การดำเนินคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัล ภายใต้หลักนิติธรรม

จัดทำโดย

นายอิทธิพร แก้วทิพย์

รหัสประจำตัว ๖๗๑๒๕๑

รายงานนี้เป็นส่วนหนึ่งของโครงการอบรมหลักสูตร

“หลักนิติธรรมเพื่อประชาธิปไตย” (นธป.) รุ่นที่ ๑๒

บทที่ ๑
บทนำ

๑.๑ ความเป็นมาและความสำคัญของปัญหา

อาชญากรรมคอมพิวเตอร์หรือ CyberCrime คือ อาชญากรรมที่ใช้เทคโนโลยีทางคอมพิวเตอร์เป็นเครื่องมือหนึ่งในการกระทำความผิด เรียกได้ว่าเป็นอาชญากรรมไร้พรมแดน เนื่องจากลงมือกระทำจากที่ใดก็ได้ที่มีสัญญาณ Internet ไม่ต้องเดินทางไปปรากฏตัวที่เกิดเหตุ มีลักษณะการกระทำในหลายรูปแบบ เช่น ลักลอบเจาะเข้าระบบข้อมูลของบุคคลอื่น หรือองค์กร เพื่อโจรกรรมข้อมูล ทำลายหรือปลอมแปลงข้อมูล นำข้อมูลไปใช้หลอกลวงฉ้อโกงนำเข้าข้อมูลอันเป็นเท็จเพื่อแสวงหาประโยชน์อันไม่ชอบด้วยกฎหมายผ่านอุปกรณ์คอมพิวเตอร์อุปกรณ์สื่อสารอิเล็กทรอนิกส์ Social Network หรือช่องทางออนไลน์อื่นๆ ตัวอย่างรูปแบบอาชญากรรม เช่น กลุ่มบุคคลร่วมกันกระทำการเป็นแก๊งค์คอลเซ็นเตอร์ปลอมตนเป็นเจ้าหน้าที่ของรัฐ หรือรัฐวิสาหกิจ หลอกลวงผู้เสียหายให้หลงเชื่อยอมให้ทรัพย์สินหรือประโยชน์อื่นใดโดยทุจริตการลักลอบเจาะระบบข้อมูลการเงินการธนาคารเพื่อโจรกรรมเงินในบัญชีของบุคคลอื่น การปลอมเสียงเป็นคนสนิทโทรศัพท์ผ่านระบบอินเตอร์เน็ตเพื่อปิดบังเบอร์โทรศัพท์แล้วหลอกให้โอนเงินผ่านระบบธนาคารบนอินเตอร์เน็ต เป็นต้น อาชญากรรมเหล่านี้นอกจากจะทำให้ประชาชนได้รับความเดือดร้อนเสียหายแล้วยังกระทบต่อระบบเศรษฐกิจของประเทศด้วย

ปัญหาและอุปสรรคสำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ส่วนใหญ่นั้นเป็นเรื่องของพยานหลักฐานที่มีความซับซ้อนในการสืบค้น รวบรวม และเก็บรักษา เนื่องจากส่วนใหญ่เป็นพยานหลักฐานอิเล็กทรอนิกส์[๑]ที่มีลักษณะแตกต่างจากวัตถุพยาน หรือ พยานเอกสารทั่วไป เพราะจับต้องไม่ได้ ไม่ทิ้งร่องรอยให้เห็นประจักษ์ ไม่เหมือนดังเช่น หยดเลือด คราบเลือด หรือ ปลอกกระสุนในที่เกิดเหตุ ไม่สามารถใช้วิธีการตรวจพิสูจน์ DNA หรือข้อมูลพันธุกรรม แต่เป็นข้อมูลที่ถูกสร้างและส่งต่อโดยวิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า รวมถึงข้อมูลในระบบดิจิทัล[๒] ที่เป็นข้อมูลในรูปแบบชุดตัวเลข มีการประมวลผลที่แม่นยำ สามารถแปลงค่าตัวเลข หรือถอดรหัสเพื่อแสดงผลเป็นตัวหนังสือ ภาพ และหรือเสียง สามารถจัดเก็บ ค้นหา จัดการข้อมูล และส่งต่อ ผ่านเทคโนโลยีสารสนเทศ (Information Technology : IT) หรือการประยุกต์ใช้คอมพิวเตอร์และอุปกรณ์โทรคมนาคม คุณลักษณะของพยานหลักฐานอิเล็กทรอนิกส์มีความเปราะบางดัดแปลง ตัดต่อเลียนแบบ ปลอมแปลง หรือลบทิ้งได้ง่ายแต่หาพบร่องรอยการดัดแปลง ตัดต่อ เลียนแบบ ปลอมแปลง หรือกู้คืนได้ยาก ต้องใช้ความรู้ อุปกรณ์ โปรแกรม หรือ เทคนิคเฉพาะทาง เช่น ภาพบันทึกจากกล้องวงจรปิด สามารถลบทิ้งได้ และอาจกู้คืนได้แค่บางกรณี หรือคลิปวิดีโอ สามารถตัดต่อได้แม้อาจทิ้งร่องรอย แต่การหาร่องรอยการตัดต่อก็ต้องใช้เทคนิคเฉพาะทางที่อาจต้องใช้บุคลากรผู้ผ่านการศึกษาอบรมให้มีความเชี่ยวชาญเฉพาะด้านเท่านั้นจึงจะสามารถทำได้ ดังนั้นในชั้นสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์ที่มีพยานหลักฐานเป็นข้อมูลอิเล็กทรอนิกส์ และข้อมูลดิจิทัล จึงไม่ใช่เรื่องง่ายที่จะรวบรวมพยานหลักฐานให้มากพอที่จะเชื่อมโยงการกระทำความผิดกับตัวผู้กระทำความผิดรวมไปถึงเครือข่ายที่เกี่ยวข้องทั้งหมด ในขณะเดียวกันพยานหลักฐาน

---

[๑] "อิเล็กทรอนิกส์" หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น, พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ๒๕๔๔ มาตรา ๔

[๒] เทคโนโลยีหรือข้อมูลที่ถูกแปลงเป็นรูปแบบเลขฐานสอง (binary) ซึ่งประกอบด้วยเลข ๐ และ ๑ ข้อมูลดิจิทัลสามารถเก็บและประมวลผลได้อย่างมีประสิทธิภาพและแม่นยำ รวมถึงสามารถถ่ายโอนและจัดการได้ง่ายผ่านอุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ สมาร์ตโฟน และอื่นๆ

ที่ได้มาก็ต้องเป็นพยานหลักฐานที่เชื่อถือได้ มีความถูกต้องแท้จริง ไม่ถูกดัดแปลง ตัดต่อ เลียนแบบหรือปลอมแปลง ตั้งแต่จุดกำเนิด และระหว่างการใช้งานข้อมูล การส่งต่อ การรวบรวม การเก็บรักษาไปจนถึงการนำไปใช้นำสืบในชั้นพิจารณาของศาล

อย่างไรก็ดี การดำเนินคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัล ต้องยึดโยงและอยู่ภายใต้หลักนิติธรรม เนื่องมาจากหลักนิติธรรม เป็นเสมือนกรอบหลักเกณฑ์ที่จะกำหนดแนวทางการขับเคลื่อนกระบวนการยุติธรรม ในสังคมให้เกิดความชอบธรรม ความเป็นธรรมและความยุติธรรม คู่ขนานกันไป ความชอบธรรมนั้นหมายถึงความชอบด้วยกฎหมายและ ความชอบด้วยศีลธรรม ส่วนความเป็นธรรมนั้น ย่อมหมายถึง ความเสมอภาคที่ทุกคนจะได้รับสิทธิและความคุ้มครองอย่างเท่าเทียมกัน ไม่เลือกปฏิบัติ ส่วนความยุติธรรมนั้น หมายถึงหากเกิดความ ไม่ชอบธรรม ไม่ชอบด้วยกฎหมายฝ่าฝืนและละเมิดกฎหมายหรือกฎเกณฑ์ของสังคม เกิดการเอารัดเอาเปรียบและเกิดความ ไม่เป็นธรรมขึ้น จะต้องถูกยุติด้วยความถูกต้องเที่ยงธรรมตามที่มีกฎหมายหรือกฎเกณฑ์ของสังคมรองรับ และได้รับการพิจารณาอย่างปราศจากอคติ ดังนั้นการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัลก็เช่นกัน นอกจากจะต้องมีการพัฒนากฎหมายและเครื่องมือการบังคับใช้กฎหมายให้เท่าทันต่อความเติบโตของอาชญากรรมที่ใช้เทคโนโลยี หรือที่ใช้คอมพิวเตอร์เข้ามาเป็นเครื่องมือในการกระทำความผิดแล้ว ในการพิจารณาดำเนินคดี ตั้งแต่ขั้นตอนการรวบรวมพยานหลักฐาน ยังต้องอยู่ภายใต้หลักนิติธรรมด้วย กล่าวคือ ต้องให้ความเป็นธรรมทั้งผู้เสียหาย และต้องเคารพสิทธิของผู้ต้องหาเช่นกัน มิให้มีการเก็บรวบรวมพยานหลักฐานอันเป็นการละเมิดสิทธิส่วนบุคคลของฝ่ายใดฝ่ายหนึ่ง อันเป็นการละเมิดสิทธิตามกฎหมายและหลักนิติธรรม ดังนั้น จะเห็นได้ว่า หลักนิติธรรมนั้น เป็นเหมือนกรอบและแนวปฏิบัติ ให้เจ้าหน้าที่ของรัฐ ดำเนินการปราบปรามอาชญากรรมในสังคมเพื่อรักษาความสงบเรียบร้อยในสังคม ตามหลักเกณฑ์ที่บัญญัติไว้อย่างชัดเจน เคารพสิทธิมนุษยชน สิทธิส่วนบุคคล ในขณะเดียวกัน ก็ต้องรักษาความเป็นธรรม ความชอบธรรมและความยุติธรรมให้กับสังคมได้ด้วย

๑.๒ วัตถุประสงค์การศึกษา

๑) เพื่อศึกษา วิเคราะห์ปัญหาและอุปสรรคเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัล

๒) เพื่อศึกษา และค้นคว้าหาแนวทางการแก้ไขปัญหาและอุปสรรคในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัล

๓) เพื่อจัดทำข้อเสนอแนะในการปรับปรุงแก้ไขปัญหาอุปสรรค ข้อบกพร่อง และข้อจำกัดในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ เพื่อใช้ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัลให้มีประสิทธิภาพมากยิ่งขึ้น และสามารถนำไปใช้ได้จริงในทางปฏิบัติเพื่อยกระดับและพัฒนาการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ในยุคดิจิทัลให้เป็นไปอย่างมีประสิทธิภาพ ภายใต้หลักนิติธรรม

๑.๓ ขอบเขต ขั้นตอนและวิธีการศึกษา

๑) ค้นคว้าและรวบรวมข้อมูลสภาพปัญหาและอุปสรรคเกี่ยวกับการจัดการพยานหลักฐานอิเล็กทรอนิกส์โดยเฉพาะขั้นตอนการเก็บรวบรวมรักษาพยานหลักฐานอิเล็กทรอนิกส์เพื่อให้สามารถนำไปใช้ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ได้โดยรวบรวมข้อมูลจากผู้ปฏิบัติงานจริง ค้นคว้าข้อมูลจากเอกสาร บทความทางวิชาการ และข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้

๒) ค้นคว้าและรวบรวมกฎหมายที่เกี่ยวข้อง เพื่อนำมาปรับใช้วิเคราะห์ปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรม คอมพิวเตอร์ในทางปฏิบัติที่เกิดขึ้นในปัจจุบัน

๓) ศึกษาวิเคราะห์ ปัญหาและอุปสรรค ทั้งในข้อเท็จจริงและข้อกฎหมาย โดยศึกษาเปรียบเทียบจากคดีที่เกิดขึ้นจริงทั้งในและต่างประเทศ

๔) ศึกษาค้นคว้าและวิเคราะห์หาแนวทางการแก้ไขปัญหาและอุปสรรค ในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์เพื่อใช้ดำเนินคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัล เพื่ออุดช่องว่างในทางกฎหมายและเพิ่มประสิทธิภาพในทางปฏิบัติตั้งแต่ขั้นตอนการรวบรวมพยานหลักฐาน ไปจนถึงการนำพยานหลักฐานไปใช้ในการพิจารณาคดี และการสืบพยานของเจ้าหน้าที่ผู้มีอำนาจหน้าที่ตามกฎหมาย ภายใต้หลักนิติธรรม

๑.๔ ประโยชน์ที่คาดว่าจะได้รับ

แนวทางการแก้ปัญหาและอุปสรรคในการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์สำหรับคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัลภายใต้หลักนิติธรรม เพื่อป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ยกระดับและพัฒนาการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ในยุคดิจิทัลให้เป็นไปอย่างมีประสิทธิภาพมากยิ่งขึ้น ไม่ให้อาชญากรรมคอมพิวเตอร์ หรืออาชญากรรมทางเทคโนโลยีนั้นมาบ่อนทำลายเศรษฐกิจสังคมประเทศชาติ และความสงบสุขของประชาชน

บทที่ ๒
การรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัล

๒.๑ ลักษณะของอาชญากรรมทางคอมพิวเตอร์

ดังที่กล่าวแล้วในบทนำถึงสภาพและลักษณะของอาชญากรรมทางคอมพิวเตอร์ หรืออาชญากรรมทางเทคโนโลยี ที่มีความซับซ้อนและมีการใช้เทคโนโลยีเข้ามาเป็นเครื่องมือในการกระทำความผิด ซึ่งตามพระราชกำหนดมาตรการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ มาตรา ๓ นิยาม *“อาชญากรรมทางเทคโนโลยี หมายความว่า การกระทำหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ”*

จะเห็นได้ว่า อาชญากรรมทางเทคโนโลยี ตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีดังกล่าว ได้รวมการกระทำความผิดที่มีลักษณะ ฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ เอาไว้ด้วย ซึ่งเป็นฐานความผิดที่ระบุไว้ในประมวลกฎหมายอาญาโดยมาตรา ๓๔๑ กำหนดว่าผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง ส่วนความผิดฐานกรรโชกทรัพย์ มีกำหนดไว้ในมาตรา ๓๓๗ ประมวลกฎหมายอาญา ซึ่งระบุไว้ว่า ผู้ใดข่มขืนใจผู้อื่นให้ยอมให้หรือยอมจะให้ตนหรือผู้อื่นได้ประโยชน์ในลักษณะที่เป็นทรัพย์สิน โดยใช้กำลังประทุษร้ายหรือโดยขู่เข็ญว่าจะทำอันตรายต่อชีวิต ร่างกาย เสรีภาพ ชื่อเสียงหรือทรัพย์สินของผู้ถูกขู่เข็ญหรือของบุคคลที่สาม จนผู้ถูกข่มขืนใจยอมเช่นว่านั้น ผู้นั้นกระทำความผิดฐานกรรโชกและมาตรา ๓๓๘ ผู้ใดข่มขืนใจผู้อื่น ให้ยอมให้ หรือยอมจะให้ตนหรือผู้อื่นได้ประโยชน์ในลักษณะที่เป็นทรัพย์สิน โดยขู่เข็ญว่าจะเปิดเผยความลับซึ่งการเปิดเผยนั้นจะทำให้ผู้ถูกขู่เข็ญหรือบุคคลที่สามเสียหาย จนผู้ถูกข่มขืนใจยอมเช่นว่านั้น ผู้นั้นกระทำความผิดฐานรีดเอาทรัพย์ซึ่งพฤติการณ์ส่วนใหญ่ของอาชญากรรมเทคโนโลยีจากคดีที่เกิดขึ้นจำนวนมากในปัจจุบันก็จะมี เช่น หลอกลวงผู้เสียหาย จนหลงเชื่อยอมโอนเงินให้ผ่านทางระบบธนาคารออนไลน์ โดยลักษณะการหลอกลวงนั้นเมื่อมีการโอนเงินเข้ามาจะมีการโอนต่อทันทีเข้าบัญชีม้าหรือบัญชีที่เปิดขึ้นมาชั่วคราวเป็นการเฉพาะ เพื่อตัดวงโคจรไม่ให้สืบสาวไปถึงกระบวนการที่แท้จริง

ทั้งนี้ ตามคำอธิบายลักษณะคดีออกตามความในข้อ ๕ ของคำสั่งสำนักงานตำรวจแห่งชาติที่ ๑๘๒/๒๕๖๖ ลงวันที่ ๑๗ มีนาคม ๒๕๖๖ ได้กำหนดรูปแบบการกระทำผิดอาชญากรรมทางเทคโนโลยีที่กระทำผิดเกี่ยวกับการฉ้อโกงกรรโชกหรือรีดเอาทรัพย์ หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย เพื่อให้เป็นไปตามพระราชกำหนดมาตรการป้องกันและปราบปรามการใช้งานทางเทคโนโลยี ๒๕๖๖ และมอบหมายพนักงานสอบสวนรับผิดชอบ ให้มีอำนาจสืบสวนสอบสวนเกี่ยวกับความผิดลักษณะดังกล่าวของหน่วยงานในสำนักงานตำรวจแห่งชาติ โดยแบ่งออกเป็น ๑๕ ประเภทคดี ดังนี้

๑. คดีหลอกลวงซื้อขายสินค้าหรือบริการที่ไม่มีลักษณะเป็นขบวนการ
๒. คดีหลอกลวงเป็นบุคคลอื่นเพื่อยืมเงิน
๓. คดีหลอกหลวงให้รักแล้วโอนเงิน
๔. คดีหลอกลวงให้โอนเงินเพื่อรับรางวัลหรือวัตถุประสงค์อื่นๆ
๕. คดีหลอกลวงให้กู้เงิน
๖. คดีหลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ
๗. คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วเราให้โอนเงิน

๘. คดีที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์โดยผิดกฎหมาย เพื่อให้ได้ไปซึ่งทรัพย์

๙. คดีที่มีการเข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อกรรโชกหรือรีดเอาทรัพย์สิน

๑๐. คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์เพื่อให้ได้ไปซึ่งทรัพย์

๑๑. คดีหลอกลวงเกี่ยวกับทรัพย์สินดิจิทัล

๑๒. คดีหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์

๑๓. คดีหลอกลวงซื้อขายสินค้าหรือบริการที่มีลักษณะเป็นขบวนการ

๑๔. คดีหลอกลวงให้ลงทุนที่เป็นความผิดตามพระราชกำหนดการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ. ๒๕๒๗

๑๕. คดีอาชญากรรมทางเทคโนโลยีลักษณะอื่นนอกเหนือจากข้อ ๑ - ๑๔

นอกจากนี้ ข้อมูลจากสำนักงานตำรวจแห่งชาติโดย พล.ต.ต.นิเวศน์ อาภาวศิน รองผบช.สอท.กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (ตำรวจไซเบอร์) ระบุว่า รูปแบบคดีอาชญากรรมเทคโนโลยีที่ประชาชนถูกหลอกลวงยังมีลักษณะคล้าย ๆ เดิม แต่ยังคงมีผู้เสียหายถูกหลอกลวงมากขึ้นเรื่อย ๆ โดยประชาชนส่วนใหญ่ที่ถูกหลอกลวงไม่ได้ติดตามข่าวสาร และไม่รู้วิธีการรับมือกับแก๊งค์คอลเซ็นเตอร์ ว่าคนร้ายสามารถปลอมเบอร์โทรศัพท์หรือ ชื่อผู้ส่งข้อความสั้นได้ ดังนั้น เมื่อคนร้ายแอบอ้างตัวเป็นเจ้าหน้าที่ของรัฐ ประชาชนจึงมีแนวโน้มที่จะหลงเชื่อ แล้วถูกดึงให้ไปต่อในแอปลิเคชั่นไลน์ ซึ่งคนร้ายสามารถปลอมโปรไฟล์เป็นใครก็ได้อย่างแนบเนียน ทำให้ผู้เสียหายหลงเชื่อและโอนเงินในให้คนร้ายที่มักใช้วิธีข่มขู่ว่าไปเกี่ยวพันกับการฟอกเงิน ต้องโอนเงินไปตรวจสอบความบริสุทธิ์ หรือ หลอกให้ติดตั้งแอปลิเคชั่นที่สามารถดึงเงินในบัญชีผู้เสียหายออกไปได้ เป็นต้น

๒.๒ ลักษณะของพยานหลักฐานอิเล็กทรอนิกส์

ก. อาชญากรรมทางคอมพิวเตอร์มักไม่ปรากฏพยานหลักฐานในเชิงประจักษ์ ต้องอาศัยการรวบรวมพยานแวดล้อมต่าง ๆ อาทิ ข้อมูลจราจรคอมพิวเตอร์ ข้อมูลการโทรศัพท์ติดต่อสื่อสารกับผู้ร่วมกระทำด้วยกัน และการติดต่อกับผู้เสียหาย ซึ่งผู้กระทำมักจะใช้วิธีติดต่อมาจากต่างประเทศโดยโทรศัพท์ผ่านระบบอินเตอร์เน็ตซึ่งไม่สามารถตรวจเช็คเบอร์โทรศัพท์ได้ นอกจากนี้ยังปลอมแปลงหรือกำหนดเบอร์ให้เสมือนเป็นเบอร์ภายในประเทศ เพื่อหลอกลวงให้เหยื่อเชื่อถือ ซึ่งความเป็นจริงไม่มีเบอร์ดังกล่าวที่ลงทะเบียนไว้ตามกฎหมาย

ข. ประเภทของพยานหลักฐานที่เกี่ยวข้องในคดีอาชญากรรมคอมพิวเตอร์ ส่วนใหญ่เป็นพยานหลักฐานอิเล็กทรอนิกส์ มีลักษณะแตกต่างจากพยานหลักฐานในคดีทั่วไป เช่น ข้อมูลจราจรทางคอมพิวเตอร์ หรือ Log file[๓] ข้อมูลคอมพิวเตอร์[๔] ข้อมูลเส้นทางการเงิน และข้อมูลการติดต่อสื่อสาร นอกจากนี้ ยังมีวัตถุพยานเป็นประเภทอุปกรณ์อิเล็กทรอนิกส์ อาทิ เครื่องคอมพิวเตอร์ - สมาร์ตโฟนและ

๓"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

๔ "ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

(ตามมาตรา ๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐)

ข้อมูลภายในอุปกรณ์ ส่วนพยานบุคคล ได้แก่ ผู้ดูแลเว็บไซต์ ผู้ดูแลระบบข้อมูลต่าง ๆ ผู้ดูแลเครือข่ายอินเตอร์เน็ต ISP ผู้ให้บริการเครือข่ายโทรศัพท์ พนักงานธนาคารที่เกี่ยวข้อง และผู้ดูแลข้อมูลธนาคาร เป็นต้น

ค. พยานหลักฐานอิเล็กทรอนิกส์มีลักษณะเปราะบางสามารถถูกดัดแปลง เปลี่ยนแปลงได้ง่าย ข้อมูลอิเล็กทรอนิกส์บางประเภทสามารถลบ ทำลายให้สูญหายโดยไม่ทิ้งร่องรอย

ดังนั้น เมื่อมีผู้เสียหายมาแจ้งความร้องทุกข์ต่อพนักงานสอบสวนเพื่อให้ดำเนินคดีกับผู้กระทำความผิดอาชญากรรมคอมพิวเตอร์ ความท้าทายของการรวบรวมและเก็บรักษาพยานหลักฐานอิเล็กทรอนิกส์ให้ครบถ้วน หรือให้ได้มากที่สุด สอดคล้องกันกับพยานหลักฐานต่าง ๆ และร้อยเรียงกันถึงขนาดที่เมื่อนำมาปะติดปะต่อกันแล้วครบองค์ประกอบความผิด และสามารถระบุได้ว่าใครเป็นผู้กระทำกระทำความผิดอย่างไร เกิดเหตุที่ใดเมื่อใด ทำให้ผู้ใดเสียหาย เสียหายอย่างไรและเพียงใด ไปจนตลอดถึงนำสืบพิสูจน์ต่อศาลให้เห็นถึงความสมบูรณ์ ถูกต้อง แท้จริง ไม่ถูกบิดเบือน ดัดแปลง หรือสูญหายทั้งหมดหรือบางส่วน จึงเป็นภาระหน้าที่ของเจ้าพนักงานชั้นสืบสวนสอบสวน รวมไปถึงพนักงานอัยการหรือโจทก์ในชั้นดำเนินคดีต้องทำความเข้าใจอย่างต่อเนื่องและเชื่อมโยงกันเพื่อสามารถนำพยานหลักฐานขึ้นสู่ชั้นพิจารณาของศาลได้อย่างชัดเจนปราศจากข้อสงสัยจนสามารถนำผู้กระทำความผิดมาลงโทษได้

๒.๓ ปัญหาและอุปสรรคในการรวบรวมเก็บรักษา และนำสืบพยานหลักฐานอิเล็กทรอนิกส์ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์

ดังที่กล่าวมาแล้วในข้อ ๒.๑ และ ๒.๒ เห็นได้ว่ารูปแบบอาชญากรรมทางคอมพิวเตอร์ ผู้กระทำมักจะกระทำเป็นขบวนการมีการตระเตรียมการวางแผนเพื่อหลอกลวงทั้งเหยื่อและเพื่อปกปิดวิธีการดำเนินการที่จะเชื่อมโยงกลุ่มผู้กระทำมิให้ถูกจับกุมได้ โดยมีทั้งการปลอมแปลงเบอร์โทรศัพท์ ปลอมแปลงข้อมูล ปลอมแปลงตัวตน ปิดบัง ซ่อนเร้นข้อมูลเกี่ยวกับตนเองได้อย่างแนบเนียน โดยการปลอมตนเป็นคนอื่น หรือแอบอ้างตนเป็นเจ้าหน้าที่ของรัฐ เป็นการกระทำที่ไม่ปรากฏตัวตนที่แท้จริงต่อหน้าเหยื่อหรือผู้เสียหาย เป็นการกระทำความผิดที่สามารถเริ่มต้นการกระทำความผิดไปจนจบสิ้นกระบวนการ ฉ้อโกง กรรโชกทรัพย์ หรือรีดเอาทรัพย์ได้โดยไม่ต้องปรากฏตัวในสถานที่ใดสถานที่หนึ่ง จึงไม่มีประจักษ์พยานที่พบเห็นตัวตนหรือหน้าตาที่แท้จริงของผู้กระทำ ไม่ทิ้งร่องรอย หรือทรัพย์ที่ใช้ในการกระทำความผิดไว้ในที่เกิดเหตุ ไม่มี ทั้งพยานบุคคลและวัตถุพยานในสถานที่เกิดเหตุ

ดังนั้น ปัญหาและอุปสรรคที่สำคัญของการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์นั้น คือความซับซ้อนในการรวบรวมพยานหลักฐานเพื่อเอาผิดกับผู้กระทำผิดให้เชื่อมโยงไปจนถึงผู้ร่วมสมคบในขบวนการทั้งหมด โดยเฉพาะอย่างยิ่งพยานหลักฐานอิเล็กทรอนิกส์ ปัญหาและอุปสรรคในการรวบรวมเก็บรักษา และนำสืบพยานหลักฐานอิเล็กทรอนิกส์ อาจแบ่งพิจารณาตามขั้นตอนในกระบวนการยุติธรรมได้เป็น ๓ ขั้นตอน ดังนี้

๑. ชั้นสืบสวนสอบสวน

ในชั้นสืบสวนสอบสวนนี้ จะเป็นความยากในการสืบค้น เข้าถึงข้อมูลอิเล็กทรอนิกส์ที่อาจมีอยู่ในเส้นทางการส่งรับข้อมูลบนระบบออนไลน์ที่ผู้ใช้โดยทั่วไปไม่สามารถลบได้ หรือข้อมูลอิเล็กทรอนิกส์บางประเภทที่อยู่ในอุปกรณ์อิเล็กทรอนิกส์สามารถลบได้ แต่อาจหลงเหลืออยู่แม้มีการพยายามลบทิ้งทำลายพยานหลักฐาน ซึ่งกรณีเช่นนี้จำเป็นต้องใช้วิธีการกู้คืนข้อมูลอิเล็กทรอนิกส์ อันเป็นเรื่องทางเทคนิคที่ต้องอาศัยผู้มีความรู้ความสามารถเฉพาะทางเทคโนโลยีคอมพิวเตอร์ ไม่ใช่พนักงานสอบสวน พนักงานตำรวจผู้จับกุมทุกคนจะสามารถทำได้ ดังนั้น จะเห็นได้ว่าในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้มีกฎหมายกำหนดพนักงานเจ้าหน้าที่ไว้โดยเฉพาะ ดังในประกาศกระทรวงเทคโนโลยี

สารสนเทศและการสื่อสาร (ปัจจุบันได้เปลี่ยนเป็นการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม)[๕] เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้กำหนดคุณสมบัติของพนักงานเจ้าหน้าที่ที่จะมาปฏิบัติงานตามพระราชบัญญัตินี้ ไว้ในข้อ ๒[๖] มีสาระสำคัญว่า พนักงานเจ้าหน้าที่ ต้องเป็นผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์ สำเร็จการศึกษาในสาขาที่เกี่ยวข้องกับงาน คือ วิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์ ที่สำคัญ คือ ต้องผ่านการอบรมทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) สืบสวน สอบสวน และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) และต้องมีประสบการณ์ในการทำงานที่เกี่ยวข้องกับการตรวจพิสูจน์พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์หรือพยานหลักฐานอิเล็กทรอนิกส์ ความมั่นคงปลอดภัยของระบบสารสนเทศ หรือการดำเนินคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ ซึ่งในการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) นั้น มีความจำเป็นและมีความสำคัญมาก เนื่องจากต้องมีมาตรฐานเป็นที่น่าเชื่อถือได้ จึงจะสามารถนำพยานหลักฐานอิเล็กทรอนิกส์ไปใช้ในชั้นพิจารณาได้ ซึ่งเรื่องมาตรฐานของการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) จะได้กล่าวโดยละเอียดในบทต่อไป

กรณีของการดำเนินคดีอาญาตามประมวลกฎหมายอาญา หรือตามกฎหมายอื่นที่มีโทษทางอาญาซึ่งอยู่ในอำนาจการสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา และพยานหลักฐานในคดีเป็นพยานหลักฐานอิเล็กทรอนิกส์ พนักงานสอบสวนสามารถร้องขอความช่วยเหลือจากพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้

---

[๕] เมื่อวันที่ ๑๕ กันยายน พ.ศ. ๒๕๕๙ ได้มีประกาศราชกิจจานุเบกษา ให้พระราชบัญญัติ ปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ ๑๗) พ.ศ. ๒๕๕๙ ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไปคือ วันที่ ๑๖ กันยายน พ.ศ. ๒๕๕๙ โดยมีสาระสำคัญ คือให้ยกเลิกกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และให้จัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมขึ้นมาแทน (เปลี่ยนชื่อกระทรวง)โดยมาตรา ๒๑ ให้โอนบรรดาอำนาจหน้าที่เกี่ยวกับการปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับประกาศ คำสั่ง และมติคณะรัฐมนตรีของรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารไปเป็นอำนาจหน้าที่ของรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมบรรดาบทบัญญัติแห่งกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ คำสั่ง หรือมติคณะรัฐมนตรีใดที่อ้างถึงรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ให้ถือว่าอ้างถึงรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

[๖] พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ต้องมีคุณสมบัติ ดังต่อไปนี้ (๑) มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์ (๒) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์ (๓) ผ่านการอบรมทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) สืบสวน สอบสวน และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) ตามภาคผนวกท้ายประกาศนี้และ (๔) มีคุณสมบัติอื่นอย่างหนึ่งอย่างใด ดังต่อไปนี้ ก. รับราชการหรือเคยรับราชการไม่น้อยกว่าสองปีในตำแหน่งเจ้าหน้าที่ตรวจ พิสูจน์พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์หรือพยานหลักฐานอิเล็กทรอนิกส์ ข. สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาตรีและมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสี่ปี ค. สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาโท หรือสอบได้ได้เป็นเนติบัณฑิตตามหลักสูตรของสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสามปี ง. สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาเอก หรือมีประสบการณ์ที่ เป็นประโยชน์ต่อการปฏิบัติงาน ตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสองปี จ.เป็นบุคคลที่ทำงานเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์หรือมีประสบการณ์ในการดำเนินคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ไม่น้อยกว่าสองปี

อย่างไรก็ดี แม้พนักงานเจ้าหน้าที่ตามพระราชบัญญัติฯดังกล่าว จะมีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์ แต่ก็ยังมีอุปสรรคเป็นระยะเวลาที่พนักงานเจ้าหน้าที่ต้องเร่งดำเนินการเก็บรวบรวมพยานหลักฐานโดยเร็วก่อนที่ข้อมูลจราจรคอมพิวเตอร์ และข้อมูลอิเล็กทรอนิกส์ต่างๆจะหายไป เนื่องจากการเก็บข้อมูลสำหรับผู้ให้บริการอินเตอร์เน็ต หรือเจ้าของแพลตฟอร์มออนไลน์ต่างๆ ต้องใช้หน่วยความจำจำนวนมากแปรผันตามจำนวนผู้ใช้บริการ อีกทั้งการใช้เนื้อที่เก็บสำรองข้อมูลไว้เป็นระยะเวลานานก็มีค่าใช้จ่ายที่สูงขึ้นเรื่อยๆ ดังนั้น เพื่อป้องกันผู้ให้บริการ[๗] ลบข้อมูลไปอย่างรวดเร็ว มาตรา ๒๖ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จึงได้ถูกแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ กำหนดให้ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปี (จากเดิม ๑ ปี) เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ดังนั้น พนักงานเจ้าหน้าที่ จึงต้องเร่งเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ให้แล้วเสร็จภายในเวลาดังกล่าว นอกจากนี้ หากเป็นกรณีข้อมูลอิเล็กทรอนิกส์ไม่ได้อยู่ในระบบของผู้ให้บริการ แต่เป็นข้อมูลอิเล็กทรอนิกส์ที่อยู่ในความครอบครองของบุคคลทั่วไป แต่สามารถใช้เป็นพยานหลักฐานได้เสมือนประจักษ์พยาน เช่น ภาพบันทึกจากกล้องวงจรปิดที่ประชาชนติดตั้งกันเองไว้ป้องกันความปลอดภัยของตนและทรัพย์สินแต่สามารถบันทึกพฤติการณ์แวดล้อมในคดีไว้ได้ เป็นต้นว่า กล้องวงจรปิดรอบๆบริเวณเส้นทาง หรือสถานที่ที่กลุ่มผู้ต้องเดินทางมาเพื่อนัดพบประชุมวางแผนกันที่สามารถเห็นหน้า หรือรูปพรรณสัณฐานผู้ต้องหาหรือภาพขณะผู้ต้องหามาใช้บริการอินเตอร์เน็ตสาธารณะในร้านกาแฟหรือ Co - Working Space ซึ่งเป็นสถานประกอบการของเอกชนให้บริการแก่บุคคลทั่วไป มีเจตนาหลบหนีการตามสืบโดยหลีกเลี่ยงการใช้คอมพิวเตอร์ในบ้านพักตนเอง หรือใช้อินเตอร์เน็ตที่ตนเองหรือครอบครัวลงทะเบียนไว้ ซึ่งภาพที่กล้องวงจรปิดของเอกชนที่บันทึกไว้ได้อาจจะสอดคล้องกับข้อมูลจราจรคอมพิวเตอร์ หรือ ข้อมูลการใช้อินเตอร์เน็ตว่ามาใช้บริการเพื่อหลอกลวงเหยื่อ และเพื่อการกระทำความผิด ณ สถานที่ใด ข้อมูลเหล่านี้อาจไม่อยู่ในกรอบเวลาตามกฎหมายที่ต้องเก็บรักษาไว้ และมีระยะเวลาการเก็บรักษาที่ไม่แน่นอน ดังนั้น ข้อมูลอิเล็กทรอนิกส์เหล่านี้จึงเปราะบางสูญหายได้ และหากถูกเก็บไว้ในเวลาอันสั้น พนักงานเจ้าหน้าที่ก็อาจเก็บรวบรวมได้ไม่ทัน ทำให้ขาดพยานหลักฐานอันสำคัญไปได้

๒. ชั้นพิจารณาสำนวนทำความเห็นและคำสั่งฟ้อง จนถึงนำพยานหลักฐานเข้าสืบในการพิจารณาคดี

ในชั้นพิจารณาสำนวนสอบสวนทำความเห็นและคำสั่งฟ้อง จนถึงนำพยานหลักฐานเข้าสืบในการพิจารณาคดี พนักงานอัยการต้องพิเคราะห์พยานหลักฐานทั้งปวงในคดีว่า คดีมีพยานหลักฐานพอฟ้อง และเพียงพอต่อการนำสืบพิสูจน์ความผิดของผู้ต้องหาในชั้นพิจารณาของศาลหรือไม่เพียงใด ตามระเบียบสำนักงานอัยการสูงสุดว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ. ๒๕๖๓ ข้อ ๓๓ ที่กำหนดให้พนักงานอัยการต้องตรวจสอบความถูกต้องของสำนวนการสอบสวนและพิจารณาสั่งสำนวนโดยละเอียดรอบคอบ เมื่อพนักงานอัยการได้รับสำนวนการสอบสวนจากพนักงานสอบสวนแล้วหากพนักงานอัยการเห็นว่าการสอบสวนยังไม่ครบถ้วนถูกต้องตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา ๑๔๓ วรรคสอง (ก) พนักงานอัยการมีอำนาจสั่งตามที่เห็นควรให้พนักงานสอบสวนดำเนินการสอบสวนเพิ่มเติมหรือส่งพยานคนใดมาให้ซักถามเพื่อสั่งต่อไป

---

[๗] ผู้ให้บริการ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หมายถึง (๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น (๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

จะเห็นได้ว่า พนักงานอัยการต้องพิจารณาพยานหลักฐานก่อนมีคำสั่งฟ้องคดีอย่างละเอียดรอบคอบ ดังนั้น ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่มีพยานหลักฐานอิเล็กทรอนิกส์ประกอบอยู่ด้วย พนักงานอัยการจึงต้องมีความเข้าใจบริบทของอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัล และลักษณะของพยานหลักฐานอิเล็กทรอนิกส์อย่างชัดแจ้งทุกขั้นตอน ก่อนที่จะพิจารณาต่อไปได้ หากพนักงานอัยการไม่เข้าใจกระบวนการ หรือเส้นทางของข้อมูลอิเล็กทรอนิกส์ ข้อมูลจราจรคอมพิวเตอร์ ไม่รู้จักวิธีการทำงานของแพลตฟอร์มออนไลน์ต่าง ๆ การนำส่งข้อมูลผ่านระบบคอมพิวเตอร์ ระบบอินเตอร์เน็ต เทคโนโลยีดิจิทัลต่าง ๆ ย่อมไม่อาจทราบได้ว่าพยานหลักฐานที่มีอยู่ในสำนวนครบถ้วนเพียงพอแล้วหรือไม่ มีความจำเป็นต้องสั่งสอบสวนเพิ่มเติมหรือไม่เพียงใด และอาจจะเป็นอุปสรรคนำไปสู่ปัญหาการพิจารณาสั่งสำนวนต่อไป

เมื่อได้รับพยานหลักฐานเข้าในสำนวนครบถ้วนเพียงพอแล้ว ในขั้นตอนการพิจารณามีคำสั่งฟ้อง หรือไม่ฟ้อง พนักงานอัยการต้องพิจารณาว่าเป็นพยานหลักฐานซึ่งน่าจะพิสูจน์ความผิดหรือความบริสุทธิ์ของผู้ต้องหาได้หรือไม่ ทั้งพยานบุคคล พยานเอกสาร พยานวัตถุ นอกจากนี้ ยังต้องพิจารณาไปถึงแนวทางการสืบพยานหลักฐาน ประกอบข้อกฎหมาย จะทำให้ศาลลงโทษได้หรือไม่

ในชั้นสืบพยาน พนักงานอัยการหรือโจทก์ ต้องนำสืบพยานหลักฐานพิสูจน์ความผิด และการกระทำความผิดของจำเลยให้เชื่อมโยงกันจนปราศจากข้อสงสัยว่าบุคคลนี้เป็นผู้กระทำความผิดตามฟ้องของโจทก์จริง ซึ่งคดีอาชญากรรมคอมพิวเตอร์นั้น จำเป็นต้องอาศัยพยานหลักฐานต่าง ๆ รวมทั้งพฤติการณ์แวดล้อมประกอบกัน ทั้งพยานอิเล็กทรอนิกส์ พยานแวดล้อม พยานบุคคล พยานเอกสาร พยานวัตถุต่าง ๆ ต้องสอดคล้องตรงกัน พุ่งเป้าไปยังจำเลยว่าเป็นผู้กระทำความผิดโดยแน่แท้ ปราศจากข้อสงสัย เป็นผู้ใดอื่นไปไม่ได้ ต้องแสดงถึงวิธีการกระทำความผิด สถานที่กระทำความผิด ที่อาจจะไม่ใช่เพียงข้อมูลภูมิลำเนาหรือการอ้างถิ่นที่อยู่ดังเช่นคดีทั่วไปเท่านั้นว่าขณะกระทำความผิดจำเลยอยู่ที่ใด แต่จะต้องเชื่อมโยงสถานที่ก่อเหตุเข้ากับข้อมูลจราจร คอมพิวเตอร์ที่ระบุได้อย่างละเอียดว่า คอมพิวเตอร์เครื่องใด เลขที่ใด ที่ใช้ในการกระทำความผิด และขณะก่อเหตุ หรือขณะเกิดเหตุนั้น ผู้ใดเป็นผู้ใช้เครื่องคอมพิวเตอร์นั้น และเพราะเหตุใดจึงระบุได้ว่าเครื่องคอมพิวเตอร์นั้น เป็นเครื่องมือที่ใช้กระทำความผิด โดยต้องเชื่อมโยงระหว่างเครื่องคอมพิวเตอร์ที่มีIP Address[๔]ตรงกับเลขหมายที่ใช้สัญญาณอินเตอร์เน็ต จนสามารถระบุว่า เครื่องคอมพิวเตอร์อยู่ที่ใด และใช้บริการอินเตอร์เน็ตเครือข่ายใด ติดต่อไปยังที่ใดบ้าง ซึ่งข้อมูลจราจรคอมพิวเตอร์จะแสดงให้เห็นความเกี่ยวข้องเชื่อมโยงและเกี่ยวพันกับเครือข่ายผู้กระทำความผิด เชื่อมโยงข้อมูล ตรงกับเหยื่อผู้ได้รับความเสียหายจากการกระทำความผิด เชื่อมโยงกับข้อมูลจากเครือข่ายผู้ให้บริการอินเทอร์เน็ต ต่างๆเหล่านี้ ต้องมีความเข้าใจในระบบคอมพิวเตอร์ เส้นทางจราจรคอมพิวเตอร์ หลักการทำงานของการเชื่อมโยงข้อมูลผ่านระบบดิจิทัล และผ่านระบบออนไลน์จึงจะสื่อสารให้ศาลเข้าใจได้

---

[๔] IP Address คือ (Internet Protocol Address) เป็นหมายเลขประจำเครื่องคอมพิวเตอร์โดยคอมพิวเตอร์ในระบบเครือข่ายจะมีหมายเลขประจำเครื่องเป็นของตัวเองที่ใช้ Protocol TCP/IP โดยสามารถเปรียบเทียบให้เข้าใจง่าย ๆ คือ IP Address ก็เหมือนเลขที่บ้าน, หมายเลขห้อง, หมายเลขโทรศัพท์, เป็นต้น IP Address มีความสำคัญ เช่น การส่งไฟล์ หากันระหว่างสองเครื่องจำเป็นต้องมีที่อยู่ผู้ส่ง และ ผู้รับเพื่อให้สามารถติดต่อสื่อสารกันได้ จะไม่ได้เกิดความผิดพลาดของข้อมูลเวลาทำการส่ง IP Address จะประกอบไปด้วยตัวเลข ๔ ชุดและจะมีเครื่องหมายจุดขั้นกลางระหว่างตัวเลขของชุด (Private IP) โดยหมายเลข IP Address ของคอมพิวเตอร์แต่ละเครื่องนั้นจะไม่ซ้ำกัน , ข้อมูลจาก https://www.vrproservice.com/ข่าวสารและความรู้/IP-Address-Subnet-Mask-ที่ควรรู้

๓. ชั้นพิจารณา รับฟัง ชั่งน้ำหนักพยานหลักฐาน และตัดสินคดี

ในชั้นนี้ เมื่อพนักงานอัยการมีคำสั่งฟ้อง คดีก็จะขึ้นสู่การพิจารณาชั้นศาล ซึ่งทั้งโจทก์และจำเลยต่างต้องนำสืบพยานหลักฐานเพื่อสนับสนุน คำฟ้องและคำให้การของตน ทั้งข้ออ้าง ข้อสนับสนุน และข้อต่อสู้ทั้งหลายต่อศาล ซึ่งศาลจะมีหลักเกณฑ์การรับฟังและชั่งน้ำหนักพยานหลักฐานอย่างเคร่งครัดเพื่อตัดสินคดี

ปัญหาการพิจารณาคดีอาญาในชั้นศาลที่มีพยานหลักฐานอิเล็กทรอนิกส์เข้ามามีส่วนสำคัญนั้น ได้มีบทความทางวิชาการ[๙] นำเสนอว่า *“เมื่อมีข้อพิพาทหรือมีการกระทำความผิดทางอาญาเกิดขึ้น ภาพหรือเสียงที่ถูกบันทึกในอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆก็จะถูกนำมาใช้อ้างเป็นพยานหลักฐานในชั้นศาล ซึ่งนับวันพยานหลักฐานประเภทนี้ก็ยิ่งจะทวีความสำคัญมากขึ้นเมื่อทนายความและพนักงานอัยการกล่าวอ้างพยานวัตถุประเภทนี้เพิ่มมากขึ้น ผู้พิพากษาจึงควรตระหนักและให้ความสำคัญกับพยานหลักฐานดังกล่าวเพราะมีความแตกต่างไปจากพยานวัตถุประเภทอื่น เช่น อาวุธหรือยาเสพติด ซึ่งสามารถเห็นประจักษ์และจับต้องได้ตั้งแต่ต้น ส่วนภาพหรือเสียงที่ถูกบันทึกในอุปกรณ์อิเล็กทรอนิกส์ ไม่สามารถเห็นประจักษ์ได้ในทันที เนื่องจากคู่ความจะต้องทำสำเนาใส่ไว้ในแผ่นซีดี แผ่นดีวีดี หรือแฟลชไดร์ฟยื่นเสนอต่อศาลเพื่อใช้เป็นพยานหลักฐานสนับสนุนข้อกล่าวอ้างหรือข้อโต้เถียงของตน หากศาลหรือคู่ความฝ่ายตรงข้ามต้องการตรวจสอบภาพหรือเสียงดังกล่าว ก็ต้องใช้เครื่องมืออุปกรณ์เฉพาะในการแสดงภาพหรือเสียงผ่านทางจอภาพหรือลำโพงในภายหลัง จึงจะสามารถรับรู้เหตุการณ์ที่ถูกบันทึกไว้ได้ ซึ่งเป็นข้อจำกัดสำคัญของพยานวัตถุประเภทนี้ หากต่างฝ่ายต่างตรวจดูภาพหรือเสียงคนละคราวกัน ย่อมสื่อสารกันได้ยากลำบาก ว่าต้องการอ้างภาพหรือเสียงสนับสนุนข้อกล่าวอ้างหรือข้อโต้เถียงของตนในลักษณะใด และอีกฝ่ายจะนำพยานหลักฐานเข้านำสืบหักล้างอย่างไร ด้วยคุณสมบัติเฉพาะดังกล่าวจึงจำเป็นอย่างยิ่งที่ทนายความหรือพนักงานอัยการต้องแสดงพยานวัตถุประเภทภาพหรือเสียงที่ถูกบันทึกในอุปกรณ์อิเล็กทรอนิกส์ต่อศาลโดยเร็ว เพื่อให้ผู้พิพากษาบริหารจัดการพยานวัตถุประเภทดังกล่าวไม่ให้เป็นอุปสรรคต่อการพิจารณาพิพากษาคดีด้วยความถูกต้อง เป็นธรรม และรวดเร็ว”*

ดังนั้น ปัญหาและอุปสรรคในการนำสืบพยานหลักฐานอิเล็กทรอนิกส์ ในชั้นศาลนั้น นอกจากความน่าเชื่อถือในความถูกต้องครบถ้วนของพยานหลักฐานอิเล็กทรอนิกส์แล้วนั้น ยังเป็นเรื่องของระยะเวลาในการยื่นพยานหลักฐานอิเล็กทรอนิกส์ให้ศาลและคู่ความอีกฝ่ายสามารถตรวจสอบได้ด้วย

---

[๙] คมศร พรหมพิทยายุทธ. (๒๕๖๖). *ข้อพิจารณาในการสืบพยานหลักฐานดิจิทัลประเภทภาพหรือเสียงที่มีผลกระทบต่อการพิจารณาคดีต่อเนื่องและคำพิพากษา.*,ห้องสมุดศาลยุติธรรม (ออนไลน์)

https://library.coj.go.th/th/media/๖๑๙๕๖/media-๖๑๙๕๖.html

บทที่ ๓
แนวทางการแก้ไขปัญหาและอุปสรรคในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัล

จากบทที่ ๒ ที่ได้กล่าวถึงสภาพปัญหาและอุปสรรคในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมคอมพิวเตอร์ สรุปสาระสำคัญได้ว่า ปัญหาและอุปสรรคในชั้นสอบสวนคดี คือ ข้อจำกัดในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์เกี่ยวกับเรื่องระยะเวลา และความซับซ้อนในการค้นพบ กู้คืน และเก็บรวบรวม ในชั้นพิจารณาสั่งฟ้อง คือ ความเข้าใจของพนักงานอัยการ หรือโจทก์ ในที่มาและความเชื่อมโยงของพยานหลักฐานอิเล็กทรอนิกส์ต่างๆในสำนวนการสอบสวน เพื่อที่จะสามารถนำไปใช้ในการสืบพยานในชั้นศาลได้อย่างครบถ้วนถูกต้องและพิสูจน์การกระทำความผิดของผู้ต้องหาได้อย่างชัดเจน สำหรับในชั้นพิจารณาของศาล คือ เรื่องของความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ และความเป็นธรรมในการตรวจสอบพยานหลักฐาน โดยในบทนี้จะนำเอาหลักเกณฑ์ บทกฎหมาย ระเบียบที่เกี่ยวข้องมาเป็นเครื่องมือในการวิเคราะห์ผ่านตัวอย่างคดีอาชญากรรมคอมพิวเตอร์ เพื่อหาแนวทางการแก้ไขปัญหาและอุปสรรคในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัล

๓.๑ กฎหมายและระเบียบกฎเกณฑ์ที่เกี่ยวข้อง

ก. ประมวลกฎหมายอาญา
ข. ประมวลกฎหมายวิธีพิจารณาความอาญา
ค. ประมวลกฎหมายวิธีพิจารณาความแพ่ง
ง. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔
จ. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
ฉ. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐
ช. พระราชกำหนดมาตรการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.๒๕๖๖
ซ. ประกาศคณะกรรมการบริหารศาลยุติธรรม เรื่อง การจัดตั้งแผนกคดีอาชญากรรมทางเทคโนโลยีในศาลอาญา
ฌ. คำสั่งสำนักงานตำรวจแห่งชาติที่ ๑๘๒/๒๕๖๖ลงวันที่ ๑๗ มีนาคม ๒๕๖๖
ญ. คำสั่งสำนักงานอัยการสูงสุดที่ ๘๓๒/๒๕๖๗ ลงวันที่ ๒๙ เมษายน ๒๕๖๗

ปัจจุบันได้มีการตรากฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และธุรกรรมทางอิเล็กทรอนิกส์ ออกมาหลายฉบับอย่างต่อเนื่อง เพื่อป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อสอดรับกับการทำธุรกรรมทางอิเล็กทรอนิกส์ที่มีเพิ่มขึ้นจำนวนมากแบบก้าวกระโดดและขยายวงกว้าง เพื่อให้เท่าทันกับยุคสมัย และรูปแบบอาชญากรรมที่เปลี่ยนแปลงพัฒนาไปอย่างรวดเร็ว และเพื่อแก้ปัญหาเกี่ยวกับการนำสืบพยานหลักฐานอิเล็กทรอนิกส์ในการดำเนินคดีต่อศาล เนื่องจากแต่เดิมมีประเด็นสงสัยว่า พยานหลักฐานอิเล็กทรอนิกส์นั้น เป็นพยานประเภทใด พยานวัตถุ หรือ พยานเอกสาร ซึ่งต่างจากพยานวัตถุที่กฎหมายไม่ได้กำหนดให้ต้องนำต้นฉบับมานำสืบ

อย่างไรก็ดี ในคดีอาญาแม้จะไม่ได้กำหนดไว้ว่าเป็นพยานประเภทใดก็ตาม แต่ก็ต้องเทียบเคียงกับคำพิพากษาฎีกาที่ ๔๓๑๑/๒๕๕๗[๑๐] ที่วางหลักให้ถือว่าเป็นพยานเอกสาร

นอกจากนี้ ยังมีประเด็นต่อมาว่าตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา ๒๓๘วางหลักให้ต้นฉบับเอกสารเท่านั้นที่อ้างเป็นพยานได้ ดังนั้น พยานหลักฐานที่มีน้ำหนักน่าเชื่อถือที่สุดและศาลจะรับฟังลงโทษจำเลยนั้น จึงเป็นต้นฉบับเอกสาร เว้นแต่ถ้าหาต้นฉบับไม่ได้ สำเนาที่รับรองว่าถูกต้องหรือพยานบุคคลที่รู้ข้อความก็อ้างเป็นพยานได้ เมื่อ พยานหลักฐานที่อยู่ในรูปแบบอิเล็กทรอนิกส์ ไม่มีรูปร่าง จับต้องไม่ได้ ในขณะที่ยังไม่มีการนำเสนอพยานหลักฐานอิเล็กทรอนิกส์ต่อศาลผ่านจอภาพ คอมพิวเตอร์หรือสื่อเทคโนโลยีระบบดิจิทัล การนำเสนอพยานหลักฐานอิเล็กทรอนิกส์จึงต้องพิมพ์ออกมาจากระบบเป็นเอกสารนำส่งศาล จึงมีประเด็นที่ต้องตีความว่า เอกสารที่พิมพ์ออกมานั้นถือว่าเป็นต้นฉบับเอกสารหรือไม่ผู้ใด หรือหน่วยงานใดเป็นผู้มีอำนาจหน้าที่ตามกฎหมายพิมพ์ออกมานำส่งเป็นพยานหลักฐานต่อศาล หากไม่ถือว่าเป็นต้นฉบับ ต้องมีการรับรองสำเนาโดยผู้มีอำนาจหน้าที่ตามกฎหมาย หรือต้องใช้พยานบุคคลที่รู้ข้อความเกี่ยวกับเอกสารมาเบิกความเป็นพยานรับรอง

อย่างไรก็ดี ปัจจุบันได้มีการตราพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ๒๕๔๔ โดยมีบทกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์[๑๑]โดยเฉพาะอยู่ในมาตรา ๑๑ ที่ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์นอกจากนี้ในประเด็นเรื่องต้นฉบับเอกสาร มาตรา ๑๐ วางหลักว่า ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ตามกฎหมายนี้ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว คือ (๑) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ (๒) สามารถแสดงข้อความนั้นในภายหลังได้

๓.๒ วิเคราะห์ปัญหาข้อเท็จจริงและข้อกฎหมายเพื่อนำไปสู่แนวทางการแก้ไขปัญหา

อาชญากรรมคอมพิวเตอร์ในปัจจุบันนั้นมีหลากหลายรูปแบบ งานศึกษานี้จะนำกรณีคดีอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นจริงในสังคมไทย มีการกระทำความผิดเป็นขบวนการที่แบ่งหน้าที่กันทำ และมีบางส่วนของ

---

[๑๐] ส่วนหนึ่งของคำพิพากษาฎีกาที่ ๔๓๑๑/๒๕๕๗ “ประมวลกฎหมายอาญา มาตรา ๑ (๗) ได้นิยามความหมายของคำว่า “เอกสาร”หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษรตัวเลขผังหรือแผนแบบอย่างอื่นจะเป็นโดยวิธีพิมพ์ถ่ายภาพหรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้นการที่จำเลยที่ ๑ ถึงที่ ๓ ร่วมกันพิมพ์หนังสือแต่งตั้งตัวแทนจำหน่ายอุปกรณ์กันระเบิดแบรนด์บาร์เทคพร้อมรายละเอียดดังกล่าวข้างต้นลงในเครื่องคอมพิวเตอร์ถือเป็นการใช้เครื่องคอมพิวเตอร์ซึ่งเป็นวัตถุอื่นใดทำให้ปรากฏความหมายซึ่งสามารถอ่านหรือเห็นความหมายได้โดยบุคคลที่พิมพ์ตัวอักษรนั้นแล้วเก็บไว้ในเครื่องคอมพิวเตอร์ดังกล่าวเพื่อเป็นหลักฐานซึ่งจำเลยที่ ๑ ถึงที่ ๓ สามารถนำไปใช้ได้เมื่อต้องการจะใช้จึงเป็นเอกสารตามความหมายของบทบัญญัติดังกล่าวแล้ว”

๑๑ **“ข้อมูลอิเล็กทรอนิกส์”** หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสารทั้งนี้ ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ๒๕๔๔มาตรา ๔

ขบวนการกระทำในต่างประเทศ หาประจักษ์พยานได้ยาก เป็นรูปแบบที่เกิดขึ้นบ่อย กระทบต่อประชาชนจำนวนมาก แต่ในที่สุดกลุ่มผู้ต้องหาได้ถูกเจ้าหน้าที่จับกุมดำเนินคดี จนมีคำพิพากษาศาลฎีกาแล้ว มาใช้เป็นกรณีศึกษาวิเคราะห์ปัญหาข้อเท็จจริงปรับเข้ากับข้อกฎหมายเพื่อเป็นแนวทางการแก้ไขปัญหา อุดช่องว่างเพื่อเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ต่อไป

คำพิพากษาฎีกาที่ ๓๒๓๖/๒๕๕๙

“คดีนี้โจทก์ฟ้อง นาย พ. จำเลย หนึ่งในขบวนการแก๊งคอลเซ็นเตอร์ โดยจำเลยร่วมกันกับพวกโทรศัพท์แสดงตนเป็นเจ้าหน้าที่ของรัฐหลอกลวงให้นางสาว ก. ผู้เสียหายและประชาชนโดยทั่วไปโอนเงินเข้าบัญชีที่จัดเตรียมไว้และใช้บัตรเอทีเอ็มเบิกถอนเงินทั้งในและนอกประเทศเป็นจำนวน ๒๙,๑๕๐,๑๘๕ บาท จำเลยให้การปฏิเสธ ศาลพิเคราะห์พยานหลักฐานของโจทก์แล้ว เห็นว่า โจทก์มี นายด. ผู้ร่วมขบวนการเบิกความประกอบ**หลักฐานการโอนเงิน**ไปยังจำเลย แสดงให้เห็นถึงการกระทำความผิดของจำเลย ที่จำเลยอ้างว่าเป็นเงินที่จำเลยรับโอนมาจากการประกอบธุรกิจโพยก๊วนและเป็นค่าผลไม้นั้น ถึงแม้อาชีพโพยก๊วนจะเป็นอาชีพที่ทำกันมาช้านาน แต่หาได้มีกฎหมายรองรับว่าเป็นการประกอบอาชีพโดยชอบแต่อย่างใดไม่ ในทางตรงกันข้ามการโอนเงินไปยังต่างประเทศโดยใช้วิธีโพยก๊วนย่อมเห็นได้ชัดว่าเป็นวิธีการโอนเงินนอกระบบมุ่งปกปิดสถานะของผู้ทำธุรกรรมทั้งสองฝ่ายเพื่อหลีกเลี่ยงการควบคุมตรวจสอบของทางราชการ อันเป็นการลักลอบนำเงินตราออกนอกประเทศเพื่อหลีกเลี่ยงการรายงานธุรกรรมทางการเงินตามกฎหมายอีกด้วย พยานหลักฐานของจำเลยขัดแย้งกับพยานหลักฐานอื่นในสำนวน ไม่มีน้ำหนักหักล้างพยานหลักฐานของโจทก์ จึงฟังได้ว่าจำเลยกระทำความผิดตามฟ้อง

พิพากษาว่า จำเลยมีความผิดตามประมวลกฎหมายอาญา มาตรา ๒๖๙/๕,๒๖๙/๖, ๒๖๙/๗, ๓๔๓ วรรคสอง ประกอบมาตรา ๓๔๒ (๑) และมาตรา ๘๓ พิเคราะห์พฤติการณ์แห่งคดีแล้ว เห็นว่า จำเลยร่วมกับพวกกระทำความผิดในลักษณะเป็นขบวนการองค์กรอาชญากรรมข้ามชาติ โดยไม่คำนึงถึงความเดือดร้อนของผู้อื่น ทั้งยังมีการแอบอ้างชื่อหน่วยงานความมั่นคงแห่งรัฐก่อให้เกิดความเสียหายอย่างร้ายแรงทางเศรษฐกิจกระทบต่อความน่าเชื่อและภาพลักษณ์ของประเทศ ซึ่งลักษณะการโอนเงินของจำเลยถือเป็นขั้นตอนสำคัญในการรวบรวมทรัพย์สินที่ได้จากการกระทำความผิดส่งออกนอกราชอาณาจักรเพื่อให้พ้นการตรวจสอบของรัฐ จึงเห็นสมควรลงโทษสถานหนัก การกระทำของจำเลยเป็นความผิดหลายกรรมต่างกันให้ลงโทษทุกกรรมเป็นกระทงความผิดไป รวมจำคุกทั้งหมด ๑๑๑ ปี แต่เนื่องจากมาตรา ๙๑(๒) กำหนดให้ลงโทษได้ไม่เกิน ๒๐ ปี ศาลจึงลงโทษได้ไม่เกินที่กฎหมายกำหนด และให้ร่วมกันคืนเงินแก่ผู้เสียหายริบของกลางทั้งหมด

จำเลยยื่นอุทธรณ์ ศาลอุทธรณ์พิพากษายกฟ้อง

คำวินิจฉัยของศาลฎีกา

จำเลยนำสืบต่อสู้ว่าไม่ได้ร่วมกระทำความผิด จำเลยมีอาชีพโพยก๊วน คือ การส่งเงินไปยังต่างประเทศโดยผ่านตัวแทนหักบัญชี ไม่มีการส่งเงินไปจริง แต่อาศัยความไว้เนื้อเชื่อใจของตัวแทนที่อยู่ในต่างประเทศ เห็นว่า การกระทำความผิดลักษณะแก๊งคอลเซ็นเตอร์เป็นขบวนการองค์กรอาชญากรรมข้ามชาติ และเกิดขึ้นเป็นประจำในประเทศไทย ซึ่ง**ยากที่จะนำสืบด้วยประจักษ์พยานได้** ส่วนตัวการสำคัญบางส่วนอยู่นอกประเทศ ส่วนที่อยู่ในประเทศจะหลบหนีออกนอกประเทศ คงเหลือแต่บางคนที่ไม่สามารถหลบหนีไปที่ใด ก็จะถูกจับกุม การพิสูจน์ความผิดต้องอาศัยคำรับของผู้กระทำความผิด พยานแวดล้อมกรณี พยานเอกสาร พฤติการณ์แห่งคดี และ พิรุธแห่งการกระทำเป็นเครื่องชี้เจตนา

สำหรับจำเลยนี้มี**หลักฐานการโอนเงิน** ที่จำเลยอ้างว่ามีอาชีพเป็นโพยก๊วน อาศัยความไว้เนื้อเชื่อใจกัน ต้องรู้จักผู้ที่โอนเงินเป็นอย่างดี ว่าเป็นใคร อยู่ที่ไหน มีอาชีพอะไร เงินที่ได้มาได้มาอย่างไร ชอบด้วยกฎหมายหรือไม่ การโอนเงินแบบโพยก๊วนเป็นการโอนเงินนอกระบบ หลีกเลี่ยงการควบคุมตรวจสอบของทางราชการ อันเป็นการลักลอบนำเงินตราออกนอกประเทศ เป็นการกระทำที่ไม่ชอบด้วยกฎหมาย ทั้งการติดต่อระหว่าง นาย ด. กับจำเลย ก็ไม่ได้ใช้ชื่อจริงตามหลักฐานทางทะเบียน จึงเป็นพิรุธ พยานหลักฐานที่โจทก์นำสืบมาฟังได้เป็นมั่นคงปราศจากข้อสงสัยว่า จำเลยได้ร่วมเป็นตัวการโดยแบ่งหน้าที่กันทำ อันเป็นความผิดตามฟ้อง ดังที่ศาลชั้นต้นได้วินิจฉัยมาโดยละเอียด ศาลฎีกาเห็นพ้องด้วย ส่วนที่ศาลอุทธรณ์พิพากษามานั้นไม่ต้องด้วยความเห็นของศาลฎีกา ฎีกาโจทก์ฟังขึ้น พิพากษาแก้เป็นว่า ให้บังคับไปตามคำพิพากษาศาลชั้นต้น แต่ไม่ริบของกลาง”

ข้อเท็จจริงในคำพิพากษาดังกล่าว เป็นตัวอย่างคดีอาชญากรรมทางคอมพิวเตอร์ที่ขณะนี้ระบาดอย่างหนัก เป็นขบวนการแก๊งคอลเซ็นเตอร์ โดยร่วมกันโทรศัพท์แอบอ้างตนเป็นเจ้าหน้าที่ของรัฐหลอกลวงให้นางสาว ก. ผู้เสียหายและประชาชนโดยทั่วไปโอนเงินเข้าบัญชีที่จัดเตรียมไว้และใช้บัตรเอทีเอ็มเบิกถอนเงินทั้งในและนอกประเทศ มีจำนวนความเสียหายทั้งสิ้นสูงถึงเกือบสามสิบล้านบาท ข้อต่อสู้ของจำเลย คือ ไม่ได้ร่วมกระทำผิดกับแก๊งค์คอลเซ็นเตอร์ การรับโอนเงินส่งเงินไปต่างประเทศ เป็นเงินที่มาจากการประกอบอาชีพรับฝากส่งเงินไปต่างประเทศ หรือ โพยก๊วน ไม่ใช่เงินที่มาจากการหลอกลวงผู้เสียหายและประชาชนตามที่โจทก์ฟ้องหมายความว่าหากพยานหลักฐานอิเล็กทรอนิกส์ในคดีนี้ คือ หลักฐานการโอนเงิน ไม่น่าเชื่อถือ และไม่สอดคล้องกับพฤติการณ์แวดล้อม คือคำเบิกความของผู้ร่วมขบวนการรัฐก็อาจเอาผิดจำเลยไม่ได้ ดังเช่น ศาลอุทธรณ์ในคดีนี้ที่พิพากษากลับคำพิพากษาศาลชั้นต้นยกฟ้องโจทก์ อย่างไรก็ดี ศาลฎีการับฟังพยานหลักฐานอิเล็กทรอนิกส์ ประกอบคำเบิกความพยานบุคคล และพฤติการณ์แวดล้อมอื่นๆ ที่เป็นพิรุธสงสัย เป็นไปตามหลักการในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ๒๕๔๔ มาตรา ๑๐ และ มาตรา ๑๑ เนื่องจาก ในการติดต่อระหว่างจำเลยกับบุคคลที่เกี่ยวข้องนั้น หากเป็นการทำธุรกิจที่ถูกต้องตามกฎหมายและประเพณี ดังที่จำเลยกล่าวอ้างจริง ก็ไม่จำเป็นต้องปกปิดชื่อจริงตามหลักฐานทางทะเบียน แต่ในกรณีนี้ จำเลยไม่ได้ใช้ชื่อจริง จึงเป็นพิรุธแสดงให้เห็นถึงการสมคบ ร่วมกันวางแผนเตรียมการกระทำผิดและหลบหนีให้พ้นจากการสืบสวนจับกุม ประกอบกับพยานหลักฐานที่นำสืบมาฟังได้เป็นมั่นคงว่าได้ร่วมเป็นตัวการแบ่งหน้าที่กันกระทำความผิดตามคำฟ้องของโจทก์ พิพากษาลงโทษจำเลย เช่นนี้ หากพยานหลักฐานอิเล็กทรอนิกส์ไม่น่าเชื่อถือ ลำพังแต่คำเบิกความพยานบุคคลประกอบพฤติการณ์พยานแวดล้อมอื่นๆ อาจไม่พอฟังลงโทษจำเลย และประชาชนจำนวนมากอาจต้องเสียหาย และประชาชนอีกจำนวนมากอาจต้องถูกหลอกลวงจากอาชญากรกลุ่มนี้

๓.๓ แนวทางการแก้ไขปัญหาอุปสรรค และเพิ่มประสิทธิภาพในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์

จากประเด็นปัญหาที่กล่าวมาในบทก่อน และจากข้อเท็จจริงในกรณีตัวอย่างข้างต้น อาจสรุปได้ว่าประเด็นสำคัญหนึ่งที่เป็นข้อท้าทายของทั้งสามขั้นตอนในกระบวนการยุติธรรมเพื่อปราบปรามอาชญากรรมคอมพิวเตอร์ คือ ความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ ผู้รวบรวมพยานหลักฐานจะต้องดำเนินการอย่างไร พนักงานอัยการหรือโจทก์จะนำสืบอย่างไร เมื่อต้องอ้างใช้พยานหลักฐานอิเล็กทรอนิกส์ต่อศาลปัญหาคือ ศาลจะทราบและเชื่อได้อย่างไรว่าพยานหลักฐานอิเล็กทรอนิกส์นั้นถูกต้อง ครบถ้วน ไม่ถูกเปลี่ยนแปลง และน่าเชื่อถือ เมื่อในทางปฏิบัติการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ต้องตรวจยึดมาจากทั้งในระบบข้อมูลคอมพิวเตอร์ และจากอุปกรณ์ เครื่องมือสื่อสารที่ใช้เก็บ ข้อมูลอิเล็กทรอนิกส์ ที่จะนำมาใช้เป็นพยานหลักฐานในคดี ยังมีข้อจำกัดและข้อบกพร่อง เนื่องจากเจ้าพนักงาน

ผู้ปฏิบัติหน้าที่ อาจจะยังขาดความเข้าใจ และทักษะในการรวบรวมข้อมูลอิเล็กทรอนิกส์ต่างๆ รวมถึง ในการตรวจยึดอุปกรณ์เครื่องมือที่บรรจุข้อมูลอิเล็กทรอนิกส์ที่จำเป็นในการใช้เป็นพยานหลักฐานในคดี จึงทำให้พยานหลักฐานอิเล็กทรอนิกส์ ที่เข้ามาสู่ในสำนวน อาจจะไม่ครบถ้วนเพียงพอ หรือเสียหายสูญหายไประหว่างทางการนำข้อมูลเข้ามาในสำนวน หรือสูญหายเสียหายไประหว่างการเก็บรักษา อีกทั้งยังมีข้อสงสัยใน การตรวจพิสูจน์ข้อมูลอิเล็กทรอนิกส์ว่ามีการถูกดัดแปลง เปลี่ยนแปลง ตัดต่อ ต่อเติมหรือไม่อย่างไร เพราะข้อมูลอิเล็กทรอนิกส์ เป็นพยานหลักฐานที่เปราะบาง สามารถแก้ไขเปลี่ยนแปลง ต่อเติม ตัดต่ออย่างหาร่องรอยได้ยาก ดังนั้น จึงต้องมีมาตรการในการตรวจสอบความถูกต้องครบถ้วน เพื่อให้พยานหลักฐานอิเล็กทรอนิกส์ สามารถนำไปใช้พิสูจน์ให้ทำความผิดของจำเลย ได้อย่างปราศจากข้อสงสัยตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ๒๕๔๔ มาตรา ๑๐ วรรคสอง ได้วางหลักเกี่ยวกับการพิจารณาความถูกต้องของข้อมูลอิเล็กทรอนิกส์ที่จะนำมาใช้เป็นพยานหลักฐานไว้ว่า ความถูกต้องของข้อความที่เป็นข้อมูลอิเล็กทรอนิกส์ ให้พิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงใดของข้อความ เว้นแต่การรับรองหรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใด ๆ ที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงข้อความซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้นและในวรรคสามได้วางหลักในการวินิจฉัยความน่าเชื่อถือของวิธีการรักษาความถูกต้องของข้อความที่เป็นข้อมูลอิเล็กทรอนิกส์ไว้ด้วยว่าให้พิเคราะห์ถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง รวมทั้งวัตถุประสงค์ของการสร้างข้อความนั้นและในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ๒๕๔๔ มาตรา ๑๑ วรรคสอง ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษาความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวงประกอบกับมาตรา ๑๒ ได้วางหลักเกณฑ์ในกรณีที่กฎหมายกำหนดให้เก็บรักษาเอกสารหรือข้อความใด ถ้าได้เก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการเก็บรักษาเอกสารหรือข้อความตามที่กฎหมายต้องการแล้ว

(๑) ข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง

(๒) ได้เก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นให้อยู่ในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์นั้น หรืออยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับให้ปรากฏอย่างถูกต้องได้ และ

(๓) ได้เก็บรักษาข้อความส่วนที่ระบุถึงแหล่งกำเนิด ต้นทาง และปลายทางของข้อมูลอิเล็กทรอนิกส์ ตลอดจนวันและเวลาที่ส่งหรือได้รับข้อความดังกล่าว ถ้ามี

ดังนั้น พยานหลักฐานอิเล็กทรอนิกส์ที่มีน้ำหนักเป็นที่น่าเชื่อถือในการนำสืบพิสูจน์ความจริง จะต้องมีคุณลักษณะสำคัญ คือ ความถูกต้อง ความครบถ้วน ไม่มีการเปลี่ยนแปลงใด ๆของข้อความ หากในกระบวนการการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงข้อความทำให้เกิดการเปลี่ยนแปลงเป็นปกติ ก็ต้องไม่กระทบต่อความถูกต้องของข้อความนั้น นอกจากนี้ การพิจารณาความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ ต้องพิจารณาลักษณะหรือวิธีการที่ใช้สร้าง การเก็บรักษา หรือการสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษา ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล และที่สำคัญการพิสูจน์ความถูกต้องแท้จริงของพยานหลักฐานอิเล็กทรอนิกส์จำเป็นต้องมีมาตรฐานของการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) ที่เชื่อถือ และมีหลักเกณฑ์อ้างอิงได้

มาตรฐานของการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

การตรวจสอบความถูกต้องและความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ จำเป็นต้องใช้ความรู้และความเข้าใจที่บูรณาการในหลายด้าน เช่น ด้านเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ ระบบดิจิทัล ระบบข้อมูลอิเล็กทรอนิกส์ ฯลฯ นอกจากนี้ ขั้นตอนในการรวบรวม เก็บรักษาพยานหลักฐานอิเล็กทรอนิกส์ต่างๆต้องมีหลักเกณฑ์และมาตรฐานที่เป็นแนวปฏิบัติ และเป็นแนวทางเพื่อใช้ในการตรวจสอบที่เชื่อถือได้ ซึ่งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์องค์การมหาชน[๑๒] ได้ประกาศข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน เพื่อประโยชน์ สำหรับการปฏิบัติงานในสถานที่เกิดเหตุและในห้องปฏิบัติการซึ่งครอบคลุมการจัดการคอมพิวเตอร์สื่อบันทึกข้อมูลดิจิทัลแบบภายใน สื่อบันทึกข้อมูลดิจิตอลแบบภายนอก ข้อมูลคอมพิวเตอร์และเครื่องมือสื่อสารเคลื่อนที่ ให้มีความเหมาะสมและสอดคล้องกับมาตรฐานสากล มีสาระสำคัญ ดังนี้

๑. การตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ ผู้ทำการตรวจพิสูจน์ต้องมีความรู้ความเข้าใจเกี่ยวกับงานตรวจพิสูจน์พยานหลักฐาน อิเล็กทรอนิกส์ เนื่องจากมีความเปราะบางและซับซ้อน เทคโนโลยีถูกพัฒนาอย่างรวดเร็ว นอกจากนี้ ผู้ปฏิบัติงาน ควรรักษาสภาพและหลักฐานไม่ให้ถูกเปลี่ยนแปลง คือทุกเปลี่ยนแปลงน้อยที่สุด และต้องสามารถอธิบาย รวมถึงบันทึกสิ่ง ที่ดำเนินการเหตุผลที่ทำให้พยานหลักฐานต้องเปลี่ยนแปลง และผลกระทบจากการดำเนินการนั้นได้อย่างละเอียดโดยทำเป็นลายลักษณ์อักษร

๒. Chain of Custody คือ การรักษาความต่อเนื่องของการครอบครองพยานหลักฐาน โดยมีข้อมูลที่จำเป็นต้องบันทึกได้แก่ ข้อมูลติดต่อและลายมือชื่อของผู้ส่งมอบพยานหลักฐาน ข้อมูลติดต่อและลายมือชื่อของผู้รับมอบพยานหลักฐานวันที่และเวลาในการรับส่งมอบพยานหลักฐาน เหตุผลในการรับส่งมอบพยานหลักฐานวิธีการส่งมอบพยานหลักฐาน และสถานที่จัดเก็บพยานหลักฐาน เป็นต้น

๓. การบันทึกขั้นตอนการปฏิบัติงานการเก็บรวบรวมและการวิเคราะห์พยานหลักฐานโดยละเอียดเพียงพอให้ผู้ตรวจพิสูจน์อื่นที่มีความเชี่ยวชาญในสาขาเดียวกันสามารถเข้าใจได้ และหากทำซ้ำโดยวิธีการเดิมและเครื่องมือที่มีลักษณะเดียวกันจะต้องได้ผลลัพธ์เหมือนกัน

๔. บุคคลที่เข้าถึงพยานหลักฐานต้องเป็นผู้ที่ได้รับมอบหมายหรือมีหน้าที่รับผิดชอบโดยตรง

๕. ผู้ปฏิบัติงานพึงตระหนักถึงหน้าที่ความรับผิดชอบในการปฏิบัติงานรวมถึงการดำเนินการตามกฎหมายที่เกี่ยวข้อง เช่น กฎหมายเกี่ยวกับพยานหลักฐาน เป็นต้น

๖. เครื่องมือและอุปกรณ์ที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์หลักฐานจำเป็นต้องมีสภาพ พร้อมใช้งานและเหมาะสมกับกระบวนการตรวจพิสูจน์พยานหลักฐานแต่ละประเภท มีมาตรฐานในการป้องกันการเปลี่ยนแปลงและปนเปื้อนของพยานหลักฐาน เช่น การปะปนข้อมูลจากคดีก่อนกับคดีปัจจุบัน หรือการปะปนข้อมูลที่เก็บรักษาปัจจุบันกับข้อมูลที่มีอยู่เดิมในเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงาน ทำให้ผลการวิเคราะห์ข้อมูลผิดพลาดไป

๗. มีการตรวจสอบความถูกต้องแม่นยำของเครื่องมือก่อนใช้งานอย่างสม่ำเสมอ และควรมีคู่มือการใช้งานและเอกสารคำอธิบาย เพื่อใช้ประกอบการอ้างอิง

ดังนี้ จะเห็นได้ว่า พยานหลักฐานอิเล็กทรอนิกส์มีความละเอียดอ่อน หากขั้นตอนการค้นหารวบรวมพยานหลักฐาน การเก็บรักษาข้อมูลอิเล็กทรอนิกส์ต่างๆ จนถึงการนำมาใช้มีความถูกต้องครบถ้วน และข้อมูลไม่ถูก

---

[๑๒] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์องค์การมหาชน จัดตั้งขึ้นตามพระราชกฤษฎีกา จัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์องค์การมหาชนพ.ศ. ๒๕๕๔

เปลี่ยนแปลงใดๆ หรือหากเปลี่ยนแปลงก็เพียงเล็กน้อยไม่กระทบต่อความถูกต้องของข้อมูล อีกทั้ง ลักษณะและวิธีการสร้างข้อมูล วิธีการเก็บรักษามีความถูกต้อง รัดกุม รอบคอบและปลอดภัย โดยผ่านการตรวจสอบและยืนยันความถูกต้องแท้จริงจากหน่วยงานที่เป็นกลางน่าเชื่อถือประกอบกับกับมีมาตรฐานดังที่กล่าวแล้ว ก็จะทำให้พยานหลักฐานอิเล็กทรอนิกส์มีความน่าเชื่อถือ

นอกจากพยานหลักฐานอิเล็กทรอนิกส์ต้องมีความน่าเชื่อถือแล้ว ในการนำเสนอพยานหลักฐานอิเล็กทรอนิกส์เพื่อให้ศาลจะรับฟังเป็นพยานเพื่อพิสูจน์ความผิดของจำเลยได้ พนักงานอัยการต้องมีความเข้าใจ และรอบรู้เกี่ยวกับองคาพยพของสังคมไทยในบริบทที่ต้องเผชิญกับอาชญากรรมคอมพิวเตอร์ขั้นรุนแรง และความเชื่อมโยงในการก่ออาชญากรรมข้ามชาติผ่านพยานหลักฐานอิเล็กทรอนิกส์ ดังนั้น สำนักงานอัยการสูงสุดจึงได้คำสั่งสำนักงานอัยการสูงสุดที่ ๘๓๒/๒๕๖๗ ลงวันที่ ๒๙ เมษายน ๒๕๖๗ แต่งตั้งคณะทำงานกำหนดแนวทางการดำเนินคดีอาชญากรรมทางเทคโนโลยี โดยมีผู้ตรวจการอัยการที่ได้รับมอบหมายให้รับผิดชอบงานของสำนักงานคดีอาญาเป็นหัวหน้าคณะทำงาน ต่อมาผู้ตรวจการอัยการฯ ได้มีคำสั่งหัวหน้าคณะทำงานกำหนดแนวทางการดำเนินคดีอาชญากรรมทางเทคโนโลยี ที่ ๑/๒๕๖๗ ณ วันที่ ๘ สิงหาคม ๒๕๖๗ เรื่อง แต่งตั้งคณะทำงานย่อยเพื่อขับเคลื่อนงานการดำเนินคดีอาชญากรรมทางเทคโนโลยีของสำนักงานอัยการสูงสุด ประกอบไปด้วย

๑. คณะทำงานย่อยเพื่อกำหนดแนวทางปฏิบัติในการรับสำนวนพิจารณาสำนวนทำความเห็นร่างคำฟ้องคดีอาชญากรรมทางเทคโนโลยี โดยมีหน้าที่หลักในการพิจารณาและดำเนินการตรวจสอบศึกษาวิเคราะห์ประเด็นปัญหาที่อาจเกิดขึ้นเกี่ยวกับการดำเนินคดีอาชญากรรมทางเทคโนโลยี พิจารณาและดำเนินการยกร่างแนวทางปฏิบัติในการรับสำนวนพิจารณาสำนวนทำความเห็นด้านคำฟ้องคดีอาชญากรรมทางเทคโนโลยี ให้หัวหน้าคณะทำงานย่อยมีอำนาจเชิญข้าราชการฝ่าย อัยการและบุคลากรของสำนักงานเพื่อให้ความเห็นประกอบการพิจารณา

๒. คณะทำงานย่อยเพื่อดำเนินการเกี่ยวกับการฝึกอบรมพนักงานอัยการในการดำเนินคดีอาชญากรรมทางเทคโนโลยี มีอำนาจหน้าที่หลักในการประสานงานกับหน่วยงานในสำนักงานอัยการสูงสุดและหน่วยงานภายนอกทางภาครัฐและภาคเอกชนเพื่อบูรณาการในการจัดทำหลักสูตรการฝึกอบรมให้มีเนื้อหาครอบคลุมเกี่ยวกับการดำเนินคดีอาชญากรรมทางเทคโนโลยี

๓ คณะทำงานย่อยเพื่อการเตรียมการด้านงบประมาณเกี่ยวกับการดำเนินคดีอาชญากรรมทางเทคโนโลยี โดยให้เตรียมความพร้อมด้านงบประมาณเพื่อการเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมทางเทคโนโลยี

๔ คณะทำงานย่อยเพื่อประสานความร่วมมือ การดำเนินคดีและงานวิชาการเกี่ยวกับอาชญากรรมทางเทคโนโลยี

จะเห็นได้ว่าจากคำสั่งดังกล่าวสำนักงานอัยการสูงสุดได้มีการเตรียมความพร้อมรับมือกับอาชญากรรมคอมพิวเตอร์ให้สอดคล้องกับกฎหมายที่แก้ไขใหม่และบริบทของสังคม เพื่อเป็นการแก้ไขปัญหาความไม่เข้าใจในลักษณะสำคัญของพยานหลักฐานอิเล็กทรอนิกส์ การนำสืบพยานหลักฐานอิเล็กทรอนิกส์ โดยเริ่มตั้งแต่การฝึกอบรม พนักงานอัยการให้มีความรู้ความเข้าใจในการดำเนินคดีอาชญากรรมทางเทคโนโลยี ร่างแนวทางปฏิบัติในการดำเนินคดีอาชญากรรมทางเทคโนโลยีที่ควรต้องสอดคล้องกับระเบียบของหน่วยงานในกระบวนการยุติธรรมที่เกี่ยวข้อง เช่น ประกาศคณะกรรมการบริหารศาลยุติธรรม เรื่อง การจัดตั้งแผนกคดีอาชญากรรมทางเทคโนโลยีในศาลอาญา และคำสั่งสำนักงานตำรวจแห่งชาติที่ ๑๘๒/๒๕๖๖ลงวันที่ ๑๗ มีนาคม ๒๕๖๖ เป็นต้น ทั้งนี้ เพื่อให้การดำเนินคดีอาชญากรรมทางเทคโนโลยีเป็นไปในทางเดียวกันมีมาตรฐาน โปร่งใสและตรวจสอบได้ รวมทั้งสามารถดำเนินคดีได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

บทที่ ๔

การดำเนินคดีอาชญากรรมคอมพิวเตอร์ภายใต้หลักนิติธรรม

๔.๑ หลักนิติธรรม

ความหมายของหลักนิติธรรมนั้น นักกฎหมายได้นิยามหลักนิติธรรมไว้มากมาย ทั้งนักกฎหมายไทย และนักกฎหมายต่างประเทศ รวมไปถึงหลักฐานทางประวัติศาสตร์กฎหมาย ร่างกฎหมายบางฉบับ[๑๓]ที่ผ่านมา ก็อธิบายถึงหลักนิติธรรมไว้ โดยสรุปแล้ว หลักนิติธรรม เปรียบเสมือนรากฐานของกฎหมายที่ออกมาเพื่อคุ้มครองสังคมให้สงบสุข โดยการออกกฎหมายนั้นหากไม่แตกแถวไปจากหลักนิติธรรมแล้ว กฎหมายนั้นย่อมเป็นกฎหมายที่มีความเป็นธรรม ความเสมอภาค เคารพสิทธิมนุษยชน ทุกคนอยู่ภายใต้กฎหมาย ผู้บังคับใช้กฎหมายดำรงความเป็นกลาง บังคับใช้ได้อย่างมีประสิทธิภาพ เกิดประสิทธิผล สร้างสังคมให้มีความมั่นคง และทำให้คนในสังคมเกิดความเชื่อมั่น สามารถอยู่ร่วมกันได้อย่างสงบสุข

“องค์ประกอบของหลักนิติธรรม[๑๔] มีอยู่ ๔ ประการ ประการแรก องค์ประกอบด้านสาระ ซึ่งหมายถึง หลักความเสมอภาคทางกฎหมาย ประการที่สอง องค์ประกอบด้านกระบวนการในการใช้กฎหมาย หมายถึง รัฐและเจ้าหน้าที่ของรัฐต้องใช้อำนาจภายในขอบเขตที่กฎหมายให้ไว้ ตามวิธีการ รูปแบบ เวลา และสถานที่ ประการที่สาม คือ องค์ประกอบด้านองค์กร หมายถึง การแบ่งแยกอำนาจและความเป็นอิสระของตุลาการ และประการสุดท้าย คือ องค์ประกอบด้านเป้าหมายซึ่งหมายถึง การใช้ การตีความกฎหมายและการตัดสินคดี นั้นจะต้องมุ่งสร้างความยุติธรรมให้เกิดขึ้นโดยเที่ยงธรรม”

---

[๑๓] ร่างรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับเสนอสภาปฏิรูปแห่งชาติ ตามมาตรา ๓๔ วรรคหนึ่ง และมาตรา ๓๖ วรรคหนึ่ง และส่งให้คณะรัฐมนตรีและคณะรักษาความสงบแห่งชาติ ตามมาตรา ๓๖ วรรคสาม ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช ๒๕๕๗

มาตรา ๒๑๗ หลักนิติธรรมอันเป็น รากฐานของรัฐธรรมนูญในระบอบประชาธิปไตย อย่างน้อยมีหลักการพื้นฐานสำคัญ ดังต่อไปนี้

(๑) ความสูงสุดของรัฐธรรมนูญและ กฎหมายเหนืออำเภอใจของบุคคล และการเคารพ รัฐธรรมนูญและกฎหมายทั้งโดยรัฐและประชาชน

(๒) การคุ้มครองศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาค

(๓) การแบ่งแยกการใช้อำนาจ การตรวจสอบการใช้อำนาจรัฐ และการป้องกันการขัดกันระหว่างประโยชน์ส่วนตนและประโยชน์ส่วนรวม

(๔) นิติกระบวน ซึ่งอย่างน้อยต้องไม่ บังคับใช้รัฐธรรมนูญหรือกฎหมายย้อนหลังเป็นโทษ ทางอาญาแก่บุคคล ให้บุคคลมีสิทธิในการปกป้อง ตนเองเมื่อสิทธิหรือเสรีภาพถูกกระทบ ไม่บังคับให้ บุคคลต้องให้ถ้อยคำซึ่งทำให้ต้องรับผิดทางอาญาไม่ทำให้บุคคลต้องถูกดำเนินคดีอาญาในการกระทำความผิดเดียวกันมากกว่าหนึ่งครั้ง และมีข้อกำหนด ให้สันนิษฐานว่าบุคคลเป็นผู้บริสุทธิ์อยู่จนกว่าจะมีคำพิพากษาว่ากระทำผิด

(๕) ความเป็นอิสระของศาล และความ สุจริตเที่ยงธรรมของกระบวนการยุติธรรม

[๑๔] บวรศักดิ์ อุวรรณโณ, หลักนิติธรรมกับการปกครองในระบอบประชาธิปไตย, วารสารพระธรรมนูญ เล่ม ๔๙ ฉบับพ.ศ. ๒๕๕๑-๒๕๕๒หน้า ๙๗-๑๐๑.

ดังนั้น หลักนิติธรรม (Rule of Law) จึงเป็นหลักการที่สำคัญในระบบกฎหมาย ที่จะช่วยให้กระบวนการยุติธรรมดำเนินไปได้อย่างมีประสิทธิภาพและเป็นธรรม โดยจากองค์ประกอบของหลักนิติธรรมข้างต้น อาจสรุปสาระสำคัญของหลักนิติธรรม ได้ดังนี้

๑. **ความเสมอภาค** ประชาชนทุกคนต้องได้รับการปฏิบัติจากรัฐอย่างเท่าเทียมตามกฎหมายไม่เลือกปฏิบัติต่อบุคคลใดบุคคลหนึ่งเพราะสถานะอาชีพ เพศ อายุหรือฐานะทางสังคม

๒. **ความโปร่งใส**รัฐต้องจัดให้มีระบบตรวจสอบการใช้กฎหมายให้เป็นไปอย่างถูกต้องเป็นธรรม

๓. **ความมีเสถียรภาพของกฎหมาย** กฎหมายต้องมีความชัดเจนเพื่อให้ประชาชนสามารถทราบและปฏิบัติตามได้ โดยเฉพาะกฎหมายที่มีโทษทางอาญานั้น บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการอันกฎหมายที่ใช้ในขณะนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่ผู้กระทำความผิดนั้นต้องเป็นโทษที่บัญญัติไว้ในกฎหมายเป็นไปตามมาตรา ๒ ประมวลกฎหมายอาญา และหลักกฎหมายละตินที่ว่าไม่มีความผิดและไม่มีโทษถ้าไม่มีกฎหมายกำหนดไว้ก่อน[๑๕]และต้องไม่บังคับใช้กฎหมายอาญาย้อนหลังเป็นโทษแก่บุคคลใด

๔. **การคุ้มครองสิทธิเสรีภาพ** กฎหมายและการบังคับใช้กฎหมายต้องไม่ละเมิดหลักสิทธิมนุษยชนต้องคุ้มครองสิทธิเสรีภาพพื้นฐานของบุคคล และบุคคลต้องไม่ถูกดำเนินคดีอาญาในการกระทำความผิดเดียวกันมากกว่าหนึ่งครั้ง

๕. **การบังคับใช้กฎหมายอย่างเป็นธรรม** รัฐและเจ้าหน้าที่ของรัฐต้องใช้อำนาจบังคับตามที่กฎหมายบัญญัติให้อำนาจ ภายในขอบเขตที่กฎหมายกำหนดไว้ ด้วยรูปแบบวิธีการที่ชอบด้วยกฎหมายเท่าที่เหมาะสมและจำเป็นต่อกรณี

๖. **การปฏิบัติตามกฎหมายอย่างเคร่งครัด** ทั้งรัฐและประชาชนต้องปฏิบัติตามกฎหมายอย่างเคร่งครัดและไม่มีผู้ใดอยู่เหนือกฎหมาย

๗. **กระบวนการยุติธรรมที่เป็นกลาง** ผู้บังคับใช้กฎหมาย ผู้ตัดสินคดี ดำรงความเป็นกลาง อย่างไร้อคติและปราศจากการถูกแทรกแซงไม่ว่าจากในหรือนอกองค์กร

๘. **การคุ้มครองทางกฎหมาย**ประชาชนทุกคนต้องมีสิทธิเข้าถึงกระบวนการยุติธรรมได้รับการปกป้องคุ้มครองสิทธิตามกฎหมายโดยปราศจากความเหลื่อมล้ำ ได้รับความช่วยเหลือทางกฎหมายจากหน่วยงานของรัฐให้สามารถปกป้องสิทธิตนเองได้อย่างเป็นธรรม

๔.๒ การรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ภายใต้หลักนิติธรรม

ในการตรวจยึดพยานหลักฐานอิเล็กทรอนิกส์ ดังได้กล่าวมาแล้วในบทก่อน เจ้าหน้าที่ย่อมมุ่งหมายที่จะเก็บรวบรวมพยานหลักฐานให้ได้มากที่สุด และโดยเร็วที่สุดเพื่อ ดำเนินคดีกับผู้กระทำความผิดได้อย่างมีประสิทธิภาพ แต่ต้องไม่ลืมว่าการตรวจยึดอุปกรณ์อิเล็กทรอนิกส์อาจมีข้อมูลอิเล็กทรอนิกส์อื่นปะปนอยู่นอกจากข้อมูลที่ใช้เป็นพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ เช่น ข้อมูลส่วนบุคคล และอาจจะไม่ใช่แค่ข้อมูลส่วนบุคคลของผู้กระทำผิดเท่านั้น อาจจะมีข้อมูลของบุคคลอื่น ๆในครอบครัว หรือบุคคลที่ไม่เกี่ยวข้องกับการกระทำความผิดรวมอยู่ด้วย หรืออาจเป็นข้อมูลของผู้ต้องหาแต่ไม่เกี่ยวกับการกระทำความผิด ดังนั้น ในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์เพื่อใช้ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์จึงต้องอยู่ภายใต้หลักนิติธรรม ซึ่งเป็นกรอบใหญ่ที่ประกอบไปด้วยทั้งกฎหมายที่เกี่ยวกับการป้องกันและปราบปรามผู้กระทำความผิดอาชญากรรมคอมพิวเตอร์ และหลักกฎหมายสิทธิมนุษยชน

---

[๑๕] ละติน: nullumcrimen, nullapoena sine praevialegepoenali

กล่าวคือต้องมีกฎหมายให้อำนาจไว้อย่างแจ้งชัดในการที่เจ้าหน้าที่ของรัฐจะกระทำการใด ๆเป็นอันกระทบต่อสิทธิของผู้ต้องหาซึ่งยังไม่ได้ถูกฟ้องเป็นจำเลยต่อศาล การตรวจยึดพยานหลักฐานอิเล็กทรอนิกส์ในอุปกรณ์คอมพิวเตอร์เครื่องมือสื่อสารต่าง ๆ จึงต้องมีกรอบกำหนดเขตอำนาจ และต้องมีกฎหมายให้อำนาจไว้อย่างชัดแจ้งว่ากระทำได้ นอกจากนี้ยังต้องยึดพยานหลักฐานเท่าที่จำเป็น กระทำโดยโปร่งใส และห้ามนำไปเผยแพร่อันเป็นการละเมิดต่อสิทธิส่วนบุคคล โดยต้องมีมาตรการควบคุมเจ้าหน้าที่ของรัฐ อย่างเคร่งครัด ปัจจุบันมีกฎหมายที่กำหนดอำนาจหน้าที่และขอบเขตการใช้อำนาจหน้าที่ ในการตรวจยึดพยานหลักฐานอิเล็กทรอนิกส์ จากอุปกรณ์คอมพิวเตอร์อุปกรณ์สื่อสารต่าง ๆ เอาไว้ โดยให้กระทำเท่าที่จำเป็น และบางกรณีต้องขออนุญาตต่อศาล จึงจะสามารถดำเนินการได้ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

นอกจากนี้ มาตรา ๑๙ ได้กำหนดการตรวจทานการใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง

อย่างไรก็ดี กฎหมายฉบับนี้ยังบังคับใช้กับเจ้าหน้าที่ของรัฐในวงจำกัด นอกจากนี้ยังมีข้อขัดข้องในขั้นตอนการตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ที่ยังไม่สอดคล้องกับหลักนิติธรรมบางประการ ดังนั้น รายงานนี้จึงมีข้อเสนอแนะในการแก้ไขข้อขัดข้อง ปัญหาและอุปสรรคการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในยุคดิจิทัลดังนี้

๔.๓ ข้อเสนอแนะ

๑. การตรวจสอบความถูกต้องแท้จริงของพยานหลักฐานอิเล็กทรอนิกส์ จำเป็นต้องมีการส่งตรวจพิสูจน์ตั้งแต่เมื่อเริ่มกระบวนการยุติธรรม กล่าวคือ เมื่อพนักงานสอบสวนตรวจยึดพยานหลักฐานอิเล็กทรอนิกส์มาได้ ต้องส่งตรวจพิสูจน์ต่อผู้ที่มีหน้าที่โดยตรง และเชื่อถือได้ เป็นผู้ที่มีความรู้ความสามารถเฉพาะทางผ่านการฝึกอบรมจนได้การรับรองคุณสมบัติแล้ว รวมถึงต้องมีหลักเกณฑ์มาตรฐานที่ชัดเจน และต้องทำการตรวจพิสูจน์ไปตามเกณฑ์มาตรฐานนั้น และเพื่อคัดกรองเฉพาะพยานหลักฐานอิเล็กทรอนิกส์ที่ไม่ถูกดัดแปลง ตัดต่อ เพิ่มเติมแก้ไข หรือบิดเบือน อันเป็นพยานหลักฐานที่ถูกต้องแท้จริงมาตั้งแต่ต้น ทั้งวิธีการสร้าง วิธีการเก็บรักษา อย่างน้อยให้ได้ตามมาตรฐานที่ได้กล่าวแล้วในบทก่อน เมื่อตรวจพิสูจน์แล้วจึงนำไปสู่สำนวนสอบสวน เพื่อพิจารณามีความเห็นและคำสั่ง ส่งไปยังพนักงานอัยการเพื่อดำเนินคดีต่อไปในชั้นศาลอันจะเป็นการขจัดปัญหาข้อจำกัดและอุปสรรคในชั้นพิจารณาของศาลที่ผ่านมากรณีมีการอ้างใช้พยานหลักฐานอิเล็กทรอนิกส์ และคู่ความโต้แย้งเกี่ยวกับความถูกต้องแท้จริงของพยานหลักฐานอิเล็กทรอนิกส์ศาลจำเป็นต้องขยายเวลาเพื่อส่งพยานหลักฐานอิเล็กทรอนิกส์ไปตรวจสอบยังหน่วยงานที่น่าเชื่อถือ เพื่อให้ได้ข้อเท็จจริงนำมาตัดสินคดี อย่างเที่ยงธรรม ปราศจากอคติ ทำให้กระบวนการยุติธรรมล่าช้า เช่นนี้แล้ว หากมีการส่งตรวจพิสูจน์ตั้งแต่เมื่อเริ่มกระบวนการยุติธรรม การดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่มีพยานหลักฐานอิเล็กทรอนิกส์ย่อมจะเป็นไปตามหลักนิติธรรม เพราะถือเป็นการให้ความเป็นธรรมกับทุกคนอย่างเสมอภาค ได้รับการคุ้มครองจากกระบวนการทางกฎหมายอย่างเท่าเทียม ไม่เกิดการเอาเปรียบกันในการพิจารณาคดี หรือการเข้าถึงความยุติธรรม

ตัวอย่างเช่นในกรณีมีการอ้างคลิปเสียงเป็นพยานหลักฐานสำคัญในคดี คู่กรณีโต้แย้งว่า เป็นคลิปเลียนเสียงคล้ายตนเพื่อเจตนาใส่ร้ายตน ไม่ใช่เสียงตนที่แท้จริง ในคดีที่เป็นข่าวดัง เหตุเกิดเมื่อ ปีพ.ศ.๒๕๖๐ คดีครูปรีชากับ ร.ต.ท.จรูญแย่งเป็นเจ้าของลอตเตอรี่จำนวน ๕ ใบ ที่ถูกรางวัล มูลค่า ๓๐ ล้าน พยานหลักฐานหนึ่ง คือ คลิปเสียงที่อ้างว่าครูปรีชาสนทนากับแม่ค้าขายสลากที่ถูกรางวัลที่แผงขายด้านหน้าธนาคารกสิกรไทย คุยโต้ตอบกันหลังหลังทราบผลสลาก ความว่า ครูปรีชาบอกว่าตนเองไม่ถูกหวย อย่างไรก็ตามมีการโต้แย้งกันว่า อาจมีการตัดต่อเสียงก็เป็นได้อย่างไรก็ดี ผู้เชี่ยวชาญทางด้านการเทียบเสียง[๑๖]ได้ให้ข้อมูลว่า การพิสูจน์โดยการเปรียบเทียบเสียงในประเทศไทยสามารถทำได้แต่ยังมีที่รองรับไม่มากนัก ส่วนผลจะสามารถยืนยันความถูกต้องได้เพียงใดนั้นขึ้นอยู่กับเงื่อนไข และปัจจัยหลายปัจจัยด้วยกัน[๑๗] และผลลัพธ์ที่ได้ต้องเอาไปตีความในชั้นศาลอีกชั้นหนึ่ง ว่าศาลจะรับเป็นพยานหลักฐานร่วมในการพิจารณา

---

[๑๖] ดร.ชัย วุฒิวิวัฒน์ชัย ผู้อำนวยการหน่วยวิจัยวิทยาการสื่อสารของมนุษย์และคอมพิวเตอร์, บทสัมภาษณ์ในข่าวไทยรัฐออนไลน์ เมื่อวันที่ ๑๖ กุมภาพันธ์ ๒๕๖๑, ที่มาจาก https://www.thairath.co.th/scoop/๑๒๐๕๑๒๓

[๑๗] เทคโนโลยีระบุเจ้าของเสียงหรือ Speaker Recognition นั้น จะจำแนกเสียงของบุคคลจากความถี่เสียง ซึ่งเป็นสิ่งที่เลียนแบบกันไม่ได้ และจะไม่ใช้ลักษณะของจังหวะการออกเสียงหรือการทำเสียงสูง-เสียงต่ำมาจำแนกบุคคล เพราะเป็นสิ่งที่เลียนแบบกันได้ โดยการตรวจหาเจ้าของเสียงนั้นจะเป็นเปอร์เซนต์ความน่าเชื่อถือของของผลตรวจสอบ ซึ่งการใช้เสียงจำแนกตัวบุคคลนั้นค่อนข้างแม่นยำถึง ๙๐%าเทคโนโลยีดังกล่าวมีความซับซ้อน ซึ่งการจำแนกว่าเสียงนั้นเป็นเสียงของบุคคลต้องสงสัยหรือไม่นั้น ต้องใช้เสียงตัวอย่างที่ผ่าน"" "*การบันทึกในสภาพแวดล้อมเดียวกับเสียงต้นแบบ เช่น เสียงต้นแบบของนาย ป. ได้รับการบันทึกผ่านโทรศัพท์มือถือด้วยสัญญาณของผู้ให้บริการเครือข่ายหนึ่ง ก็ต้องให้ นาย ป.พูดผ่านโทรศัพท์ด้วยสัญญาณของของผู้ให้บริการรายเดียวกัน โดยใช้เวลาบันทึกอย่างต่ำ ๓ นาที จากนั้นนำเสียงมาเปรียบเทียบได้เป็นเปอร์เซ็นต์ความน่าจะเป็น เมื่อผลทดสอบออกมาเสียงดังกล่าวมีความน่าเป็นเสียงของ นาย ป.๘๐% เราก็ยังไม่สามารถระบุว่าได้ ใช่หรือไม่ใช่เสียงของนาย ป. จึงต้องมีวิธีสร้างความมั่นใจต่อผลการดังกล่าวให้มากขึ้น ยกตัวอย่างว่าประเทศมาเลเซียนั้นมีเทคโนโลยีที่ตรวจสอบเสียได้ ซึ่งในกระบวนการสร้างความมั่นใจต่อผลการตรวจสอบเสียงนั้น โดยใช้ข้อมูลเพิ่มเติมเป็นข้อมูลเสียงของคนอื่นๆ มาพูดในสภาพแวดล้อมเดียวกับเสียงต้นแบบ ซึ่งต้องใช้ข้อมูลเสียงหลายคน เช่น ๓๐, ๕๐ และ ๑๐๐ คนหากมีความน่าจะเป็นเสียงนาย ป.๘๐% และเสียงคนอื่นๆ มีความน่าจะเป็น ๔๐% แสดงว่าผลทดสอบที่ออกมานี้มีความน่าเชื่อถือ ๑๐๐% และนำไปใช้งานได้ แต่หากมีคนอื่นที่ไม่อยู่ในข่ายต้องสงสัยแต่มีความน่าจะเป็นเจ้าของเสียงในคลิปถึง ๘๐% ด้วย แสดงว่าผลการทดสอบนั้นไม่น่าเชื่อถือ และต้องหาวิธีอื่นในการจำแนกบุคคล เปอร์เซ็นต์ที่แตกต่างกันนั้น มีหลายสาเหตุ เช่น บันทึกเสียงผ่านไมโครโฟน หรือมีเสียงรบกวนพื้นหลัง*

ได้หรือไม่ ถูกต้องตามกฎหมายหรือไม่ เพราะต้องดูที่มาของการได้มาของคลิปเสียงด้วยเป็นต้น ดังนี้ หากพนักงานสอบสวนสามารถส่งไปตรวจสอบกับพยานผู้เชี่ยวชาญที่เชื่อถือได้ก่อนนำเข้ามาเป็นพยานหลักฐานในคดี ก็จะป้องกันไม่ให้เกิดข้อต่อสู้ว่าเป็นการจู่โจมพยาน และทำให้พยานดังกล่าวมีน้ำหนักรับฟังได้ เกิดความเป็นธรรมทั้งสองฝ่าย และเป็นการกระทำด้วยความเป็นกลาง ปราศจากอคติ

ตัวอย่างกรณีต่อสู้กันเรื่องเอกสารอิเล็กทรอนิกส์ปลอม ลายมือชื่ออิเล็กทรอนิกส์ปลอม ปัจจุบันมีเทคโนโลยีที่ตรวจสอบความแท้จริงของข้อมูลอิเล็กทรอนิกส์หรือลายมือชื่ออิเล็กทรอนิกส์ได้ เรียกว่า Hash Value[๑๘] โดย Hash จะทำงานโดยการแบ่งย่อยไฟล์หรือข้อมูลที่มีขนาดใหญ่ ให้มีขนาดที่เล็กลงในสัดส่วนที่เท่ากัน โดยกระบวนการของ Hash มีหลายรูปแบบในการแบ่งย่อย เมื่อทำการแบ่งย่อยและทำการส่งไฟล์หรือข้อมูล จากต้นทางไปยังปลายทาง เมื่อปลายทางได้รับไฟล์หรือข้อมูลนั้นแล้วปลายทางจะทำการตรวจสอบไฟล์หรือข้อมูลที่ถูกส่งมาประกอบเข้ากันด้วยกระบวนการ Hash ในรูปแบบเดียวกัน เพื่อดูว่าไฟล์หรือข้อมูลที่ถูกส่งมาจากต้นทางถูกแก้ไข้หรือเปลี่ยนแปลงในระหว่างทางที่ทำการส่งมาหรือไม่

๒. รัฐและหน่วยงานของรัฐ ต้องให้ความสำคัญ สนับสนุนกระบวนการตรวจสอบ ตรวจพิสูจน์ความถูกต้องแท้จริงของพยานหลักฐานอิเล็กทรอนิกส์ ทั้งในเรื่องของการฝึกอบรมงบประมาณ เครื่องมืออุปกรณ์ และบุคลากรอย่างพอเพียง ไม่ปล่อยพนักงานสอบสวนให้โดดเดี่ยวต้องดำเนินการตรวจพิสูจน์เพียงลำพัง ที่สำคัญต้องมีมาตรฐานในการตรวจสอบที่เป็นเอกภาพเป็นมาตรฐานเดียวกัน และควรมีหน่วยงานกลางสำหรับตรวจสอบและตรวจทานมาตรฐานการตรวจพิสูจน์พยานหลักฐานของหน่วยงานผู้ตรวจพิสูจน์พยานหลักฐานอย่างสม่ำเสมอเพื่อให้การตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ได้มาตรฐานเป็นที่น่าเชื่อถือ ส่งผลให้ประชาชนเกิดความเชื่อมั่นในกระบวนการยุติธรรม

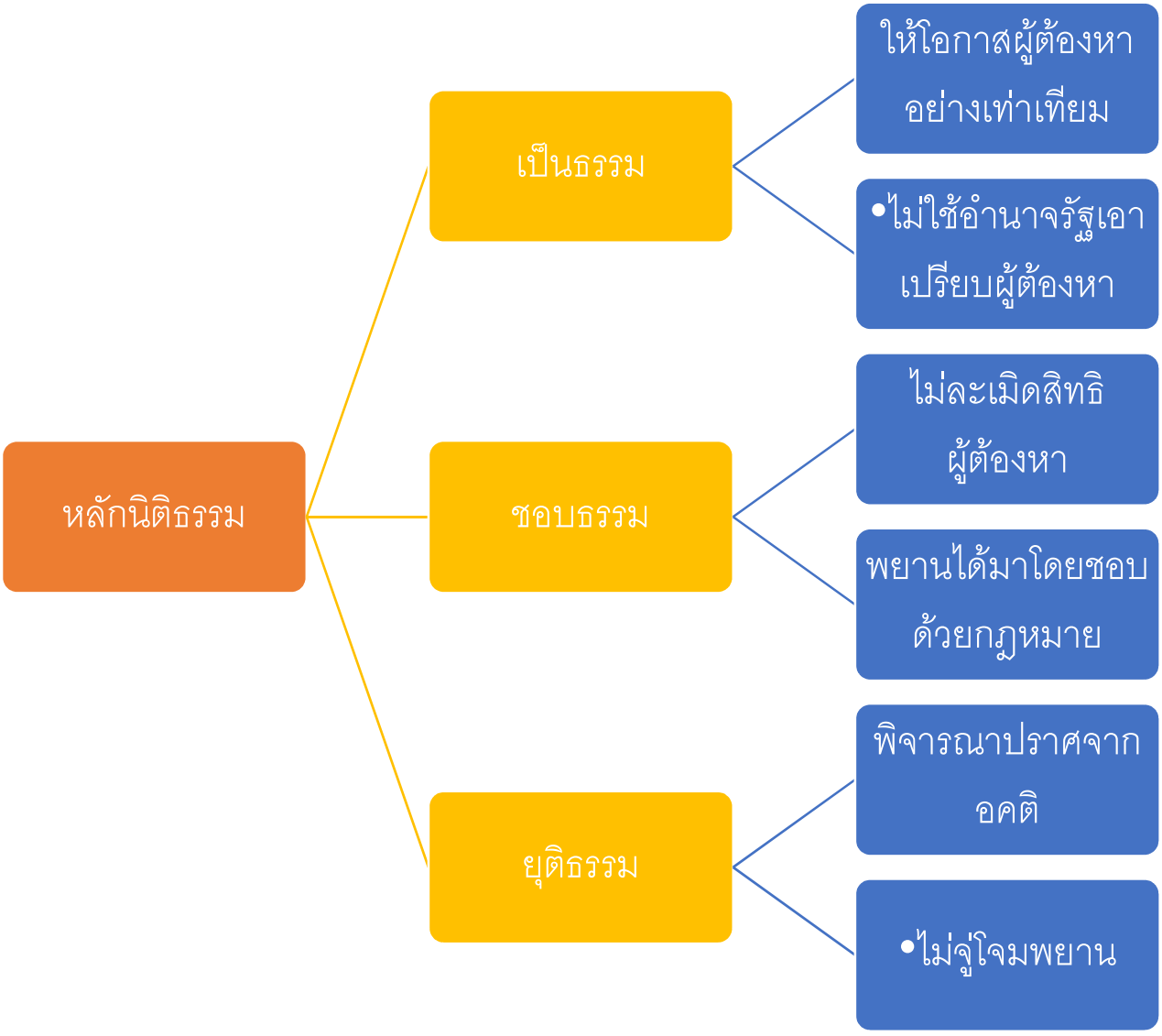
๓. รัฐควรจัดให้มีหน่วยงานกลางที่ทำหน้าที่ศึกษาค้นคว้าวิวัฒนาการใหม่ๆที่เกิดขึ้นให้เท่าทันต่อรูปแบบอาชญากรรมทางเทคโนโลยีที่พัฒนาขึ้นอย่างรวดเร็วและเปลี่ยนรูปแบบใหม่ๆไปเรื่อย ๆ เพื่อหลอกลวงเหยื่อ และเพื่อหนีการค้นพบและจับกุมจากเจ้าหน้าที่รัฐ อีกทั้งยังเป็นหน่วยงานที่สามารถให้ข้อมูล ให้ความรู้ แจ้งเตือนประชาชน และเจ้าหน้าที่ของรัฐในการระวังภัยที่อาจเกิดขึ้นกับประชาชนในรูปแบบต่าง ๆ เป็นหน่วยงานที่รวบรวมสถิติ ข้อมูลอาชญากรและขบวนการอาชญากรรม โดยมีการเปิดเผยข้อมูลที่จำเป็นแก่เจ้าหน้าที่ของทั้งภาครัฐ และภาคเอกชนเพื่อประสานความร่วมมือ สามารถระงับยับยั้งการก่ออาชญากรรมทางเทคโนโลยีได้อย่างทันที ไม่เกิดการลุกลามของความเสียหายไปสู่ประชาชน ป้องกันมิให้ประชาชนตกเป็นเหยื่ออาชญากรรมคอมพิวเตอร์ ทั้งนี้ จะส่งผลให้สามารถรักษาสวัสดิภาพของประชาชน ปกป้องสังคมและเศรษฐกิจของประเทศมิให้ถูกทำลาย สามารถให้ความเป็นธรรมกับทุกฝ่ายภายใต้หลักนิติธรรมอันเป็นการรักษาผลประโยชน์ของรัฐและประชาชนอย่างยั่งยืน

ดังนั้น หากได้มีการดำเนินการตรวจพิสูจน์ความถูกต้องแท้จริงของพยานหลักฐานอิเล็กทรอนิกส์ตั้งแต่เริ่มเข้าสู่กระบวนการยุติธรรมในชั้นต้นน้ำ ด้วยความเป็นมาตรฐานเดียวกันที่เชื่อถือได้ ผ่านหน่วยงานที่เป็นกลางในการตรวจวัดมาตรฐานการตรวจสอบ กระบวนการยุติธรรมขั้นต่อๆไปย่อมจะสามารถอำนวยความยุติธรรมให้กับประชาชนได้โดยรวดเร็ว เป็นกลางและเป็นธรรมกับทุกฝ่าย สอดคล้องกับหลักนิติธรรม และทำให้กระบวนการยุติธรรมนั้นมีความน่าเชื่อถือ พึ่งพาได้สำหรับประชาชนและสังคม

ที่แทรกเข้ามา และเมื่อเทียบความน่าเชื่อถือของวัตถุพยานในการจำแนกบุคคลนั้น ดีเอ็นเอมีความน่าเชื่อถือเป็นอันดับหนึ่ง รองลงมาคือเรตินาในดวงตา ถัดลงมาคือลายนิ้วมือ ส่วนเสียงนั้นตามอันดับหลัง แต่ก็มีความเชื่อถือและแม่นยำถึง ๙๐%", บทสัมภาษณ์ ของ ดร.ชัย วุฒิวิวัฒน์ชัย นักวิจัยอาวุโส ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ผู้พัฒนาผลงานวิจัยนวัตกรรมการประมวลผลสัญญาณเสียง, ข้อมูลจาก https://mgronline.com/science/detail/๙๖๑๐๐๐๐๐๑๖๐๓๒

[๑๘] ข้อมูลจาก https://www.vrproservice.com เมื่อวันที่ ๑๖ กันยายน ๒๕๖๗


สถานที่กระทำความผิด : ไร้พรมแดน
อาชญากรรมคอมพิวเตอร์
พยานหลักฐาน : อิเล็กทรอนิกส์ เปราะบาง ลบทำลาย ตัดต่อได้ กู้คืนยาก ข้อมูลโทรศัพท์ จราจรคอมพิวเตอร์ ภาพกล้องวงจรปิด คลิปเสียง
ผู้กระทำ : ปกปิดปลอมแปลงตัวตน ทำเป็นขบวนการ


หลักนิติธรรม
เป็นธรรม
ให้โอกาสผู้ต้องหาอย่างเท่าเทียม
•ไม่ใช้อำนาจรัฐเอาเปรียบผู้ต้องหา
ชอบธรรม
ไม่ละเมิดสิทธิผู้ต้องหา
พยานได้มาโดยชอบด้วยกฎหมาย
ยุติธรรม
พิจารณาปราศจากอคติ
•ไม่จูโจมพยาน


•ข้อเสนอแนะ
การตรวจสอบ
พยานหลักฐาน
ในคดี
อาชญากรรม
คอมพิวเตอร์
•ส่งตรวจสอบ
แต่ต้น
•สร้าง
มาตรฐานให้
เป็นเอกภาพ
•พัฒนา
เทคโนโลยีให้
ทันสมัย