

บทที่ 2

แนวคิดว่าการรับฟังพยานหลักฐานอิเล็กทรอนิกส์

เป็นที่ยอมรับกันโดยทั่วไปว่า คดีเกี่ยวกับเทคโนโลยีคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศจำนวนมาก หรือโดยส่วนใหญ่เป็นคดีที่มักไม่มี "ประจักษ์พยาน" (Eyewitness) ซึ่งหมายถึง พยานบุคคลที่ได้รู้เห็นหรือสัมผัส (perceive) กับข้อเท็จจริงหรือเหตุการณ์ที่มาเบิกความด้วยตนเองโดยตรง ทั้งนี้ไม่ว่าจะรู้เห็นมาด้วยประสาทสัมผัสใดก็ตาม ดังนั้น ข้อยืนยันแบบแน่นอนต้องถือว่าจำเป็น ผู้กระทำความผิดจึงแทบเป็นไปไม่ได้เลย คดีลักษณะนี้จึงจำเป็นต้องอาศัย "พยานแวดล้อมกรณี" (Circumstantial Evidence) หรือ "พยานแวดล้อม" เป็นสำคัญ กล่าวคือ พยานหลักฐานที่มุ่งพิสูจน์ข้อเท็จจริง ซึ่งมีได้เป็นประเด็นพิพาทในคดีโดยตรง หากแต่ใช้พิสูจน์ข้อเท็จจริงอื่น ๆ ที่จะช่วยบ่งชี้ได้ว่าข้อเท็จจริงอันเป็นประเด็นพิพาทนั้นน่าจะเกิดขึ้นหรือไม่ หรือถ้าเกิดขึ้นแล้วใครน่าจะเป็นผู้กระทำการนั้น

อย่างไรก็ตาม ด้วยหลักสำคัญที่เกี่ยวกับการพิจารณาและพิพากษาคดีอาญาที่ว่า ในคดีอาญานั้นต้องสันนิษฐานไว้ก่อนว่าผู้กล่าวหา หรือจำเลยยังเป็นผู้บริสุทธิ์อยู่จนกว่าศาลมีคำพิพากษาถึงที่สุดว่าเขาเป็นผู้กระทำความผิด ซึ่งความผิดนั้นจะต้องได้รับการพิสูจน์จนสิ้นสงสัยด้วย (All defendants in criminal case are presumed to be innocent until proven guilty beyond a reasonable doubt) อันเป็นหลักที่ปรากฏในประมวลกฎหมายวิธีพิจารณาความอาญา ตามมาตรา 227 ความว่า

“ศาลมีดุลยพินิจในการชั่งน้ำหนักพยานหลักฐานทั้งปวง อย่าพิพากษาลงโทษจนกว่าจะแน่ใจว่ามีการกระทำความผิดจริง และจำเลยเป็นผู้กระทำความผิดนั้น เมื่อมีความสงสัยตามสมควรว่าจำเลยได้กระทำความผิดหรือไม่ ให้ยกประโยชน์แห่งความสงสัยนั้นให้จำเลย”

ดังนั้น แม้คดีที่เกิดขึ้นจะแสวงหาประจักษ์พยานได้ยาก แต่ก็มิได้หมายความว่าคดีประเภทนี้ ศาลสามารถพิพากษาลงโทษจำเลยได้ แม้ยังปรากฏข้อสงสัยอยู่ คดีลักษณะนี้ต้องอาศัยพยานแวดล้อมที่เพียงพอแน่นอนจนจริง ๆ หรือที่มีอาจโต้แย้งได้ และเพื่อให้เกิดการอำนวยความสะดวกธุรกรรมได้อย่างแท้จริง ฝ่ายต่าง ๆ ที่เกี่ยวข้องจึงต้องใช้ความรู้ความสามารถ และความพยายามในการแสวงหา วิเคราะห์ และรับฟังพยานหลักฐานต่าง ๆ มากกว่าในคดีปกติธรรมดา อาทิ ผู้พิพากษาควร

ต้องเปิดโอกาสให้มีการสืบพยานแวดล้อมประเภทต่าง ๆ ที่น่าจะเกี่ยวข้องกับคดีอย่างกว้างขวางและเท่าเทียม แม้อาจทำให้ดูเหมือนล่าช้าไปบ้าง อนุญาตให้มีการนำอุปกรณ์อิเล็กทรอนิกส์เข้าสืบโดยตรง ไม่ใช่แค่เพียงสืบจาก ลำเนา หรือ Print out โดยเฉพาะอย่างยิ่งกรณีที่ต้องมีการแสดงให้เห็นถึงวิธีการทำงาน หรือระบบการประมวลผลของอุปกรณ์เหล่านั้น กระทั่งความเป็นไปได้ในกรณีที่ข้อมูลซึ่งนำมาเป็นพยานอาจถูกแก้ไข เปลี่ยนแปลง หรือสร้างขึ้น ฯลฯ ในขณะที่ฝ่ายโจทก์เองก็ต้องหาพยานหลักฐานที่น่าเชื่อถือเพียงพอ ที่สามารถบ่งชี้ได้อย่างแน่นอนหน้าว่าจำเลยเป็นบุคคลคนเดียวกับผู้กระทำความผิด แม้จะไม่มีประจักษ์พยานผู้พบเห็นขณะกระทำความผิดก็ตาม ซึ่งในที่นี้อาจหมายถึงพยานหลักฐานทางอิเล็กทรอนิกส์ต่าง ๆ ที่เชื่อมโยงถึงตัวผู้เป็นจำเลยได้ตามสมควร หรือพยานที่แสดงพฤติกรรมของจำเลยที่เกี่ยวกับการใช้งานคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์

2.1 การรับฟังพยานหลักฐาน

นิยาม “พยานหลักฐาน” คืออะไร กฎหมายไม่ได้มีบทนิยามศัพท์ไว้เป็นการเฉพาะ แต่มีผู้ทรงคุณวุฒิด้านกฎหมาย ได้อธิบายความหมายของคำว่า พยานหลักฐาน ไว้ดังนี้ ในทางวิชาการพยานหลักฐาน (evidence) หมายถึง สิ่งใด ๆ ที่มีคุณสมบัติที่จะแสดงให้เห็นถึงข้อเท็จจริงใดได้⁴

ตามกฎหมาย Common Law พยานหลักฐาน หมายถึง สิ่งที่มีคุณค่า (Probative Value) ในการพิสูจน์ข้อเท็จจริงหนึ่งข้อเท็จจริงใด⁴

พยานหลักฐาน หมายถึง สิ่งใด ๆ ที่แสดงข้อเท็จจริงให้ปรากฏแก่ศาลได้ ซึ่งบางทีก็เรียกสั้น ๆ ว่า “พยาน”⁵

พยานหลักฐาน หมายถึง สิ่งใด ๆ ก็ตาม ที่มีคุณสมบัติสามารถที่จะชี้บ่งหรือสื่อแสดงให้เห็นถึงความเป็นจริงหรือความไม่เป็นจริง ในปัญหาที่พิพาทกันในทางอรรถคดีได้ ไม่ว่าจะอยู่ในสภาพของพยานบุคคล หรือพยานเอกสาร หรือพยานวัตถุ หรือพยานผู้เชี่ยวชาญก็ตาม⁶ ประเภทของพยานหลักฐาน พยานหลักฐานนั้นในทางดราได้แบ่งประเภทไว้ต่าง ๆ กันตามความต้องการที่จะใช้ให้มีความหมายในการพูดแต่ละกรณีไป แยกออกได้ดังนี้

1. พยานบุคคล พยานเอกสาร พยานวัตถุ พยานบุคคล คือบุคคลที่มาเบิกความให้ข้อเท็จจริงในคดีต่อศาล ศาลรับรู้ข้อเท็จจริงจากพยานชนิดนี้โดยการที่พยานเล่าเรื่อง หรือตอบคำถามของศาลหรือคู่ความเกี่ยวกับข้อเท็จจริงหรือเหตุการณ์ที่พยานได้เห็น ได้ฟังหรือได้ทราบมาก่อน ความจริงแล้วสิ่งที่เป็นพยานหลักฐานก็คือ คำเบิกความหรือถ้อยคำของพยาน หากใช้ตัวพยาน (witness) เอง

⁴ พรเพชร วิชิตชลชัย. เรื่องเดียวกัน

⁵ โสภณ รัตนกร, คำบรรยายกฎหมายลักษณะพยาน กรุงเทพฯ สำนักพิมพ์นิติบรรณาการ, 2539 หน้า 18

⁶ จริญ รักดิธนากุล, กฎหมายลักษณะพยานหลักฐาน, กรุงเทพฯ หจก.จิรัชการพิมพ์, 2551 หน้า 57

ไม่ ฉะนั้นเมื่อกล่าวถึงพยานชนิดนี้ จึงหมายความว่าถึง คำเบิกความของพยาน (testimony) หรือบางทีเรียกว่าเป็นพยานถ้อยคำ (oral evidence or parol evidence) เพราะถ้าพยานอยู่เฉย ๆ ไม่เบิกความ ศาลก็จะได้ข้อเท็จจริงอะไร ผิดกับพยานเอกสารหรือพยานวัตถุ ซึ่งตัวอักษรหรือวัตถุนั้นเองแสดงข้อเท็จจริงต่อศาล หรือศาลตรวจสอบได้ และเนื่องจากศาลต้องบันทึกคำเบิกความของพยานเป็นลายลักษณ์อักษรเก็บรวมไว้ในสำนวนเพื่อเป็นหลักฐานในการวินิจฉัยคดี พยานบุคคลจึงหมายถึงบันทึกคำพยานที่ปรากฏอยู่ในสำนวน ซึ่งใช้ในการตัดสินคดีนั้นเองด้วย แต่ถ้าบันทึกคำพยานดังกล่าวนำไปใช้ในอีกคดีหนึ่งก็อาจกลายเป็นพยานเอกสารไป⁷ พยานบุคคลนับว่าเป็นพยานที่สำคัญที่สุด โดยเฉพาะอย่างยิ่งในคดีอาญาจะเป็นพยานหลักตั้งแต่ในชั้นสืบสวนสอบสวนและในชั้นศาล แม้ในคดีแพ่งก็จะขาดพยานบุคคลไม่ได้

พยานเอกสาร หมายถึงสิ่งซึ่งมีการบันทึกตัวอักษร ตัวเลข รูปรอยหรือเครื่องหมายซึ่งสามารถแสดงข้อความหรือความหมายอย่างใดอย่างหนึ่งให้ศาลตรวจสอบได้ สิ่งนั้นจะเป็นอะไรก็ได้ และจะบันทึกไว้โดยวิธีเขียนด้วยมือ พิมพ์ พิมพ์ดีด แกะสลัก ถักร้อยหรือวิธีอื่นใดก็ได้ ถ้าสามารถใช้เป็นพยานหลักฐานได้ พยานเอกสารอาจจะเป็นหนังสือสำคัญแสดงการจดทะเบียน หนังสือสัญญา จดหมาย บันทึกข้อความ สมุดบัญชี บันทึกคำให้การ ฯลฯ ซึ่งปกติก็มักจะเป็นการบันทึกข้อความด้วยตัวอักษรบนแผ่นกระดาษ ซึ่งสามารถสื่อความหมายหรือแสดงข้อเท็จจริงบางอย่างได้ แต่อาจบันทึกไว้ในวัสดุอื่นนอกจากกระดาษ เช่นบันทึกไว้ในผ้า กระดาน แผ่นโลหะ หรือมีการบันทึกไว้ที่แผ่นกำแพง ถ้าเป็นการนำสืบถึงถ้อยคำหรือความหมายที่บันทึกไว้ กำเพงนั้นก็อาจเป็นเอกสารได้ แม้การบันทึกตัวเลขที่เครื่องยนต์ของรถยนต์ก็เป็นเอกสารได้เช่นกัน สิ่งที่จะพิสูจน์ข้อเท็จจริงก็คือ ข้อความหรือความหมายของตัวอักษร ตัวเลขหรือเครื่องหมายที่บันทึกไว้ หาใช้วัสดุที่ใช้บันทึกไม่ ถ้านำสืบเกี่ยวกับตัววัตถุ เช่น นำสืบถึงความมีอยู่และรูปลักษณะ วัตถุนั้นก็เป็นพยานวัตถุไป⁸ พยานเอกสารนับว่าเป็นพยานสำคัญในคดีแพ่งยิ่งกว่าคดีอาญา เพราะคดีแพ่งมักจะมีการทำข้อตกลงกันไว้เป็นลายลักษณ์อักษรก่อน และในบางกรณีกฎหมายก็บังคับว่านิติกรรมจะต้องทำหลักฐานเป็นหนังสือไว้ด้วย พยานวัตถุ ได้แก่วัตถุหรือสิ่งใดที่อาจพิสูจน์ความจริงต่อศาลได้โดยการตรวจสอบมิใช่โดยการอ่านหรือพิจารณาข้อความที่บันทึกไว้ ตัวอย่างเช่น มีดหรือปืนของกลางที่โจทก์นำสืบเพื่อแสดงว่าจำเลยกระทำความผิด สถานที่ที่คู่ความขอให้ศาลไปเดินเผชิญสืบเพื่อพิสูจน์ว่ามีการบุกรุกกันหรือไม่ หรือบาดแผลที่ตัวผู้เสียหายเพื่อแสดงให้เห็นว่าจำเลยมีเจตนาเพียงทำร้ายหรือมีเจตนาฆ่า หรือข้อต่อสู้ของจำเลยในเรื่องป้องกันตัวฟังขึ้นหรือไม่ เอกสารที่นำสืบเพื่อพิสูจน์ว่าได้มีการทำขึ้นหลายปีแล้วหรือเพิ่งทำขึ้น หรือนำสืบเพื่อแสดงว่ามีการทำความผิดฐานปลอมเอกสาร มิได้นำสืบหรือพิสูจน์ข้อความที่บันทึกไว้

⁷ โสภณ รัตนกร , เรื่องเดียวกัน หน้า 20

⁸ พรเพชร วิชิตชลชัย. เรื่องเดียวกัน

เช่นนี้ ย่อมเป็นการนำสืบพยานวัตถุ ตัวบุคคลเองก็อาจเป็นพยานวัตถุได้ เช่น การที่ศาลดูบาดแผลที่ตัวผู้เสียหาย เป็นต้น⁹ พยานวัตถุที่เป็นสังหาริมทรัพย์อาจนำมาให้ศาลตรวจดูในศาลได้ เช่น การนำอาวุธที่จำเลยใช้ในการกระทำความผิด หรือนำเอกสารมาให้ศาลตรวจดู และถ้าเป็นอสังหาริมทรัพย์ เช่น ที่ดินและสิ่งปลูกสร้าง ก็อาจให้ศาลไปเดินเผชิญสืบ

พยานชั้นที่ 1 และพยานชั้นที่ 2 คำว่าพยานชั้นที่ 1 และพยานชั้นที่ 2 ไม่มีในกฎหมายไทยเรา และโดยปกติ ก็ไม่นิยมใช้กัน แต่ได้มีการอธิบายในตำรากฎหมายลักษณะพยาน โดยเอามาจากหลักกฎหมายพยานของอังกฤษ ซึ่งเกี่ยวข้องกับหลักกฎหมาย 2 เรื่อง¹⁰ คือ 1 พยานที่ดีที่สุด และพยานชั้นรอง (best and inferior evidence) 2 พยานชั้นแรกและพยานชั้นสอง (primary and secondary evidence) หลักประการแรกนั้นบางทีก็เรียกกันว่าหลักพยานดีที่สุด (the best evidence rule) ซึ่งมีหลักว่า คู่ความต้องเอาพยานที่ดีที่สุดมาสืบ จึงเกิดเป็นหลักกฎหมายต่อมาว่า คู่ความต้องนำต้นฉบับเอกสารมาสืบ มิใช่สำเนาหรือสำเนาสำเนามาสืบ ถ้ามีพยานวัตถุก็ต้องนำพยานวัตถุเองมาแสดงต่อศาล มิใช่ให้พยานบุคคลมาเบิกความกล่าวถึงวัตถุนั้น กล่าวกันว่าหลักประการนี้เป็นที่มาของหลักที่ว่าจะต้องนำพยานที่รู้เห็นเหตุการณ์โดยตรงมาสืบ มิใช่สืบด้วยพยานบอกเล่า หลักประการนี้ในปัจจุบันไม่ค่อยได้ใช้กัน คงใช้อยู่กับในกรณีของเอกสารเอกชน กล่าวกันว่า The Best Evidence Rule ของคอมมอนลอว์นั้นเป็นการเรียกชื่อให้สั้นเพื่อความสะดวก เกี่ยวกับกฎเกณฑ์การพิสูจน์ข้อความในเอกสารเพื่อให้ได้พยานชั้นแรก (primary evidence) เท่านั้น หากเพื่อให้ได้พยานที่ดีที่สุด (the best evidence) ไม่เป็นส่วนหนึ่งของกฎห้ามรับฟังพยานหลักฐาน (exclusionary rule) ซึ่งเกิดจากความกลัวว่าจู้และผู้พิพากษาจะถูกจูงใจให้ตัดสินคดีโดยไม่เป็นธรรม เพราะมีการหลอกลวงหรือเบิกความเท็จโดยคู่ความ ความจึงถูกจำกัดว่าจะเสนอพยานหลักฐานได้เฉพาะที่เป็นพยานชั้นนั้น หรือพยานที่รู้เห็นเองโดยตรงเท่านั้น

ประการที่สอง เป็นผลของหลักประการแรกซึ่งยังคงใช้อยู่ในส่วนที่เกี่ยวกับเอกสารเอกชน ซึ่งถือว่าต้นฉบับเอกสารเป็นพยานชั้นแรก คู่ฉบับและสำเนารวมถึงคำเบิกความกับข้อความในเอกสารนั้นเป็นพยานชั้นรอง หลักดังกล่าวนี้ปรากฏอยู่ในประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 93, 94 และประมวลกฎหมายอาญามาตรา 238

พยานหลักฐานที่รับฟังได้และรับฟังไม่ได้ ในการพิจารณาพยานของศาลนั้นจะมีขั้นตอนหลักอยู่สองประการคือ ขั้นตอนหนึ่งขั้นตอนการรับฟังพยานหลักฐาน ขั้นตอนนี้เป็นการคัดเลือกพยานหลักฐานว่าพยานหลักฐานใด รับฟังได้หรือรับฟังไม่ได้เท่านั้น ยังไม่ได้พิจารณาว่าฟังแล้วเชื่อหรือไม่เชื่อ

⁹ พรเพชร วิชิตชลชัย, เรื่องเดียวกัน

¹⁰ โสภณ รัตนกร, เรื่องเดียวกัน หน้า 26

พยานหลักฐานนั้นแต่อย่างใด ดังนั้น คำว่าพยานหลักฐานที่รับฟังได้ในที่นี้ จึงหมายถึงพยานหลักฐานที่ไม่ต้องห้ามมิให้รับฟังตามกฎหมาย ไม่เกี่ยวกับความน่าเชื่อถือของพยานหลักฐานนั้นแต่อย่างใด

ส่วนคำว่าพยานหลักฐานที่รับฟังไม่ได้ หมายถึง พยานหลักฐานที่ต้องห้ามมิให้รับฟังตามกฎหมาย ซึ่งตามหลักของการรับฟังพยานหลักฐาน ว่าโดยหลักแล้วพยานหลักฐานทุกชนิด ทุกประเภทสามารถรับฟังเป็นพยานหลักฐานทางคดีได้ทั้งหมด ยกเว้นแต่มีกฎหมายบทใดบทหนึ่งบัญญัติห้ามมิให้รับฟังพยานหลักฐานนั้นไว้ พยานหลักฐานนั้นจึงจะต้องห้ามมิให้รับฟัง และได้ชื่อว่าเป็นพยานหลักฐานที่รับฟังไม่ได้ ฉะนั้น เวลาจะวิเคราะห์ว่าพยานหลักฐานชิ้นใดรับฟังได้หรือไม่ ก็ต้องพิจารณาที่หลักกฎหมายก่อนว่า มีกฎหมายบทใดห้ามรับฟังพยานหลักฐานชิ้นนั้นหรือไม่ ถ้าไม่มีก็แสดงว่าพยานหลักฐานชิ้นนั้นเป็นพยานหลักฐานที่รับฟังได้ แต่ถ้ามีกฎหมายบทใดบทหนึ่งบัญญัติห้ามไว้ไม่ให้รับฟังเป็นพยาน พยานหลักฐานชิ้นนั้นก็ถูกตัดไม่ให้รับฟังและเป็นพยานหลักฐานที่รับฟังไม่ได้ บทกฎหมายที่มาบัญญัติห้ามมิให้รับฟังพยานหลักฐานเรียกชื่อรวมว่า บทตัดพยานหลักฐาน หมายถึงบทกฎหมายใดก็ได้ที่มีเนื้อหาไปห้ามรับฟังพยานหลักฐานชิ้นใดชิ้นหนึ่งในทางอรรถคดี กฎหมายนั้นได้ชื่อว่าเป็นบทตัดพยานหลักฐาน การวิเคราะห์เรื่องการรับฟังพยานหลักฐาน จึงไม่ไปเรียนกฎหมายบทที่ให้รับฟังได้ แต่ต้องไปเรียนกฎหมายบทที่ห้ามรับฟัง คือ บทตัดพยานหลักฐาน บทตัดพยานหลักฐานของกฎหมายไทยมีดังนี้¹¹

1. บทตัดพยานที่เป็นเท็จหรือปลอม บทนี้ไม่ได้เขียนไว้ในกฎหมายเป็นลายลักษณ์อักษร แต่เป็นหลักพื้นฐานหรือหลักกฎหมายทั่วไปในทางพยานหลักฐาน

2. บทตัดพยานหลักฐานที่ฟุ่มเฟือย ประวิงให้ชักช้าหรือไม่เกี่ยวแก่ประเด็น บทนี้ปรากฏอยู่ในประมวลกฎหมายวิธีพิจารณาความแพ่งมาตรา 86 วรรคสอง ซึ่งวางหลักไว้ว่า เมื่อศาลเห็นพยานหลักฐานใดฟุ่มเฟือยเกินสมควร หรือประวิงให้ชักช้าหรือไม่เกี่ยวแก่ประเด็น ให้ศาลมีอำนาจงดการสืบพยานหลักฐานเช่นนั้น หรือพยานหลักฐานอื่นต่อไป และมาตรา 87 (1) ซึ่งวางหลักไว้ว่า ห้ามมิให้ศาลรับฟังพยานหลักฐานใดเว้นแต่ (1) พยานหลักฐานนั้นเกี่ยวข้องกับข้อเท็จจริงที่คู่ความฝ่ายหนึ่งฝ่ายใดในคดีจะต้องนำสืบ และมาตรา 118 วรรคสาม ซึ่งวางหลักไว้ว่า ไม่ว่ากรณีใด ๆ ห้ามมิให้คู่ความถามพยานด้วยคำถามที่ไม่เกี่ยวกับประเด็นแห่งคดี ซึ่งสามารถอนุมานนำไปใช้ในคดีอาญาได้ด้วย ฉะนั้นพยานหลักฐานที่ไม่เกี่ยวกับคดีจึงเป็นพยานหลักฐานที่รับฟังไม่ได้ความยากอยู่ที่หลักเกณฑ์อะไรเป็นตัวตัดสินว่าพยานหลักฐานชิ้นใดเกี่ยวแก่ประเด็น พยานหลักฐานชิ้นใดไม่เกี่ยวแก่ประเด็น มาตรา 114 บัญญัติไว้ว่าให้เป็นอำนาจเด็ดขาดของศาลในการที่จะวินิจฉัยว่า

¹¹ จริฎ ภักดิธนากุล,คำบรรยายกฎหมายลักษณะพยานหลักฐาน, สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา ไม่ปรากฏปีที่พิมพ์, หน้า 42 - 50

พยานหลักฐานขึ้นใดเกี่ยวแก่ประเด็นหรือไม่เกี่ยวแก่ประเด็น ในทางวิชาการก็เลยไม่สามารถวางหลักกฎหมายตรงนี้ให้ชัดเจนได้ เป็นเรื่องดุลพินิจของศาลในแต่ละคดี

3. บทคัดพยานที่เกิดขึ้นหรือได้มาโดยมิชอบ บทนี้ปรากฏอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 ที่บัญญัติห้ามมิให้รับฟังพยานหลักฐานที่เกิดขึ้นจากการจงใจ ชูเจ้อ หลอกลวง หรือโดยมิชอบประการอื่น และมาตรา 226/1 ที่บัญญัติห้ามมิให้รับฟังพยานหลักฐานที่แม้เกิดขึ้นโดยชอบแต่ได้มาเนื่องจากการกระทำโดยมิชอบ หรือเป็นพยานหลักฐานที่ได้มาโดยอาศัยข้อมูลที่เกิดขึ้นหรือได้มาโดยมิชอบ

4. บทคัดพยานบอกเล่า บทคัดพยานบอกเล่าปรากฏตามประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 95/1 และมาตรา 104 กับประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/3 และมาตรา 227/1 ซึ่งมีสาระสำคัญโดยสรุปคือ ห้ามมิให้ศาลรับฟังพยานบอกเล่า เว้นแต่จะเข้าข้อยกเว้นให้รับฟังได้

5. พยานหลักฐานที่เกี่ยวกับประวัติอาชญากรรมหรือความประพฤติชั่วร้ายของจำเลยในคดีอาญา ต้องห้ามมิให้รับฟังมาใช้ในการพิสูจน์ความผิดในคดีปัจจุบันของจำเลย ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/2 ซึ่งบัญญัติสรุปได้ใจความที่ ห้ามมิให้ศาลรับฟังพยานหลักฐานที่เกี่ยวกับการกระทำความผิดครั้งอื่น ๆ หรือความประพฤติในทางเสื่อมเสียของจำเลย เพื่อพิสูจน์ว่าจำเลยเป็นผู้กระทำความผิดในคดีที่ถูกฟ้อง เว้นแต่พยานหลักฐานอย่างหนึ่งอย่างใด ดังต่อไปนี้ (1) พยานหลักฐานที่เกี่ยวข้องโดยตรงกับองค์ประกอบความผิดของคดีที่ฟ้อง (2) พยานหลักฐานที่แสดงถึงลักษณะ วิธี หรือรูปแบบเฉพาะในการกระทำความผิดของจำเลย (3) พยานหลักฐานที่หักล้างข้อกล่าวอ้างของจำเลยถึงการกระทำ หรือความประพฤติในส่วนดีของจำเลย

6. บทคัดพยานหลักฐานที่แสดงถึงพฤติกรรมทางเพศของผู้เสียหายในคดีความผิดเกี่ยวกับเพศ ห้ามมิให้จำเลยนำสืบด้วยพยานหลักฐานหรือถามค้านด้วยคำถามอันเกี่ยวกับพฤติกรรมทางเพศของผู้เสียหายกับบุคคลอื่นนอกจากจำเลย เว้นแต่จะได้รับอนุญาตจากศาลตามคำขอ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/4 ซึ่งบัญญัติสรุปได้ใจความว่า ในคดีความผิดเกี่ยวกับเพศ ห้ามมิให้จำเลยนำสืบด้วยพยานหลักฐานหรือถามค้านด้วยคำถามอันเกี่ยวกับพฤติกรรมทางเพศของผู้เสียหายกับบุคคลอื่นนอกจากจำเลย เว้นแต่จะได้รับอนุญาตจากศาลตาม คำขอ

7. บทคัดพยานบุคคล มีอยู่ 3 บท คือบทแรกตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 232 ใช้ในคดีอาญาเท่านั้น คือห้ามโจทก์ในคดีอาญาอ้างจำเลยเป็นพยานโจทก์ บทที่สองอยู่ในประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 95 (1) ห้ามมิให้รับฟังพยานบุคคลที่ไม่สามารถเข้าใจคำถามและไม่สามารถตอบคำถามได้ บทที่สาม โน้มนำไปใช้ในคดีอาญาด้วย และบทที่สาม ตาม

ประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 94 ที่ใช้เฉพาะในคดีแพ่ง กรณีที่มีกฎหมายบังคับให้ต้องมีเอกสารมาแสดง ห้ามมิให้นำสืบพยานบุคคลแทนเอกสาร หรือแก้ไขเปลี่ยนแปลงเพิ่มเติมตัดทอนข้อความในเอกสาร เว้นแต่จะเข้าข้อยกเว้น

8. บทคัดพยานเอกสารในคดีแพ่ง ตามประมวลรัษฎากร มาตรา 118 เอกสารที่เป็นตราสารที่ประมวลรัษฎากรบังคับให้ต้องปิดอากรแสตมป์ให้ครบถ้วน และขีดฆ่าให้ถูกต้องนั้น ถ้าไม่ได้ปิดให้ครบถ้วนหรือไม่ได้ขีดฆ่าให้ถูกต้องยังใช้เป็นพยานหลักฐานในคดีแพ่งไม่ได้จนกว่าจะไปปิดให้ครบ ขีดฆ่าให้ถูกต้อง

พยานหลักฐานอิเล็กทรอนิกส์เนื่องจากกฎหมายของแต่ละประเทศในเรื่องของการนำเสนอหลักฐานนั้นมีความแตกต่างกัน ดังนั้นการนำหลักฐานดิจิทัลไปใช้ในชั้นศาลซึ่งเป็นกฎที่มีการคิดค้น และพัฒนาในต่างประเทศจนได้รับการยอมรับมากที่สุด ซึ่งมีด้วยกันทั้งหมด 4 ข้อ¹² ดังนี้คือ

1) ความสมบูรณ์ของหลักฐาน (Preservation) ในกรณีที่หลักฐานเป็นสำเนาที่สร้างขึ้นมาจากเครื่องมือใด ๆ ก็ตามต้องสามารถตรวจสอบได้ว่ามีต้นฉบับมาจากที่ใด บางครั้งตัวต้นฉบับอาจถูกลบไปโดยเจตนาของผู้กระทำผิด จึงต้องใช้การกู้ข้อมูลนั้นกลับมาซึ่ง ไม่ว่าหลักฐานนี้จะได้มาจากการทำสำเนา หรือการกู้ข้อมูลก็จะต้องมีความถูกต้องตรงกับต้นฉบับแบบบิตต่อบิต ซึ่งการตรวจสอบความถูกต้องของสำเนานี้ใช้การตรวจสอบที่เรียกว่า Error Check Sum ที่สามารถใช้ตรวจสอบความถูกต้องของข้อมูลนั้นได้ซึ่งวิธีการนี้สามารถทำให้รู้ได้ว่าสำเนาหลักฐานนั้น ได้มีถูกเปลี่ยนแปลงมากก่อนหรือไม่ โดยการตรวจสอบค่าของ CRC ซึ่งค่านี้จะต้องมีค่าเหมือนกับไฟล์ที่มีต้นฉบับจึงจะถือว่าไฟล์สำเนาดังกล่าวนั้นมีความสมบูรณ์ ซึ่งโอกาสที่ค่า CRC ของแต่ละไฟล์จะเหมือนกันโดยบังเอิญนั้นมีแค่ 1 ใน 4 ล้านเท่านั้นซึ่งทำให้วิธีสามารถตรวจสอบความสมบูรณ์ของหลักฐานได้ดีที่สุด

2) ระบุที่มาของหลักฐานได้ (Identification) หลักฐานดิจิทัลต้องสามารถระบุได้ว่าเป็นรูปแบบใด? , ได้มาจากที่ใด? , ใช้วิธีการอย่างไร? อย่างเช่น การเก็บหลักฐานที่เป็นไฟล์จากฮาร์ดดิสก์ หรือซีดี ซึ่งในที่นี้ตัวฮาร์ดดิสก์ หรือซีดีนั้นไม่ใช่ตัวหลักฐาน แต่เป็นเพียงสิ่งที่เก็บหลักฐานไว้ การระบุที่มาของไฟล์จึงมีความสำคัญเพราะหลักฐานที่บ่งชี้ว่าไฟล์นี้ได้มาจากอุปกรณ์ใด? และไฟล์นี้ถูกกู้ขึ้นมาด้วยวิธีอะไร? ซึ่งทั้งหมดนี้จะนำไปเชื่อมโยงกับหลักฐานอื่น หรือบุคคลที่เกี่ยวข้อง

¹² หลักการนำหลักฐานดิจิทัลหรืออิเล็กทรอนิกส์ไปใช้ในทางกฎหมาย, เข้าถึงได้จาก

http://www.orionforensics.com/w_th_page/digitallaw_th.php

ได้ ดังนั้นหลักฐานที่เก็บมาได้นั้นจะต้องมีการระบุที่มา เช่น ฮาร์ดดิสก์ของนาย ก และวิธีการได้มาของหลักฐานอย่างชัดเจนเพื่อให้สามารถตรวจสอบความถูกต้องได้

3) บุคคลผู้ที่ดูแล หรือเก็บหลักฐานต้องเป็นผู้เชี่ยวชาญ (Providing Expert) บุคคลผู้ที่ดูแลหรือเก็บหลักฐานในที่นี้จะต้องเป็นผู้เชี่ยวชาญที่ได้รับการฝึกอบรมในด้านของ Computer Forensic มากแล้ว ซึ่งบุคคลนี้จะเป็นผู้รับผิดชอบในการดูแล และตรวจสอบหลักฐานให้มีความถูกต้อง พร้อมกับป้องกันบุคคลอื่นเข้ามาแก้ไข หรือสร้างความเสียหายให้กับหลักฐานด้วย นอกจากนี้การพิจารณาคดีในชั้นศาลส่วนใหญ่บุคคลกลุ่มนี้จะเป็นผู้ที่นำหลักฐานไปแสดงต่อศาลในระหว่างการพิจารณาคดี ซึ่งหากว่าไม่ใช่ผู้เชี่ยวชาญด้าน Computer Forensic แล้วความน่าเชื่อถือของหลักฐานที่ได้มาก็จะลดลง ซึ่งในจุดนี้จัดเป็นเรื่องที่สำคัญไม่แพ้ข้ออื่นเลยทีเดียว

4) หลักฐานต้องได้รับการตรวจสอบด้วยกระบวนการทางกฎหมาย (Rules of Evidence) ในส่วนนี้จะเป็นการตรวจสอบทางกฎหมายที่ขึ้นอยู่กับ กฎหมายในบางประเทศว่าจะมีการตรวจสอบที่มา และความถูกต้องของหลักฐานว่าเป็นอย่างไร

2.2 ข้อมูลอิเล็กทรอนิกส์

ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 กำหนดความหมายของข้อมูลอิเล็กทรอนิกส์ไว้ดังนี้

2.2.1 “ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อมูลที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์จดหมายอิเล็กทรอนิกส์โทรเลข โทรพิมพ์ หรือโทรสารโดยคำว่า “ข้อความ” ไม่ได้หมายถึงตัวหนังสือเท่านั้น แต่ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ.2544 “ข้อความ” หมายความว่า เรื่องราวหรือ ข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ ดังนั้น ข้อมูลอิเล็กทรอนิกส์นี้จึงอาจเป็นแหล่งข้อมูลทุกอย่าง ที่สามารถสื่อความหมายให้มนุษย์สามารถเข้าใจได้

ส่วนคำว่า “อิเล็กทรอนิกส์” นั้น หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น

ความหมายของข้อมูลอิเล็กทรอนิกส์ตามกฎหมายฉบับนี้ไม่ได้จำกัดอยู่เฉพาะข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการติดต่อสื่อสารเท่านั้น แต่มุ่งประสงค์ให้ครอบคลุมถึงข้อมูลหรือบันทึก

ที่สร้างขึ้นโดยคอมพิวเตอร์ แม้จะไม่ได้ใช้เป็นตัวในการติดต่อสื่อสารกับบุคคลอื่นก็ตาม และวิธีการทางอิเล็กทรอนิกส์ในที่นี้รวมถึงพัฒนาการทางเทคโนโลยีลักษณะอื่นที่คล้ายคลึงกันในอนาคต ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กำหนดความหมายของข้อมูลคอมพิวเตอร์ไว้ ซึ่งหมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ด้วย

ดังนั้น “ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

2.2.2 ลักษณะและประเภทของข้อมูลอิเล็กทรอนิกส์

ข้อมูลอิเล็กทรอนิกส์นั้น อาจบันทึกอยู่ในคอมพิวเตอร์ กล้องถ่ายรูป กล้องถ่ายภาพยนตร์ วีดีทัศน์ ฟิล์ม เครื่องบันทึกเสียง แต่ข้อมูลอิเล็กทรอนิกส์ที่บันทึกในคอมพิวเตอร์มีลักษณะพิเศษและยังมีประสิทธิภาพมากกว่าเดิม เพราะการเดินทางของสื่อะนั้น ไม่มีขอบเขตจำกัดไร้พรมแดนและมีผลในทันที นอกจากนี้ยังมีประสิทธิภาพในการประมวลผลโดยเฉพาะในทางคณิตศาสตร์และในทางวิทยาศาสตร์อื่น ๆ โดยสามารถแสดงคำตอบและผลลัพธ์ออกมาซึ่งอาจค้นดูได้ และอ่านเป็นภาษามนุษย์ได้ด้วย

ข้อมูลอิเล็กทรอนิกส์จะอยู่ในรูปของแม่เหล็กไฟฟ้า ไม่มีรูปร่าง อาจปรากฏในรูปของสื่ออิเล็กทรอนิกส์ที่วิ่งตามสายโทรศัพท์ และจับต้องไม่ได้ แต่อาจให้แสดงผลปรากฏออกมาให้มีรูปร่างเห็นได้โดยต้องอาศัยอุปกรณ์ เครื่องมือใด ๆ เป็นสื่อกลางช่วยประมวลผลความหมายของข้อมูลออกมา การมีธรรมชาติและลักษณะเฉพาะดังกล่าวนี้ ทำให้ยากแก่การรวบรวมพยานหลักฐาน เพราะข้อมูลนั้นเป็นสิ่งที่อยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลอื่น ในระบบเลขฐานสอง คือแสดงด้วยสัญลักษณ์เลข 0 และ 1 แต่ไม่สามารถแสดงให้ปรากฏเป็นความหมายบนเอกสารหรือสิ่งที่สามารถสัมผัสทางสายตาได้ นอกจากข้อมูลอิเล็กทรอนิกส์จะเป็นสิ่งที่ไม่มีรูปร่างแล้วยังมีธรรมชาติที่สามารถถูกดัดแปลงแก้ไขข้อมูล ถูกลบหรือกำจัดหรือถูกทำลายได้ง่าย ในบางครั้งถูกตั้งโปรแกรมให้ทำลายตนเองได้ด้วย สิ่งนี้อาจมีผลกระทบต่องานข้อมูลอิเล็กทรอนิกส์ อาจเป็นการกระทำของมนุษย์ที่เข้ามาแก้ไขเปลี่ยนแปลงข้อมูล หรืออาจเกิดจากธรรมชาติ เช่น ความร้อนจัด เย็นจัด สนามแม่เหล็กไฟฟ้า เป็นต้น

โดยทั่วไปแล้วในสภาพแวดล้อมของระบบคอมพิวเตอร์หรือระบบในเครือข่ายคอมพิวเตอร์ พยานหลักฐานอิเล็กทรอนิกส์ คือ สารสนเทศ (Information) หรือข้อมูล (Data) ที่อาจมีประโยชน์ต่อการสืบสวนสอบสวน ซึ่งสารสนเทศและข้อมูลจะถูกเก็บบันทึกไว้ในอุปกรณ์อิเล็กทรอนิกส์ได้แก่ คอมพิวเตอร์ โทรศัพท์มือถือ เป็นต้น หรือถูกส่งไปยังแหล่งอื่นโดยอุปกรณ์

ดังกล่าวเช่นเดียวกัน พยานหลักฐานดังกล่าวจะเกิดขึ้นก็ต่อเมื่อได้มีการรวบรวมข้อมูลหรืออุปกรณ์อิเล็กทรอนิกส์และจัดเก็บรักษาเพื่อการตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์สามารถส่งข้ามประเทศอื่นทั่วโลกได้โดยง่ายและรวดเร็วโดยผ่านระบบเครือข่ายอื่นที่มีสภาพอบบางสามารถถูกแก้ไขเปลี่ยนแปลง ทำลาย หรือทำให้เสียหายได้ง่ายกว่าพยานหลักฐานประเภทอื่นๆ เช่น พยานหลักฐานที่เป็นวัตถุที่จับต้องได้เป็นต้น ข้อมูลอิเล็กทรอนิกส์หรือข้อมูลดิจิทัลมีอยู่หลายประเภทซึ่งแต่ละประเภทอาจมีสารสนเทศที่อาจเป็นประโยชน์ในการสืบสวนความผิดทางอาญาและนำมาใช้เป็นพยานหลักฐานเพื่อพิสูจน์ความผิดของผู้ต้องหาว่ากระทำความผิดได้ ในประเทศสหรัฐอเมริกาคณะกรรมการที่ปรึกษาได้ให้ความหมายของคำว่าข้อมูลคอมพิวเตอร์และสารสนเทศในรูปแบบดิจิทัลหรืออิเล็กทรอนิกส์อื่นๆ ไว้อย่างกว้างๆ โดยให้ความหมายรวมถึงแฟ้มไปรษณีย์เสียง (Voice Mail Files) แฟ้มไปรษณีย์เสียงสำรอง (Backup Voice Mail Files) แฟ้มและไปรษณีย์อิเล็กทรอนิกส์หรืออีเมล (E-mail Messages and Files) แฟ้มอีเมลสำรอง (Backup E-mail Files) อีเมลที่ถูกลบทิ้ง (Deleted E-mail) แฟ้มข้อมูลชั่วคราว (Temporary Files) แฟ้มประวัติระบบ (System History Files) สารสนเทศของเว็บไซต์ที่เก็บอยู่ในรูปแบบของข้อความ (Text) รูปภาพ (Graphics) หรือเสียง (Audio) แฟ้มลงบันทึกเข้าออกเว็บไซต์ (Web Site Log Files) แฟ้มแคช (Cache Files) คุกกี้ (Cookies) และสารสนเทศอื่นๆ ที่บันทึกขึ้นโดยอุปกรณ์อิเล็กทรอนิกส์

จากข้างต้นจึงอาจแบ่งข้อมูลอิเล็กทรอนิกส์ได้ ดังนี้

1. แบ่งตามลักษณะการสร้าง

1.1 ข้อมูลอิเล็กทรอนิกส์ที่เพียงจัดเก็บไว้ในระบบคอมพิวเตอร์ ซึ่งมนุษย์เป็นผู้สร้างข้อมูลดังกล่าวขึ้น

1.2 ข้อมูลอิเล็กทรอนิกส์ที่สร้างขึ้นโดยระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ ความแตกต่างของทั้งสองประเภทคือข้อมูลอิเล็กทรอนิกส์นั้นมนุษย์หรือเครื่องคอมพิวเตอร์เป็นผู้สร้างข้อความในข้อมูลอิเล็กทรอนิกส์นั้น ฉะนั้นข้อมูลที่จัดเก็บไว้ในระบบคอมพิวเตอร์ได้แก่ แฟ้มไปรษณีย์เสียง แฟ้มไปรษณีย์เสียงสำรอง แฟ้มอีเมล แฟ้มอีเมลสำรอง อีเมลที่ถูกลบทิ้ง แฟ้มข้อมูลแถบบันทึกสำรองและถาวร แลสารสนเทศของเว็บไซต์ที่เก็บอยู่ในรูปแบบของข้อความ รูปภาพหรือเสียง สำหรับข้อมูลอิเล็กทรอนิกส์ที่สร้างขึ้นโดยระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ได้แก่ แฟ้มโปรแกรม แฟ้มข้อมูลชั่วคราว แฟ้มประวัติระบบ แฟ้มลงบันทึกเข้าออกเว็บไซต์ แฟ้มแคช และคุกกี้เป็นต้น

1.3 ข้อมูลอิเล็กทรอนิกส์ที่ประกอบด้วยข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บไว้ในระบบคอมพิวเตอร์และที่สร้างขึ้นโดยระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ทั้งสองประเภท ตัวอย่างเช่น ข้อมูลอิเล็กทรอนิกส์ที่เป็นแผนภูมิ (Chart) ซึ่งเป็นผลลัพธ์ที่ได้จากการทำงานของ

โปรแกรมตารางการทำงานหรือคำนวณ (Spreadsheet Program) เป็นต้น ข้อมูลอิเล็กทรอนิกส์ดังกล่าวเป็นผลที่ได้จากการที่ระบบคอมพิวเตอร์ประมวลผลข้อมูลตัวเลขต่างๆ ที่มนุษย์ใส่เข้าไปในระบบคอมพิวเตอร์

2. แบ่งตามลักษณะความซับซ้อน

การแบ่งประเภทของข้อมูลอิเล็กทรอนิกส์ตามลักษณะความซับซ้อนนี้ จะมีผลต่อการรับฟังพยานหลักฐาน ในเรื่องของการรับรองความถูกต้องแท้จริงของข้อมูลอิเล็กทรอนิกส์ ยิ่งข้อมูลมีความซับซ้อนมากขึ้นก็ยิ่งต้องมีการในการรับรองความถูกต้องแท้จริงที่น่าเชื่อถือมากขึ้น และอาจต้องมีบุคคลและอุปกรณ์ต่าง ๆ เข้ามาเกี่ยวข้องหลายอย่าง

2.1 ข้อมูลอิเล็กทรอนิกส์ในระบบเครือข่ายข้อมูลอิเล็กทรอนิกส์ ที่อยู่ในระบบเครือข่ายนี้จะมีการรับส่งกันไปมาได้ง่ายและอาจเก็บรักษาอยู่ในฐานข้อมูลหลายแห่ง ขึ้นอยู่กับประเภทของระบบเครื่อข่ายนั้น ๆ ซึ่งก็อาจทำให้มีข้อมูลอิเล็กทรอนิกส์เดียวกันอยู่ในข้อมูลหลายแห่ง ,ข้อมูลอิเล็กทรอนิกส์ในระบบอินเทอร์เน็ต หากมีการส่งหรือรับข้อมูลกัน ก็จะมีข้อมูลอิเล็กทรอนิกส์เก็บอยู่ที่เครื่องคอมพิวเตอร์ของผู้ส่งและเครื่องคอมพิวเตอร์ของผู้ให้บริการอินเทอร์เน็ตทั้งผู้ให้บริการอินเทอร์เน็ตของผู้รับและผู้ส่ง

2.2 ข้อมูลอิเล็กทรอนิกส์ที่ไม่อยู่ในระบบเครือข่ายข้อมูลอิเล็กทรอนิกส์ที่ไม่อยู่ในระบบเครือข่ายนี้อาจเป็นข้อมูลที่เก็บไว้ในเครื่องคอมพิวเตอร์ หรือสื่อบันทึกข้อมูลใดๆ ที่ไม่ได้เชื่อมต่อกับระบบเครือข่าย ซึ่งก็จะมีขอบเขตที่จะค้นหาน้อยกว่าข้อมูลในระบบเครือข่ายซึ่งก็เป็นผลดีในแง่ของการค้นหาทำได้ง่ายแต่ก็มีข้อเสียเพราะหากข้อมูลสูญหายไปอาจหาไม่ได้อีก ในขณะที่ระบบเครือข่ายอาจมีการรับส่งและเก็บไว้ที่เครื่องคอมพิวเตอร์หลายเครื่อง นอกจากนี้ข้อมูลอิเล็กทรอนิกส์ที่มีการส่งและรับฝ่ายเดียว เช่น โทรศัพท์ การกระจายเสียง ก็อาจค้นหาข้อมูลได้จำกัด เฉพาะที่ผู้ส่งเท่านั้น ในส่วนของเครื่องมือและอุปกรณ์ของผู้รับเช่น โทรศัพท์วิทยุ หากไม่มีการสำเนาข้อมูลไว้ต่างหากก็จะไม่มีข้อมูลอิเล็กทรอนิกส์นั้นเหลืออยู่

3. แบ่งตามลักษณะการใช้เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

3.1 ข้อมูลอิเล็กทรอนิกส์ในเครื่องมือและอุปกรณ์ที่ใช้เป็นปกติ กรณีของข้อมูลอิเล็กทรอนิกส์ที่เกิดขึ้นจากเครื่องมือและอุปกรณ์นี้ หากเป็นการใช้งานเครื่องมือและอุปกรณ์ตามปกติ ไม่ว่าจะเป็นการใช้งานตามปกติของภาคราชการ

2.3 สถานะทางกฎหมายและการรับฟังของข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน

การรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน ในการรับฟังพยานหลักฐานอิเล็กทรอนิกส์นั้นในคดีแพ่งประมวลกฎหมายวิธีพิจารณาความแพ่งมิได้บัญญัติแนวทางในการรับฟังพยานหลักฐาน

อิเล็กทรอนิกส์ไว้ซึ่งทำให้การดำเนินคดีที่มีการอ้างพยานหลักฐานอิเล็กทรอนิกส์นั้นเกิดความไม่ชัดเจนในการที่ศาลจะใช้ดุลพินิจในการรับฟังพยานหลักฐานอิเล็กทรอนิกส์

ต่อมาจึงได้มีการบัญญัติพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ออกมาเพื่อกำหนดแนวทางในการรับฟังพยานหลักฐานอิเล็กทรอนิกส์

2.3.1 การรับฟังพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ในคดีแพ่งที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์นั้น พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์มาตรา 10 บัญญัติว่า “ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

(1) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างความเสร็จสมบูรณ์ และ

(2) สามารถแสดงข้อความนั้นในภายหลังได้ความถูกต้องของข้อความตาม (1) ให้พิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงใดของข้อความ เว้นแต่การรับรองหรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใดๆที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงผลข้อความซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้นในการวินิจฉัยความน่าเชื่อถือของวิธีการรักษาความถูกต้องของข้อความตาม (1) ให้พิจารณาถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง รวมทั้งวัตถุประสงค์ของการสร้างความนั้นในกรณีที่มีการทำสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ตามวรรคหนึ่ง

สำหรับใช้อ้างอิงข้อความของข้อมูลอิเล็กทรอนิกส์ หากสิ่งพิมพ์ออกนั้นมีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์ และมีการรับรองสิ่งพิมพ์ออกโดยหน่วยงานที่มีอำนาจตามที่คณะกรรมการประกาศกำหนดแล้ว ให้ถือว่าสิ่งพิมพ์ออกดังกล่าวใช้แทนต้นฉบับได้”

จากบทบัญญัติในมาตรา 10 แห่งพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ เป็นบทบัญญัติที่มีการแก้ไขเพิ่มเติมในปี พ.ศ. 2551 โดยเพิ่มในส่วนของวรรคสี่ขึ้นมา โดยจะเห็นได้ว่ามาตรา 10 แห่งพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ เป็นบทบัญญัติที่กำหนดขึ้นมาเพื่อเป็นแนวทางในการกลั่นกรองความถูกต้องแท้จริงของข้อมูลอิเล็กทรอนิกส์ที่ถูกเสนอขึ้นมาในการพิจารณาคดีโดยเริ่มตั้งแต่ในชั้นการเก็บรักษาหลักฐานตามวรรคหนึ่ง สิ่งที่ต้องพิจารณาถึงความถูกต้องแท้จริงในวรรคสองและวรรคสาม และในวรรคสี่ที่บัญญัติเพิ่มขึ้นมาเพื่อเป็นการตัดปัญหาเรื่องความถูกต้องแท้จริงของสิ่งพิมพ์ออกที่คู่ความนำมาสู่ศาล แต่อย่างไรก็ตามในทางปฏิบัติยังไม่มีประกาศจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมายให้หน่วยงานใดเป็นผู้มีอำนาจในการรับรอง

บทบัญญัติตามมาตรา 11 แห่งพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งบัญญัติว่า “ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมาย เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

ในการชี้แจงน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิจารณาถึง ความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษา ความครบถ้วน และไม่มี การเปลี่ยนแปลงของข้อความลักษณะหรือวิธีการที่ใช้ ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวงให้น้ำความในวรรคหนึ่ง มาใช้บังคับกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย”

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ได้กำหนดห้ามมิให้ปฏิเสธการรับฟังข้อมูล อิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุที่ข้อมูลนั้นอยู่ใน รูปข้อมูลอิเล็กทรอนิกส์ ทั้งนี้เพราะนอกจากศาลชั้นอุทธรณ์ที่มีข้อกำหนดของตนเองแล้ว ศาลอื่น ๆ เป็นดุลพินิจของศาลที่จะรับฟังหรือไม่ก็ได้ เพราะมิได้มีหลักเกณฑ์บัญญัติชัดเจนว่าต้องรับฟัง แต่ เมื่อบัญญัติให้ต้องรับฟังแล้ว มิได้หมายความว่าจะมีน้ำหนักน่าเชื่อถือเสมอไป

2.3.2 การรับฟังพยานหลักฐานอิเล็กทรอนิกส์ในคดีทรัพย์สินทางปัญญาและการค้า ระหว่างประเทศ และคดีล้มละลาย ปัจจุบันศาลทรัพย์สินทางปัญญา และการค้าระหว่างประเทศ และ ศาลล้มละลายกลาง ได้ออกข้อกำหนดเกี่ยวกับการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ โดยกำหนดไว้ดังนี้

ข้อกำหนดคดีทรัพย์สินทางปัญญา และการค้าระหว่างประเทศ พ.ศ. 2540 ข้อ 33 ศาลอาจริับฟังข้อมูลที่ บันทึกลงโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์เป็นพยานหลักฐานในคดีได้ หาก

1) การบันทึกข้อมูลโดยเครื่องคอมพิวเตอร์ หรือการประมวลโดยเครื่อง คอมพิวเตอร์เป็นการกระทำตามปกติในการประกอบกิจการของผู้ใช้เครื่องคอมพิวเตอร์

2) การบันทึกและการประมวลผลข้อมูลเกิดจากการใช้เครื่องคอมพิวเตอร์ ปฏิบัติงานตามขั้นตอนการทำงานของเครื่องคอมพิวเตอร์อย่างถูกต้องและหากมีกรณีการทำงานของ เครื่องคอมพิวเตอร์ขัดข้องก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

การกระทำตามปกติของผู้ใช้ตาม (1) และความถูกต้องของการบันทึกข้อมูลและการ ประมวลผลข้อมูลตาม (2) ต้องมีการรับรองของบุคคลที่เกี่ยวข้องหรือดำเนินการนั้น

ข้อกำหนดศาลล้มละลาย พ.ศ. 2542 ข้อ 18 ศาลอาจริับฟังข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์ หรือประมวลผลโดยเครื่องคอมพิวเตอร์เป็นพยานหลักฐานในคดีได้ หาก

(1) การบันทึกข้อมูลโดยเครื่องคอมพิวเตอร์ หรือการประมวลผลโดยเครื่องคอมพิวเตอร์ เป็นการกระทำตามปกติในการประกอบกิจการของผู้ใช้เครื่องคอมพิวเตอร์

(2) การบันทึกและการประมวลผลข้อมูลเกิดจากการใช้เครื่องคอมพิวเตอร์ปฏิบัติงาน ตามขั้นตอนการทำงานของเครื่องคอมพิวเตอร์อย่างถูกต้องและหากมีกรณีการทำงานของเครื่องคอมพิวเตอร์ขัดข้องก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

การกระทำตามปกติของผู้ใช้ตาม (1) และความถูกต้องของการบันทึกข้อมูลและการประมวลผลข้อมูล ตาม (2) ต้องมีการรับรองของบุคคลที่เกี่ยวข้องหรือดำเนินการนั้น”

จะเห็นได้ว่าข้อกำหนดของศาลชั้นอุทธรณ์ทั้งสองนั้นเป็นการนำหลักในการรับรองความแท้จริงของพยานอิเล็กทรอนิกส์ในกฎหมายต่างประเทศ ซึ่งเป็นลักษณะเดียวกับหลักการในกฎหมายสหรัฐอเมริกาในเรื่องข้อยกเว้นพยานบอกเล่าของบันทึกธุรกิจที่จะต้องเป็นการบันทึกตามปกติทางธุรกิจ และการรับรองความถูกต้องแท้จริงของการประมวลผลของคอมพิวเตอร์โดยโปรแกรมที่บรรจุชุดคำสั่งไว้ แต่ของไทยเปิดกว้างกว่า กล่าวคือแม้จะเกิด error ในโปรแกรมคอมพิวเตอร์แต่หากไม่กระทบต่อความถูกต้องในการบันทึก อีกทั้งมิได้กำหนดว่าการบันทึกนั้นจะต้องเป็นการกระทำโดยคอมพิวเตอร์เอง หรือบันทึกโดยมนุษย์ ก็สามารถรับฟังได้หากเป็นไปตามข้อกำหนด

2.3.3 การรับฟังพยานหลักฐานอิเล็กทรอนิกส์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในส่วนของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้น มาตรา 25 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 บัญญัติว่า“ข้อมูล ข้อมูลคอมพิวเตอร์หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มีได้เกิดจากการจงใจ มีคำมั่นสัญญา ชูเชิญ หลอกลวง หรือโดยมิชอบประการอื่น”

ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่จะถือเป็นพยานหลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัตินี้ได้นั้นต้องเป็นไปตามบทนิยามมาตรา 2 ซึ่งบัญญัติว่า

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทาง อิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณระยะเวลาชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น”

มาตรา 25 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นบทบัญญัติที่เสริมมาตรา 226 แห่งประมวลกฎหมายวิธีพิจารณาความอาญานอกจากพยานบุคคล พยานวัตถุและพยานเอกสารแล้ว ข้อมูลคอมพิวเตอร์ก็รับฟังและอ้างเป็นพยานหลักฐานได้ตามกฎหมายวิธีพิจารณาความอาญา หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน เพื่อเป็นการตัดปัญหาว่าพยานคอมพิวเตอร์เป็นพยานประเภทใดส่วนการตรวจสอบพยานหลักฐานอาชญากรรมหลักตามมาตรา 226 กฎหมายวิธีพิจารณาความอาญาก็ต้องเป็นพยานหลักฐานที่มีได้เกิดขึ้นจากการจงใจ มีคำมั่นสัญญา ชูเชื้อหลอกลวงหรือโดยมิชอบประการอื่น³²และศาลอาจใช้อำนาจตามมาตรา 104 แห่งกฎหมายวิธีพิจารณาความแพ่งประกอบกับมาตรา 15 แห่งกฎหมายวิธีพิจารณาความอาญาที่ให้ศาลมีอำนาจเต็มในอันที่จะวินิจฉัยว่าพยานหลักฐานที่คู่ความนำมาสืบนั้นจะเกี่ยวกับประเด็นและเป็นอันเพียงพอให้เชื่อฟังเป็นที่ยุติได้หรือไม่ แล้วพิพากษาคดีไปตามนั้น ซึ่งเป็นการใช้ดุลพินิจของศาลที่จะรับฟังพยานหลักฐานนั้นหรือไม่ก็ได้

มาตรา 25 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ข้อมูลทางอิเล็กทรอนิกส์ หรือข้อมูลจราจรทางคอมพิวเตอร์นั้นจะต้องเป็นข้อมูลที่พนักงานเจ้าหน้าที่ได้มาโดยอำนาจหน้าที่ตามมาตรา 18 ประกอบมาตรา 19 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หากไม่ปฏิบัติให้ถูกต้องก็ไม่สามารถรับฟังได้ บทบัญญัตินี้เป็นการควบคุมการได้มาซึ่งพยานหลักฐานของเจ้าหน้าที่เท่านั้น จำเลยจึงอาจอ้างข้อมูลคอมพิวเตอร์เป็นหลักฐานโดยไม่อยู่ในบังคับของ มาตรา 25

พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้จะต้องเป็นผู้ที่ได้รับการแต่งตั้งจากรัฐมนตรีจึงมีประกาศจากรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเรื่องหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีความชัดเจนและเป็นไปอย่างมีประสิทธิภาพโดยอาศัยอำนาจตามความใน มาตรา 28 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550 รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้กำหนดหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ดังต่อไปนี้

1. “พนักงานเจ้าหน้าที่”หมายความว่าผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 “รัฐมนตรี”หมายความว่ารัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

2. พนักงานเจ้าหน้าที่ต้องมีคุณสมบัติดังต่อไปนี้

(1) มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์

(2) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือ รัฐประศาสนศาสตร์

(3) ผ่านการอบรมทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) สืบสวน สอบสวน และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) ตามภาคผนวกท้ายประกาศนี้และ

(4) มีคุณสมบัติอื่นอย่างหนึ่งอย่างใด ดังต่อไปนี้

ก. รับราชการหรือเคยรับราชการไม่น้อยกว่าสองปีในตำแหน่งเจ้าหน้าที่ตรวจพิสูจน์ พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์หรือพยานหลักฐานอิเล็กทรอนิกส์

ข. สำเร็จการศึกษาตามข้อ 2 (2) ในระดับปริญญาตรีและมีประสบการณ์ที่เป็นประโยชน์ ต่อการปฏิบัติงานตามพระราชบัญญัตินี้ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสี่ปี

ค. สำเร็จการศึกษาตามข้อ 2 (2) ในระดับปริญญาโท หรือสอบไล่ได้เป็นเนติบัณฑิต ตามหลักสูตรของสำนักงานกฤษฎีกาหมายแห่งเนติบัณฑิตยสภา และมีประสบการณ์ที่เป็นประโยชน์ ต่อการปฏิบัติงานตาม พระราชบัญญัตินี้ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสามปี

ง. สำเร็จการศึกษาตามข้อ 2 (2) ในระดับปริญญาเอก หรือมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงาน ตามพระราชบัญญัตินี้ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสองปี

จ. เป็นบุคคลที่ทำงานเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศการตรวจพิสูจน์ หลักฐานทางคอมพิวเตอร์หรือมีประสบการณ์ในการดำเนินคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ไม่น้อยกว่าสองปี

3. ในกรณีที่มีความจำเป็นเพื่อประโยชน์ของทางราชการในการสืบสวนและสอบสวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จำเป็นต้องมีบุคลากรซึ่งมีความรู้ความชำนาญหรือ ประสบการณ์สูง เพื่อดำเนินการสืบสวนและสอบสวนการกระทำผิดหรือคดีเช่นนั้น หรือเป็นบุคลากรในสาขาที่ขาดแคลน รัฐมนตรีอาจยกเว้นคุณสมบัติตามข้อ 2 ไม่ว่าทั้งหมดหรือบางส่วน สำหรับการบรรจุและแต่งตั้งบุคคลใดเป็นการเฉพาะก็ได้

4. การแต่งตั้งบุคคลหนึ่งบุคคลใดเป็นพนักงานเจ้าหน้าที่ให้แต่งตั้งจากบุคคลซึ่งมีคุณสมบัติตามข้อ 2 หรือข้อ 3 โดยบุคคลดังกล่าวต้องผ่านการประเมินความรู้ความสามารถหรือทดสอบตามหลักสูตรและหลักเกณฑ์ที่รัฐมนตรีประกาศกำหนดการแต่งตั้งบุคคลใดเป็นพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ดำรงตำแหน่ง ในวาระคราวละ 4 ปีและการแต่งตั้งให้ประกาศในราชกิจจานุเบกษา

5. พนักงานเจ้าหน้าที่ต้องไม่มีลักษณะต้องห้าม ดังต่อไปนี้

- (1) เป็นบุคคลล้มละลาย บุคคลไร้ความสามารถ หรือบุคคลเสมือนไร้ความสามารถ
- (2) เป็นสมาชิกสภาผู้แทนราษฎร สมาชิกวุฒิสภา ข้าราชการการเมือง สมาชิกสภาท้องถิ่น ผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งที่รับผิดชอบในการบริหารพรรคการเมือง ที่ปรึกษา พรรคการเมือง หรือเจ้าหน้าที่ในพรรคการเมือง
- (3) เป็นผู้อยู่ระหว่างถูกสั่งให้พักราชการหรือถูกสั่งให้ออกจากราชการ ไว้ก่อน
- (4) ถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐหรือรัฐวิสาหกิจ เพราะทำผิดวินัย หรือรัฐมนตรีให้ออกจากการเป็นพนักงานเจ้าหน้าที่เพราะมีความประพฤติเสื่อมเสีย บกพร่องหรือไม่สุจริตต่อหน้าที่หรือหย่อนความสามารถ
- (5) ได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิด ที่กระทำโดยประมาท หรือความผิดลหุโทษ บทบัญญัตินี้เป็นการควบคุมการได้มาซึ่งพยานหลักฐานของเจ้าหน้าที่เท่านั้นจำเลยจึงอาจอ้างข้อมูลคอมพิวเตอร์เป็นหลักฐานโดยไม่อยู่ในบังคับของ มาตรา 25 เกิดปัญหาขึ้นว่าข้อมูลคอมพิวเตอร์ที่ได้มานั้นมีความน่าเชื่อถือเพียงใด จะถือเป็นพยานหลักฐานตามกฎหมายวิธีพิจารณาความอาญาประเภทใดและมีวิธีการนำเสนออย่างไร และการที่ศาลมีอำนาจเต็มในการใช้ดุลพินิจในการวินิจฉัยที่จะรับฟังพยานหลักฐานที่คู่ความนำมาสืบนั้นอาจทำให้เกิดปัญหาขึ้นได้ในกรณีที่พยานหลักฐานที่เป็นบันทึกหรือข้อมูลอิเล็กทรอนิกส์ซึ่งต้องอาศัยทักษะอย่างสูงทางคอมพิวเตอร์เพื่อที่จะพิจารณาถึงความถูกต้องแท้จริงของบันทึกนั้น ซึ่งการใช้ดุลพินิจของศาลเพียงอย่างเดียวในการวินิจฉัยว่าพยานหลักฐานนั้นรับฟังได้หรือไม่ อาจไม่เพียงพอและอาจจะทำให้เกิดความไม่ยุติธรรมขึ้นกับคู่ความฝ่ายที่นำมาสืบได้

2.4 วิธีการนำสืบข้อมูลอิเล็กทรอนิกส์ในฐานะพยานหลักฐาน

2.4.1 หน้าที่ในการนำสืบ

ประมวลกฎหมายวิธีพิจารณาความอาญา. มาตรา 226 บัญญัติว่า “พยานวัตถุพยานเอกสาร หรือพยานบุคคล ซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่ไม่ได้เกิดขึ้นจากการจงใจ มีกำมันสัญญา ชูเชิญหลอกลวง หรือโดยมิชอบ

ประการอื่นและให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน”

จากหลักของ ป.วิ.อ. มาตรา 226 ถือว่า โจทก์ในคดีอาญามีหน้าที่นำสืบหรือมีภาระการพิสูจน์เสมอว่า ได้มีการกระทำความผิดอาญาเกิดขึ้นและจำเลยเป็นผู้กระทำความผิดนั้น ซึ่งในการนำพยานหลักฐานอิเล็กทรอนิกส์มานำสืบโจทก์ก็มีหน้าที่ที่จะต้องนำสืบถึงประเด็นในคดีอาญาว่าจำเลยได้กระทำความผิด ดังนั้นพยานหลักฐานที่ไม่เกี่ยวกับประเด็น ศาลมีอำนาจไม่ยอมให้นำสืบได้ เช่น คุณพินิจในการลงโทษ ศาลไม่จำเป็นต้องรับฟังจากพยานหลักฐานที่มีการนำสืบเท่านั้น ศาลอาจรับฟังจากคำร้อง คำแถลง ตลอดจนรายงานของพนักงานคุมประพฤติได้ เป็นต้น และมีข้อสังเกตดังต่อไปนี้

1. ในคดีอาญาจำเลยจะให้การปฏิเสธหรือไม่ให้การใดๆ ก็ได้ ถือว่าโจทก์มีหน้าที่นำสืบให้ครบทุกประเด็นในองค์ประกอบความผิด
2. กรณีที่จำเลยให้การรับสารภาพตามฟ้องโจทก์ทุกประการ ศาลย่อมฟังข้อเท็จจริงเป็นยุติว่าจำเลยกระทำความผิดตามฟ้องและลงโทษจำเลยได้โดยโจทก์ไม่จำเป็นต้องสืบพยานเว้นแต่เข้าด้วยข้อยกเว้นที่จะต้องมีการสืบพยานประกอบคำให้การรับสารภาพตาม ป.วิ.อ. มาตรา 176

2.4.2 การนำสืบข้อมูลอิเล็กทรอนิกส์ในฐานะพยานหลักฐาน

ในการนำ สืบพยานหลักฐานอิเล็กทรอนิกส์นั้น เนื่องจากพยานหลักฐานอิเล็กทรอนิกส์เป็นสิ่งที่ไม่มีรูปร่าง เป็นข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์ หรือระบบอิเล็กทรอนิกส์อื่น ๆ ทำให้ในการนำพยานมาสู่ศาลนั้นโจทก์ผู้นำสืบจำต้องพิจารณาว่าจะนำเสนอพยานหลักฐานในรูปแบบใด ซึ่งในทางปฏิบัตินั้นมีการนำพยานหลักฐานอิเล็กทรอนิกส์มานำสืบต่อศาลในลักษณะดังต่อไปนี้

1. การนำสืบพยานหลักฐานอิเล็กทรอนิกส์อย่างพยานเอกสารเป็นการนำข้อมูลอิเล็กทรอนิกส์ที่บันทึกไว้ในระบบคอมพิวเตอร์ ทำการประมวลผลผ่านชุดคำสั่ง และอุปกรณ์ต่างๆ โดยทำออกมาเป็น สิ่งพิมพ์ออก (print out) ซึ่งเป็นการแสดงข้อมูลออกมาในรูปของเอกสารโดยจะต้องมีคำเบิกความของผู้ที่ทำข้อมูลประกอบด้วยว่าได้มีการทำข้อมูลนั้นขึ้นมาจริงและมีเนื้อหาตรงกันกับที่แสดงอยู่ใน print out นั้น
2. การนำสืบพยานหลักฐานอิเล็กทรอนิกส์อย่างพยานวัตถุเป็นการนำสืบโดยนำระบบคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์ที่บันทึกข้อมูลอิเล็กทรอนิกส์ไว้มาสู่ศาล ซึ่งจะต้องนำระบบคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์มาเชื่อมต่อกับอุปกรณ์แสดงผลภาพออกมาให้มนุษย์สามารถเห็นและเข้าใจภาษาได้ เพื่อเป็นการพิสูจน์ว่ามีพยานหลักฐานนั้นอยู่ และฝ่ายที่นำสืบต้องแสดงให้เห็น

เห็นว่าข้อมูลที่ระบบคอมพิวเตอร์แสดงออกมานั้นเป็นข้อมูลที่ถูกต้องแท้จริง ไม่มีการแก้ไข หรือทำลายให้เกิดความเสียหาย

3. การนำสืบโดยอาศัยพยานผู้เชี่ยวชาญในการให้ความเห็นในทางวิชาการ หรืออธิบายถึงกระบวนการทำงานของระบบคอมพิวเตอร์ในการสร้างข้อมูลนั้น ซึ่งเป็นดุลพินิจของศาลที่จะเชื่อหรือไม่ก็ได้ หากเป็นคำเบิกความที่ไม่ใช่ข้อมูลในเชิงวิชาการแต่เป็นคำเบิกความเกี่ยวกับข้อเท็จจริงก็จะมีน้ำหนักมากขึ้น เนื่องจากประเทศไทยมิได้ใช้ระบบลูกขุน ดุลพินิจในการชั่งน้ำหนักพยานหลักฐานต่าง ๆ จึงเป็นของศาล

2.5 การชั่งน้ำหนักพยานหลักฐานอิเล็กทรอนิกส์

ในการพิจารณาว่าพยานหลักฐานเกี่ยวกับประเด็นหรือมีน้ำหนักเพียงพอหรือไม่นั้น มาตรา 227 วรรคหนึ่ง แห่งประมวลกฎหมายวิธีพิจารณาความอาญา “ให้ศาลใช้ดุลพินิจวินิจฉัยน้ำหนักพยานหลักฐานทั้งปวง อย่าพิพากษาลงโทษจนกว่าจะแน่ใจว่าได้มีการกระทำความผิดจริงและจำเลยเป็นผู้กระทำความผิดนั้น” โดยพยานหลักฐานนั้นต้องเป็นพยานหลักฐานที่ได้มาโดยชอบตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 และอาศัยอำนาจจากประมวลกฎหมายวิธีพิจารณาความแพ่งโดยอาศัยประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 15 ซึ่งบัญญัติว่า “วิธีพิจารณาข้อใดซึ่งประมวลกฎหมายนี้มีได้บัญญัติไว้โดยเฉพาะให้นำบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความแพ่งมาใช้บังคับเท่าที่พอจะใช้บังคับได้” ซึ่งในการการใช้ดุลพินิจวินิจฉัยความเกี่ยวข้องกับประเด็นและการชั่งน้ำหนักพยานหลักฐานนั้น ประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 104 บัญญัติว่า “ให้ศาลมีอำนาจเต็มที่ในอันที่จะวินิจฉัยว่าพยานหลักฐานที่คู่ความนำมาสืบนั้นจะเกี่ยวกับประเด็นและเป็นอันเพียงพอให้เชื่อฟังเป็นยุติหรือไม่ แล้วพิพากษาไปตามนั้น

ในการวินิจฉัยว่าพยานบอกเล่าตามมาตรา 95/1, หรือบันทึกถ้อยคำที่ผู้ให้ถ้อยคำมิได้มาศาลตาม มาตรา 120/1 วรรคสามและวรรคสี่ หรือบันทึกถ้อยคำตามมาตรา 120/2 จะมีน้ำหนักให้เชื่อได้หรือไม่เพียงใดนั้น ศาลจะต้องกระทำด้วยความระมัดระวังโดยคำนึงถึงสภาพลักษณะ และแหล่งที่มาของพยานบอกเล่าหรือบันทึกถ้อยคำนั้นด้วย”

กฎหมายได้ให้อำนาจศาลในการใช้ดุลพินิจในการชั่งน้ำหนักพยานหลักฐานตามที่ศาลเห็นสมควร ยังมีได้กำหนดหลักเกณฑ์ที่ชัดเจนในการ ชั่งน้ำหนักพยานที่เป็นข้อมูลอิเล็กทรอนิกส์ หรือบันทึกคอมพิวเตอร์ ทำให้ศาลต้องอาศัยหลักปฏิบัติ หรือประสบการณ์ของศาลเองในการพิจารณาว่าพยานหลักฐานทางอิเล็กทรอนิกส์ที่นำมาสู่กระบวนการพิจารณานั้น มีความน่าเชื่อถือหรือไม่ อีกทั้ง มาตรา 226/1 วรรคหนึ่ง แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ได้กำหนดให้อำนาจศาลในการใช้ดุลพินิจพิจารณาพยานหลักฐานที่เกิดขึ้นโดยชอบแต่ได้มาเนื่องจากการกระทำโดยมิชอบ

หรือเป็นพยานหลักฐานที่ได้มาโดยอาศัยข้อมูลที่เกิดขึ้น หรือได้มาโดยมิชอบ ในกรณีที่การรับฟังพยานหลักฐานดังกล่าวจะเป็นประโยชน์ต่อการอำนวยความสะดวกมากกว่าผลเสียที่จะเกิดจากผลกระทบต่อมาตรฐานของระบบงานยุติธรรมทางอาญาหรือสิทธิเสรีภาพพื้นฐานของประชาชน ซึ่งเป็นการเปิดโอกาสให้ศาลมากขึ้นในการพิจารณาดีในการเลือกรับฟังพยานหลักฐานเพื่อใช้ประกอบการพิจารณา โดยคำนึงถึงปัจจัยที่กำหนดไว้ในมาตรา 226/1 วรรคสอง แห่งประมวลกฎหมายวิธีพิจารณาความอาญาเป็นสำคัญ จึงขึ้นอยู่กับดุลพินิจศาลว่าจะให้ความเชื่อถือต่อพยานดังกล่าวในระดับใดโดยพิจารณาพร้อมกับเงื่อนไขการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ ซึ่งมีเพียงในศาลชำนาญพิเศษตามที่กล่าวไปแล้วข้างต้น

มาตรา 25 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นบทบัญญัติที่เสริมมาตรา 226 แห่งประมวลกฎหมายวิธีพิจารณาความอาญานอกจากพยานบุคคล พยานวัตถุและพยานเอกสารแล้ว ข้อมูลคอมพิวเตอร์ที่รับฟังและอ้างเป็นพยานหลักฐานได้ตามกฎหมายวิธีพิจารณาความอาญา หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน เพื่อเป็นการตัดปัญหาว่าพยานคอมพิวเตอร์เป็นพยานประเภทใด

ส่วนการตรวจสอบพยานหลักฐานอาสัยหลักตามมาตรา 226 ประมวลกฎหมายวิธีพิจารณาความอาญา ก็ต้องเป็นพยานหลักฐานที่มีได้เกิดขึ้นจากการจงใจ มีคำมั่นสัญญา ชูเชิญ หลอกลวง หรือโดยมิชอบประการอื่น

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ผ่านการเห็นชอบจากสภานิติบัญญัติ การลงพระปรมาภิไธย เมื่อวันที่ 10 มิถุนายน พ.ศ. 2550 และประกาศลงในราชกิจจานุเบกษาแล้ว เมื่อ 18 มิถุนายน พ.ศ. 2550 และมีผลใช้บังคับตั้งแต่ 18 กรกฎาคม พ.ศ. 2550 แบ่งออกเป็น 2 หมวด โดยหมวดแรกนั้น จะกำหนดเกี่ยวกับฐานความผิดและบทลงโทษเกี่ยวกับคอมพิวเตอร์ ส่วนหมวดที่สองนั้น จะกำหนดเกี่ยวกับพนักงานเจ้าหน้าที่ที่มีการกำหนดคำนิยามที่สำคัญไว้หลายคำ ได้แก่ “ระบบคอมพิวเตอร์”, “ข้อมูลคอมพิวเตอร์”, “ข้อมูลจราจรทางคอมพิวเตอร์”, “ผู้ให้บริการ”, “ผู้ใช้บริการ”, “พนักงานเจ้าหน้าที่”, และ “รัฐมนตรี” กำหนดลักษณะการกระทำความผิดซึ่งกระทบโดยตรงต่อการ รักษาความลับ (Confidentiality), ความครบถ้วน (Integrity), และสภาพพร้อมใช้งาน (Availability) ของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ สำหรับการกระทำความผิดที่กระทบต่อการรักษาความลับเช่น การเข้าถึงระบบคอมพิวเตอร์ของบุคคลอื่นซึ่งมีมาตรการป้องกันการเข้าถึงเอาไว้ การล่วงรู้มาตรการการป้องกันการเข้าถึงระบบคอมพิวเตอร์ (ตัวอย่างคือการล่วงรู้รหัสผ่าน (Password)) หรือรหัสลับ (secret code) เป็นต้น) การเข้าถึงข้อมูลคอมพิวเตอร์ของบุคคลอื่น หรือการดักข้อมูลคอมพิวเตอร์

ส่วนการกระทำความผิดที่กระทบต่อความครบถ้วนของระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้น ความครบถ้วนในที่นี้ หากกล่าวให้เข้าใจโดยง่ายหมายความว่า ในกรณีที่มีการป้อนหรือพิมพ์ข้อมูลคอมพิวเตอร์ไว้เช่นใด โดยทั่วไปหากจะเรียกข้อมูลคอมพิวเตอร์นั้นมาอ่านเรียกดูหรือใช้ข้อมูลดังกล่าวอีกครั้ง ข้อมูลคอมพิวเตอร์ที่อยู่หรือเก็บไว้ในคอมพิวเตอร์นั้น ก็ควรจะแสดงบนจอคอมพิวเตอร์ด้วยข้อมูลหรือข้อความที่ครบถ้วนเหมือนที่พิมพ์ หรือป้อนไว้แต่เดิม ตัวอย่างการกระทำผิดในลักษณะนี้ เช่น การรบกวนการทำงานของข้อมูลคอมพิวเตอร์ด้วยการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมข้อมูลคอมพิวเตอร์ เป็นต้น

ส่วนการกระทำความผิดที่กระทบต่อสภาพพร้อมใช้งานตามปกติของระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ เช่น การกระทำผิดด้วยการป้อนชุดคำสั่งหรือโปรแกรมคอมพิวเตอร์ที่ไม่พึงประสงค์ อาทิ “ไวรัส” ในคอมพิวเตอร์ เพื่อให้ระบบคอมพิวเตอร์ทำงานผิดเพี้ยนไปจากเดิมหรือไม่สามารถทำงานได้ตามปกติ

อย่างไรก็ตามในการกระทำผิดอันเป็นการรบกวนระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ให้ทำงานหรือแสดงผลต่างไปจากเดิมหรือไม่เป็นไปตามปกตินั้นพระราชบัญญัติก็ได้มีการกำหนดโทษหนักขึ้นในกรณีที่มีเหตุฉกรรจ์ไว้ด้วย กล่าวคือ หากการกระทำผิดก่อให้เกิดผลอันเป็นความเสียหายแก่ข้อมูลคอมพิวเตอร์ หรือกระทบต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ การบริการสาธารณะ หรือการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ หรือการกระทำดังกล่าวก่อให้เกิดอันตรายแก่ร่างกายหรือชีวิตของประชาชน ผู้กระทำผิดดังกล่าวก็ต้องรับโทษหนักขึ้น นอกจากนั้น ยังได้มีการกำหนดฐานความผิดสำหรับการจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นเพื่อใช้เป็นเครื่องมือในการกระทำผิดที่กล่าวมาข้างต้น เช่น การจงใจหรือเจตนาเผยแพร่ไวรัสที่ใช้ในการก่อให้เกิดความเสียหายหรือทำลาย ข้อมูลคอมพิวเตอร์ หรือชุดคำสั่งที่เรียกว่า spyware เพื่อไว้ใช้โจรกรรมความลับทางการค้า เป็นต้น

การกำหนดลักษณะการกระทำผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ในทางมิชอบเพื่อกระทำผิดในลักษณะต่างๆ เช่น การปลอมแปลงข้อมูลคอมพิวเตอร์, การเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จซึ่งก่อให้เกิดความตื่นตระหนกกับประชาชน, การเผยแพร่ข้อมูลคอมพิวเตอร์อันมีลักษณะลามก, การกระทำผิดของผู้ให้บริการที่มีได้ลบข้อมูลคอมพิวเตอร์อันไม่เหมาะสม, และการตัดต่อภาพอันทำให้นักคนอื่นเสียหาย

ในหมวดกำหนดอำนาจของพนักงานเจ้าหน้าที่ที่มีสาระสำคัญ ดังนี้ คุณสมบัติของพนักงานเจ้าหน้าที่, อำนาจของพนักงานเจ้าหน้าที่, การตรวจสอบการใช้อำนาจ, อำนาจสั่งการเกี่ยวกับชุดคำสั่ง

ไม่พึงประสงค์ (โปรแกรมชั่วร้าย), การควบคุมการใช้อำนาจและข้อห้ามมิให้เปิดเผยยานหลักฐานที่ได้, หน้าที่ของผู้ให้บริการในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์และการทำงานร่วมกันระหว่างพนักงานเจ้าหน้าที่ และพนักงานสอบสวน

ตามพระราชบัญญัติว่าด้วยความรับผิดชอบเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในส่วนการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในความผิดฐานหมิ่นประมาทนั้น ตามพ.ร.บ.คอมพิวเตอร์ พ.ศ.2550 ในประเด็นที่เกี่ยวข้อง เช่น มาตรา 14 “ผู้ใดกระทำด้วยประการใด ๆ ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้”

เห็นได้ว่าความผิดในลักษณะดังกล่าวนี้ มีการนำข้อมูลคอมพิวเตอร์ ซึ่งหมายถึง ข้อมูลข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย เข้าสู่ระบบคอมพิวเตอร์ “โดยมีลักษณะอันลามก” โดยคำว่า “ลามก” เป็นคำสามัญที่ไม่มีการนิยามศัพท์ แต่เป็นคำที่ใช้เป็นองค์ประกอบความผิดตามประมวลกฎหมายอาญา เช่น มาตรา 287, 287/1 เป็นต้น

ทั้งนี้ประมวลกฎหมายอาญา มาตรา 287 บัญญัติว่า “ผู้ใด (1) เพื่อความประสงค์แห่งการค้าหรือโดยการค้า เพื่อการแจกจ่ายหรือเพื่อการแสดงอวดแก่ประชาชน ทำ ผลิต มีไว้ นำเข้าหรือยังให้นำเข้าในราชอาณาจักร ส่งออกหรือยังให้ส่งออกป็นนอกราชอาณาจักร พาไปหรือยังให้พาไปหรือทำให้แพร่หลายโดยประการใด ๆ ซึ่งเอกสาร ภาพเขียน ภาพพิมพ์ ภาพระบายสี สิ่งพิมพ์ รูปภาพ ภาพโฆษณา เครื่องหมาย รูปถ่าย ภาพยนตร์ แถบบันทึกเสียง แถบบันทึกภาพหรือสิ่งอื่นใดอันลามก (2) ประกอบการค้า หรือมีส่วนหรือเข้าเกี่ยวข้องในการค้าเกี่ยวกับวัตถุหรือสิ่งของลามกดังกล่าวแล้ว จำหน่ายแจกหรือแสดงอวดแก่ประชาชน หรือให้เช่าวัตถุหรือสิ่งของเช่นนั้น (3) เพื่อจะช่วยให้แพร่หลาย หรือการค้าวัตถุหรือสิ่งของลามกดังกล่าวแล้ว โฆษณาหรือโฆษณาโดยประการใด ๆ ว่ามีบุคคลกระทำการอันเป็นความผิดตามมาตรา นี้ หรือโฆษณาหรือโฆษณาว่าวัตถุ หรือสิ่งของลามกดังกล่าวแล้วจะหาได้จากบุคคลใด หรือโดยวิธีใด ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ”

ประมวลกฎหมายอาญา มาตรา 287/1 บัญญัติว่า “ผู้ใดครอบครองสื่อลามกอนาจารเด็กเพื่อแสวงหาประโยชน์ในทางเพศสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ถ้าผู้กระทำความผิดตามวรรคหนึ่งส่งต่อซึ่งสื่อลามกอนาจารเด็กแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินเจ็ดปี หรือปรับไม่เกินหนึ่งแสนสี่หมื่นบาท หรือทั้งจำทั้งปรับ”

ซึ่งเป็นความผิดฐานเผยแพร่วัตถุอันลามก ดังนั้นข้อมูลคอมพิวเตอร์ใดจะเข้าองค์ประกอบความผิด “ลามก” หรือไม่ จึงใช้มาตรฐานเดียวกันกับความผิดตามประมวลกฎหมายอาญาทั้งสองมาตราดังกล่าวข้างต้น ศาลฎีกาได้มีคำพิพากษาไว้เป็นบรรทัดฐานหลายเรื่องแล้วในเรื่องการพิจารณาลักษณะอันลามก

เห็นได้ว่าการนำเข้าข้อมูลคอมพิวเตอร์อันมีลักษณะลามกนั้นย่อมจะต้องมีผู้เสียหายจากการนำข้อมูลดังกล่าวเข้าสู่ระบบคอมพิวเตอร์อันมีลักษณะเป็นความผิดฐานหมิ่นประมาทอยู่ในตัวด้วย เพราะถือได้ว่าการนำข้อมูลคอมพิวเตอร์อันมีลักษณะลามกเข้าสู่ระบบคอมพิวเตอร์นั้นย่อมเป็นการใส่ความผู้เสียหายโดยตรง

ในกรณีการพิจารณาการรับฟังพยานอันเป็นข้อมูลอิเล็กทรอนิกส์นั้น ตามพระราชบัญญัติว่าด้วยความรับผิดชอบเกี่ยวกับความรับผิดชอบต่อคอมพิวเตอร์ พ.ศ. 2550 มาตรา 25 บัญญัติว่า “ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มีได้เกิดขึ้นจากการจงใจ มีคำมั่นสัญญา ชูเชื้อ หลอกลวง หรือโดยมิชอบประการอื่น”

เห็นว่าหลักการที่สำคัญของมาตรา 25 คือ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์นั้น คู่ความสามารถอ้างเป็นพยานหลักฐานและศาลมีอำนาจรับฟังได้ตามประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยาน ส่วนการตรวจสอบพยานหลักฐานที่ได้จากคอมพิวเตอร์ก็ใช้หลักการเกี่ยวกับพยานหลักฐานประเภทอื่นตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 และ 226/1 ก็ต้องเป็นพยานหลักฐานที่มีได้เกิดขึ้นจากการจงใจ มีคำมั่นสัญญา ชูเชื้อ หลอกลวง หรือโดยมิชอบประการอื่น

2.6 เอกสารและวรรณกรรมที่เกี่ยวข้อง

รายงานการวิจัย

1. “รายงานการวิจัย จากปิติกุล จีระมงคลพาณิชย์ เรื่อง ปัญหาการรับฟังพยานหลักฐานคณะนิติศาสตร์¹³ ผู้ศึกษาเห็นว่าสื่อบันทึกเสียงและภาพเป็นพยานเอกสารเมื่อได้พิจารณาถึงความหมายของพยานเอกสาร ประกอบกับเมื่อพิจารณาถึงขั้นตอนในการนำเสนอ และการตรวจสอบ

¹³ มหาวิทยาลัยธรรมศาสตร์, 2545. URL : www.lawthai.org/read/acharnpitikul18.doc

ความถึงถูกต้องแท้จริงของพยานเอกสาร เพราะพยานเอกสารมีการตรวจสอบที่ดีกว่าพยานวัตถุ เมื่อมีการนำพยานเอกสารเข้าสู่สำนวนแล้วก็จะให้ศาลใช้ดุลพินิจในการชั่งน้ำหนักพยานหลักฐานหรือการชี้ขาดข้อเท็จจริง แต่การพิสูจน์ความจริงของศาลถึงแม้จะมีการผ่านกระบวนการพิจารณาของศาลก็ยังไม่ได้อาศัยข้อเท็จจริงที่ครบถ้วนบริบูรณ์ ฉะนั้นแล้วจะหวังให้การวินิจฉัยข้อเท็จจริงของศาลครบถ้วนบริบูรณ์ และถูกต้องตรงกับความจริงทุกครั้งไปย่อมเป็นไปได้ แต่หากถือบันทึกเสียงเป็นพยานเอกสารก็จะมีผลทำให้การวินิจฉัยและตัดสินคดีของศาลจะดำเนินไปอย่างเที่ยงธรรมที่สุด นอกจากนั้น ผู้ศึกษายังเห็นว่าควรให้คำจำกัดความของคำว่าพยานเอกสารตามกฎหมายลักษณะพยานว่ามีความหมายว่าอย่างไร ก็สามารถจัดความสงสัยได้ว่าอะไรคือพยานเอกสาร โดยผู้ศึกษามีความเห็นว่ “พยานเอกสาร คือ สิ่งที่ถูกเขียนหรือบันทึกขึ้นเพื่อเป็นพยานเอกสาร โดยให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่นจะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น โดยไม่จำเป็นต้องจะต้องปรากฏบนวัตถุใด อาจจะปรากฏบนกระดาษ ก้อนหิน ดิน โลหะ หรือวัตถุอื่นใด แต่จะต้องคงทนอยู่ในช่วงระยะเวลาอันใดอันหนึ่ง”

บทความ

1. บทความของ นายโชคชัย ตั้งรักษาสัตย์ และนายวินัย ศักดาไกร หลักสูตร เรื่อง การรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์, “กฎหมายธุรกรรมทางอิเล็กทรอนิกส์”¹⁴ เสนอว่าสำหรับคดีที่เกี่ยวข้องกับอินเทอร์เน็ตและคอมพิวเตอร์ พยานหลักฐานของทั้งฝ่ายโจทก์และฝ่ายจำเลยที่จะนำมาสนับสนุนข้ออ้าง ข้อเถียงของตนในชั้นศาลนั้น ล้วนแต่เป็นพยานหลักฐานที่มาจากข้อมูลคอมพิวเตอร์ทั้งสิ้น ซึ่งหากผู้พิพากษาไม่พิจารณาให้น้ำหนักหรือความน่าเชื่อถือแก่ข้อมูลคอมพิวเตอร์แล้ว การทำธุรกรรมทางอิเล็กทรอนิกส์ย่อมไม่สามารถเกิดขึ้นได้

การได้มาซึ่งพยานหลักฐานนั้น โดยทั่วไปจะได้มาจากผู้กระทำความผิดและผู้เสียหาย เมื่อเจ้าหน้าที่ได้พยานหลักฐานอย่างหนึ่งอย่างใดมาแล้ว จะต้องต้องนำมาวิเคราะห์ข้อมูลเพื่อนำเสนอต่อศาลในชั้นพิจารณา การที่พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์เป็นสิ่งที่ไม่มีรูปร่างและไม่สามารถจับต้องได้ จึงทำให้ถูกโต้แย้งง่าย เมื่อฝ่ายโจทก์และฝ่ายจำเลยนำเสนอหลักฐานของฝ่ายโจทก์และจำเลย ในชั้นพิจารณาแล้ว ผู้พิพากษาต้องนำพยานหลักฐานดังกล่าวมาวิเคราะห์ว่าเป็นพยานหลักฐานที่มีน้ำหนักน่าเชื่อถือและเป็นธรรม ปัญหาที่เกี่ยวกับการนำข้อมูลเข้าสู่กระบวนการพิจารณาคดีและเขตอำนาจศาล ลักษณะของพยานหลักฐานส่วนนี้คือ ใครเป็นผู้กระทำความผิดและใช้ข้อมูลนั้น โดยจำเป็นต้องระบุว่า ความผิดนั้นอยู่ที่ใดและใครเป็นผู้ส่ง นอกจากนี้ยังต้องระบุว่าข้อมูลนั้นส่งมาจากผู้ใดและใครเป็นผู้ใช้สถานที่ความผิดเกิดเหตุและความผิดเกิดขึ้นที่ใด เนื่องจากระบบ

¹⁴ คลวินแมรี มหาวิทยาลัยลอนดอน ประเทศอังกฤษ ระหว่างวันที่ 6 – 21 มิถุนายน 2552

คอมพิวเตอร์ ผู้ใช้สามารถเข้าถึงระบบคอมพิวเตอร์จากสถานที่ที่ต่างกัน เช่น สหราชอาณาจักรหรือประเทศสหรัฐอเมริกา นอกจากนี้ในระบบ Cloud Computer เมื่อส่งข้อมูลอิเล็กทรอนิกส์ เช่น ในจดหมายอิเล็กทรอนิกส์(E-mail) หนึ่งฉบับ อาจมีข้อมูลส่วนหนึ่งถูกเก็บไว้ที่ประเทศสหรัฐอเมริกา อีกส่วนหนึ่งถูกเก็บไว้ที่ประเทศสวีเดน และอีกส่วนหนึ่งถูกเก็บไว้ที่ประเทศญี่ปุ่นก็ได้ จากปัญหาดังกล่าว ทำให้เกิดปัญหาเรื่อง เขตอำนาจศาลตามมาเพราะเมื่อเจ้าหน้าที่ต้องการได้มาซึ่งพยานหลักฐาน ที่อยู่ในพื้นที่ซึ่งมีเขตอำนาจศาลที่ซ้อนกัน ทำให้ไม่เจ้าหน้าที่ไม่สามารถรวบรวมพยานหลักฐานนั้น ๆ ได้ ในบางประเทศ การเก็บข้อมูลเพื่อใช้เป็นพยานหลักฐาน จากเครื่องคอมพิวเตอร์หรือในระบบอินเทอร์เน็ต ซึ่งอยู่กับที่และ ไม่ได้เคลื่อนไหวนั้นสามารถทำได้ง่าย แต่ถ้าเป็นการเก็บข้อมูลที่อยู่ในระหว่างการส่งและรับ จะทำให้เกิดปัญหาเรื่องเขตอำนาจศาล ในการรวบรวมพยานหลักฐานได้ ข้อมูลที่อยู่ในระหว่างการส่งจากแหล่งที่หนึ่งไปแหล่งที่สอง การดักจับข้อมูลที่อยู่ในระหว่างการส่งและการรับ ทำให้เกิดปัญหาเรื่องเขตอำนาจศาล เพราะการขอข้อมูลแบบนี้จะแตกต่างจากข้อมูลที่อยู่กับที่, ความถูกต้องสมบูรณ์ของพยานหลักฐานที่ได้มา เพราะหากทำให้เกิดการเปลี่ยนแปลงข้อมูลในระหว่างรวบรวมพยานหลักฐานขึ้น จะทำให้เกิดปัญหาว่าจะอย่างไรที่ทำให้ข้อมูลมีความน่าเชื่อถือ หากพนักงานอัยการต้องการใช้ข้อมูลเป็นพยานหลักฐาน แต่พบว่ามีข้อมูลดังกล่าวถูกแก้ไขเปลี่ยนแปลงในระหว่างตรวจสอบในชั้นเจ้าพนักงานตำรวจ ซึ่งจะทำให้พยานหลักฐานดังกล่าวมีน้ำหนักลดน้อยลง, Stickiness Problem เป็นปัญหาเมื่อมีการลบข้อมูลจะส่งผลทำให้เครื่องคอมพิวเตอร์ลบ Index ของข้อมูลนั้นออก แต่เนื้อหาของข้อมูลยังคงมีอยู่จนกว่าจะถูกเขียนทับขึ้น แต่เมื่อกู้ข้อมูลคืน อาจทำให้ข้อมูลถูกเขียนทับบางส่วน ทำให้ข้อมูลไม่สมบูรณ์และฝ่ายจำเลยสามารถยกปัญหานี้มาโต้แย้งในชั้นศาลได้, ปัญหาในการวิเคราะห์ข้อมูล หากมีการลบข้อมูลและกู้ข้อมูลขึ้นมาได้ Code ที่จะกู้มาจะไม่สามารถเข้าใจเป็นภาษามนุษย์ ผู้วิเคราะห์จะต้องแปลงพยานหลักฐานออกมาในรูปที่มนุษย์สามารถเข้าใจได้, เวลาและสถานที่ที่กระทำความผิด เพราะเวลาและสถานที่ที่เกิดจะขึ้นอยู่กับการตั้งเวลาในเครื่องคอมพิวเตอร์นั้นๆ เช่น ขณะส่ง E-mail อาจเป็นเวลาหนึ่ง เครื่องรับจะเป็นอีกเวลาหนึ่ง ขึ้นอยู่กับว่าจะเป็นเวลาของประเทศไหน

Law and Evidence

1. Discloser ในประเทศอังกฤษ จำเลยจะไม่สามารถถูกลงโทษได้ หากไม่เห็นพยานหลักฐานมาก่อน ดังนั้นเจ้าพนักงานตำรวจและพนักงานอัยการ จึงต้องส่งพยานหลักฐานทั้งหมดที่กล่าวหาว่าจำเลยกระทำความผิดและหลักฐานที่จะพิสูจน์ว่าจำเลยเป็นผู้บริสุทธิ์ หากพนักงานอัยการไม่ส่ง ศาลสามารถหยุดการพิจารณาได้ทันที หลักเกณฑ์ดังกล่าวใช้ทั้งคดีแพ่งและคดีอาญา การพิจารณาในประเทศอังกฤษจะใช้ระยะเวลาในการตรวจพยานหลักฐานมากกว่าการพิจารณา เพื่อมิให้เกิดการดำเนินคดีที่ไม่เป็นธรรม นอกจากนี้จำเลยก็มีหน้าที่เปิดเผยพยานหลักฐานให้พนักงานอัยการเช่นกัน

แต่จำเลยสามารถไม่เปิดเผยหลักฐานที่พิสูจน์ว่าจำเลยกระทำความผิดได้ การเปิดเผยข้อมูลของสาธารณะก็ไม่จำเป็นต้องเปิดเผยเช่นกัน แต่ทั้งนี้ ปัญหาในการเปิดเผยข้อมูลคือปริมาณข้อมูลที่ใช้เป็นหลักฐาน

2. Admissibility การรับฟังพยานหลักฐาน บางประเทศสามารถรับฟังพยานหลักฐานที่เสนอมาได้ บางประเทศมีข้อจำกัดในเรื่องการรับฟังพยานหลักฐาน ในประเทศอังกฤษ ศาลบอกว่าการรับฟังพยานหลักฐาน โดยใช้หลัก Best Evidence นั้นไม่มีแล้ว แต่จะใช้วิธีการชั่งน้ำหนักพยานหลักฐานแทน

Jurisdiction of Court ต้องพิจารณาว่ามีการ abuse of process, Fair trial หรือไม่ เช่นการล่อซื้อ หากเจ้าพนักงานตำรวจล่อซื้อยาเสพติดถือได้ว่าเป็นการโน้มน้าวให้เกิดการกระทำความผิด

3. Probation Value มีการนำมาใช้ในกฎหมายไทย มาตรา ๑๑ วรรค ๒

- a. พิจารณาน้ำหนักความตรงกันของข้อมูล
- b. Reliability of the manner
- c. การแสดงตัวและระบุตัวข้อมูล

ในกฎหมายไทยให้ความสำคัญกับการสื่อสารข้อมูล, การรับข้อมูลและการส่งข้อมูล พยานหลักฐานในส่วนนี้จะรับฟังให้น้ำหนักได้จะต้องสามารถพิสูจน์ว่ามีความเชื่อถือว่ามียุ่จริง ข้อมูลที่มีอยู่มีความถูกต้อง และเจ้าพนักงานสามารถนำมาพิสูจน์ได้ ในแง่การเป็นพยานหลักฐานที่แท้จริงหรือไม่ต้องดูว่า สามารถเชื่อมโยงผู้คนกับข้อมูลที่กระทำความผิดในการทำงานเครื่องคอมพิวเตอร์ หากเห็นหน้า Website หน้าหนึ่งอาจมีการสร้างข้อมูลหลบหลีก เมื่อนำข้อมูลมารวมกัน ก็จะเห็นได้ว่าเป็นข้อมูลเดียวกัน หากเป็นภาพลามกต้องใช้การทำงานพิเศษที่จะพิสูจน์ว่ามาจากต่างสถานที่กันหรือไม่

การทำงานของเครื่องคอมพิวเตอร์ อาจใช้เครื่องคอมพิวเตอร์ 4 เครื่อง ซึ่งตั้งอยู่ในแต่ละประเทศ เพื่อทำงานในเวลาเดียวกันเพื่อให้ได้ภาพลามกดังกล่าว ในการนี้จึงต้องใช้โปรแกรมพิเศษ หากไม่มีก็ไม่สามารถประมวลผลเป็นภาพได้ และการพิสูจน์ว่าเครื่องคอมพิวเตอร์ มีการทำงานและสามารถนำมาใช้กระทำความผิดตามที่กล่าวหาได้ ต้องใช้ผู้เชี่ยวชาญพิเศษเป็นผู้อธิบายขั้นตอนต่างๆ ต่อศาล

4. Expert Witness กระบวนการทั้งหมดต้องการใช้ ผู้เชี่ยวชาญในการรวบรวมพยานหลักฐาน ในความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ อาจต้องใช้ผู้เชี่ยวชาญหลายคน เพราะผู้เชี่ยวชาญคนหนึ่งอาจไม่เชี่ยวชาญในอีกโปรแกรมหนึ่งได้ ในฐานะศาลมีความจำเป็นต้องหาผู้เชี่ยวชาญช่วยทำบัญชี ทำความเข้าใจเกี่ยวกับคำศัพท์เฉพาะทาง เพื่อให้เข้าใจความหมายได้ จากกรณีดังกล่าวในกรณีที่โจทก์ และจำเลยต่างมีผู้เชี่ยวชาญมาพิสูจน์พยานหลักฐาน เช่นนี้ผู้เชี่ยวชาญต้องมีความเชี่ยวชาญได้ในระดับ

หนึ่ง แต่ทั้งนี้ พยานผู้เชี่ยวชาญแตกต่างกับพยานผู้รู้เห็นเหตุการณ์ แต่ผู้เชี่ยวชาญเป็นผู้ให้ความคิดเห็นทางวิชาการ จึงต้องอยู่ในความดูแลของศาลในระดับหนึ่ง

วิทยานิพนธ์

1. “พยานหลักฐานในคดี อาชญากรรมคอมพิวเตอร์” สุรพันธ์ มั่นคงดี วิทยานิพนธ์นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย , 2541 ผู้เขียนพบว่า การนำเทคโนโลยีคอมพิวเตอร์ไปใช้ในการก่ออาชญากรรมได้เกิดขึ้นแล้วในประเทศไทยวิทยานิพนธ์ฉบับนี้จึงมีจุดมุ่งหมายเพื่อที่จะหาคำตอบว่า การรวบรวมพยานหลักฐานเพื่อบำบัดคดีกับอาชญากรรมคอมพิวเตอร์จะพบกับปัญหาและอุปสรรคใดหรือไม่ ผลการวิจัยพบว่าในการสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์ ต้องประสบปัญหาสำคัญ คือความสามารถทางเทคนิคของผู้สืบสวน ความจำเป็นในการเพิ่มทักษะการเรียนรู้ของเจ้าหน้าที่ตำรวจ ความยากลำบากในการแกะรอยผู้บุกรุกเข้าสู่ระบบ ปัญหาในการชี้และรวบรวมพยานหลักฐาน การขาดสถิติและความรู้เกี่ยวกับรูปแบบและลักษณะของอาชญากรรมคอมพิวเตอร์ ความยากลำบากในการติดตามวิวัฒนาการทางคอมพิวเตอร์ที่เปลี่ยนแปลงไปอย่างรวดเร็ว ข้อจำกัดในการปรับใช้กฎหมายลักษณะพยานกับอาชญากรรมคอมพิวเตอร์ ในประเทศสหรัฐอเมริกามีการจัดตั้งหน่วยงานที่มีอำนาจหน้าที่โดยเฉพาะ สังกัดอยู่ในหลายหน่วยงานทั้งในภาครัฐและเอกชนมีการจัดตั้งคณะทำงานสืบสวนสอบสวน มีพนักงานสืบสวนสอบสวนที่ได้รับการฝึกอบรมให้ทราบถึงการค้นหาหลักฐานทางคอมพิวเตอร์การจับกุมและขนย้ายรวมทั้งการรักษาสภาพพยานหลักฐานที่เกี่ยวข้องกับคอมพิวเตอร์อย่างปลอดภัย มีกฎหมายอาญาพิเศษเฉพาะเกี่ยวกับการกระทำผิดที่เกี่ยวข้องกับคอมพิวเตอร์ทั้งในระดับมลรัฐและรัฐบาลกลางและมีกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานซึ่งเป็นผลลัพธ์จากคอมพิวเตอร์ การดำเนินคดีอาชญากรรมคอมพิวเตอร์ ในประเทศสหรัฐอเมริกาสามารถนำตัวผู้กระทำความผิดมาฟ้องลงโทษได้ จึงเป็นตัวอย่างที่ดีแก่ประเทศไทยที่จะเตรียมการแก้ไขปัญหา ซึ่งเป็นที่คาดหมายได้ว่าจะเกิดขึ้นกับประเทศไทยในอนาคตอันใกล้

2. “กฎหมายคุ้มครองข้อมูลในฐานะข้อมูลอิเล็กทรอนิกส์,” ปารเมศ บุญญานันต์ วิทยานิพนธ์นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย , 2543 การศึกษาวิจัยนี้เกิดจากความเป็นจริงในปัจจุบันที่โลก มีการพัฒนาระบบข้อมูลข่าวสารเทคโนโลยีสารสนเทศเป็นไปอย่างรวดเร็ว และมีความนิยมแพร่หลายอย่างกว้างขวางทั่วโลก จนก่อให้เกิดการปฏิวัติในระบบความคิดและวิธีการปฏิบัติงานและการแก้ไขปัญหาต่าง ๆ โดยอาศัยเทคโนโลยีสารสนเทศ เป็นแนวทางหลักรวมทั้งในเรื่องของการเก็บบันทึกข้อมูล (data) การรวบรวมข้อมูลให้อยู่เป็นระบบหรือเรียกว่าฐานข้อมูล (database) ที่ล้วนแต่ปรับเปลี่ยนรูปแบบให้เป็นอิเล็กทรอนิกส์อย่างเต็มตัว ข้อมูล (data) ไม่ว่าจะอยู่ในรูปแบบใด เกิดจากการสะสมความรู้ความสามารถและสติปัญญาของมนุษย์ได้ถูกนำไปใช้ในการคิดสร้างสรรค์งานต่าง ๆ ที่เป็นประโยชน์แก่สังคมโดยรวมสมัยก่อน ข้อมูลจะเก็บไว้ในสมองของผู้คิด

สร้างสรรค์บ้าง จดบันทึกไว้เป็นลายลักษณ์อักษรบ้าง กระจายกันอย่างไม่เป็นระเบียบแบบแผน ต่อเมื่อมีการจัดหมวดหมู่ในภายหลังหรือเรียกว่า ฐานข้อมูล(database) ทำให้ข้อมูลมีระเบียบมากขึ้น นำไปใช้ได้อย่างมีประสิทธิภาพและเมื่อนำข้อมูลในฐานข้อมูลมาสร้างสร้งงานจะได้ผลงานออกมา เรียกว่าทรัพย์สินทางปัญญา (intellectual property) อย่างไรก็ดี แม้ในประเทศที่พัฒนาก้าวหน้าทาง อิเล็กทรอนิกส์ เช่นประเทศสหรัฐอเมริกา ประเทศสหราชอาณาจักร และประเทศในกลุ่มประเทศ สหภาพยุโรป ยังมีปัญหาทางด้านจริยธรรม และการควบคุมเพื่อให้เกิดความเป็นธรรมแก่ทุกฝ่ายมี ปัญหาผู้ทุจริต ปลอมแปลง ลอกเลียน เอาไปใช้ประโยชน์ในทางที่ไม่เหมาะสมเกิดความไม่เป็นธรรม แก่ผู้สร้างสร้งงาน จนในที่สุดก็ได้ใช้มาตรการทางกฎหมายอย่าง เช่น กฎหมายทรัพย์สินทางปัญญา มาใช้บังคับและมีการพัฒนากฎหมายดังกล่าวอยู่ตลอดเวลา พร้อมกันนี้ก็มีการผลักดันให้ประเทศภาคี ในองค์การ ทรัพย์สินทางปัญญาโลกยอมรับกฎหมายคุ้มครองทรัพย์สินทางปัญญาที่พัฒนามาจาก กฎเกณฑ์ของเหล่ามหาอำนาจทางการสื่อสาร มาใช้แต่ปัจจุบันยังไม่บรรลุผล ผลจากการศึกษาพบว่า ประเทศไทยเห็นความสำคัญของการคุ้มครองงานสร้างสรรค์และมีกฎหมายให้ความคุ้มครอง ทรัพย์สินทางปัญญาหลายฉบับออกใช้ เช่น กฎหมายลิขสิทธิ์ สิทธิบัตร และเครื่องหมายการค้า แต่ ยังล้าหลังไม่สอดคล้องกับมาตรฐาน โลกและความก้าวหน้าทางวิทยาการที่เปลี่ยนไป อย่างรวดเร็ว โดยเฉพาะอย่างยิ่งในเรื่องของการคุ้มครองข้อมูลในฐานข้อมูลอิเล็กทรอนิกส์ จึงควรมหามาตรการและ วิธีการคุ้มครองข้อมูลในฐานข้อมูลอิเล็กทรอนิกส์ที่เหมาะสม โดยศึกษาจากรูปแบบที่ใช้กันในระดับ ระหว่างประเทศ และกฎหมายที่มีอยู่ในประเทศไทย เพื่อเป็นพื้นฐาน ในการบัญญัติกฎหมายที่มี ประสิทธิภาพต่อไป

3. “อาชญากรรมทางเศรษฐกิจ: ศึกษากรณีระบบงานพิจารณาพิพากษาคดี” ศกร หลิมศิริ วงษ์, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย , 2543 ผู้เขียนพบว่าปัจจุบันคดี อาชญากรรมทางเศรษฐกิจจะได้รับการพิจารณาพิพากษาจากองค์กรในการพิจารณาพิพากษาคดีอาญา ธรรมดา ทั้ง ๆ ที่ลักษณะและรูปแบบของอาชญากรรมทางเศรษฐกิจจะมีความแตกต่างกับคดีอาญา ธรรมดาอยู่หลายประการ ซึ่งพยานหลักฐานต่าง ๆ ในคดีอาชญากรรมทางเศรษฐกิจจะมีส่วนเกี่ยวข้องกับเทคโนโลยีสมัยใหม่แต่ยังไม่มีความหมายกำหนดหลักเกณฑ์ให้พิสูจน์ความน่าเชื่อถือ ตลอดจนการ พิจารณาพิพากษาคดีจะใช้ระยะเวลาานาน ระบบงานพิจารณาพิพากษาคดีธรรมดาจึงยังไม่มี ความเหมาะสมสอดคล้องกับคดีอาชญากรรมทางเศรษฐกิจ ซึ่งจำเป็นที่การพิจารณาคดีอาชญากรรมทาง เศรษฐกิจจะต้องกำหนดให้มีระบบงานพิเศษขึ้นเป็นการเฉพาะให้เหมาะสมกับประเภทคดีเนื่องจากผู้ ประกอบอาชญากรรมทางเศรษฐกิจมักจะเป็นผู้ที่มีความรู้ ความเชี่ยวชาญชำนาญเฉพาะด้าน มีที่ ประึกษากฎหมาย อาศัยช่องว่างของกฎหมายมาเป็น โอกาสในการกระทำผิด ระบบงานพิจารณา พิจารณาคดีอาชญากรรมทางเศรษฐกิจควรกำหนดให้ผู้พิพากษาขององค์กรในการพิจารณาพิพากษา

คดีอาชญากรรมทางเศรษฐกิจต้องมีความรู้ความเชี่ยวชาญทางด้านเศรษฐกิจเพื่อให้ทันต่อการดำเนินธุรกิจและอาชญากร นอกจากนั้นกระบวนการในการพิจารณาพิพากษายังต้องพัฒนาให้เหมาะสมกับประเภทคดีอาชญากรรมทางเศรษฐกิจ โดยให้มีการกำหนดแนวทางการดำเนินคดี การสืบและการส่งตรวจรักษาพยานหลักฐานทุกประเภทไว้ก่อนได้ การนั่งพิจารณาคดีติดต่อกันการเสนอบันทึกถ้อยคำในการสืบพยานบุคคล การรับฟังข้อมูลคอมพิวเตอร์ และกำหนดให้มีการบันทึกถ้อยคำความพยานทุกถ้อยคำของพยานเป็นต้น ซึ่งระบบงานทุกอย่างจะต้องมีความสอดคล้องรองรับกันเพื่อให้การดำเนินกระบวนการยุติธรรมเป็นไปได้อย่างรวดเร็วและแม่นยำสามารถนำผู้กระทำผิดมาลงโทษได้ เพื่อส่งผลให้เป็นการป้องกันและปราบปรามอาชญากรรมทางเศรษฐกิจ

4. “ปัญหาการรวบรวมและพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีอาญา”¹⁵ ผู้ศึกษาเสนอว่า การที่จะให้เจ้าหน้าที่รัฐเข้าถึงหลักฐานข้อมูลอิเล็กทรอนิกส์ได้อย่างรวดเร็ว จะต้องมีการกฎหมายให้อำนาจเจ้าหน้าที่เพิ่มในบางเรื่องที่เกี่ยวข้องการปฏิบัติงาน ทั้งนี้การรวบรวมพยานหลักฐานมิใช่เป็นเรื่องของกฎหมายเท่านั้น แต่สิ่งที่จำเป็นจำเป็นอย่างยิ่งคือประสิทธิภาพของคนและเทคนิคในการตรวจค้นด้วย จึงจำเป็นต้องมีการพัฒนาเจ้าหน้าที่ให้มีความรอบรู้ในเทคนิควิทยาการคอมพิวเตอร์เพื่อปฏิบัติงานสำหรับการยึดและรักษาพยานหลักฐานที่จะทำให้ข้อมูลอิเล็กทรอนิกส์น่าเชื่อถือ ควรต้องมียุทธศาสตร์เฉพาะที่เชื่อถือได้ว่าเป็นกลางที่สุดเป็นผู้เก็บรักษาพยานหลักฐาน และในขั้นตอนการนำเสนอพยานหลักฐานควรต้องมีหลักกฎหมายลักษณะพยานในเรื่องนี้ให้ชัดเจนกว่าที่เป็นอยู่ และมีหลักในการรับรองความถูกต้องแท้จริงของหลักฐานอิเล็กทรอนิกส์ในคดีอาญา รวมทั้งพยานผู้ชำนาญการพิเศษอาจมีบทบาทสำคัญมากขึ้นในการดำเนินคดีอาญาที่ต้องใช้ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานคดี

5. “ปัญหาในการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์”¹⁶ ผู้เขียนพบว่า ความผิดที่กระทำบนอินเทอร์เน็ตก่อให้เกิดปัญหามากมายในการสืบสวน โดยเฉพาะในขั้นตอนการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากสภาพที่แท้จริงของสิ่งที่จะใช้เป็นพยานหลักฐานไม่อยู่ในสถานะที่มนุษย์สามารถมองเห็นและเข้าใจได้ทั้งยังมีการเคลื่อนไหวที่รวดเร็วแต่ไม่คงทนถาวร จึงมีปัญหารื่องความน่าเชื่อถือของพยานหลักฐานปัญหาดังกล่าวยิ่งทวีความรุนแรงขึ้นเมื่อรัฐธรรมนูญฉบับปัจจุบันได้ตอบรับกระแสเรียกร้องในเรื่องสิทธิส่วนบุคคล โดยบัญญัติไว้อย่างชัดเจนในรัฐธรรมนูญพร้อมกับสร้างกลไกทางกฎหมายเพื่อคุ้มครองสิทธิดังกล่าว ซึ่งส่งผลกระทบต่อการทำงานของเจ้าหน้าที่ของเจ้าพนักงานลักษณะที่สวนกระแสกันเช่นนี้ก่อให้เกิดความสับสนในการปฏิบัติงาน

¹⁵ วไลก้า อุ่นศรี, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2544.

¹⁶ อณัญไพไล เงินวิจิตร วิทยานิพนธ์นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2544.

ของเจ้าพนักงานตำรวจอย่างมาก การปรับปรุงกฎหมายเพื่อแก้ไขปัญหาดังกล่าวจึงต้องศึกษาแนวความคิดในเรื่องการรักษาดุลยภาพระหว่างสิทธิและเสรีภาพของปัจเจกชนกับการใช้อำนาจของรัฐในการรักษาความสงบเรียบร้อยของสังคม และใช้วิธีศึกษากฎหมายเปรียบเทียบกับประเทศสหรัฐอเมริกาซึ่งประสบกับปัญหาดังกล่าวมาแล้ว วิทยานิพนธ์ฉบับนี้ผู้เขียนได้เสนอแนวทางว่าในระหว่างที่ยังไม่มีกฎหมาย อาชญากรรมคอมพิวเตอร์ใช้บังคับควรปรับใช้กฎหมายวิธีพิจารณาความอาญาที่มีอยู่เท่าที่พอใช้บังคับได้ โดยกำหนดกรอบอำนาจเจ้าพนักงานในการค้นหาหลักฐานตลอดจนกำหนดระเบียบวิธีการยึดและเก็บรักษาพยานหลักฐานทางอิเล็กทรอนิกส์ และผู้เขียนยังเสนอแนวทางในการปรับปรุงกฎหมายวิธีพิจารณาความอาญาในส่วนที่เกี่ยวข้องกับการค้นและการยึดพยานหลักฐานทางอิเล็กทรอนิกส์ให้มีประสิทธิภาพสอดคล้องกับแนวทางที่บัญญัติไว้ในรัฐธรรมนูญฉบับปัจจุบัน

6. “การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์.”¹⁷ ผู้ศึกษาเห็นว่า อาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมที่ร้ายแรงเป็นภัยต่อสังคมรูปแบบหนึ่ง ที่ก่อให้เกิดความเสียหายแก่ระบบเศรษฐกิจเป็นอย่างมาก แทบทุกประเทศต่างก็เล็งเห็นถึงอันตรายจากอาชญากรรมประเภทนี้และผลกระทบที่เกิดกับกฎหมายอาญาของประเทศต่างๆ ทั่วโลก เนื่องจากกฎหมายอาญาที่ใช้อยู่ไม่เพียงพอที่จะดำเนินคดีกับอาชญากรได้ จึงพยายามหามาตรการทางกฎหมายใหม่ๆ เพื่อค้นหาวิธีการป้องกันและปราบปราม สำหรับประเทศไทยเป็นประเทศหนึ่งที่ไม่เห็นความสำคัญของปัญหาดังกล่าว จึงมีการร่างกฎหมายอาชญากรรมคอมพิวเตอร์ขึ้นเป็นกฎหมายเฉพาะ อย่างไรก็ตามสิ่งที่ควรคำนึงถึงควบคู่กันไปด้วยคือต้องมีการปรับปรุงกฎหมายวิธีสบัญญัติให้มีประสิทธิภาพด้วย โดยเฉพาะในการรวบรวมพยานหลักฐานและการรับฟังพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ที่เป็นข้อมูลส่วนบุคคล รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 29 ได้บัญญัติรับรองสิทธิและเสรีภาพของประชาชนไว้เป็นหลักพื้นฐาน แต่ก็มีข้อยกเว้นที่ให้อำนาจรัฐสามารถบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ในบางกรณี ภายใต้ขอบเขตที่รัฐธรรมนูญกำหนด เช่น ในมาตรา 37 บัญญัติรับรองคุ้มครองความเป็นอยู่ส่วนตัวของบุคคล ซึ่งเป็นสิทธิส่วนบุคคลและรัฐธรรมนูญก็มีบทบัญญัติให้อำนาจรัฐกระทำการใดๆ ก็ได้หากเป็นกรณีที่กระทำไปเพื่อประโยชน์สาธารณะ ดังนั้น รัฐอาจอาศัยข้อยกเว้นดังกล่าวบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคลเกินความจำเป็น หรือตามอำเภอใจโดยอ้าง“ประโยชน์สาธารณะ” เช่น รัฐอาจบัญญัติกฎหมายอนุญาตให้เจ้าหน้าที่ของรัฐเข้าตรวจสอบข้อมูลส่วนบุคคลของบุคคลใดบุคคลหนึ่งได้ตลอดเวลา ตามแต่จะเห็นสมควร โดยเฉพาะข้อมูล

¹⁷ นริ กิตติสมบุญสุข, วิทยานิพนธ์นิติศาสตรมหาบัณฑิตมหาวิทยาลัยธุรกิจบัณฑิต, 2549.

ข่าวสารส่วนบุคคลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ เป็นต้น การกระทำความผิดถือเป็นการกระทำที่กระทบกระเทือนต่อสาระสำคัญแห่งสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล ซึ่งจะมีผลตามบทบัญญัติในมาตรา 6 ที่ถือว่าบทบัญญัติดังกล่าวขัดหรือแย้งกับรัฐธรรมนูญ ซึ่งถือเป็นกฎหมายสูงสุดของประเทศ ทำให้บทบัญญัตินี้ดังกล่าวไม่สามารถใช้บังคับได้ทั้งๆ ที่การเข้าสู่ข้อมูลส่วนบุคคลนี้ เป็นมาตรการจำเป็นสำหรับรัฐมาใช้แสวงหาพยานหลักฐานเพื่อบำบัดอาชญากรรมที่การแสวงหาพยานหลักฐานรูปแบบดั้งเดิมไม่สามารถแก้ปัญหาได้ เช่น อาชญากรรมคอมพิวเตอร์ ดังนั้นจึงควรมีการบทบัญญัติกฎหมายขึ้นมาให้อำนาจแก่เจ้าหน้าที่ของรัฐ ในการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลได้ภายในขอบเขตที่ไม่เป็นการกระทบกระเทือนต่อสาระสำคัญแห่งสิทธิในข้อมูลข่าวสารส่วนบุคคล พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ มีลักษณะแตกต่างไปจากพยานหลักฐานทั่วไป กล่าวคือพยานหลักฐานประเภทนี้เป็นสิ่งที่ไม่มีการรูปร่าง มองไม่เห็นด้วยตาเปล่า และอยู่ในรูปของคลื่นแม่เหล็กไฟฟ้าอาจถูกแก้ไขเปลี่ยนแปลง ลบ ทำลายได้ง่าย เจ้าหน้าที่ในกระบวนการยุติธรรมทั้งหลายจึงต้องประสบปัญหาในการดำเนินคดีกับผู้กระทำความผิด โดยเฉพาะพนักงานสอบสวนที่มีหน้าที่ในการรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดของจำเลย ผู้วิจัยได้ทำการศึกษาวิจัยปัญหาการรวบรวมพยานหลักฐานและการพิสูจน์พยานหลักฐานที่เป็นอิเล็กทรอนิกส์และเป็นข้อมูลส่วนบุคคล ภายในกรอบของ 3 หัวข้อใหญ่ คือ หนึ่งลักษณะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ สองสิทธิส่วนบุคคล สามกระบวนการค้น และกระบวนการนำเสนอพยานหลักฐานต่อศาล ภายใต้สมมติฐานว่าการรวบรวมพยานหลักฐานที่เป็นการละเมิดสิทธิส่วนบุคคลที่ได้รับการคุ้มครองตามรัฐธรรมนูญและกฎหมายอาญา เจ้าหน้าที่ของรัฐสามารถกระทำได้เพียงใดปัจจุบันมีกฎหมายฉบับใดให้อำนาจกระทำได้หรือไม่อย่างไร และควรจะกระทำอย่างไรเพื่อที่จะนำตัวผู้กระทำความผิดมาลงโทษให้ได้ ผลจากการศึกษาและวิเคราะห์ปัญหาทั้งในประเทศและต่างประเทศ ตลอดจนศึกษาแนวทางแก้ไขปัญหามาจากต่างประเทศ โดยเฉพาะของประเทศสหรัฐอเมริกา อังกฤษ และญี่ปุ่น พบว่า การที่จะให้เจ้าหน้าที่ของรัฐเข้าถึงหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ได้เร็ว และไม่เป็นการละเมิดสิทธิในข้อมูลข่าวสารส่วนบุคคลจะต้องมีกฎหมายให้อำนาจในการปฏิบัติงานได้ ควรต้องมีองค์กรที่เป็นกลางเป็นผู้ให้อำนาจและตรวจสอบการใช้อำนาจและควรมีหลักกฎหมายลักษณะพยานหลักฐานเกี่ยวกับพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ที่ชัดเจนกว่านี้

7. “การรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในคดีแพ่ง,” โกวิท หนูโชม, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2551

ผู้ศึกษาเสนอแนวทางในการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน ดังนี้

1) ความหมายของข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 กำหนดไว้มีขอบเขตครอบคลุมถึงข้อมูลอิเล็กทรอนิกส์ทุกประเภทที่มีอยู่ใน

ปัจจุบันและที่อาจจะมีในอนาคต และมีความสอดคล้องกันกับกฎหมายต่างประเทศ จึงขอกำหนดความหมายของข้อมูลอิเล็กทรอนิกส์เช่นเดียวกับที่กำหนดไว้ในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

2) ในส่วนการจัดประเภทพยานหลักฐานนั้น ข้อมูลอิเล็กทรอนิกส์แม้จะมีลักษณะเป็นพยานเอกสารและพยานวัตถุ แต่ก็มีลักษณะพิเศษแตกต่างจากพยานเอกสารและพยานวัตถุทั่วไปในการนำสืบจึงต้องมีวิธีการพิเศษ โดยเฉพาะ การยอมรับให้ข้อมูลอิเล็กทรอนิกส์เป็นพยานอีกประเภทหนึ่งจึงมีความเหมาะสมมากกว่า

3) เมื่อจัดข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานอีกประเภทหนึ่งแล้ว ข้อที่ต้องพิจารณาต่อมาก็คือ จะต้องมีการนำสืบและหลักในการรับฟังอย่างไร และจะนำบทคัดพยาน ได้แก่ หลักการรับฟังพยานหลักฐานที่ดีที่สุด และหลักการรับฟังพยานบอกเล่า มาใช้ด้วยหรือไม่

4) ดังนั้น การรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานจำเป็นต้องมีกฎหมายกำหนดวิธีการนำสืบและการรับฟังพยานหลักฐาน โดยควรบัญญัติหลักการไว้ในประมวลกฎหมายวิธีพิจารณาความแพ่ง ส่วนรายละเอียดให้กำหนดเป็นข้อกำหนดของประธานศาลฎีกา

8. “การประทับตราเวลา: ความจำเป็นสำหรับการให้บริการพาณิชย์อิเล็กทรอนิกส์และตามผลกฎหมายของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544,” พรชัย นพประโคน กับพวก, วิทยานิพนธ์บัณฑิตวิทยาลัย มหาวิทยาลัยกรุงเทพ, 2553 ความจำเป็นของการประทับตราเวลาของ ผู้ให้บริการประทับตราเวลาสำหรับธุรกรรมทางอิเล็กทรอนิกส์นับว่ามีความสำคัญมาก โดยวันและเวลาต้องได้มาตรฐานสากลและให้เป็นที่ยอมรับของคู่กรณีที่เกี่ยวข้อง โดยผลที่เกิดขึ้นสามารถรับรองการกระทำของบุคคลซึ่งผูกพัน โดยสัญญาของกระบวนการประทับตราเวลาของ ผู้ให้บริการประทับตราเวลาสามารถจัดปัญหาทางด้านเทคนิค แนวปฏิบัติ และกฎหมายแม่แบบพาณิชย์อิเล็กทรอนิกส์ กฎหมายแม่แบบลายมือชื่ออิเล็กทรอนิกส์ได้เปิดกว้างสำหรับการออกเป็นกฎหมายภายใน โดยให้ประเด็นความน่าเชื่อถือการบริการสารสนเทศ และเทคโนโลยีกลายเป็นความสำคัญกับ การพัฒนาความน่าเชื่อถือระหว่างองค์กรธุรกิจกับผู้บริโภค ตลอดจนผู้มีส่วนได้เสียอื่นๆ ในพาณิชย์อิเล็กทรอนิกส์และการพัฒนาเทคโนโลยีในปัจจุบันเปิดโอกาสให้มืออาชีพที่มีความแตกต่างในวิทยาการต่างๆ มาทำงานร่วมกัน หรือเรียกว่าการบูรณาการร่วมกันของการพัฒนาเทคโนโลยีการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมีแนวนโยบาย แนวปฏิบัติ และกฎหมายเพื่อเป็นการรองรับการพัฒนาพาณิชย์อิเล็กทรอนิกส์ สำหรับการประยุกต์ใช้ผู้ให้บริการประทับตราเวลามีความสำคัญมากสำหรับผู้ประกอบการการค้าระหว่างประเทศ มีการเตรียมข้อเสนอเกี่ยวกับสารสนเทศ และหน่วยงานของรัฐที่เกี่ยวข้องในการใช้เอกสารอิเล็กทรอนิกส์การนำเข้าส่งออกเพื่อประโยชน์สำหรับผู้ประกอบการการค้าระหว่างประเทศ และหน่วยงานของรัฐที่เกี่ยวข้อง และส่วนที่

สำคัญอีกอย่างหนึ่งคือพยานหลักฐานดิจิทัลที่นำมาใช้เป็นพยาน หลักฐานในการพิจารณาคดีต้องสามารถพิสูจน์ความจริงและมีความน่าเชื่อถือได้ ข้อเสนอแนะเกี่ยวกับการประทับตราเวลาของ ผู้ให้บริการประทับตราเวลาสำหรับประเทศไทยปัจจุบันไม่มีการออกกฎหมายในขณะนี้ กลุ่มอาเซียน ผู้ทำวิจัยได้ศึกษากฎหมายประเทศมาเลเซียมีกฎหมายเรื่องการประทับตราเวลา ดังนั้นแนวทางการออกกฎหมายของไทยเพื่อเป็นการส่งเสริม สนับสนุนการพาณิชย์อิเล็กทรอนิกส์ให้เป็นมาตรฐานสากล และเป็นที่ยอมรับต่อนานาชาติประเทศ แนวคิดการประทับตราเวลาของผู้ให้บริการประทับตราเวลายังเป็นประเด็นที่มีความจำเป็นและสำคัญต่อไป

ข้อเสนอแนะเกี่ยวกับพยานหลักฐานดิจิทัล หรือพยานหลักฐานอิเล็กทรอนิกส์ของข้อมูลอิเล็กทรอนิกส์จากการกระทำของคู่กรณี โดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์(ฉบับที่ 2) พ.ศ. 2551 มาตรา 6 ให้ศาลรับฟังพยานหลักฐานดิจิทัลเป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีพาณิชย์ คดีอาญา คดีทรัพย์สินทางปัญญา คดีล้มละลาย และคดีอื่นๆ ซึ่งเป็นพยานหลักฐานใหม่และสำคัญในสังคมสารสนเทศ โดยมีแนวคิดที่สำคัญ คือการตรวจสอบความถูกต้องและเป็นพยานหลักฐานที่ดี

ข้อเสนอแนะทางกฎหมายสำหรับประเทศไทย การออกกฎหมายแต่ละฉบับใช้ระยะพอสมควรด้วยเหตุปัจจัยหลายประการ ผู้ทำวิจัยเห็นว่ายังไม่เพียงพอสำหรับการเพิ่มศักยภาพการทำธุรกรรมทางอิเล็กทรอนิกส์ให้เป็นมาตรฐานสากล รัฐต้องบัญญัติกฎหมายเพื่อกำหนดนโยบาย แนวปฏิบัติ เพื่อรองรับการทำธุรกรรมทางอิเล็กทรอนิกส์เพื่อเป็นการอุดช่องว่างของการพัฒนาเทคโนโลยีที่เกิดขึ้นเพื่อเป็นการส่งเสริมพาณิชย์อิเล็กทรอนิกส์ให้มีประสิทธิภาพให้ทัดเทียมกับนานาชาติประเทศต่อไป

ข้อสรุปจากการทบทวนวรรณกรรม

พบว่า มาตราหลักในเรื่องการรับฟังข้อมูลอิเล็กทรอนิกส์ เป็นพยานหลักฐาน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น ได้แก่ มาตรา 25 ซึ่งจำเป็นต้องพิจารณาถึงการได้มาของพยานหลักฐาน, พนักงานเจ้าหน้าที่ รวมทั้งหลักกฎหมายที่เกี่ยวข้องในการรับฟังพยานหลักฐาน ซึ่งจากการทบทวนวรรณกรรมข้างต้น พบว่า การรับฟังข้อมูลอิเล็กทรอนิกส์, การรวบรวมและพิสูจน์, การแสวงหาและได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ยังคงเป็นปัญหาทั้งในทางปฏิบัติและในข้อกฎหมาย ดังนี้ จึงจำเป็นต้องศึกษาต่อไปอีกว่า สำหรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น มีปัญหาที่เกี่ยวกับการรับฟังข้อมูลอิเล็กทรอนิกส์ เป็นพยานหลักฐาน มากน้อยแค่ไหน และมีความสำคัญในการดำเนินคดีและพิจารณาคดีที่เกี่ยวข้องกับคอมพิวเตอร์อย่างไร