

วิเคราะห์ปัญหาและมาตรการทางกฎหมายของประเทศไทยที่เกี่ยวข้อง กับการทุจริตในการใช้บัตรเครดิตบนอินเทอร์เน็ต

ปัญหาการไม่เปิดเผยตัวตนในระบบเครือข่ายคอมพิวเตอร์

ลักษณะเฉพาะประการหนึ่งของคอมพิวเตอร์ คือ สามารถปกปิดตัวตนของผู้ใช้ได้ ในระดับหนึ่ง หรือการใช้ชื่อที่ไม่ใช่ชื่อจริง ซึ่งจะไม่เหมือนกับสิ่งต่างๆ ที่ไม่ใช่สิ่งที่เป็นอิเล็กทรอนิกส์ ผู้ที่ใช้ระบบเครือข่ายสามารถที่จะทำตัวเป็นใครก็ได้ตามต้องการ โดยการหลอก ลวงว่าเป็นผู้ใช้รายอื่น หรือระบุตนตามที่เห็นว่าสมควร การปกปิดตัวตนเช่นนี้มีผลอย่างสำคัญในทางกฎหมาย อาญา เพราะนอกจากจะทำให้การตรวจสอบอาชญากรรมคอมพิวเตอร์ และตัวผู้กระทำผิดยากขึ้น แล้ว ยังทำให้เกิดปัญหาความยุ่งยากในการพิสูจน์ความผิดในระหว่างการพิจารณาด้วย ตัวอย่าง เช่น หากพบว่ามี การแพร่เชื้อไวรัสและสำเนาข้อมูลที่มีไวรัสนั้นถูกเก็บไว้ในคอมพิวเตอร์ที่ Jsmith@gsu.edu โดยผู้รับผิดชอบก็คือผู้ใช้ที่มีชื่อว่า J.Smith ซึ่งอยู่ที่ Gigantic State University แต่กรณีนี้ก็ไม่ได้มีหลักฐานที่แน่นอนพอที่จะสรุปได้ว่า J.Smith เป็นเจ้าของหรือผู้เผยแพร่ไวรัสนั้น ซึ่งผู้ใช้คนอื่นที่มีความสามารถในการที่จะลักลอบหรือปลอมแปลงใช้ E-mail ของ J.Smith พร้อมทั้งสามารถที่จะเก็บไวรัสนั้นไว้ในคอมพิวเตอร์ภายใต้รายชื่อบัญชีของ J.Smith ซึ่งการพิสูจน์ความเป็นเจ้าของไวรัสนั้นเป็นปัญหาที่ยุ่งยาก

การปกปิดตัวตนของผู้ใช้ในระบบเครือข่ายคอมพิวเตอร์นั้น เป็นสาเหตุหนึ่งที่ชักจูงให้พวกเขาไม่คิดจะกระทำผิดในที่อื่นใดนอกจากในระบบเครือข่ายคอมพิวเตอร์ เหตุผลหนึ่งคือ ความไร้จริยธรรมในระบบเครือข่ายคอมพิวเตอร์ ภายนอกระบบเครือข่ายมีการวางรากฐานโครงสร้างจริยธรรมเกี่ยวกับพฤติกรรมที่ยอมรับได้และที่ยอมรับไม่ได้ผ่านประสบการณ์นานนับปี เช่น กรณีลูกค้าของโรงแรมทราบดีว่าเขาสามารถที่จะเข้าไปพักในห้องโรงแรมได้นานทราบเท่าที่เขาจ่ายค่าห้องพัก และไม่ได้ก่อความไม่สงบ สิ่งคล้ายกันก็คือการที่เราทราบว่าพื้นที่สาธารณะในโรงแรม เช่น ลิโอบบี้ และห้องอาหารเป็นบริเวณที่ใครก็สามารถเข้าไปใช้บริการได้ไม่ว่าจะเป็นแขกของโรงแรมหรือไม่ก็ตาม ทำที่สุดเราทราบว่าเราไม่สามารถเข้าไปในพื้นที่หวงห้ามของโรงแรมได้ เช่น สำนักงาน บริเวณส่งสินค้า หรือห้องครัว เราทราบสิ่งเหล่านี้โดยไม่ต้องมีใครมาบอกเนื่องจากมันเป็นสิ่งที่รู้ได้จากประสบการณ์ แต่ไม่มีประสบการณ์เกี่ยวกับจริยธรรมในระบบเครือข่าย ผู้ที่เข้าไปในระบบคอมพิวเตอร์ของผู้อื่นนั้น อาจเข้าไปโดยที่เจ้าของเครื่องมิได้รับรู้ หรือผู้ที่เข้าไปไม่

อาจทราบได้ว่าแฟ้มข้อมูลบางอย่างสามารถเข้าถึงได้ แต่บางอย่างก็ไม่สามารถเข้าถึงได้ ยังไม่มีการกำหนดขอบเขตของพฤติกรรมที่ยอมรับได้ หรือแม้แต่พฤติกรรมทางจริยธรรมในระบบเครือข่าย และก็ยังไม่มีการเห็นชอบเกี่ยวกับเรื่องที่ว่า ข้อมูลใดที่เป็นทรัพย์สินของเครือข่าย และการกระทำใดที่ถือว่าเป็นการขโมย หรือละเมิดต่อทรัพย์สินนั้น ในความเป็นจริงแล้วยังไม่มีการเห็นพ้องต้องกันเกี่ยวกับมารยาทในการใช้รหัสผ่าน (password) ร่วมกัน และสิ่งที่เกิดขึ้นบ่อยครั้งก็คือ ความยากลำบากในการที่จะระบุว่าการใช้ระบบคอมพิวเตอร์ของบุคคลนั้น เป็นการใช้ที่ได้รับอนุญาตโดยถูกต้องหรือไม่ และหากได้รับอนุญาตโดยถูกต้องแล้ว ใครเป็นคนอนุญาต¹

ปัญหาเกี่ยวกับทรัพย์สินในโลกคอมพิวเตอร์

ในไม่ช้าผู้ที่ดำเนินคดีอาญาเกี่ยวกับคอมพิวเตอร์ในยุคแรกๆ ก็พบว่าการใช้แนวความคิดทางกฎหมายปกติกับสื่ออิเล็กทรอนิกส์มีปัญหาเกิดขึ้น เช่น กรณีจำเลยซึ่งเป็นอดีตลูกจ้างของบริษัท ABC และปัจจุบันได้ทำงานให้กับนายจ้างใหม่ คือ บริษัท XYZ ซึ่งเป็นคู่แข่ง นายจ้างเก่าของลูกจ้างคนนี้ได้ลบข้อมูลของจำเลยออกจากระบบ และจำเลยก็ได้เข้าไปขโมยข้อมูลเกี่ยวกับการประมวลงานและนำมาใช้เป็นประโยชน์ให้กับนายจ้างใหม่ ในกรณีนี้จำเลยได้กระทำความผิดทางอาญาหรือไม่ สิ่งที่เห็นได้ชัดเจนก็คือ ข้อมูลการประมวลงานของนายจ้างเก่ามีความละเอียดอ่อน แต่สิ่งที่ไม่ชัดเจนก็คือข้อมูลนั้นอยู่ภายใต้การปกป้องโดยกฎหมายหรือไม่ ยิ่งไปกว่านั้น การกระทำของลูกจ้างก็ไม่ชัดเจนว่าเป็นการกระทำผิดตามกฎหมายอาญาหรือไม่ คำถามก็คือ ข้อมูลนั้นถูกขโมยไปจริงหรือไม่ จะเห็นได้ชัดเจนว่าข้อมูลนั้นยังคงอยู่ในคอมพิวเตอร์ของนายจ้างเก่า และนายจ้างเก่าสามารถใช้ข้อมูลนั้นได้อยู่ ฉะนั้น จะถือว่ามี การขโมยข้อมูลเกิดขึ้นจริงหรือไม่ ถ้ามีคำถามที่ตามมาก็คือข้อมูลประเภทใดที่จัดว่าเป็นทรัพย์สิน ข้อมูลนั้นจะต้องเป็นข้อมูลลับหรือไม่ หากจำเลยเข้าไปในคอมพิวเตอร์เพื่อดูรายนามโทรศัพท์ของนายจ้างเก่า ซึ่งรายนามนั้นอาจจะมิได้อยู่ในสมุดรายนามโทรศัพท์ก็ได้ การกระทำเช่นนั้นถือว่าเป็นการขโมยหรือไม่ การที่จำเลยจะมีความผิดจริงเขาต้องรู้หรือไม่ว่าข้อมูลนั้นเป็นความลับและได้มีการปกปิดและป้องกันแล้ว การกระทำผิดเกิดขึ้นขณะที่ทำการขโมยหรือขณะที่นำข้อมูลนั้นมาใช้ในภายหลัง การกระทำ

¹ ข้อมูลดังกล่าวแปลมาจาก Criminal Law and The Internet ใน <http://www.cla.org/ruhbook/chp11.htm>, (3 November 2000).

โดที่ถือเป็นการใช้ข้อมูลแล้ว เห็นได้ว่า การใช้แนวคิดทางกฎหมายเกี่ยวกับการกระทำผิดกฎหมาย ยกยอก ข้อโกง บุกรุก และลักทรัพย์ ตามกฎหมายเดิมนั้นไม่เหมาะสมกับเทคโนโลยีสมัยใหม่²

สภาพปัญหาพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย

ในปี พ.ศ.2542 อัตราความแพร่หลายของผู้ใช้อินเตอร์เน็ตในประเทศไทย ประมาณ 600,000 คน คิดเป็นสัดส่วนต่อประชากรทั้งประเทศอยู่ที่ร้อยละ 1 ซึ่งหากเป็นไปตาม คาดการณ์ของสถาบันวิจัยเพื่อการพัฒนาประเทศไทย (TDRI) จำนวนผู้ใช้อินเตอร์เน็ตในอีก 5 ปี ข้างหน้า จะขยายตัวเพิ่มขึ้นร้อยละ 30-40 นั่นเท่ากับว่าจำนวนผู้ใช้อินเตอร์เน็ตจะสูงถึง 2.78-3.21 ล้านคน หรือร้อยละ 4.29-4.94 ของประชากรทั้งประเทศ นอกจากนั้น แรงกดดันของการเปิดตลาด การค้าเสรี โดยเฉพาะแรงบีบของ WTO มีส่วนผลักดันให้พาณิชย์อิเล็กทรอนิกส์ไทยเติบโตขึ้น ทั้ง ในด้านตลาดระดับธุรกิจกับธุรกิจ (B to B) หรือระดับธุรกิจกับผู้บริโภค (B to C) จากการสำรวจ ของ TDRI พบว่าอุตสาหกรรมของไทยที่ดำเนินพาณิชย์อิเล็กทรอนิกส์สูงสุดคือ อุตสาหกรรม คอมพิวเตอร์ ในสัดส่วนร้อยละ 17 รองลงมาได้แก่ ธุรกิจบริการร้อยละ 16 การท่องเที่ยวและโรงแรมร้อยละ 12 การพาณิชย์อิเล็กทรอนิกส์ของแต่ละธุรกิจดังกล่าวนำไปใช้เพื่อวัตถุประสงค์ในการ โฆษณาสินค้าและบริการ แต่ยังไม่เปิดให้สั่งซื้อสินค้า มีสัดส่วนสูงถึง 53.3 สำหรับบริษัทที่เปิดรับ การสั่งซื้อสินค้าและบริการทางอินเทอร์เน็ตแล้ว (Web Order Taking) มีสัดส่วน 31.9 และมีเพียง 14.8 เท่านั้นที่เปิดรับชำระเงินผ่านทางอินเทอร์เน็ต (Web Payment) ซึ่งสะท้อนให้เห็นว่าพาณิชย์ อิเล็กทรอนิกส์ของไทยยังอยู่ในขั้นเริ่มต้นเท่านั้น³

แม้ว่าประเทศไทยจะเริ่มมีการให้บริการอินเทอร์เน็ตในเชิงพาณิชย์มาตั้งแต่ปี พ.ศ.2537 แต่สำหรับการพาณิชย์อิเล็กทรอนิกส์แล้ว นับว่ายังไม่มีการพัฒนาเท่าที่ควร ดังนั้น เพื่อ เป็นการส่งเสริมการพาณิชย์อิเล็กทรอนิกส์ของไทยให้มีความแพร่หลาย ทางกรจึงได้สนับสนุนให้ กระทรวงพาณิชย์ดำเนินโครงการพาณิชย์อิเล็กทรอนิกส์นำร่องขึ้นเมื่อปี 2541 โดยได้รับความร่วมมือจากภาคเอกชน ทั้งนี้คาดว่าโครงการดังกล่าวจะสามารถสร้างความพร้อมให้กับภาค ธุรกิจและประชาชนให้มีความรู้ความเข้าใจเกี่ยวกับการพาณิชย์อิเล็กทรอนิกส์มากขึ้น โดยในระยะ

² Ibid.

³ กองบรรณาธิการ , "อี-คอมเมิร์ซ ทางเลือกใหม่ของธุรกิจไทย," นิตยสารธุรกิจก้าวหน้า , (มีนาคม 2543) : หน้า 34-38.

แรกโครงการดังกล่าวจะเป็นโครงการพาณิชย์อิเล็กทรอนิกส์นำร่องเพื่อสนับสนุนการส่งออกเท่านั้น ซึ่งมีทั้งการดำเนินงานในรูปแบบการโฆษณาและเผยแพร่ประชาสัมพันธ์บริษัท รวมถึงสินค้าและบริการของผู้ประกอบการไทยให้แพร่กระจายไปทั่วโลก การซื้อขายสินค้าในระดับธุรกิจกับธุรกิจ และการซื้อขายสินค้าในระดับธุรกิจกับผู้บริโภค ทั้งนี้ ได้เปิดโอกาสให้ผู้ประกอบการขนาดกลาง และขนาดย่อม หรือที่เรียกว่า SMEs ได้เข้ามามีส่วนร่วมในการประกอบธุรกิจและขยายตลาดไปยังต่างประเทศ โดยใช้งบประมาณทั้งสิ้น 5.7 ล้านบาท

กระทรวงพาณิชย์ได้เร่งดำเนินการต่างๆ ที่เอื้อต่อกิจกรรมพาณิชย์อิเล็กทรอนิกส์เพื่อเพิ่มความสามารถของผู้ประกอบการไทยในเวทีการแข่งขันโลกรวมถึงการลดและหลีกเลี่ยงภาวะเบียดเบียนที่จะปิดกั้นการพัฒนาพร้อมทั้งทำหน้าที่ในการควบคุมการแข่งขันให้เป็นธรรมและคุ้มครองผู้บริโภคให้มากที่สุด และเร่งสร้างความเชื่อมั่นระหว่างผู้ประกอบการและผู้บริโภค และส่งเสริมให้มีการทำธุรกิจเพิ่มมากขึ้น ซึ่งที่ผ่านมากรมเศรษฐกิจการพาณิชย์ กระทรวงพาณิชย์ได้จัดโครงการพาณิชย์อิเล็กทรอนิกส์เพื่อสนับสนุนการส่งออก โดยจัดทำ Homepage ในลักษณะของ Cyber Mall ซึ่งผู้ส่งออกจะได้ประโยชน์จากการโฆษณาสินค้าและบริการผ่านอินเทอร์เน็ต โดยใช้เว็บไซต์ของกระทรวงพาณิชย์ www.thaiecommerce.net เป็นประตูที่จะเชื่อมโยง Homepage ของบริษัทธุรกิจส่งออกที่จะเผยแพร่ข้อมูลต่างๆ ไปสู่ผู้ซื้อทั่วโลก สำหรับธุรกิจส่งออกที่ประสงค์จะเข้าร่วมโครงการ มีหลักเกณฑ์เบื้องต้นคือ เป็นบริษัทนิติบุคคล ประกอบการค้าสินค้าหรือบริการ โดยถูกต้องตามกฎหมาย ไม่ประกอบธุรกิจผิดศีลธรรม สินค้าหรือบริการมีคุณภาพมาตรฐานเป็นที่ยอมรับได้ เช่น มี Brand Name , ISO , Barcode รับรอง หรืออยู่ในบัญชีรายชื่อผู้ส่งออกของกรมส่งเสริมการส่งออก ตลาดเป้าหมายในระยะเริ่มต้นจะเน้นใน 6 แห่งคือ U.S.A. , Japan , Europe , Asia , Australia , Hongkong โดยสินค้าเป้าหมายคือ อัญมณีและเครื่องประดับ อาหาร สิ่งทอ เสื้อผ้าสำเร็จรูป เครื่องหนัง ของเล่น เฟอร์นิเจอร์ ส่วนบริการเป้าหมาย คือ การท่องเที่ยว โรงแรม ร้านอาหาร บริการรถเช่า การจองตั๋วเครื่องบิน

ปัญหาสำคัญที่เกี่ยวข้องกับการทำพาณิชย์อิเล็กทรอนิกส์มีมากมายหลายประการ ทั้งปัญหาที่เป็นปัญหาเฉพาะของประเทศไทย เช่น ความพร้อมเรื่องโครงสร้างพื้นฐานทางด้านสารสนเทศ (Information Infrastructure) และปัญหาทั่วไปที่ทุกประเทศจะต้องพบ เช่น

ปัญหาการคุ้มครองผู้บริโภค การคุ้มครองข้อมูล ภาษีอากร และปัญหาอื่น⁴ สำหรับปัญหาสำคัญของไทยและนานาประเทศที่นับว่าร้ายแรงมากในปัจจุบัน มีดังนี้

1. ด้านความปลอดภัย (Security) โดยเฉพาะความปลอดภัยของข้อมูล นับเป็นสิ่งสำคัญที่มีผลต่อการพัฒนาระบบพาณิชย์อิเล็กทรอนิกส์ เนื่องจากพาณิชย์อิเล็กทรอนิกส์เป็นการค้าบนเครือข่าย ทำให้โอกาสที่จะถูกโจรกรรมข้อมูลโดยนักเจาะระบบคอมพิวเตอร์ที่เรียกว่า Hacker เข้าไปล้วงข้อมูลที่เป็นความลับ เพื่อก่อกวนหรือใช้ประโยชน์ในทางมิชอบ โดยเฉพาะการซื้อขายสินค้าผ่านอินเทอร์เน็ตในรูปของบัตรเครดิต ทำให้เกิดปัญหาการลักลอบขโมยข้อมูลจากบัตรเครดิตค่อนข้างมาก จึงได้มีการคิดค้นและพัฒนาเทคโนโลยีระบบรักษาความปลอดภัยของข้อมูล ที่เรียกว่า "Cryptography" ประกอบไปด้วยการเข้ารหัสและการถอดรหัส (Encryption & Decryption) ซึ่งเป็นวิธีการเก็บรักษาความลับของข้อมูล โดยผู้ที่รู้รหัสเท่านั้นจะสามารถอ่านข้อมูลนั้นได้ มีการนำเอาเทคโนโลยีระบบความปลอดภัยของข้อมูลมาใช้ในการระงับการชำระเงิน เช่น ระบบ SET เพื่อเป็นการป้องกันอาชญากรรมทางคอมพิวเตอร์ที่อาจจะมีการลักลอบใช้ข้อมูลดังกล่าว

2. ความเชื่อมั่น (Trust) ปัจจุบันผู้ที่เกี่ยวข้องกับพาณิชย์อิเล็กทรอนิกส์ยังขาดความไว้วางใจในระบบดังกล่าวอยู่มาก ทั้งนี้ เนื่องจากขาดความมั่นใจในคู่สัญญาว่ามีตัวตนอยู่จริงหรือไม่ ดังนั้น เพื่อเป็นการสร้างความมั่นใจให้กับผู้ผลิตและผู้บริโภค จึงมีการจัดตั้งหน่วยงานที่เรียกว่า "องค์กรรับรองความถูกต้อง" (Certification Authority : CA) เพื่อทำหน้าที่ให้การรับรองว่าคู่สัญญาที่ประกอบธุรกรรมพาณิชย์อิเล็กทรอนิกส์เป็นบุคคลตามที่ได้กล่าวอ้างจริง

3. ด้านโครงสร้างพื้นฐาน (Infrastructure) การขาดความพร้อมทางด้านโครงสร้างพื้นฐาน โดยเฉพาะด้านโทรคมนาคม ไม่ว่าจะเป็นความไม่เพียงพอของเครือข่ายการสื่อสาร การกำหนดอัตราค่าบริการที่อยู่ในระดับสูง ล้วนเป็นอุปสรรคสำคัญต่อการพัฒนาการพาณิชย์อิเล็กทรอนิกส์ให้มีความแพร่หลาย ทั้งนี้ เนื่องจากการดำเนินธุรกรรมดังกล่าวจำเป็นต้องอาศัย

⁴ สมเกียรติ ตั้งกิจวานิชย์, "การพาณิชย์อิเล็กทรอนิกส์ (ส่วนหนึ่งของโครงการแผนแม่บทกระทรวงพาณิชย์ พ.ศ.2540-2549)," กรุงเทพมหานคร : สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, 2541.

เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารต่างๆ ดังนั้น ความพร้อมของโครงสร้างพื้นฐาน จึงเป็นปัจจัยสำคัญต่อการพาณิชย์อิเล็กทรอนิกส์

4. ด้านกฎหมาย (Law) กฎหมายเป็นปัจจัยสำคัญอย่างหนึ่งที่มีผลต่อการคุ้มครองและสร้างความมั่นใจให้กับผู้ที่เกี่ยวข้องกับการพาณิชย์อิเล็กทรอนิกส์ ประเทศไทยจึงจำเป็นต้องมีกฎหมายที่เหมาะสมกับสภาพแวดล้อมภายในประเทศและสอดคล้องกับมาตรฐานสากล อันจะเป็นการกระตุ้นการพาณิชย์อิเล็กทรอนิกส์ให้พัฒนาได้ในระดับหนึ่ง ซึ่งปัจจุบันการดำเนินการดังกล่าวอยู่ภายใต้ความรับผิดชอบของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) กับกระทรวงยุติธรรม

กรณีการทำความผิดเกี่ยวกับพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย

1. การสั่งซื้อของจากการประมูล ebay.com ซึ่งเป็นเว็บไซต์ที่เปิดโอกาสให้บุคคลทั่วไปประกาศขายสินค้าโดยการประมูลบนเว็บ กรณีปัญหาคือมีบุคคลในประเทศไทยได้เข้าไปในเว็บไซต์ดังกล่าว และพบว่ามีการซื้อขายเครื่องโทรทัศน์ใช้แล้วขนาดจอภาพ 50 นิ้ว เกิดความสนใจจึงได้เข้าร่วมประมูล ต่อมาชายชาวอเมริกันคนดังกล่าวได้ส่งอีเมลล์ว่าคุณเป็นผู้ชนะการประมูล ขอให้ส่งเงินเข้าบัญชีเป็นจำนวน 266,000 บาท หลังจากนั้นบุคคลในประเทศไทยได้รับกล่องพัสดุขนาดใหญ่จากบริษัทขนส่ง Fedex ที่บนกล่องเขียนว่าเป็น "อิเล็กทรอนิกส์" แต่เมื่อเปิดกล่องดูพบว่าเป็นเพียงตุ๊กตา และเครื่องแก้วที่แตกแล้ว⁵

2. เว็บไซต์ส่งเสริมการขายสินค้าของไทย 3 แห่งถูกใส่ร้าย โดยถูกกลุ่มผู้ไม่หวังดีปลอมอีเมลล์ของเว็บดังกล่าว แล้วส่งไปยังผู้ใช้อินเทอร์เน็ตทั่วโลกประมาณ 4 ล้านฉบับ ลักษณะ Spam Mail และได้ใส่ร้ายเว็บดังกล่าวว่า "เป็นเว็บไซต์ที่ฉ้อโกง ซึ่งจะนำชื่อและหมายเลขบัตรเครดิตของผู้ที่สนใจเข้ามาซื้อของไปใช้ในทางที่ผิด ขอให้อย่าเข้าเว็บไซต์ของไทยทั้งสามดังกล่าว" ผลร้ายที่เกิดขึ้นนอกจากจะทำให้คนทั้งโลกไม่เข้าชมเว็บดังกล่าวแล้ว ยังทำให้องค์กรต่อต้าน Spam Mail สั่งให้เว็บไซต์ยุติ และปิดการให้บริการเว็บไซต์ไทยทั้งสามอีกด้วย⁶

⁵ พันตำรวจเอก ญาณพล ยั่งยืน , "กรณีตัวอย่างอาชญากรรมทางคอมพิวเตอร์," กรุงเทพมหานคร : ศูนย์ข้อมูลข้อสนเทศ สำนักงานตำรวจแห่งชาติ , 2544.

⁶ เรื่องเดียวกัน.

3. การจัดทำเว็บไซต์ขายสินค้าแล้วไม่ส่งสินค้าให้ หรือทำหลอกไว้เพื่อเพียงต้องการหมายเลขและข้อมูลบัตรเครดิตไปใช้ในกรณีอื่นๆ ถือเป็นกรณข้อโกง⁷

4. การสั่งซื้อสินค้าโดยใช้หมายเลขบัตรเครดิตของผู้อื่น หรือเลขที่บัตรที่ไม่มีตัวตนจริงแล้วให้ไปส่งที่บ้านบุคคลอื่น ซึ่งคนร้ายสามารถตรวจสอบทางอินเทอร์เน็ตได้ว่าของจะส่งถึงวันใด เวลาใด คนร้ายจะไปเฝ้ารออยู่หน้าบ้าน แล้วแสดงตัวรับสินค้าไปทำให้ยากแก่การสืบสวนติดตาม⁸

5. ความผิดที่เกิดขึ้นโดย Hacker วัยรุ่นชื่อ Raphael Gray อายุ 18 ปี ได้บุกกรุกเข้าไปยังเว็บไซต์ที่ให้บริการ E-commerce ต่างๆ จนสามารถขโมยหมายเลขบัตรเครดิตมาได้เป็นจำนวนกว่า 26,000 หมายเลข ซึ่งหนึ่งในจำนวนนั้นมีหมายเลขบัตรเครดิตของนายบิลล์เกตส์ ประธานบริษัท Microsoft รวมอยู่ด้วย เจ้าหน้าที่ FBI ออกมาให้ข้อมูลเกี่ยวกับการจับกุมในครั้งนี้อย่างไรว่าได้จับกุม Raphael Gray และเพื่อนผู้สมคบคิดในการขโมยบัตรเครดิตจำนวนกว่า 26,000 หมายเลข จากเว็บไซต์ E-commerce เล็กๆ ทั่วโลกถึง 8 แห่ง เป็นเว็บไซต์ที่อยู่ในประเทศสหรัฐอเมริกา แคนาดา ไทย ญี่ปุ่น และอังกฤษ โดยผู้กระทำผิดอาศัยช่องโหว่ในโปรแกรมของ Microsoft เจาะเข้าไปยังฐานข้อมูลดังกล่าว Hacker เริ่มกระทำผิดครั้งแรกในเดือนมกราคม 2544 ที่เว็บไซต์ซึ่งเป็นของ ISP (Internet Service Provider) รายหนึ่งในประเทศไทย นั่นก็คือ www.shoppingthailand.com และในคราวนั้นเขาได้หมายเลขบัตรเครดิตไปกว่า 1,000 หมายเลข และนำหมายเลขบัตรเครดิตพร้อมชื่อเจ้าของบัตรไปโพสต์ไว้บนเว็บไซต์ส่วนตัวที่ www.xoom.com ต่อมาอีกไม่นานเขาและเพื่อนได้เข้าไปขโมยข้อมูลบัตรเครดิตจากเว็บไซต์ E-commerce รายอื่น ๆ เช่น promobility.net , itamedia.com , ascp.org , ntd.co.uk เป็นต้น โดยความเสียหายที่เกิดขึ้นในครั้งนี้อย่างไร คาดว่าจะมีมูลค่าสูงถึง 3 ล้านดอลลาร์สหรัฐ Raphael Gray ผู้ซึ่งตั้งฉายาให้ตัวเองว่า "Saint of E-commerce" หลังจากถูกจับกุมได้เปิดเผยถึงการกระทำดังกล่าวว่า เขาแค่ต้องการพิสูจน์ความแน่นอนของระบบรักษาความปลอดภัยบนเว็บไซต์เหล่านั้น โดยเขาเคยทำลงไปด้วยวิธีการที่ถูกต้องและสุจริตแต่กลับไม่ได้รับความสนใจ ดังนั้น เขาและเพื่อนจึง

⁷ เรื่องเดียวกัน.

⁸ เรื่องเดียวกัน.

ส่ง E-mail ที่มีข้อมูลหมายเลขบัตรเครดิตที่ไปขโมยมาได้ทั้งหมดไปยัง NBCi บริษัทในเครือของกลุ่มสถานีวิทยุโทรทัศน์ NBC ซึ่งใช้ชื่อผู้ส่งใน E-mail ว่า Curador⁹

จากกรณีของบริษัท ลีอกซเลย์ อินฟอร์เมชั่น จำกัด หรือลีโออินโฟ ได้ถูกแฮกเกอร์เจาะระบบเข้าไปโจรกรรมฐานข้อมูลบัตรเครดิตของลูกค้าที่เข้ามาซื้อสินค้าจากร้านค้าต่างๆ ที่อยู่ในไซเบอร์มอลล์ของบริษัทแล้วนำข้อมูลดังกล่าวไปโพสต์ไว้ในเว็บไซต์ www.xoom.com และไอซีดีดีพร้อมกับทิ้งข้อความเย้ยหยันถึงความบกพร่องของระบบไว้ด้วย ส่งผลให้บริษัทต้องเสียความเชื่อมั่นจากลูกค้าไปในระดับหนึ่ง และได้เป็นตัวกระตุ้นให้หน่วยงานที่เกี่ยวข้องมาทบทวนกระบวนการดำเนินงานครั้งใหญ่ ซึ่งเกี่ยวกับกรณีนี้นางธริษา วัฒนเกษ ผู้ช่วยผู้ว่าการธนาคารแห่งประเทศไทย(ธปท.) เปิดเผยว่าปัจจุบันความก้าวหน้าของเทคโนโลยีที่ทันสมัยได้เปลี่ยนแปลงอย่างรวดเร็วมีผลให้สถาบันการเงินต้องพัฒนาการประกอบธุรกิจและการให้บริการ เพื่อสอดคล้องกับภาวะการแข่งขันในตลาดโลก ระบบเครือข่ายอินเทอร์เน็ตเป็นเทคโนโลยีที่สถาบันการเงินนำมาใช้และให้บริการเพื่อเพิ่มช่องทางในการประกอบธุรกิจ และช่วยลดต้นทุน เนื่องจากเป็นเครือข่ายสื่อสารข้อมูลที่ยังได้ทั่วโลกสะดวกและค่าใช้จ่ายที่ไม่สูงมากนัก ซึ่งสถาบันการเงินมีแนวโน้มให้บริการมากขึ้น ดังนั้น เพื่อให้การกำกับและควบคุมการใช้บริการเครือข่ายอินเทอร์เน็ต ในการประกอบธุรกิจของธนาคารพาณิชย์ บริษัทเงินทุน และบริษัทเครดิตฟองซิเอร์ ธนาคารแห่งประเทศไทยและกระทรวงการคลังจึงได้ออกประกาศ เรื่องการใช้บริการเครือข่ายอินเทอร์เน็ตในการประกอบธุรกิจ ในการให้อำนาจธนาคารแห่งประเทศไทยพิจารณาอนุญาตในกรณีที่สถาบันการเงินเหล่านี้จะให้บริการผ่านอินเทอร์เน็ต โดยสถาบันการเงินใดๆ ใน 3 ประเภท สามารถใช้บริการผ่านเครือข่ายอินเทอร์เน็ตในการเผยแพร่ข้อมูลข่าวสารของกิจการในลักษณะการโฆษณา หรือเผยแพร่ธุรกิจที่ให้บริการทั้งเป็นการทั่วไปหรือให้แก่ลูกค้ารายใด ได้โดยไม่ต้องขออนุญาตจากธนาคารแห่งประเทศไทย แต่ในการให้บริการผ่านอินเทอร์เน็ต ในการทำธุรกรรมหรือนิติกรรมใดๆ รวมทั้งโอนเงินหรือรับโอนเงินหรือการปฏิบัติการอื่นที่เกี่ยวกับธุรกรรมหรือนิติกรรมนั้น สถาบันการเงินจะต้องได้รับอนุญาตจากธนาคารแห่งประเทศไทย โดยสถาบันการเงินต้องยื่นคำขออนุญาตตามที่ธนาคารแห่งประเทศไทยกำหนดมาเพื่อขอพิจารณาก่อน "ในกรณีที่สถาบันการเงินใด จะให้บริการในการทำธุรกรรมผ่านอินเทอร์เน็ตต้องมาขออนุญาตจากธนาคารแห่งประเทศไทยก่อน ซึ่งธนาคารแห่งประเทศไทยจะพิจารณาระบบการรักษาความปลอดภัยของข้อมูลและดูว่าธนาคารมีแผนรองรับเหตุการณ์

⁹ กองบรรณาธิการ, "Hot News," *Internet Magazine* ปีที่ 5 ฉบับที่ 3 (45) (เดือนมีนาคม 2543) , หน้า 25-26.

ถูกเงินอย่างไร มีการอบรมบุคลากรพร้อมหรือไม่ ระบบควบคุมภายในเป็นอย่างไร และโปรแกรมที่ใช้ได้มาตรฐานหรือไม่ หากธนาคารแห่งประเทศไทยพิจารณาเห็นว่าสถาบันการเงินที่ขอมาสามารถดูแลระบบข้อมูลให้มีความปลอดภัยได้ระดับหนึ่งก็อนุญาตให้ทำได้ โดยตอบกลับไปภายใน 60 วัน”¹⁰

ปัญหาทางกฎหมายของประเทศไทย

ตามประมวลกฎหมายอาญา มาตรา 2 บัญญัติว่า “บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการอันกฎหมายที่ใช้อยู่ในขณะกระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่ผู้กระทำความผิดนั้น ต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย” บทบัญญัติดังกล่าวนี้ถือเป็นหลักการใช้กฎหมายอาญา หรือที่เรียกว่าหลัก Nulla poena sine lege ซึ่งเป็นแนวความคิดในเรื่องให้มีการจำกัดขอบเขตอำนาจในการลงโทษ

จากหลักการใช้กฎหมายข้างต้น เห็นได้ว่าอาชญากรรมคอมพิวเตอร์ซึ่งรวมถึงการทุจริตต่อบัตรเครดิตบนอินเทอร์เน็ตนั้น เป็นความผิดรูปแบบใหม่ที่มืองค์ประกอบความผิดในส่วนของกรกระทำ คือ การเจาะระบบ (Hacking) และวัตถุประสงค์แห่งการกระทำ คือ ข้อมูลหมายเลขบัตรเครดิตหรือข้อมูลส่วนบุคคลของผู้อื่น องค์ประกอบของความผิดดังกล่าวแตกต่างไปจากอาชญากรรมรูปแบบเดิมอย่างมาก ซึ่งหากความผิดในลักษณะนี้เกิดขึ้นในประเทศไทยก็ไม่แน่ว่าผู้กระทำความผิดจะมีความผิดตามกฎหมายไทยหรือไม่ การบัญญัติกฎหมายในฐานะที่เป็นกระบวนการแก้ปัญหาของสังคมประการหนึ่งมักเป็นสิ่งที่เกิดขึ้นภายหลังการก่อตัวขึ้นของปัญหา โดยเฉพาะอย่างยิ่งปัญหาทางด้านเทคโนโลยีเป็นปัญหาที่ซับซ้อน ซึ่งส่วนใหญ่เป็นปัญหาทางด้านเทคนิค ปัจจุบันพบว่าสังคมของผู้ใช้อินเทอร์เน็ตนั้นนับวันยิ่งทวีความรุนแรงมากขึ้น ในขณะที่กฎหมายที่เกี่ยวข้องและมีผลใช้บังคับกับปัญหาอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะนั้นยังไม่มี ดังนั้น เมื่อมีความผิดเกิดขึ้น พนักงานสอบสวนผู้รับผิดชอบคดีจะพยายามปรับข้อเท็จจริงให้เข้ากับฐานความผิดในประมวลกฎหมายอาญา และดำเนินคดีไปตามประมวลกฎหมายวิธีพิจารณาความอาญาเพียงเท่าที่มีอยู่ ซึ่งตามสภาพความเป็นจริงแล้วอาชญากรรมเหล่านี้มีลักษณะที่แตกต่างไปจากอาชญากรรมรูปแบบเดิมโดยสิ้นเชิง ปัญหาที่ตามมาคือกฎหมายเหล่านั้นเพียงพอหรือไม่ เพราะเป็น

¹⁰ หนังสือพิมพ์ผู้จัดการธุรกิจและการเงิน ปีที่ 10 ฉบับที่ 2862 (2860) วันศุกร์ที่ 11 กุมภาพันธ์ 2543 หน้า 17-19.

กฎหมายที่บัญญัติขึ้นในสมัยที่เทคโนโลยียังไม่มีความเจริญก้าวหน้าเทียบเท่าปัจจุบันนี้ การพยายามนำกฎหมายเท่าที่มีอยู่มาปรับใช้จึงอาจก่อให้เกิดปัญหาการบังคับใช้กฎหมายได้

1. ประมวลกฎหมายอาญา

ความผิดฐานลักทรัพย์

คำว่า “ทรัพย์” ตามประมวลกฎหมายอาญามาตรา 334¹¹ หมายถึงทรัพย์ที่มีเจ้าของ จึงต้องเป็นทรัพย์ที่เป็นทรัพย์สืบตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 138¹² คือ มีราคาและถือเอาได้ แต่ทรัพย์สืบลักกันได้จะหมายความถึงทรัพย์อันเป็นวัตถุที่มีรูปร่างตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137¹³ เท่านั้นหรืออย่างไร เพราะถ้าเป็นสิ่งที่ไม่มีรูปร่างก็ย่อมจะหยิบฉวยเอาไปไม่ได้ ถ้าทรัพย์ที่ถูกลักเป็นวัตถุที่มีรูปร่าง มีเจ้าของ ก็เป็นความผิดตามมาตรา 334 อย่างแน่นอน วัตถุที่มีรูปร่าง หมายความว่า สิ่งที่มีรูปร่างโดยตัวของมันเองหรือที่อาศัยสิ่งอื่นเป็นรูปร่าง เช่น น้ำในภาชนะ อากาศ หรือแก๊สที่บรรจุอยู่ในถังหรือในท่อที่ปล่อยแก๊สให้ไหลไปด้วย

“ทรัพย์” หมายความว่า กระแสไฟฟ้าด้วยหรือไม่ คำพิพากษาฎีกาที่ 877/2501 2501 ฎ.986 วินิจฉัยว่า “ข้อกฎหมายที่จำเลยที่ 1 ฎีกาขึ้นมาว่า ฯลฯ ตามประมวลกฎหมายแพ่งและพาณิชย์ วิเคราะห์ว่าทรัพย์ได้แก่วัตถุอันมีรูปร่าง แต่กระแสไฟฟ้าเป็นพลังงานมิใช่วัตถุที่มีรูปร่าง และไม่อาจหยิบฉวยเอาไปได้ ทั้งไม่อาจคิดราคาซื้อขายได้ จึงไม่เป็นทรัพย์ที่ลักกันได้ ปัญหาข้อนี้ศาลฎีกาโดยที่ประชุมใหญ่มีมติว่า การลักกระแสไฟฟ้าย่อมเป็นความผิดตามประมวลกฎหมายอาญา มาตรา 334 หรือ 335 แล้วแต่กรณี ฯลฯ” เป็นการหักล้างข้อโต้แย้งที่ว่ากระแสไฟฟ้าไม่ใช่

¹¹ ประมวลกฎหมายอาญา มาตรา 334 บัญญัติว่า “ผู้ใดเอาทรัพย์ของผู้อื่น หรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วยไปโดยทุจริตผู้นั้นกระทำความผิดฐานลักทรัพย์ ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินหกพันบาท”

¹² ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 138 บัญญัติว่า “ทรัพย์สืบ หมายความว่า รวบรวมทั้งทรัพย์และวัตถุไม่มีรูปร่างซึ่งอาจมีราคาและอาจถือเอาได้”

¹³ ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137 บัญญัติว่า “ทรัพย์ หมายความว่า วัตถุที่มีรูปร่าง”

วัตถุที่มีรูปร่างโดยตรง เป็นทำนองที่ศาลฎีกาถือว่ากระแสไฟฟ้าเป็นวัตถุที่มีรูปร่างตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137

ส่วนพลังงานอย่างอื่น ความร้อน ความเย็น แสง รวมทั้งรูปที่มองเห็นด้วยตา เสียง ที่ได้ยินด้วยหู ในตัวของมันเองไม่ใช่สิ่งที่จับต้องได้ จึงไม่เป็นทรัพย์สินที่จะลักได้ แต่ตัววัตถุ คือ สิ่งที่เป็นรูปหรือเกิดเสียง แก๊สที่ร้อนหรือเย็นอันเป็นวัตถุที่ให้ความร้อนความเย็นนั้น เป็นทรัพย์สินที่ถือเอาได้ เพราะฉะนั้นก็ลักได้แต่จะมีการเอาไปหรือเพียงแต่ใช้ทรัพย์สินของเขาหมดเปลืองสิ้นไป เป็นปัญหาที่จะพิจารณากันต่อไปอีกชั้นหนึ่ง¹⁴

"เอาไป" เป็นองค์ประกอบในส่วนของกรกระทำ หมายความว่า พาทรัพย์สินเคลื่อนที่ไปจากการครอบครองของผู้อื่น จึงต้องมีการกระทำเป็นสองประการ คือ แย่งการครอบครองประการหนึ่ง และพาเคลื่อนที่ไปอีกประการหนึ่ง เพียงแต่แย่งการครอบครองแต่ยังไม่ได้พาทรัพย์สินเคลื่อนที่ไป ก็ยังไม่เป็นการลักทรัพย์สินสำเร็จ เหตุนี้ทรัพย์สินที่ลักจึงต้องมีผู้ครอบครองอยู่ประการหนึ่ง ผู้กระทำเข้าครอบครองทรัพย์สินนั้นประการหนึ่ง การเข้าครอบครองนั้นเป็นการแย่งการครอบครองซึ่งผู้ครอบครองทรัพย์สินอยู่เดิมมิได้อนุญาตประการหนึ่ง แล้วได้พาทรัพย์สินเคลื่อนที่ไปอีกประการหนึ่ง จึงจะถือว่ามีการเอาทรัพย์สินไปสำเร็จบริบูรณ์¹⁵

ขณะที่เอาทรัพย์สินไปต้องมีผู้อื่นครอบครองทรัพย์สินนั้นอยู่ มิใช่ทรัพย์สินมีเจ้าของแต่ไม่อยู่ในความครอบครองของผู้ใด เช่น ทรัพย์สินสูญหาย การครอบครองนั้นไม่จำเป็นต้องมีการจับต้องตัวทรัพย์สินยึดถือไว้ในมือเสมอไป การยึดถือในการครอบครองหมายความว่าความถึงการหวงกันตามควรแก่พฤติการณ์และสภาพของทรัพย์สิน การเข้าครอบครองในการลักทรัพย์สินต้องเป็นการแย่งการครอบครอง คือ เข้าถือเอาโดยผู้ครอบครองเดิมไม่อนุญาต

ตามประมวลกฎหมายอาญา มาตรา 334 มุ่งหมายถึงตัวทรัพย์สินซึ่งเป็นวัตถุที่มีรูปร่าง แต่ข้อมูลทางคอมพิวเตอร์มิใช่วัตถุที่มีรูปร่างและอาจหยิบถือเอาได้ นอกจากนี้ องค์ประกอบในส่วนของกร "เอาไป" คือ พาทรัพย์สินเคลื่อนที่ไปจากความครอบครองของผู้อื่นนั้น ทรัพย์สินที่ไม่มี

¹⁴ จิตติ ดิงศภักดิ์, กฎหมายอาญา ภาค 2 ตอน 2 และภาค 3, พิมพ์ครั้งที่ 3

(กรุงเทพมหานคร : เนติบัณฑิตยสภา, 2532), หน้า 2479.

¹⁵ เรื่องเดียวกัน, หน้า 2495-2496.

รูปร่างซึ่งหมายถึงสิ่งที่ไม่มรูปร่างจริงๆ อันเป็นสิ่งสมมติ เช่น สิทธิเรียกร้อง โดยเฉพาะชุดคำสั่งหรือข้อมูล โดยสภาพเป็นสิ่งที่จับต้องไม่ได้ จึงไม่เป็นสิ่งที่ล็อกกันได้ เพราะถ้าเป็นสิ่งที่ไม่มีรูปร่างก็จะไม่สามารถหยิบฉวยเอาไปได้จึงไม่มีการพาเคลื่อนที่ไป ดังนั้น ข้อมูลหมายเลขบัตรเครดิตที่เก็บไว้ในระบบคอมพิวเตอร์จึงไม่สามารถที่จะล็อกได้¹⁶

จากบทบัญญัติดังกล่าวทำให้เห็นถึงปัญหาในการบังคับใช้กฎหมายที่ยึดติดกับอาชญากรรมรูปแบบเดิมที่วัตถุแห่งการกระทำความผิดส่วนใหญ่ต้องเป็นทรัพย์สินที่จับต้องได้ (Tangible Object) เช่น รถยนต์ ของมีค่าหรือเงินทอง เป็นต้น แต่ในปัจจุบันอาชญากรรมคอมพิวเตอร์มีวัตถุแห่งการกระทำความผิดส่วนใหญ่เป็นข้อมูลข่าวสารในรูปของคลื่นแม่เหล็กไฟฟ้า (Electronic Impulse) ซึ่งเป็นสิ่งที่ไม่สามารถจับต้องได้ (Intangible Object) ผู้กระทำความผิดสามารถทำซ้ำข้อมูลสารสนเทศไปโดยไม่ต้องเคลื่อนย้ายหรือพรากเอาทรัพย์สินของผู้อื่นไป

ความผิดฐานบุกรุก

องค์ประกอบความผิดฐานบุกรุกตามประมวลกฎหมายอาญา มาตรา 362¹⁷ มีวัตถุแห่งการกระทำ คือ อสังหาริมทรัพย์ซึ่งรวมถึงสิทธิเกี่ยวกับกรรมสิทธิ์ในที่ดินด้วย ต้องเป็นทรัพย์สินที่มีการครอบครองได้ เพราะผู้กระทำต้องมีเจตนาพิเศษที่จะเข้าครอบครองหรือรบกวนการครอบครอง และต้องเป็นทรัพย์สินที่ผู้กระทำเข้าไปได้ จึงต้องเป็นทรัพย์สินชนิดที่มีรูปร่าง¹⁸

“เข้าไป” หมายถึง ตัวผู้กระทำได้ล่วงล้ำเข้าไปในอสังหาริมทรัพย์ จะเป็นทางพื้นดิน ใต้ดิน หรือทางอากาศก็ต้องถือเป็นการเข้าไป แม้การเข้าไปจะเป็นเพียงส่วนใดส่วนหนึ่งของ

¹⁶ ภาณุ รังสีสหัส, “การกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์,” (วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย . 2533) , หน้า 61-64.

¹⁷ ประมวลกฎหมายอาญา มาตรา 362 บัญญัติว่า “ผู้ใดเข้าไปในอสังหาริมทรัพย์ของผู้อื่นเพื่อถือการครอบครองอสังหาริมทรัพย์นั้นทั้งหมดหรือแต่บางส่วน หรือเข้าไปกระทำการใดๆ อันเป็นการรบกวนการครอบครองอสังหาริมทรัพย์ของเขาโดยปกติสุข ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองพันบาท หรือทั้งจำทั้งปรับ”

¹⁸ จิตติ ดิงศภัทย์ , กฎหมายอาญา ภาค 2 ตอน 2 และภาค 3 , หน้า 3009.

ร่างกาย เช่น มือ เท้า หรือปลายนิ้วลวงล้ำเข้าไป ก็เป็นบุกรุกได้ ไม่ต้องเข้าไปทั้งตัวหรือส่วนใหญ่ของร่างกาย¹⁹

ปัญหาการบังคับใช้กฎหมายตามมาตรา 341 นี้กับอาชญากรรมคอมพิวเตอร์เกิดขึ้นเนื่องจากองค์ประกอบความผิดของอาชญากรรมรูปแบบเดิมให้ความสำคัญต่อการกระทำผิดทางกายภาพ คือ ต้องมีการเข้าไปในแดนกรรมสิทธิ์ของบุคคลอื่นอย่างชัดเจน แต่อาชญากรรมทางคอมพิวเตอร์นั้นเป็นการกระทำความผิดรูปแบบใหม่ที่อาจไม่ต้องมีการกระทำทางกายภาพ เช่น การเข้าไปในระบบคอมพิวเตอร์ที่อยู่ในบ้านเรือนของผู้อื่นโดยไม่ได้รับอนุญาต (Unauthorized Access) ซึ่งผู้กระทำความผิดไม่จำเป็นต้องเข้าไปทางกายภาพแต่ประการใด แต่สามารถเข้าดู แก้ไข เปลี่ยนแปลง หรือทำซ้ำซึ่งข้อมูลสารสนเทศที่เก็บไว้ในคอมพิวเตอร์ที่ตั้งอยู่ในอาคารสำนักงานของผู้อื่นได้โดยที่ตัวของผู้กระทำความผิดไม่จำเป็นต้องเข้าไปในอาคารของผู้เสียหายนั้น ผู้กระทำความผิดเพียงแต่นั่งอยู่ในบ้านก็สามารถกระทำความผิดด้วยวิธีการที่แปลกใหม่และซับซ้อนนี้ได้ เช่น ด้วยวิธีการเจาะระบบ (Hacking) เป็นต้น²⁰

ความผิดฐานฉ้อโกง

การฉ้อโกงตามประมวลกฎหมายอาญา มาตรา 341²¹ มีองค์ประกอบในส่วนของการกระทำเริ่มต้นด้วย “หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ” การหลอกลวง คือ ทำให้ผู้อื่นหลงเชื่อผิดจากความจริง การแสดงข้อความเท็จไม่จำกัดว่าต้องแสดงด้วยวิธีใด จะกระทำด้วยวาจา เอกสาร กิริยา หรือวิธีการอื่นใดก็เป็นการแสดงข้อความเท็จได้ทั้งสิ้น เพียงแต่ให้ข้อ

¹⁹ เรื่องเดียวกัน , หน้า 3019.

²⁰ โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ, “ประเทศไทยกับการพัฒนากฎหมายเทคโนโลยีสารสนเทศ”, กรุงเทพมหานคร : สำนักงานเลขาธิการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, 2542.

²¹ ประมวลกฎหมายอาญา มาตรา 341 บัญญัติว่า “ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังวานั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สามทำ ถอน หรือทำลายเอกสารสิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ”

ความที่แสดงออกนั้นได้ทราบถึงผู้อื่น เป็นเหตุให้ผู้กระทำผิดได้ไปซึ่งทรัพย์สินจากผู้ถูกลอกหลวง หรือบุคคลที่สาม "ทรัพย์สิน" ตามมาตรานี้หมายความถึงทรัพย์สินที่เป็นวัตถุที่มีรูปร่างและวัตถุไม่มีรูปร่างซึ่งมีราคาและถือเอาได้ ไม่มีปัญหาว่าต้องเป็นวัตถุมีรูปร่างดังความผิดฐานลักทรัพย์ จะเป็นสังหาริมทรัพย์หรืออสังหาริมทรัพย์ รวมทั้งสิทธิที่เป็นทรัพย์สินก็ข้อโกงได้

การข้อโกงตามบทบัญญัติข้างต้น ผู้กระทำความผิดจะต้องมีการหลอกหลวงผู้อื่น คำว่า "ผู้อื่น" ย่อมหมายความถึงบุคคล (Person) แต่อาชญากรรมรูปแบบใหม่ที่เกิดขึ้นในปัจจุบัน การได้มาซึ่งหมายเลขบัตรเครดิตของผู้อื่นที่ถูกเก็บไว้ในระบบคอมพิวเตอร์นั้น ผู้กระทำผิดอาจกระทำโดยใช้เทคนิควิธีการต่างๆ เช่น การใช้รหัสผ่าน (Password) ของผู้อื่นโดยปราศจากอำนาจ ทั้งนี้เพื่อหลอก หลวงเครื่องคอมพิวเตอร์ให้เข้าใจว่าผู้กระทำผิดเป็นผู้มีสิทธิเข้าใช้เครื่อง รวมทั้งมีสิทธิสั่งการให้ระบบคอมพิวเตอร์แสดงข้อมูลต่างๆ ที่เก็บไว้ได้ การหลอกหลวงด้วยวิธีการดังกล่าว เป็นการหลอกหลวงเครื่องคอมพิวเตอร์ มิใช่หลอกหลวง "ผู้อื่น" ซึ่งหมายถึงบุคคลตามกฎหมายนี้

ปัญหาเรื่องเขตอำนาจศาล

ขอบเขตการใช้กฎหมายอาญานั้นมีหลักให้พิจารณาที่สำคัญ 4 ประการ²² คือ

1. หลักดินแดน (Territorial Principle)

สิ่งที่กำหนดการใช้กฎหมาย คือ สถานที่กระทำความผิด การกระทำความผิดเกิดขึ้นในรัฐโดยยอมตกอยู่ภายใต้กฎหมายของรัฐนั้นๆ ไม่ว่าจะผู้กระทำความผิดหรือผู้เสียหายจะมีสัญชาติใด ผู้กระทำความผิดจะถูกดำเนินคดีภายใต้กฎหมายของรัฐที่ความผิดเกิดเท่านั้น ดังนั้นหากประเทศไทยถือตามหลักนี้ กฎหมายไทยย่อมใช้กับผู้กระทำความผิดทั้งหลายไม่ว่าสัญชาติใดที่กระทำความผิดในราชอาณาจักรไทย แต่ไม่อาจบังคับกับผู้ไปกระทำความผิดนอกราชอาณาจักร

ประมวลกฎหมายอาญา มาตรา 4 บัญญัติเรื่องหลักดินแดน เป็นประการ

²² พงศ์ธร บุญอารีย์, "ปัญหาการก่อการร้ายระหว่างประเทศ," (วิทยานิพนธ์ปริญญา มหาบัณฑิต ภาควิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย . 2532) , หน้า 70.

สำคัญในการใช้กฎหมาย “ผู้ใดกระทำความผิดในราชอาณาจักร ต้องรับโทษตามกฎหมาย...” ด้วยเหตุที่กฎหมายอาญาบัญญัติขึ้นเพื่อให้เกิดความสงบสุขและความปลอดภัยในพื้นที่ จึงใช้บังคับกับการกระทำความผิดทุกประเภทในราชอาณาจักร

2. หลักบุคคล (Nationality Principle)

สิ่งที่กำหนดในการใช้กฎหมาย คือ สัญชาติของบุคคล “กฎหมายของรัฐใด ย่อมใช้บังคับและคุ้มครองคนของรัฐนั้นๆ ไม่ว่าจะอยู่ ณ ที่ใด” ซึ่งแบ่งออกได้ 2 ประเภท คือ

- 2.1 หลักบุคคล กฎหมายอาญาของรัฐใดย่อมใช้บังคับกับบุคคลที่ถือสัญชาติของรัฐนั้น ที่กระทำความผิดทั้งในและนอกอาณาเขตของรัฐนั้นๆ ไม่ว่าจะผู้เสียหายจะเป็นคนสัญชาติใดก็ตาม หลักนี้ถือสัญชาติของผู้กระทำความผิดเป็นสำคัญ
- 2.2 ผู้เสียหาย กฎหมายอาญาของรัฐใดย่อมใช้คุ้มครองบุคคลที่ถือสัญชาติของรัฐนั้น ที่ได้รับความเสียหายจากการกระทำความผิด ไม่ว่าจะในหรือนอกอาณาเขตของรัฐนั้น ไม่ว่าจะผู้กระทำความผิดจะเป็นบุคคลสัญชาติใดก็ตาม หลักนี้ถือสัญชาติของผู้เสียหายเป็นสำคัญ ผู้กระทำความผิดจะถูกดำเนินคดีโดยกฎหมายแห่งรัฐที่ผู้เสียหายมีสัญชาติ

เนื่องจากการถือหลักดินแดนโดยเคร่งครัด จะเป็นอุปสรรคหรือเป็นข้อจำกัดต่อการลงโทษการกระทำที่เกิดขึ้นนอกราชอาณาจักร กฎหมายอาญาจึงบัญญัติรับรองหลักบุคคลเข้าไว้ด้วย เพื่อเสริมหลักดินแดน ดังที่บัญญัติไว้ในมาตรา 8 “ผู้ใดกระทำความผิดนอกราชอาณาจักรและ (ก) ผู้กระทำความผิดนั้นเป็นคนไทย... (ข) ผู้กระทำความผิดเป็นคนต่างด้าวและรัฐบาลไทยหรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ”

3. หลักความมั่นคงแห่งรัฐ (Protective Principle)

เป็นหลักที่ทุกรัฐถือว่ารัฐจำเป็นที่จะต้องใช้อำนาจลงโทษผู้ที่กระทำการอันถือว่าเป็นการกระทบกระเทือนต่อความมั่นคงของรัฐ ไม่ว่าจะ เป็นในทางการหรือเศรษฐกิจ แม้ว่าการกระทำนั้นจะเกิดนอกราชอาณาจักรก็ตาม

หลักความมั่นคงได้บัญญัติไว้ในประมวลกฎหมายอาญา มาตรา 7(1) และ (2) เป็นความผิดเกี่ยวกับความมั่นคงทางเศรษฐกิจและการปลอมแปลง แม้ว่าการกระทำผิดจะเกิดนอกราชอาณาจักร หรือผู้กระทำผิดจะเป็นบุคคลสัญชาติใดก็ตาม ศาลไทยก็ยังมีอำนาจพิจารณาพิพากษาคดี

4. หลักอำนาจลงโทษสากล (Universal Principle)

ประเทศใดที่จับกุมตัวผู้กระทำผิดได้ เป็นผู้ที่มีอำนาจพิจารณาและลงโทษ ตามกฎหมายของประเทศนั้น โดยไม่ต้องคำนึงถึงสัญชาติของผู้กระทำผิด หรือของผู้เสียหาย และไม่ต้องคำนึงถึงสถานที่ที่ความผิดได้เกิดขึ้น อำนาจลงโทษสากลดังกล่าว ตามปกติมักจะมีกฎหมายหรือข้อตกลงที่เห็นร่วมกันในระหว่างรัฐ กำหนดลักษณะของความผิดบางประเภทที่กระทบกระเทือนต่อผลประโยชน์ร่วมกันของรัฐทั้งหลาย เช่น ความผิดฐานโจรสลัด การค้ายาเสพติด เป็นต้น

หลักอำนาจลงโทษสากลนั้น เนื่องจากยังไม่มีข้อตกลงร่วมกันอย่างชัดเจน จึงเป็นไปตามกฎหมายอาญาของแต่ละประเทศที่จะบัญญัติขึ้น ประเทศไทยได้บัญญัติลักษณะความผิดทางอาญาที่ใช้หลักนี้ไว้ในมาตรา 7 อันได้แก่ ความผิดฐานชิงทรัพย์หรือปล้นทรัพย์ในทะเลหลวง

สำหรับอาชญากรรมคอมพิวเตอร์นั้น สามารถเกิดขึ้นได้โดยไม่จำกัดเวลา และสถานที่โดยเฉพาะอย่างยิ่งอาชญากรรมบนเครือข่ายอินเทอร์เน็ต ซึ่งเป็นเครือข่ายที่ใช้กันทั่วโลกมีลักษณะไร้เขตแดนทางภูมิศาสตร์ (Cyberspace) บางครั้งไม่ปรากฏว่าการกระทำผิดเริ่มต้นที่ใด เมื่อมีผลร้ายเกิดขึ้นผู้เสียหายอาจอยู่ในประเทศต่างๆ อีกหลายประเทศ

ในขณะที่กฎหมายอาญาในข้อหาหลักๆ เช่น ปล้น ฆ่า ข่มขืน หรือที่เรียกว่าอาชญากรรมพื้นฐาน (Conventional Crime) มีลักษณะเป็นสากล กล่าวคือนานาอารยประเทศถือว่าการกระทำในลักษณะดังกล่าวเป็นความผิดที่มีโทษตามกฎหมาย แท้จริงแล้วกฎหมายเป็นเครื่องมือในการปกครองและเป็นสื่อที่แสดงให้เห็นถึงความมีเอกภาพเหนือดินแดนและประชาชนของรัฐ (Sovereignty of State) องค์ประกอบพื้นฐานที่สำคัญอันอาจถือเป็น "ธรรมชาติ" ของกฎหมายใดๆ ก็คือ อาณาเขตดินแดนในการปกครอง (Jurisdiction) โดยกฎหมายจะมีอำนาจเหนือประชาชนเฉพาะเพียงภายในอาณาเขตดินแดนของประเทศ กล่าวคืออำนาจตาม

กฎหมายถูกกำหนดโดยเขตพรมแดนทางภูมิศาสตร์ของรัฐนั้นๆ ธรรมชาติของกฎหมายที่มีผลใช้บังคับต่อประชาชนเฉพาะภายในอาณาเขตดินแดนนี้ ตรงกันข้ามกับธรรมชาติของอินเทอร์เน็ต ซึ่งปราศจากขีดจำกัด ไร้พรมแดนทางภูมิศาสตร์ นั่นก็คือ บุคคลไม่ว่าจะอยู่ ณ จุดใดของโลก สามารถที่จะเรียกใช้ข้อมูลข่าวสารที่อยู่ในอินเทอร์เน็ตได้โดยไม่ถูกสกัดกั้นด้วยพรมแดนอาณาเขตพื้นที่ ดังนั้น เมื่อบุคคลเข้าสู่อินเทอร์เน็ตหรือเครือข่ายข้อมูล www ก็เปรียบเสมือนอยู่ในดินแดนที่เกินกว่าขอบเขตอำนาจของกฎหมายแห่งดินแดนที่จะเข้าไปถึงได้ ที่เรียกว่า Cyberspace ความแตกต่างกันระหว่างธรรมชาติพื้นฐานของกฎหมายแผ่นดิน กับธรรมชาติพื้นฐานของอินเทอร์เน็ตนี้ทำให้เกิดช่องโหว่อย่างมากในการบังคับใช้กฎหมาย การสืบสวน การสอบสวน และการดำเนินกระบวนการยุติธรรม

2. ประมวลกฎหมายวิธีพิจารณาความอาญา

เทคโนโลยีสารสนเทศที่ก้าวหน้าเป็นอย่างมากได้ส่งผลให้อาชญากรรมคอมพิวเตอร์ก้าวหน้าตามไปด้วยเช่นกัน การก่ออาชญากรรมในลักษณะนี้สามารถกระทำได้ทั้งในและต่างประเทศ โดยผู้กระทำเพียงนั่งอยู่ที่หน้าจอภาพและแป้นพิมพ์ (Terminal) ก็สามารถกระทำความผิดได้ ในการประกอบอาชญากรรมคอมพิวเตอร์นั้น ผู้กระทำผิด ผู้เสียหาย รวมถึงระบบคอมพิวเตอร์ต่างๆ อาจเกี่ยวพันกับหลายประเทศ ซึ่งอาจเป็นอาณาเขตดินแดนที่มีกฎหมายแตกต่างกัน นอกจากจะทำให้การรวบรวมพยานหลักฐานเป็นไปด้วยความยากลำบากเนื่องจากอุปสรรคด้านการเดินทาง ภาษาที่แตกต่างกัน และความแตกต่างของความคิดพื้นฐานที่ว่า การกระทำความผิดที่เกิดขึ้นนั้น เป็นการกระทำที่ถูกกำหนดไว้ให้เป็นความผิดในประเทศต่างๆ ที่เกี่ยวข้องด้วยหรือไม่ นอกจากนี้ เทคโนโลยีสารสนเทศซึ่งมีความยุ่งยากซับซ้อน ทำให้การรวบรวมพยานหลักฐานเป็นเรื่องยากที่จะดำเนินการได้เหมือนอย่างคดีอาญาทั่วไป เพราะไม่ทราบว่ามีใครเป็นผู้กระทำและเริ่มกระทำ ณ ที่ใด การค้นหาพยานหลักฐานที่เกี่ยวข้องกับระบบคอมพิวเตอร์จึงควรอาศัยหน่วยงานพิเศษที่มีความเชี่ยวชาญโดยเฉพาะในการตรวจค้นและเก็บรักษาพยานหลักฐาน

การสืบสวนสอบสวนและรวบรวมพยานหลักฐาน

ปัญหาที่อาจเกิดขึ้นในส่วนนี้เนื่องจากยังไม่มี ความชัดเจนว่า ผู้รับผิดชอบการสืบสวนควรเป็นหน่วยงานใด ตำรวจท้องที่หรือหน่วยงานพิเศษ เมื่อมีข่าวอาชญากรรมคอมพิวเตอร์

เกิดขึ้นจะสามารถเข้าไปสืบสวนได้ทันทีหรือไม่ รวมทั้งการที่พนักงานสืบสวนยังไม่เข้าใจปัญหาที่เกิดขึ้นว่าตนมีอำนาจจับกุมผู้ก่ออาชญากรรมได้กว้างขวางเพียงใด จะถือว่าเป็นความผิดต่ออาญาแผ่นดิน หรือความผิดส่วนตัว

อาชญากรรมคอมพิวเตอร์เป็นการกระทำความผิดที่ใช้เวลานานมาก ดังนั้น การจะจับกุมผู้กระทำความผิดให้ได้ค่างานเขาจึงแทบจะเป็นไปไม่ได้ สำหรับการเก็บรวบรวมของกลางเพื่อเป็นหลักฐานประกอบคดีนั้น อาจมีเพียงสัญญาณคอมพิวเตอร์ที่มีลักษณะเป็นเพียงคลื่นกระแสไฟฟ้าและรหัสโปรแกรมที่ไม่สามารถจับต้องได้ทางกายภาพ จึงไม่สามารถตรวจค้น และยึดของกลางโดยวิธีการแบบดั้งเดิมได้ ซึ่งหากเจ้าหน้าที่ผู้ทำการสืบสวนจับกุมไม่มีความรู้ความเข้าใจเกี่ยวกับระบบการทำงานของคอมพิวเตอร์แล้ว อาจจะไม่ยึดเฉพาะตัวเครื่องคอมพิวเตอร์ไว้โดยที่ไม่ได้ให้ความสนใจที่จะเก็บข้อมูลที่ปรากฏอยู่บนจอหรือในหน่วยความจำของคอมพิวเตอร์ ซึ่งเป็นข้อมูลที่อยู่ในอินเทอร์เน็ต (URL) บนข้อมูลเกี่ยวกับการเชื่อมต่อกับคอมพิวเตอร์หลัก (Host) และเครือข่าย www ในช่วงเวลาที่ผู้ต้องหา กำลังกระทำความผิด และร่องรอยเส้นทางการส่งผ่านข้อมูลไว้เป็นหลักฐาน ทำให้ขาดความสมบูรณ์ในการรวบรวมหลักฐานประกอบคดี แม้ว่าข้อมูลเหล่านี้จะไม่สามารถจับต้องได้ทางกายภาพแต่เป็นหลักฐานที่มีความสำคัญและเป็นประโยชน์อย่างมากในการสอบสวนดำเนินคดีต่อไป ซึ่งหลักฐานข้อมูลดังกล่าว จะสูญหายไปโดยอาจไม่สามารถเรียกคืนมาได้

พนักงานสอบสวนต้องมีความรู้ความเข้าใจพื้นฐานในหลักการ วิธีการ ของการเชื่อมโยงของระบบเครือข่ายและวิธีการทำงานของอินเทอร์เน็ต หรือข่ายข้อมูล www และหลักการที่คอมพิวเตอร์ใช้ในการรับส่งผ่านข้อมูล พนักงานสอบสวนจำเป็นต้องมีความรู้เบื้องต้นในภาษาคอมพิวเตอร์ตลอดจนมีความเข้าใจถึงความหมายของข้อมูล มีความเข้าใจและทราบถึงวิธีการที่จะนำพยานหลักฐานที่ยึดได้จากที่เกิดเหตุไปใช้ให้เกิดประโยชน์ในทางคดี ทั้งต้องเข้าใจว่าพยานหลักฐานใดสามารถใช้พิสูจน์ความผิดของผู้ต้องหาได้ มีความสามารถในการตรวจ ค้น ยึด และเก็บรักษาหลักฐานต่างๆ ที่เกี่ยวข้องอย่างถูกต้องเพื่อป้องกันการสูญหายเสียหายของหลักฐานพยานนั้นๆ ซึ่งปัจจุบันพนักงานสอบสวนที่มีความรู้ความสามารถเช่นนี้ยังหาได้ไม่มากนัก จึงควรจัดตั้งหน่วยงานพิเศษเพื่อดำเนินคดีเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ดังเช่น หน่วยงานลับของสหรัฐอเมริกา (United State Secret Service หรือ U.S.S.S.) ซึ่งผ่านประสบการณ์ในการหาพยานหลักฐานและต่อสู้คดีในศาลหลายปี หน่วยงานดังกล่าวเมื่อต้องประสานงานกับประเทศที่ยังไม่มีหน่วยงานพิเศษจะประสบกับปัญหาในการติดต่อ ดังนั้น ความร่วมมือระหว่างประเทศจะ

เกิดขึ้นได้ หากมีหน่วยงานพิเศษเกิดขึ้นโดยได้รับการฝึกฝน เรียนรู้ มีความเชี่ยวชาญในการจัดการกับคดีพิเศษเหล่านี้

การรับฟังพยานหลักฐานในรูปของสื่ออิเล็กทรอนิกส์

กฎหมายลักษณะพยานหลักฐานของไทยบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความแพ่งและประมวลกฎหมายวิธีพิจารณาความอาญา โดยเฉพาะประมวลกฎหมายวิธีพิจารณาความแพ่งมีความสำคัญมากเนื่องจากกฎหมายกำหนดโย่งไปใช้ในคดีอาญาด้วยโดยอนุโลม นอกจากนี้ยังรวมไปใช้ในการพิจารณาคดีในศาลอื่นๆ เช่น ศาลเยาวชนและครอบครัว ศาลภาษีอากร และศาลแรงงาน เป็นต้น แต่สำหรับการพาณิชย์อิเล็กทรอนิกส์นั้นเป็นการทำการค้าผ่านเครือข่ายอินเทอร์เน็ตและคอมพิวเตอร์ ดังนั้น ข้อมูลที่เกี่ยวข้องกับการซื้อขาย หรือทำการค้ำนั้นย่อมอยู่ในลักษณะของข้อมูลคอมพิวเตอร์ จึงเป็นการเก็บรักษาข้อมูลในลักษณะของสื่ออิเล็กทรอนิกส์ จึงเกิดมีปัญหว่าข้อมูลที่ได้จากสื่ออิเล็กทรอนิกส์เหล่านี้สามารถนำมาใช้เป็นพยานหลักฐานในชั้นพิจารณาพิพากษาคดีของศาลได้หรือไม่เพียงใด

เกี่ยวกับข้อมูลในรูปของสื่ออิเล็กทรอนิกส์นี้ คณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติ (United Nation Commission on International Trade Law หรือ UNCITRAL) ซึ่งเป็นองค์กรหนึ่งของสหประชาชาติที่จัดตั้งขึ้นเพื่อส่งเสริมให้ประชาคมโลกมีกฎหมายการค้าระหว่างประเทศที่เป็นไปในแนวทางเดียวกัน (Harmonization and Unification of the Law of International Trade) ได้ตระหนักถึงความจำเป็นในการมีกฎหมายร่วมกันที่ใช้บังคับกับการติดต่อสื่อสารหรือทำการค้าโดยใช้ข้อมูลอิเล็กทรอนิกส์ จึงได้ประชุมเพื่อยกร่างกฎหมายแม่แบบเกี่ยวกับเรื่องนี้ ซึ่งประเทศต่างๆ สามารถนำไปใช้เป็นแนวทางในการออกกฎหมายภายในของตนให้สอดคล้องกันเพื่อส่งเสริมการค้าระหว่างประเทศ ในที่สุดการยกร่างกฎหมายแม่แบบก็บรรลุผลสำเร็จโดยปรากฏออกมาเป็น UNCITRAL Model Law Electronic Commerce และสมัชชาใหญ่แห่งสหประชาชาติได้มีมติรับกฎหมายแม่แบบดังกล่าวนี้ โดยเชื่อว่า จะช่วยให้ทุกประเทศใช้เป็นแนวทางตรากฎหมายของตนรองรับวิธีการรับส่งและเก็บรักษาข้อมูลโดยใช้วิธีการทางอิเล็กทรอนิกส์แทนรูปแบบที่ยังดำเนินการด้วยกระดาษ (Paper-based Method) สมัชชาใหญ่แห่งสหประชาชาติยังแนะนำให้ทุกประเทศให้ความสำคัญและคำนึงถึง

กฎหมายแม่แบบนี้อย่างที่สุดในการตราหรือแก้ไขกฎหมายของตนเพื่อจรรโลงให้กฎหมายการค้าระหว่างประเทศในเรื่องนี้มีความสอดคล้องกันและเป็นอันหนึ่งอันเดียวกัน²³ มีสาระสำคัญดังนี้

1. ลักษณะทั่วไปของกฎหมายแม่แบบของ UNCITRAL

โดยที่ระบบกฎหมายภายในของแต่ละประเทศมีความแตกต่างกัน กฎหมายแม่แบบของ UNCITRAL ว่าด้วยพาณิชย์อิเล็กทรอนิกส์จึงมุ่งหมายเพื่อกำหนดหลักเกณฑ์สำคัญๆ ที่ประเทศต่างๆ นำไปใช้เป็นแนวทางในการตราหรือแก้ไขกฎหมายของตนเพื่อรองรับวิธีการรับส่งหรือเก็บรักษาข้อมูลโดยใช้วิธีการทางอิเล็กทรอนิกส์ เพื่อให้กฎหมายของประชาคมโลกเป็นไปในทิศทางเดียวกัน จึงเป็นกฎหมายกำหนดกรอบเบื้องต้นเท่านั้น ซึ่งตั้งอยู่บนพื้นฐานของแนวทางที่ให้การยอมรับว่าการติดต่อหรือทำการค้าโดยใช้ข้อมูลอิเล็กทรอนิกส์มีผลทางกฎหมายเสมือนกับการติดต่อหรือทำการค้าโดยใช้เอกสารธรรมดา แนวทางดังกล่าวเรียกกันว่า Function-equivalent approach อย่างไรก็ตาม ข้อมูลอิเล็กทรอนิกส์ย่อมมีความเสี่ยงที่จะถูกเปลี่ยนแปลงแก้ไขง่ายกว่าเอกสารธรรมดา ในบางกรณีกฎหมายแม่แบบจึงให้การรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์เมื่อการสร้างหรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นได้มีการใช้วิธีการที่น่าเชื่อถือได้เท่านั้น ซึ่งเป็นวิธีการที่ป้องกันมิให้ข้อมูลนั้นถูกเปลี่ยนแปลงแก้ไขจากเดิม

ใน Article 1 ได้บัญญัติว่ากฎหมายนี้ใช้บังคับกับข้อมูลชนิดใดๆ ที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ซึ่งใช้ในกิจกรรมใช้เชิงพาณิชย์เท่านั้น และได้กำหนดคำว่าข้อมูลอิเล็กทรอนิกส์ (Data Message) ว่าหมายถึง "ข้อมูลที่สร้าง ส่ง รับ หรือเก็บรักษาโดยวิธีการทางอิเล็กทรอนิกส์ วิธีการทางแสง หรือวิธีการทำนองเดียวกัน รวมถึงวิธีการแลกเปลี่ยนข้อมูลระหว่างคอมพิวเตอร์ด้วยกันโดยใช้มาตรฐานที่คู่กรณีตกลงกันไว้ล่วงหน้า (EDI) การใช้ไปรษณีย์อิเล็กทรอนิกส์ โทรเลข เทล็กซ์ และ Telecopy"

2. บทบัญญัติทั่วไปที่รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์

ใน Article 5 : Legal recognition of data messages บัญญัติว่า "ข้อมูลจะไม่

²³ ดร. พิณัย ณ นคร , "กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์" บทบัญญัติฯ , เล่มที่ 56 ตอน 2 (มิถุนายน 2543) : หน้า 4.

ถูกปฏิเสธผลทางกฎหมาย หรือปฏิเสธความสมบูรณ์หรือการมีผลบังคับทางกฎหมายเพียงเพราะเหตุที่ว่าเป็นข้อมูลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์" บทบัญญัตินี้เป็นหัวใจของกฎหมายฉบับนี้

3. หลักเกณฑ์เกี่ยวกับต้นฉบับ

บางกรณีกฎหมายกำหนดให้ต้องแสดงหรือเก็บรักษาเอกสารต้นฉบับ ผู้ที่ใช้ข้อมูลอิเล็กทรอนิกส์อาจประสงค์จะแสดงหรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์แทนการนำเอกสารมาแสดงหรือแทนการเก็บรักษาเอกสาร แต่ข้อมูลอิเล็กทรอนิกส์ไม่มีคุณสมบัติของความเป็นต้นฉบับ ในความหมายที่เข้ากับเอกสารทั่วไป เพราะผู้ที่รับข้อมูลอิเล็กทรอนิกส์ส่วนแล้วแต่รับสำเนาของสื่อที่สร้างขึ้นทั้งสิ้น กฎหมายแม่แบบของ UNCITRAL จึงมีบทบัญญัติที่ว่า หากมีการแสดงหรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์โดยวิธีการที่น่าเชื่อถือได้ซึ่งสามารถรักษาความถูกต้องของข้อมูลอิเล็กทรอนิกส์ตั้งแต่ที่แรกสร้างข้อมูลนั้นขึ้นเป็นข้อมูลรูปแบบสุดท้าย ก็ให้ถือว่าเป็นการแสดงหรือเก็บรักษาเอกสารต้นฉบับตามกฎหมายนั้นแล้ว การรักษาความถูกต้องของข้อมูลอิเล็กทรอนิกส์ ต้องพิจารณาว่าข้อมูลอิเล็กทรอนิกส์ยังอยู่ในสภาพที่สมบูรณ์โดยปราศจากการเปลี่ยนแปลงของข้อมูลอิเล็กทรอนิกส์เป็นวิธีการที่น่าเชื่อถือได้หรือไม่ก็เป็นเรื่องที่ต้องพิจารณาจากพฤติการณ์ที่เกี่ยวข้องทั้งปวง นอกจากนี้ หากเป็นกรณีที่กฎหมายกำหนดให้แสดงเอกสารต้นฉบับ ถ้าบุคคลเลือกที่จะนำข้อมูลอิเล็กทรอนิกส์ที่ไม่มีการเปลี่ยนแปลงแก้ไขมาแสดงแทนการแสดงเอกสารต้นฉบับ ข้อมูลอิเล็กทรอนิกส์นั้นต้องอยู่ในสภาพที่สามารถทำให้ปรากฏแก่บุคคลที่เป็นผู้รับข้อมูลนั้นด้วย²⁴

²⁴ Article 8.

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by 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.

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

4. การรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน

เมื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์โดยให้มีผลทางกฎหมายเช่นเดียวกับเอกสารธรรมดา ก็จำเป็นต้องให้บุคคลสามารถนำข้อมูลอิเล็กทรอนิกส์มาเป็นพยานหลักฐานได้ กฎหมายแม่แบบของ UNCITRAL จึงมีบทบัญญัติเกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานด้วย ส่วนการชั่งน้ำหนักพยานหลักฐานนั้นเป็นเรื่องที่ต้องพิจารณาถึงพฤติการณ์ทั้งปวง โดยคำนึงถึงวิธีการสร้าง เก็บ รับ และส่งข้อมูลอิเล็กทรอนิกส์นั้น และวิธีการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์นั้นด้วย²⁵

-
- (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.

²⁵ Article 9. Admissibility and evidence weight of data messages

- (1) In any legal proceeding, 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 data message shall be given due evidence weight. In assessing the evidential weight of 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.

5. หลักเกณฑ์เกี่ยวกับการเก็บรักษาข้อมูลหรือเอกสาร

กฎหมายแม่แบบของ UNCITRAL มีบทบัญญัติให้เก็บรักษาข้อมูลในรูปของข้อมูลอิเล็กทรอนิกส์ได้โดยให้มีผลทางกฎหมายเช่นเดียวกับการเก็บรักษาข้อมูลในรูปของเอกสารธรรมดา โดยกำหนดหลักเกณฑ์ให้การเก็บรักษาข้อมูลอิเล็กทรอนิกส์ที่มีผลเช่นเดียวกับการเก็บรักษาข้อมูลในรูปของเอกสารธรรมดาจะต้องปรากฏว่าข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำมาใช้ในภายหลังได้ และการเก็บรักษาข้อมูลอิเล็กทรอนิกส์ต้องกระทำในรูปแบบที่สามารถแสดงว่าข้อมูลอิเล็กทรอนิกส์ที่เก็บรักษานั้นมีเนื้อหาตรงกันกับข้อมูลหรือเอกสารที่ต้องเก็บรักษา แต่ไม่ได้หมายความว่าข้อมูลอิเล็กทรอนิกส์นั้นต้องไม่มีการเปลี่ยนแปลงจากรูปเดิม ทั้งนี้เพราะการเก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นมักมีการเข้ารหัสข้อมูล การบีบข้อมูล หรือการเปลี่ยนข้อมูลอยู่เป็นปกติ²⁶

ภาระการพิสูจน์พยานหลักฐาน

สภาพทางกายภาพของพยานหลักฐานที่เป็นหนังสือนั้นอยู่ในสถานะที่บุคคลทั่วไปสามารถอ่านออกเขียนได้ แต่ในส่วนของเอกสารอิเล็กทรอนิกส์นั้นไม่มีคุณลักษณะประการนี้ จึงเป็นเรื่องยากที่คนทั่วไปจะได้รับความเสมอภาคกันในการเข้าถึงและสามารถตรวจสอบความถูกต้องของเอกสารประเภทนี้ได้ เพราะคนส่วนใหญ่ไม่รู้แม้กระทั่งว่าตนจะต้องนำเครื่องมือหรือผู้เชี่ยวชาญ

²⁶ Article 10. Retention of data messages

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

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

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

ชาวนาโดมาพิสูจน์รวมทั้งไม่มีเงินเพียงพอที่จะจัดหาเครื่องมือหรือว่าจ้างผู้เชี่ยวชาญมาได้ ในขณะที่กฎหมายของไทยในปัจจุบันยังคงผลักระการพิสูจน์ให้ตกแก่ฝ่ายที่อ้างข้อเท็จจริง ซึ่งหากนำสืบไม่ได้ ก็ต้องตกเป็นฝ่ายแพคดีในที่สุด ในกรณีของบัตรเครดิตนั้น หากผู้ถือบัตรถูกบุคคลที่สามขโมยข้อมูลบัตรเครดิตไปใช้โดยที่เจ้าของบัตรไม่รู้ตัว หรือกรณีเกิดความผิดพลาดในระบบคอมพิวเตอร์ของธนาคาร ทำให้ตนถูกเรียกเก็บค่าใช้จ่ายที่เกิดขึ้นต่างๆ ที่ตนมิได้เป็นผู้ใช้บัตรเครดิต ในรายการนั้น ผู้ถือบัตรโดยทั่วไปย่อมไม่มีทางที่จะปลดเปลื้องภาระการพิสูจน์ของตนตามข้อต่อสู้ที่ว่า คอมพิวเตอร์ของธนาคารเกิดความผิดพลาด หรือตนมิใช่ผู้ทำธุรกรรมนั้น เพราะตามหลักการในมาตรา 84 ของประมวลกฎหมายวิธีพิจารณาความแพ่งวางหลักว่า “ถ้าคู่ความฝ่ายใดฝ่ายหนึ่งกล่าวอ้างข้อเท็จจริงอย่างใด เพื่อสนับสนุนคำฟ้องหรือคำให้การของตน ให้นำที่นำสืบข้อเท็จจริงนั้นตกอยู่แก่คู่ความฝ่ายที่กล่าวด้วย” กรณีดังกล่าวย่อมเกิดความไม่เป็นธรรมต่อผู้ถือบัตรเป็นอย่างมาก

ดังนั้น จึงควรจะหาทางตีความบังคับใช้หลักกฎหมายพยานและวิธีพิจารณาความแพ่ง เพื่อผลักระการพิสูจน์ทั้งหมดกลับไปยังผู้ให้บริการบัตรเครดิตในทุกกรณีที่มีการอ้างเอกสารอิเล็กทรอนิกส์เป็นพยาน โดยกำหนดเป็นเงื่อนไขบังคับก่อนการอนุญาตให้นำเอกสารอิเล็กทรอนิกส์เข้าสืบว่า ผู้ให้บริการต้องนำสืบถึงความถูกต้องสมบูรณ์ของกลไกการทำงานของเครื่องมืออิเล็กทรอนิกส์ที่เกี่ยวข้อง และการกำกับควบคุมที่ต้องมีโดยบุคลากรทางช่างอิเล็กทรอนิกส์ เพื่อเปิดโอกาสให้ผู้ใช้บริการสามารถโต้แย้งคัดค้านได้ โดยจัดให้มีคณะผู้เชี่ยวชาญทางเทคนิคผู้เป็นกลางมาช่วยตรวจสอบคัดค้านให้ โดยบังคับให้ผู้ให้บริการเป็นผู้รับภาระจ่ายค่าปวยการของผู้เชี่ยวชาญ มาตรการที่ศาลอาจนำมาใช้เพื่อกรณี เช่น ตีความมาตรา 93 (2) ของประมวลกฎหมายวิธีพิจารณาความแพ่ง ให้ทุกกรณีที่กฎหมายกำหนดให้รับฟังเฉพาะพยานเอกสารว่ารวมถึงเอกสารอิเล็กทรอนิกส์ แต่โดยสภาพทางกายภาพเป็นกรณีที่ไม่สามารถนำต้นฉบับมาแสดงได้โดยประการอื่น จึงให้นำสืบเอกสารกระดาษที่ผลิตโดยเครื่องอิเล็กทรอนิกส์แทนได้เสมือนเป็นสำเนาของต้นฉบับ โดยมีเงื่อนไขบังคับก่อนว่าในเมื่อผู้อ้างเอกสารอิเล็กทรอนิกส์นำสืบเบื้องต้นถึงความน่าเชื่อถือให้เป็นที่พอใจแก่ศาลว่ากลไกอิเล็กทรอนิกส์ และการกำกับควบคุมโดยช่างเทคนิคไม่เปิดช่องให้สงสัยว่าเอกสารอิเล็กทรอนิกส์นั้นอาจจะไม่ถูกต้องแม่นยำในแง่ของเนื้อหาและแหล่งที่มา เพราะผู้ให้บริการสามารถกระจายต้นทุนส่วนนี้ลงไปเป็นค่าบริการที่เขาอาจเรียกเก็บจากผู้ใช้บริการทั้งหลายได้ และหากผู้ให้บริการไม่แน่ใจว่าจุดอ่อนและขีดความสามารถของระบบให้บริการทางอิเล็กทรอนิกส์ของตนจะก่อความเสียหายแก่ผู้ใช้บริการรายใด เมื่อใด ผู้ให้บริการก็ควรเอาประกันภัยความรับผิดเพื่อความเสียหายนั้นไว้เสียแต่แรก หากเกิดความเสียหายขึ้นเมื่อใด บริษัทผู้รับ

ประกันภัยก็จะจ่ายค่าเสียหายแทน ส่วนภาระต้นทุนเบี้ยประกันภัยนี้ ผู้ให้บริการก็สามารถกระจายต่อไปยังผู้ใช้บริการในราคาค่าบริการได้เองอยู่แล้ว²⁷

3. กฎหมายคุ้มครองผู้บริโภค

หากกล่าวถึงมาตรการทางกฎหมายที่เกี่ยวข้องกับการคุ้มครองผู้บริโภคในประเทศไทย อาจกล่าวได้ว่าเป็นครั้งแรกที่ในรัฐธรรมนูญแห่งราชอาณาจักรไทย ฉบับปัจจุบัน (พ.ศ.2540) ได้วางหลักการเรื่องการคุ้มครองผู้บริโภคไว้ในมาตรา 57 ดังนี้

“สิทธิของบุคคลซึ่งเป็นผู้บริโภคย่อมได้รับความคุ้มครอง ทั้งนี้ ตามที่กฎหมายบัญญัติ

กฎหมายตามวรรคหนึ่งต้องบัญญัติให้มีองค์กฤษฎะซึ่งประกอบด้วยตัวแทนผู้บริโภคทำหน้าที่ให้ความเห็นในการตรากฎหมาย กฎ และข้อบังคับ และให้ความเห็นในการกำหนดมาตรการต่างๆ เพื่อคุ้มครองผู้บริโภค”

กฎหมายรัฐธรรมนูญถือเป็นกฎหมายหลักที่วางหลักการเรื่องนี้ ในส่วนที่เกี่ยวกับการบัญญัติกฎหมายเรื่องการคุ้มครองสิทธิของผู้บริโภค และการจัดตั้งองค์กฤษฎะที่ทำหน้าที่ออกกฎเกณฑ์ ระเบียบ และมาตรการต่างๆ เพื่อบรรลุดัตถประสงค์ตามกฎหมายในเรื่องนั้นๆ กล่าวคือ ผู้บริโภคในความหมายทั่วไป ย่อมหมายถึงบุคคลทั่วไปที่เกี่ยวข้องกับกิจกรรมต่างๆ ในชีวิตประจำวัน ไม่ว่าจะเป็นผู้ประกอบการบริโภคสินค้า ผู้ใช้บริการของร้านค้าหรือสถานบริการ ในบางกรณีบุคคลเหล่านี้จะได้รับความคุ้มครองสิทธิตามกฎหมาย แต่ในบางกรณีจะต้องเป็นบุคคลที่ระบุไว้ในกฎหมายเฉพาะเรื่องเท่านั้นจึงจะได้รับความคุ้มครอง อาทิเช่น เป็นผู้ซื้อสินค้าหรือผู้รับบริการจากผู้ประกอบธุรกิจ จึงเป็นผู้บริโภคตามความหมายใน “พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ.2522” “พระราชบัญญัติการแข่งขันทางการค้า พ.ศ.2542” เป็นต้น ซึ่งส่วนใหญ่มักเป็นกฎหมายเฉพาะเรื่องที่เกี่ยวข้องกับการควบคุมการประกอบการชนิดนั้นๆ

²⁷ พรชัย วิวัฒน์ภัทรกุล, “การพาณิชย์อิเล็กทรอนิกส์ และเทคโนโลยีสารสนเทศภายใต้กฎหมายไทยและผลกระทบที่มีต่อธุรกิจการธนาคาร,” วารสารนิติศาสตร์, ปีที่ 28 ฉบับที่ 4 (ธันวาคม 2541) : หน้า 724 – 725.

กฎหมายสำคัญที่วางหลักการพื้นฐานเรื่องการคุ้มครองสิทธิของผู้บริโภคในเรื่อง การซื้อขายสินค้าและบริการ คือ “พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ.2522” แก้ไขเพิ่มเติม พ.ศ.2541 มีหลักการสำคัญเรื่องคุ้มครองสิทธิของผู้บริโภค 5 ประการ คือ

1. สิทธิที่จะได้รับข่าวสารข้อมูลเกี่ยวกับสินค้าหรือบริการที่ถูกต้อง
2. สิทธิที่จะเลือกซื้อสินค้าและบริการ
3. สิทธิที่จะได้รับความปลอดภัยจากการใช้สินค้าหรือบริการ
4. สิทธิที่จะได้รับความเป็นธรรมในการทำสัญญา และ
5. สิทธิที่จะได้รับการชดเชยความเสียหาย

หลักการทั้ง 5 ประการนี้ได้บัญญัติไว้ในมาตราต่างๆ ของกฎหมายฉบับนี้ คือ การโฆษณาสินค้าและบริการ, การควบคุมฉลาก, การทำสัญญา, การดำเนินคดีเกี่ยวกับการ ละเมิดสิทธิของผู้บริโภคโดยเจ้าหน้าที่คุ้มครองผู้บริโภค เป็นต้น แนวคิดทางกฎหมายข้างต้นเกิด จากพัฒนาการทางสังคมและท้องถิ่น ซึ่งในอดีตบุคคลมีเสรีภาพในการตกลงเพื่อทำกิจกรรมหนึ่ง กิจกรรมใดตามหลักเศรษฐกิจแบบเสรี (Laissez-Faire) การประกอบการค้าแข่งขันอย่างเสรีเปิด โอกาสให้มีการสร้างผลกำไรอย่างเต็มที่ ผู้ประกอบการซึ่งมีอยู่น้อยรายเมื่อเทียบกับผู้บริโภค ผู้ ประกอบการบางรายอาจเอาเปรียบผู้บริโภคเกินสมควร และบางครั้งอาจก่อให้เกิดอันตรายต่อผู้ บริโภคด้วย ผู้ซึ่งอาจไม่มีความรู้เกี่ยวกับสินค้าหรือผลิตภัณฑ์นั้น รัฐจึงออกกฎหมายเพื่อบังคับต่อ ผู้ประกอบการธุรกิจบางประเภท เพื่อคุ้มครองสิทธิของผู้บริโภคตามความจำเป็น ซึ่งโดยหลักกฎหมาย แล้วยอมให้ความคุ้มครองแก่ผู้บริโภคทุกรายอย่างเท่าเทียมกัน แต่สภาพของการค้าในปัจจุบันซึ่ง กระทำบนเครือข่ายอินเทอร์เน็ตที่เรียกว่าพาณิชย์อิเล็กทรอนิกส์นั้น ผู้บริโภคอาจไม่ได้รับความคุ้ม ครองตามกฎหมาย และปัจจุบันก็ยังไม่มีกฎหมายที่เกี่ยวข้องโดยตรง ทำให้เกิดปัญหาว่าสิทธิของ ผู้บริโภคจะได้รับความคุ้มครองเพียงใด เช่น ผู้บริโภคควรได้รับข้อมูลที่ชัดเจนเพียงพอแก่การตัด สินใจ ควรกำหนดให้ผู้ประกอบการมีข้อมูลในเว็บไซต์ที่แสดงรายละเอียดของบริษัท ข้อมูลของสิน ค่าหรือบริการ ระดับการคุ้มครองข้อมูลของลูกค้า กลไกการรักษาความปลอดภัย วิธีการชำระเงิน ความรับผิดชอบของผู้ออกบัตรเครดิต ความรับผิดชอบของร้านค้า และโดยเฉพาะอย่างยิ่งความรับผิดชอบผู้ บริโภคต่อค่าใช้จ่ายต่างๆ ที่เกิดขึ้นจากการที่ผู้ยื่นบัตรเครดิตของเขาไปใช้โดยปราศจากอำนาจ เป็นต้น

นอกจากปัญหากฎหมายเกี่ยวกับการใช้บัตรเครดิตแล้ว ปัญหาสำคัญเกี่ยวกับ บัตรเครดิตอีกประการหนึ่งก็คือ ปัญหาเกี่ยวกับการควบคุมการประกอบธุรกิจบัตรเครดิต โดย

พิจารณาในแง่สถานประกอบธุรกิจที่ออกบัตรว่า การประกอบธุรกิจประเภทนี้ มีกฎหมายโดยตรงควบคุมไว้อย่างใดหรือไม่ ซึ่งจากการวิเคราะห์ปรากฏว่า สถานประกอบธุรกิจบัตรเครดิตหาได้อยู่ภายใต้การควบคุมของพระราชบัญญัติประกอบธุรกิจเงินทุน ธุรกิจหลักทรัพย์และธุรกิจเครดิตฟองซิเออร์ พ.ศ.2522 ไม่ และก็มีได้อยู่ภายใต้การควบคุมของประกาศคณะปฏิวัติ ฉบับที่ 58 แต่ถ้าหากผู้ออกบัตรเป็นธนาคารพาณิชย์ก็จะอยู่ภายใต้การควบคุมของพระราชบัญญัติการธนาคารพาณิชย์ พ.ศ.2505 และถ้ามีการนำบัตรเครดิตไปใช้ยังต่างประเทศก็จะอยู่ภายใต้การควบคุมของพระราชบัญญัติควบคุมการแลกเปลี่ยนเงินตรา พ.ศ.2485 นอกจากนี้ก็ยังคงอยู่ภายใต้การควบคุมของธนาคารแห่งประเทศไทยด้วย เนื่องจากการไม่มีกฎหมายเฉพาะเพื่อควบคุมบัตรเครดิตนี้เอง ทำให้สิทธิและหน้าที่ของคู่สัญญาในระบบบัตรเครดิตต้องตกอยู่ในลักษณะสัญญาทั่วไปตามประมวลกฎหมายแพ่งและพาณิชย์ ทำให้เกิดความได้เปรียบเสียเปรียบขึ้นในระหว่างคู่สัญญาโดยเฉพาะปัญหาทางด้านภาระการเสี่ยงภัยและความรับผิดชอบกล่าวจะตกกับผู้ถือบัตร ดังนั้น จึงควรมีกฎหมายโดยเฉพาะเพื่อควบคุมผู้ออกบัตร และให้ความคุ้มครองแก่ผู้ถือบัตรในการทำสัญญาบัตรเครดิต เพราะการใช้บัตรเครดิตเป็นการให้สินเชื่อประเภทหนึ่ง ซึ่งเป็นเรื่องที่กระทบต่อผู้บริโภคโดยทั่วไป การมีกฎหมายเพื่อใช้ในการควบคุมและคุ้มครองโดยเฉพาะ ย่อมทำให้ความผูกพัน และวิธีปฏิบัติในเรื่องความรับผิดชอบและการเสี่ยงภัยเป็นไปในแนวทางเดียวกัน อันจะก่อให้เกิดความเป็นธรรมแก่คู่กรณีทั้งหลาย และส่งผลให้บัตรเครดิตมีการใช้กันอย่างแพร่หลายมากยิ่งขึ้น²⁸

อย่างไรก็ตาม เพื่อให้ผู้บริโภคซึ่งเป็นผู้ใช้บัตรเครดิตได้รับการคุ้มครองในระดับหนึ่ง รัฐบาลจึงได้ออกพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการกำหนดธุรกิจที่ควบคุมสัญญาและลักษณะของสัญญา พ.ศ.2542 กำหนดให้คณะกรรมการว่าด้วยสัญญามีอำนาจให้การประกอบธุรกิจขายสินค้าหรือให้บริการใดเป็นธุรกิจที่ควบคุมสัญญา และมีอำนาจกำหนดหลักเกณฑ์ เงื่อนไข และรายละเอียดเกี่ยวกับลักษณะของสัญญา ทั้งนี้ ตามมาตรา 35 ทวิ แห่งพระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ.2522 แก้ไขเพิ่มเติมโดยพระราชบัญญัติคุ้มครองผู้บริโภค (ฉบับที่ 2) พ.ศ.2541

การประกอบธุรกิจขายสินค้าหรือให้บริการนั้นจะต้องเข้าลักษณะหนึ่งลักษณะใด

²⁸ รองศาสตราจารย์ระพีพงษ์ บุญโญภาส, อาชญากรรมทางเศรษฐกิจ (Economic Crime), (กรุงเทพมหานคร : สำนักพิมพ์นิติธรรม, 2540) หน้า 187-190.

ดังต่อไปนี้²⁹

1. เป็นธุรกิจที่มีการใช้ข้อตกลงที่ไม่เป็นธรรมต่อผู้บริโภค
2. เป็นธุรกิจที่มีการใช้สัญญาสำเร็จรูปอย่างแพร่หลาย
3. เป็นธุรกิจที่ผู้ประกอบการมีอำนาจต่อรองเหนือว่าผู้บริโภค ทั้งนี้ โดยพิจารณาจากฐานะทางเศรษฐกิจ ความรู้ความเข้าใจ ความสันทัดจัดเจน

การกำหนดลักษณะของสัญญาต้องเป็นไปตามหลักเกณฑ์ ดังต่อไปนี้³⁰

1. ให้ผู้บริโภคทราบสิทธิและหน้าที่ของตนตลอดจนข้อมูลข่าวสารเกี่ยวกับสินค้าหรือบริการโดยชัดเจนตามควรแก่กรณี
2. ไม่เป็นการจำกัดหรือยกเว้นความรับผิดชอบของผู้ประกอบการในส่วนที่เป็นสาระสำคัญโดยไม่มีเหตุผลที่สมควรเพียงพอ
3. ต้องคำนึงถึงความสุจริตในการประกอบธุรกิจ
4. ให้เยี่ยวยาความเสียหายในเวลาอันสมควรในกรณีที่มีการฝ่าฝืนสัญญา
5. จัดให้มีหลักฐานที่ชัดเจนเกี่ยวกับการแสดงเจตนาของผู้ประกอบการในเรื่องที่เป็นสาระสำคัญต่อการคุ้มครองผู้บริโภค
6. ต้องไม่เป็นการเพิ่มภาระเกินควรแก่การประกอบธุรกิจ

ต่อมาคณะกรรมการว่าด้วยสัญญาได้ออกประกาศเรื่อง ให้ธุรกิจบัตรเครดิตเป็นธุรกิจที่ควบคุมสัญญา พ.ศ.2542 ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 1 มกราคม 2543 เป็นต้นไป โดยประกาศฉบับนี้คำว่า “บัตรเครดิต” หมายความว่า บัตรที่ผู้ประกอบการออกให้แก่ผู้บริโภคตามหลักเกณฑ์และวิธีการที่ผู้ประกอบการกำหนด เพื่อใช้ชำระค่าสินค้า บริการ หรือค่าอื่นใดแทนการชำระด้วยเงินสดหรือเพื่อใช้เบิกถอนเงินสด แต่ไม่รวมถึงบัตรที่ได้มีการชำระค่าสินค้า

²⁹ พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการกำหนดธุรกิจที่ควบคุมสัญญา และลักษณะของสัญญา พ.ศ.2542 , ราชกิจจานุเบกษา , เล่ม 116 ตอนที่ 92 ก , (วันที่ 5 ตุลาคม 2542) , มาตรา 3.

³⁰ เรื่องเดียวกัน , มาตรา 5.

ค่าบริการ หรือค่าอื่นใดไว้ล่วงหน้าแล้ว นอกจากนี้ยังให้หมายความรวมถึงบัตรเดบิตด้วย เว้นแต่จะกำหนดเป็นอย่างอื่น³¹

สาระสำคัญของประกาศฉบับนี้ในส่วนที่เกี่ยวข้องกับการใช้บัตรเครดิตบนอินเทอร์เน็ตมีดังนี้

ข้อ 3. สัญญาที่ผู้ประกอบการธุรกิจทำกับผู้บริโภคต้องมีข้อความภาษาไทยที่สามารถเห็นและอ่านได้ชัดเจน มีขนาดของตัวอักษรไม่เล็กกว่าสองมิลลิเมตร และต้องใช้ข้อสัญญาที่มีสาระสำคัญและเงื่อนไข ดังต่อไปนี้

(6) การแจ้งให้ผู้บริโภคชำระเงินที่เกิดจากการใช้บัตรเครดิต ให้ผู้ประกอบการธุรกิจส่งใบแจ้งรายการใช้บัตรให้ผู้บริโภคทราบล่วงหน้าก่อนวันถึงกำหนดชำระเป็นระยะเวลาไม่น้อยกว่า 10 วัน

(7) ในกรณีที่ผู้ประกอบการธุรกิจมีข้อตกลงกับผู้ขายสินค้าหรือผู้ให้บริการที่ให้ผู้บริโภคสั่งซื้อสินค้าหรือใช้บริการที่ผู้บริโภคเพียงแจ้งความประสงค์ขอชำระค่าสินค้าหรือค่าบริการโดยการแจ้งหมายเลขบัตรเครดิตด้วยวาจาหรือลายลักษณ์อักษรให้ผู้ขายสินค้าหรือผู้ให้บริการ ทำการเรียกเก็บเงินจากผู้ประกอบการธุรกิจ ต้องมีข้อสัญญาดังต่อไปนี้

(ก) ถ้าผู้บริโภคทักท้วงว่าไม่ได้เป็นผู้สั่งซื้อสินค้าหรือไม่ได้เป็นผู้ขอรับบริการ จากผู้ขายหรือผู้ให้บริการดังกล่าว ผู้ประกอบการธุรกิจจะระงับการเรียกเก็บเงินจากผู้บริโภคทันที หรือในกรณีที่เรียกเก็บเงินไปแล้วจะคืนเงินให้กับผู้บริโภคทันที เว้นแต่ผู้ประกอบการธุรกิจจะพิสูจน์ได้ว่าภาระหนี้ที่เกิดขึ้นเป็นการกระทำของผู้บริโภคเองและใช้สิทธิเรียกคืนจากผู้บริโภคในภายหลัง

(ข) ไม่เป็นการตัดสิทธิของผู้บริโภคที่จะขอยกเลิกการสั่งซื้อสินค้าหรือรับ

³¹ ประกาศคณะกรรมการว่าด้วยสัญญา เรื่อง ให้ธุรกิจบัตรเครดิตเป็นธุรกิจที่ควบคุมสัญญา พ.ศ.2542 , ราชกิจจานุเบกษา , เล่ม 116 ตอนพิเศษ 89 ง , (วันที่ 3 พฤศจิกายน 2542) , ข้อ 1.

บริการภายในระยะเวลา 45 วัน นับตั้งแต่วันที่สั่งซื้อ หรือขอรับบริการหรือภายในระยะเวลา 30 วัน นับตั้งแต่วันถึงกำหนดการส่งมอบสินค้าหรือบริการ ในกรณีที่มีการกำหนดระยะเวลาส่งมอบสินค้าหรือบริการเป็นลายลักษณ์อักษร ถ้าผู้บริโภคพิสูจน์ได้ว่าไม่ได้รับสินค้า หรือไม่ได้รับบริการ หรือได้รับแต่ไม่ตรงตามกำหนดเวลา หรือได้รับแล้วแต่ไม่ครบถ้วน หรือชำรุดบกพร่อง หรือไม่ถูกต้องตรงตามวัตถุประสงค์โดยผู้ประกอบการจะระงับการเรียกเก็บเงินจากผู้บริโภค หรือในกรณีที่เรียกเก็บเงินไปแล้ว ถ้าเป็นการสั่งซื้อสินค้าหรือบริการภายในประเทศ จะคืนเงินให้กับผู้บริโภคภายในระยะเวลา 60 วัน นับตั้งแต่วันที่ผู้บริโภคแจ้ง

(8) ในกรณีมีการใช้บัตรเครดิต หรือบัตรเดบิตที่ผู้บริโภคแจ้งความประสงค์ขอรับใบแจ้งรายการใช้บัตร ผู้ประกอบการต้องส่งใบแจ้งรายการใช้บัตรให้ผู้บริโภคทราบ และกำหนดระยะเวลาให้ผู้บริโภคทราบ และกำหนดระยะเวลาให้ผู้บริโภคทักท้วง ดังนี้

(ก) ภายใน 10 วันทำการเป็นอย่างน้อย นับแต่วันที่ผู้บริโภคได้รับใบแจ้งรายการใช้บัตรจากผู้ประกอบการ ในการพิจารณาวันครบกำหนดดังกล่าวให้ผู้ประกอบการเป็นผู้มีหน้าที่นำสืบวัน เวลา ที่นำส่งใบแจ้งรายการใช้บัตรให้แก่ผู้ขนส่งและการทำงานของผู้ขนส่ง

(ข) ไม่เป็นการตัดสิทธิของผู้บริโภคในภายหลัง ถ้าผู้บริโภคสามารถพิสูจน์ได้

ว่าค่าใช้จ่ายในใบแจ้งรายการใช้บัตรบางรายการไม่ถูกต้อง และไม่ไ้เป็นความผิดหรือความบกพร่องของผู้บริโภคเอง แต่ผู้บริโภคจะต้องทักท้วงภายในระยะเวลาไม่เกิน 60 วัน นับแต่วันที่ผู้บริโภคได้รับใบแจ้งรายการใช้บัตรจากผู้ประกอบการ

ข้อ 4. สัญญาที่ผู้ประกอบการทำกับผู้บริโภคต้องไม่ใช่ข้อสัญญาที่มีลักษณะหรือมีความหมายทำนองเดียวกัน ดังต่อไปนี้

(1) ข้อสัญญาที่กำหนดให้ผู้บริโภคต้องผูกพันตามประกาศหรือหลักเกณฑ์ของผู้ประกอบการโดยผู้บริโภคไม่ได้รับแจ้งให้ทราบล่วงหน้าเป็นลายลักษณ์อักษร

(2) ข้อสัญญาที่เป็นการยกเว้น หรือจำกัดความรับผิดชอบที่เกิดจากการผิดสัญญา

ของผู้ประกอบธุรกิจ

(3) ข้อสัญญาที่ให้ผู้บริโภครับผิดชอบในค่าใช้จ่ายจากการใช้บัตรเครดิตโดยที่ไม่ได้เป็นความผิดของผู้บริโภค

(4) ข้อสัญญาที่ให้ผู้ประกอบธุรกิจมีสิทธิเรียกบัตรเครดิตคืนจากผู้บริโภค หรือ ยกเลิกบัตรเครดิตเมื่อใดก็ได้ โดยผู้ประกอบธุรกิจไม่ต้องแจ้งหรือแสดงผลให้ผู้บริโภคทราบล่วงหน้า

(5) ข้อสัญญาที่ให้ผู้ประกอบธุรกิจจ่ายเงินให้แก่ผู้ขายสินค้าหรือผู้ให้บริการแก่ผู้บริโภค โดยไม่ให้ผู้บริโภคยกเหตุใดๆ มากล่าวอ้างปฏิเสธความรับผิดชอบกับผู้ประกอบธุรกิจ

ข้อ 5. ข้อสัญญาตามข้อ 3 (3) ไม่ใช้บังคับกับสัญญาบัตรเครดิตที่ทำขึ้นก่อนประกาศฉบับนี้ใช้บังคับโดยมีข้อตกลงแจ้งชัดเป็นอย่างอื่น จนกว่าจะครบรอบระยะเวลาตามสัญญาบัตรเครดิต หรือครบ 1 ปี นับแต่วันที่ประกาศนี้ใช้บังคับ แล้วแต่ระยะเวลาใดจะสั้นกว่ากัน

จากหลักกฎหมายดังกล่าวจะเห็นได้ว่า กรณีที่บุคคลใดสั่งซื้อสินค้าและบริการผ่านเว็บไซต์ต่างๆ บนอินเทอร์เน็ตโดยการกรอกหมายเลขบัตรเครดิต ชื่อนามสกุล และวันหมดอายุของบัตรเครดิตให้แก่เว็บไซต์ผู้ขายเพื่อชำระราคาสินค้าและบริการนั้น หากมีบุคคลอื่นนำหมายเลขบัตรเครดิตนั้นไปใช้โดยมิชอบหรือมี Hacker เข้ามาเจาะข้อมูลในเว็บไซต์ของผู้ขายสินค้าและบริการรายนั้นแล้วนำหมายเลขบัตรเครดิตไปใช้โดยปราศจากอำนาจ ผู้บริโภคมีสิทธิปฏิเสธที่จะไม่ชำระเงินให้แก่ธนาคารหรือผู้ให้บริการบัตรเครดิตได้ หากสามารถพิสูจน์ได้ว่าตนมิได้เป็นผู้ซื้อสินค้าหรือบริการดังกล่าวจริงหากในสัญญาให้บริการบัตรเครดิตระหว่างผู้ถือบัตรกับธนาคารมิได้ระบุถึงข้อสัญญาที่ให้สิทธิผู้บริโภคในการปฏิเสธการชำระเงินเอาไว้ โดยหลักกฎหมายฉบับนี้ถือว่าสัญญาให้บริการบัตรเครดิตของธนาคารมีข้อสัญญาดังกล่าวโดยปริยายและมีผลบังคับใช้ทันที แม้ไม่มีข้อสัญญาในส่วนนี้ระบุไว้ก็ตาม

มาตรการปราบปรามโดยวิธีการสืบย้อนรอย

ลักษณะการทำงานของอินเทอร์เน็ตประกอบด้วยส่วนสำคัญอย่างหนึ่ง คือ TCP/IP หรือ Transmission Control Protocol / Internet Protocol เนื่องจากอินเทอร์เน็ตนับว่าเป็นเครือข่ายบนเครือข่าย ที่เปิดโอกาสให้เครือข่ายคอมพิวเตอร์อื่นเชื่อมโยงเข้ามาใช้งานหรือเป็นศูนย์กลางเชื่อมโยงเครือข่ายคอมพิวเตอร์อื่นๆ แต่ปัญหาที่เกิดขึ้นในการเชื่อมโยงเครือข่าย

คอมพิวเตอร์เข้าด้วยกันคือ แต่ละเครือข่ายใช้คอมพิวเตอร์ต่างชนิด ต่างยี่ห้อ และระบบปฏิบัติการที่ต่างกัน มาตรฐานของ TCP/IP จึงถูกใช้เป็นกฎเกณฑ์สำคัญในการแก้ไขปัญหาเหล่านี้ โดยจะกลายเป็นระบบเปิดที่สมบูรณ์แบบที่มีการเชื่อมโยงคอมพิวเตอร์ได้ตั้งแต่พีซีจนถึงเมนเฟรม และไม่จำกัดระบบปฏิบัติการใช้ TCP/IP จึงเป็นมาตรฐานที่ทั่วโลกยอมรับ³²

TCP/IP (Transmission Control Protocol / Internet Protocol)

คือ ข้อกำหนดเกี่ยวกับรูปแบบการเชื่อมโยงในเครือข่าย จัดทำขึ้นเพื่อใช้เป็นกฎเกณฑ์ให้เครื่องคอมพิวเตอร์ใช้งานร่วมกันในลักษณะของระบบเปิด คือ ไม่ว่าจะเป็คอมพิวเตอร์ชนิดใดหรือระบบใดก็ตาม จะสามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้ TCP/IP เป็นการกำหนดรูปแบบการสื่อสารระหว่างซอฟต์แวร์ การจัดการโอนย้ายข้อมูล การแสดงสถานะของเครื่องคอมพิวเตอร์ที่อยู่บนเครือข่าย เป็นต้น

รหัสประจำเครื่อง IP (IP Address)

การสื่อสารกันในระบบเครือข่ายอินเทอร์เน็ตที่มี TCP/IP เป็นมาตรฐานนี้ เครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่ออยู่เป็นจำนวนมาก เครื่องคอมพิวเตอร์แต่ละเครื่องต้องสามารถระบุ หรืออ้างอิงได้โดยไม่เกิดความซ้ำซ้อนกับเครื่องคอมพิวเตอร์อื่น มิฉะนั้นข่าวสารที่เครือข่ายรับมาจะไม่สามารถส่งไปให้กับเครื่องคอมพิวเตอร์ที่ต้องการข่าวสารนั้นได้ ดังนั้น เครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่ออยู่จึงต้องมีหมายเลขประจำตัวเอาไว้อ้างอิงให้เครื่องคอมพิวเตอร์อื่นๆ ได้ทราบ เหมือนกับคนทุกคนต้องมีชื่อให้คนอื่นเรียก หมายเลขอ้างอิงดังกล่าวถูกเรียกว่า IP Address หรือหมายเลข IP (Internet Protocol)³³

IP Address ประกอบด้วยเลขฐานสอง จำนวน 32 บิต แบ่งออกเป็น 4 ส่วน แต่ละส่วนมี 8 บิต เมื่อดูเฉพาะแต่ละส่วนเป็นเลขฐานสิบจะได้เลขจำนวน 256 ค่าไม่ซ้ำกัน (0-255)

³² กิตติ ภัคดีวัฒน์กุล, NETSCAPE ALL-IN-ONE (กรุงเทพมหานคร : ไทยเจริญการพิมพ์, 2539) , หน้า 8.

³³ ตัน ตันท์สุทธิวงศ์ สุพจน์ ปุณณชัยยะ สุวัฒน์ ปุณณชัยยะ, รอบรู้ Internet และ World Wide Web. (กรุงเทพมหานคร : โปรวีชั่น, 2539) , หน้า 37-39.

IP Address จะนำเอาหมายเลขทั้ง 4 ส่วนมารวมกัน โดยแยกแต่ละส่วนด้วยจุด ดังนั้น หมายเลขทั้งหมดที่เป็นไปได้โดยค่าไม่ซ้ำกัน คือ 256 ยกกำลัง 4 หรือ 4,294,967,296 จำนวน มีค่าหมายเลขจาก 000.000.000.000 จนถึง 255.255.255.255 หมายเลขเหล่านี้เองที่อินเทอร์เน็ตใช้กำหนดให้กับเครือข่ายและเครื่องคอมพิวเตอร์เพื่อใช้อ้างอิง³⁴

ในการจัดตั้งหรือกำหนดหมายเลข IP Address นี้มีวิธีการกำหนดที่ชัดเจนและมีกฎเกณฑ์ที่รัดกุม ผู้ใช้ที่อยากจัดตั้งโฮสต์คอมพิวเตอร์เพื่อเชื่อมต่อเข้าอินเทอร์เน็ตและให้บริการต่างๆ สามารถขอหมายเลข IP Address ได้ที่หน่วยงาน Inter Network Information Center (InterNIC) ขององค์กร Network Solution Incorporated (NSI) ที่รัฐเวอร์จิเนีย สหรัฐอเมริกา แต่ถ้าผู้ใช้สมัครเข้าเป็นสมาชิกขอใช้บริการอินเทอร์เน็ตจากบริษัทผู้ให้บริการ หรือ ISP (Internet Service Provider) รายใดก็แล้วแต่ก็ไม่จำเป็นต้องติดต่อขอ IP Address อีก เนื่องจากหน่วยงาน ISP เหล่านั้นจะกำหนดหมายเลข IP ให้ใช้ หรือส่งค่า IP ชั่วคราวให้ใช้งาน ทั้งนี้ขึ้นอยู่กับแบบของการขอใช้บริการ

IP Address เปรียบเสมือนบ้านเลขที่ที่มีเบอร์เดียวในโลก ในการใช้บริการอินเทอร์เน็ตในแต่ละครั้ง โดยทั่วไปผู้ให้บริการ (ISP) จะเป็นผู้จัดสรรหมายเลข IP ให้แก่สมาชิกเพื่อใช้เป็นที่อยู่ในการติดต่อในการท่องอินเทอร์เน็ต เช่น ในกรณีที่ผู้ให้บริการรายหนึ่งมีหมายเลข IP จำนวน 1,000 หมายเลข และ ณ เวลา 9.30 นาฬิกา ของวันที่ 14/3/43 มีผู้ขอใช้บริการอินเทอร์เน็ตเข้ามา ผู้ให้บริการอาจจัดสรร IP หมายเลข 212.150.111.101 ให้แก่ผู้ใช้บริการรายนั้น เมื่อผู้ใช้บริการรายนี้จะไปอยู่ ณ จุดใดบนอินเทอร์เน็ต หมายเลข IP นี้ก็จะติดตามไปด้วยเสมอ โดยผู้ให้บริการ (ISP) จะเปรียบเสมือนโรงแรม ส่วนหมายเลข IP จะเปรียบเสมือนเบอร์ห้องพัก ดังนั้น เมื่อมีการกระทำผิดเกิดขึ้นหมายเลข IP จะเป็นข้อมูลเบื้องต้นที่จะต้องสืบค้นว่า ณ วันเวลาเกิดเหตุใครเป็นผู้ใช้บริการนั้น ซึ่งจะสันนิษฐานในเบื้องต้นได้ว่าผู้นั้นเป็นผู้ต้องสงสัยในการกระทำความผิด

โดยทั่วไปการที่ Hacker จะเข้าไปเปลี่ยนแปลงแก้ไขหรือขโมยข้อมูลในคอมพิวเตอร์หรือเว็บไซต์ต่างๆ บนอินเทอร์เน็ตได้นั้น จะต้องมีอุปกรณ์ดังนี้

1. โทรศัพท์และโมเด็ม เพื่อเข้าสู่คอมพิวเตอร์เซิร์ฟเวอร์ของผู้ให้บริการ

³⁴ กิตติ ภัคดีวัฒน์กุล, NETSCAPE ALL-IN-ONE, หน้า 15.

2. คอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์ภายในร้านอินเทอร์เน็ตคาเฟ่ที่เข้าไปใช้บริการ
3. คอมพิวเตอร์เซิร์ฟเวอร์ของผู้ให้บริการ
4. โปรแกรมคอมพิวเตอร์ที่ใช้เจาะข้อมูล

Hacker ต้องหมุนโทรศัพท์ผ่านโมเด็มเพื่อเข้าไปสู่ระบบอินเทอร์เน็ต โดยผ่านเครื่องคอมพิวเตอร์ของตนไปยังคอมพิวเตอร์เซิร์ฟเวอร์ของผู้ให้บริการที่ตนเป็นสมาชิก เพื่อเข้าไปกระทำความผิดต่อไป ดังนั้น ข้อมูลที่จะปรากฏร่องรอยการกระทำความผิดดังกล่าวจะอยู่ใน

1. คอมพิวเตอร์ส่วนบุคคลของ Hacker รายนั้น
2. คอมพิวเตอร์เซิร์ฟเวอร์ของผู้ให้บริการ โดยดูจาก IP Address ที่ผู้ให้บริการจัดสรรให้ว่าเป็นหมายเลขใดที่ใช้ในวันเวลาที่ความผิดเกิดขึ้น ซึ่งหมายเลขดังกล่าวจะไปปรากฏอยู่บนทุกเว็บไซต์ที่ Hacker เข้าไป
3. คอมพิวเตอร์เซิร์ฟเวอร์ของผู้เสียหาย
4. หมายเลขโทรศัพท์ (Caller I.D.) ที่ Hacker ใช้เชื่อมต่อระบบไปยังผู้ให้บริการอินเทอร์เน็ต (ISP)

Caller I.D. คือ หมายเลขโทรศัพท์ที่ผู้เรียกทำการเรียกเข้ามา เช่น โทรศัพท์มือถือจะแสดงให้เห็นบนหน้าจอว่าหมายเลขใดเรียกเข้ามา ปัจจุบันองค์การโทรศัพท์ไม่ได้ส่ง Caller I.D. ให้บริษัทผู้ให้บริการอินเทอร์เน็ต (ISP) บริษัทจึงไม่อาจทราบว่าโทรศัพท์มาจากที่ใด เช่น นาย ก. ใช้บริการของบริษัทเคเอสซี และได้เข้าสู่เครือข่ายอินเทอร์เน็ตเพื่อสักหมายเลขบัตรเครดิตของผู้อื่น หาก ISP ทราบถึง Caller I.D. ย่อมทราบได้ว่าโทรศัพท์มาจากที่ใด หากปรากฏว่าโทรศัพท์มาจากบ้านหรือสำนักงานของเจ้าของบัญชีดังกล่าว อาจสันนิษฐานในเบื้องต้นได้ว่านาย ก. เป็นผู้ต้องสงสัยในการกระทำความผิดนั้น ดังนั้น ISP จึงควรเก็บ Caller I.D. ไว้เป็นหลักฐานในคอมพิวเตอร์ โดยจะไม่นำมาใช้จนกว่าการกระทำความผิดจะเกิดขึ้นซึ่งไม่น่าจะถือว่าเป็นการลิดรอนสิทธิ³⁵ อย่างไรก็ตามยังมีข้อจำกัดบางประการที่เป็นอุปสรรคต่อการสืบสวนหาตัวผู้กระทำความผิด เช่น กรณีเป็นเบอร์กลางของบริษัท ห้างร้าน ซึ่งยากในการตรวจสอบถึงผู้ใช้ที่แท้จริง หากองค์กร

³⁵ ศรีศักดิ์ จามรมาน, รายงานการเสวนาทางวิชาการ เรื่อง "สื่อลามกและการค้าประเวณีทางอินเทอร์เน็ต : มะเร็งร้ายที่ทำลายเยาวชนไทย ," บทบัญญัติ, เล่มที่ 55 ตอน 1 (มีนาคม 2542) : หน้า 109.

ต่างๆ นั้นมิได้กำหนดประเภทหรือระดับชั้นของบุคลากรที่สามารถเข้าถึงและใช้เครื่องคอมพิวเตอร์ นอกจากนี้ปัจจุบันยังมีการจำหน่ายโปรแกรม Anti Caller I.D.

จากข้อมูลดังกล่าวข้างต้นจะเห็นได้ว่า การที่จะดำเนินคดีกับ Hacker ได้นั้น เจ้าหน้าที่ตำรวจหรือผู้เสียหายจะต้องพิสูจน์ให้ได้ว่า มีการเจาะเข้าสู่ระบบโดยใช้โทรศัพท์เครื่องใดในการติดต่อ ข้อมูลจากเครื่องคอมพิวเตอร์ส่วนบุคคลของ Hacker ซึ่งโดยปกติจะบันทึกข้อมูลในการทำธุรกรรมแต่ละครั้งไว้ ข้อมูลทางอิเล็กทรอนิกส์ที่คอมพิวเตอร์เซิร์ฟเวอร์ของผู้ให้บริการอินเทอร์เน็ตบันทึกไว้ และข้อมูลอิเล็กทรอนิกส์จากเครื่องคอมพิวเตอร์ของผู้เสียหายมาเปรียบเทียบกัน แต่ปัจจุบันประเทศไทยยังไม่มีกฎหมายที่เกี่ยวข้องกับการดำเนินการเพื่อให้ได้มาซึ่งพยานหลักฐานดังกล่าว รวมทั้งไม่มีกฎหมายที่ให้อำนาจผู้เสียหายหรือ ศาลในการยึดอายัดบรรดาเอกสารอิเล็กทรอนิกส์ดังกล่าวจาก Hacker ได้ นอกจากนี้การที่จะรวบรวมหลักฐานดังกล่าวได้นั้น ต้องอาศัยความร่วมมือจากหลายบุคคลและหลายองค์กร เช่น องค์กรโทรศัพท์ การสื่อสารแห่งประเทศไทย ผู้ให้บริการอินเทอร์เน็ต ผู้เสียหาย และเจ้าหน้าที่ที่เกี่ยวข้อง ซึ่งโดยปกติมักจะต้องเก็บรักษาความลับของลูกค้า ดังนั้น การได้มาซึ่งข้อมูลในการกระทำความผิดของ Hacker จึงเป็นไปได้ค่อนข้างยากหากไม่มีกฎหมายให้อำนาจไว้

วิเคราะห์มาตรการทางกฎหมายที่จะนำมาใช้กับการทุจริตต่อบัตรเครดิตบนอินเทอร์เน็ตในประเทศไทย

อินเทอร์เน็ตเป็นเครือข่ายคอมพิวเตอร์ขนาดใหญ่ มีผู้ให้บริการจำนวนมาก มีความหลากหลายในเนื้อหาข้อมูลข่าวสาร แต่การบริหารระบบอินเทอร์เน็ตนั้นเป็นการกระจายความรับผิดชอบโดยที่ไม่มีศูนย์กลางของระบบ หรือกล่าวอีกนัยหนึ่งก็คือไม่มีองค์กรหรือหน่วยงานใดเป็นผู้ดูแลระบบอินเทอร์เน็ตทั้งหมด แต่เป็นการดูแลและจัดการกันเองระหว่างหน่วยงานด้านโทรคมนาคม และผู้ให้บริการระบบอินเทอร์เน็ตในแต่ละพื้นที่เพื่อให้การเชื่อมต่อเครือข่ายคอมพิวเตอร์ในพื้นที่นั้นกับระบบอินเทอร์เน็ตทั้งหมดเกิดขึ้นได้³⁶

³⁶ ดร.เลอสรุ ธนสุกาญจน์ ผศ.ดร.จิตตภัทร เครือวรรณ ผศ.สุธรรม อยู่ในธรรม , กฎหมายสำหรับบริการอินเทอร์เน็ตในประเทศไทย , (กรุงเทพฯ : สำนักพิมพ์นิติธรรม , 2540) , หน้า 1.

อินเทอร์เน็ตได้ขยายตัวเข้ามามีบทบาทในชีวิตประจำวันมากขึ้นเรื่อยๆ และมีแนวโน้มว่าจะได้รับการพัฒนาขึ้นจนส่งผลกระทบต่อทางสังคม การเมือง และเศรษฐกิจ โดยการเชื่อมต่อระหว่างบุคคลในปัจจุบันจะเป็นไปในรูปแบบที่เรียกว่า “สังคมเครือข่าย” ปรากฏจากการควบคุมของรัฐ ผู้ให้บริการและผู้ให้บริการสามารถเข้าถึงและใช้เครือข่ายได้อย่างเสรีปลอดภัยจากการแทรกแซงของรัฐ สำหรับในส่วนของด้านเศรษฐกิจนั้น เครือข่ายอินเทอร์เน็ตได้เข้ามามีส่วนสำคัญอย่างมากต่อการทำธุรกรรมผ่านเครือข่ายที่เรียกว่าพาณิชย์อิเล็กทรอนิกส์ หลายประเทศได้พัฒนาโครงสร้างพื้นฐานและกฎหมายใหม่ๆ เพื่อรองรับและอำนวยความสะดวกให้กับพาณิชย์อิเล็กทรอนิกส์ คอมพิวเตอร์มีบทบาทสำคัญอย่างมากต่อระบบการสื่อสารและการคมนาคมในการลดระยะทาง เวลา รวมถึงค่าใช้จ่ายเพื่อการแลกเปลี่ยนข้อมูลข่าวสารซึ่งกันและกัน อันเป็นคุณประโยชน์แก่การพัฒนาสังคมทุกด้าน แต่ในขณะเดียวกันอาชญากรก็ได้อาศัยเทคโนโลยีคอมพิวเตอร์นี้ เป็นเครื่องมือและหาช่องทางที่จะประกอบอาชญากรรมรูปแบบใหม่ที่ซับซ้อน เช่น อาชญากรรมทางเศรษฐกิจ โดยเฉพาะอย่างยิ่งอาชญากรรมคอมพิวเตอร์ ภัยจากอาชญากรรมประเภทนี้อาจเกิดขึ้นกับระบบข้อมูลด้านความมั่นคงของประเทศ สถาบันการเงิน ธนาคาร ข้อมูลอันเป็นความลับทางธุรกิจ ข้อมูลในระบบสาธารณูปโภคของรัฐ เครือข่ายการสื่อสารโทรคมนาคม ตลอดจนประชาชนผู้ใช้คอมพิวเตอร์ทั่วไปล้วนอาจตกเป็นเหยื่ออาชญากรรมประเภทนี้ได้ทั้งสิ้น กระบวนยุติธรรมจึงจำเป็นต้องมีการปรับปรุงพัฒนาให้เท่าทันกระแสของการเปลี่ยนแปลง

จากการศึกษาวิเคราะห์ที่ผ่านมาแล้วนั้น เห็นได้ว่าปัญหาการทุจริตต่อบัตรเครดิตบนอินเทอร์เน็ตก่อให้เกิดความเสียหายทั้งในทางแพ่งและทางอาญา ในส่วนของทางแพ่งนั้นผู้ที่ได้รับความเสียหายอาจเป็นเจ้าของบัตรเครดิต ร้านค้า และผู้ออกบัตร ส่วนผู้กระทำผิดที่ขโมยข้อมูลหมายเลขบัตรเครดิตหรือนำหมายเลขบัตรเครดิตของผู้อื่นไปใช้โดยทุจริตย่อมถือเป็นการกระทำละเมิดซึ่งผู้กระทำผิดจำต้องชดใช้ค่าสินไหมทดแทน เมื่อพิจารณาจากกฎหมายไทยที่มีอยู่ในปัจจุบัน เห็นว่า ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420³⁷ สามารถนำมาปรับใช้ได้ แต่ก็ยังไม่ถือว่าเป็นกฎหมายที่สามารถนำมาบังคับใช้ได้อย่างมีประสิทธิภาพ ดังนั้น การบัญญัติกฎหมายที่จะนำมาบังคับใช้กับบัตรเครดิตโดยเฉพาะจึงมีความจำเป็นอย่างยิ่ง เพื่อกำหนดหลักเกณฑ์และ

³⁷ ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 บัญญัติว่า “ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิด จำต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้น”

ความรับผิดชอบของผู้ที่เกี่ยวข้องให้ชัดเจน ทั้งนี้ไม่ว่าจะเป็นการใช้บัตรเครดิตโดยวิธีการตามปกติทั่วไป หรือจะเป็นการใช้บัตรเครดิตผ่านเครือข่ายอินเทอร์เน็ตและคอมพิวเตอร์ก็ตาม แต่ปัจจุบันประเทศไทยยังไม่มีกฎหมายที่ควบคุมในเรื่องของบัตรเครดิตโดยเฉพาะ คงมีบทบัญญัติเพียงบางส่วนที่เกี่ยวข้องกับการปฏิเสธการชำระเงินในกรณีที่มีค่าใช้จ่ายรายการใดเกิดขึ้นจากการใช้บัตรเครดิต ด้วยวิธีการแจ้งหมายเลขบัตรเครดิตด้วยวาจาหรือลายลักษณ์อักษร และเจ้าของบัตรที่แท้จริงทักท้วงว่ามีได้เป็นผู้สั่งซื้อสินค้าและบริการนั้น อันเป็นบทบัญญัติที่ปรากฏอยู่ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการกำหนดธุรกิจที่ควบคุมสัญญาและลักษณะของสัญญา พ.ศ.2542 และประกาศคณะกรรมการว่าด้วยสัญญา เรื่อง ให้ธุรกิจบัตรเครดิตเป็นธุรกิจที่ควบคุมสัญญา พ.ศ.2542 ซึ่งเมื่อพิจารณาบทบัญญัตินี้ดังกล่าวแล้ว เห็นได้ว่าการกำหนดสิทธิและหน้าที่ระหว่างคู่สัญญาบัตรเครดิตนั้นยังไม่ชัดเจนเพียงพอ จากการศึกษาเปรียบเทียบกับหลักกฎหมายของประเทศสหรัฐอเมริกาและประเทศอังกฤษไม่ว่าจะเป็น Fair Credit Billing Act หรือ Consumer Credit Act of 1974 จะเห็นว่ามีบทบัญญัติเกี่ยวกับภาระหน้าที่ของผู้ถือบัตรและผู้ออกบัตรไว้ โดยในส่วนของผู้ถือบัตรนั้นจะต้องแจ้งถึงการสูญหายของบัตรเป็นลายลักษณ์อักษรภายในระยะเวลาที่กำหนดจึงจะได้รับการคุ้มครองในการจำกัดความรับผิดชอบหรือไม่ต้องรับผิดชอบใด ในส่วนของผู้ออกบัตรนั้นหากมีความประสงค์ที่จะให้ผู้ถือบัตรรับผิดชอบต่อค่าใช้จ่ายต่างๆ ที่เกิดขึ้น ผู้ออกบัตรมีภาระการพิสูจน์ว่าผู้ที่นำบัตรเครดิตไปใช้นั้นเป็นผู้ที่มีอำนาจ ดังนั้น จึงเห็นควรนำบทบัญญัติในส่วนนี้มาใช้เป็นแนวทางกำหนดสิทธิหน้าที่และความรับผิดชอบระหว่างคู่สัญญาบัตรเครดิตที่พึงจะปฏิบัติต่อกัน เพื่อให้คู่สัญญาได้รับรู้ถึงภาระหน้าที่ของตนอย่างชัดเจน มิใช่เพียงแต่กำหนดสิทธิของผู้ถือบัตรในการที่จะทักท้วงหรือปฏิเสธการชำระเงินสำหรับค่าใช้จ่ายรายการใดที่ตนมิได้เป็นผู้สั่งซื้อสินค้าและบริการเท่านั้น โดยมีได้กำหนดว่าผู้ถือบัตรจะต้องใช้สิทธิของตนภายในกำหนดระยะเวลาเท่าใด ทั้งยังควรกำหนดลักษณะของการกระทำที่ถือเป็นความยินยอมของผู้ถือบัตรที่ให้ผู้อื่นนำบัตรของตนไปใช้โดยปริยาย ทั้งนี้เพื่อเป็นการพิจารณาว่าการใช้บัตรดังกล่าวเกิดจากการใช้โดยผู้ได้รับมอบอำนาจจากผู้ถือบัตรหรือไม่ อันส่งผลถึงความรับผิดชอบของผู้ถือบัตร

ในส่วนของความผิดทางอาญานั้น เห็นว่า ปัจจุบันประเทศไทยยังไม่มีกฎหมายใดที่ให้ความคุ้มครองข้อมูลส่วนบุคคล ไม่มีกฎหมายในเรื่องบัตรเครดิต และไม่มีกฎหมายที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ ความผิดตามประมวลกฎหมายอาญาที่มีอยู่ อันได้แก่ ความผิดฐานลักทรัพย์ ฐานบุกรุก และฐานฉ้อโกง ไม่สามารถบังคับใช้กับการทุจริตต่อบัตรเครดิตบนอินเทอร์เน็ตได้อย่างครอบคลุม ดังนั้น หากคนร้ายได้มาซึ่งหมายเลขบัตรเครดิตของผู้อื่นหรือมีหมายเลขบัตรเครดิตของผู้อื่นไว้ในครอบครองโดยทุจริต หรือเจาะระบบเข้าไปขโมยหมายเลขบัตรเครดิต

ของผู้อื่น แล้วนำหมายเลขบัตรเครดิตเหล่านั้นไปใช้สั่งซื้อสินค้าและบริการบนอินเทอร์เน็ต ตามกฎหมายไทยที่มีอยู่อาจนำความผิดฐานฉ้อโกงมาปรับใช้ได้เท่านั้น โดยถือว่าคนร้ายได้ประโยชน์ในทางทรัพย์สินไปโดยการหลอกลวง ซึ่งเป็นการเอาผิดกับการกระทำขั้นสุดท้ายของคนร้าย ส่วนการกระทำผิดก่อนหน้านั้นไม่ว่าจะเป็นการขโมยข้อมูลส่วนบุคคลของผู้อื่น การเจาะระบบและขโมยข้อมูลผ่านระบบคอมพิวเตอร์ รวมถึงความผิดที่กระทำผ่านระบบคอมพิวเตอร์ ยังไม่มีบทบัญญัติใดของกฎหมายไทยที่จะลงโทษผู้กระทำผิดได้ ซึ่งปัญหาสำคัญประการหนึ่งที่พบก็คือข้อมูลในรูปของสื่ออิเล็กทรอนิกส์นั้นถือเป็นทรัพย์สินหรือไม่

จากการศึกษาวิเคราะห์กฎหมายของประเทศสหรัฐอเมริกาและประเทศอังกฤษพบว่าทั้งสองประเทศมีพัฒนาการด้านกฎหมายอาชญากรรมคอมพิวเตอร์มาโดยตลอด โดยประเทศสหรัฐอเมริกามีบทบัญญัติ The Computer Fraud and Abuse Act of 1986 ส่วนประเทศอังกฤษมี Computer Misuse Act of 1990 ซึ่งกฎหมายทั้งสองฉบับนี้สามารถนำมาบังคับใช้กับการกระทำผิดเกี่ยวกับคอมพิวเตอร์ได้อย่างกว้างขวาง มีการบัญญัติความผิดสำหรับผู้เข้าถึงคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจ การขโมยข้อมูลของผู้อื่น และการกระทำผิดผ่านระบบคอมพิวเตอร์ โดยพัฒนาการด้านกฎหมายของทั้งสองประเทศก็เคยพบกับอุปสรรคของคำจำกัดความคำว่า "ทรัพย์สิน" เช่นกันว่าจะหมายความรวมถึงข้อมูลในระบบคอมพิวเตอร์ด้วยหรือไม่ ซึ่งในที่สุดก็มีการบัญญัติกฎหมายที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ขึ้นมาเป็นการเฉพาะเพื่อแก้ไขปัญหาคือข้อขัดข้องต่างๆ ทำให้การบังคับใช้กฎหมายกับความผิดที่เกิดขึ้นเป็นไปอย่างมีประสิทธิภาพ นอกจากนี้ ประเทศสหรัฐอเมริกายังกำหนดให้การลักลอบดักฟังหรือรบกวนการสื่อสารระหว่างบุคคลทางสื่ออิเล็กทรอนิกส์เป็นการกระทำที่มีขอบด้วยกฎหมายและมีโทษทางอาญาตาม The Electronic Communication Privacy Act of 1986

ในส่วนในเรื่องเขตอำนาจศาลนั้น จากการศึกษาคดีตัวอย่างที่เกิดขึ้นในประเทศสหรัฐอเมริกา ศาลที่จะพิจารณาและมีอำนาจเหนือจำเลยซึ่งอยู่ต่างประเทศนั้นจะต้องมีจุดคาบเกี่ยวเกิดขึ้น เช่นเจตนาของจำเลยในการกระทำความผิด ภาระของจำเลยในการรู้คดีในศาล ข้อขัดแย้งระหว่างอำนาจอธิปไตยของจำเลยและโจทก์ ผลประโยชน์ของรัฐที่ได้จากการตัดสินคดี ทางแก้ไขข้อพิพาทที่มีประสิทธิภาพมากที่สุด ผลประโยชน์ของโจทก์และมาตรการเยียวยาความเสียหายของโจทก์ ทางเลือกของการฟ้องคดีในศาลอื่น หรืออาจกำหนดไว้ในตัวบทกฎหมายให้ชัดเจนว่าการกระทำผิดที่ได้กระทำต่อคอมพิวเตอร์ในลักษณะใดจะถือเป็นความผิดในเขตอำนาจศาล อย่างไรก็ตามประเทศสหรัฐอเมริกาได้กำหนดความหมายของคอมพิวเตอร์ที่ได้รับการปก

ป้อง (Protected Computer) ว่าหมายถึง คอมพิวเตอร์ของรัฐบาล สถาบันการเงิน และ คอมพิวเตอร์ติดต่อระหว่างรัฐหรือระหว่างประเทศ ซึ่งคำจำกัดความที่มีความหมายกว้างขวางเช่นนี้จะช่วยแก้ไขปัญหาการโจรกรรมข้อมูลคอมพิวเตอร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ทำให้สหรัฐมีเขตอำนาจเหนือคดีอาชญากรรมคอมพิวเตอร์ระหว่างประเทศ ในส่วนของประเทศอังกฤษก็ได้บัญญัติในเรื่องเขตอำนาจศาลไว้ ในมาตรา 4-9 ของ Computer Misuse Act of 1990 ภายใต้กฎหมายนี้กำหนดเรื่องความสัมพันธ์เอาไว้ โดยระบุว่าความผิดที่อยู่ในเขตอำนาจศาลอังกฤษต้องเกิดจากการกระทำในหรือมุ่งต่อระบบคอมพิวเตอร์ใน Home Country ซึ่งหมายถึงอังกฤษ เวลส์ สก็อตแลนด์ และไอร์แลนด์เหนือ ที่รวมเรียกว่าสหราชอาณาจักร หรือ UK ความผิดที่อยู่ภายใต้บังคับของกฎหมายนี้ต้องเป็นความผิดที่เกิดขึ้นใน UK

ในส่วนความผิดที่เกี่ยวข้องกับบัตรเครดิตนั้น ประเทศสหรัฐอเมริกา มีบทบัญญัติที่เกี่ยวข้องกับบัตรเครดิตเป็นการเฉพาะ ทั้งยังมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งกฎหมายทั้งสองฉบับมีความสัมพันธ์และสามารถนำมาบังคับใช้ร่วมกันได้อย่างมีประสิทธิภาพ นั่นคือ The Credit Card Fraud Act of 1984 มาตรา 1029 ซึ่งได้บัญญัติคำว่า "access device" ให้มีความหมายอย่างกว้างขวางโดยครอบคลุมถึงตัวบัตรเครดิต หมายเลขบัตรเครดิต และอุปกรณ์เชื่อมต่ออื่นด้วย ซึ่งสัมพันธ์กับ Identity Theft and Assumption Deterrence Act of 1998 มาตรา 1028 ที่ได้กำหนดชนิดของข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองไว้ โดยให้คำจำกัดความของคำว่า Means of Identification ว่าหมายถึง ชื่อหรือตัวเลขใดๆ ที่อาจจะถูกใช้เพียงลำพังหรือโดยสัมพันธ์กับข้อมูลอื่นใด เพื่อที่จะบ่งชี้ความเฉพาะของบุคคลนั้น ซึ่งรวมถึง "access device" ด้วย ดังนั้นการที่บุคคลใดผลิต โยกย้าย หรือครอบครองหมายเลขบัตรเครดิตของผู้อื่นโดยเจตนาที่จะใช้โดยทุจริตย่อมมีความผิดตาม Identity Theft and Assumption Deterrence Act of 1998 มาตรา 1028 และหากบุคคลนั้นโดยเจตนาที่จะฉ้อโกงได้ทำการผลิต ปลอม หรือใช้หมายเลขบัตรเครดิตของผู้อื่นโดยปราศจากอำนาจ หรือครอบครองหมายเลขบัตรเครดิตที่ได้รับมาโดยปราศจากอำนาจ ตั้งแต่ 15 หมายเลขขึ้นไป ย่อมมีความผิดตาม The Credit Card Fraud Act of 1984 มาตรา 1029 ในส่วนของประเทศอังกฤษแม้จะไม่มีกฎหมายเฉพาะในเรื่องที่เกี่ยวกับการใช้หมายเลขบัตรเครดิตโดยทุจริตก็ตาม แต่ก็มีกฎหมายที่สามารถนำมาปรับใช้ได้ คือ Theft Act of 1968 ที่กำหนดความผิดฐานได้รับทรัพย์สินมาโดยการหลอกลวง

ดังนั้น หากจะป้องกันและปราบปรามการทุจริตต่อบัตรเครดิตบนอินเทอร์เน็ตได้

อย่างมีประสิทธิภาพ ประเทศไทยควรจะมีบัญญัติกฎหมายเฉพาะขึ้นมาควบคุม ไม่ว่าจะเป็ กฎหมายเกี่ยวกับบัตรเครดิต กฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎหมายอาชญากรรม ทางคอมพิวเตอร์ เนื่องจากเป็นกฎหมายในเชิงเทคนิคที่จะใช้ลงโทษผู้กระทำความผิด ซึ่งแตกต่าง จากความผิดตามกฎหมายอาญาทั่วไป เช่น ลักทรัพย์ ทำร้ายร่างกาย ทั้งนี้ ควรบัญญัติถึงอำนาจ ของเจ้าหน้าที่ที่เกี่ยวข้อง วิธีการได้มาซึ่งพยานหลักฐาน และวิธีพิจารณาความ ซึ่งมีรูปแบบและวิธี การเฉพาะ รวมไว้ในกฎหมายฉบับเดียวกันนี้ เพื่อให้การปรับใช้บทกฎหมายมีความสอดคล้องกัน กฎหมายอาชญากรรมทางคอมพิวเตอร์ฉบับนี้ ควรระบุให้อำนาจหน่วยงาน Computer Emergency Response Team (CERT) ซึ่งปัจจุบันอยู่ในความดูแลของศูนย์เทคโนโลยีอิเล็กทรอนิกส์ และคอมพิวเตอร์แห่งชาติ (NECTEC) ให้มีอำนาจในการดำเนินการตรวจค้นร่วมกับเจ้าหน้าที่ ตำรวจ อัยการ หรือศาล เช่นเดียวกับคณะกรรมการ เช่นเดียวกับหน่วยงาน CERT หรือหน่วยงาน ลับ United State Secret Service (U.S.S.S.) ของสหรัฐอเมริกา รวมถึงให้มีหน่วยงานรับเรื่องร้อง เรียนและให้ความช่วยเหลือในเบื้องต้นแก่เหยื่อเช่นเดียวกับหน่วยงาน Federal Trade Commission (FTC) ของสหรัฐอเมริกา

ในส่วนของกฎหมายลักษณะพยานหลักฐาน ควรมีการปรับปรุงแก้ไขกฎหมาย ด้วยการกำหนดประเภทของข้อมูลอิเล็กทรอนิกส์ที่จะนำมาใช้เป็นพยานหลักฐานและกำหนดวิธี การนำสืบที่ชัดเจนของการนำสืบพยานหลักฐานประเภทนี้ โดยผลลัพท์การพิสูจน์ทั้งหมดกลับไป ยังผู้ให้บริการบัตรเครดิตในทุกกรณีที่มีการอ้างเอกสารอิเล็กทรอนิกส์เป็นพยาน นอกจากนี้ควร ปรับปรุงแก้ไขกฎหมายให้ชัดเจนในเรื่องความหมายของต้นฉบับและสำเนาของเอกสาร และควร กำหนดวิธีการนำสืบข้อมูลอิเล็กทรอนิกส์ในลักษณะเดียวกับพยานเอกสาร และพยานที่เป็นสิ่ง บันทึกร (Recordings) เช่นเดียวกับ The Federal Rules of Evidence ของสหรัฐอเมริกาที่ยอมรับ สถานะของ Recordings เช่น แผ่นเสียง เทป ซีดี ภาพนิ่ง ว่าเป็นพยานเอกสาร และยกเลิกหลัก เกณฑ์การห้ามสืบพยานบุคคลเปลี่ยนแปลงแก้ไขพยานเอกสาร ทั้งนี้เนื่องจากเมื่อมีการยอมรับนิต กรรมสัญญาที่เกิดจากข้อมูลอิเล็กทรอนิกส์แล้ว หากมีข้อผิดพลาดที่ข้อมูลอิเล็กทรอนิกส์บันทึกไม่ ตรง คู่ความย่อมมีสิทธินำสืบพยานเพื่อเปลี่ยนแปลงแก้ไขได้ ดังนั้น เมื่อสัญญาเขียนเป็นหนังสือก็ ควรที่จะมีสถานะแบบเดียวกัน เมื่อมีข้อผิดพลาดคู่ความย่อมนำสืบเปลี่ยนแปลงแก้ไขได้เสมอ

นอกจากมาตรการทางกฎหมายแล้ว จากการศึกษายังพบว่าคำสั่งซื้อและการ ชำระเงินที่ทำผ่านระบบเครือข่ายนั้นจะอยู่ในรูปของข้อมูลข่าวสารอิเล็กทรอนิกส์ ซึ่งหัวใจสำคัญ อย่างหนึ่งของพาณิชย์อิเล็กทรอนิกส์ คือ การรักษาความปลอดภัยของข้อมูลข่าวสารเหล่านี้ ดัง

นั้น เพื่อป้องกันการทุจริตที่อาจเกิดขึ้นได้ในระหว่างการส่งข้อมูลผ่านระบบเครือข่าย จึงควรนำเทคโนโลยีรักษาความปลอดภัยอย่างระบบ SET (Secure Electronics Transactions) ซึ่งประกอบด้วยเทคนิคการเข้ารหัสและถอดรหัสข้อมูลมาใช้ในการรักษาความลับของข้อมูล ความถูกต้องของข้อมูล และรับรองความถูกต้องของคู่สัญญาที่เข้ามาเกี่ยวข้องกับการทำธุรกรรมนั้น ทั้งด้านผู้ซื้อ ร้านค้าและธนาคาร และกำหนดให้ร้านค้าควรมีระบบตรวจสอบว่าผู้ที่ตนกำลังทำธุรกรรมอยู่ด้วยนั้นเป็นเจ้าของบัตรเครดิตที่แท้จริงหรือไม่ด้วย.