส่งแฟกซ์ต่อประชาชนโดยทั่วไป

ประเด็นสำคัญคือว่าแฟกซ์ที่ได้รับโดยตัวแทนบริษัทให้เขาพื้นที่ถูกต้องแท้จริงเพียงพอหรือไม่ (ที่จะแสดงว่าอะไรคือสิ่งที่แท้จริง) ที่จะยอมรับเป็นพยานหลักฐานในการพิจารณาคดี

การยอมรับฟัง (Admissibility)

⁹⁰ 426 A.2d 305 (Conn.1979)

⁹¹ 583 N.E.2d 494 (Ill. 1991)

ศาลในคดี Hagan กล่าวว่าไม่เคยกำหนดมาตรฐานสำหรับแฟกซ์เพื่อการยอมรับฟังเป็นพยานหลักฐาน ศาลจึงตัดสินใจที่จะใช้มาตรฐานเช่นเดียวกับที่ใช้กับเอกสารที่พิมพ์จากเครื่องคอมพิวเตอร์มาใช้กับ Fax ในคดีนี้

มาตรฐานของการยอมรับฟังพยานหลักฐานคอมพิวเตอร์ของอิลลินอยส์ที่ใช้กับเอกสารที่พิมพ์จากเครื่องคอมพิวเตอร์ได้กำหนดไว้เป็นครั้งแรกในคดี Grand Liquor Co. v. Department of Revenue⁹² และคดี King v. State ex rel. Murdock Acceptance Corp.⁹³ กำหนดให้เอกสารที่พิมพ์ออกจากเครื่องคอมพิวเตอร์จะสามารถยอมรับฟังได้ถ้าแสดงให้เห็นว่า

(1) อุปกรณ์ในการคำนวณทางอิเล็กทรอนิกส์มีมาตรฐานตามที่รับรองโดยทั่วไป (2) รายการบันทึก (Entries) ที่ทำขึ้นทำเป็นปกติหรือใกล้เคียงกับเวลาที่มีการบันทึกข้อมูลดังกล่าว และ (3) พยานบุคคลสามารถนำเสนอให้เป็นที่น่าพอใจกับศาลว่าที่มาของข้อมูล วิธีและเวลาในการจัดเตรียมเอกสารมีความน่าเชื่อถือและมีเหตุผลเพียงพอที่จะยอมรับฟังเป็นพยานหลักฐานได้⁹⁴

โจทก์ในคดีนี้ได้นำเสนอถึงพยานแวดล้อมกรณี เจ้าหน้าที่ของ Mailboxes, Etc. ได้อธิบายว่ากระบวนการโดยปกติในการใช้แฟกซ์จากร้านและกระบวนการในการหาข้อผิดพลาดในระหว่างการทำงาน ส่วนบริษัทให้เข้าพื้นที่สืบพยานว่าเขาได้รับแฟกซ์ดังกล่าวจริงและไม่มีใครกล่าวอ้างว่าแฟกซ์ดังกล่าวมีข้อผิดพลาด เครื่องแฟกซ์ก็ได้ถูกใช้หลายครั้งและก็ไม่เคยพบว่ามีปัญหาแต่อย่างใด และเนื้อหาของแฟกซ์ที่ส่งก็ตรงกับข้อเท็จจริงอื่นๆและพฤติกรรมในคดี

3.1.6 การพิสูจน์ความถูกต้องแท้จริงเอกสารอิเล็กทรอนิกส์ในฐานะที่เป็นสัญญา

การพิสูจน์ความถูกต้องแท้จริงสามารถทำได้โดยวิธีการดังต่อไปนี้

พิสูจน์แหล่งที่มาของอำนาจ : ชุดรายการข้อมูล EDI ที่มุ่งจะให้มีความผูกพันเป็นสัญญาควรจะสามารถตรวจสอบถึงตัวบุคคลได้เพื่อจะยืนยันอำนาจในการทำคำเสนอ ลายมือชื่อทางอิเล็กทรอนิกส์เป็น

⁹² 367 N.E.2d 1238 (Ill. 1977)

⁹³ 222 So. 2d 393 (miss. 1969)

⁹⁴ Hagan, 583 N.E.2d p. 504

ตัวอย่างหนึ่งในการพิสูจน์ว่าบุคคลใดเป็นผู้ทำคำเสนอ แหล่งอื่นๆ ที่สามารถใช้พิสูจน์ได้คือ System Monitor's Log ระบบการจัดเก็บเอกสาร (Record Custodian) หรือเจ้าหน้าที่ที่มีหน้าที่ในการจัดเก็บสามารถใช้เป็นเครื่องยืนยันในฐานะที่เป็นหลักฐานชั้นที่สอง (Secondary Record)

พิสูจน์ความน่าเชื่อถือของระบบฮาร์ดแวร์ ระบบซอฟต์แวร์ การฝึกอบรมพนักงานและสื่อการเก็บข้อมูล (Record Storage Media) : เอกสารทางธุรกิจมักจะยอมรับการให้การของพยานบุคคลที่ให้การถึงว่าระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ และสื่อเก็บข้อมูลได้รับการดูแลรักษาเป็นอย่างดี รวมทั้งพนักงานที่เกี่ยวข้องได้รับการฝึกอบรมการดูแลดังกล่าวมาอย่างเหมาะสมเช่นกัน ประกอบกับคำยืนยันที่ว่าระบบทั้งหมดได้ใช้เพื่อวัตถุประสงค์ในทางธุรกิจอันเป็นปกติ นอกจากนั้นยังอาจต้องยืนยันว่าไม่มีปัญหาหรือข้อขัดข้องเกิดขึ้นกับระบบทั้งหมดรวมทั้งสื่อเก็บข้อมูล โปรแกรมคอมพิวเตอร์ หรือเอกสารอื่นๆ เป็นต้น

การพิสูจน์เส้นทางการเก็บเอกสาร (Prove the Chain of Custody of the Record) : ควรใช้พยานบุคคลนำสืบให้ชัดเจนถึงเส้นทางการเก็บเอกสาร EDI ความจริงที่ว่าเอกสารอาจถูกย่อหรือแปลในระหว่างการโอนจากผู้เก็บรักษาข้อมูลหนึ่งไปยังอีกฝ่ายหนึ่งควรจะได้รับ การสนับสนุนโดยการแสดงความน่าเชื่อถือของกระบวนการที่ใช้ ความสำคัญอยู่ที่ว่าในแต่ละขั้นตอนของการเก็บรักษาข้อมูลมีหน้าที่ทางธุรกิจที่จะต้องปกป้องและเก็บรักษาเอกสารให้ถูกต้องและหน้าที่ดังกล่าวได้ทำไปอย่างเพียงพอ

พิสูจน์ความถูกต้องของเอกสารที่น่าเสนอ : เอกสารทางธุรกิจจะได้รับการยอมรับขึ้นอยู่กับความน่าเชื่อถือของระบบและการแสดงว่าได้เก็บรักษา (Custody) เอกสารดังกล่าวอย่างเหมาะสม อย่างไรก็ตาม เอกสาร EDI ของฝ่ายตรงข้ามอาจเสนอเอกสารที่น่าเชื่อถือในรายการข้อมูลที่ต้องการ ในกรณีที่เอกสารมีความขัดแย้งกัน อาจจำเป็นต้องมีการอธิบายถึงความแตกต่างดังกล่าว

พิสูจน์การตีความของเอกสารที่น่าเสนอ : เอกสาร EDI หลายชิ้นจะไม่มีน้ำหนักมากนักหากไม่มีข้อกำหนดในสัญญาการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ อาจต้องใช้สัญญาดังกล่าวเพื่อช่วยในการตีความเอกสาร EDI ดังกล่าว

3.2 การชั่งน้ำหนักพยาน (Weighting)

กฎหมายเรื่องพยานหลักฐานเดิมมักจะคำนึงถึงน้ำหนักของพยานหลักฐานสามประการด้วยกันคือ 1. น้ำหนักของพยานหลักฐาน (Preponderance of the evidence) 2. ความชัดเจนและความน่าเชื่อถือของพยานหลักฐาน และ 3. ไม่มีข้อสงสัยอย่างอื่น (Beyond the reasonable doubt evidence)

สำหรับการพิจารณาคดีแพ่งโดยทั่วไป โฉมท่งจะต้องแสดงถึง “น้ำหนักของพยานหลักฐาน” (Preponderance of the Evidence)

นโยบายพื้นฐานสำหรับกฎหมายพยานหลักฐานทางคอมพิวเตอร์ จะแสดงไว้ใน Manual for Complex Litigation⁹⁵ ซึ่งมีรายละเอียดดังต่อไปนี้

1. เอกสารต้องมีอยู่ (Record Must Exist)

ขั้นตอนแรกในการหาพยานหลักฐานที่ยอมรับได้ทางกฎหมายคือการสร้างเอกสารทางอิเล็กทรอนิกส์ ถ้าเอกสารไม่ได้สร้างมาในตอนแรก เอกสารเหล่านี้ก็ไม่สามารถใช้ต่อไปได้ เอกสารชิ้นไหนที่จะต้องใช้เป็นเอกสารที่จะต้องใช้เป็นพยานหลักฐานในอนาคต เอกสารบางอย่างอาจได้รับการยอมรับว่ามีประโยชน์สำหรับยืนยันข้อเท็จจริงบางอย่าง นอกจากนั้นอาจต้องคิดล่วงหน้าว่า เอกสารดังกล่าวที่จะนำมาใช้เป็นพยานหลักฐานในอนาคตมีข้อบกพร่องอย่างไรและแก้ไขอย่างไร อย่างไรก็ตาม กิติเอกสารที่เกี่ยวข้องกับการใช้ EDI ควรที่จะเก็บไว้ให้มากที่สุดเท่าที่จะเก็บได้จะเป็นการดี

เอกสารของรายการข้อมูล EDI ควรจะมีองค์ประกอบพื้นฐานดังต่อไปนี้ 1. สำเนาของรายการข้อมูล 2. วิธีที่จะติดตามรายการข้อมูลทั้ง Forward และ Backward ระหว่างผู้ส่งและผู้รับ 3. ตัวชี้บางอย่างที่ระบุว่าเอกสารมีความถูกต้องแท้จริง และ 4. ดัชนีและการตรวจสอบข้ามระบบเพื่อที่จะสามารถกู้ (Recover) ข้อมูลมาใช้ได้หากจำเป็น

2. พยานหลักฐานจะต้องมีความเกี่ยวข้อง

⁹⁵ Sections 2.711 – 2.716 Manual for Complex Litigation, 5th ed. (New York: Clark Boardman, 1982)

พยานหลักฐานที่จะสามารถยอมรับฟังได้จะต้องมีความเกี่ยวข้องกับประเด็นแห่งคดี โดยปกติแล้วพยานหลักฐานจะถือว่า “เกี่ยวข้อง” หากมีแนวโน้มที่จะแสดงอย่างมีเหตุผลว่าการยืนยันบางอย่างอาจมีผลต่อกระบวนการตัดสินใจน่าจะเป็นความจริง⁹⁶ ตามหลักกฎหมายว่าด้วยพยานหลักฐาน พยานหลักฐานจะมีความเกี่ยวข้องในฐานะเป็นข้อเท็จจริงที่มาสนับสนุนข้อเท็จจริงที่ต้องการพิสูจน์⁹⁷

3. พยานหลักฐานต้องน่าเชื่อถือ (Evidence Must Be Credible)

พยานหลักฐานจะไม่มีประโยชน์แต่อย่างใดหากไม่สามารถเชื่อถือได้ ผู้ที่ค้นหาความจริงจะต้องถูกทำให้เชื่อว่าเอกสาร EDI นั้นเป็นเอกสารที่ถูกต้องแท้จริง สมบูรณ์และไม่ได้ถูกแก้ไขแน่นอนเป็นไปได้ว่าพยานหลักฐานอาจดูน่าเชื่อถือมากเกินไป ตัวอย่างเช่นผู้ค้นหาความจริงอาจเห็นบางสิ่งบางอย่างที่มาจากเครื่องคอมพิวเตอร์ว่าไม่มีข้อผิดพลาดเลยซึ่งอาจไม่เป็นประเด็นอย่างชัดเจน⁹⁸ องค์ประกอบหลายอย่างจะเกี่ยวข้องกับการวัดความน่าเชื่อถือของพยานหลักฐานที่อาจทำให้เรื่องนี้เป็นเรื่องที่ไม่ค่อยมีความชัดเจนในกฎหมาย ไม่มีใครสามารถบอกได้ว่าพยานหลักฐานอะไรที่เพียงพอกับการยืนยันข้อเท็จจริง อย่างไรก็ตามก็มีหลักในเบื้องต้นดังต่อไปนี้

การเก็บรักษาเอกสาร EDI (Custody of EDI Records)

การเก็บรักษาเอกสาร EDI มีความสำคัญเนื่องจากเหตุผลหลายประการ ความสำคัญที่เกี่ยวกับวัตถุประสงค์ในการสืบพยานคือว่าเอกสารที่เก็บรักษาไว้อย่างเหมาะสมนั้นย่งที่จะสืบค้น และยากที่จะถูกแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต การเก็บรักษาเอกสารที่เหมาะสมจะเป็นส่วนสำคัญในการยอมรับเอกสารที่จับต้องได้เป็นพยานหลักฐาน

ข้อตกลงการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic Data Interchange Agreement) และ/หรือ ข้อตกลงการใช้บริการเครือข่าย (Network Agreement) จะต้องวางข้อกำหนดว่าด้วยการเก็บรักษาเอกสารที่เหมาะสม (Proper Custodian) ผู้เก็บรักษาเอกสารมักจะเป็นที่ซึ่งสามารถหาพยาน

⁹⁶ โปรดดู 5.01 [c]. Federal Rule of Evidence 401

⁹⁷ โปรดดู 5.01 [c]. Federal Rule of Evidence 401 (b)

⁹⁸ โปรดดู D. Bender, Computer Law: Litigation, Chapter 8, "Probative Value" (1990)

หลักฐานที่มีความสำคัญอันดับแรก (Primary Source) ในกรณีที่มีข้อพิพาท คู่พิพาทมักจะใช้เอกสารอื่นๆ (เช่น Working File และ Transaction Log) มาช่วยสนับสนุนเอกสารที่เก็บรักษาไว้ (Archivist's record)

การเสนอให้เอกสาร EDI เป็นพยานหลักฐาน อาจมีความจำเป็นที่จะต้องใช้คำให้การเป็นลายลักษณ์อักษร (Affidavit) หรือสืบพยานบุคคล (Live Testimony) เกี่ยวกับการจัดเก็บเอกสาร (Custody of Records) ประวัติการจัดเก็บเอกสารจำเป็นที่จะต้องนำมาชี้แจงให้เห็นชัดเจน จะต้องไม่มีส่วนที่ไม่สามารถอธิบายได้หรือมีความคลุมเครือ เอกสาร การจัดเก็บแฟ้มข้อมูล (Archive) การทำดัชนี และระบบ Log สำหรับรายการข้อมูล EDI ที่ได้รับการออกแบบอย่างเหมาะสมควรจะสามารถติดตามรายการข้อมูลจากบุคคลที่จัดทำรายการข้อมูลส่งไปยังบุคคลที่จัดส่งข้อมูล

การเสนอเอกสาร EDI เป็นพยานหลักฐาน⁹⁹ จะต้องมียอดประกอบ 6 ประการดังต่อไปนี้ 1. บุคคลที่รับรู้ข้อเท็จจริงจะต้องได้จัดทำเอกสารต้นฉบับ (Original) หรือเอกสารฉบับสมบูรณ์ (Complete) 2. เอกสารต้นฉบับ (Original Record) จะต้องจัดทำขึ้นในวันทำการซึ่งตรงกับที่บันทึกไว้ในเอกสาร 3. เอกสารเก็บไว้ได้อย่างระมัดระวังและลงตราประทับอันแสดงถึงความน่าเชื่อถือทางธุรกิจตั้งแต่จัดทำเอกสารดังกล่าว 5. เอกสารต้นฉบับจะต้องไม่ยากเกินกว่าที่จะเข้าใจได้และจะต้องไม่ยากเกินกว่าที่จะค้นหาได้อย่างสะดวก 6. บทคัดย่อจะต้องมีความสอดคล้องและตรงกับเนื้อหาของเอกสาร

พยานหลักฐานจะต้องสามารถเข้าใจได้

นอกจากพยานหลักฐานจะต้องมีความเกี่ยวข้องและน่าเชื่อถือแล้ว ผู้ค้นหาความจริงจะต้องสามารถเข้าใจพยานหลักฐานดังกล่าวได้ เนื่องจากเอกสาร EDI จะปรากฏเพียงแต่ตัวย่อหรือตัวเลข มีวิธีการอยู่สามวิธีที่จะจัดการกับปัญหาดังกล่าวนี้อย่างมีประสิทธิภาพ

หนึ่ง เป็นไปได้ที่จะต้องใช้ผู้เชี่ยวชาญเพื่อให้ความรู้ผู้ตรวจสอบความจริง โดยทั่วไปแล้วเทคนิคนี้จะสามารถใช้ได้ดีเมื่อความรู้ที่จะให้กับผู้ค้นหาความจริงเป็นความรู้ที่ไม่ยากหรือมีความซับซ้อนมากนัก

⁹⁹ โปรดดูคดี United States v. Vela, 673 F.2d 86 (5th Cir. 1982) และ Perma Research & Development Co. v. Singer Co., 542 F.2d 111, 125 (2d Cir. 1976) cert. Denied, 429 U.S. 987 (1976)

สอง ผู้ค้นพบความจริงอาจอาศัยพยานผู้เชี่ยวชาญเกี่ยวกับความน่าเชื่อถือและความหมายของเอกสาร EDI วิธีการนี้จะมีประสิทธิภาพและประสิทธิผลถ้าความหมายของเอกสารดังกล่าวไม่มีความขัดแย้งกันในคดีมากนัก อย่างไรก็ตามหากผู้เชี่ยวชาญไม่มีความเห็นพ้องต้องกันและผู้ค้นหาความจริงต้องตัดสินใจว่าจะเชื่อใครดี อาจจะต้องใช้วิธีการสาบาน (Swearing Contest)

สาม ข้อมูล EDI สามารถรื้อฟื้นขึ้นใหม่ (Reconstitute) จากรูปแบบเดิมที่เข้ารหัสและทำให้เล็กลง (Condense and encode) ให้อยู่ในรูปแบบที่มนุษย์สามารถอ่านเข้าใจได้ การรื้อฟื้นดังกล่าวควรที่จะกำหนดไว้ให้ชัดเจนในข้อตกลง

การตรวจสอบพยานหลักฐานทางอิเล็กทรอนิกส์นั้นจะต้องทำโดยตรวจสอบจุดต่างๆอย่างระมัดระวังดังต่อไปนี้

ฟังก์ชันการทำงานของเครื่องคอมพิวเตอร์ฮาร์ดแวร์และอุปกรณ์เชื่อมต่อ

ฟังก์ชันการทำงานของระบบคอมพิวเตอร์ซอฟต์แวร์

ความถูกต้องของข้อมูลที่ป้อนเข้าสู่เครื่องคอมพิวเตอร์

ระบบรักษาความปลอดภัยที่ดีพอที่จะป้องกัน

Random Loss ของข้อมูลในหน่วยความจำ

การเข้าไปแก้ไขเพิ่มเติมเอกสาร (Record tampering) โดยบุคคลที่สามผู้ไม่มีอำนาจ

การเข้าไปแก้ไขเพิ่มเติมเอกสาร (Record tampering) โดยคู่พิพาท

การเข้าไปแก้ไขเพิ่มเติมเอกสาร (Record tampering) โดยผู้เก็บรักษาเอกสาร (Recordkeeper)

การเข้าไปแก้ไขเพิ่มเติมเอกสาร (Record tampering) ในระหว่างการส่งผ่านข้อมูลดังกล่าว

ความสมบูรณ์ของพยาน (The strength of evidence)

หลักกฎหมายพยานหลักฐานจะกำหนดหลักการยอมรับฟังพยานหลักฐาน (Admission) แต่โดยทั่วไปแล้วจะไม่ได้กำหนดว่าพยานหลักฐานดังกล่าวนั้นมีความน่าเชื่อถือหรือไม่ กล่าวคือการยอมรับฟังพยานหลักฐาน (Admissibility) จะตัดสินโดยศาล แต่ความน่าเชื่อถือ (Believability) หรือ “น้ำหนัก” ของพยานหลักฐานโดยปกติจะตัดสินโดยข้อเท็จจริงที่นำมาพิสูจน์ (Trier of Fact) ประสพการณ์และการวิเคราะห์เชิงตรรก (Logical analysis) ในเหตุการณ์ที่เป็นปัญหาจะถือเป็นแนวทางที่ดีที่สุดที่จะทำให้รู้ว่าอะไรเป็นสิ่งที่มีความน่าเชื่อถือ ผู้ที่มีวิชาชีพในการตรวจสอบ (Auditing Profession) ได้พัฒนาข้อสันนิษฐานเบื้องต้นเพื่อช่วยให้ผู้ตรวจสอบ (Auditors) สามารถวัดระดับความน่าเชื่อถือดังต่อไปนี้

เมื่อหลักฐานสามารถได้มาจากแหล่งอื่นนอกจากในหน่วยงาน (เช่น บริษัทที่ทำการตรวจสอบ) จะถือว่ามีความน่าเชื่อถือเนื่องจากได้จากหน่วยงานตรวจสอบที่เป็นกลาง (Independence audit) มากกว่าข้อมูลที่จะมาจากภายในหน่วยงานแต่เพียงอย่างเดียว

ยังมีโครงสร้างการควบคุมภายใน (Internal Control Structure) ที่มีประสิทธิภาพมากเท่าใด ยิ่งทำให้เชื่อมั่นได้ว่าข้อมูลทางบัญชีและเอกสารทางการเงิน (Financial Statement) ยิ่งมีความน่าเชื่อถือมากเพียงนั้น

ข้อมูลที่ผู้ตรวจสอบรับรู้ด้วยตัวเอง โดยการตรวจสอบข้อเท็จจริง (Physical Examination) การสังเกต การคำนวณ และการตรวจสอบ จะมีความน่าเชื่อถือมากกว่าข้อมูลที่ได้รับโดยทางอ้อม

ในการให้น้ำหนักพยานหลักฐานในศาล ความสนใจจะมุ่งไปที่ความเกี่ยวเนื่องของเหตุผล (Logical connection) ระหว่างพยานหลักฐานและประเด็นที่ต้องการจะพิสูจน์ พยานหลักฐาน “โดยตรง” (Direct) จะสามารถแสดงความเกี่ยวเนื่องกันในทางเหตุผลได้ดีกว่าและชัดกว่า พยานหลักฐาน “แวดล้อมกรณี” (Circumstantial) จะมีน้ำหนักน้อยกว่า และต้องการข้อเท็จจริงที่จะมาช่วยพิสูจน์ (Trier of Fact) ประกอบกับพยานหลักฐานเพื่อให้เข้าใจประเด็นปัญหาที่ต้องการพิสูจน์ ตัวอย่างเช่น Data Log ที่ยังไม่ได้ถูกแก้ไข (Unmodified) ข้อความที่แลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI Messages) ที่ได้รับโดยผู้ใช้ EDI จะถือเป็นพยานหลักฐานโดยตรงในการกำหนดว่าข้อมูล EDI ได้ส่งถึงเขาแล้ว แต่เพียงเฉพาะ Log จะเป็นเพียงแค่พยานแวดล้อมกรณีว่าผู้ส่งได้ส่งข้อมูลให้ผู้รับ การพิจารณาจาก Log ถึงว่าจะอะไรได้ส่งไปจำเป็นที่จะต้องใช้ความรู้ในเรื่องของการมีอยู่และหน้าที่ (Function) ของการเชื่อมต่อทางการสื่อสาร (Communication Link) ระหว่างผู้ส่งและผู้รับ

เส้นแบ่งที่ชัดเจนระหว่างพยานหลักฐานโดยตรงและพยานแวดล้อมกรณีนั้นไม่มีความชัดเจนมากนัก แต่อย่างไรก็ดีการแบ่งแยกดังกล่าวก็เป็นเรื่องที่มีประโยชน์ พยานแวดล้อมกรณีของสิ่งใดสิ่งหนึ่งจะมีคุณค่าน้อยกว่าพยานโดยตรงของสิ่งเดียวกัน ยิ่งพยานหลักฐานมีคุณค่าน้อยเพียงใดยังมีน้ำหนักน้อยเพียงนั้นเมื่อพิจารณาประกอบกับข้อเท็จจริงในคดี (Trier of Fact) และจะส่งผลให้พยานหลักฐานดังกล่าวได้ได้รับการพิจารณาเนื่องจากมีพยานอื่นๆที่น่าเชื่อถือตามหลักกฎหมายพยานหลักฐาน¹⁰⁰

ยิ่งใช้พยานแวดล้อมกรณีมากเพียงใดน้ำหนักยิ่งมีน้อยลงเพียงนั้น เช่นตามข้อเท็จจริง (Trier of Fact) จะต้องพิจารณาพยานที่ขัดแย้งกันในเรื่องช่วงเวลา เช่นกรณีของเวลาที่ส่งโทรสาร (Fax) เอกสารที่ส่งมาทาง Fax (Incoming fax printout) ได้สูญหายไป ผู้ส่งจึงพยายามพิสูจน์ว่าเขาได้ส่งเอกสารดังกล่าวในตอนเช้าและเก็บหลักฐานในการส่งไว้ แต่ผู้รับอ้างว่าเขาได้รับแฟกซ์ดังกล่าวในตอนบ่ายซึ่งเป็นเวลาที่ศูนย์การสื่อสาร (Communications Center) ของเขาบอกกล่าวว่าแฟกซ์ได้มาถึงแล้ว อย่างไรก็ตามพยานหลักฐานอื่นๆ แสดงให้เห็นว่า (1) ศูนย์การสื่อสารของผู้รับมักจะเพิกเฉยหรือชักช้าในการบอกกล่าวให้ทราบว่ามีแฟกซ์ส่งมาถึง (2) ผู้รับออกไปจากสำนักงานหลายครั้งในวันดังกล่าว และ (3) ศูนย์การสื่อสารมักจะไม่สามารถทิ้งข้อมูลให้ผู้รับได้เนื่องจากผู้รับไม่อยู่ พฤติการณ์แวดล้อมกรณีดังกล่าวจะต้องมีการแก้ต่างโดยผู้รับ และหากมองจากรูปการณดังกล่าวผู้ส่งมีเหตุผลที่น่าเชื่อถือทีเดียว

น้ำหนักที่ให้กับพยานหลักฐานบางส่วนจะขึ้นอยู่กับข้อสงสัยในการตรวจสอบว่ามีความผิดพลาดหรือการหลอกลวงเกิดขึ้นหรือไม่ ตัวอย่างเช่น ในกรณีพิพาทเรื่องเวลาการส่งแฟกซ์ ผู้ส่งซึ่งเป็นนักหลอกลวงด้วย ได้พิสูจน์ว่าตนได้ส่งแฟกซ์ในตอนเช้า แฟกซ์ที่ส่งไปได้รับจริงแต่เวลาที่แสดงเป็นเวลาบ่ายสอง เครื่องแฟกซ์ของผู้รับตั้งอยู่ตั้งอยู่ที่ร้านพิมพ์เอกสารที่เป็นเจ้าของเครื่องแฟกซ์ดังกล่าวซึ่งอยู่คนละฝั่งถนนของสำนักงานของผู้รับ ข้อเท็จจริงที่นำมาพิสูจน์อาจทำให้เวลาของการรับแฟกซ์ดังกล่าวดูมีน้ำหนักมากขึ้นและสรุปได้ว่าแฟกซ์ถูกส่งไปในเวลา บ่ายสองโมงจริง¹⁰¹ *** (Zink Communications v. Elliott, 1990 WL 176382 (S.D.N.Y. 1990) ประเด็นของข้อพิพาทอยู่ที่ว่าการใช้ Option ที่จะเข้า Game show host ได้รับโดยแฟกซ์ก่อนที่จะ option จะหมดกำหนด Gordon Elliott ได้ตกลงกับ Zink Communications ว่า Zink จะยังคงได้รับบริการในฐานะที่เป็น Host หากได้แจ้งให้ Elliott Option ใน 1 มิถุนายน 1990 Zink ได้อ้างว่า

¹⁰⁰ โปรดดู Tomassini v. Saunders, 274 N.J. Super. 203, 643 A.2d 665 (1994)

¹⁰¹ โปรดดู Zink Communications v. Elliott, 1990 WL 176382 (S.D.N.Y. 1990)

ในวันดังกล่าว Zink ได้ส่งคำบอกกล่าวไปยังตัวแทนของ Elliott โดยแฟกซ์จำนวน 14 หน้า Zink สนับสนุนคำกล่าวอ้างของตนโดยใช้พยานบุคคลผู้ที่ส่งและสังเกตการณ์การส่งแฟกซ์และเป็นผู้ที่โทรศัพท์ติดต่อกับตัวแทนของ Elliott เพื่อยืนยันการได้รับแฟกซ์อย่างสมบูรณ์ นอกจากนั้น Zink ยังได้เสนอพยานบุคคลที่เป็นผู้รับปลายทางว่าเอกสารที่ได้รับมี 14 แผ่นจริงและการรับมีความสมบูรณ์ แต่อย่างไรก็ดีทางฝ่ายตัวแทนของ Elliott ได้ต่อสู้ว่าเขาได้รับแฟกซ์ดังกล่าวจริง แต่ว่าเอกสารดังกล่าวมีการกล่าวถึงทุกเรื่องยกเว้นเรื่อง Option และเขาไม่สามารถพิสูจน์ว่าแฟกซ์ดังกล่าวไม่มี Option จริงเพราะว่าเขาได้โยนมันทิ้งไปแล้ว ศาลจึงสรุปว่าตัวแทนของ Elliott ด้วยมูลเหตุจูงใจและพฤติการณ์ของตัวแทนดังกล่าว เป็นการโกหก จึงตัดสินว่าได้มีการใช้ Option ภายในกำหนดเวลาวันที่ 1 มิถุนายน

การพิจารณาคดีของศาลในคดีนี้เหมือนกับวิธีที่ใช้โดยทั่วไปในกรณีที่คำบอกกล่าวได้ส่งทางไปรษณีย์ โดยมีใบรับยืนยันจากไปรษณีย์ ถ้าใบรับแสดงเพียงว่ามีบางสิ่งบางอย่างได้ส่งไปจริง ไม่ได้แสดงเนื้อหาของสิ่งที่ส่ง การจะดูว่าคำบอกกล่าวดังกล่าวมีเนื้อหาอย่างไรจะอาศัยพยานบุคคลมาให้การ

ผู้ที่เสนอพยานหลักฐานอาจดำเนินการพิเศษ (Extra step) เมื่อทำการเสนอพยานหลักฐานเพื่อจะทำให้เชื่อว่าข้อเท็จจริง (Trier) นั้นสามารถเชื่อถือได้ ตัวอย่างเช่นเขาอาจแสดงว่าเอกสาร (Record) มีสัญลักษณ์ที่น่าเชื่อถือ ในคดี United States v. Greenlee¹⁰² รัฐบาลได้เสนอให้เอกสารคอมพิวเตอร์ (Computer Record) ของ Internal Revenue Service (IRS) แสดงให้เห็นว่าจำเลยไม่ได้ยื่นแบบแสดงรายการภาษีเงินได้ เพื่อที่จะเสริมให้พยานหลักฐานแน่นหนาขึ้น รัฐบาลได้พยายามแสดงว่าจะไม่มีการผิดพลาดหากมีการยื่นแบบแสดงรายการภาษีจริง เจ้าหน้าที่ของ IRS ได้พิสูจน์ว่าในขณะที่รับแบบดังกล่าวจะแยกออกเป็นหมวดละ 100 ฉบับและจะมีการกำหนดเลขคู่มือรายการให้ พนักงานแต่ละคนจะบันทึกข้อมูลในเครื่องคอมพิวเตอร์จากแบบแสดงรายการภาษีแต่ละฉบับ รวมทั้งเลขประจำตัวประกันสังคม (Social Security Number) ของผู้เสียภาษี และจะมีเจ้าหน้าที่คนอื่นหนึ่งคอยตรวจสอบการบันทึกข้อมูลดังกล่าวอีกครั้งหนึ่งเพื่อหาข้อบกพร่อง นอกจากนั้นยังมีพนักงานคนที่สามนับยอดแบบแสดงรายการในหมวดหมู่นั้นว่าครบหนึ่งร้อยฉบับหรือไม่ และในที่สุดข้อมูลคอมพิวเตอร์ดังกล่าวจะได้รับการนำไปเปรียบเทียบกับข้อมูลของหน่วยงานประกันสังคม (Social Security Administration) ว่าตรงกับเลข

¹⁰² 380 F. Supp. 652 (E.D. Pa. 1974), aff'd, 517 F.2d 899 (3d Cir.), cert. Denied, 423 U.S. 985 (1975)

ประจำตัวประกันสังคมที่หน่วยงานมีหรือไม่ รัฐบาลดูเหมือนว่าจะประสบความสำเร็จในการแสดงว่าข้อมูลของ IRS เป็นสิ่งที่น่าเชื่อถือเนื่องจากศาลอนุญาตให้มีการรับฟังข้อมูลที่ได้จากเครื่องคอมพิวเตอร์และในที่สุดจึงตัดสินว่าจำเลยไม่ได้ยื่นแบบแสดงรายการภาษีเงินได้

ในบางกรณีจำเลยอาจยื่นพยานหลักฐานของตนเพื่อคัดค้านพยานต้นฉบับ (Original Evidence) ในคดี *Blackston v. United States*¹⁰³ ศาลปฏิเสธที่จะรับฟังข้อสันนิษฐานที่ไม่สามารถอธิบายได้ว่าในความเป็นจริงแล้ว IRS ได้ส่งไปรษณีย์เป็นหนังสือบอกกล่าวเมื่อเอกสารคอมพิวเตอร์ของ IRS แสดงให้เห็นว่าหนังสือบอกกล่าวได้ส่งไปแล้ว ผู้เสียภาษีได้แสดงหลักฐานถึงความไม่แน่นอนระหว่างเอกสารคอมพิวเตอร์ของ IRS ที่ออก และเอกสารของ IRS ตามโปรแกรมคอมพิวเตอร์ และศาลก็ได้ตัดสินว่า IRS ไม่ได้ส่งไปรษณีย์ตามที่กำหนดในการประเมินภาษี¹⁰⁴ ศาลยอมรับฟังพยานบุคคลและไม่เชื่อถือพยานเอกสารที่ได้จากคอมพิวเตอร์ (Computer Record) ลูกค้านำข้ออ้างให้ธนาคารทำการปรับปรุงบัญชีในรายการถอนเงินใหม่ ธนาคารได้แสดงหลักฐานที่พิมพ์ออกมาจากเครื่องคอมพิวเตอร์ (Printout) และแสดงให้เห็นว่าเครื่องเอทีเอ็มสามารถเชื่อถือได้ (แม้ว่าพยานบุคคลของธนาคารจะยอมรับว่าเครื่องเอทีเอ็มอาจขัดข้องทางเทคนิคก็ได้) อย่างไรก็ตามลูกค้าได้แสดงพยานบุคคลนำสืบว่าเธอไม่ได้ถอนเงินจำนวนดังกล่าว พร้อมกับแสดงจดหมายจากนายจ้างยืนยันว่าเธออยู่ในที่ทำงานขณะที่มีการถอนเงินเกิดขึ้น ศาลได้พิจารณาความน่าเชื่อถือระหว่างลูกค้าและเครื่องคอมพิวเตอร์ อย่างไรก็ตามศาลเห็นว่าเป็นนโยบายสาธารณะที่ดี (Good Public Policy) ที่จะให้ความน่าเชื่อถือคนมากกว่าเครื่องจักรกล)

เทคนิคใดๆ ก็ตามที่ทำให้เอกสารคอมพิวเตอร์มีความน่าเชื่อถือและสามารถยืนยันข้อเท็จจริงได้จะช่วยให้พยานหลักฐานดังกล่าวได้รับการยอมรับฟัง (Admissibility) และมีน้ำหนัก ระบบการควบคุมที่จะทำให้กระบวนการในการทำเอกสารดังกล่าวไม่มีข้อผิดพลาดและไม่ถูกต้องเป็นสิ่งที่มีความจำเป็นอย่างยิ่ง ยิ่งไปกว่านั้นเอกสารที่ใช้เป็นพยานหลักฐานที่มีความเป็นเหตุการณ์แวดล้อมกรณีน้อยที่สุดย่อมจะมีคุณค่ามากขึ้น

การตรวจสอบ (Audit trail) ที่ปลอดภัยและน่าเชื่อถือจะช่วยลดความจำเป็นในการเชื่อมต่อเอกสารที่มาจากทางไกลและขั้นตอนที่มีความสำคัญทางกฎหมายในการประมวลผล ตัวอย่างเช่น

¹⁰³ 778 F. Supp. 224 (D. Md. 1991)

¹⁰⁴ *Judd v. Citibank*, 107 Misc. 2d 526, 435 N.Y.S.2d 210 (Civ. Ct. 1980)

คอมพิวเตอร์ ก ได้ออกแบบมาให้สามารถรับคำสั่งซื้อตามกฎหมายโดยบริษัทใดๆก็ได้ สำหรับเหตุผลทางเทคนิค บริษัทจะเลือกที่จะส่งผ่านคำสั่งที่ได้รับไปยังเครื่องคอมพิวเตอร์ ข ก่อนที่จะทำการบันทึกข้อมูล จะเป็นการง่ายที่จะสรุปได้ว่าข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์ ข ถือเป็นเครื่องหนึ่งของบริษัทได้รับคำสั่งดังกล่าวถ้าการทดสอบที่เป็นประโยชน์ (Useful audit trail) (รวมทั้งบางกรณีใช้เวลาและเลขลำดับเอกสาร (Sequence number) ได้ประทับลงบนข้อมูลโดยคอมพิวเตอร์ ก) แสดงเส้นทางข้อมูลระหว่างคอมพิวเตอร์

อย่างไรก็ตามมีความจำเป็นที่จะต้องพิจารณาความน่าเชื่อถือของเอกสารไม่ว่าเอกสารดังกล่าวจะอยู่ในรูปของกระดาษหรือรูปของอิเล็กทรอนิกส์ ไม่มีกระบวนการที่แน่นอนที่จะใช้กับทุกกรณี อย่างไรก็ตามก็ยังมีหลักบางอย่างที่อาจเป็นประโยชน์ที่เกี่ยวข้องกับการจัดเก็บและการบำรุงรักษาเอกสารดังกล่าวเนื่องจากเป็นไปไม่ได้ที่จะเก็บสำเนาของข้อมูลอิเล็กทรอนิกส์ทุกฉบับในทุกๆ ครั้งที่ส่งหรือได้รับ การตัดสินใจควรที่จะกระทำในแต่ละช่วงเวลาของอายุของเอกสารว่าจุไหนจะมีความสำคัญในอนาคต โดยปกติแล้ว จะเป็นจุดเริ่มต้นหรือจุดสิ้นสุดของการส่งข้อมูล เช่นเดียวกัน Log ของข้อมูลที่ส่งหรือรับควรจะได้รับ การเก็บรักษาไว้ ข้อมูลทางอิเล็กทรอนิกส์ควรจะเป็นรักษาในรูปแบบ (Format) ดั้งเดิมที่ข้อมูลดังกล่าวส่งมา

ต้องใช้ความพยายามทุกวิถีทางที่จะให้เกิดความมั่นใจได้ว่าระบบการเก็บเอกสารมีความถูกต้องตรงกับการทำงานในปัจจุบันของการสร้าง การประมวลผลและการเก็บข้อมูลอิเล็กทรอนิกส์ ทั้งระบบคอมพิวเตอร์ ในเดือนตุลาคมปี 1990 กระทรวงยุติธรรมสหรัฐได้จัดทำคู่มือ "การยอมรับฟังเอกสารที่เก็บรวบรวมทางอิเล็กทรอนิกส์เป็นพยานหลักฐาน (Admissibility of Electronically Filed Federal Records as Evidence) โดยแนะนำวิธีการที่จะให้เกิดความมั่นใจว่าข้อมูลทางอิเล็กทรอนิกส์จะเป็นประโยชน์ในการใช้เป็นพยานในศาลดังต่อไปนี้ "เป็นความสำคัญอย่างยิ่งที่หัวหน้าการเก็บเอกสารของสหรัฐ (Federal records managers) หรือ ผู้เก็บรักษาเอกสาร (Custodians) จะทำให้เกิดความมั่นใจว่าการมีอยู่ของข้อมูลที่ได้รับการปรับปรุงแล้วจะเป็นไปตามอย่างสมบูรณ์กับกระบวนการควบคุม (Procedural control) ที่ใช้ (แฟ้มข้อมูลทางอิเล็กทรอนิกส์) นอกจากนั้นเจ้าหน้าที่บันทึกข้อมูลและผู้เก็บข้อมูลจะต้องเตรียมพร้อมสำหรับการอธิบายถึงระบบการควบคุมดังกล่าวให้คนโดยทั่วไป (Layman) สามารถเข้าใจได้ในความเชื่อมโยงของแต่ละเหตุการณ์ที่เกี่ยวกับการจัดทำเอกสารดังกล่าว¹⁰⁵

¹⁰⁵ Justice Mgmt. Div. Systems Policy Staff, U.S. Dep't of Justice, Admissibility of Electronically Filed Federal Records as Evidence (Oct. 1990)

การยอมรับฟังเอกสารทางอิเล็กทรอนิกส์โดยทั่วไป (The Admission of Electronic Records Generally)

เพื่อวางพื้นฐานในการรับฟังพยานหลักฐานที่เป็นเอกสารคอมพิวเตอร์ (Computer Record) คู่กรณีฝ่ายที่ยื่นพยานหลักฐานดังกล่าวอาจจำเป็นต้องให้พยานผู้เชี่ยวชาญกล่าวยืนยันดังต่อไปนี้

ความน่าเชื่อถือของระบบฮาร์ดแวร์ ระบบซอฟต์แวร์ และกระบวนการต่างๆที่ใช้ในการเก็บรักษาข้อมูล (Record) และการพิมพ์เอกสารออกจากเครื่องคอมพิวเตอร์ (Printout) รวมทั้งสภาพการณ์และวิธีการในการบันทึกข้อมูลเข้าสู่ระบบ ขั้นตอนที่ใช้และจะก่อให้เกิดความมั่นใจได้ว่าข้อมูลที่บันทึกมีความถูกต้อง ขั้นตอนที่ใช้ในการเก็บข้อมูลและรักษาข้อมูลให้มีพร้อมที่จะนำมาใช้ ความน่าเชื่อถือของซอฟต์แวร์ที่ใช้ในการประมวลผลข้อมูล ความน่าเชื่อถือของขั้นตอนที่ใช้ในการพิมพ์ข้อมูลออกมาจากเครื่องคอมพิวเตอร์ (Printout)

ความเหมาะสมของคอมพิวเตอร์ฮาร์ดแวร์ ซอฟต์แวร์ และกระบวนการต่างๆที่ช่วยให้ระบบสามารถทำงานตามที่ได้วางไว้ รวมทั้งกระบวนการในการรักษาความปลอดภัยที่จะช่วยป้องกันการเข้ามาแก้ไขเพิ่มเติมโดยไม่ได้รับอนุญาตและการทำลายระบบข้อมูล

การสร้างเอกสาร (Record) ในทางปฏิบัติอันเป็นปกติของธุรกิจ รวมทั้งพยานหลักฐานที่แสดงว่าข้อมูลได้ถูกบันทึกในทางปฏิบัติอันเป็นปกติของธุรกิจ และที่แสดงว่าการบันทึกข้อมูลดังกล่าวได้เสร็จสมบูรณ์ภายในระยะเวลาที่เหมาะสม (Reasonable Time)

บุคคลที่จะต้องใช้ระบบความปลอดภัยของคอมพิวเตอร์ (Computer Security System) ไม่ควรที่จะรอจนกว่าจะได้รับคำสั่งจากศาลให้ทำการพิสูจน์ยืนยัน แต่ผู้ดูแลระบบข้อมูล (Information System Manager) ควรที่จะพิจารณาไว้ล่วงหน้าว่าเขาสามารถ

ให้ความมั่นใจได้ว่าใครก็ตามที่เข้ามาใช้ระบบเข้าใจดีว่าเอกสารคอมพิวเตอร์ (Computer Records) รวมทั้ง E-mail อาจถูกค้นพบโดยคู่กรณี เช่นเดียวกับเอกสารที่เป็นกระดาษ

กำหนดว่าเอกสารคอมพิวเตอร์ (Computer Record) ที่ต้องการให้ค้นพบจะมีอยู่หรือเก็บรวบรวมไว้หรือไม่

ให้ความมั่นใจได้ว่าไม่มีเอกสารที่เกี่ยวข้องที่ถูกทำลายอย่างมีเจตนาในขณะที่มีการฟ้องร้องเกิดขึ้น

บทที่ 7

ตัวอย่างโครงการจัดทำใบตราส่ง (Bill of Lading) ให้เป็นอิเล็กทรอนิกส์

SEADOCS ความพยายามครั้งแรกที่จะพัฒนาระบบอิเล็กทรอนิกส์

ความพยายามครั้งแรกที่จะพัฒนาระบบของใบตราส่ง (Bill of Lading) ให้เป็นอิเล็กทรอนิกส์นั้นมีชื่อเรียกว่า SEADOCS

ปัญหาและข้อสงสัยเกี่ยวกับการใช้ตราสารเปลี่ยนมือ (Negotiable Transaction) ในรูปแบบของ EDI โดยเฉพาะในเรื่องของลายมือชื่อนั้นถือว่าเป็นอุปสรรคอย่างมาก การนำเอาเอกสารอิเล็กทรอนิกส์หรือ EDI มาใช้แทนตราสารเปลี่ยนมือที่เป็นกระดาษทำให้เกิดปัญหาหลายประการที่ยากจะก้าวข้ามพ้นไปได้ ทำอย่างไรจึงจะให้เอกสารอิเล็กทรอนิกส์สามารถทำสำเนาตนเองและเปลี่ยนมือไปตามผู้ทรงเอกสารนั้นได้

ตราสารเปลี่ยนมือนั้นจะรวมถึง ใบตราส่ง (Bill of Lading), ใบรับสินค้า (Warehouse Receipt) เช็ก ใบหุ้นกู้ (Bonds) นิติกรรม (Deeds) หรือตราสารอื่นๆที่สามารถใช้โอนสิทธิหรือกรรมสิทธิได้ การถือครองใบตราส่งจะเป็นเครื่องหมายบอกว่าผู้ทรงตราสารดังกล่าวมีกรรมสิทธิในสินค้านั้นๆ สำหรับเอกสารไม่เปลี่ยนมือ (Non-negotiable) แต่สามารถโอนกันได้ (Transferable) อย่างเช่น Common Receipts หรือ Parking Check เป็นต้น จะถือว่าผู้ทรงตราสารดังกล่าวมีสิทธิครอบครอง (Possession) แต่ไม่มีมีการเปลี่ยนแปลงกรรมสิทธิ แต่ถ้าเป็นตราสารเปลี่ยนมืออย่างใบตราส่งสำหรับสินค้าเรือได้ท์ บุคคลมีสิทธิครอบครองและเป็นเจ้าของกรรมสิทธิหากเปลี่ยนมือผู้ถือครองตราสารดังกล่าวทั้งสิทธิการครอบครองและกรรมสิทธิในเรือได้ท์ดังกล่าวก็สามารถเปลี่ยนมือไปด้วย

ดังนั้นหน้าที่ของใบตราส่งจะมีหน้าที่ดังต่อไปนี้ 1. เป็นใบรับสินค้า 2. เป็นสัญญากับผู้ส่งสินค้า (Shipping Company) และ 3. เป็นใบที่แสดงกรรมสิทธิในสินค้า นอกจากนั้นยังเป็นใบที่แสดงว่ารายการสินค้าที่นำส่งมีอะไรบ้าง (เช่นระบุจำนวนและประเภทสินค้า วันที่ส่งและเมืองท่าที่ส่งสินค้า เป็นต้น) เป็นเอกสารที่ใช้ในการตรวจสอบเพื่อวัตถุประสงค์ในการประกันภัย หรือเพื่อวัตถุประสงค์ในการเป็น Letter of Credit สำหรับใบตราส่งที่ไม่เปลี่ยนมือ (Non-negotiable bill of lading) (ที่สามารถโอนกันได้) จะยังคงมีหน้าที่เป็นใบรับสินค้า สัญญาขนส่ง (Contract of Carriage) ใบรายการสินค้า เป็นเอกสารที่ใช้ในการตรวจสอบเพื่อวัตถุประสงค์ในการประกันภัย และวิธีการโอนกรรมสิทธิแต่ไม่สามารถพิสูจน์ได้ว่าใครมีกรรมสิทธิ

ทราบใดที่เรายังติดขัดอยู่ที่เรื่องของการลงลายมือชื่อ หรือเอกสารต้นฉบับ ปัญหาจะเป็นเรื่องยาก แต่หากพิจารณาสาระสำคัญของใบตราส่งแล้วหรือเอกสารเปลี่ยนมือแล้วจะเห็นว่าสาระสำคัญไม่ได้อยู่ที่การลงลายมือชื่อหรือเอกสารต้นฉบับ หากแต่อยู่ที่กระบวนการที่ก่อให้เกิดความน่าเชื่อถือในผ่านกระดาษดังกล่าวมากกว่า

มีผู้กล่าวว่า “การทำใบตราส่งให้เป็นอิเล็กทรอนิกส์นั้นจะทำให้ใบตราส่งไม่สามารถใช้ได้” คำกล่าวนี้เป็นคำกล่าวที่ละเลยความเป็นจริงที่ว่าใบตราส่งหรือเอกสารแสดงกรรมสิทธิต่างๆ นั้นเป็นสัญลักษณ์ทางนามธรรมที่แสดงถึงการมีอยู่ของสินค้า ตัวอย่างเช่นเงินธนบัตร นั้นเป็นตัวแทนทางนามธรรมในค่าของเงินที่ได้กำหนดขึ้น ทั้งสองกรณีจะเห็นได้ว่ากระดาษในตัวของมันเองไม่ได้มีคุณค่ามากเมื่อเทียบกับสิ่งที่มันเป็นตัวแทน คุณค่าของมันจะคงอยู่ก็ต่อเมื่อยังมีความเชื่อมั่นว่ามันสามารถใช้เป็นตัวแทนค่าที่ตกลงกันได้ได้ ลายมือชื่อ การตีตราประทับ หรือสัญลักษณ์อื่นๆ ที่ทำให้เกิดความเชื่อถือ บุคคลที่ฉลาดจะพิจารณาถึงกระบวนการที่จะทำให้บรรลุถึงวัตถุประสงค์ของตราสารมากกว่าที่จะพิจารณาว่าตราสารดังกล่าวจะต้องทำเป็นกระดาษหรือไม่

เราจะต้องตระหนักเสมอว่าตราสารเป็นเพียงสื่อในการแลกเปลี่ยนเท่านั้น สื่ออื่นๆ ก็สามารถใช้เป็นตัวแทนการแลกเปลี่ยนได้เช่นกัน เช่นกรณีของ EDI ซึ่งอาจให้ความน่าเชื่อถือและความปลอดภัยมากกว่าสื่อที่เป็นกระดาษเสียอีก

ข้อมูลต่างหากที่มีความสำคัญมิใช่กระดาษ

ไม่มีสิ่งใดในเช็ค ดราฟต์ โบรับสินค้า (Warehouse Receipt) หรือใบตราส่ง เป็นต้น ที่จะได้รับความน่าเชื่อถืออย่างสมบูรณ์ ในความเป็นจริงแล้วเรายังใช้เอกสารดังกล่าวทั้งๆที่รู้ว่ามันยังไม่มีความปลอดภัยมากนัก ความเสี่ยงของการใช้ตราสารดังกล่าวจึงถูกทำให้ลดน้อยลงโดยกฎเกณฑ์ที่พัฒนาขึ้นเช่น UCP 500, INCOTERMS 1990 กฎเกณฑ์เหล่านี้จะกำหนดกระบวนการที่ใช้สำหรับตราสารเพื่อป้องกันการเข้าใจผิดหรือใช้ในทางที่ผิด หากปราศจากกฎเกณฑ์ที่เป็นลายลักษณ์อักษร (และกฎเกณฑ์ต่างๆที่พัฒนาโดยศาล) ความน่าเชื่อถือในตราสารดังกล่าวคงจะไม่มี อย่างไรก็ตามก็อาจเป็นการเสี่ยงหากการซื้อขายอสังหาริมทรัพย์จะอาศัยโดยเพียงแต่การกระทำเท่านั้นที่ใช้ยืนยันการซื้อขายดังกล่าว ไม่มีการลงตราประทับหรือลายมือชื่อแต่ประการใด สำหรับการทำธุรกรรมที่มีความสำคัญอย่างเช่นการซื้อขายอสังหาริมทรัพย์ ระบบการลงทะเบียนที่เป็นอิสระมีความสำคัญที่จะทำให้เกิดความน่าเชื่อถือที่พินิจกรรมดังกล่าวมีคุณค่า แน่แน่นอนถ้าระบบการจดทะเบียนมีข้อสงสัยว่าจะมีข้อผิดพลาด เพียงแค่กระดาษที่เป็นตัวแทนการจดทะเบียนดังกล่าวคงไม่สามารถสร้างความน่าเชื่อถือได้

ดังนั้นอาจกล่าวได้ว่าไม่ใช่กระดาษหรือการพิมพ์ข้อความบนแผ่นกระดาษที่เป็นสาระสำคัญของตราสารเปลี่ยนมือ หากแต่เป็นกระบวนการที่ตกลงกันไว้ว่าสื่อ (ซึ่งเดิมเป็นกระดาษ) ที่จะใช้เป็นตราสารเปลี่ยนมือมากกว่า หากเราต้องการที่จะเปลี่ยนแปลงสื่อดังกล่าวให้เป็นในรูปแบบของอิเล็กทรอนิกส์หรือ EDI เราก็เพียงแค่จะจัดให้มีกระบวนการที่เหมาะสมที่จะให้เกิดความมั่นใจได้

อย่างไรก็ดี กระบวนการใดๆ ที่ใช้จะต้องสามารถตรวจสอบความถูกต้องได้ (Verifiable) การโอนตราสารเปลี่ยนมือสามารถตรวจสอบความถูกต้องแท้จริงของเอกสารหรือของเนื้อหาได้อย่างไร ในระบบ EDI ที่ไม่มีการใช้กระดาษ อาจเพียงแค่การส่งผ่านข้อมูลจากผู้โอนและการตรวจสอบความถูกต้องมีความจำเป็นในทุกขั้นตอน เนื่องจากกระบวนการในการตรวจสอบความถูกต้องที่ปลอดภัยอาจเป็นการใช้การจดทะเบียนกับหน่วยงานหรือองค์กรที่ไว้วางใจได้ (Trustworthy registry) ตรรกที่กำหนดว่ากระบวนการตรวจสอบความถูกต้องได้ทำขึ้นในการส่งผ่านข้อมูลในแต่ละครั้งได้ผ่านผู้จดทะเบียนทั้งโดยผู้จดทะเบียนกลางและผู้จดทะเบียนที่ดำเนินการโดยผู้ออกตราสาร

การใช้ระบบจดทะเบียน ตราสารเปลี่ยนมือสามารถถูกทำสำเนาทางอิเล็กทรอนิกส์ซึ่งหากการส่งเอกสารดังกล่าวมีการผิดพลาดสามารถทำตราสารเปลี่ยนมือใหม่มาใช้แทนได้เสมอ เมื่อมีการรับรองว่าตราสารเปลี่ยนมือในรูปแบบเดิมที่เป็นกระดาษสามารถนำตราสารทางอิเล็กทรอนิกส์มาใช้แทนได้ การทำธุรกรรมดังกล่าวก็อาจไม่มีปัญหามากนัก

ข้อจำกัดของการนำเอา EDI มาใช้จึงเป็นเรื่องทางจิตวิทยาเท่านั้น สำหรับบุคคลดัดยทั่วไปอาจไม่คุ้นเคยที่จะใช้เอกสารที่ปรากฏบนจอคอมพิวเตอร์หรือเป็นเอกสารที่พิมพ์มาจากเครื่องคอมพิวเตอร์ (Printout) สำหรับผู้ที่ต้องการจะใช้ EDI จะต้องตระหนักอยู่เสมอว่าเราไม่ได้ใช้กระดาษเป็นสื่ออีกต่อไปแล้ว หากแต่เป็นกระบวนการทางอิเล็กทรอนิกส์ ซึ่งจำเป็นที่จะต้องทำให้เกิดความคุ้นเคย

หน้าที่ของผู้จดทะเบียนและประเภทการจดทะเบียน

รูปแบบของการโอน (Transferability) หรือการเปลี่ยนมือ (Negotiability) ตามการประกอบพาณิชย์อิเล็กทรอนิกส์จำเป็นต้องมีรูปแบบของการจดทะเบียน ที่จะต้องเป็น บุคคลที่เป็นกลางที่ “ไว้วางใจได้” ปัญหาสำคัญคือจะจดทะเบียนอย่างไรและจดทะเบียนอะไร ใครควรที่จะทำหน้าที่ดังกล่าว

ตัวอย่างเช่น CMI ได้กำหนดกฎเกณฑ์มาตรฐานขั้นต่ำในการทำใบตราส่งทางอิเล็กทรอนิกส์ซึ่งมีองค์ประกอบที่สำคัญคือ “Private Key” ที่จะทำหน้าที่แทนใบตราส่งที่ถูกโอน ในรูปแบบเดิมผู้ทรงใบตราส่งคือผู้ที่มีใบตราส่งต้นฉบับ ในทางอิเล็กทรอนิกส์ ผู้ทรงจะมี Private Key ที่มีลักษณะคล้ายกับรหัสเอทีเอ็ม แต่สำหรับ Private Key นี้จะใช้สำหรับการทำรายการข้อมูลเพียงครั้งเดียวเท่านั้น โดย Private Key จะใช้ตรวจสอบความถูกต้องของข้อมูลที่ส่งมาจากผู้ทรงใบตราส่ง เมื่อใบตราส่งได้โอนไปให้กับผู้ทรงคนใหม่ Private Key ใหม่จะออกให้กับผู้ทรงคนใหม่และ Private Key ใหม่ที่ใช้นั้นจะใช้กับผู้รับส่งสินค้า (Carrier) อย่างไรก็ตามจะต้องเข้าใจว่า Private Key เป็นเพียงวิธีการตรวจสอบความถูกต้องของข้อความซึ่งไม่ได้ใช้เพื่อวัตถุประสงค์ในการรักษาความปลอดภัยแต่อย่างใด วิธีการรักษาความปลอดภัยอื่นๆ เช่น รหัสผ่าน (Password) รหัสเข้า (Access Code) ลายมือชื่อทางดิจิทัล (Digital Signature) เป็นต้นก็ยังคงมีความจำเป็น

ใบตราส่งทางอิเล็กทรอนิกส์ของ CMI ยังคงรักษาหน้าที่ของใบตราส่งในรูปแบบเดิมที่ทำหน้าที่ดังต่อไปนี้ ใบรับสินค้า สัญญา ข้อมูล กรรมสิทธิ์ เป็นเอกสารที่ใช้ในการตรวจสอบเพื่อวัตถุประสงค์ในการประกันภัยหรือใช้ในการตรวจสอบเอกสารเครดิตต่างๆ (Documentary Credit Verification) สำหรับใบตราส่งที่เป็นกระดาษอาจใช้กระดาษเพียงเดียวสำหรับกระบวนการทั้งหมด แต่ใบตราส่งทางอิเล็กทรอนิกส์นั้นอาจมีหลายข้อความ (Messages) ตามข้อกำหนดของ CMI แต่อย่างไรก็ดีผลที่ปรากฏจะออกมาเหมือนกัน

เพื่อที่จะให้เป็นไปตามข้อกำหนดของ CMI จำเป็นที่จะต้องแยกย่อยขั้นตอนและกระบวนการของใบตราส่งออกเป็นขั้นตอนย่อยๆ แล้วจึงค่อยพิจารณาว่าขั้นตอนใดบ้างที่จำเป็นต้องมีการเปลี่ยนมือ จึงทำให้ไม่มีการเปลี่ยนแปลงมากนักในทางปฏิบัติ กล่าวคือก็ดำเนินตามขั้นตอนแบบเดิมที่ใช้สำหรับใบตราส่งที่เป็นกระดาษ แต่สามารถควบคุมกระบวนการต่างๆ ได้ดีกว่าและความผิดพลาดมีน้อยกว่า

บทสรุป

จากทั้งหมดที่ได้กล่าวมาข้างต้นสามารถสรุปได้ดังต่อไปนี้

1. กฎพาณิชย์อิเล็กทรอนิกส์ถือเป็นความจำเป็นของสังคมไทยที่จะต้องจัดทำโดยคำนึงถึงความสอดคล้องกับสังคม ความก้าวหน้าทางเทคโนโลยีและหลักพื้นฐานทางกฎหมาย
2. เนื่องจากปรากฏการณ์ที่เรียกว่าพาณิชย์อิเล็กทรอนิกส์นั้นมีผลทำให้กฎหมายต้องมีการปรับเปลี่ยนอย่างมากดังนั้นกระบวนการในการร่างกฎหมายควรที่จะต้องคำนึงถึงรากฐานทางวิชาการอันจะเป็นการสร้างองค์ความรู้ในด้านนี้ให้สังคมไทยสามารถพัฒนากฎเกณฑ์ให้กับสังคมได้อย่างยั่งยืน
3. ในเรื่องของกระบวนการในการทำสัญญาทางอิเล็กทรอนิกส์นั้น เนื่องจากมีลักษณะเฉพาะตัวแตกต่างจากกระบวนการทำสัญญาในรูปแบบเดิม จึงควรที่จะพิจารณากระบวนการใหม่ให้มีระบบที่รัดกุม โดยเฉพาะในเรื่องของการคุ้มครองผู้บริโภค
4. ในเรื่องของพยานหลักฐานทางอิเล็กทรอนิกส์ซึ่งถือเป็นจุดสำคัญในการที่จะทำให้กิจการพาณิชย์สามารถดำเนินการได้อย่างมีประสิทธิภาพ จึงควรที่จะมีกฎเกณฑ์ในเรื่องของพยานหลักฐานที่เหมาะสมและรัดกุมพอที่จะให้ความยุติธรรมกับสังคมในยุคแห่งเทคโนโลยีสารสนเทศได้
5. กฎหมายพาณิชย์อิเล็กทรอนิกส์ควรที่จะกำหนดให้มีความสอดคล้องกับกฎหมายอื่นๆ โดยเฉพาะกฎหมายที่เกี่ยวกับเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

บรรณานุกรม

- Mads Bryde Andersen, Electronic Commerce: A Challenge to Private Law?, CENTRO DI STUDI E RICERCHE DI DIRITTO COMPARATO E STRANIERO, Roma, Maggio 1998
- Roy Goode, The Concept of "Good Faith" in English Law,
- Allan Farnsworth, The Concept of Good Faith in American Law,
- Nimmer, Raymond T., "*Electronic Contracts*", Computers and Law : Society for Computers and Law (London) 7:1:36-42, April-May 1996 (Part I); 7:2:37-40, June-July 1996 (Part II) ; 7:3:31-36, Aug.-Sept. 1996 (Part III).
- Nicoll, C.C, "Can Computer make contracts?", Journal of Business law (London) 35 – 49, January 1998
- Benjamin Wright; Jane K. Winn, The Law of Electronic Commerce, Aspen Law & Business; New York, 1997
- TEDIS Programme, The Legal Position of the Member States with respect to Electronic Data Interchange, Commission of the European Communities, 1989
- Bernard D. Reams, Jr.; L.J. Kutten and Allen E. Strehler, Electronic Contracting Law, Clark Broadman Callaghan, New York, 1995-96

- Edward Wilding, Computer Evidence: A Forensic Investigations Handbook, Sweet & Maxwell, 1997
- Ian Walden (ed.), EDI and The Law, Blenheim Online, London, 1989
- Rob Bradgate, "Evidential issues of EDI", in Ian Walden (ed.), EDI and The Law, Blenheim Online, London, 1989
- Cristopher J Millard, "Contractual Issues of EDI", in Ian Walden (ed.), EDI and The Law, Blenheim Online, London, 1989
- Sa'id Mosteshar, "Liability issues of EDI", in Ian Walden (ed.), EDI and The Law, Blenheim Online, London, 1989
- Micheal S Baum, "Electronic contracting in the US", in Ian Walden (ed.), EDI and The Law, Blenheim Online, London, 1989
- Clare Johnson, "Electronic Data Interchange", International Yearbook of Law Computers and Technology, Vol. 6, 1992
- Ian Walden, "EDI: Contracting for Legal Security", International Yearbook of Law Computers and Technology, Vol. 6, 1992
- Phil Coathup, "The Basic of EDI", International Yearbook of Law Computers and Technology, Vol. 6, 1992
- Solomon E Salako, "Transition to a 'Paperless' System Using RDI Techniques: the Evidential Minefield", International Yearbook of Law Computers and Technology, Vol. 6, 1992

- P.V.D. Marsh, Comparative Contract Law England, France, Germany; Gower, England, 1997
- Guy Lefebvre, "Electronic Data Interchange and the New Civil Code of Quebec", Overseas Business Law, 1998
- Amelia H. Boss, "The Emerging Law of International Electronic Commerce", Temple Int'L & Comp. L.J., Vol.6, 1992
- Kevin J. Kotch, Addressing "The Legal Problems of International Electronic Data Interchange: The Use of Computer Records As Evidence in Different Legal Systems" Temple Int'L & Comp. L.J., Vol.6, 1992
- Raymond T. Nimmer, "Article 2B: An Introduction", Journal of Computer & Information Law, Vol. XV, 1997
- Raymond T. Nimmer, "Electronic Contracting: Legal Issues", Journal of Computer & Information Law, Vol. XIV, 1996
- Micheal L. Rustad, "Commercial Law Infrastructure for the Age of Information", Journal of Computer & Information Law, Vol. XV, 1997
- George F. Chandler, III, "Maritime Electronic Commerce for the Twenty-First Century", Tulane Maritime Law Journal, Vol 22 Summer 1998 Number 2
- Chris Reed (ed.) , Computer Law, Blackstone Press Limited, London, 1990

- Joseph J. Norton, Chris Reed and Ian Walden, Cross-Border Electronic Banking, Lloyd's of London Press Ltd., 1995
- Thomas J. Smedinghoff, Multimedia Legal Handbook, Vol.1 – 2, Aspen Law & Business, New York, 1997
- Stephen Saxby (ed.), Encyclopedia of Information Technology Law, Sweet&Maxwell, London, 1997
- นางสาว เลิศลักษณ์ ปานเลิศ, การใช้คอมพิวเตอร์เป็นพยานในศาล, วิทยานิพนธ์ ภาควิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, พ.ศ. 2531

ภาคผนวก

ตารางการเปรียบเทียบกฎหมาย
พาณิชย์อิเล็กทรอนิกส์ของประเทศต่างๆ

UNCITRAL Model Law on Electronic Commerce	NCCUSL Uniform Electronic Transactions Act (March 19, 1999 draft)	Illinois Electronic Commerce Security Act (Effective Date July 1, 1999)	Massachusetts Massachusetts Electronic Records and Signature Act (Nov 4, 1997 draft)	South Korea The Basic Law on Electronic Commerce (Effective July 1, 1999)	Philippine An act Promoting the use of EDI in Trade Transaction, and for other purposes.	Singapore Electronic Transaction Bill 1998	Uniform Commercial Code Article 2B: Computer Information Transactions Draft February 1, 1999
Art. 1 Sphere of Application*	Sec. 103 Scope		Sec. 66 Scope	Art.3 Scope		Sec. 4 Application	Sec. 2B-103 Scope
Art. 2 Definitions	Sec. 102 Definitions	Sec. 5-105 Definitions	Sec. 65 Definitions	Art.2 Definition	Sec. 3 Definition of terms	Sec. 2 Interpretation	Sec. 2B-104 Exclusions from the article
Art. 3 Interpretation	Sec. 105 Application and Construction	Sec. 1-102 Purpose and Construction	Sec. 2 Purpose and Construction	Art.1 Purpose	Sec. 2 Primary objective	Sec. 3 Purpose and Construction	Sec. 2B-102 Definitions
Art. 4 Variation by Agreement	Sec. 104 Variation by Agreement	Sec. 1-110 Variation by Agreement		Art.4 Variation Subject to Electronic Interchange Agreement		Sec. 5 Variation by Agreement	Sec. 2B-106 Variation by Agreement: rules of construction: questions determined by court
Art. 5 Legal recognition of data message	Sec. 106 Legal recognition of E-records, E- signatures and E-contacts	Sec. 5-110 Legal recognition Sec. 5-115 Electronic records	Sec. 67 Electronic record Sec. 5 Writing and Signatures generally	Art.5 Validity of Electronic Messages (Art. 12 Effect of application)	Sec. 6 para 1.2. Legal Unity of Electronic Documents	Sec. 6 Legal recognition of Electronic record	Sec. 2B-113 Legal recognition of Electronic records and authentications
Art. 6 Writing	Sec. 107 Provision of information in writing					Sec. 7 Writing	
Art. 7 Signature	Sec. 108 (b) Effect of E-signatures	Sec. 5-120 Electronic Signatures	Sec. 68 Electronic Signatures	Art.6 Validity of Digital signature	Sec. 7 Validity of Electronic Signature	Sec. 8 Electronic Signature	
Art. 8 Original	Sec. 111 (a) Originals	Sec. 5-125 Original	Sec. 70 Original		Sec. 6 para 3. Legal Unity of Electronic Documents		
Art. 9 Admissibility and evidential weight of data message	Sec. 112 Admissibility in evidence	Sec. 5-130 Admissibility into evidence	Sec. 69 Admissibility into Evidence	Art.7 Admissibility of Electronic Messages as Evidence			
Art. 10 Retention of data messages	Sec. 111 (a)(1); (e)-(g) Retention of Electronic records	Sec. 5-135 Retention of electronic records	Sec. 71 Retention of electronic record	Art.8 Retention of electronic messages		Sec. 9 Retention of Electronic record	
Art. 11 Formation & Validity of contract	Sec. 113 Formation of contract			Art.10 Where the Originator is deemed to have sent electronic messages Art.11 Individuality of the electronic Message Received		Sec. 11 Formation and Validity	Sec. 2B-204 Offer and Acceptance: Electronic Agents Sec. 2B-120(a)(b) Electronic message Timing of contract: Effectiveness of message: Acknowledging message.
Art. 12 Recognition by parties						Sec. 12 Effectiveness between parties	
Art. 13 Attribution of data messages	Sec. 108 (a) Attribution and effect of electronic record and electronic signature					Sec. 13 Attribution	Sec. 2B-117 Attribution procedure for detection of changes and errors: effect of use
Art. 14 Acknowledgement of receipt	Sec. 110 Notification and acknowledgement			Art.12 Acknowledgement of Receipt:		Sec. 14 Acknowledgement of receipt	Sec. 2B-120(g) Electronic message Timing of contract: Effectiveness of message: Acknowledging message
Art. 15 Time and place of dispatch and receipt	Sec. 115 Time and place of sending and receipt			Art.9 Time and place of dispatch and receipt of electronic messages	Sec. 8 Transit times	Sec. 15 Time and place of dispatch and receipt	
Art. 16 Actions related to contract: s of carriage of goods							
Art. 17 Transport document				Chap III Security on electronic commerce**	Sec. 10 Security of Electronic Document	Sec. 16 Secure electronic record	
		Sec. 10-105 Secure electronic records				Sec. 17 Secure E-signature	
		Sec. 10-110 Secure electronic signature				Sec. 18 Presumptions	
		Sec. 10-120 Presumptions				Part V Secure electronic records and signatures	
		Article 15. effect of a digital signature Article 20. duties of subscribers					

					*การลงนามทางอิเล็กทรอนิกส์ signature		Part VI Effect of digital signatures Part VII General duties relating to digital signatures Part VIII Duties of Certification Authorities Part IX Duties of Subscribers Part X Regulation of Certification Authorities *การลงนามทางอิเล็กทรอนิกส์ signature		Part VI Effect of digital signatures Part VII General duties relating to digital signatures Part VIII Duties of Certification Authorities Part IX Duties of Subscribers Part X Regulation of Certification Authorities *การลงนามทางอิเล็กทรอนิกส์ signature	
	Part 2 governmental electronic records and signatures				Article 25. State agency use of electronic records and signatures	Sec. 72 Role of Chief Information Officer			Part XI Government use of Electronic records and signatures	

						or opt out of Article 28 is enforceable only if the transaction involves subject matter governed by Article 28 and subject matter governed by other contract law, or if there is good faith uncertainty about whether Article 28 or other contract law governs. (B) The agreement cannot opt the law applicable to distribution of information in non-electronic form. (3) Except for mass market transactions, the following rules apply: (A) An agreement to opt out of Article 28 is not enforceable unless the transaction involves subject matter not governed by Article 28 or there is good faith uncertainty about whether Article 28 or other contract law governs. (B) An agreement to opt into Article 28 is not enforceable unless the subject matter of the transaction includes information or informational rights or there is good faith uncertainty about whether Article 28 or other contract law governs. Sec. 28-104. Exclusions from this article. This article does not apply to: (1) a contract or a transaction that provides access to, use, transfer, clearance, settlement, or processing of: (A) deposits, loans, funds, or monetary value represented in electronic form and stored or capable of storage electronically and retrievable and transferable electronically; or other right to payment to or from a person; (B) an instrument or other item; (C) a payment order, credit card transaction, debit card transaction, or a funds transfer; automated clearing house transfer, or similar wholesale or retail transfer of funds; (D) a letter of credit, document of title, financial asset, investment property, or similar asset held in a fiduciary or agency capacity; or (E) related identifying, verifying, access-enabling, authenticating, or monitoring information; (2) a contract to create, perform in, include information in, acquire, use, reproduce, distribute, license, display, or perform: (A) audio or visual programming that is provided by broadcast, satellite, or cable as defined in the Federal Communications Act as that Act existed
--	--	--	--	--	--	--

[illegible]

Definitions

UNCITRAL	NCUCL	Illinois	Massachusetts	South Korea	Philippine	Singapore	UCC
Art. 2 Definitions For the purposes of this Law (1) "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 teletext; (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 does not include a person acting as an intermediary with respect to that data message; (3) "Computer program" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result. The term does not include informational content (4) "Contract" means the total legal obligation resulting from the parties' agreement as affected by this [Act] and other applicable rules of law; (5) "Electronic" means of or relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities (6) "Electronic agent" means a computer program, electronic, or other automated means used to initiate or respond to electronic records or performances in whole or in part without review by an individual in the ordinary course of a transaction. (7) "Electronic record" means a record created, stored, generated, received, or communicated by electronic means.	Sec. 102 Definitions In this [Act] (1) "Agreement" means the bargain of the parties in fact as found in their language or inferred from other circumstances, or derived from other circumstances, and rules, regulations, and procedures given the effect of agreements under rules of law otherwise applicable to a particular transaction. (2) "Automated transaction" means a transaction conducted formed or performed, in whole or in part, by electronic means or electronic records in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling any obligation required by the transaction. (3) "Computer program" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result. The term does not include informational content (4) "Contract" means the total legal obligation resulting from the parties' agreement as affected by this [Act] and other applicable rules of law; (5) "Electronic" means of or relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities (6) "Electronic agent" means a computer program, electronic, or other automated means used to initiate or respond to the untransformed electronic record, the encrypted transformation, and the signer's corresponding public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key Has been altered since the transformation	Sec. 5-105 Definitions "Asymmetric cryptosystem" means a computer-based system capable of generating and using a key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature. "Certificate" means a record that at a minimum: (a) identifies the certification authority issuing it; (b) names or otherwise identifies its subscriber; or (c) device or electronic agent under the control of the subscriber. (c) contains a public key that corresponds to a private key under the control of the subscriber; (d) specifies its operational period; and (e) is digitally signed by the certification authority issuing it. "Certification authority" means a person who authenticates and causes the issuance of a certificate "Certification practice statement" is a statement published by a certification authority that specifies the policies or practices that the certification authority employs in issuing, managing, suspending, and issuing certificates and providing access to them. "Correspond" with reference to keys, means to belong to the same key pair. "Digital signature" means a type of an electronic signature created by transforming an electronic record using a message digest function, and encrypting the resulting transformation with an asymmetric cryptosystem using the signer's private key such that any person having the initial key can verify the integrity of the record, the untransformed electronic record, the encrypted transformation, and the signer's corresponding public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key	Sec. 65 Definitions As used in sections sixty-five to seventy-two the following words shall have the following meanings: "Electronic" means electrical, digital, magnetic, optical, electromagnetic, or any other technology that is similar to these technologies "Electronic Record" means a record generated, communicated, received, or stored by electronic means. "Electronic signature" means any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the person using it to have the same force and effect as a manual signature. "Record" means information that is recorded on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. "Rule of law" means a statute, regulation, ordinance, common-law rule, court decision, or other law enacted, established, or promulgated by the Commonwealth or any agency, commission, department, court, other authority, or political subdivision of the Commonwealth 6. "Cyber mail" shall mean a virtual shipping mail established to trade goods or services using information technology facilities as well as the information system; 7. "Certification authority" shall mean a person who identifies the use of digital signature and conducts other related business upon request; 8. "Authorized certification authority" shall mean a certification authority authorized pursuant to Article 16.	Article 2. Definitions The terms used herein are defined as follows: 1. "Electronic message" shall mean information generated, sent, received or stored by electronic or similar means using electronic data processing devices including computers (hereinafter referred to as the "information system"). 2. "Originator" of an electronic message shall mean a person by whom, or on whose behalf, the electronic message is generated, sent, received, stored, transmitted, or otherwise communicated by electronic means. This system utilizes telecommunications facilities installed between organizations having data processing capability, such as but not limited to: computer, "Computer". Any device or apparatus which by electronic, electronic mechanical, magnetic, impulse, or other means, is capable of receiving, recording, transmitting, storing, processing, retrieving or producing information, data, figures, symbols or other modes of written expression, according to mathematical and logical rules, or of performing any one or more of those functions. Where two or more computers carry one or more of those functions in combination or in succession or otherwise however jointly, they shall be treated as a single computer. "Electronic Document" Any information, data, figures, symbols or other modes of written expression, describes or however represented, which is received, recorded, transmitted, stored, processed, retrieved or produced by a computer, which is capable of authentication by electronic signatures, a trade VAN or Trade VAS, or other acceptable means. "Electronic Signature": Characters, figures or symbols representing the normalized	Sec. 3 Definition of terms The terms used in this Act are defined as follows: "Electronic Data Interchange (EDI)" The transmission of business transactions information in computer-readable standard format, over the computer and telecommunications network, either via direct communication or through a third party network provider; "Electronic Data Interchange System (EDI System)" A system which provides the ability to receive, record, transmit, store process, retrieve, or produce electronic documents. This system utilizes telecommunications facilities installed between organizations having data processing capability, such as but not limited to: computer, "Computer". Any device or apparatus which by electronic, electronic mechanical, magnetic, impulse, or other means, is capable of receiving, recording, transmitting, storing, processing, retrieving or producing information, data, figures, symbols or other modes of written expression, according to mathematical and logical rules, or of performing any one or more of those functions. Where two or more computers carry one or more of those functions in combination or in succession or otherwise however jointly, they shall be treated as a single computer. "Electronic Document" Any information, data, figures, symbols or other modes of written expression, describes or however represented, which is received, recorded, transmitted, stored, processed, retrieved or produced by a computer, which is capable of authentication by electronic signatures, a trade VAN or Trade VAS, or other acceptable means. "Electronic Signature": Characters, figures or symbols representing the normalized	Sec. 2 Interpretation In this Act, unless the context otherwise requires - "Asymmetric cryptosystem" means a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key to verify the digital signature. "Certification authority" means a person or an organization that issues a certificate. "Certification practice statement" means a statement issued by a certification authority to specify the policies that the certification authority employs in issuing certificates. "Controller" means the Controller of Certification Authorities appointed under section 4(1)(1) and includes a Deputy or an Assistant Controller of Certification Authorities appointed under section 4(1)(3). "Correspond" in relation to private or public keys, means to belong to the same key pair. "Digital signature" means an electronic signature consisting of a transformation of a record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine: (a) whether the transformation was created using the private key that corresponds to the signer's public key, and (b) whether the initial electronic record has been altered since the transformation was made. "Electronic record" means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another. "Electronic signature" means any letters, characters, numbers, or other symbols in digital form attached to or logically associated with an electronic	Sec. 202. DEFINITIONS (a) In this article: (1) "Access control" means a contract electronically to obtain access to or information from, an information processing system of another person, or the equivalent of such access. (2) "Access material" means any information or material, such as a document, address, or access code, necessary for a party to obtain authorized access to information, or control or possession of a copy of information. (3) "Attornment procedure" means a procedure established by law, regulation, or agreement, or a procedure otherwise adopted by the parties, to verifying that an electronic message authentication record, or performance is that of a specific person, or to detect changes or errors in the information. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, callback or other acknowledgment procedures, or any other procedures that are reasonable under the circumstances. (4) "Authenticable" means to sign, or otherwise to execute or adopt a symbol or sound, or to use encryption or another process with respect to a record, with intent of the authenticating person to: (A) identify that person; (B) adopt or accept the terms of a particular term of a record that includes or is logically associated with, or related to, the authentication, or to which a symbol is associated with, or related to, the authentication, or to which a symbol is logically associated with an electronic

(8) "Electronic signature" means an electronic identifying sound, symbol or process attached to or logically connected with an electronic record and executed or adopted by a person with the intent to associate the person with the electronic record. (9) "Governmental agency" means an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a state or any county, municipality, or other political subdivision of a state. (10) "Information" means data, text, images, sounds, codes, computer programs, software, databases, or the like. (11) "Information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information. (12) "Informational content" means information that is intended to be communicated to or perceived by an individual in the ordinary use of the information (13) "Person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, or public corporation, or any other legal or commercial entity. (14) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. (15) "Security procedure" means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the informational content of an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying	was made. A digital signature is a security procedure. "Electronic" includes electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to these technologies. "Electronic record" means a record generated, communicated, received, or stored by electronic means for use in an information system or for transmission from one information system to another. "Electronic signature" means a signature in electronic form attached to or logically associated with an electronic record. "Information" includes data, text, images, sounds, codes, computer programs, software, databases, and the like. "Key pair" means, in an asymmetric cryptosystem, two mathematically related keys, referred to as a private key and public key, having the property that (i) one key (the private key) can encrypt the message which only the other key (the public key) can decrypt, and (ii) even knowing one key (the public key), it is computationally infeasible to discover the other key (the private key). "Message" means an electronic record into comprising an electronic record into another, generally smaller, set of bits (the message digest), without requiring the use of any secret information such as a key, such that an electronic record yields the same message digest every time the algorithm is executed using such record as input and it is computationally infeasible that any two electronic records can be found or deliberately generated that would produce the same message digest. The two records are precisely identical. "Operational period of a certificate" begins on the date and time the certificate is issued by a certification authority (or on a later date and time certain is stated in the certificate) and ends on the date and time it expires as noted in the certificate or is earlier	persons on documents and signs and symbols identifying their writers. "Electronic Trade": A system that allows Traders and Trade-Related Institutions, whether government or private, to electronically exchange documents that are circulars, rules and regulations (hereinafter collectively referred to as "Trade-Related Laws"), and connects between pertinent parties: "Traders": persons or organizations that are required by Trade-Related Laws to apply, declare and report to Trade-Related Institutions in accordance with such Trade-Related Laws refining trade procedures: "Trade-Related Institutions": institutions which are required by Trade-Related Laws to accept declarations, entries and manifests and issue of entry approvals, clearances, permits, orders, releases and certificates to traders in accordance with Trade-Related Laws defining trade procedures: "Trade VANS or Trade VAS": value-added networks or value-added service providers registered with the national telecommunications Commission pursuant to Republic Act No. 7925, otherwise known as the "Telecommunications Policy Act of the Philippines", and which provide electronic trade services connecting Traders and Trade-Related Institutions through the transmission, switching and local distribution facilities of local exchanges and inter-exchange operators and overseas carriers hereinafter "EDI Trade Network"; and "Accredited Trade VANS or Trade VAS": Trade VANS or Trade VAS duly accredited with the E-look Development Council in accordance with Section 4 of this Act.	record and executed or adopted with the intention to authenticating or approving the electronic record: "Hash function" means an algorithm mapping or translating one sequence of bits into another, generally smaller, set (the hash result) such that (a) a record yields the same hash result every time the algorithm is executed using the same record as input; (b) it is computationally infeasible that a record can be derived or reconstructed from the hash result produced by the algorithm; and (c) it is computationally infeasible that two records can be found that produce the same hash result using the algorithm. "Information" includes data, text, images, sounds, computer programs, software, databases: "Key pair": in an asymmetric cryptosystem, means a private key and its mathematically related public key, having the property that the public key can verify a digital signature that the private key creates. "Certified certification authority" means a certification authority licensed by the Commission pursuant to Regulations made under section 42. "Operational period of a certificate" begins on the date and time the certificate is issued by a certification authority (or on a later date and time if stated in the certificate) and ends on the date and time it expires as stated in the certificate or is earlier revoked or suspended. "Private key" means the key of a key pair used to create a digital signature. "Public key" means the key of a key pair used to verify a digital signature.) "Record" means information that is inscribed, stored, or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. "Repository" means a system for storing and retrieving certificates or other information relevant to certificates: "Revoke a certificate" means to permanently end the operational period of	refers. (5) "Automated transaction" means a contract formed or performed in whole or in part by electronic means or by electronic messages in which the electronic actions or messages of one or both parties that establish the contract are not intended to be reviewed in the ordinary course by an individual. (6) "Cancellation" means the ending of a contract by a party because of a breach by the other party. "Cancel" has a corresponding meaning. (7) "Computer" means an electronic device that can perform substantial calculations, including numerous arithmetic operations or logic operations, without human intervention during the computation or operation. (8) "Computer information" means electronic information, that is in a form directly capable of being processed or used by, or obtained from or through, a computer, but does not include information referred to in Section 28, 104 (2). (9) "Computer information transaction" means a license or other contract whose subject matter is (i) the creation or development of computer information or (ii) to provide access to, acquire, transfer, use, license, modify, or distribute computer information. The term does not include a contract to distribute or create for purposes of distribution, information in print form. (10) "Computer program" means a set of statements or instructions to be used directly or indirectly in a computer to bring about a certain result. The term does not include security derivative informational content. (11) "Consequential damages" include compensation for losses resulting from a party's general or particular requirements and needs of which the other party at the time of contracting had reason to know
---	---	--	---	---

					words or numbers, encryption, calendar, or other acknowledgment procedures. (16) "Transaction" means an action or set of actions relating to the conduct of business or governmental affairs and occurring between two or more persons. (17) "Transferable record" means an electronic record that (a) if the electronic record were in writing would be a note under Article 3 of the Uniform Commercial Code; and (b) the debtor has agreed expressly is subject to the provisions of this Act. (18) "Writing" includes printing, typewriting, and any other intentional reduction of a record to tangible form. "Writer" has a corresponding meaning.	revoked, but does not include any period during which a certificate is suspended. "Person" means an individual, corporation, business trust, estate, trust, partnership, limited partnership, limited liability company, partnership, limited liability company, association, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal or commercial entity. "Private key" means the key of a key pair used to create a digital signature. "Public key" means the key of a key pair used to verify a digital signature. "Record" means information that is inscribed, stored, or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. "Repository" means a system for storing and retrieving certificates or other information relevant to certificates, including information relating to the status of a certificate. "Revoke a certificate" means to permanently end the operational period of a certificate from a specified time forward. "Rule of law" means any statute, ordinance, common law rule, court decision, or other rule of law enacted, established, or promulgated by the State of Illinois, or any agency, commission, department, court, other authority or political subdivision of the State of Illinois. "Security Procedure" means a methodology or procedure used for the purpose of (1) verifying that an electronic record is that of a specific person, or (2) detecting error or alteration in the communication, content, or storage of the electronic record since a specific point in time. A security procedure may require the use of algorithms or codes, identifying words or numbers, encryption, analog, or acknowledgment procedures, or similar security devices. "Signature device" means unique information, such as codes, algorithms, letters, numbers, private keys, or personal identification	a certificate from a specified time. "Rule of law" includes written law. "Security Procedure" means a procedure for the purpose of (a) verifying that an electronic record is that of a specific person, or (b) detecting error or alteration in the communication, content or storage of an electronic record since a specific point in time, which may require the use of algorithms or codes, identifying words or numbers, encryption, acknowledgment procedures, or similar security devices. "Signed" or "signature" and its grammatical variations includes any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic or digital methods. "Subscriber" means a person who is the subject named or identified in a certificate issued to him or who holds a private key that corresponds to a public key listed in that certificate. "Suspend a certificate" means to temporarily suspend the operational period of a certificate for a specified time. "Trustworthy system" means computer hardware, software, and procedures that (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures. "Valid certificate" means a certificate that a certification authority has issued and which the subscriber listed in it has accepted. "Verify a digital signature" means to determine accurately (a) that the digital signature was created using the private key corresponding to the public key listed in the certificate; and (b) the record has not been altered since its digital signature was created.	and which issues could not reasonably be prevented by the aggrieved party, and compensation for losses from injury to person or property proximately resulting from any breach of warranty. The term does not include direct or incidental damages. (12) "Conspicuous", with reference to a term, means so written, displayed, or otherwise presented that a reasonable person against which it is to operate ought to have noticed it. A term in an electronic record intended to enable a response by an electronic agent is conspicuous if it is presented in a form that would enable a reasonably configured electronic agent to take it into account or reject without review of the record by an individual. Conspicuous terms include, but are not limited to, the following: (A) with respect to a person, (i) a heading in capitals in a size equal or greater than, or in contrasting type, font or color to, the surrounding text, (ii) language in the body of a record or display in larger or bolder contrasting type, font or color or is set off from the surrounding text by symbols or other marks that call attention to the language; and (ii) a term prominently referenced in an electronic record or display which is readily accessible and retrievable from the record or display; and (B) with respect to a person or an electronic agent, a term or reference to a term that is so placed in a record or display that the person or electronic agent cannot proceed without taking some action with respect to the term or reference. (13) "Consumer" means an individual who is a licensee of information or informational rights that the individual intended at the time of contracting to be used primarily for personal, family, or household purposes. The term does not include an individual who is a licensee primarily for profit, trading, professional, or commercial purposes, including agriculture, business
--	--	--	--	--	---	--	--	---

						management, and investment management other than management of the individual's personal or family investments. (14) "Consumer transaction" means a contract in which a consumer is the licensee. (15) "Contract fee" means the price, fee, rent, or royalty payable in a contract under this article. (16) "Contractual use restriction" means an enforceable restriction created by contract, which restriction concerns the use or disclosure of, or access to licensed information or informational rights, including a limitation on scope or manner of use. (17) "Copy" means the medium in which information is fixed on a temporary or permanent basis and from which it can be perceived, reproduced, used, or communicated, either directly or with the aid of a machine. (18) "Court" includes an arbitration or dispute-resolution forum if the parties have agreed to use of that forum or its use is required by law. (19) "Delivery" means the voluntary physical or electronic transfer of possession or control of a copy. (20) "Direct damages" includes compensation for losses measured by Section 28.708(b)(1). or 28.709a(1). The term does not include consequential or incidental damages. (21) "Electronic" means of or relating to technology having electrical, digital, magnetic, wireless, optical, or electromagnetic, or similar capabilities. "Electronically" has a corresponding meaning. (22) "Electronic agent" means a computer program, electronic, or other automated means used to independently initiate an action or to respond to electronic messages or performances without review by an individual.				numbers (PINs), or a uniquely configured physical device, that is required alone or in conjunction with other information or devices, in order to create an electronic signature attributable to a specific person. "Signed" or "signature" includes any symbol executed or adopted, or any security procedure employed or adopted using electronic means or otherwise, by or on behalf of a person with intent to authenticate a record. "State agency" means and includes all officers, boards, commissions, courts, and agencies created by the Illinois Constitution whether in the executive, legislative, or judicial branch, all officers, departments, boards, commissions, agencies, institutions, authorities, universities, colleges, public and corporate of the State, and administrative units or corporate outgrowths of the State government which are created by or pursuant to State law. other than units of local government and their officers, school districts and boards of education commissioners, all administrative units and corporate outgrowths of the above and as may be created by executive order of the Governor. "Subscriber" means a person who is the subject named or otherwise identified in a certificate who controls a private key that corresponds to the public key listed in that certificate, and who is the person to whom digitally signed messages verified by reference to such certificate are to be attributed. "Suspend a certificate" means to temporarily suspend the operational period of a certificate for a specified time period or from a specified time forward. "Trustworthy system" means through the use of computer hardware, software, and procedures that, in the context in which they are used, (a) can be shown to be reasonably resistant to penetration, compromise, and misuse (b) provide a reasonable level of reliability, and correct operation, (c) are reasonably
--	--	--	--	--	--	---	--	--	--	--

					limited to performing their intended functions or serving their intended purposes, and (ii) comply with applicable agreements between the parties, if any, and (i) adhere to generally accepted security procedures. "Valid certificate" means a certificate that a certification authority has issued and which that the subscriber listed in the certificate has accepted. "Verify a digital signature" means to use public key listed in a valid certificate, along with the appropriate message digest function and asymmetric cryptosystem, to evaluate a digitally signed electronic record, such that the result of the process concludes that the digital signature was created using the private key corresponding to the public key listed in the certificate and the electronic record has not been altered since its digital signature was created.				(23) "Electronic message" means an electronic record or display stored, generated or transmitted by electronic means for purposes of communication to another. (24) "Good faith" means honesty in fact and the observance of reasonable commercial standards of fair dealing. (25) "Intentional damages" (a) include compensation for any commercially reasonable charge, expense, or compensation reasonably incurred by an aggrieved party after breach of contract in an inspection, repair, replacement, repair through care, or custody of original or replicated copies or information (i) in receiving delivery, shipment or storage; (ii) in an affecting cover; (iii) in repair or replacement of copies or information; or (iv) otherwise incident to the breach, and (b) do not include consequential or special damages. (26) "Information" means data, text, images, sounds, music, works or works of authorship. The term includes software. (27) "Information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information. (28) "Information content" means information that is intended to be communicated to or perceived by an individual in the ordinary use of the information or the equivalent of such information. The term does not include computer instructions that control the interaction of a computer program with other computer programs or with a machine or device. (29) "Intellectual rights" include all rights in information created under laws governing patents, copyrights, mask works, trade secrets, trademarks, publicity rights or any other law that grants a person, independently of contract, a right to control or exclude another person's use of or access to the information or the
--	--	--	--	--	--	--	--	--	---

basis of the rights holder's interest in that information. (30) "License" means a contract within this article that authorizes access to or use of information or of informational rights and expressly limits the contractual rights, permissions, or uses granted expressly prohibits some uses or expressly grants less than all rights in the information. A contract may be a license whether or not the transferee has title to a licensed a copy. "License" includes an access contract and, for purposes of the Uniform Commercial Code, a consignment of a copy. The term does not include a reservation or creation of a security interest. (31) "Licensee" means a transferee in a license or other agreement under this article. A licensor is not a licensee with respect to rights reserved to it under the agreement. (32) "Licensor" means a transferor in a license or other agreement under this article. Between a provider of access in an access contract and its customer, the provider of access is the licensor. Between the provider of access and a provider of the informational content to be accessed, the provider of content is the licensor. In an exchange of information or informational rights, each party is a licensor with respect to the information, informational rights, or accesses it provides. (33) "Mass market license" means a standard form that is prepared for and used in a mass market transaction. (34) "Mass market transaction" means a transaction under this article that is: (A) a consumer transaction, or (B) any other transaction with an end user licensee if (i) the transaction is for information or informational rights directed to the general public, or (ii) the transaction is for the use of information or informational rights under substantially the same terms for the							
---	--	--	--	--	--	--	--

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Purpose, construction, and interpretation

UNCITRAL	UNCUSL	Illinois	Massachusetts	South Korea	Philippine	Singapore	UCC
Art. 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.	Sec.105 Application and Construction This [Act] must be construed and applied consistently with reasonable practices under the circumstances, to facilitate electronic transactions, and to effectuate its general purpose to make uniform the law with respect to the subject of this [Act] among states enacting it.	Sec. 1-102 Purposes and Construction This chapter shall be construed and applied consistently with what is commercially reasonable under the circumstances and to effectuate the following purposes: (1) To facilitate electronic communications by means of reliable electronic records (2) To facilitate and promote electronic commerce, by eliminating barriers resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce (3) To facilitate electronic filing of documents with State and local government agencies, and promote efficient delivery of government services by means of reliable electronic records (4) To minimize the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce (5) To help to establish uniformity of rules and standards regarding the authentication and integrity of electronic records (6) To promote public confidence in the integrity and reliability of electronic records and electronic commerce	Sec.2 Purpose & Construction The provisions of this act shall be construed: (a) to facilitate and promote electronic commerce and online government by clarifying the legal status of electronic records and electronic signatures in the context of writing and signing requirements imposed by law; (b) to permit and encourage the continued expansion of electronic commerce and online government through the operation of free market forces rather than prescriptive legislation; (c) to promote public confidence in the validity, integrity and reliability of electronic commerce and online government; and (d) to promote the development of the legal and business infrastructure necessary to support and encourage electronic commerce and online government	Article 1. Purpose The purpose of this Law is to contribute to the national economy by clarifying the legal effect of transactions by means of electronic messages so as to ensure the security and reliability thereof and to secure fair trade, and further by establishing sound and orderly transactions, and promoting electronic commerce.	Sec.2 Primary objective The objective of this Act is to promote the utilization of Electronic Data Interchange ("EDI") in order to simplify trade procedures and facilitate exchange of EDI in facilitating trade transactions will contribute to the national economy by improving the ability of Filipino business to compete in the international trading community	Sec.3Purposes and Construction The Act shall be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes: (a) to facilitate electronic communications by means of reliable electronic records; (b) to facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce; (c) to facilitate electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of reliable electronic records; (d) to minimize the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions; (e) to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records; and (f) to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.	

PERMISSIVE

UNCITRAL	NCCUSL	Illinois	Massachusetts	South Korea	Philippine	Singapore	UCC
Art. 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.	Sec. 104. Use of Electronic Records and Agreement Electronic signatures: Variation by Agreement (a) This [Act] does not require that records or signatures be generated, stored, sent, received, or otherwise processed or used by electronic means or in electronic form. (b) The use of an electronic record or electronic signature in a transaction must be reasonable. Whether the use of an electronic record or electronic signature in a transaction is reasonable must be determined from the circumstances and context in which it is used, including the parties' statements and agreement, if any, and other applicable law. The obligation of reasonableness prescribed in this subsection may not be disclaimed by agreement. (c) Except as otherwise provided in this [Act], the effect of any provision of this [Act] may be varied by agreement between parties involved in generating, storing, sending, receiving, or otherwise processing or using electronic records or electronic signatures. The presence in certain provisions of this [Act] of the words "unless otherwise agreed" or words of similar import, does not imply that the effect of other provisions may not be varied by agreement. [(c) Whether an agreement has legal consequences is determined by this [Act], if applicable, or otherwise by other applicable rules of law.]	Sec. 1-110 Variation by Agreement As between parties involved in generating, sending, receiving, storing or otherwise processing electronic records, the provisions of this Act may be varied by agreement of the parties, except for the provisions of Sections 10-140, 15-210, 15-215, 15-220, and subsection (b) of Section 10-130 of this Act.		Article 4. Variation Subject to Electronic Interchange Agreement The provisions under Articles 9 through 12 may be modified by an agreement between the originator and the addressee except as otherwise provided in other laws and decrees.		Sec 5 Variation by Agreement As between parties involved in generating, sending, receiving, storing or otherwise processing electronic records, any provision of Part II or IV may be varied by agreement.	Sec 2B-106. Variation by Agreement rules of construction, questions determined by court (a) Except as otherwise expressly provided in this article or in Section 1-102 (3), the effect of any provision of this article, including allocation of risk or imposition of a burden, may be varied by agreement of the parties. (b) Except to the extent provided in the following sections, an agreement may not vary the effect of: (1) the limitations on agreed choice of law in Section 2B-107(a); (2) the limitations on agreed choice of forum in Section 2B-108; (3) the provisions of Sections 2B-110, 2B-208(a), 2B-602(c), and 2B-703(c); (4) the provisions defining manifest assent and opportunity to rescind in Sections 2B-111 and 2B-112; (5) the provisions on electronic errors in Section 2B-118; (6) the limitations on enforceability of an agreement in Section 2B-201; (7) the limits on mass market licenses in Section 2B-208; (8) the requirements for an enforceable term in Sections 2B-303(c), 2B-307(f), 2B-406, and 2B-703(a); (9) the restrictions on altering the period of the statute of limitations in Section 2B-705(a), or (10) the limitations on self-help repossession in Sections 2B-715(a) and 2B-716. (c) In applying this article, the following rules of construction apply: (1) The use of mandatory language or the absence of a phrase such as "unless otherwise agreed" in a provision of this article does not preclude the parties from varying the effect of the provision by agreement. (2) The fact that a provision of this article states a condition for a result does not of itself mean that the absence of that condition yields a different result. (3) To be enforceable, a term need not be conspicuous, negotiated, or expressly assented or agreed to unless this article expressly so requires.

							(d) Whether a term is conspicuous or is excluded under Section 28-105(a) or (b) or 28-208(a) is a question to be determined by the court
--	--	--	--	--	--	--	--

Legal recognition of data message

UNCITRAL	NOCCSL	Illinois	Massachusetts	South Korea	Philippine	Singapore	UCC
Art. 5 Legal recognition of data message Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.	Sec. 106 Legal recognition of electronic records, electronic signatures and electronic contracts (a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form. (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation. (c) If a law requires a record to be in writing, or provides consequences if it is not, an electronic record satisfies the law. (d) If a law requires a signature, or provides consequences in the absence of a signature, the law is satisfied with respect to an electronic record if the electronic record includes an electronic signature. (e) As part of a transaction, nothing in this [Act] precludes a person from establishing reasonable requirements regarding the type of record or signatures acceptable to it.)	Sec. 5-110 Legal recognition Information, records, and signatures shall not be denied legal effect, validity or enforceability solely on the grounds that they are in electronic form	Sec. 67 Electronic Records A record may not be denied legal effect, validity, or enforceability solely because it is in the form of an electronic record if a rule of law requires a record to be in writing, or provides consequences if it is not, an electronic record satisfies that rule of law.	Article 5 Validity of Electronic Messages An electronic message shall not be denied effectiveness or validity relative to other forms of paper-based messages, on the grounds that it is in the electronic form except as specifically provided in any other laws.	Sec. 6 Legal Use of Electronic Documents para (1), (2) When Traders or Trade-Related Institutions utilize an EDI system to submit or apply for declarations, entries, manifests, approvals, clearances, permits, orders, releases and certificates as prescribed by Trade-Related Laws, such submissions or applications shall be considered as having been properly processed according to requirements prescribed by Trade-Related Laws.	Sec. 6 Legal recognition of Electronic records For the avoidance of doubt, it is hereby declared that information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.	Sec. 2B-113 Legal recognition of Electronic records and authentications (a) A record or authentication may not be denied legal effect solely because it is in electronic form. (b) This article does not require that a record or an authentication be generated, stored, sent, received, or otherwise processed by electronic means or in electronic form. (c) In any transaction, a person may establish requirements regarding the type of authentication or record acceptable to it.
Art. 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: [...]	Sec. 107 Provision of information in writing (a) If a law requires a person to provide information in writing to another person, that requirement is satisfied if the information is provided to the person in an electronic record that the person is capable of accessing and retaining for subsequent reference. (b) The effect of this section may not be varied by agreement.	Sec. 5-115 Electronic records (a) Where the rule of law requires information to be "written," or "in writing," or provides for certain consequences if it is not, an electronic record satisfies that rule of law. (b) The provisions of this section shall not apply: (1) when its application would involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the lawmaking body or responsible to the context of the same rule of law, provided that the more requirement that information be "in writing," "written," or "printed" shall not by itself be sufficient to establish such intent; (2) to any rule of law governing the creation or execution of a will or trust, living will, or healthcare power of attorney; and (3) to any record that serves as a unique and transferable instrument of rights and obligations including, without limitation, negotiable instrument and other instruments of the wherein possession of the instrument is	Sec. 5 Writings and Signatures generally Section seven of chapter four of the General Laws is hereby amended by striking out the thirty-eight clause and inserting in place thereof the following: "written" and "in writing" shall include any method, including electronic and digital methods, for inscribing information on a tangible medium or for storing information in an electronic or other medium from which it can be retrieved in perceivable form. In general, where any rule of law purports to specify a particular medium for the creation, storage, communication or authentication of any records or information, that requirement shall be liberally construed to allow the broadest possible use of electronic or digital methods unless there is clear public interest to the contrary.	Sec. 5 Writings and Signatures generally Section seven of chapter four of the General Laws is hereby amended by striking out the thirty-eight clause and inserting in place thereof the following: "written" and "in writing" shall include any method, including electronic and digital methods, for inscribing information on a tangible medium or for storing information in an electronic or other medium from which it can be retrieved in perceivable form. In general, where any rule of law purports to specify a particular medium for the creation, storage, communication or authentication of any records or information, that requirement shall be liberally construed to allow the broadest possible use of electronic or digital methods unless there is clear public interest to the contrary.	The electronic documents constituting such submissions or applications, processed through an EDI system by Traders or Trade-Related Institutions, shall be regarded as the proper paper documents prescribed by Trade-Related Laws.	Sec. 7 Requirement for writing Where a rule of law requires information to be written, in writing, to be presented in writing, or provides for certain consequences if it is not, an electronic record satisfies that rule of law if the information contained therein is accessible so as to be usable for subsequent reference.	

[illegible]

Signature

UNCITRAL	NCCUSL	Illinois	Massachusetts	South Korea	Philippine	Singapore	UCC
Art. 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: [.]	Sec. 108 (b) Attribution and Effect of Electronic Record and Electronic Signature (b) The effect of an electronic record or electronic signature attributed to a person under subsection (a) must be determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law.	Sec. 203 Electronic Signature A new section ____ is added to 5 ILCS 70, to read as follows: (a) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law. (b) An electronic signature may be proved in any manner, including by showing that a procedure existed by which a party must of necessity have executed a symbol or methodology adopted by the party, complies with an authentication procedure / security procedure previously agreed to by the parties. Otherwise, a signature may be proved in any manner, including by showing that a procedure existed by which a party must of necessity have executed a symbol in order to proceed further in the use or processing of the information. (c) Where a rule of law requires that a signature be notarized or acknowledged for the field of record, that requirement shall be deemed satisfied with respect to an electronic record which has not been notarized if (i) the electronic record included a secure electronic signature, or (ii) the creation, transmission and storage of the electronic record itself, and/or the signing such electronic record, provide substantial evidence of the identity of the person signing the electronic record. Whether the substantial evidence standard has been met is for decision by the court. (d) Absent agreement to the contrary, the recipient of a signed electronic record is entitled to establish reasonable requirements with respect to the symbol or methodology adopted by the person signing. (e) The provisions of this section do not apply where:	Sec. 5-120 Electronic Signatures (a) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law. (b) An electronic signature may be proved in any manner, including by showing that a procedure existed by which a party must of necessity have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party in order to proceed further with a transaction. (c) The provisions of this section shall not apply (1) when its application would involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the lawmaking body or repugnant to the context of the same rule of law, provided that the mere requirement of a "signature" or that a record be "signed" shall not by itself be sufficient to establish such intent; (2) to any rule of law governing the creation or execution of a will or trust, living will, or healthcare power of attorney; and (3) to any record that serves as a unique and transferable instrument of rights and obligations including, without limitation, negotiable instruments and other instruments of title wherein possession of the instrument is deemed to confer title, unless an electronic version of such record is created, stored, and transferred in a manner that allows for the existence of only one unique, identifiable, and unverifiable original with the functional attributes of an equivalent physical instrument, that can be possessed by only one person, and which cannot be copied except in a form that is readily identifiable as a copy.	Article 6. Validity of Digital Signatures (1) A digital signature certified by the authorized certification authority pursuant to Article 16 shall be deemed as a valid signature or seal as prescribed by the relevant laws, except as provided otherwise. (2) An electronic message with a digital signature affixed in accordance with Paragraph (1) shall be presumed to have been in its maintained unchanged substance after the originator affixed the signature.	Sec. 7 Validity of Electronic Signature Electronic document used for submission or applications under Section 7 of this Act containing electronic signatures shall be regarded as properly signed, stamped and notarized as prescribed by Trade-Related Laws, where notarization is prescribed by Trade-Related Laws, by entering the electronic signature on an electronic document the person doing so conclusively represents that he executed the same under oath and that he has a paper copy of the electronic document duly notarized in accordance with law Upon demand by the intended recipient of the electronic document or a paper Trade-related institution of the government, said person shall show a copy of the duly notarized paper document. The entering of the proper or agreed electronic signature on an electronic document shall be sufficient for the intended recipient of the electronic document to consider the electronic document as having been duly authorized and insinuated	Sec. 8 Electronic signatures (1) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, and electronic signature satisfies that rule of law. (2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, 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 such party	

UNCITRAL	NCCUSL	Illinois	Massachusetts	South Korea	Philippine	Singapore	UCC
Art. 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 []	Sac. 111 (d) Original (d) If a rule of law (for a commercial practice) requires a record 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 record is not presented or retained in its original form, that rule of law for commercial practice is satisfied by an electronic record retained in accordance with subsection (a).	Sac. 5-125 Original (a) Where a rule of law requires information to be presented or retained in its original form, or provides consequences for the information not being presented or retained in its original form, that rule of law is satisfied by an electronic record if there exists reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as an electronic record or otherwise. (b) The criteria for assessing integrity shall be whether the information has remained complete and unaltered apart from the addition of any endorsement or other information that change which arises in the normal course of communication, storage and display. The standard of reliability required to ensure that information has remained complete and unaltered shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances. (c) The provisions of this section do not apply to any record that serves as a unique and transferable instrument of rights and obligations including, without limitation, negotiable instruments and other instruments of title when possession of the instrument is deemed to confer title, unless an electronic version of such record is created, stored, and transferred in a manner that allows for the existence of only one unique, identifiable and unalterable original with the functional attributes of an equivalent physical instrument, that can be possessed by only one person, and which cannot be copied except in a form that is readily identifiable as a copy.	Sac. 70 Originals If a rule of law requires a record to be presented or retained in its original form, or provides consequences for the record not being presented or retained in its original form, that requirement is met by an electronic record if it accurately reproduces the original record as it existed at the time in question.		Sac. 6 para 2.3 Legal Unit of Electronic Documents Para 2 The electronic documents constituting such submissions or applications, processes through an EDI System by Traders or Trade Related Institutions, shall be regarded as the proper paper documents prescribed by Trade-related Laws Para 3 The print out of an electronic document, duly authenticated by the Accredited Trade Van or Trade WAS, shall be considered as an original of the document for its purposes, the Accredited Trade Van or Trade WAS shall periodically provide its clients/subscribers with a list of EDI transmission made by or to them.		

Admissibility and evidential weight

UNCITRAL	NCCUSL	Illinois	Massachusetts	South Korea	Philippine	Singapore	UCC
Art. 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.	Sec 112 Admissibility in evidence (a) In a legal proceeding, evidence of an electronic record or electronic signature may not be excluded because it is an electronic record or electronic signature, or it is not an original or it is not in its original form. (b) In assessing the persuasive effect of an electronic record or electronic signature, the trier of fact shall consider the manner in which the electronic record or electronic signature was generated, stored, communicated, or retrieved, the reliability of the manner in which the integrity of the electronic record or electronic signature was maintained, the manner in which its originator was identified, and any other relevant circumstances.)	Sec. 5-130 Admissibility into evidence (a) In any legal proceeding, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of an electronic record or electronic signature into evidence: (1) on the sole ground that it is an electronic record or electronic signature; or (2) on the grounds that it is not in its original form or is not an original record shall be given evidential due evidential weight by the trier of fact in assessing the evidential weight of an electronic record or electronic signature where its authenticity is in issue. The trier of fact may consider the manner in which it was generated, stored or communicated, the reliability of the manner in which its integrity was maintained, the manner in which its originator was identified, or the electronic record was signed, and any other relevant information or circumstances	Sec 68 Admissibility into Evidence In any legal proceeding, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of an electronic record or electronic signature into evidence on the sole ground that it is an electronic record or electronic signature or on the sole grounds that it is not in its original form or is not an original.	Article 7. Admissibility of Electronic Messages as Evidence An electronic message shall not be denied admissibility in evidence in litigation or any other legal proceedings on grounds that it is in the electronic form.			

Retention

UNCITRAL	NCCUSL	Illinois	Massachusetts	South Korea	Philippine	Singapore	UCC
Art. 10 Retention of data messages (1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining an electronic record if 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 originally 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 and 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.	Sec. 111 (a)-(c), (f)-(h) Retention of Electronic records (a) If a law requires that certain records be retained, that requirement is met by retaining an electronic record of the information in the record, if the electronic record reflects accurately the information set forth in the record after it was first generated in its final form as an electronic record or otherwise, and the electronic record remains accessible for later reference. (b) A requirement to retain records in accordance with subsection (a) does not apply to any information whose sole purpose is to enable the record to be sent or received. (c) A person satisfies subsection (a) by using the services of any other person if the conditions set forth in subsection (a) are met. (d) If a law requires retention of a check, that requirement is satisfied by retention of an electronic record of the front and back of the check in accordance with subsection (a). (f) A record retained as an electronic record in accordance with subsection (a) satisfies laws requiring a person (other than a governmental agency) to retain records for evidentiary, audit, or tax purposes, unless a law promulgated after the effective date of this Act specifically prohibits the use of an electronic record for a specified purpose. (g) This section does not preclude a governmental agency of this State from specifying additional requirements for the retention of records, either written or electronic, subject to the agency's jurisdiction.	Sec. 5-135 Retention of electronic records (a) Where a rule of law requires that certain documents, records or information be retained, that requirement is met by retaining an electronic record if it accurately reproduces the original record as it existed at the time in question and for so long as may be required by law. Nothing in this section shall preclude any federal or state agency from specifying additional requirements for the retention of records, either written or electronic, that are subject to the jurisdiction of such agency. (1) The electronic record must be retained. (2) The information must be retained in the format in which it was generated, sent or received, or in a format that can be demonstrated to represent accurately the information originally generated, sent or received, and (3) such data as enables the identification of the origin and destination of the information, the authenticity and integrity of the information and the date and time when it was sent and received, if any, is retained. (b) An obligation to retain documents, records or information in accordance with subsection (a) does not extend to any information the sole purpose of which is to enable the record to be sent or received. (c) Nothing in this section shall preclude any State agency from specifying additional requirements for the retention of records that are subject to the jurisdiction of such agency.	Sec. 71 Retention of electronic records If a rule of law requires that a record to be retained, that requirement is met by retaining an electronic record if it accurately reproduces the original record as it existed at the time in question and for so long as may be required by law. Nothing in this section shall preclude any federal or state agency from specifying additional requirements for the retention of records, either written or electronic, that are subject to the jurisdiction of such agency.	Article 8. Retention of Electronic Messages (1) Where an electronic message satisfies the following conditions, the requirement that certain documents or records be retained as set forth in the relevant laws may be regarded as having been met by the retention of the electronic message: 1. the information contained therein is accessible; 2. the electronic message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to accurately represent the information generated, sent or received, and 3. such information, if any, is retained to enable the identification of the origin and destination of the electronic message and the date and time when it was sent or received. (2) A certain message may not be deemed as an electronic message under Paragraph (1) regarding the periods required only for the dispatch or receipt thereof.		Sec. 9 Retention of electronic records (1) Where a rule of law requires that certain documents, records or information be retained, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied: (a) the information contained therein remains accessible so as to be usable for subsequent reference, (b) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received, (c) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained, and (d) the content of the department or ministry of the Government, organ of State, or the statutory corporation which has supervision over the requirement for the retention of such records has been obtained. (2) An obligation to retain documents, records or information in accordance with subsection (1)(c) shall not extend to any information necessary and automatically generated solely for the purpose of enabling the record to be sent or received. (3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in paragraphs (a) to (d) of that subsection are complied with. (4) Nothing in this section shall: (a) apply to any rule of law which expressly provides for the retention of documents, records or information in the form of electronic records; (b) preclude any department or ministry of the Government, organ of State or a statutory corporation from	

[illegible]

Formation and validity of contracts

UNCITRAL	NCCUSL	Illinois	Massachusetts	South Korea	Philippine	Singapore	UCC
Art.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 [. . .]	Sec.113 Formation of contract (a) If an offer in an electronic record initiated by a person, or by its electronic agent, evokes an electronic record in response, a contract is formed in the same manner and with the same effect as if the electronic records were not electronic, except that a contract is formed, if at all, if the response consists of electronic performance of the requested consideration in whole or in part, when the responding communication is to be performed electronically, is received unless the offer prohibits that form of response. (b) In an automated transaction, the following rules apply: (1) A contract may be formed by the initiation of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements. (2) A contract may be formed by the initiation of a person's electronic agent and an individual, including by an individual in which the individual performs, acts, or is free to refuse to perform, and that individual knows or has reason to know will cause the electronic agent to complete the transaction or performance. (c) The terms of a contract are determined by the substantive law applicable to the particular contract.		Art. 10 Where the Originator is Deemed to Have Sent Electronic Messages An electronic message is deemed to be sent by the originator if it was sent by a person who has been authorized to act on behalf of the originator, or by an information system or any other electronic means programmed by, or on behalf of, the originator to operate automatically. Originator however, that the following code does not apply: 1. where the addressee has received notice from the originator that the electronic message was sent against the intention of the originator either at the same time, or within a reasonable time after, the receipt thereof; or 2. where the addressee used any agreed upon communication procedure, or view or signal that is known, had it received notification that the electronic message was sent against the intention of the originator. Art. 11 Individuality of the Electronic Message Received The electronic message shall be deemed to be individual for each message received provided, however, that such individuality does not apply where the addressee has agreed upon a communication procedure, or knew or should have known, had it exercised reasonable care, that the originator's electronic message was sent repeatedly.	Art. 10 Where the Originator is Deemed to Have Sent Electronic Messages An electronic message is deemed to be sent by the originator if it was sent by a person who has been authorized to act on behalf of the originator, or by an information system or any other electronic means programmed by, or on behalf of, the originator to operate automatically. Originator however, that the following code does not apply: 1. where the addressee has received notice from the originator that the electronic message was sent against the intention of the originator either at the same time, or within a reasonable time after, the receipt thereof; or 2. where the addressee used any agreed upon communication procedure, or view or signal that is known, had it received notification that the electronic message was sent against the intention of the originator. Art. 11 Individuality of the Electronic Message Received The electronic message shall be deemed to be individual for each message received provided, however, that such individuality does not apply where the addressee has agreed upon a communication procedure, or knew or should have known, had it exercised reasonable care, that the originator's electronic message was sent repeatedly.	Sec.11 Formation and validity (1) For the avoidance of doubt, it is hereby declared that in the context of the formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic records. (2) Where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose.	Sec. 2B-204 Offer and Acceptance, Electronic Agents (a) A contract may be formed by the interaction of electronic agents, if the interaction results in the electronic agents' engaging in operations that confirm or indicate the existence of a contract. A contract is formed unless the operations resulted from fraud or electronic mistake or the like. (b) A contract may be formed by the interaction of an electronic agent and an individual. A contract is formed if the individual takes actions that it is free to refuse to take or makes a statement that the individual has reason to know will, at its clause, the electronic agent to perform, provide benefits, permit the use or access to information, or the like. (c) The terms of a contract formed under subsection (b) are determined under subsection (b) or 2B-208, as applicable, but do not include terms provided by the individual if it had reason to know that the electronic agent could not react to the terms as provided. Sec. 2B-120 (a)(b) Electronic message, binding of contract, effectiveness of message, acknowledging message (a) Except as otherwise provided in subsection (b) and (c), an electronic record is effective when received even if no individual is aware of its receipt. (b) If an offer in an electronic message evokes an electronic message in response, a contract is formed: (1) when an acceptance is received; or (2) if the response consists of furnishing or giving access to information, when the information or notice of access is received or use is enabled, unless the originating message required acceptance in a different manner.	

Recognition by parties

UNCITRAL	NCCUSL	Illinois	Massachusetts	Korea	Philippine	Singapore	UCC
Art. 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: []						Sec. 12 Effectiveness between parties As between the originator and the addressee of an electronic record, a declaration of intent or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of an electronic record	

Attribution

UNCITRAL	NCCUSL	Illinois	Korea	Philippine	Singapore	UCC
Art. 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 electronic records as its own. (4) Paragraph (3) does not apply, (5) as of the time when 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 ought to 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, 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	Sec. 108 (a) Attribution and Effect of Electronic Record and Electronic Signature (1) An electronic record or electronic signature is attributable to a person if it was in fact the act of the person, or its electronic agent. Attribution may be proved in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.				Sec. 13 Attribution (1) An electronic record is that of the originator if it was sent by the originator himself. (2) As between the originator and the addressee, an electronic record 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 electronic record; 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 an electronic record as being that of the originator and to act on that assumption if: (a) in order to ascertain whether the electronic record 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 electronic records as its own. (4) Subsection (3) shall not apply, (a) from the time when addressee has both received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly; (b) in a case within subsection (3)(b), at any time when the addressee knew or ought to have known, had it exercised reasonable care or used any agreed procedure, that the electronic record was not that of the originator; or (c) in all the circumstances of the case, it is unconscionable for the addressee to regard the electronic record as that of the originator or to act on that assumption. (5) Where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is deemed	Sec. 2B-117 Attribution procedure for detection of changes and errors: effect of use. (a) In this section, "electronic record" means an electronic authentication, message record, or performance. (b) If the parties use to a commercially reasonable attribution procedure to detect errors or changes in an electronic record, the following rules apply: (1) The effect of the procedure is determined by the agreement or, in the absence of agreement, by this section or any law establishing the procedure. (2) If the procedure indicates that an electronic record was unaltered since a point in time, it is presumed not to not have been altered since that time. (3) As to portions to which the procedure applies, if a procedure indicates that there is no error in content, an electronic is presumed at the time it was sent to have had the content intended by the person creating or sending it pursuant to the procedure. (4) If the sender has conformed to the procedure but the other party has not and the nonperforming party would have detected the change or error had that party also conformed the sender is not bound by the change or error.

[illegible]

Acknowledgment

UNCITRAL	NCCUSL	Illinois	Massachusetts	South Korea	Philippine	Singapore	UCC
Art. 14 Acknowledgment 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 agreed with the addressee that receipt of a data message be acknowledged. (2) Where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment 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 acknowledgment, the data message is treated as though it has never been sent, until the acknowledgment is received. (4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, with in a reasonable time, the originator - (a) may give notice to the addressee stating that no acknowledgment has been received and specifying a reasonable time by which the acknowledgment must be received, and (b) if the acknowledgment 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 acknowledgment of receipt, it is presumed that the related data message was received by the addressee. This presumption does not imply that the	Sec. 110 Notarization and acknowledgement If a law requires that a signature be notarized or acknowledged, or provides consequences in the absence of a notarization or acknowledgement, the law is satisfied with respect to an electronic signature if a security procedure was applied which establishes the identity of the person signing the electronic record (and that the electronic record has not been altered since it was electronically signed).		Art. 12 Acknowledgement of Receipt (1) Where the originator has requested the acknowledgement of receipt of a sent electronic message, but fails to designate the communication method, the addressee shall provide an acknowledgement of receipt thereof in such a manner as the originator may be fully informed. (2) Where the originator has sent the electronic message stating that it is conditional on receipt of the acknowledgement, the electronic message shall be deemed as if it had never been sent, until the acknowledgement is received by the originator. (3) Where the originator has requested the acknowledgement of receipt of the electronic message without stating that it is conditional on receipt of the acknowledgement, the originator may withdraw the dispatch of the electronic message unless it receives the acknowledgement thereof within a reasonable time, or within the time specified by the originator, or as agreed upon by the originator and the addressee.		Sec. 14 Acknowledgement of receipt (1) Subsections (2), (3) and (4) shall apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or agreed with the addressee that receipt of electronic record 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 electronic record has been received. (3) Where the originator has stated that the electronic record is conditional on receipt of the acknowledgement, the electronic record is treated as though it had never been sent, until the acknowledgement is received. (4) Where the originator has not stated that the electronic record 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, with in 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 paragraph (a), may, upon notice to the addressee, treat the electronic record as though it has 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, unless evidence to the contrary is adduced, that the related electronic record was received by the	Sec. 28-129 (6). Electronic message: timing of contract, effectiveness of message, acknowledging message. (d) Receipt of an electronic acknowledgement creates a presumption that the message was received, but, in itself, does not establish that the content sent corresponds to the content received.	

[illegible]

Time and place of dispatch and receipt

UNCITRAL	NCCUSL	Illinois	Massachusetts	South Korea	Philippine	Singapore	UCC
Art. 15 Time and place of dispatch and receipt (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 sent to the addressee. (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	Sec. 115 Time and place of sending and receipt (a) Unless otherwise agreed between the sender and the recipient, an electronic record is sent when the information is addressed or otherwise directed properly to the recipient and enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender. (b) Unless otherwise agreed between the sender and the recipient, an electronic record is received when the electronic record enters an information processing system that the recipient has designated or used for the purpose of receiving electronic records or information of the type sent, in a form capable of being processed by that system, and from which the recipient is able to retrieve the electronic record. (c) Subsection (b) applies even if the place the information processing system is located is different from the place the electronic record is considered to be received under Subsection (a). (d) Unless otherwise expressly provided in the electronic record or agreed between the sender and the recipient, an electronic record is deemed to be sent from the sender's place of business and is deemed to be received at the recipient's place of business. For the purposes of this subsection, the following rules apply: (1) if the sender or recipient has more than one place of business, the place of business of that person is that which has the closest relationship to the underlying transaction; (2) if the sender or recipient does not have a place of business, the place of business is the sender's or recipient's residence; (3) if the case may be (e) An electronic record is effective when received even if no individual is aware of its receipt. (f) Receipt of an electronic acknowledgment establishes that a			Art. 9 Time and Place of Dispatch and Receipt of Electronic Messages (1) The dispatch of an electronic message shall be deemed to occur when it enters an information system outside the control of the originator or of the person who sent the electronic message on behalf of the originator. (2) The receipt of an electronic message is deemed to occur 1. at the time when the electronic message enters the designated information system if the addressee has designated an information system for the purpose of receiving electronic messages; provided, however, that at the time when the electronic message is retrieved by the addressee the electronic message is sent to an information system of the addressee that is not the designated information system, or 2. at the time when the electronic message enters an information system of the addressee if the addressee has not designated an information system. (3) An electronic message is deemed to be sent or received at the place where the originator or the addressee has its place of business, provided however, that, 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, provided further, however, that if the originator or the addressee does not have a place of business, reference is to be made to its normal place of residence.	Sec. 8 Transmittal Times for Electronic Documents Electronic documents used for submissions or approvals under Section 7 of this Act shall be deemed as having been received by the identified receiving party at the moment they are recorded in the computer files of the receiving party as verified by the Accredited Trade VAN or Trade VAS. The manner of verification of receipt of electronic documents shall be agreed upon by the Trade Van or Trade VAS and the client/subscriber, or in the absence thereof, shall be set by the Trade VAN or Trade VAS and communicated to its client/subscribers	Sec. 15 Time and place of dispatch and receipt (1) Unless otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters an information system outside the control of the originator or the person who sent the electronic record on behalf of the originator. (2) Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record is determined as follows: (a) if the addressee has designated an information system for the purpose of receiving electronic records, receipt occurs—(i) at the time when the electronic record enters the designated information system, or (ii) if the electronic record is sent to an information system of the addressee that is not the designated information system, at the time when the electronic record is retrieved by the addressee. (b) If the addressee has not designated an information system, receipt occurs when the electronic record enters an information system of the addressee. (3) Subsection (2) shall apply notwithstanding that the place where the information system is located may be different from the place where the electronic record is deemed to be received under subsection (4). (4) Unless otherwise agreed between the originator and the addressee, an electronic record 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 section—(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	

addressee does not have a place of business, reference is to be made to his habitual residence. (5) The provisions of this article do not apply to the following []	record was received but, in itself, does not establish that the content sent corresponds to the content received					business, (b) if the originator or the addressee does not have a place of business, reference is to be made to the usual place of residence, and (c) "usual place of residence" in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted (6) This section shall not apply to such circumstances as the Minister may by regulations prescribe	
---	--	--	--	--	--	---	--

Secure electronic record

Illinois	South Korea	Philippine	Singapore
Sec.10-105 Secure Electronic record. (a) If, through the use of a qualified security procedure it can be verified that an electronic record has not been altered since a specified point in time, then such electronic record shall be considered to be a secure electronic record from such specified point in time of verification, if the relying party establishes that the qualified security was: (1) commercially reasonable under the circumstances, (2) applied by the relying party in a trustworthy manner, and (3) reasonably and in good faith relied upon by the relying party. (b) A qualified security procedure for purposes of this Section is a security procedure to detect changes in the content of an electronic record that is: (1) previously agreed to by the parties; or (2) certified by the Secretary of State in accordance with Section 10-135 as being capable of providing reliable evidence that an electronic record has not been altered.	Art.14. Security of Information Systems (1) The electronic traders shall take protective measures to ensure the security of the information system used for electronic commerce. (2) Where the electronic traders entrust another person to operate the information systems, the party which can ensure the optimum level of security shall be entrusted. In so doing, if there occurs a breakdown due to the negligence of such trustee, the electronic traders shall notify the counterparty of the breakdown and promptly remedy such breakdown.	Sec.10 Security of Electronic Documents and Trade Information It shall be unlawful to forge, alter, damage, or violate the secrecy of, otherwise mislead, electronic documents recorded in computer files or the trade information compiled in the data bases of Trade VANS or Trade VAS. Traders, Trade-Related Institutions or other agencies Officers or employees, or ex-employees, of a Trade VAN or Trade VAS shall not disclose or appropriate confidential trade information or secrets or electronic documents obtained in the line of duty. Trade VAN or Trade VAS, Traders, Trade-Related Institutions or other agencies shall maintain their electronic documents and data base for the time duration prescribed by accounting and tax rules and regulations. Trade VAN and Trade VAS shall install and use safeguard devices required for the safekeeping of electronic documents and trading information.	Sec.10 Secure electronic record (1) If a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved has been properly applied to an electronic record to verify that the electronic record has not been altered since a specified point in time, such record shall be treated as a secure electronic record from such specified point in time to the time of verification. (2) For the purposes of this section and section 17, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including - (a) the nature of the transaction; (b) the sophistication of the parties; (c) the volume of similar transactions engaged in by either or all parties; (d) the availability of alternatives offered to but rejected by any party; (e) the cost of alternative procedures; and (f) the procedures in general use for similar types of transactions.

Secure electronic signature

Illinois	Korea	Philippine	Singapore
Sec. 10-110 Secure electronic signature (a) If, through the use of a qualified security procedure, it can be verified that an electronic signature is the signature of a specific person, then such electronic signature shall be considered to be a secure electronic signature at the time of verification, if the relying party establishes that the qualified security procedure was: (1) commercially reasonable under the circumstances, (2) applied by the relying party in a trustworthy manner, and (3) reasonably and in good faith relied upon by the relying party. (b) A qualified security procedure for purposes of this Section is a security procedure for identifying a person that is: (1) previously agreed to by the parties; or (2) certified by the Secretary of State in accordance with Section 10-135 as being capable of creating, in a trustworthy manner, an electronic signature that: (A) is unique to the signer within the context in which it is used; (B) can be used to objectively identify the person signing the electronic record; (C) was reliably created by such identified person (e.g., because some aspect of the procedure involves the use of a signature device or other means or method that is under the sole control of such person); and that cannot be readily duplicated or compromised; and (D) is created, and is linked to the electronic record to which it relates, in a manner such that if the record or the signature is intentionally or unintentionally changed after signing the electronic signature is invalidated.			Sec. 17 Secure electronic signature If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made - (a) unique to the person using it; (b) capable of identifying such person; (c) created in a manner or using a means under the sole control of the person using it; and (d) is linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated, such signature shall be treated as a secure electronic signature.

Presumptions

Illinois	Korea	Philippine	Singapore
Sec. 10-120 Presumptions (a) In resolving a civil dispute involving a secure electronic record, it shall be rebuttably presumed that the electronic record has not been altered since the specific point in time to which the secure status relates. (b) In resolving a civil dispute involving a secure electronic signature, it shall be rebuttably presumed that the secure electronic signature is the signature of the person to whom it correlates. (c) The effect of presumptions provided in this Section is to place on the party challenging the integrity of a secure electronic record or challenging the genuineness of a secure electronic signature both the burden of going forward with evidence to rebut the presumption and the burden of persuading the trier of fact that the nonexistence of the presumed fact is more probable than its existence. (d) In the absence of a secure electronic record or a secure electronic signature, nothing in this [Act] shall change existing rules regarding legal or evidentiary rules regarding the burden of proving the authenticity and integrity of an electronic record or an electronic signature.			Sec. 18 Presumptions relating to secure electronic records and signatures (1) In any proceedings involving a secure electronic record, it shall be presumed, unless evidence to the contrary is adduced, that the secure electronic record has not been altered since the specific point in time to which the secure status relates. (2) In any proceedings involving a secure electronic signature, it shall be presumed, unless evidence to the contrary is adduced, that - (a) the secure electronic signature is the signature of the person to whom it correlates, and (b) the secure electronic signature was affixed by that person with the intention of signing or proving the electronic record. (3) In the absence of a secure electronic record or a secure electronic signature, nothing in this Part shall create any presumption relating to the authenticity and integrity of the electronic record or an electronic signature. (4) For the purpose of this section, "secure electronic record" means an electronic record treated as a secure electronic record by virtue of section 16 or 19, "secure electronic signature" means an electronic signature treated as a secure electronic signature by virtue of section 17 or 20.

Government use of electronic record

NCCUSL	Illinois	Massachusetts	Singapore
PART 2 Governmental electronic records and signatures Sec. 201. Creation and Retention of Electronic Records and Conversation of written Records by Governmental Agencies. [Each governmental agency] [The designated state official] of this State shall determine if, and the extent to which, it will create and retain electronic records and convert written records to electronic records. Sec. 202. Acceptance and Distribution of Electronic Records by Governmental Agencies. (a) Except as otherwise provided in Section 111(e), [each governmental agency] [the designated state official] of this State shall determine whether, and the extent to which, it will send and accept electronic records and electronic signatures. Signatures to and from other persons, and otherwise create, use, store, and rely upon electronic records and electronic signatures. (b) In a case governed by subsection (a), the [governmental agency] [designated state official], by appropriate regulation giving due consideration to security, shall specify: (1) the manner and format in which the electronic records must be created, sent, received, and stored, and the systems established for such purposes; (2) if electronic records must be electronically signed, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person using a document to facilitate the process; (3) control processes and procedures as appropriate to ensure adequate integrity, security, confidentiality, and availability of such electronic records; and (4) any other required attributes for electronic records which are currently specified for corresponding non-electronic records, or reasonably necessary under the circumstances. (c) Except as otherwise provided in Section 111(e), this [Act] does not require any governmental agency of this State to use or permit the use of electronic records or electronic signatures. Sec. 203. Interpretability. Regulations adopted by [a governmental agency] [designated state official] of this State pursuant to Section 202 must be designed to encourage and promote consistency and interoperability with similar requirements adopted by other governmental agencies of this and other States and the federal government, and non-governmental persons interacting with governmental agencies of this State. If appropriate, those regulations must specify differing levels of standards from which governmental agencies of this State may choose in implementing the most appropriate standard for a particular application.	ART 25 State agency use of electronic records and signatures Sec. 25-101 State agency use of electronic records. (a) Each State agency shall determine if, and the extent to which, it will send and receive electronic records and electronic signatures to and from other persons and otherwise create, use, store, and rely upon electronic records and electronic signatures. (b) In any case where a State agency decides to send or receive electronic records, or to accept document filings by electronic records, the State agency may, by appropriate agency rule (or court rule where appropriate), giving due consideration to security, specify: (1) the manner and format in which such electronic records must be created, sent, received, and stored; (2) if such electronic records must be signed, the type of electronic signature required, the manner and format in which such signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by the person filing the document to facilitate the process; (3) control processes and procedures as appropriate to ensure adequate integrity, security, confidentiality, and availability of such electronic records; and (4) any other required attributes for such electronic records that are currently specified for corresponding paper documents, or reasonably necessary under the circumstances. (c) All rules adopted by a State agency shall include the relevant minimum security requirements established by the Department of Central Management Services, if any. (d) Whenever any rule of law requires or authorizes the filing of any information, notice, petition, or other document or record with any State agency, a filing made by an electronic record shall have the same force and effect as a filing made on paper in all cases where the State agency has authorized or agreed to such electronic filing and the filing is made in accordance with applicable rules or agreement. (e) Nothing in this Act shall be construed to require any State agency to use or to permit the use of electronic records or electronic signatures. Sec. 25-105 Department of Central Management Services to adopt State standards. (a) The Department of Central Management Services may adopt rules setting forth minimum security requirements for the use of electronic records and electronic signatures by State agencies: (b) The Department of Central Management Services shall specify appropriate minimum security requirements to be implemented and followed by State agencies for (1) the generation, use, and storage of key pairs; (2) the issuance, acceptance, use, suspension, and revocation of certificates; and (3) the use of digital signatures. (c) Each State agency shall have the authority to issue or contact for the issuance of, certificates to (1) its employees and agents, and (2) persons conducting business or other transactions with such State agency and to take other actions consistent therewith, including the establishment of repositories, and the suspension or revocation of certificates so issued, provided that the foregoing is conducted in accordance with all the rules, procedures, and policies specified by the Department of Central Management Services. The Department of Central Management Services shall have the authority to specify the rules, procedures, and policies whereby State agencies may issue or contact for the issuance of certificates. (d) The Department of Central Management Services may specify appropriate minimum standards and requirements that must be satisfied by a certification authority before (1) its services are used by any State agency for the issuance, collection, revocation, and suspension of certificates to such agency, or its employees or agents for official use; or (2) the certificates it issues will be accepted for purposes of verifying digitally signed electronic records sent to any State agency by any person.	Sec. 72 Role of the Chief Information Officer The Chief Information Officer designated in section four A of Chapter seven shall have the authority to coordinate, oversee, operate, and approve the use of information security and authentication technologies by an public entity within the executive department.	Sec. 47 Acceptance of electronic filing and issue of documents. (1) Any department or ministry of the Government, organ of State, statutory corporation, or public body shall accept the filing of documents, or requests that documents be created or retained: (b) issued any permit, licence or approval; or (c) provides for the method and manner of payment, may notwithstanding anything to the contrary in such written law: (i) accept the filing of such documents, or the creation or retention of such documents in the form of electronic records; (ii) issue such permit, licence or approval in the form of electronic records; or (iii) make such payment in electronic form. (2) In any case where a department or ministry of the Government, organ of State or statutory corporation decides to perform any of the functions in subsection (1)(b), (ii) or (iii), such agency may specify: (a) the manner and format in which such electronic records shall be filed, created, retained or issued; (b) where such electronic records have to be signed, the type of electronic signature required including, if applicable, a requirement that the sender use a digital signature or other secure electronic signature; (c) the manner and format in which such signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any certification authority used by the person filing the document; (d) control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; and (e) any other required attributes for electronic records or payments that are currently specified for corresponding paper documents. (3) Nothing in this Act shall by itself compel any department or ministry of the Government, organ of State or statutory corporation to accept or issue any document in the form of electronic records.

		(e) Where appropriate, the rules adopted by the Department of Central Management Services pursuant to this Section shall specify differing levels of minimum standards from which implementing State agencies can select the standard most appropriate for a particular application. (f) The General Assembly, through the Joint Committee on Legislative Support Services, and the Supreme Court, separately for the respective branches, may adopt rules setting forth the minimum security requirements for the use of electronic records and electronic signatures by the respective branches. The rule shall generally be consistent with the rules adopted by the Department of Central Management Services. The Joint Committee on Legislative Support Services and the Supreme Court may also accept the rules adopted by the Department of Central Management Services for the use of electronic records and electronic signatures by the respective branches. (g) Except as provided in subsection (f) and in Section 25-101, the Department of Central Management Services shall have exclusive authority to adopt rules authorized by this Section. Sec 25-115 Interpretability To the extent reasonable under the circumstances, rules adopted by the Department of Central Management Services or a State agency relating to the use of electronic records or electronic signatures shall be drafted in a manner designed to encourage and promote consistency and interoperability with similar requirements adopted by government agencies of other states and the federal government.	
--	--	--	--



ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม

73/1 ชั้น 6 อาคาร สวทช. ถนนพระรามที่ 6 เขตราชเทวี กรุงเทพฯ 10400

โทรศัพท์: 044-8150..99 โทรสาร: 044-8653

E-mail : nitc-sec@nectec.or.th

Web Site : <http://www.nitc.go.th>