ภาคผนวก ง.
ความเป็นส่วนตัว (Privacy)
และการวัดทางชีวภาพ (Biometric measure)

(อ้างอิง จากบทที่ 9 หัวข้อ 2.2.2)

ความเป็นส่วนตัว (Privacy)

ความเป็นส่วนตัวนี้ สามารถถูกพิจารณาในหลายมุมมอง ทั้งในด้านสิทธิตามกฎหมาย หรือสิทธิตามหลักศีลธรรม จริยธรรม ความเป็นส่วนตัวนี้รวมถึง

1. ความเป็นส่วนตัวในร่างกาย ได้แก่ การโยกย้ายถ่ายเท และใช้ประโยชน์จากอวัยวะ เนื้อเยื่อ ของเหลวที่ได้จากร่างกาย โดยปราศจากการยินยอม

2. ความเป็นส่วนตัวในพฤติกรรม ครอบคลุมถึงพฤติกรรมการกระทำทั้งในที่ลับ และที่แจ้ง ตัวอย่างเช่น การลักลอบบันทึกเสียงในห้องน้ำหญิง ซึ่งไม่มีความผิดในทางกฎหมาย

3. ความเป็นส่วนตัวในการติดต่อสื่อสารกับบุคคลอื่นผ่านทางสื่อต่างๆ อย่างเป็นอิสระ โดยไม่ถูกลักลอบ ดักฟัง หรืออยู่ในสายตา หน่วยงาน องค์กร นิติบุคคลใด หรือ ปัจเจกบุคคล เช่น การลักลอบดักฟังโทรศัพท์

4. ความเป็นส่วนตัวในข้อมูลข่าวสารส่วนบุคคล เช่น ชื่อ ที่อยู่ ข้อมูลสุขภาพ ข้อมูลการเงิน ข้อมูลไบโอเมตริกซ์ ฯลฯ ที่เป็นการบ่งชี้ความเป็นตัวตนของปัจเจกบุคคล ย่อมต้องเป็นสมบัติของบุคคลนั้น ต้องไม่ถูกเผยแพร่ต่อบุคคลอื่น หน่วยงาน หรือ สาธารณชน และบุคคลย่อมมีสิทธิที่จะควบคุมการใช้ประโยชน์ แก้ไข เปลี่ยนแปลงข้อมูลข่าวสารส่วนบุคคลของตนได้

ตัววัดทางชีวภาพ หรือ ไบโอเมตริกซ์ (Biometric) หมายถึงวิธีการ หรือ เทคนิคในการตรวจสอบแยกแยะสิ่งมีชีวิต โดยวัดจากคุณลักษณะของสิ่งมีชีวิตนั้นๆ ในด้านคำจำกัดความไบโอเมตริกซ์ คือ เทคนิคอัตโนมัติต่างๆ ในการตรวจวัดคุณลักษณะทางกายภาพ (Physical Characteristics) พฤติกรรม (Behaviors) ตลอดจนร่องรอยอื่นๆ ในชีวิตประจำวัน (Personal traits) ของบุคคลที่มีชีวิต แล้วนำมาเปรียบเทียบกับคุณลักษณะนั้นๆ ที่ได้มีการบันทึกไว้ก่อนหน้านี้ในฐานข้อมูล เพื่อวัตถุประสงค์ในการแยกแยะ (Recognizing) บุคคลนั้นจากบุคคลอื่น สำหรับไบโอเมตริกซ์นั้น คุณลักษณะต่างๆ ไม่ว่าจะเป็นคุณลักษณะทางกายภาพ ทางพฤติกรรม หรือร่องรอยอื่นๆ ในชีวิตประจำวันของบุคคลต้องสามารถที่จะวัดในเชิงปริมาณได้ คุณลักษณะทาง

กายภาพนั้นส่วนใหญ่จะไม่แปรเปลี่ยนไปตามกาลเวลาในขณะที่คุณลักษณะทางพฤติกรรม หรือร่องรอยในชีวิตประจำวันอาจมีการเปลี่ยนแปลงไปตามกาลเวลา ตามการเรียนรู้ของเจ้าของได้ ดังนั้นไบโอเมตริกซ์ที่ใช้คุณลักษณะทางกายภาพมาเป็นตัววัดจึงได้รับความเชื่อถือมากกว่า ตัวอย่างคุณลักษณะทางกายภาพที่นำมาเป็นตัวบ่งชี้ทางไบโอเมตริกซ์ อย่างแพร่หลาย ได้แก่ ลายนิ้วมือ ม่านตา เส้นเลือดที่ผนังลูกตาดำ รูปพรรณสัณฐานของมือ โครงสร้างรูปหน้า ดังตาราง ง.1

ตาราง ง.1 ไบโอเมตริกซ์เทคโนโลยีที่ได้รับการพัฒนาจนเป็นผลิตภัณฑ์เชิงพานิชย์ นอกจากนี้ยังมีคุณลักษณะทางกายภาพอื่นๆ ที่กำลังศึกษา เช่น ลักษณะรอยย่นของข้อนิ้ว (Knuckle creases) คลื่นสมอง (Acoustic Head Resonance) หรือ กลิ่นตัว (Body Odors) เป็นต้น คุณสมบัติบางประการแปรเปลี่ยนไปตามกาลเวลา เช่น เสียงพูด ลายเซ็น (Hand - written signature) โดยพิจารณาพลวัตการใช้แป้นพิมพ์ (Keystroke dynamics)

ข้อมูลไบโอเมตริกซ์ต้องเก็บบันทึกจาก บุคคลที่ยังมีชีวิตอยู่เท่านั้น โดยระบบจะทำการตรวจเช็คความมีชีวิตของบุคคลด้วย ดังนั้นจึงไม่สามารถนำข้อมูลจากผู้ไม่มีชีวิตแล้วมาใช้งานได้ คุณสมบัติข้อนี้ทำให้เทคโนโลยีไบโอเมตริกซ์แตกต่างไปจากศาสตร์ทางด้านการชันสูตรศพ (Forensic Sciences)

ไบโอเมตริกซ์ถูกนำมาใช้เพื่อ การทำความรู้จัก หรือ แยกแยะตัวบุคคล โดยแบ่งการใช้งานออกมาได้เป็น 2 โอกาส คือ

1. การทวนสอบ เพื่อบ่งชี้ความเป็นตัวจริง (Verification) เป็นการเปรียบเทียบข้อมูลไบโอเมตริกซ์ที่เก็บได้ใหม่ (ณ จุดใช้งาน) กับข้อมูลของบุคคลนั้นที่ได้เคยลงทะเบียนไว้ เพื่อพิสูจน์ว่าบุคคลที่มากล่าวอ้างเป็นตัวจริง

2. การระบุ (Identification) ว่าบุคคลนั้นๆ เป็นใคร เป็นการเปรียบเทียบข้อมูลไบโอเมตริกซ์ที่เก็บใหม่ ณ จุดใช้งานกับข้อมูลไบโอเมตริกซ์ทั้งหมดที่มีอยู่ในฐานข้อมูลเพื่อพิสูจน์ว่าเจ้าของข้อมูล ณ จุดใช้งานเป็นใครในฐานข้อมูล

เทคโนโลยีไบโอเมตริกซ์จะใช้เทคนิคการทำงานแบบอัตโนมัติ ซึ่งมีขั้นตอน ดังนี้

1. เก็บตัวอย่างคุณลักษณะที่ต้องการวัด เช่น สแกนลายนิ้วมือออกมาเป็นภาพถ่ายลายนิ้วมือ

2. เก็บข้อมูลไบโอเมตริกซ์จากตัวอย่างที่สแกนได้ในข้อ 1 เช่น เก็บข้อมูลเชิงปริมาณจากภาพถ่ายลายนิ้วมือด้วยการคำนวณโดยใช้อัลกอริทึมเฉพาะ

3. เปรียบเทียบข้อมูลเชิงปริมาณที่วัดได้จากข้อ 2 กับข้อมูลที่ได้บันทึกไว้ก่อนหน้านี้ ซึ่ง

ไบโอเมตริกซ์	รายละเอียด	ข้อดี	ข้อเสีย
เรตินาสแกน	ภาพสแกนการจัดเรียงของเส้นเลือดดำ (vein pattern) ที่ผนังชั้นในสุดของลูกตา	เรตินาจะมีรูปแบบไม่เปลี่ยนแปลงตลอดชั่วอายุคน จึงทำให้บ่งชี้ตัวบุคคลได้อย่างแม่นยำ	จะต้องแนบลูกตาให้ติดกับอุปกรณ์ (ประมาณ 3 นิ้ว) ทำให้ไม่สะดวกกับการใช้งานในที่สาธารณะ เพราะถือว่าต้องมีการล่วงล้ำทางกายภาพ
ไอริส	เก็บภาพพื้นผิวด้านที่มองเห็นของไอริสโดยใช้กล้องวิดีโอมาตรฐาน	ไม่ต้องล่วงล้ำทางกายภาพเพราะกล้องสามารถสแกนไอรสได้ในระยะห่างประมาณ 2-3 ฟุต	อุปกรณ์มีราคาค่อนข้างแพง อีกทั้งต้องการเนื้อที่ในการเก็บข้อมูลค่อนข้างมาก และเนื่องจากเป็นส่วนที่เกี่ยวข้องกับดวงตาจึงอาจจะไม่ได้รับการยอมรับจากสาธารณะชนเท่าที่ควร
ลายนิ้วมือ	ออปติคอลสแกนลักษณะเส้นลายนิ้วมือ	เป็นที่ยอมรับโดยทั่วไปว่าลายนิ้วมือของคนจะเป็นหนึ่งเดียว และไม่ซ้ำกับลายนิ้วมือของคนอื่นในโลกนี้	ต้องวางนิ้วมือติดกับเครื่องสแกนเนอร์ซึ่งเสี่ยงต่อการติดเชื้อ และร่องรอยลายนิ้วมือที่หลงเหลืออยู่บนเครื่อง หรือรอยมีดบาดอาจสร้างปัญหาได้ ทั้งยังให้ภาพลักษณ์ว่ามีความเกี่ยวข้องกับอาชญากรรม
โครงสร้างของมือและนิ้ว	ออปติคอลสแกนรูปร่างมือและนิ้ว (สามมิติ) ซึ่งจะบันทึกความกว้าง ความยาว และความหนาของมือและนิ้ว	สะดวกต่อการใช้งาน และใช้เนื้อที่ในการเก็บข้อมูลไม่มากนัก	ไม่มีคุณสมบัติที่เป็นหนึ่งเดียว เช่นเดียวกับลายนิ้วมือ หรือเรตินา อีกทั้งบาดแผลบนมือก็สามารถทำให้เป็นอุปสรรคได้เหมือนกัน
ภาพถ่ายใบหน้า	รหัสดิจิทัลที่แปลงจากภาพถ่ายใบหน้า	สะดวกและไม่ต้องมีการล่วงล้ำทางกายภาพ	คนที่หน้าคล้ายกันอาจทำให้อุปกรณ์สับสนได้ และใบหน้าคนก็เปลี่ยนไปตามกาลเวลาด้วย นอกจากนั้นการไว้หนวดเคราก็สามารถที่จะหลอกเครื่องให้เข้าใจผิดได้แล้ว
เสียงพูด	รหัสดิจิทัลที่แปลงจากสัญญาณเสียงพูดแบบอะคูสติก	ใช้งานได้ดีกับเครื่องโทรศัพท์ โดยสามารถตรวจความแตกต่างระหว่างเสียงพูดสดกับเสียงที่อัดเทป หรือการเลียนเสียงพูดได้	เสียงคนอาจเปลี่ยนแปลงได้อีกทั้งเสียงรบกวนรอบข้างก็อาจเป็นอุปสรรคต่อความแม่นยำ และยังต้องใช้เนื้อที่ในการเก็บข้อมูลมาก
พลวัตของลายเซ็น	การเก็บข้อมูลคุณลักษณะต่างๆ ของลายเซ็น ไม่ว่าจะเป็นการจรดปากกา การลากลายเส้น ความเร็ว น้ำหนักและทิศทางของลายเส้น	สะดวกและง่ายต่อการใช้งานเพราะผู้ใช้คุ้นเคยกับการเซ็นชื่ออยู่แล้ว	หากมีการเปลี่ยนแปลงลายเซ็นก็จะต้องให้เครื่องเรียนรู้ใหม่ ทำให้ไม่สามารถประกันความแม่นยำได้ดีเท่าที่ควร

ตาราง ง.1 ไบโอเมตริกซ์เทคโนโลยีที่ได้รับการพัฒนาจนเป็นผลิตภัณฑ์เชิงพาณิชย์

อาจบันทึกไว้ในฐานข้อมูลกลาง หรือบันทึกบนบัตรอัจฉริยะ

4. พิจารณาผลการเปรียบเทียบว่าถูกต้องตรงกันหรือไม่

5. ตัดสินว่าเป็นบุคคลนั้นจริง หรือ บุคคลนี้เป็นใคร

การนำเทคโนโลยีไบโอเมตริกซ์มาใช้กับงานต่างๆ เช่น

1. ควบคุมการผ่านเข้า-ออก อาคารสถานที่ หรือ ควบคุมการผ่านชายแดน โดยใช้เครื่องกราดตรวจ มือ นิ้ว หรือ โครงสร้างรูปหน้า

2. รักษาความปลอดภัยของระบบคอมพิวเตอร์ ใช้การตรวจสอบลายนิ้วมือ ม่านตา โครงสร้างใบหน้า พลวัตการพิมพ์

3. การทำธุรกรรม เช่น ใช้การกราดตรวจม่านตา (Iris scanning) การรู้จำรูปหน้า (Facial recognition) มาใช้กับเครื่องฝากถอนเงินอัตโนมัติ แทนการใช้รหัส

4. จัดการฐานข้อมูลอาชญากรและนักโทษ

5. ควบคุมการลงเวลาทำงาน เช่น ใช้การกราดตรวจมือเพื่อลงเวลาเข้าออกพนักงาน

6. ป้องกันการโกงใช้โทรศัพท์เคลื่อนที่

การนำไบโอเมตริกซ์มาใช้เพื่อบ่งชี้ความเป็นตัวตนที่แท้จริงของบุคคลมากขึ้น ความเสี่ยงในการถูกคุกคามความเป็นส่วนตัวก็มากขึ้นเช่นกัน ไบโอเมตริกซ์จึงมีความเกี่ยวข้องกับความเป็นส่วนตัวในข้อมูลข่าวสารส่วนบุคคล เช่น การดำเนินชีวิตประจำวันสามารถถูกตรวจสอบได้ง่ายว่ากระทำกิจกรรมใดบ้างในแต่ละวัน นอกจากนั้นข้อมูลในรูปดิจิทัลสามารถทำซ้ำหรือถ่ายโอนผ่านทางเครือข่ายคอมพิวเตอร์ไปสู่บุคคลอื่น หรือสู่สาธารณชนได้ง่าย และไวต่อความเสียหายมากกว่าข้อมูลรูปแบบอื่น

อย่างไรก็ตามตัววัดทางชีวภาพ ถูกนำมาใช้ประโยชน์ในการระบุตัวบุคคลที่แท้จริงกว้างขวาง เพราะยังเป็นตัววัดที่ลอกเลียนปลอมแปลงได้ยากขึ้น เช่น การเข้าถึงสถานที่หวงห้าม โดยตรวจสอบลายนิ้วมือ การเข้าถึงข้อมูลส่วนบุคคล ข้อมูลสำคัญที่เป็นความลับ ตัววัดทางชีวภาพเมื่อนำมาใช้ร่วมกับเทคโนโลยีอื่น เช่น การใช้บัตรอัจฉริยะและเทคโนโลยีการเข้ารหัสข้อมูล วิธีการนี้ข้อมูลตัววัดทางชีวภาพจะถูกเข้ารหัสและเก็บบันทึกไว้บนบัตรอัจฉริยะ โดยที่ ณ จุดใช้งานการตรวจสอบการระบุตัวตนจะทำโดยการถอดรหัสข้อมูลตัววัดทางชีวภาพที่บันทึกไว้บนบัตรด้วยตัววัดทางชีวภาพที่กราดตรวจใหม่จากตัวบุคคล ถ้าเข้ากันได้ แสดงว่าผ่านขั้นตอนการตรวจสอบความเป็นตัวจริง รูปแบบนี้เป็นตัวอย่างการตรวจสอบความเป็นตัวจริง (Verification) ของบุคคลเท่านั้น ยังไม่สามารถระบุได้ว่าบุคคลนั้นเป็นใคร (Identification) ถ้าต้องการระบุความ

เป็นตัวตนต้องตรวจสอบกับข้อมูลส่วนบุคคลที่บันทึกไว้ล่วงหน้าบนฐานข้อมูลกลาง

ดังนั้นการนำเทคโนโลยีมาใช้งาน จำเป็นต้องมีกฎ และ ระเบียบต่างๆ ในสังคม ที่มีการปรับปรุงแก้ไขให้เหมาะสม สามารถรองรับหลักการกว้างๆ สำหรับการใช้ตัววัดทางชีวภาพได้ ได้แก่

1. การแจ้งให้ทราบล่วงหน้า การจัดเก็บข้อมูลส่วนบุคคลต้องกระทำเปิดเผย แจ้งให้ทราบโดยทั่วกัน มิใช่ลักลอบเก็บ

2. การเข้าถึงข้อมูลตัววัดทางชีวภาพ บุคคลย่อมมีสิทธิที่จะตรวจสอบข้อมูลตัววัดทางชีวภาพของตนที่เก็บอยู่ในฐานข้อมูล และมีสิทธิที่จะรับรู้ว่าข้อมูลนั้นๆ ของตนถูกนำไปใช้งานอย่างไร โดยที่ผู้จัดเก็บข้อมูลตัววัดทางชีวภาพจะต้องเปิดเผยแนวทางการจัดการเกี่ยวกับความเป็นส่วนตัว (Privacy practices) ต่อสาธารณะ

3. การแก้ไขข้อมูลตัววัดทางชีวภาพ บุคคลย่อมมีสิทธิในการแก้ไขปรับปรุงหรือเปลี่ยนแปลงรายการข้อมูลตัววัดทางชีวภาพของตนได้

4. การยินยอม เจ้าของต้องได้รับแจ้งล่วงหน้าเกี่ยวกับการใช้ข้อมูลโดยปกติ และถ้าจะมีการใช้นอกเหนือจากที่มีการแจ้ง จะต้องได้รับการยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูลก่อนการใช้งาน

5. ความปลอดภัยและความน่าเชื่อถือ หน่วยงานที่จัดเก็บข้อมูลตัววัดทางชีวภาพ ต้องมีระบบการจัดเก็บฐานข้อมูลที่น่าเชื่อถือ ตลอดจนมีการรักษาความปลอดภัย

สำหรับประเทศไทย ตัววัดทางชีวภาพยังถูกนำมาใช้ค่อนข้างน้อย และมักเป็นไปเฉพาะในภาคราชการเท่านั้น เช่น การเก็บทะเบียนประวัติอาชญากรพร้อมตัวอย่างลายนิ้วมือทั้ง 10 นิ้ว สำหรับภาคเอกชน จะเป็นการนำเทคโนโลยีนี้มาใช้ควบคู่กับเทคโนโลยีอื่น เช่น บัตรอัจฉริยะ และเทคโนโลยีการเข้ารหัสข้อมูล เพื่อใช้กับงานด้านการเงิน การธนาคาร เพราะงานเหล่านี้ต้องการความปลอดภัยของข้อมูลส่วนบุคคล (Security of personal data) และความเป็นส่วนตัวของเจ้าของบัตรค่อนข้างสูง

ในการเก็บทะเบียนประวัติอาชญากร ที่กองทะเบียนประวัติอาชญากร ของสำนักงานตำรวจแห่งชาติ มีระบบตรวจสอบลายนิ้วมืออัตโนมัติ (Automated Fingerprints Identification System, AFIS) ใหญ่เป็นอันดับสองในเอเชีย รองจากประเทศญี่ปุ่น เก็บฐานข้อมูลทะเบียน-ประวัติคนร้ายทั่วประเทศพร้อมตัวอย่างลายนิ้วมือสิบนิ้วมากกว่า 4 ล้านระเบียน (มิถุนายน 2541) ฐานข้อมูลนี้หน่วยราชการอื่นสามารถใช้ในการอ่านข้อมูลได้ (Read only) เช่น สำนักงานคณะ-

กรรมการป้องกันและปราบปรามยาเสพติด กองตรวจคนเข้าเมือง เป็นต้น

โครงการจีเน็ต หรือ Government Information Network เป็นโครงการที่จะสนับสนุนให้หน่วยงานภาครัฐได้มีการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและเอกสารราชการกันทางเครือข่ายคอมพิวเตอร์ เชื่อมโยงข้อมูล ระหว่างหน่วยงานภาครัฐเข้าด้วยกัน โครงการนี้ได้มีการวางมาตรฐานระดับความปลอดภัยของการเข้าถึงข้อมูล ตลอดจนการส่งผ่านข้อมูลที่มีความไวต่อความเสียหายกับระบบราชการ และ/หรือ ความมั่นคงของประเทศ โดยกำหนดให้ใช้บัตรอัจฉริยะควบคู่ไปกับข้อมูลตัววัดทางชีวภาพ จึงเป็นทางเลือกหนึ่งของมาตรการการรักษาความปลอดภัยของข้อมูล มาตรการนี้สร้างความมั่นใจใน ความเป็นตัวจริง (Authentication) ของเอกสาร ที่ส่งโดยผู้มีอำนาจ (Authorized personnel) ในเอกสารที่ผ่านมาทางเครือข่ายอินเทอร์เน็ต และการควบคุมการเข้าถึง (Accessibility) เอกสารที่ต้องการความปลอดภัยค่อนข้างสูง ก็สามารถใช้มาตรการนี้ในการแสดงความเป็นตัวจริง (Identity) ของผู้ที่ต้องการเข้าถึงเอกสาร ว่าเป็นผู้มีสิทธิในการเข้าดูหรือ ทำการแก้ไข

จากพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พุทธศักราช 2540 ดังแสดงในหน้า 331 – 333 เป็นกฎหมายไทยฉบับแรกๆ ที่มีการกล่าวถึงการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลตามพระราชบัญญัติฉบับนี้ ข้อมูลข่าวสารส่วนบุคคลซึ่งเก็บรักษาไว้โดยหน่วยราชการถือเป็นส่วนหนึ่งของข้อมูลข่าวสารของราชการ ซึ่งหน่วยงานราชการมิได้เป็นเจ้าของโดยตรง การเปิดเผยดังกล่าวเป็นจุดเริ่มต้น ซึ่งมีหลักการที่ดี แต่ยังขาดความชัดเจนในทางปฏิบัติ ถ้ามีการใช้เทคโนโลยีไบโอเมตริกซ์อย่างกว้างขวางมากขึ้น ก็ต้องมีการปรับปรุงแก้ไขพระราชบัญญัติเพื่อคุ้มครองข้อมูลข่าวสารส่วนบุคคล ในด้าน

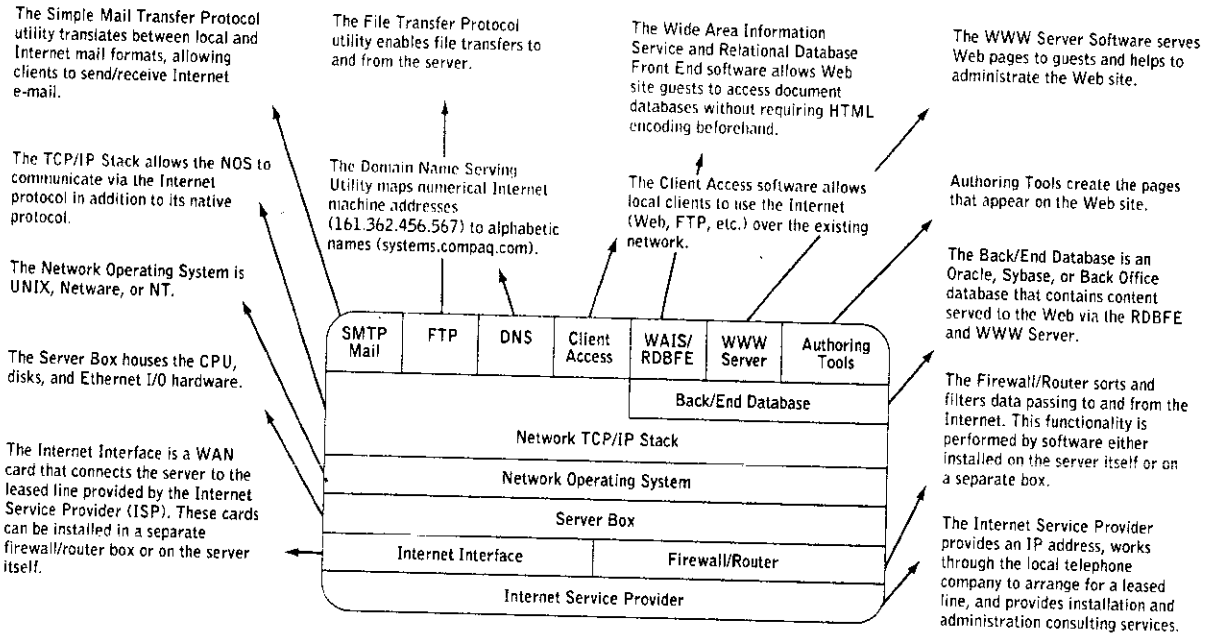
1. ความรับผิดชอบ (Accountability) มีผู้ที่ดูแลการดำเนินการขององค์กรในส่วนที่เกี่ยวกับข้อมูลข่าวสารส่วนบุคคล

2. ความเปิดเผย (Openness) ให้สาธารณชนรับทราบเกี่ยวกับการมีฐานข้อมูลข่าวสารส่วนบุคคลไว้ในครอบครอง ประกาศนโยบายที่เกี่ยวข้องกับการจัดการข้อมูล

3. วัตถุประสงค์ (Purposes) ของการเก็บข้อมูลข่าวสารส่วนบุคคล

4. การยินยอม (Consent) เจ้าของข้อมูลต้องรับรู้ และให้การยินยอมในการจัดเก็บ ใช้หรือเปิดเผยข้อมูล

5. ข้อจำกัดในการจัดเก็บ (Collection limitation) เก็บข้อมูลข่าวสารส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์ (ไม่เก็บเกินกว่าที่จำเป็น)



รูปที่ จ.3 องค์ประกอบของเครื่องให้บริการอินเทอร์เน็ต

ที่มา : Compaq Computer Corporation

2. การคุกคามต่อระบบเครือข่าย

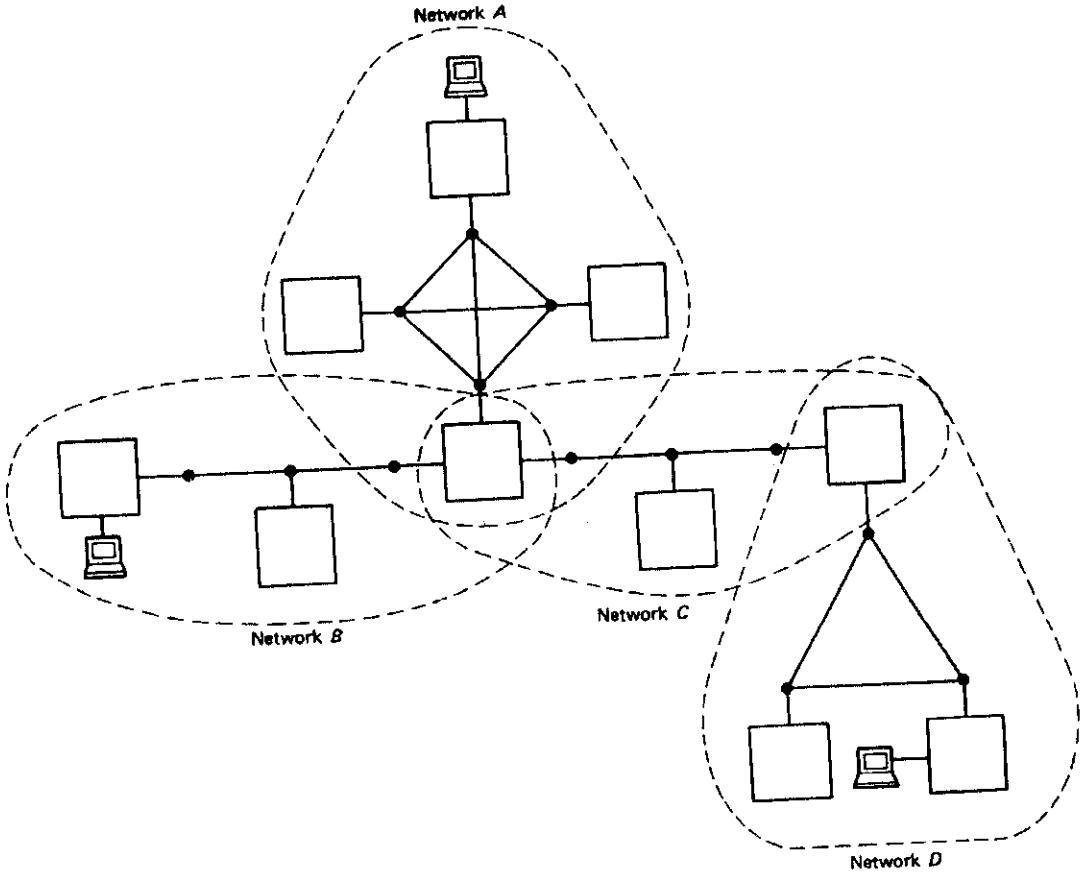
2.1 ประเด็นพิจารณาเกี่ยวกับความมั่นคงในระบบเครือข่าย

ระบบเครือข่ายเผชิญกับปัญหาความมั่นคง ความปลอดภัยมากขึ้น เพราะ

1. การใช้งานร่วม ระบบเครือข่ายเป็นการใช้ทรัพยากร และภาระงานร่วมกัน จากผู้ใช้จำนวนมาก

2. ความซับซ้อนของระบบ ระบบปฏิบัติการที่ใช้ในระบบเครือข่ายมีความซับซ้อนมากกว่าระบบปฏิบัติการในเครื่องเดี่ยว

3. ไม่มีกรอบที่แน่นอน การขยายของเครือข่ายทำให้ขอบเขตของเครือข่ายไม่แน่นอน เครื่องแม่ข่าย 1 เครื่อง อาจเป็นจุดต่อ (Node) บน 2 เครือข่ายที่ต่างกัน ดังนั้น ทรัพยากรของเครือข่ายหนึ่งอาจถูกเข้าถึงโดยผู้ใช้จากอีกเครือข่ายหนึ่ง ดังรูป จ.4



รูป จ.4 ขอบเขตเครือข่ายที่ไม่แน่นอน

4. มีจุดที่ถูกคุกคามได้มากมาย ความไม่มีขอบเขตที่แน่นอนของเครือข่าย เครื่องแม่ข่ายไม่ได้ถูกเข้าถึงเฉพาะจากลูกข่ายในเครือข่ายเดียว ผู้บริหารเครือข่ายไม่สามารถกำหนดการควบคุมไปถึงเครือข่ายอื่นๆ ได้

5. การคุกคามไม่ได้เกิดขึ้น ณ ตำแหน่งใดตำแหน่งหนึ่ง แต่สามารถจะถูกคุกคามจากที่ใดๆ ก็ได้

6. ผู้ใช้เครือข่ายไม่ทราบ และไม่สามารถควบคุมเส้นทางการติดต่อสื่อสารที่เกิดขึ้นได้

2.2 การวิเคราะห์การคุกคามต่อความมั่นคง

ในเครือข่ายนั้น

(1) จุดต่อเฉพาะที่ (Local nodes) เชื่อมต่อผ่าน

(2) สายสื่อสารเฉพาะที่ (Local communications links) ไปยัง

(3) เครือข่ายเฉพาะที่ (Local area network, LAN) ซึ่งมี

(4) ส่วนเก็บข้อมูลเฉพาะที่ (Local data storage),

(5) การประมวลผลเฉพาะที่ (Local processes) และ

(6) อุปกรณ์เฉพาะที่ต่างๆ (Local devices) เครือข่ายเฉพาะที่นี้จะเชื่อมต่อไปยัง

(7) เกตเวย์เครือข่าย (Network gateway) ซึ่งให้การเข้าถึงผ่าน

(8) สายสื่อสารเครือข่าย (Network communications links) ไปยัง

(9) ทรัพยากรควบคุมเครือข่าย (Network control resources)

(10) ตัวจัดเส้นทางเครือข่าย (Network routers) และ

(11) ทรัพยากรเครือข่าย (network resources) เช่น ฐานข้อมูล

การคุกคามต่างๆ ที่เกิดขึ้น คือ

- การขวาง ยึด ข้อมูลในระหว่างเส้นทาง
- การเข้าถึงโปรแกรม หรือข้อมูลที่เครื่องแม่ข่ายระยะไกล
- การปรับเปลี่ยนโปรแกรม หรือข้อมูลที่เครื่องแม่ข่ายระยะไกล
- การปรับเปลี่ยนข้อมูลในระหว่างเส้นทาง
- การปิดกั้นเส้นทางที่ข้อมูลเดินทาง
- การปิดกั้นเส้นทางทุกเส้นทาง

3. การควบคุมความมั่นคงของเครือข่าย

เครื่องมือที่มีประสิทธิภาพที่ช่วยควบคุมความมั่นคง และปลอดภัยของเครือข่าย ได้แก่

3.1 **การเข้ารหัสลับ** (Encryption)

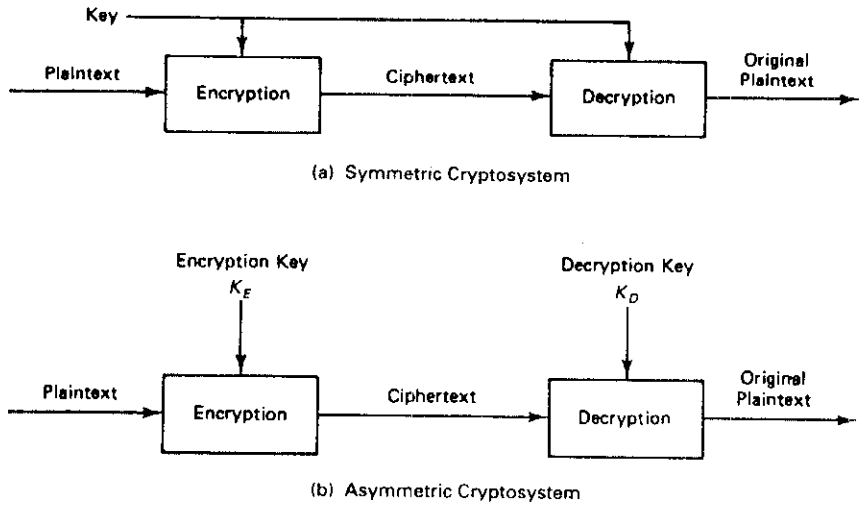
เป็นกระบวนการเข้ารหัสข้อความเพื่อไม่ให้ข้อความดังกล่าวเป็นที่เปิดเผย ส่วนการถอดรหัสลับ (Decryption) เป็นกระบวนการย้อนกลับ เปลี่ยนจากข้อความเข้ารหัสกลับไปเป็นรูปแบบปกติ (โดยมากมักจะใช้คำศัพท์ Encode Decode Encipher และ Decipher แทนคำว่า Encrypt และ Decrypt)

รูปแบบเดิมของข้อความเรียกว่า Plaintext ส่วนรูปแบบของข้อมูลที่เข้ารหัสลับแล้วเรียก Ciphertext ดังรูป จ.5

รูป จ.5 การเข้ารหัสลับ

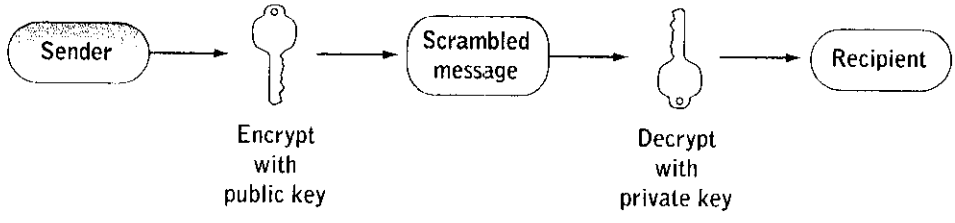
3.1.1 อัลกอริทึมการเข้ารหัสลับ (Encryption Algorithms)

อัลกอริทึมการเข้ารหัสลับรูปแบบหนึ่งคือ การใช้กุญแจ (Key, K) ดังนั้น ข้อความที่เข้ารหัสลับแล้ว จะขึ้นกับข้อความเดิม และค่า K ถ้ากุญแจในการเข้ารหัส และถอดรหัสเหมือนกัน จะเรียกว่า เป็นการเข้ารหัสลับสมมาตร (Symmetric encryption) ดังรูป จ.6 (a) แต่ถ้ากุญแจการเข้ารหัสมาเป็นคู่กับกุญแจการถอดรหัส จะเรียกว่าเป็น การเข้ารหัสลับอสมมาตร (Asymmetric encryption) ดังรูป จ.6 (b)



รูป จ.6 การเข้ารหัสลับโดยใช้กุญแจเข้ารหัส

การเข้ารหัสที่เป็นที่นิยมเรียก 'Public key' encryption หรือการเข้ารหัสโดยใช้กุญแจสาธารณะ ดังแสดงในรูป จ.7



รูป จ.7 Public key encryption

การเข้ารหัสโดยใช้กุญแจสาธารณะ จะใช้กลุ่มของกุญแจสาธารณะ (Public key) และกุญแจส่วนตัว (Private key) ทำการเข้ารหัสข้อมูล ก่อนจะส่ง แล้วจึงถอดรหัสเมื่อข้อมูลไปถึงผู้รับ ผู้ส่งข้อมูลจะระบุกุญแจสาธารณะของผู้รับในสารบบ (Directory) และใช้กุญแจสาธารณะนั้นนำข้อมูลเข้ารหัส ข้อมูลถูกส่งในลักษณะที่เข้ารหัสแล้วเข้าสู่เครือข่าย เมื่อข้อมูลเข้ารหัสมา

ถึงผู้รับ ผู้รับจะใช้กุญแจส่วนตัวเพื่อถอดรหัสข้อมูลแล้วอ่านข้อความนั้นๆ

การเข้ารหัสเป็นประโยชน์อย่างมากในการช่วยปกป้องข้อมูลต่างๆ ในเครือข่ายอินเทอร์-เน็ต และเครือข่ายสาธารณะอื่นๆ เพราะเครือข่ายทั้ง 2 รูปแบบมีความปลอดภัยน้อยกว่าเครือข่ายส่วนตัว การเข้ารหัสช่วยป้องกันการส่งผ่านข้อมูลการชำระเงิน เช่น ข้อมูลบัตรเครดิต เป็นต้น

ข้อความเดียวกันถ้าเปลี่ยนกุญแจเข้ารหัส ก็จะได้การเข้ารหัสลับที่แตกต่างกันออกไป การวิจัยเพื่อศึกษาการเข้ารหัสลับ และการถอดรหัสลับ เรียกว่า Cryptology

รูปแบบหลักในการเข้ารหัสลับ ได้แก่ การแทนค่า (Substitutions) คือ ตัวอักษรแต่ละตัวถูกเปลี่ยนแปลงไปเป็นตัวอักษรอื่น และ การสลับตำแหน่ง (Transpositions) คือ เปลี่ยนแปลงลำดับของตัวอักษร

3.1.2 การถอดรหัสลับ

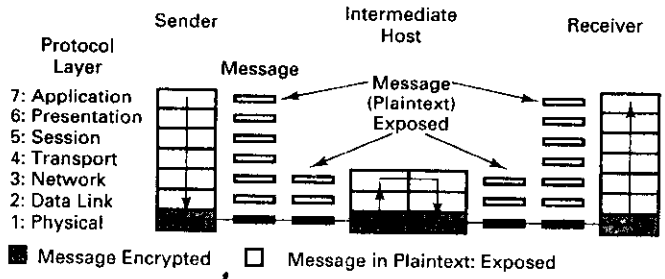
หมายถึงการทำลายการเข้ารหัสลับ เป็นการพยายามหาความหมายของข้อความที่เข้ารหัสลับ หรือ พยายามหาอัลกอริทึมการถอดรหัสที่เข้าคู่กับอัลกอริทึมการเข้ารหัสโดยมีรูปแบบที่แตก-ต่างกัน คือ

- พยายามทำลายข้อความเดี่ยว
- พยายามหารูปแบบของข้อความที่เข้ารหัสลับ เพื่อที่จะสามารถถอดรหัสข้อความต่อๆ ไปโดยใช้อัลกอริทึมการถอดรหัส
- พยายามหาจุดอ่อนในอัลกอริทึมเข้ารหัสลับ

3.1.3 การเข้ารหัสลับสำหรับเครือข่าย

สำหรับระบบเครือข่ายนั้น การเข้ารหัสลับอาจดำเนินการระหว่างแม่ข่ายของเครือข่ายหรือระหว่างงานประยุกต์ และยังต้องคำนึงถึงกุญแจที่ใช้งานด้วย เพราะกุญแจเข้ารหัสจะต้องส่งให้กับทั้งผู้ส่งและผู้รับอย่างปลอดภัย

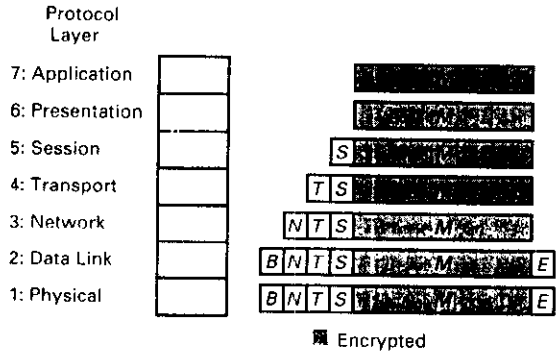
รูปแบบการเข้ารหัสสำหรับเครือข่าย ได้แก่ Link encryption โดยข้อมูลจะถูกเข้ารหัสก่อนที่ระบบจะถูกเชื่อมต่อทางกายภาพ การเข้ารหัสนี้จะเกิดขึ้นในขั้นที่ 1 หรือขั้นที่ 2 ใน OSI model ส่วนการถอดรหัสเกิดขึ้นเมื่อการสื่อสารผ่านไปที่คอมพิวเตอร์เครื่องรับ ดังรูป ข.8



รูป จ.8 Link encryption

การเข้ารหัสนี้ช่วยป้องกันข้อมูลในระหว่างการส่งผ่านระหว่างเครื่องคอมพิวเตอร์ 2 เครื่อง แต่ข้อความจะอยู่ในรูปแบบปกติในขณะที่อยู่ที่แม่ข่าย

อีกรูปแบบของการเข้ารหัสสำหรับเครือข่าย คือ End-to-End Encryption เป็นการรักษาความปลอดภัยจากด้านหนึ่งของการส่งผ่านข้อมูลไปจนถึงอีกด้านหนึ่งซึ่งรับข้อมูล การเข้ารหัสนี้สามารถดำเนินการโดยฮาร์ดแวร์ ระหว่างผู้ใช้และแม่ข่าย หรือ ดำเนินการโดยซอฟต์แวร์ที่ทำงานอยู่บนเครื่องแม่ข่าย ซึ่งไม่ว่าในกรณีใดก็ตามการเข้ารหัสจะเกิดในระดับสูงสุดของ OSI model ดังรูป จ.9



รูป จ.9 End-to-End Encryption

เนื่องจากการเข้ารหัสเกิดขึ้นก่อนหน้าการกำหนดเส้นทาง และการส่งผ่านข้อมูล ดังนั้นข้อมูลข้อความจะถูกส่งผ่านในรูปที่ถูกเข้ารหัสแล้วตลอดเครือข่าย รูปแบบนี้จึงครอบคลุมในกรณีที่ถ้าระดับล่างของOSI Model เกิดความผิดพลาด และข้อมูลถูกเปิดเผย แต่ยังจะรักษาความปลอดภัยของข้อมูลได้

CT 489

3.2 **การควบคุมการเข้าถึง** (Access control)

การเข้ารหัสจะถูกใช้เพื่อป้องกันข้อมูลภายในเครือข่าย อย่างไรก็ตาม ยังต้องคำนึงถึงการเข้าถึงข้อมูล โปรแกรม และทรัพยากรอื่นๆ ของเครือข่าย ในระบบเครือข่าย ผู้ใช้ หรือ แม้แต่ผู้บริหารเครือข่ายอาจไม่ทราบว่ามีผู้ใช้ใดบ้างที่เชื่อมต่ออยู่ในเครือข่ายเดียวกัน ดังนั้นในสภาพแวดล้อมของเครือข่าย การควบคุมการเข้าถึง จะต้องป้องกันระบบของเครือข่ายและป้องกันผู้ใช้ที่ไม่ได้รับอนุญาตผ่านจากระบบหนึ่งของเครือข่าย เพื่อเข้าถึงระบบอื่นๆ ของเครือข่าย

3.2.1 การป้องกันช่องทาง (Port protection)

โดยปกติแล้ว ในระบบคอมพิวเตอร์เดี่ยวนั้น การระบุตัวผู้ใช้ก็เป็นสิ่งที่ทำได้ยาก แต่เมื่อผู้ใช้สามารถต่อเข้าระบบโดยการโทรศัพท์นั้น ยิ่งทำให้การระบุตัวผู้ใช้ยากขึ้นอีกมาก การเข้าถึงช่องทางโดยการต่อโทรศัพท์ จึงเป็นจุดที่ไม่มั่นคงจุดใหญ่ของระบบเครือข่าย จึงจำเป็นต้องมีการป้องกันช่องทาง และใช้เทคนิคนี้ร่วมกับเทคนิคฮาร์ดแวร์ และเทคนิคการบริหารหลายรูปแบบ

1. การเรียกกลับอัตโนมัติ (Automatic call-back) ในระบบเรียกกลับอัตโนมัติ เมื่อผู้ใช้ที่ได้รับอนุญาตต่อโทรศัพท์เข้าสู่ระบบคอมพิวเตอร์ หลังจากที่ระบุตัวผู้ใช้เองแล้ว ระบบคอมพิวเตอร์ จะตรวจสอบหมายเลขโทรศัพท์จากรายการเลขหมายที่มีอยู่ แล้วเรียกกลับไปตามหมายเลขที่ระบุไว้ ซึ่งถ้าผู้ใช้มีหลายเครื่องในหลายสถานที่ จะต้องแจ้งหมายเลขทั้งหมดไว้กับระบบ เมื่อต้องการต่อเข้าระบบจากเครื่องใด ก็แจ้งหมายเลขนั้นไป ถ้าระบบตรวจสอบหมายเลขแล้วไม่ตรงกับในรายการที่ระบุไว้ ระบบจะเตือนไปที่เจ้าหน้าที่รักษาความปลอดภัยของระบบ

2. สร้างสิทธิการเข้าถึงที่แตกต่างกัน (Differentiated access rights) ข้อมูลที่สำคัญสามารถได้รับการปกป้องโดยจำกัดตำแหน่งในการเข้าถึง โดยการเข้าถึงข้อมูลสำคัญจะต้องเข้าถึงจากสถานที่ที่ปลอดภัยเท่านั้น เช่น พนักงานขายสามารถโทรศัพท์และป้อนข้อมูลการขายเข้าสำนักงาน แต่ข้อมูลสำคัญ เช่น การพยากรณ์ยอดขาย หรือ โครงสร้างราคา ข้อมูลเหล่านี้จะเข้าถึงได้จากเฉพาะภายในสำนักงานเท่านั้น

3.3 **การระบุตัวตน** (Authentication)

หมายถึงความสามารถของแต่ละฝ่ายที่ทำธุรกรรมต่อกัน สามารถระบุอัตลักษณ์ (Identity) ของอีกฝ่ายหนึ่งได้ ธุรกรรมที่เกิดขึ้นในสมัยก่อนจะใช้ลายเซ็นเพื่อระบุตัวตน แต่ธุรกรรมปัจจุบันหลีกเลี่ยงการใช้ลายเซ็น เช่น ธนาคารอิเล็กโทรนิกส์ จะใช้เครือข่ายส่วนตัวที่มีการปกป้องเป็นอย่างดี สามารถบันทึกและพิสูจน์การจ่ายเงินของผู้จ่ายได้

CT 489 ยกที่ 44

พระราชบัญญัติ

ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540

.....

หมวด ๓

ข้อมูลข่าวสารส่วนบุคคล

มาตรา ๒๑ เพื่อประโยชน์แห่งหมวดนี้ "บุคคล" หมายความว่า บุคคลธรรมดาที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทย แต่มีถิ่นที่อยู่ในประเทศไทย

มาตรา ๒๒ สำนักข่าวกรองแห่งชาติ สำนักงานสภาความมั่นคงแห่งชาติ และหน่วยงานของรัฐแห่งอื่นตามที่กำหนดในกฎกระทรวงอาจออกระเบียบ โดยความเห็นชอบของคณะกรรมการกำหนดหลักเกณฑ์ วิธีการและเงื่อนไขที่มิให้นำบทบัญญัติวรรคหนึ่ง (๓) ของมาตรา ๒๓ มาใช้บังคับกับข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของหน่วยงานดังกล่าวก็ได้

หน่วยงานของรัฐแห่งอื่นที่จะกำหนดในกฎกระทรวงตามวรรคหนึ่งนั้น ต้องเป็นหน่วยงานของรัฐซึ่งการเปิดเผยประเภทข้อมูล ข่าวสารส่วนบุคคลตามมาตรา ๒๓ วรรคหนึ่ง (๓) จะเป็นอุปสรรคร้ายแรงต่อการดำเนินการของหน่วยงานดังกล่าว

มาตรา ๒๓ หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลดังต่อไปนี้

(๑) ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็นเพื่อการดำเนินงาน ของหน่วยงานของรัฐให้สำเร็จ ตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น

(๒) พยายามเก็บข้อมูลข่าวสาร โดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของ บุคคลนั้น

(๓) จัดให้มีการพิมพ์ในราชกิจจานุเบกษาและตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้

(ก) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

(ข) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

(ค) ลักษณะการใช้ข้อมูลตามปกติ

(ง) วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล

(จ) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล

(ฉ) แหล่งที่มาของข้อมูล

(๔) ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ

(๕) จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคลตามความเหมาะสมเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

ในกรณีที่เก็บข้อมูลข่าวสาร โดยตรงจากเจ้าของข้อมูลหน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูลถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ ลักษณะการใช้ข้อมูลตามปกติ และกรณี

ที่ขอข้อมูลนั้นเป็นกรณีที่อาจให้ข้อมูลได้โดยความสมัครใจ หรือเป็นกรณีมีกฎหมายบังคับ

หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคล ทั่วไปทราบ ข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติ

มาตรา ๒๔ หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่น หรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผย ดังต่อไปนี้

(๑) ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตนเพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

(๒) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

(๓) ต่อหน่วยงานของรัฐที่ทำงานด้านการวางแผนหรือการสถิติหรือสำมะโนต่างๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคล ไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

(๔) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัยโดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

(๕) ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา ๒๖ วรรคหนึ่ง เพื่อการตรวจดูคุณค่าใน การเก็บรักษา

(๖) ต่อเจ้าหน้าที่ของรัฐเพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็น คดีประเภทใดก็ตาม

(๗) เป็นการให้ซึ่งจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(๘) ต่อศาลและเจ้าหน้าที่ของรัฐหนือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

(๙) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

การเปิดเผยข้อมูลข่าวสารส่วนบุคคลตามวรรคหนึ่ง (๓) (๔) (๕) (๖) (๗) (๘) และ (๙) ให้มีการจัดทำบัญชีแสดงการเปิดเผยกำกับไว้ กับข้อมูลข่าวสารนั้นตามหลักเกณฑ์และวิธีการที่กำหนดในกฎกระทรวง

มาตรา ๒๕ ภายใต้บังคับมาตรา ๑๔ และมาตรา ๑๕ บุคคลย่อมมีสิทธิที่จะได้รู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้น หรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น และให้นำมาตรา ๙ วรรคสอง และวรรคสาม มาใช้บังคับ โดยอนุโลม การเปิดเผยรายงานการแพทย์ที่เกี่ยวกับบุคคลใด ถ้ากรณีมีเหตุอันควรเจ้าหน้าที่ของรัฐจะเปิดเผยต่อเฉพาะแพทย์ที่บุคคลนั้น มอบหมายก็ได้ ถ้าบุคคลใดเห็นว่าข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้องตามที่เป็นจริง ให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนนั้นได้ ซึ่งหน่วยงานของรัฐจะต้องพิจารณาคำขอดังกล่าว และแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า ในกรณีที่หน่วยงาน

ของรัฐไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารให้ตรงตามที่มีคำขอให้ผู้นั้นมีสิทธิอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายในสามสิบวัน นับแต่วันได้รับแจ้งคำสั่งไม่ยินยอมแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสาร โดยยื่นคำอุทธรณ์ ต่อคณะกรรมการและไม่ว่ากรณีใดๆ ให้เจ้าของข้อมูลมีสิทธิร้องขอให้หน่วยงานของรัฐหมายเหตุคำขอของตนแนบไว้กับข้อมูลข่าวสารส่วนที่เกี่ยวข้องได้

ให้บุคคลตามที่กำหนดในกฎกระทรวงมีสิทธิดำเนินการตามมาตรา ๒๓ มาตรา ๒๔ และมาตรานี้แทนผู้เยาว์ คนไร้ความสามารถ คนเสมือนไร้ความสามารถหรือเจ้าของข้อมูลที่ถึงแก่กรรมแล้วได้

6. ข้อจำกัดการใช้งาน การเปิดเผย และการเก็บไว้ในครอบครอง (Use, Disclosure, Retention Limitation) ไม่ใช้ข้อมูลเกินวัตถุประสงค์ที่แจ้งไว้ในตอนแรกตามความยินยอมของเจ้าของข้อมูล และไม่เก็บรักษาข้อมูลไว้นานเกินความจำเป็น

7. การรักษาความปลอดภัย (Safeguards) มีการรักษาความปลอดภัยที่เหมาะสมกับความเสี่ยงต่อการสูญเสีย การเข้าถึง การทำลาย การใช้ การแก้ไขดัดแปลง หรือ เปิดเผยข้อมูลโดยมิชอบ ต้องมีสถานที่ บุคลากร งบประมาณ พอเพียงต่อการประกันความปลอดภัย

8. คุณภาพของข้อมูล (Data quality) ข้อมูลส่วนบุคคลต้องมีความถูกต้อง ครบถ้วน และทันสมัย กับการใช้งานตามวัตถุประสงค์

9. การมีส่วนร่วมของเจ้าของข้อมูล (Individual participation) เจ้าของข้อมูลมีสิทธิเรียกดูรายละเอียดการใช้งาน หรือการเปิดเผยข้อมูลของตน สามารถตรวจสอบความถูกต้องและความสมบูรณ์ของข้อมูล รวมทั้งขอแก้ไขได้ตามความเหมาะสม

CT 489 333