การถ่ายทอดความรู้ภายในหน่วยงาน

โดย นายชิษชัย เหล่าฤทธิ์
นิติกรชำนาญการพิเศษ

เรื่อง "Big Data, Blockchain and Digital Evidence"

"Crime Sensing With Big Data : The Potentiale And Limitation of Using Big Data for Crime Estimation" (การตรวจจับอาชญากรรมด้วยข้อมูลขนาดใหญ่ : ศักยภาพ และข้อจำกัด ในการใช้ข้อมูลขนาดใหญ่สำหรับประเมินอาชญากรรม)

๑) Big Data คือ ข้อมูลทุกอย่างที่เรามีอยู่ ทั้งข้อมูลที่มีแหล่งที่มาจากภายในองค์กรเองและข้อมูลที่มาจากแหล่งที่มาภายนอก อย่างเช่น Social medias ซึ่งทั้งหมดเป็นข้อมูลที่สามารถนำมาวิเคราะห์ได้หรือก็คือ ข้อมูลดิบนั้นเอง ทั้งนี้ข้อมูลเหล่านี้สามารถนำมาวิเคราะห์ได้ด้วยวิธีการหลากหลายวิธีการ ขึ้นอยู่กับว่าเราต้องการนำข้อมูลเหล่านั้นไปใช้งานด้านไหน ในปัจจุบันนิยมทำ Big Data Analysis เพื่อใช้ในการสำหรับการคาดการณ์เหตุการณ์ในอนาคต หรือก็คือเพื่อใช้ดูแนวโน้มสิ่งที่จะเกิดขึ้นนั้นเอง

Big data คือ ข้อมูลที่ประกอบด้วยคุณลักษณะ ๓ อย่าง คือ

(๑) Volume ข้อมูลมีขนาดใหญ่ มีปริมาณข้อมูลมาก ซึ่งสามารถเป็นได้ทั้งข้อมูลแบบ offline หรือ online

(๒) Variety ข้อมูลมีความหลากหลาย สามารถเป็นได้ทั้งที่มีโครงสร้างและข้อมูลที่ไม่มีรูปแบบที่ชัดเจน

(๓) Velocity ข้อมูลมีการเปลี่ยนแปลงตลอดเวลาอย่างรวดเร็ว มีการส่งผ่านข้อมูลอย่างต่อเนื่อง ทำให้การวิเคราะห์ข้อมูลแบบเดิม มีข้อจำกัด

๒) การเก็บข้อมูล ในลักษณ Big Data มีที่มาจากหลากหลายแหล่งข้อมูล เช่น

- ข้อมูลเกี่ยวกับบุคคล เช่น ข้อมูลเกี่ยวกับสุขภาพ อายุ การศึกษา เป็นต้น
- ข้อมูลของค่าพิกัด (GPS) ของโทรศัพท์มือถือระบบ smart phones
- การส่งข้อความในสื่อสังคมออนไลน์ (Social media posts)
- ข้อมูลการใช้งานโทรศัพท์
- ข้อมูลการใช้งานคอมพิวเตอร์

กรณีตัวอย่าง ของประเทศสิงคโปร์ที่มีรายละเอียดการเก็บข้อมูล เช่น

- ข้อมูลการใช้โทรศัพท์มือ ที่ การเก็บข้อมูลทั้งหมายเลขโทรศัพท์ที่มีการติดต่อไปมาระหว่างกัน ตำแหน่งการใช้โทรศัพท์ ระยะเวลาการใช้โทรศัพท์ ข้อความและ อีเมล์
- ข้อมูลจากส่วนอื่นๆ เช่น ข้อมูลการใช้ทางด่วนอัตโนมัติ เครื่องตรวจจับความเร็ว เสาอิเล็กทรอนิกส์ติดตามความเคลื่อนไหวเป็นต้น

(๑) กฎหมายและระเบียบข้อบังคับในปัจจุบันที่เกี่ยวข้องกับ Big Data ในสิงคโปร์ ซึ่งประกอบด้วย

-พระราชบัญญัติ...

- พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล
- กฎหมายอาญา (ประมวลกฎหมายอาญาและกฎหมายอื่นๆ)
- ประมวลกฎหมายวิธีพิจารณาความอาญา เกี่ยวพยานหลักฐาน
- พระราชบัญญัติเกี่ยวกับการรักษาความปลอดภัยในโลกอินเตอร์เน็ต

ประเทศสิงคโปร์ ได้มีการออกกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ในปี พ.ศ. ๒๕๕๕ (ค.ศ.๒๐๑๒) ซึ่งข้อมูลส่วนบุคคลดังกล่าว ประกอบด้วย

- ชื่อ-สกุล
- บัตรประจำตัวประชาชน
- หมายเลขโทรศัพท์
- อีเมล์

ซึ่งข้อมูลส่วนบุคคลดังกล่าว หน่วยงานภาครัฐสามารถเก็บรวบรวมใช้หรือเปิดเผยข้อมูลได้ (ยกเว้นในบางกรณีที่ต้องได้รับความยินยอมของเจ้าของข้อมูล) ดังนั้นการคุ้มครองข้อมูลส่วนบุคคลดังกล่าว ส่วนใหญ่จึงมีผลคุ้มครองเฉพาะในส่วนของภาคธุรกิจ หรือเอกชน เท่านั้น เนื่องจากกฎหมายของประเทศสิงคโปร์ได้รับอิทธิพลจากกฎหมายของประเทศอินเดีย จึงได้รับอิทธิพลตามหลักกฎหมายระบบคอมมอนลอว์สูง ทำให้ตำรวจสามารถติดตาม บุคคลที่ต้องสงสัยและหากข้อมูลที่มีความเสี่ยงที่อาจจะก่อให้เกิดอาชญากรรม เช่น มีข้อสงสัยว่ามีการวางแผนในการกระทำความผิด สามารถเข้าทำการจับกุมได้โดยทันทีตามขั้นตอน

(๒) การวิเคราะห์อาชญากรรม

มีการใช้ข้อมูลจาก Big Data เพื่อวิเคราะห์อาชญากรรม ในการหาตัวผู้กระทำความผิด เช่น ภาพจากกล้องวงจรปิด ข้อมูลการใช้โทรศัพท์ ข้อมูลจากการส่งข้อความในโลกอินเตอร์เน็ต เป็นต้น เพื่อใช้เป็นหลักฐานในการหาตัวผู้กระทำความผิด

(๓) การคาดการณ์ถึงอาชญากรรมที่จะเกิดขึ้น

มีการใช้ข้อมูลจาก Big Data เพื่อเฝ้าระวังการเกิดอาชญากรรม ซึ่งมีหลายประเทศที่นำไปใช้ ทั้งในประเทศสหรัฐอเมริกา และประเทศอังกฤษ ซึ่งพบว่า มีผลทำให้การกระทำความผิดเล็กๆ น้อยๆ ลดลง ทำให้ตำรวจสามารถมุ่งความสนใจไปยังพื้นที่ ที่มีสถิติการก่ออาชญากรรมสูงเมื่อเทียบกับพื้นที่อื่น โดยใช้จากสถิติข้อมูลแทนที่การคาดเดาจากสัญชาตญาณ รวมทั้งเป็นการลดความเป็นอคติส่วนตัวในการทำงาน

(๔) ข้อจำกัดและความเสี่ยง

การคาดการณ์เกี่ยวกับการเกิดอาชญากรรมสามารถเกิดข้อผิดพลาดได้จากหลายสาเหตุ เช่น

- ข้อมูลเบื้องต้นที่ใช้ประกอบการตัดสินใจที่มีความผิดพลาด
- ผู้พิพากษาให้ความเชื่อมั่นในความถูกต้องของการทำนายอาชญากรรมจาก Big Data มากเกินไป เช่น การกำหนดโทษ เป็นต้น
- การใช้ข้อมูลจากภาคธุรกิจ อาจทำให้การคาดการณ์เกี่ยวกับอาชญากรรมไม่ถูกต้อง เนื่องจากเป็นข้อมูลที่มีวัตถุประสงค์ที่แตกต่างกัน จึงต้องใช้ด้วยความระมัดระวัง

- ความผิดพลาดจากการคาดการณ์ในทางธุรกิจการค้า ก่อให้เกิดความเสียหายไม่มากแต่หากเกิดความผิดพลาดในการจับกุมดำเนินคดีอาญาสร้างความเสียหายมาก ดังนั้น การใช้ข้อมูลจากภาคเอกชน จึงจำเป็นต้องใช้ด้วยความระวัดระวังอย่างสูง

- การแปลความผิด เช่น ข้อผิดพลาดจากการดึงข้อมูลจากเพลงที่มีเนื้อหาเกี่ยวข้องกับอาชญากรรม ทั้งที่แท้จริงแล้วเป็นเพียงเนื้อร้องของเพลงเท่านั้น

นอกจากนี้ เนื่องจากข้อมูล Big Data มีลักษณะเป็นข้อมูลที่มีความหลากหลาย และเป็นการใช้ข้อมูลในเชิงสถิติ ตัวเลข ดังนั้น อาจจะจากความคาดเคลื่อนจากเหตุอื่นๆ ซึ่งได้เคยเกิดขึ้นแล้วในประเทศสหรัฐอเมริกา ดังนั้น การใช้ข้อมูลดังกล่าว และเนื่องจากเป็นการเข้าไปควบคุมประชาชนของตนโดยภาครัฐในลักษณะหนึ่ง จึงควรดำเนินการบนพื้นฐานของความโปร่งใส ตรวจสอบได้ และมีการทดสอบความถูกต้องเที่ยงตรงอยู่ตรงเวลา โดยเฉพาะความมีอคติที่เกิดจากการเขียนโปรแกรมหรือเงื่อนไข (Algorithms) รวมทั้งการมีระบบป้องกัน การรั่วไหลของข้อมูลที่ดีและรัดกุม เพราะหากข้อมูลดังกล่าวหากมีรั่วไหลออกไปก็อาจจะถูกนำไปใช้เพื่อการวางแผนในการก่ออาชญากรรมได้

“The Law, Blockchain and Big Data Analytics” (กฎหมาย,Blockchain และการวิเคราะห์ข้อมูลขนาดใหญ่)

๑) Blockchain คืออะไร และสำคัญอย่างไร

“Blockchain นั้นเป็นเทคโนโลยีที่ช่วยนำมาซึ่งความปลอดภัย น่าเชื่อถือ <u>โดยไม่ต้องอาศัยคนกลาง</u>”

โดยปกติแล้วเรามักต้องพึ่งพิงบุคคลที่สาม (centralized trusted party) มาช่วยทำหน้าที่เป็นคนกลางคอยตรวจสอบความน่าเชื่อถือเวลาทำธุรกรรม ถ้าหากเราทำธุรกรรมออนไลน์ จะสังเกตเห็นว่า มักจะต้องมีคำที่ระบุว่า Secured by หรือ Protected by ตามด้วยชื่อตัวกลางใดๆ ซึ่งเป็นเรื่องที่สำคัญมาก เพราะโดยปกติคนที่กล้ากรอกข้อมูลบัตรเครดิต เพราะมั่นใจว่ามันจะไม่รั่วไหล หรือถูกทำให้เปลี่ยนแปลง การมาของบล็อกเชนมีส่วนช่วยอย่างมาก เพราะบล็อกเชนเป็นเทคโนโลยีใหม่ ที่ประโยชน์ของมันคือมันเป็นเทคโนโลยีที่นำมาซึ่งความปลอดภัย น่าเชื่อถือ โดยไม่ต้องอาศัยคนกลาง ทำให้การทำธุรกรรมออนไลน์ใดๆ สามารถทำได้อย่างสะดวกมากขึ้น ใส่ความคิดสร้างสรรค์ได้มากขึ้น creative มากขึ้น innovative มากขึ้น ประหยัดขึ้น รวดเร็วขึ้น ถึงแม้สองบุคคลจะไม่เคยรู้จักกันมาก่อน ก็สามารถแลกเปลี่ยนข้อมูลกันได้ด้วยความมั่นใจ พูดถึงคำว่าแลกเปลี่ยนข้อมูล

การทำงานของ Blockchain

บล็อกเชน เป็นรูปแบบการเก็บข้อมูล (Data structure) แบบหนึ่ง ที่ทำให้ข้อมูล Digital transaction ของแต่ละคนสามารถแชร์ไปยังทุกๆ คนได้ เป็นเสมือนห่วงโซ่ (Chain) ทำให้ block ของข้อมูลลิ้งก์ต่อไปยังทุกๆ คน โดยที่จะทราบว่าใครที่เป็นเจ้าของและมีสิทธิในข้อมูลนั้นจริง ๆ

เมื่อบล็อกของข้อมูลได้ถูกบันทึกไว้ในบล็อกเชน มันจะเป็นเรื่องยากมากๆ ที่จะเข้าไปเปลี่ยนแปลง เวลาที่มีใครต้องการจะเพิ่มข้อมูล ทุกๆ คนในเครือข่ายซึ่งล้วนแต่มีสำเนาของบล็อกเชน สามารถเชื่อมต่อเงื่อนไขหรือข้อกำหนด (Algorithm) เพื่อตรวจสอบการเชื่อมต่อ (Transaction) โดย หรือผู้ที่จะเข้ามาเชื่อมต่อ (Transaction) ใหม่จะต้องได้รับอนุญาต จากในเครือข่ายส่วนใหญ่

เสียก่อน ทำให้เกิดการเชื่อมต่อขยายออกไปได้มากขึ้นเรื่อยๆ และหากกล่าวถึง บล็อกเชน แล้ว สิ่งที่มาพร้อมและต้องกล่าวถึง คือ

(๑) ลักษณะของ Big data คือ ข้อมูลที่ประกอบด้วยคุณลักษณะ ๓ อย่าง คือ

- Volume ข้อมูลมีขนาดใหญ่
- Variety ข้อมูลมีความหลากหลาย
- Velocity ข้อมูลมีการเปลี่ยนแปลงตลอดเวลาอย่างรวดเร็ว

ปัจจุบัน ยังมีการเพิ่มความสำคัญใน คุณลักษณะที่ ๔ คือ Veracity (ความถูกต้องของข้อมูล)

เนื่องจากความก้าวหน้าของเทคโนโลยีสารสนเทศ ทำให้มีการเปลี่ยนแปลงเกิดขึ้นหลายอย่าง เช่น การเกิดขึ้นของสัญญาระหว่าง คำเสนอ กับ คำสนอง ซึ่งมีลักษณะที่ก้าวล้ำไปจากประมวลกฎหมายแพ่งและพาณิชย์ที่ใช้กันอยู่ในปัจจุบัน จึงจำเป็นต้องมีการปรับปรุงกฎหมายต่างๆ เพื่อรองรับกับความก้าวหน้าและความเปลี่ยนแปลงที่กำลังเกิดขึ้น เช่น เรื่องภาษีอากร

(๒) Internet of Things (IOT)

เนื่องจากความก้าวหน้าของเทคโนโลยีสารสนเทศ ทำให้มีการเปลี่ยนแปลงเกิดขึ้นหลายอย่างการติดต่อสื่อสารที่ข้ามพรมแดน รวมทั้งการเปลี่ยนในวิถีการดำเนินชีวิตที่มีการได้ประโยชน์จากอินเตอร์เน็ตมากขึ้น เช่น ธุรกรรมทางการเงิน จึงจำเป็นต้องมีการปรับปรุงกฎหมายต่างๆ เพื่อรองรับกับความก้าวหน้าและความเปลี่ยนแปลงที่กำลังเกิดขึ้น

แม้ว่าบล็อกเชน จะมีความมั่นคงและตรวจสอบได้ค่อนข้างดี แต่สิ่งที่ถือเป็นจุดอ่อนและควรพึงระวัง คือ

- ลิขสิทธิ์ เนื่องจากในขั้นตอนของการเชื่อมต่อของบล็อกต่างๆ ที่อาจจะมีการสวมการเชื่อมต่อได้ ที่เรียกกันว่า การแฮก (hack) ข้อมูล นำไปสู่การสวมสิทธิ์เข้าไปใช้ข้อมูลโดยคนที่ไม่ใช่เจ้าของ เป็นสิ่งที่ยังต้องพึงระวังและให้ความสำคัญ เพราะนั่นหมายถึงการที่ผู้อื่นเข้ามาใช้และดำเนินการต่างๆ โดยที่เจ้าของบล็อกไม่รับรู้และไม่รับทราบ ซึ่งจะกลายเป็นทางปัญหาทางกฎหมายต่อไป

- ลักษณะของ Big Data จะมีลักษณะสวนทางกับความเป็นส่วนตัวหรือข้อมูลส่วนบุคคล คือ เมื่อให้ความสำคัญและใช้งานเกี่ยวกับ Big Data อาจจะไปกระทบกับข้อมูลส่วนบุคคล ซึ่งจำเป็นต้องพิจารณาถึงสมดุลของการใช้งาน รวมทั้งกรณีของผู้มีอำนาจหรือผู้เข้าถึงข้อมูล นำข้อมูลจาก Big Data ไปใช้ประโยชน์ส่วนตน จึงจำเป็นต้องให้ดำเนินการด้วยความโปร่งใส ตรวจสอบได้

ปัจจุบัน ประเทศไทยได้มีการพัฒนาและปรับปรุงกฎหมายหลายฉบับ เพื่อรองรับกับการเปลี่ยนแปลงที่กำลังเกิดขึ้น คือ

- ร่างพระราชบัญญัติเกี่ยวกับระบบอิเล็กทรอนิกส์ของภาครัฐ
- ร่างพระราชบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- ร่างพระราชบัญญัติเกี่ยวกับความปลอดภัยในโลกไซเบอร์
- ร่างพระราชบัญญัติเกี่ยวกับการพาณิชย์ในระบบอิเล็กทรอนิกส์
- ร่างพระราชบัญญัติเกี่ยวกับการกระบวนการประเมินผลการออกกฎหมาย

“Criminal Justice : The Use of Big Data as Evidence” (ความยุติธรรมทางอาญา : การใช้ข้อมูลขนาดใหญ่เพื่อหาพยานหลักฐาน)

คำว่า “Big Data”นั้น ยังไม่มีคำนิยามที่เป็นข้อยุติแต่โดยทั่วไปเป็นที่ยอมรับร่วมกันว่ามีองค์ประกอบ ๓ อย่าง คือ

๑) มีการเก็บรวบรวมข้อมูล

- ข้อมูลมีขนาดใหญ่
- ข้อมูลมีความหลากหลายจากแหล่งที่มา
- ฐานข้อมูลส่วนใหญ่ไม่มีโครงสร้างที่ชัดเจน

๒) มีการวิเคราะห์ข้อมูล

- มีการวิเคราะห์ข้อมูลด้วยความรวดเร็ว
- มีการสร้างหรือกำหนดเงื่อนไข (Algorithms) ในการวิเคราะห์ข้อมูล
- มีเครื่องมือหรืออุปกรณ์อิเล็กทรอนิกส์ เช่น ระบบคอมพิวเตอร์เข้าช่วยในการทำงาน
- มีเครื่องมือทางสถิติ เพื่อหาความสัมพันธ์ต่างๆ

๓) มีการนำไปใช้

- ภาครัฐ เช่น ข้อมูลด้านสุขภาพของประชาชน ความต้องการประชาชน การระบาดของโรคติดต่อ การพยากรณ์อากาศเป็นต้น
- ภาคเอกชน เช่น บริษัทประกันภัย ธนาคาร สินเชื่อ การลงทุน การโฆษณา และข้อมูลการค้าขายสินค้าต่างๆ เป็นต้น

การใช้ “Big Data” ในการหาพยานหลักฐานทางอาชญากรรมของต่างประเทศ

กรณีของประเทศสิงคโปร์และประเทศอังกฤษ

๑) ในลักษณะมองย้อนกลับ เป็นการใช้เพื่อหาพยานหลักฐาน กรณีที่เกิดอาชญากรรมขึ้นแล้ว เช่น ข้อมูลการใช้งานโทรศัพท์มือถือ ซึ่งระบุสถานที่ของผู้ต้องสงสัย การติดต่อการส่งข้อความในโลกออนไลน์ กล้องโทรทัศน์วงจรปิด และหลักฐานการเสียภาษีหรือบันทึกเกี่ยวกับการทำธุรกรรมทางการเงิน เป็นต้น

๒) ในลักษณะมองไปข้างหน้า การใช้เพื่อคาดการณ์ถึงอาชญากรรมที่จะเกิดขึ้นในอนาคต จากข้อมูลทางสถิติแทนการคาดเดาโดยสัญชาติญาณ เพื่อลดอคติในการประเมินสถานการณ์ เป็นการป้องกันอาชญากรรมที่อาจจะเกิดขึ้น หรือเพื่อเตรียมความพร้อมในการตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็ว และทันต่อสถานการณ์

ข้อจำกัดหรือข้อพึงระวังในการใช้ “Big Data”

๑) การใช้งาน “Big Data” อาจจะไปกระทบเกี่ยวกับข้อมูลส่วนบุคคลของประชาชน โดยเฉพาะกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

๒) ความแม่นยำ เนื่องจากผลลัพท์ที่ได้อาจจะขาดความแม่นยำ ซึ่งองค์ประกอบที่เกี่ยวข้องกับระดับของความแม่นยำในผลลัพท์จาก “Big Data” ขึ้นอยู่กับ

- การใส่ข้อมูลความต้องการ ที่ต้องมีความชัดเจน และตรงความต้องการ

- การป้อนข้อ...

- การป้อนข้อมูลดิบ ที่ต้องคำนึงถึงความถูกต้องของข้อมูลพื้นฐาน

- การกำหนดกรอบของความสัมพันธ์ของสิ่งต่างๆ ไม่ถูกต้อง ซึ่งเป็นส่วนของการกำหนดเงื่อนไขทางสถิติ

๓) การเลือกปฏิบัติ ซึ่งการเลือกปฏิบัติอาจจะเกิดจากลักษณะของข้อมูลที่เป็นผลลัพท์ของการประมวลผลทางสถิติ โดยเกิดจากลักษณะของข้อมูลดิบ หรือจากการสร้าง หรือกำหนดเงื่อนไข (Algorithms) ในการวิเคราะห์ข้อมูล

๔) การรั่วไหลของข้อมูล ซึ่งการรั่วไหลของข้อมูลนี้ อาจจะเกิดผลกระทบต่างๆ ตามมา เช่น กระทบต่อกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ผู้มีอำนาจในการเข้าถึงข้อมูลนำไปใช้ในเรื่องส่วนตัว หรือ กลุ่มอาชญากรนำไปใช้ในการวางแผนก่ออาชญากรรม เป็นต้น

“ The Challenges of Big Data in Criminal Procedure How to Handle Digital Discovery and Use as Digital Evidence” (ความท้าทายของใช้ข้อมูลขนาดใหญ่ในกระบวนวิธีพิจารณาความอาญา การใช้ข้อมูลดิจิทัลเพื่อเป็นพยานหลักฐาน)

เมื่อพิจารณาพยานหลักฐานอิเล็กทรอนิกส์ สิ่งที่ต้องพิจารณา คือ

๑) พยานหลักฐานอิเล็กทรอนิกส์นั้นเกี่ยวข้องกับคดีหรือไม่

สิ่งที่ต้องพิจารณาและคำนึงถึง คือ

- พยานหลักฐานนั้นมีความเกี่ยวข้องกับคดี และมีแนวโน้มที่พยานหลักฐานนั้นจะพิสูจน์ถึงองค์ประกอบของฐานการกระทำความผิด ข้อต่อสู้เกี่ยวกับความผิดที่เกิดขึ้น หรือข้อเรียกร้อง ที่เกี่ยวข้องกับคดีแพ่ง

- ต้องพิจารณาถึงมาตรฐานขั้นต่ำ ว่าสามารถใช้เป็นพยานในลักษณะใด

- คู่ความที่เสนอพยานหลักฐานดังกล่าวต่อศาล มีภาระในการนำสืบถึงพยานหลักฐานนั้น

๒) มีบทบัญญัติของกฎหมายห้ามรับฟังพยานหลักฐานนั้นหรือไม่

สิ่งที่ต้องพิจารณาและคำนึงถึง คือ

- เอกสิทธิ์ในการไม่เบิกความเป็นผลร้ายแก่ตนเอง

- เอกสิทธิ์ของหน่วยงานของรัฐ

- การได้มาซึ่งพยานหลักฐานนั้น ได้มาโดยชอบด้วยกฎหมายหรือไม่

๓) พยานหลักฐานนั้นถูกต้องแท้จริงและมีความน่าเชื่อถือหรือไม่

สิ่งที่ต้องพิจารณาและคำนึงถึง คือ

- คู่ความที่นำเสนอพยานหลักฐานนั้น สามารถพิสูจน์ถึงความน่าเชื่อถือของพยานนั้นหรือไม่

- พยานหลักฐานนั้นอาจถูกแก้ไข เปลี่ยนแปลง หรือบิดเบือนโดยคนที่ทำให้เกิดพยานหลักฐานนั้นขึ้นหรือไม่

- การพิสูจน์ความถูกต้องแท้จริงหรือความน่าเชื่อถือของพยานหลักฐาน : การพิสูจน์จากองค์ประกอบภายนอกหรือพิสูจน์จากพยานหลักฐานชิ้นนั้นเอง

๔) พยานหลัก...

๔) พยานหลักฐานนั้นเป็นต้นฉบับหรือเป็นข้อมูลจากแหล่งอื่น

สิ่งที่ต้องพิจารณาและคำนึงถึง คือ

- การใช้ต้นฉบับหรือสำเนาต้นฉบับ เป็นที่พึงประสงค์มากกว่า
- พยานหลักฐานดังกล่าว เป็นต้นฉบับหรือสำเนาต้นฉบับ
- คู่ความพยายามจะพิสูจน์ถึงเนื้อหาของเอกสารหรือบันทึกทางอิเล็กทรอนิกส์นั้น หรือไม่
- ถ้าต้นฉบับหรือสำเนาต้นฉบับมาไม่สามารถนำมาได้ สามารถใช้พยานหลักฐานอื่นได้หรือไม่ เช่น ร่างเอกสาร หรือคำเบิกความของคนอ่านหรือเห็นเอกสาร เป็นต้น

“หลักการชั่งน้ำหนักและการรับฟังพยานหลักฐานดิจิทัลในชั้นศาล (The Principles of Weight and Admissibility of Digtal Evidence in the Court)”

๑) พยานหลักฐานดิจิทัล

หมายถึง สารสนเทศ (information) หรือข้อมูล(Data) ที่เก็บรักษาไว้โดยสื่อบันทึกข้อมูล หรือที่อยู่ในระหว่างการรับส่งโดยวิธีการทางอิเล็กทรอนิกส์ ซึ่งมีคุณค่าต่อการแสวงหาความจริง และสามารถอ้างอิงเป็นพยานหลักฐานเพื่อพิสูจน์ข้อเท็จจริง หรือการกระทำความผิดในกระบวนการยุติธรรมได้

ข้อมูลพยานหลักฐานจาก Big Data เป็นพยานหลักฐานในรูปแบบดิจิทัล โดยส่วนใหญ่จะใช้คอมพิวเตอร์ในการปฏิบัติการ ได้แก่

- ในระบบคอมพิวเตอร์หรือในอุปกรณ์อิเล็กทรอนิกส์
- ในเครือข่ายคอมพิวเตอร์
- รูปภาพ (Graphics) หรือเสียง (Audio) ที่ถูกจัดเก็บอยู่ในรูปสัญญาณดิจิทัล
- ไฟล์บันทึกของกล้องวงจรปิด และอุปกรณ์สารสนเทศอื่นๆ ที่บันทึกขึ้นโดยอุปกรณ์คอมพิวเตอร์

๒) การรับฟังพยานหลักฐานดิจิทัลในศาลไทย

ศาลไทยไม่อาจปฏิเสธการรับฟังพยานหลักฐาน เพียงเพราะเหตุที่พยานหลักฐานนั้น อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ เนื่องจากได้มีการกำหนดไว้ในกฎหมายอย่างชัดเจน เช่น มาตรา ๑๑ วรรคแรก ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ แก้ไข (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ “ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์”

ซึ่งพยานหลักฐานที่รับฟังได้ ต้องไม่เข้าข่าย “ต้องห้ามรับไม่ให้รับฟัง” (Exclusionany Rule) ตามกฎหมาย ประกอบด้วย

- ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา ๒๒๖ , ๒๒๖/๑
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และแก้ไขเพิ่มเติม ตาม มาตรา ๒๕ “ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่

พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญา หรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น”

- พยานบอกเล่า (Hearsay Rule)

- พยานที่ดีที่สุด (The Best Evidence Rule) หรือต้นฉบับ (Original)

๓) สถานภาพทางกฎหมายของพยานหลักฐานดิจิทัล

สถานภาพทางกฎหมายของพยานหลักฐานดิจิทัล มีใน ๒ ลักษณะ คือ

(๑) พยานเอกสาร หมายถึงอยู่ในรูปแบบของ ข้อความด้วยตัวอักษร ตัวเลข ผัง หรือเครื่องหมายอื่นใดอันปรากฏความหมายที่ปรากฏอยู่บนกระดาษหรือวัตถุอื่นใดซึ่งคู่ความนำเสนอต่อศาล เพื่อใช้ความหมายของข้อความหรือเครื่องหมายนั้นพิสูจน์ข้อเท็จจริง

(๒) พยานวัตถุ หมายถึงอยู่ในรูปแบบของ สิ่งใดๆ ที่นำเอารูปร่าง ลักษณะและสภาพของสิ่งของชิ้นนั้นมาใช้เป็นพยานหลักฐานพิสูจน์ข้อเท็จจริงในทางคดี

๔) การนำสืบพยานหลักฐานดิจิทัลในคดีอาญาต่อศาล

กฎหมายกำหนดวิธีการนำสืบพยานหลักฐานไว้เพียง ๔ ประเภท คือ

- พยานบุคคล

- พยานเอกสาร (ต้องส่งต้นฉบับล่วงหน้าก่อนวันสืบพยาน ไม่น้อยกว่า ๑๕ วัน)

- พยานวัตถุ

- พยานผู้เชี่ยวชาญ

แต่ไม่มีข้อกำหนดเกี่ยวกับวิธีการสืบพยานหลักฐานดิจิทัลไว้ รวมทั้งการพิสูจน์ความแท้จริงของพยานหลักฐานดิจิทัล

๕) ลักษณะการรับรองหรือยืนยันความแท้จริงของพยานดิจิทัล

(๑) รับรองความแท้จริงของบันทึกคอมพิวเตอร์ คือ แท้จริงเนื่องจากไม่เคยถูกแก้ไขเปลี่ยนแปลง

- การโต้แย้งความแท้จริงว่ามีการแก้ไขเปลี่ยนแปลง ต้องมีเหตุผลสนับสนุนว่ามีการแก้ไขดังกล่าวเกิดขึ้นจริง

- ลำพังความเป็นไปได้ที่จะมีการแก้ไข ไม่มีผลต่อความแท้จริงของบันทึกคอมพิวเตอร์

(๒) พิสูจน์ความน่าเชื่อถือของโปรแกรม หรือระบบที่สร้างหรือระบบจัดเก็บบันทึกคอมพิวเตอร์

- ระบบทำงานไม่ผิดพลาด

- ระบบถูกใช้อยู่เป็นประจำหรือเป็นปกติทางธุรกิจการค้า

(๓) แสดงความน่าเชื่อถือของบุคคลผู้สร้าง หรือจัดเก็บบันทึกคอมพิวเตอร์

(๔) โดยการยืนยันความแท้จริงทุกประเภท ต้องเปิดโอกาสอย่างเต็มที่ให้คู่ความฝ่ายตรงข้าม (ไม่ได้เป็นผู้อ้างอิงพยานหลักฐานนั้น) พิสูจน์หรือทดสอบเพื่อโต้แย้งด้วย