บทสัมภาษณ์ ดร. ธีร์รัฐ บุนนาค
ว่าด้วย “พยานหลักฐานดิจิทัล (digital evidence)”[1]
The Interview of Dr.Theerat Bunnag on “Digital Evidence”

Received: 23 ธันวาคม 2564
Revised: -
Accepted: 27 ธันวาคม 2564

ธนภัทร ข่ายม่าน
นัสรี อาจวาริน[2]
Thanapat Khaimarn
Nasree Achwarin

ในการสัมภาษณ์ครั้งนี้มุ่งเน้นไปที่มุมมองการศึกษาเกี่ยวกับคดีอาญา

<u>ถาม</u>: ท่านธีร์รัฐคิดว่าควรใช้คำว่า “electronic evidence” หรือ “digital evidence” ทั้งนี้ เพื่อความครอบคลุม

<u>ตอบ</u>: “electronic” กับ “digital” ในทางทฤษฎีนั้น มีการแบ่งแยกกัน “อิเล็กทรอนิกส์” คือ เครื่องมือที่มีการใช้ระบบอิเล็กทรอนิกส์ แต่ ดิจิทัลจะต้องมีระบบประมวลผล คือ มันจะเป็นคอมพิวเตอร์ กล่าวคือ อิเล็กทรอนิกส์อาจจะไม่รวมไปถึงคอมพิวเตอร์ เช่น วอลค์กี้ทอลค์กี้ (walkie-talkie) โทรศัพท์รับคลื่นวิทยุรับส่งของตำรวจที่แปลงสัญญาณเสียงเป็นสัญญาณไฟฟ้า หรือ แปลงจากสัญญาณไฟฟ้าเป็นสัญญาณเสียง สิ่งเหล่านี้ล้วนเป็นเครื่องมืออิเล็กทรอนิกส์ แต่หากเราจะพูดถึงในมุมมองของคอมพิวเตอร์น่าจะไปทางด้านข้อมูลคอมพิวเตอร์หรือข้อมูลดิจิทัลครับ

<u>ถาม</u>: ถ้าเช่นนั้น คำว่า “digital” เป็น sub-set ของ “electronic” หรือไม่ครับ

<u>ตอบ</u>: คำว่า “digital” เป็น “electronic” อยู่แล้ว แต่ “electronic” อาจจะไม่ใช่ “digital” กล่าวคือ คำว่า electronic กว้างกว่าครับ ถ้าเกิดเราพูดถึงอิเล็กทรอนิกส์ มันอาจจะรวมไปถึง walkie-talkies ซึ่งไม่ใช่ดิจิทัล อย่างไรก็ตาม หากเราจะร่างกฎหมาย นั้นก็ขึ้นอยู่กับว่าเราจะร่างนิยามศัพท์อย่างไร แต่โดยทฤษฎีแล้วคำว่า digital อาจจะตรงกว่า

---

[1] ผู้พิพากษาหัวหน้าคณะในศาลอาญากรุงเทพใต้

[2] นักศึกษาระดับปริญญาตรี ชั้นปีที่ 3 คณะนิติศาสตร์ มหาวิทยาลัยอัสสัมชัญ

<u>ถาม</u>: ก่อนเรียนถามท่านต่อไป ในที่นี้ ขออนุญาตใช้คำว่า “electronic evidence (e-evidence)” และ “digital evidence” สลับกัน โดยทั้งสองคำหมายถึงพยานหลักฐานที่มีลักษณะเป็น intangible (จับต้องไม่ได้) เป็นหลัก นะครับ และ ขอถามว่าท่านอาจารย์คิดว่าบทบัญญัติที่เกี่ยวกับพยานหลักฐานที่ปรากฏใน ประมวลกฎหมายวิธีพิจารณาความอาญา (ป. วิ. อาญา) เพียงพอที่จะนำมา ปรับใช้กับ e-evidence ในคดีอาญาหรือไม่ เพราะอะไร

<u>ตอบ</u>: ผมว่าไม่พอครับ เนื่องจากเพราะว่า ตั้งแต่ตอนสมัยมีการร่าง ป.วิ.อาญา ตอนนั้น ยังไม่มีการนำระบบคอมพิวเตอร์มาใช้เลย ประเภทของพยานหลักฐาน ไม่ว่าจะเป็น พยานบุคคล พยานเอกสารก็ยังไม่อาจรวมถึงระบบที่เป็นดิจิทัลหรือระบบคอมพิวเตอร์ ตอนนี้กฎหมายอาจล้าสมัยไปแล้ว ในปัจจุบัน เทคโนโลยีได้พัฒนาไปไกลแล้ว และ ในปัจจุบัน ได้มีหลักฐานที่ได้จากคอมพิวเตอร์หรือที่เป็นดิจิทัลมากขึ้น และแนวโน้มมากขึ้นเรื่อย ๆ แต่เรากลับไปใช้หลักเกณฑ์ซึ่งมันย้อนหลังไปหลายสิบปี ซึ่งยังไม่เหมาะกับพยานดิจิทัล ดังนั้นหากว่าเรานำมาใช้อาจจะมีข้อจำกัดบางอย่าง เช่น ปัญหาว่า closed circuit television (CCTV) จะต้องนำพยานบุคคลมาสืบด้วยหรือไม่ แต่ถ้าเราเขียนกฎหมายให้ชัดเจน-ก็อาจจะฟังได้ว่าไม่ต้องมีพยานบุคคลมาสืบด้วยก็ได้ ดังนั้น หลักเกณฑ์ใน ป.วิ.อาญา รวมถึงประมวลกฎหมายวิธีพิจารณาความแพ่ง (ป.วิ. แพ่ง) ที่ยังขาดตกบกพร่องในการนำมาใช้กับพยานหลักฐานดิจิทัลอยู่คือหลักเกณฑ์เรื่องการรับฟัง การนำสืบ และการชั่งน้ำหนัก ซึ่งหากจะใช้หลักเกณฑ์เท่าที่มีอยู่โดยไม่มีการแก้กฎหมายก็อาจนำมาสู่ปัญหาในอนาคตอย่างแน่นอน เพราะจะทำให้คำพิพากษาของศาลคลาดเคลื่อนจากความถูกต้อง เนื่องด้วยขาดหลักเกณฑ์การรับฟังและชั่งน้ำหนักที่ครบถ้วน

<u>ถาม</u>: ในปัจจุบัน มีบทบัญญัติในกฎหมายอื่นใดที่อาจนำมาใช้ปิดช่องโหว่ (loopholes) ดังกล่าวได้ครับ

<u>ตอบ</u>: มีอยู่บ้างครับที่ปิดช่องว่างได้ในระดับหนึ่ง แต่ไม่สามารถปิดได้หมด ในตอนนี้ก็มี 2 ฉบับที่เห็นอยู่ คือ พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 (ตามที่แก้ไขแล้ว) (หรือที่เรียกกันว่า พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ฯ) และ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ตามที่แก้ไขแล้ว) (หรือที่เรียกกันว่า พ.ร.บ. คอมพิวเตอร์ฯ) ยกตัวอย่าง เช่น ใน พ.ร.บ. คอมพิวเตอร์ฯ มีการพูดถึงพยานหลักฐานหรือข้อมูลอิเล็กทรอนิกส์ (e-evidence) ว่า ห้ามศาลปฏิเสธการรับฟัง เพราะ จะมีปัญหาในการตีความว่า ตกลงพยานหลักฐานมีแค่ 3 ประเภท คือพยานบุคคล พยานเอกสาร และพยานวัตถุ แต่พยานอิเล็กทรอนิกส์นี้กฎหมายจะรับรองหรือไม่ ยกตัวอย่าง เช่น printout ที่ออกมาจากคอมพิวเตอร์และมีการตีความว่าตกลงใช่พยานอิเล็กทรอนิกส์หรือไม่ ซึ่ง ถ้าเกิดตีความแบบตรง ๆ มันก็ไม่ใช่สัญญา หากแต่เป็นการปริ้นท์ออกมาเลย ซึ่งพ.ร.บ. คอมพิวเตอร์ฯ ก็ได้เขียนกำกับในส่วนนี้ไว้ ส่วน พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ฯ ได้มีการอุดช่องว่างไว้ 2 ประการ

ประการแรกคือ เรื่องการรับฟัง ประการที่สอง คือ การชั่งน้ำหนัก โดยเรื่องการรับฟังนั้น ได้วางหลักเกณฑ์ไว้ว่า ห้ามศาลปฏิเสธไม่รับฟังข้อมูลอิเล็กทรอนิกส์ ทั้งในคดีแพ่งและคดีอาญา ส่วนวิธีการรับฟังนั้น ถูกบัญญัติไว้ในมาตราอื่นใน พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ฯ เช่น จะต้องมีการยืนยันตัวบุคคล (authentication) ต้องไม่เปลี่ยนแปลงหรือปลอมแปลงใด แต่ว่าหลักเกณฑ์ที่เขียนไว้ก็ยังไม่เพียงพอให้รับฟังในทางปฏิบัติอยู่ดี ซึ่งควรจะต้องมีหลักเกณฑ์อื่น ๆ ดังที่ในต่างประเทศเขาก็ใช้กันอยู่ ตัวอย่างเช่น หลักเกณฑ์เรื่องห่วงโซ่การเก็บ การรักษาและการดูแลพยานหลักฐาน (chain of custody of evidence) ก็ยังเขียนไม่ชัดเจนว่าจะต้องมีหรือไม่ รวมทั้งมาตรฐานในซอฟท์แวร์ แอพพลิเคชั่น หรือเครื่องมือที่ใช้ และขั้นตอนการดำเนินการตั้งแต่ เก็บรวบรวมพยานหลักฐาน การดูแลรักษาพยานก่อนตรวจพิสูจน์ และขั้นตอนการตรวจพิสูจน์พยานดิจิทัล

ถาม: ถ้าต้องแก้ไขกฎหมาย ควรแก้อยู่ใน ป.วิ. อาญา หรือไม่ และอย่างไรครับ

ตอบ: อันนี้เป็นประเด็นที่กำลังคุยกันอยู่นะครับ ในต่างประเทศบางแห่งเขาแยกออกมาเป็นกฎหมายเฉพาะ แต่บางแห่งนี้เข้าไปเขียนเสริมไว้ในกฎหมายวิธีพิจารณาความว่าเป็นพยานอีกประเภทหนึ่ง ว่าเป็นพยานอิเล็กทรอนิกส์หรือพยานคอมพิวเตอร์ เป็นต้น สำหรับบ้านเราผมมองว่าอยู่ที่เราจะเขียนอะไรในส่วนนั้น ถ้าเราจะเขียนแค่เพียงว่าให้ศาลรับฟังเหมือนกับที่ พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ฯ หรือ พ.ร.บ. คอมพิวเตอร์ฯ เขียน ถ้าเป็นเช่นนี้ก็อาจจะแก้ไขใน ป.วิ. อาญา หรือ ป.วิ. แพ่ง ก็ได้ ว่าให้มีพยานหลักฐานเพิ่มมารูปแบบหนึ่งและมีวิธีการรับฟังเป็นอย่างไร แต่ ถ้าเรามองไปถึงอนาคตเทคโนโลยีพัฒนาอยู่ตลอด อย่างเช่นเทคโนโลยี artificial intelligence (AI) ที่อาจจะพัฒนาไปเป็นอย่างอื่น ซึ่งกฎหมายที่ดีก็ควรที่จะเขียนเผื่อไว้ในอนาคต ผมจึงมีความเห็นว่า ควรจะบัญญัติขึ้นมาเป็นกฎหมายเฉพาะต่างหากเลยว่าเป็น พ.ร.บ. ว่าด้วยข้อมูลอิเล็กทรอนิกส์ และบัญญัติถึงหลักเกณฑ์ทั้งหมด ตั้งแต่นิยามว่า e-evidence คือพยานหลักฐานอะไร มีกี่ประเภท และมีความสอดคล้องกับกฎหมายวิธีพิจารณาความอย่าง รวมถึงการนำสืบ ยกตัวอย่าง เช่น ในต่างประเทศมีการนำสืบพยานที่เรียกว่า demonstrative testimony การสืบพยานโดยการฉายภาพประธานาธิบดี Kennedy ถูกยิงเป็นภาพสามมิติ หรือ การแสดงตัวอย่าง การเจาะเข้าโปรแกรมคอมพิวเตอร์อย่างผิดกฎหมาย (hacking หรือ การแฮค) ให้ศาลเห็นว่ามีวิธีการแฮค เป็นต้น ดังนั้น ควรจะต้องบัญญัติถึงวิธีการนำสืบพยานรูปแบบใหม่ ๆ ที่สำคัญคือเรื่องการรับฟัง การได้มา และการชั่งน้ำหนักพยานหลักฐานที่เป็นดิจิทัล เรื่องพยานผู้เชี่ยวชาญที่สอดคล้องกันกับเรื่องพยานดิจิทัล รวมถึง การตรวจพิสูจน์พยานหลักฐาน (forensic examination of digital evidence) ที่มีผลต่อการชั่งน้ำหนักพยานหลักฐาน จึงมีความเห็นว่าหากบัญญัติออกมาเป็นพระราชบัญญัติแยกต่างหากจะทำให้สามารถเขียนได้ครอบคลุมและเหมาะสมกว่า

ถาม: ท่านคิดว่า โดยทั่วไปแล้ว การเก็บ e-evidence (e-evidence collecting) ต่างจากการเก็บพยานหลักฐานอื่น (เช่น พยานเอกสาร) หรือไม่ เพียงใด และอย่างไร

<u>ตอบ</u>: การเก็บพยานหลักฐานในที่เกิดเหตุ หากเป็นการเก็บ พยานหลักฐานโดยทั่วไปที่จับต้องได้ (tangible) ไม่ว่าจะเป็นพยานวัตถุหรือพยานเอกสาร (physical evidence or documentary evidence) ก็อาจจะมีการเก็บได้โดยที่ไม่ต้องใช้องค์ความรู้หรือมีขั้นตอนมากนัก ในขณะที่พยานดิจิทัลนั้นมีลักษณะเป็นทรัพย์ที่ไม่มีรูปร่าง (intangible) แต่พยานหลักฐานที่เป็น physical หรือ tangible นั้นมีรูปร่างโดยตัวของมันเอง สามารถมองเห็นได้ด้วยตาเปล่า ส่วนพยานดิจิทัลนั้นเป็นข้อมูลคอมพิวเตอร์ที่อยู่ในระบบเลขฐานสอง (01 - 10) ย่อมไม่สามารถมองเห็นได้ด้วยตาเปล่า หรือข้อมูลใน iPhone ที่สามารถเห็นเนื้อหา (contents) บนหน้าจอ แต่เราก็ไม่สามารถเห็นข้อมูลเชิงระบบได้ ข้อมูลติดต่อสื่อสารคอมพิวเตอร์ที่อยู่ภายใต้อุปกรณ์นั้นไม่ว่าจะเป็นภาพเขียนที่บันทึกไว้ก็เป็นข้อมูลคำสั่งซึ่งมองไม่เห็นด้วยตาเปล่า (intangible) ดังนั้น เมื่อไม่อาจมองเห็นได้ด้วยตาเปล่า ก็ทำให้ยิ่งง่ายต่อการเปลี่ยนแปลงแก้ไข และยากที่จะตรวจพิสูจน์ได้ มีหลายปัจจัยที่อาจทำให้พยานหลักฐานประเภทนี้ถูกเปลี่ยนแปลงแก้ไข เช่น เหตุธรรมชาติ ความผิดพลาดในการทำนิติวิทยาศาสตร์ รวมถึงความจงใจกลั่นแกล้ง ยกตัวอย่าง หากมีการนำไวรัสเข้าไปในระบบว่า หากมีการพิมพ์ ก. ไก่ ให้แสดงผลเป็น ข. ไข่ เมื่อสั่งพิมพ์ออกมา (print out) พยานหลักฐานนี้ออกมาก็ย่อมไม่สามารถรู้ได้เลยว่ามันเป็น ข.ไข่ ที่แท้จริงหรือ ข. ไข่ที่เกิดจากไวรัส สิ่งเหล่านี้เป็นความแตกต่างของพยานดิจิทัลและพยานที่ จับต้องได้หรือที่เป็นกายภาพ (tangible or physical) จึงจำเป็นที่การเก็บพยานหลักฐานแบบดิจิทัลจึงต้องมีเครื่องมือหรือเทคนิคในการเก็บโดยใช้ความรู้องค์พิเศษมากกว่าปกติ จึงตอบได้ว่าการเก็บพยานดิจิทัลมีความแตกต่างจากการเก็บพยานหลักฐานปกติอย่างมาก หากมีการเก็บพยานดิจิทัลโดยไม่ได้ทำตามมาตรฐานขั้นตอน จะส่งผลให้ข้อมูลมีการเปลี่ยนแปลงก็ทำให้มีผลต่อการตัดสินคดีของศาลได้

<u>ถาม</u>: ท่านคิดว่าหลักห่วงโซ่ของการเก็บ การรักษาและการดูแลพยานหลักฐาน (chain of custody of evidence - COC) นำมาใช้กับการเก็บ การรักษาและการดูแล e-evidence หรือไม่เพียงใด และอย่างไร อีกทั้งควรมีข้อควรระวังในการจัดเก็บอย่างไรครับ

<u>ตอบ</u>: คำว่า chain of custody นั้นอาจจะมองได้หลายมุม ถ้าเป็นมุมมองนักกฎหมายที่ไม่เกี่ยวกับระบบดิจิทัล หรือ การตรวจพิสูจน์พยานหลักฐานดิจิทัล (digital evidence forensics) และถ้าพูดถึง COC เราก็อาจจะตีความว่าหมายถึงพยานที่สอดคล้องกันไป เหมือนกับพยานแวดล้อม พยานแวดล้อมไม่สามารถรับฟังโดยปราศจากข้อสงสัยได้ แต่ ถ้าพยานแวดล้อมมีความเชื่อมโยงกันเป็นห่วงโซ่ล้อมไว้จนไม่มีทางออกมันก็อาจจะพิสูจน์จนปราศจากข้อสงสัย (beyond reasonable doubts) ได้

ความจริงแล้ว COC เป็น ศัพท์เฉพาะ (technical term) ในส่วนที่เกี่ยวกับ digital evidence หรือพยานหลักฐานทางวิทยาศาสตร์อื่น ๆ จะต้องมี chain of custody of evidence ตั้งแต่พยานหลักฐานนั้นถูกเก็บในที่เกิดเหตุ ผ่านขั้นตอนการขนย้ายไปยังที่เก็บรักษา (keeping) จาก keeping ส่งกลับไปยังคนที่ทำการตรวจพิสูจน์และจาก การตรวจพิสูจน์ส่งไปยังที่ศาล การเปลี่ยนผ่าน

ของพยานหลักฐานชิ้นนั้นไปยังบุคคลต่างๆ มันจะต้องมีความเชื่อมโยงต่อเนื่องไปยังบุคคลที่เกี่ยวข้องโดยตรงเท่านั้น พร้อมทั้งทำหลักฐานที่เราอาจจะเรียกว่าบันทึก เช่น ทำบันทึกไว้ว่าพันตำรวจโทกฤษฎาเป็นคนเก็บพยานหลักฐานในที่เกิดเหตุ พร้อมทั้งลงชื่อ เวลา สถานที่ไว้พร้อมทั้งติดสติกเกอร์ใส่ไว้ในถุงป้องกันคลื่นแม่เหล็ก (Faraday bag) หลังจากนั้นมีการส่งไปเก็บยังสถานที่เก็บ ผู้ที่เก็บก็ต้องลงชื่อไว้ว่าได้รับพยานหลักฐานไว้เมื่อเวลาใด ทั้งนี้โดยที่ไม่มีคนที่ไม่เกี่ยวข้องเข้ามาแทรกแซงหรือมาตัดห่วงโซ่เหล่านั้น ความเชื่อมโยงของบุคคลที่เข้าไปสัมพันธ์กับพยานหลักฐานชิ้นนั้นมีความเชื่อมโยงพิสูจน์ได้ว่าไม่มีใครผ่าห่วงโซ่เข้าไป แบบนี้เรียกว่า chain of custody เช่น คดีบอส กระทิงแดงที่เป็นข่าวว่าในระหว่างการตรวจพิสูจน์ในเรื่องความเร็วของรถยนต์ รวมถึงการตรวจผู้ขับขี่ว่ามีอาการเมาหรือ เสพย์ยาหรือไม่ และมีคลิปออกมาว่ามีเจ้าพนักงานที่ไม่เกี่ยวข้องมายุ่งกับพยานหลักฐาน กรณีเช่นนี้ถือว่าห่วงโซ่พยานหลักฐานขาดแล้ว chain of custody of evidence จึงมีความสำคัญและควรจะมีการเขียนไว้ในกฎหมายถึงการรับฟังพยานหลักฐานโดยพิจารณาจากหลักเกณฑ์นี้ด้วย ซึ่งในปัจจุบันยังไม่มีกฎหมายใดบัญญัติรองรับหลักเกณฑ์ดังกล่าวไว้เลย

<u>ถาม</u>: ขอถามว่า ถ้าต้องส่งอุปกรณ์ (ซึ่งบรรจุ e-contents/data อันจะใช้เป็น e-evidence) ไปยังต่างประเทศเพื่อถอดรหัส e-contents/data ที่ได้จากการถอดรหัสนั้นจะใช้ในศาลไทยหรือไม่ และ เพื่อให้แน่ใจว่าจะใช้ได้ พนักงานเจ้าหน้าที่จะต้องดำเนินอย่างไรบ้าง

<u>ตอบ</u>: โดยหลักแล้ว มาตรา 18 แห่ง พ.ร.บ.คอมพิวเตอร์ฯ[3] กำหนดไว้ว่า

---

[3] มาตรา 18 บัญญัติว่า

"ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดหรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวนอาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริงดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่รีบรวบรวมข้อเท็จจริงและหลักฐานแล้วแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (1) (2) และ (3) ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงานเจ้าหน้าที่กำหนดซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่ ทั้งนี้

การถอดรหัสเครื่องมืออิเล็กทรอนิกส์ นั้นถือเป็นอำนาจของพนักงานเจ้าหน้าที่ โดยต้องร้องขอต่อศาลก่อน ถ้าเครื่องมืออิเล็กทรอนิกส์นั้นไม่ต้องถอดรหัส เจ้าหน้าที่ก็มีอำนาจในการเข้าถึงข้อมูลด้านในและถือว่าข้อมูลที่ได้มานั้นได้มาโดยชอบสามารถรับฟังได้ แต่หากเป็นกรณีที่ต้องมีการถอดรหัสพนักงานเจ้าหน้าที่จะต้องกระทำการร้องขอต่อศาลก่อน มิฉะนั้นจะถือว่าสิ่งที่ได้มาก็ย่อมเป็นพยานหลักฐานที่ถูกตัดโดยบทตัดพยานตาม ป.วิ.อาญา มาตรา 226[4] ส่วนกรณีที่ส่ง อุปกรณ์ไปยังต่างประเทศเพื่อถอดรหัสก็ใช้หลักเกณฑ์เดียวกัน กล่าวคือ หากเป็นเรื่องที่ต้องร้องขอต่อศาลก็ต้องกระทำเช่นนั้นก่อน สิ่งที่ได้จากการถอดรหัสมาจากต่างประเทศจึงถือเป็นพยานหลักฐานที่ได้มาจากกระบวนการที่ชอบด้วยกฎหมาย แต่ถ้าหากเป็นเรื่องที่ไม่ต้องมีการร้องขอต่อศาล พนักงานเจ้าหน้าที่ก็ย่อมมีอำนาจกระทำได้เอง

<u>ถาม</u>: ในส่วนของบทตัด e-evidence หากไม่มีกฎหมายบัญญัติไว้เป็นการเฉพาะ จะสามารถนำมาตรา 94 แห่ง ป.วิ. แพ่ง[5] มาใช้โดยอนุโลมได้หรือไม่ครับ

รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดระยะเวลาที่ต้องดำเนินการที่เหมาะสมกับประเภทของผู้ให้บริการก็ได้”

[4] มาตรา 226 บัญญัติว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน”

[5] มาตรา 94 บัญญัติว่า

“เมื่อใดมีกฎหมายบังคับให้ต้องมีพยานเอกสารมาแสดง ห้ามมิให้ศาลยอมรับฟังพยานบุคคลในกรณีอย่างใดอย่างหนึ่งดังต่อไปนี้ แม้ถึงว่าคู่ความอีกฝ่ายหนึ่งจะได้ยินยอมก็ดี

(ก) ขอสืบพยานบุคคลแทนพยานเอกสาร เมื่อไม่สามารถนำเอกสารมาแสดง

(ข) ขอสืบพยานบุคคลประกอบข้ออ้างอย่างใดอย่างหนึ่ง เมื่อได้นำเอกสารมาแสดงแล้วว่า ยังมีข้อความเพิ่มเติม ตัดทอน หรือเปลี่ยนแปลงแก้ไขข้อความในเอกสารนั้นอยู่อีก

แต่ว่าบทบัญญัติแห่งมาตรานี้ มิให้ใช้บังคับในกรณีที่บัญญัติไว้ในอนุมาตรา (2) แห่งมาตรา 93 และมิให้ถือว่าเป็นการตัดสิทธิคู่ความในอันที่จะกล่าวอ้างและนำพยานบุคคลมาสืบประกอบข้ออ้างว่า พยานเอกสารที่แสดงนั้นเป็นเอกสารปลอม

ตอบ: แม้ e-evidence จะมีลักษณะพิเศษ แต่ก็ไม่ได้หมายความว่ามันไม่ใช่พยานหลักฐาน เพราะฉะนั้น ไม่ว่าจะเป็น tangible evidence หรือจะ e-evidence หลักเกณฑ์กฎหมายที่เขียนไว้ก็ย่อมใช้บังคับได้ ดังนั้น จึงสามารถใช้ ม.94 แห่ง ป.วิ.แพ่ง หรือ ม.226 แห่ง ป.วิ.อาญา ได้ ตามหลักพยานหลักฐานที่ดีที่สุด (Best Evidence Rule) เพียงแต่ว่าอาจจะต้องมีกระบวนการในทางปฏิบัติเสริมเข้ามานอกเหนือจากกฎหมายที่มีอยู่แล้ว ยกตัวอย่างเช่น บทตัดพยานตาม ม. 226 แห่ง ป.วิ. อาญา ที่วางหลักถึงการล่อซื้อนั้นให้ถือว่าใช้เป็นพยานหลักฐานที่ฟังได้ แต่ถ้าหากเป็นการล่อให้กระทำความผิด (entrapment)-ให้ถือว่าเป็นพยานหลักฐานที่รับฟังไม่ได้ แต่เราไม่สามารถเห็นภาพว่าการล่อซื้อหรือล่อให้กระทำความผิดทางคอมพิวเตอร์ที่เป็นดิจิทัล ได้ว่าทำอย่างไร จึงเป็นเพียงปัญหาในทางปฏิบัติ โดยสรุปคือ ไม่ว่าจะเป็นพยานหลักฐานแบบดิจิทัลหรือธรรมดาก็ใช้หลักเกณฑ์เดียวกัน

ถาม: **ปัญหาเรื่องความแตกต่างในอำนาจหน้าที่ระหว่างพนักงานเจ้าหน้าที่ตาม พ.ร.บ. คอมพิวเตอร์ฯ กับเจ้าพนักงานหรือเจ้าพนักงานตำรวจ**

ตอบ: ก่อน พ.ร.บ. คอมพิวเตอร์ฯ จะบังคับใช้ ในประเทศไทยเรามี ป.วิ. อาญา ซึ่งเป็นเรื่องของการเข้าไปรวบรวมพยานหลักฐานอยู่แล้ว ซึ่งปัญหาอยู่ตรงที่ว่า โดยทั่วไปแล้ว ตำรวจก็มีอำนาจในการยึดของที่จำเป็นรวมถึงพยานหลักฐานได้อยู่แล้วตาม ป.วิ. อาญา ดังนั้น เวลาที่พนักงานสอบสวนจะขอหมายค้นในบ้านนั้น ก็มีเหตุอันควรสงสัยหรือมีเหตุอันควรเชื่อว่าจะมีหลักฐานที่ใช้ในการกระทำความผิดอยู่ ณ ที่ใดที่หนึ่ง ตำรวจจึงมาขอหมายค้นจากศาล ต่อมาในยุคที่มีการใช้โทรศัพท์มือถืออย่างแพร่หลายมากขึ้น คนร้ายก็มักจะใช้โทรศัพท์มือถือในการกระทำความผิด เมื่อตำรวจจับกุมผู้ต้องสงสัยได้ก็จะยึดโทรศัพท์นั้นมาเพื่อเปิดดูว่าเมื่อกี้โทรหาใคร โทรหาจะรับหรือเปล่า แล้วเปิดในการขยายผลต่อไป

แต่หลังจากที่มี พ.ร.บ. คอมพิวเตอร์ฯ ก็ได้มีการตั้งพนักงานเจ้าหน้าที่พิเศษขึ้นมาโดยมีวัตถุประสงค์เพื่อ สร้างมนุษย์ล่องหนที่มีความรู้ระดับเดียวกับ hacker เพื่อที่จะมาสืบสวนจับกุม hackers เหล่านี้ ซึ่งสะท้อนให้เห็นว่าได้มีการให้ความสำคัญกับการเก็บพยานหลักฐานดิจิทัลมากขึ้นว่าบุคคลคนที่จะมาเก็บพยานดิจิทัลนี้จะต้องเป็นพนักงานเจ้าหน้า มิใช่พนักงานสอบสวน ดังนั้นอำนาจในการเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 18 แห่ง พ.ร.บ. คอมพิวเตอร์ฯ จึงเป็นอำนาจของพนักงานเจ้าหน้าที่ซึ่งต้องขออนุญาตศาลก่อนที่จะเข้าถึงข้อมูลซึ่งเป็นการละเมิดสิทธิส่วนบุคคลในโทรศัพท์ เนื่องจากการเข้าไปถึงข้อมูล จะเป็นการเข้าไปในระบบโดยใช้เครื่องมือ (tools) เป็น application พิเศษที่มีชื่อทางการค้าว่า “EnCase” หรือว่า “XRY” ซึ่งเป็นเครื่องมือที่สามารถเข้าไปดูข้อมูลที่ถูกลบ

หรือไม่ถูกต้องทั้งหมด หรือแต่บางส่วน หรือสัญญาหรือหนี้อย่างอื่นที่ระบุไว้ในเอกสารนั้นไม่สมบูรณ์ หรือคู่ความอีกฝ่ายหนึ่งตีความหมายผิด”

(formatted) แล้ว หรือซ่อนไว้ จึงเป็นขั้นตอนที่ต้องการคนที่มีความรู้พิเศษ และอุปกรณ์พิเศษเข้ามาทำหน้าที่ดังกล่าวแทนพนักงานสอบสวน ดังนั้น ในปัจจุบันต้องพิจารณาว่าการที่พนักงานสอบสวนหรือตำรวจยึดโทรศัพท์นั้น จะยึดไปเพื่อดูสิ่งใด หากเป็นการดูข้อมูลทั่วไปที่ไม่ต้องการใช้เครื่องมือพิเศษ ก็เป็นอำนาจทั่วไปที่พนักงานสอบสวนสามารถกระทำได้ แต่หากเป็นการดูข้อมูลที่ลึกลงไปในระบบ เช่น ประวัติการโทรศัพท์ย้อนหลังทุกรายการใน 1 ปี ที่มีการบันทึกการโทรศัพท์เข้าโทรศัพท์ออก รวมถึงบันทึกเสียงสนทนาเอาไว้ การเข้าถึงข้อมูลคอมพิวเตอร์ในลักษณะนี้ ถือเป็นอำนาจของเจ้าพนักงานที่ต้องไปขออนุญาตศาล พนักงานสอบสวนไม่มีอำนาจแต่อย่างใด หากเจ้าพนักงานสอบสวนกระทำการเข้าถึงข้อมูลด้วยตนเอง พยานหลักฐานที่ได้มาก็ต้องถูกตัดตามบทตัดพยานมาตรา 226 แห่ง ป.วิ. อาญา เป็นปัญหาอย่างมากในทางปฏิบัติด้านการตีความกฎหมาย

ถาม: ในมุมมองของท่าน พยานหลักฐานแบบดิจิทัลเป็นพยานเอกสาร หรือ พยานวัตถุ และควรมีการบัญญัติกฎหมายที่แบ่งแยกเป็นประเภทที่แน่นอนเป็นเอกเทศ รวมถึงวิธีการเก็บ การนำสืบ การรับฟังพยานหลักฐานดิจิทัลโดยเฉพาะอย่างไร

ตอบ: ผมจะตอบเป็น 2 ประเด็นดังนี้

ประเด็นแรก ในเรื่องที่ว่าพยานดิจิทัลควรจะเป็นพยานบุคคล พยานเอกสาร หรือพยานวัตถุ ควรจะมีกฎหมายบัญญัติรองรับหรือไม่

ประเด็นที่สอง ก็คือ เรื่องบทบัญญัติกฎหมายที่เกี่ยวกับเรื่องการชั่งน้ำหนักและการรับฟัง ซึ่งผมได้ตอบไปแล้วว่าควรจะมีและก็ควรจะเป็นกฎหมายเฉพาะ เป็นพระราชบัญญัติแยกออกมา

ในส่วนของประเด็นแรกนั้น ในบางประเทศ เช่น ประเทศสิงค์โปร์ พยานดิจิทัลไม่ใช่พยานเอกสาร แต่เป็นพยานดิจิทัลถือเป็นสิ่งที่เกิดขึ้นมาใหม่ ในกรณีนี้ หากถามว่าประเทศไทยควรทำแบบใด ก็ต้องไปดูประเทศสิงค์โปร์หรือประเทศอื่นที่มีนิยามพยานดิจิทัลว่าเมื่อนิยามออกมาแล้ว จะมีประโยชน์อะไรหรือไม่ มีประโยชน์หรือไม่ที่จะไปเขียนให้สอดคล้องกับการรับฟังหรือการช่างน้ำหนัก ถ้ามีประโยชน์ก็ควรที่จะนิยาม แต่ถ้าไม่มีประโยชน์ก็ไม่จำเป็นก็ได้ เพราะ คำว่าพยานหลักฐาน 3 ประเภทคือ พยานบุคคล พยานเอกสาร พยานวัตถุเป็นการแบ่งตามลักษณะรูปแบบ (formation, characteristic) ของลักษณะของพยานแต่ละรูปแบบซึ่งแบ่งไปเพื่อระบุว่าเวลานำเสนอต่อศาลต้องนำเสนอแบบไหนเป็นไปเพื่อระบุว่าเวลานำเสนอต่อศาลต้องนำเสนอแบบไหน เป็นแบบไหน ถ้าเราไม่รู้เป็นอะไร ก็ไม่รู้จักนำเสนอแบบไหน แล้วก็จะมีบทตัดพยานและขนาดไหนก็จะไม่ชัดเจน แต่หากมีการเขียนเราบอกว่าเป็นพยานบุคคลเพื่ออะไรเพื่อแสดงให้ เห็นว่า หากเป็นพยานบุคคล เวลาต้องไปเบิกความ ถ้าเป็นสิ่งของก็ต้องไปแสดงให้อีกฝ่ายและให้ศาลเห็น ถ้าเป็นเอกสารก็ต้องทำสำเนาให้อีกฝ่ายหนึ่งเพื่อไปอ่าน ทั้งหมดคือวัตถุประสงค์ในการแบ่งประเภท ประเภท ก็จะรู้ว่าจะทำยังไงกับพยานเหล่านั้นต่อไปเท่านั้นเอง

ในกรณีของ digital evidence เป็นแบบไหนนั้น ถ้าผมตอบว่าไม่ได้เป็นสักแบบหนึ่ง ในกรณีที่ว่ามาและ ก็ไม่จำเป็นต้องเขียนด้วย เพราะเวลาเป็นพยานดิจิตอลนั้น ถ้าคนที่ตรวจพิสูจน์เองต้องไปเบิกความที่ศาล เขาก็คือพยานบุคคล เป็น expert witness testimony ไป แต่หากเป็นรายงานการตรวจสอบพิสูจน์ รายงานดังกล่าวก็คือพยานเอกสาร (documentary evidence) ไม่มีปัญหาใด ๆ และ หากจะต้องการเอารูปหรือโทรศัพท์ซึ่งใช้ในการกระทำความผิดไปแสดงต่อศาล รูปหรือโทรศัพท์ก็จะเป็นพยานวัตถุ ในความเห็นของผมแล้วจึงไม่มีความจำเป็นที่จะต้องไปบอกว่าพยานดิจิทัลเป็นพยานประเภทไหนใน 3 ประเภท เพราะมันไม่ใช่ทั้งสามประเภท เพียงแต่ขึ้นอยู่กับการนำเสนอต่อศาลในรูปแบบใดก็จะเป็นแบบนั้น เป็นคนก็เป็นพยานบุคคล สิ่งของก็พยานวัตถุ เอกสารก็พยานเอกสาร ไม่มีปัญหาที่จะต้องนิยามหรือไม่นิยาม เพียงแต่หากจะกำหนดให้มีนิยามแล้วจะเกิดความต่อเนื่องชัดเจนก็ควรจะนิยาม แต่การไม่นิยามพยานดิจิทัลนั้นไม่ได้สร้างปัญหา แต่ที่มีปัญหาคือการรับฟังและการชั่งน้ำหนักมากกว่า

<u>ถาม</u>: ท่านคิดว่าศาลมีหน้าที่ในการตรวจสอบความถูกต้องของ e-evidence รวมถึง contents หรือเนื้อหาข้อมูล ที่อยู่ในนั้นหรือไม่ และ ในทางปฏิบัตินั้น ศาลตรวจสอบ e-evidence เพียงใดและอย่างไร

<u>ตอบ</u>: องค์ความรู้ในเรื่องของ e-evidence นั้นบุคลากรในกระบวนการยุติธรรมนั้นค่อนข้างจะมีน้อย โดยผู้ที่เชี่ยวชาญนั้นจะเป็นบุคคลากรในด้านวิทยาศาสตร์และคอมพิวเตอร์ แต่ ในทางกลับกันบุคคลากรเหล่านี้นั้นก็แทบจะไม่มีองค์ความรู้ในเรื่องของกฎหมายเช่นเดียวกับบุคคลากรทางกฎหมายที่มักจะไม่มีองค์ความรู้เกี่ยวกับด้านเทคโนโลยีเหล่านี้

คำตอบของคำถามดังกล่าวนั้นคือ ศาลต้องมีหน้าทีตรวจสอบอยู่แล้ว คือ การชั่งน้ำหนักพยานหลักฐานว่ารับฟังได้หรือไม่ ได้มาโดยชอบด้วยกฎหมายหรือไม่ มีความถูกต้องหรือไม่ มีความน่าเชื่อถือเพียงใด ปัญหาในทางปฏิบัติ คือ ความหมายของการตรวจสอบนี้มีขอบเขตเพียงใด ยกตัวอย่าง กรณีการใช้กรอบแนวคิดของประมวลกฎหมายวิธีพิจารณาความแพ่งและวิธีพิจารณาความอาญามาจับกับเรื่องพยานหลักฐาน (evidence) ก็มิได้ผิดแต่จะขาดบางส่วนไปเช่น Chain of Custody of evidence ที่อาจไม่ได้เอามาใช้ชั่งน้ำหนักพยานหลักฐานเลยหรือไม่ได้มีการนำกระบวนการขั้นตอนที่ได้มาตรฐานมาใช้ในการชั่งน้ำหนักด้วยซึ่งสิ่งเหล่านี้ไม่ได้มีเขียนอยู่ในกฎหมาย ท่านจึงไม่ได้มีการนำมาใช้เนื่องจากนักกฎหมายมักจะดูจากตัวบทกฎหมาย ถ้าไม่มีตัวบทกฎหมายก็อาจจะไม่รู้ไปเลยซึ่งในความเป็นจริงแล้ว ศาลมีหน้าที่ต้องใช้แต่คงใช้ได้ไม่สมบูรณ์แบบนักเนื่องจากขาดองค์ความรู้ ยกตัวอย่างเช่น พยานผู้เชี่ยวชาญ (expert witness) เช่น หมอมาเบิกความ ในไทยนั้นมีแนวโน้มที่ตำรวจ อัยการ ศาล จะเชื่อหมอทั้งหมด แต่ในต่างประเทศวิธีการชั่งน้ำหนักพยานผู้เชี่ยวชาญในต่างประเทศนั้นมีหลักเกณฑ์ แต่ในกฎหมายไทยทั้งประมวลกฎหมายวิธีพิจารณาความแพ่งและประมวลกฎหมายวิธีพิจารณาความอาญา ไม่พูดถึงการชั่งน้ำหนักพยานผู้เชี่ยวชาญเลย เมื่อศาลไม่ได้ชั่งน้ำหนัก

พยานผู้เชี่ยวชาญตามหลักเกณฑ์ดังกล่าวซึ่งไม่มีในกฎหมายไทยนั้นจึงมิได้ขัดต่อกฎหมายไทย เพียงแต่ผิดไปจากหลักการสากล เพราะขาดองค์ความรู้นั่นเอง ตอนนี้เราขาดบุคลากรที่มีความรู้ทั้งด้านดิจิทัลและด้านกฎหมายโดยเน้นกฎหมายมากกว่าเนื่องจากเป็นเรื่องของกระบวนการยุติธรรม เราต้องการผลิตนักกฎหมายที่ความรู้ทางด้านดิจิทัล

<u>ถาม</u>: ขอถามว่าท่านธีร์รัฐคิดว่า deepfakes จะสร้างปัญหาในการชั่งน้ำหนักพยานหรือไม่เพียงใด

<u>ตอบ</u>: ขึ้นอยู่กับว่ารูปคดีที่อัยการฟ้องเข้ามาเป็นการฟ้องในฐานความผิดฐานใด เช่น การตัดต่อภาพตามพระราชบัญญัติคอมพิวเตอร์ฯ เป็นการหมิ่นประมาทด้วยการตัดต่อภาพ เช่น เป็นใบหน้าของดาราแต่ร่างกายนั้นเป็นของผู้อื่นปรากฏในสื่อลามก จึงเกิดการฟ้องหมิ่นประมาทผู้ที่กระทำ สิ่งที่อัยการโจทก์ต้องนำสืบคือภาพดังกล่าวมีการตัดต่อเปลี่ยนแปลงใบหน้าจริงหรือไม่ ประเด็นนี้จึงต้องมีการพิสูจน์ หากจำเลยยืนยันว่าเป็นทั้งใบหน้าและร่างกายของดาราจริง หน้าที่โจทก์ต้องนำสืบในการทำ deepfake คือการเปลี่ยนแปลงใบหน้า กรณีนี้ต้องใช้การนำสืบซึ่งอาศัยตามระบบดิจิทัล

แต่ถ้าหากไม่ใช่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ แต่เป็นการที่กล้องวงจรปิดจับภาพคนร้ายได้ แต่เจ้าหน้าที่ของรัฐได้ไปทำการเปลี่ยนแปลงใบหน้าในกล้องวงจรปิดให้เป็นหน้าคนร้ายซึ่งต้องการจะกลั่นแกล้งในขณะกระทำความผิด เช่น กำลังกระทำความผิดฐานปล้นทรัพย์ เมื่อเข้าสู่ศาล ศาลไม่ได้มีการตรวจสอบเว้นแต่จะเกิดการตรวจสอบเมื่อเป็นประเด็นข้อพิพาท จำเลยต้องต่อสู้ว่านั่นไม่ใช่จำเลยในวิดีโอ ขณะเกิดเหตุจำเลยอ้างฐานที่อยู่อีกสถานที่หนึ่ง เพียงเท่านี้อัยการโจทก์ต้องมีการนำสืบว่าภาพนั้นเป็นภาพจริงหรือไม่ หากอัยการนำสืบว่าเป็นภาพจริง จำเลยต้องนำสืบแก้ว่าเป็นภาพซึ่งเกิดจากการตัดต่อ เพราะฉะนั้น เมื่อศาลไทยนั้นไม่ใช่ศาลที่ใช้ระบบไต่สวน แม้ศาลสงสัยเองแต่คู่ความไม่ตรวจ ศาลก็จะนิ่งเฉยและถือเสียว่าเป็นการรักษาผลประโยชน์ของคู่ความกันเอง เพราะศาลไทยนั้นใช้ระบบกล่าวหา ศาลไทยจะตรวจสอบก็ต่อเมื่อเกิดเป็นประเด็นข้อพิพาท หรือในกรณีที่คู่ความไม่ต่อสู้และศาลนั้นอาจจะส่งไปตรวจพิสูจน์เองก็ได้ในเมื่อไม่มีผู้ใดต่อสู้ว่าใช่จำเลยหรือไม่ในภาพ แต่ศาลไม่สามารถเขียนคำพิพากษาและมั่นใจได้ว่าอาจจะมีการตัดต่อ ศาลก็สามารถส่งตรวจพิสูจน์เองได้ กฎหมายวิธีพิจารณาความอาญาก็เปิดช่องให้กระทำได้

<u>ถาม</u>: เนื่องจากการพิสูจน์กรณี deepfake นั้นมีค่าใช้จ่ายค่อนข้างสูง จึงอาจทำให้จำเลยไม่ยกประเด็นดังกล่าวต่อสู้ อยากทราบว่าศาลมีการช่วยเหลืออย่างใดหรือไม่

<u>ตอบ</u>: ไม่มีปัญหาใดๆ สมมุติจำเลยนั้นเป็นคนจน จำเลยจะบอกศาลว่าขอให้ศาลส่งพยานหลักฐานเพื่อไปทำการตรวจพิสูจน์เช่นเดียวกับกรณีการตรวจลายมือชื่อว่าปลอมหรือไม่

การส่งตรวจพิสูจน์นั้นจะมี 2 แบบ

แบบที่ 1 คือ คู่ความขอตรวจเอง ยกตัวอย่างเช่น จำเลยอ้างว่าไม่ใช่ลายมือของตน เป็นการตัดต่อ จำเลยขออนุญาตส่งตรวจพิสูจน์ กรณีนี้ผู้ขอตรวจต้องออกค่าใช้จ่ายเอง

แบบที่ 2 คือ ให้เป็นอำนาจศาล จำเลยอาจแถลงว่าตนนั้นไม่มีกำลังทรัพย์ไม่สามารถตรวจสอบเองได้ รบกวนศาลส่งตรวจ กรณีนี้ศาลสามารถส่งตรวจเองได้

ถาม: ท่านคิดว่า e-evidence ที่เกี่ยวข้องกับการสอบปากคำเด็กอยู่ในบังคับ ป.วิ. อาญา มาตรา 133ทวิ[6] (ที่ต้องมีสหวิชาชีพร่วม) หรือไม่

---

[6] มาตรา 133ทวิ บัญญัติว่า

"ในคดีความผิดเกี่ยวกับเพศ ความผิดเกี่ยวกับชีวิตและร่างกายอันมิใช่ความผิดที่เกิดจากการชุลมุนต่อสู้ ความผิดเกี่ยวกับเสรีภาพ ความผิดฐานกรรโชก ชิงทรัพย์และปล้นทรัพย์ตามประมวลกฎหมายอาญา ความผิดตามกฎหมายว่าด้วยการป้องกันและปราบปรามการค้าประเวณี ความผิดตามกฎหมายว่าด้วยมาตรการในการป้องกันและปราบปรามการค้าหญิงและเด็ก ความผิดตามกฎหมายว่าด้วยสถานบริการ หรือคดีความผิดอื่นที่มีอัตราโทษจำคุก ซึ่งผู้เสียหายหรือพยานที่เป็นเด็กอายุไม่เกินสิบแปดปีร้องขอ การถามปากคำผู้เสียหายหรือพยานที่เป็นเด็กอายุไม่เกินสิบแปดปี ให้พนักงานสอบสวนแยกกระทำเป็นส่วนสัดในสถานที่ที่เหมาะสมสำหรับเด็กและให้มีนักจิตวิทยาหรือนักสังคมสงเคราะห์ บุคคลที่เด็กร้องขอ และพนักงานอัยการร่วมอยู่ด้วยในการถามปากคำเด็กนั้น และในกรณีที่นักจิตวิทยาหรือนักสังคมสงเคราะห์เห็นว่าการถามปากคำเด็กคนใดหรือคำถามใด อาจจะมีผลกระทบกระเทือนต่อจิตใจเด็กอย่างรุนแรง ให้พนักงานสอบสวนถามผ่านนักจิตวิทยาหรือนักสังคมสงเคราะห์เป็นการเฉพาะตามประเด็นคำถามของพนักงานสอบสวน โดยมิให้เด็กได้ยินคำถามของพนักงานสอบสวนและห้ามมิให้ถามเด็กซ้ำซ้อนหลายครั้งโดยไม่มีเหตุอันสมควร

ให้เป็นหน้าที่ของพนักงานสอบสวนที่จะต้องแจ้งให้นักจิตวิทยาหรือนักสังคมสงเคราะห์ บุคคลที่เด็กร้องขอ และพนักงานอัยการทราบ รวมทั้งแจ้งให้ผู้เสียหายหรือพยานที่เป็นเด็กทราบถึงสิทธิตามวรรคหนึ่งด้วย

นักจิตวิทยาหรือนักสังคมสงเคราะห์ หรือพนักงานอัยการที่เข้าร่วมในการถามปากคำอาจถูกผู้เสียหายหรือพยานซึ่งเป็นเด็กตั้งรังเกียจได้ หากมีกรณีดังกล่าวให้เปลี่ยนตัวผู้นั้น

<u>ตอบ</u>: โดยปกติ เวลาสหวิชาชีพไปสอบสวนจะมีการถ่ายภาพและวิดีโอไว้ นอกจากนั้น พนักงานสอบสวนยังต้องถ่ายภาพวิดีโอเคลื่อนไหวไว้ด้วยซึ่งนั่นคือ digital evidence แต่มันจะไม่เป็นประเด็นขึ้นมาสู่ศาลอีก

สมมุติว่ามีการตัดต่อเปลี่ยนเสียงหรือใบหน้าว่าให้การเป็นอย่างอื่นและนำเสนอต่อศาล ก็เป็นหน้าที่ของเด็กผู้นั้นที่ได้รับความเสียหายต้องต่อสู้ว่าวิดีโอที่ถ่ายในชั้นสอบสวนนั้นทำโดยถูกกลั่นแกล้งเป็นพยานหลักฐานที่ได้มาหรือเกิดขึ้นโดยไม่ชอบด้วยกฎหมายแล้วศาลจึงจะส่งไปตรวจพิสูจน์อีกครั้งหนึ่งว่ามีการดัดแปลงแก้ไขจริงหรือไม่ต่อไป

<u>ถาม</u>: เนื่องด้วยกฎหมายวิธีพิจารณาความแต่ละประเทศแตกต่างกัน e-evidence จะบังคับใช้ในคดีอาชญากรรมข้ามแดน (transnational crime) ความผิดเกิดหลายเขตอำนาจศาลหรือคดีใช้ extraterritorial jurisdiction ได้หรือไม่ และอย่างไร

<u>ตอบ</u>: คำถามที่ตรงมากกว่าคือพยานหลักฐานที่เกิดขึ้นจากต่างประเทศซึ่งเป็นดิจิทัลจะเอามาได้อย่างไร เช่น server ของ Facebook อยู่ที่สหรัฐอเมริกาและเราต้องการข้อมูลของคนร้ายซึ่งใช้ Facebook ในการกระทำความผิด หรือสมมุติคนร้ายต้องการจะเจาะระบบคอมพิวเตอร์ที่เมืองไทย คนร้ายเหล่านี้จะไม่ใช้เครื่องคอมพิวเตอร์ของตนเจาะระบบโดยตรงแต่จะใช้วิธีการหลบซ่อนหรืออำพรางด้วยการเข้าไปควบคุมเครื่องคอมพิวเตอร์ในประเทศอื่นโดยควบคุมคอมพิวเตอร์เครื่องอื่นจากหลากหลายประเทศ เช่น คุมเครื่องที่ญี่ปุ่นด้วยโปรแกรมบางอย่างและใช้เครื่องคอมพิวเตอร์ที่ญี่ปุ่นนั้นควบคุมให้เครื่องคอมพิวเตอร์ที่สหรัฐอเมริกาทำการเจาะระบบคอมพิวเตอร์ของเครื่องเป้าหมายในประเทศไทย เมื่อมีการตรวจสอบย้อนเส้นทางการเชื่อมต่อจึงจะสามารถตามไปยังที่ประเทศสหรัฐอเมริกา แล้วจึงตามย้อนไปถึงประเทศญี่ปุ่นและย้อนกลับมาซึ่งผู้กระทำความผิดอีกทอดหนึ่ง ในทางทฤษฎีแล้วนั้น ไม่มีปัญหาใด ๆ ทั้งการรับฟังได้หรือไม่ หรือ เป็นปัญหาเรื่องการบังคับใช้

ภายใต้บังคับแห่งมาตรา 139 การถามปากคำเด็กตามวรรคหนึ่ง ให้พนักงานสอบสวนจัดให้มีการบันทึกภาพและเสียงการถามปากคำดังกล่าวซึ่งสามารถนำออกถ่ายทอดได้อย่างต่อเนื่องไว้เป็นพยาน

ในกรณีจำเป็นเร่งด่วนอย่างยิ่งซึ่งมีเหตุอันควรไม่อาจรอนักจิตวิทยาหรือนักสังคมสงเคราะห์ บุคคลที่เด็กร้องขอ และพนักงานอัยการเข้าร่วมในการถามปากคำพร้อมกันได้ ให้พนักงานสอบสวนถามปากคำเด็กโดยมีบุคคลใดบุคคลหนึ่งตามวรรคหนึ่งอยู่ร่วมด้วยก็ได้ แต่ต้องบันทึกเหตุที่ไม่อาจรอบุคคลอื่นไว้ในสำนวนการสอบสวน และมิให้ถือว่าการถามปากคำผู้เสียหายหรือพยานซึ่งเป็นเด็กในกรณีดังกล่าวที่ได้กระทำไปแล้วไม่ชอบด้วยกฎหมาย”

(enforcement) โดยเป็นพยานดิจิทัลและอยู่ในต่างประเทศ ทางทฤษฎีนั้นไม่มีปัญหาใดๆ มีทั้งหลักความร่วมมือระหว่างประเทศ สนธิสัญญาระหว่างสองประเทศหรือหลักต่างตอบแทนถ้อยทีถ้อยปฏิบัติ

แต่ในทางปฏิบัติแล้วนั้นเป็นไปได้ยาก ตัวอย่าง เช่น เมื่อพนักงานสอบสวนอยู่ในอำเภอหนึ่งในจังหวัดในไทย ต้องทำหนังสือให้ผู้บัญชาการสำนักงานตำรวจแห่งชาติเพื่อให้ผู้บัญชาการตำรวจแห่งชาติส่งหนังสือไปขอข้อมูลจากสำนักงานอัยการสูงสุดและส่งไปยังอัยการสูงสุดในการขอข้อมูลจากประเทศสหรัฐอเมริกา จากนั้นอัยการสูงสุดต้องทำหนังสือไปยังกระทรวงการต่างประเทศ และกระทรวงการต่างประเทศต้องทำหนังสือส่งไปยังกระทรวงต่างประเทศของประเทศสหรัฐอเมริกาและจากนั้นกระทรวงต่างประเทศของประเทศสหรัฐอเมริกาต้องตามไปถึง proxy ของเว็บไซต์ซึ่งคนร้ายได้กระทำความผิด เพียงแค่ทั้งหมดที่กล่าวมานั้นก็เป็นไปแทบไม่ได้เลยที่จะเกิดขึ้นเนื่องจากต้องมีค่าใช้จ่าย เวลา ค่าแปลเอกสารจากต่างประเทศและสิ่งอื่นมากมายที่ต้องเสียไปนั้นเกิดเป็นคำถามว่าจะคุ้มค่ากับสิ่งที่ต้องแลกไปหรือไม่

ทั้งหมดที่กล่าวมานั้นเป็นเพียงแค่ขั้นตอนสำหรับการต้องการข้อมูลในการสืบสวนเพียงแค่ประเทศเดียวเพียงเท่านั้น ในทางปฏิบัติจึงพูดได้ว่าแทบจะเป็นไปไม่ได้ก็มิผิด แต่ ในทางทฤษฎีนั้นเป็นไปได้ นี่คือปัญหาของ cyber crime ที่กระทำผ่านมาจากต่างประเทศหรือกระทำจากในประเทศแต่ผู้กระทำมีความรู้เรื่องการปกปิดเส้นทางการเชื่อมต่อไปต่างประเทศส่งผลให้เกิดปัญหาเรื่องการได้มาซึ่งพยานหลักฐาน

<u>ถาม</u>: ท่านคิดว่า e-evidence จะช่วยลดภาระของสายลับ (ซึ่งเข้าแฝงตัวกับองค์กรอาชญากรรมค้ายาหรือค้าสื่อลามกเด็กเพื่อหาพยานหลักฐาน) ในการให้การเป็นพยานหรือไม่ และอย่างไร

<u>ตอบ</u>: มองว่าไม่มีความเกี่ยวข้องกัน เพราะว่า e-evidence นั้นเป็นการพูดถึงข้อมูลที่เกี่ยวข้องกับการกระทำความผิดที่มาอยู่ในระบบคอมพิวเตอร์ใน server, desktop computer หรือ หน้าจอมือถือ ไม่เกี่ยวกับพยานบุคคล ซึ่งพยานบุคคลที่เกี่ยวข้องนั้น คือ พยานผู้เชี่ยวชาญ (expert witness) ซึ่งต้องมาเบิกความเนื่องจากเป็นบุคคลที่ตรวจพิสูจน์ e-evidence

ส่วนการทำการแฝงตัวนั้นจะเป็นประเด็นในการล่อซื้อเสียมากกว่า เมื่อแฝงตัวเข้าไปแล้วได้หลักฐานมา เช่น มีการติดกล้องซ่อนและนำภาพนั้นมาสืบพยานในศาลว่าคนร้ายกำลังค้ายาเสพติด มีการเป็นสายลับและแฝงตัวเข้าไป ประเด็นจึงเป็นเรื่องมีการล่อซื้อหรือไม่? ถ้าไม่ติดกล้องก็จะไม่มีประเด็นเรื่อง e-evidence เลย สายลับจะต้องเบิกความในฐานะประจักษ์พยานว่าเป็นคนล่อซื้อ แต่ถ้ามีกล้อง ก็ต้องเบิกความว่ากล้องนี้อยู่กับตน ในภาพทั้งหมดเป็นภาพจริง จึงมีความเห็นว่าไม่มีความเกี่ยวข้องกัน

การแฝงตัว (undercover) ถ้าการแฝงตัวนั้นมีการล่อ ยุ หรือบังคับให้คนทั่วไปกระทำความผิด (entrap) ถือว่าพยานหลักฐานดังกล่าวจะถูกตัดตามประมวลกฎหมายวิธีพิจารณาความอาญาตามมาตรา 226[7]

แต่หากเป็นการแฝงตัวแล้วไปล่อซื้อจริงจากบุคคลที่ต้องสงสัย กรณีนี้พยานหลักฐานที่ได้มาสามารถรับฟังได้ จะเกี่ยวกับ e-evidence หรือไม่ขึ้นอยู่กับว่าจะมีข้อมูลที่เป็นภาพ เสียง หรือใช้ระบบดิจิทัลหรือไม่ประการใด

สมมุติว่า A มีการแฝงตัวเข้าไปอยู่ในกลุ่มคนร้าย แต่ได้มีกล้องติดตัวไปถ่ายหรือมีการบันทึกเสียง อย่างไรก็ตาม นาย A ต้องมาเบิกความว่าตนเป็นบุคคลที่มีกล้องติดตัวใช่หรือไม่

ในสมัยก่อนนั้นไม่มีกล้องถ่ายวิดีโอ ตัวสายลับนั้นจะเป็นประจักษ์พยานซึ่งศาลจะมาชั่งน้ำหนักในเวลาต่อมานั้น มีกล้องและมีตัวสายลับเป็นพยาน หากยืนยันโดยใช้แค่พยานหลักฐานจากตัวสายลับก็เพียงพอแล้ว แต่เมื่อมีกล้องแล้วนั้นก็เป็นการเพิ่มความน่าเชื่อถือมากขึ้นว่าประจักษ์พยานปากนี้ได้มีการล่อซื้อจริงปรากฏตามหลักฐานจากกล้อง เวลานำเสนอก็ต้องนำเสนอไปตาม digital evidence ไป แต่อาจจะมีปัญหาคล้ายกับกรณีพยานคู่เบิกความตรงกันก็จะไม่มีปัญหา คือ ภาพที่ปรากฏนั้นจะต้องตรงกับประจักษ์พยานเบิกความ ถ้ามีหลักฐานอะไร ศาลจะเอามาดูรวมกันหมดเลย หากมีชิ้นเดียวก็จะชิ้นเดียว หากมีพยานหลักฐานสองชิ้นคล้าย ๆ พยานคู่ ศาลก็จะมาเทียบความตรงว่าพยานกล้องและพยานบุคคลมีความตรงกันหรือไม่ ถ้าตรงกันก็ไม่มีปัญหา สามารถรับฟังได้มากยิ่งขึ้น

แต่ในกรณีที่มีแต่พยานหลักฐานจากกล้องไม่มีพยานบุคคล ในสหรัฐอเมริกานั้นมีการพัฒนาทฤษฎีแนวคิดการรับฟังพยานหลักฐานที่เป็นประจักษ์พยานไปแล้ว แต่ประเทศไทยยังไม่มีการพัฒนานั่นคือ silent witness rule

Silent witness คือ ภาพที่ปรากฏจากกล้องวงจรปิดหรือภาพนิ่งที่เป็นดิจิทัล มันสามารถบอกเป็นคำพูดได้หมื่นคำหรือหมายความว่า ไม่จำเป็นต้องมีประจักษ์พยานก็สามารถรับฟังจากกล้องวงจรปิดที่เห็นขณะเกิดเหตุว่าจำเลยเป็นคนทำได้เท่ากับประจักษ์พยาน

หลักว่าประจักษ์พยานคือพยานที่รู้เห็นเหตุการณ์โดยตรงซึ่งเราก็เข้าใจเสมอมาว่าคือพยานบุคคล แต่ ปัจจุบัน ถ้าไม่มีพยานบุคคล ศาลไทยเราจะมองว่าไม่มีประจักษ์พยาน แต่แนวคิดของ

---

[7] มาตรา 226 บัญญัติว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน”

ต่างชาติเห็นว่าประจักษ์พยานที่เป็นดิจิทัลในปัจจุบันก็คือกล้องวงจรปิดโดยที่ไม่ต้องนำบุคคลมาเบิกความซ้อนกันกับกล้องอีก แต่อาจจะต้องเอาบุคคลมาเบิกความว่ากล้องนั้นทำงานปกติและเห็นเป็นภาพนั้นจริง ๆ แต่ไม่ได้เอากล้องมายืนยันข้อเท็จจริงที่กล้องเห็น ในปัจจุบันประเทศไทยยังไม่มีแนวคิดดังกล่าว

<u>ถาม</u>: ถ้าหากคดีลักษณะที่กล่าวมานี้ท่านธีร์รัฐเป็นผู้พิพากษา ท่านจะมีความคิดเห็นเป็นอย่างไร

ผมมีความเห็นว่าคงจะใช้องค์ความรู้ของต่างประเทศเข้ามาปรับใช้ด้วย ยกตัวอย่างเช่นคดีที่อากงส่ง sms ไปดูหมิ่นพระราชินีนั้นคำพิพากษาของศาลชั้นต้นนั้น มีการใช้หลักการรับฟังพยานผู้เชี่ยวชาญ (expert witness) ซึ่งกฎหมายไทยในเวลานั้นยังไม่มีหลักการดังกล่าว สะท้อนให้เห็นถึงการที่ผู้พิพากษาซึ่งตัดสินคดีดังกล่าวศึกษาค้นคว้าองค์ความรู้จากต่างประเทศและพัฒนาหลักการชั่งน้ำหนักพยานรวมถึงมีการเขียนเป็นแนวทาง แม้ประเทศไทยนั้นจะไม่ได้ใช้หลักการ judge made law หรือผู้พิพากษาเป็นผู้สร้างกฎหมาย เพียงแต่คำพิพากษานั้นมีการพัฒนาและมีการนำเอาหลักการของต่างประเทศมาใช้ แม้กฎหมายไทยจะยังไม่เปิดช่อง แต่ถ้าหากศาลจะทำการวางแนวทาง ผมเชื่อว่าก็ไม่ได้ผิดอะไร เพราะการชั่งน้ำหนักนั้นเขียนในกฎหมายไว้ค่อนข้างกว้างซึ่งเปิดให้ศาลนั้นสามารถใช้ดุลพินิจได้มาก แต่หากมีการบัญญัติไว้ก็จะเป็นการทำให้ผู้พิพากษามองเห็นภาพเดียวกันทั่วประเทศ

ผมมีประเด็นที่อยากจะฝาก คือเรื่องการที่กฎหมายไทยได้แก่ พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ฯ และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ฯ ยังเขียนไว้ไม่ครอบคลุมในเรื่องของการชั่งน้ำหนักพยานหลักฐาน ในจุดที่ยังไม่ครอบคลุมและสิ่งที่น่าจะต้องมีการแก้ไขเพิ่มเติมเข้าไปหากมีการแก้ไขกฎหมายในภายภาคหน้า นั่นก็คือ

เนื่องจากพยานหลักฐานที่เป็นดิจิทัลเปลี่ยนแปลงแก้ไขง่ายและมองไม่เห็น ดังนั้น กระบวนการเข้าไปรวบรวมพยานหลักฐานในที่เกิดเหตุ ขั้นตอนการเก็บพยานหลักฐานชิ้นนั้นในระหว่างการรอตรวจพิสูจน์ ขั้นตอนการตรวจพิสูจน์ ทั้ง 3 ขั้นตอนดังกล่าวนั้นจะมีผลในเรื่องของการชั่งพยานหลักฐาน (weighing of evidence) โดยต่างประเทศจะใช้คำว่า admissibility

ยกตัวอย่าง เครื่องคอมพิวเตอร์ หากเป็นระบบโบราณ หากเจ้าหน้าที่ต้องการจะเข้าไปยึดเครื่อง ต้องทำอย่างไร ถ้าไม่ได้ทำตามขั้นตอนที่ถูกต้อง ข้อมูลที่ได้อาจจะมีการผิดเพี้ยนไป เช่น สมมุติว่ามาตรฐานบอกว่า ถ้าจะไปยึดเครื่องคอมพิวเตอร์ที่เป็นระบบ Linux จะต้องปิดเครื่องก่อนแล้วค่อยดึงปลั๊ก แต่ ถ้าเป็น Microsoft Word ต้องดึงปลั๊กก่อน ถ้าไม่ทำตามจะมีผลในเรื่องของพยานหลักฐานที่จะสูญหายไป นี่เป็นเพียงตัวอย่างแรก

การที่จะมีความน่าเชื่อถือหรือไม่นอกจากดู physical evidence แล้ว ยังต้องดูขั้นตอนการรวบรวมพยานหลักฐานของ digital evidence ในลักษณะของพยานหลักฐานแต่ละชิ้นนั้นหรือไม่

ในต่างประเทศนั้นมีการประชุมกันของผู้พิพากษา ตำรวจ ทนาย อาจารย์มหาวิทยาลัยเพื่อการวางมาตรฐานเรื่องการรวบรวมพยานหลักฐาน การเก็บรักษา และการตรวจพิสูจน์ของ e-evidence

โดยระดมสมองและประกาศมาตรฐานจากมติที่ประชุม จากนั้นศาลจึงจะใช้มติดังกล่าวมาเป็นมาตรฐานในการชั่งน้ำหนักพยานหลักฐาน

ในปัจจุบันนั้นการตรวจพิสูจน์หลักฐานซึ่งมี 2 หน่วยงาน คือ สถาบันนิติวิทยาศาสตร์ของกระทรวงยุติธรรม และหน่วยพิสูจน์หลักฐานของสำนักงานตำรวจแห่งชาติ ซึ่งแน่นอนว่ามาตรฐานนั้นคงจะแตกต่างกัน จึงเกิดคำถามว่าต้องทำอย่างไรเพื่อให้มีการร่วมกันสร้างมาตรฐานเดียวเพื่อให้ศาลหยิบไปใช้ในการชั่งน้ำหนักได้

หากเป็นเครื่องคอมพิวเตอร์นั้นเวลาเก็บเป็นไปได้หรือไม่ที่จะห้ามไม่ให้เก็บใกล้แหล่งกำเนิดไฟฟ้าหรือเครื่องใช้ไฟฟ้า

หากทำการตรวจพิสูจน์คอมพิวเตอร์นั้น มีการใช้ application หรือโปรแกรมใด ต้องใช้ hard disk ใหม่หรือไม่ สิ่งเหล่านี้คือวิธีการและขั้นตอนในการปฏิบัติ ได้มาตรฐานหรือไม่

Application(s) หรือเครื่องมือต่าง ๆ ที่ใช้ ได้มาตรฐานและเป็นที่ยอมรับหรือไม่ ถ้าทั้งสองสิ่งนี้ได้มาตรฐานจะถือว่า weighing of evidence นี้มีความน่าเชื่อถือ (creditability) แต่หากเครื่องมือหรือ applications เหล่านั้นไม่ได้มาตรฐานตามที่ลงมติกันไว้หรือผิดขั้นตอน จะส่งผลให้พยานหลักฐานนั้นไม่น่าเชื่อถือทันที

สิ่งนี้ประกอบกับ Chain of Custody of evidence ไม่มีในกฎหมายของประเทศไทย หากจะทำการร่างกฎหมาย ผมเห็นว่า สิ่งเหล่านี้เป็นสิ่งจำเป็นที่ต้องบัญญัติไว้ในกฎหมาย

หากจะต้องเสนอแนะศาลยุติธรรมจริง ๆ ศาลยุติธรรมนั้นต้องออกข้อกำหนดประธานศาลฎีกาว่าด้วยเรื่องมาตรฐานในการตรวจพิสูจน์ เก็บรักษาและการรวบรวมพยานหลักฐานดิจิทัล

ในปัจจุบันอาจารย์ ดร. สุรทศ คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยมหิดล ได้มีการจัดทำมาตรฐานเกี่ยวกับเครื่องมือและขั้นตอนที่เกี่ยวข้องกับพยานดิจิทัลซึ่งทำโดยองค์กรกลางทางวิชาการ ทำให้น่าจะนำมารับฟังได้มากกว่าเกณฑ์ของหน่วยงานรัฐที่ยังไม่ชัดเจนซึ่งน่าจะสามารถรับฟังได้มากกว่าหน่วยงานที่ยังมีการถกเถียงกัน แต่หากศาลยุติธรรมนำมาตรฐานกลางที่จัดทำโดยมหาวิทยาลัยและหน่วยงานของรัฐที่เกี่ยวข้องได้ว่า การเก็บ การตรวจพิสูจน์มีมาตรฐานขั้นตอนของอุปกรณ์ที่ใช้อย่างไร หากศาลยอมรับก็อาจออกเป็นข้อกำหนด ข้อบังคับ หรือคำแนะนำประธานศาลฎีกาในเรื่องการรับฟังและชั่งน้ำหนักพยานหลักฐานที่เป็นดิจิทัล ศาลก็น่าจะนำหลักเกณฑ์ดังกล่าวมาใช้ เจ้าหน้าที่ตำรวจ และพนักงานอัยการก็จะได้รับทราบและใช้เกณฑ์เดียวกันนั้นเป็นแนวทางในการทำสำนวนสอบสวนและสั่งคดี วิธีนี้ อาจจะเป็นทางลัดที่จะทำให้กระบวนการยุติธรรมในเรื่องการรับฟังและชั่งน้ำหนักพยานหลักฐานดิจิทัลของบ้านเราให้เป็นไปตามมาตรฐานสากลได้โดยเร็ว

กิตติกรรมประกาศ

ผู้สัมภาษณ์ขอกราบขอบพระคุณท่านผู้พิพากษา ดร. ธีร์รัฐ บุนนาค เป็นอย่างสูงที่กรุณาให้สัมภาษณ์เกี่ยวกับพยานหลักฐานดิจิทัลกับกฎหมายไทยตามที่ปรากฏข้างต้น นอกจากนั้นแล้ว ผู้สัมภาษณ์ขอขอบคุณท่านผู้ให้ความช่วยเหลือในการเตรียมการสัมภาษณ์และการจัดทำบทถอดคำสัมภาษณ์นี้ซึ่งรวมถึงอัยการปกรณ์ ธรรมโรจน์ พันตำรวจตรี นิติ สัมฤทธิ์เดชขจร รองผู้อำนวยการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ นางสาวภูมิจิต ศิระวงศ์ประเสริฐ และ รองศาสตราจารย์ ดร. พิศวาท สุคนธพันธุ์