(Sepcial Article)

Identification With Biometrics Technology And The Risk of Privacy Violations

Supon Phrommaphan

Department of Business Computer, School of Information Technology, Sripatum University.

Correspondences to : supon.ph@spu.ac.th

Nowadays, Internet security technology has helped ease the human workload and greatly propel the national economic system, because the crime problems occurring on a daily basis are numerous and varied. Humans have tried to invent high technology to protect the security of property and important information, both personal and organization, to be most stable and technology that can answer this problem well is Biometric Technology. Which is considered as the most accepted security innovation at this time, but there may be a risk of privacy violations as well. If public or private organizations are using biometrics technology to store too many sensitive data such as fingerprints, Pictures, face recognition, signature, retina, iris, DNA (etc.). Biometrics Technology means the concept of adopting medical biotechnology and computer technology integrated In order to specify or specify personal characteristics, both physical and behavior, such as fingerprints, Pictures, palms, iris, face, voice, DNA signature, etc. to use in many

activities, such as Identification card, Passport preparation, Mobile phone SIM registration etc.

Keywords : Biometrics Technology, Internet security, Privacy violations, Computer Crime.

Royal Thai Air Force Medical Gazette, Vol. 66 No. 1 January - April 2020

(บทความพิเศษ)

การพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมาตรกับความเสี่ยงในการละเมิดสิทธิส่วนบุคคล

สุพล พรหมมาพันธุ์

สาขาวิชาคอมพิวเตอร์ธุรกิจ, คณะเทคโนโลยีสารสนเทศ, มหาวิทยาลัยศรีปทุม

ปัจจุบันเทคโนโลยีรักษาความมั่นคงปลอดภัยทางอินเทอร์เน็ต ได้ช่วยแบ่งเบาภาระงานของมนุษย์ และช่วยขับเคลื่อน ระบบเศรษฐกิจของประเทศชาติได้เป็นอย่างมาก เนื่องด้วยปัญหาอาชญากรรมที่เกิดขึ้นในแต่ละวันมีมากมายหลากหลายรูปแบบ มนุษย์จึงได้พยายามคิดค้นเทคโนโลยีชั้นสูง เพื่อปกป้องรักษาความปลอดภัยของทรัพย์สิน และข้อมูล

สำคัญทั้งส่วนบุคคล และองค์กรไว้ให้มั่นคงที่สุด และเทคโนโลยีที่สามารถตอบโจทย์นี้ได้อย่างดี คือเทคโนโลยีชีวมาตร (Biometrics Technology) ซึ่งนับว่าเป็นสุดยอดนวัตกรรมการรักษาความปลอดภัยที่ได้รับการยอมรับมากที่สุดในเวลานี้ แต่อาจมีความเสี่ยงต่อการ ละเมิดสิทธิส่วนบุคคลได้เช่นกัน หากองค์กรภาครัฐหรือเอกชนมีการใช้เทคโนโลยีชีวมาตร จัดเก็บข้อมูลที่ละเอียดอ่อนหลายชนิด มากเกินไป เช่น ลายพิมพ์นิ้วมือ ภาพ่าย การจดจำใบหน้า ลายเซ็น เรตินา ม่านตา ดีเอ็น (DNA) เป็นต้น เทคโนโลยีชีวมาตร (Biometrics Technology) หมายถึง แนวคิดการนำเอาเทคโนโลยีด้านชีวภาพทางการแพทย์ และเทคโนโลยีด้านคอมพิวเตอร์มา บูรณาการเข้าด้วยกัน เพื่อใช้กำหนดหรือระบุคุณลักษณะเฉพาะส่วนบุคคลทั้งด้านกายภาพ และพฤติกรรม ได้แก่ ลายพิมพ์นิ้วมือ ภาพถ่าย ฝ่ามือ ม่านตา ใบหน้า เสียงพูด ลายเซ็น ดีเอ็นเอ เป็นต้น เพื่อใช้ประโยชน์ในกิจกรรมหลายอย่าง เช่น การทำบัตรประจำตัวประชาชน การจัดทำหนังสือเดินทาง การลงทะเบียนซิมโทรศัพท์มือถือ เป็นต้น

คำสำคัญ : เทคโนโลยีชีวมาตร, ความมั่นคงปลอดภัยทางอินเทอร์เน็ต, การละเมิดสิทธิส่วนบุคคล, อาชญากรรมคอม

เทคโนโลยีชีวมาตร หรือชีวมิติ คืออะไร

เทคโนโลยีชีวมาตร (Biometrics Technology) คือ แนวคิดการนำเอาเทคโนโลยีด้านชีวภาพทางการแพทย์ และเทคโนโลยีด้านคอมพิวเตอร์มาบูรณาการเข้าด้วยกัน เพื่อใช้กำหนดหรือระบุคุณลักษณะเฉพาะส่วนบุคคลทั้งด้าน กายภาพและพฤติกรรม ได้แก่ ลายพิมพ์นิ้วมือ ภาพถ่าย ฝ่ามือ ม่านตา ใบหน้า เสียงพูด ลายเซ็น ดีเอ็นเอ เป็นต้น นายแพทย์สุธี ทุวิรัตน์[1] กรรมการสมาคมความมั่นคง ปลอดภัยระบบสารสนเทศ กล่าวถึงความหมายของ “ชีวมาตร” ในมติชนออนไลน์ เรื่อง เทคโนโลยีระบุตัวตน “ชีวมาตร” น่ากลัวหรือไม่ วันที่ 21 กันยายน พ.ศ. 2562 โดยกล่าวเอาไว้ว่า ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่เพิ่ง ประกาศใช้เมื่อเร็ว ๆ นี้ว่า “ชีวมาตร” หรือไบโอเมทริกซ์ คือข้อมูลส่วนบุคคลที่เป็นเทคโนโลยีในการระบุตัวตน ได้แก่ 1. ภาพถ่าย 2. ลายนิ้วมือ และ 3. ม่านตา ซึ่ง “หน้าตา” เปลี่ยนได้ แต่ช้า เป็นเหตุผลให้ต้องทำบัตรประชาชนใหม่ทุก 5 ปี ทว่า “ลายนิ้วมือ” คือเซลล์ที่ตายของผิวหนังจึงไม่เปลี่ยน แปลง ส่วน “ม่านตา” เป็นอวัยวะที่ไม่ได้บอกแค่เพียงลักษณะ แต่ยังบอกถึงสุขภาพ พฤติกรรม และโรคทางพันธุกรรมได้ หลายโรคอีกด้วย

เทคโนโลยีชีวมาตร (Biometrics Technology) สามารถแบ่งออกเป็น 2 ประเภทใหญ่ คือ (1) การใช้ ลักษณะทางกายภาพ (Physiological Biometrics) ได้แก่ ลายนิ้วมือ (Fingerprint), ลักษณะใบหน้า (Facial Recognition), ลักษณะของมือ (Hand Geometry), ลักษณะ ของนิ้วมือ (Finger Geometry), ลักษณะใบหู (Ear Shape),
ลักษณะของตา เช่น ม่านตา (Iris) และจอตา (Retina) ภายในดวงตา, กลิ่น (Human Scent) และการใช้ลักษณะ ทางพฤติกรรม (Behavioral Biometrics) ในการระบุ ตัวบุคคล ได้แก่ การพิมพ์ (Keystroke Dynamics), การเดิน (Gait Recognition), เสียง (Voice Recognition), การเซ็นชื่อ (Signature) กระบวนการในการตรวจสอบหรือระบุตัวบุคคลด้วยไบโอเมทริกซ์ไม่ว่าจะเป็นการใช้ลักษณะเฉพาะแบบใดก็ตามจะมีขั้นตอนเหมือนกันดังต่อไปนี้ (1) ผู้ใช้ระบบต้องทำ การให้ตัวอย่าง (Samples) ของลักษณะทางไบโอเมทริกซ์ ที่จะใช้หรือเป็นการลงทะเบียนเริ่มต้นก่อน ที่จะทำการใช้ระบบ
(2) ตัวอย่างทางไบโอเมทริกซ์ที่ถูกเก็บมาในขั้นตอนแรกจะถูก ทำการแปลงและจัดเก็บ ให้เป็นแม่แบบ (Template) ที่จะใช้ในการเปรียบเทียบ (3) เมื่อผู้ใช้ต้องการที่จะใช้ระบบ ก็จะถูกตรวจสอบหรือระบุผู้ใช้ โดยทำการเก็บตัวอย่างทาง ไบโอเมท

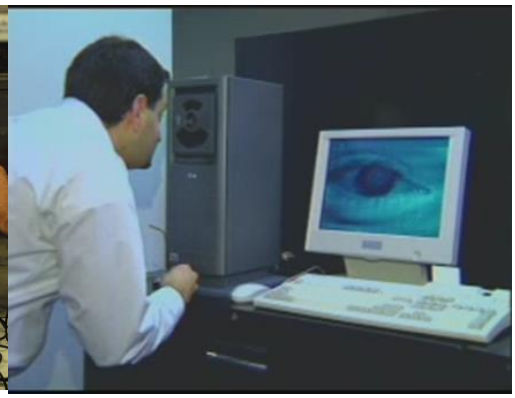
ริกซ์ของผู้ใช้และทำการเปรียบเทียบกับแม่แบบ (Template) ที่เก็บไว้ แล้วทำการตรวจสอบความเหมือนของ ตัวอย่างกับแม่แบบ จากนั้นก็จะทำการอนุญาตหรือปฏิเสธ การเข้ามาใช้งานระบบของผู้ใช้ เราเรียกขั้นตอนที่ 1 และ 2 ว่าเป็นขั้นตอนของการลงทะเบียน (Enrolment) ซึ่งจะเป็น การทำเพียงครั้งเดียว ก่อนการที่จะเริ่มใช้งาน ส่วนขั้นตอนที่ 3 เป็นกระบวนการตรวจสอบ (Authentication) หรือระบุ ตัวผู้ใช้ (Identification) ซึ่งผลของการตรวจสอบหรือระบุ ตัวผู้ใช้นี้มีผลออกมาได้ 4 กรณีดังนี้ 1. Correct Accept : อนุญาตให้ผู้ใช้ที่มีสิทธิใช้ระบบ เข้าใช้ระบบ, 2. Correct Reject : ปฏิเสธผู้ที่ไม่มีสิทธิใช้ระบบ, 3. False Accept : อนุญาตให้ผู้ที่ไม่มีสิทธิ เข้าใช้ระบบจำนวนของ False Accept ถ้าคำนวณออกมาเป็นเปอร์เซนต์ จะเรียกว่า อัตราการอนุญาต ผิดพลาด (False Accept Rate หรือ FAR) และ 4. False Reject : ปฏิเสธผู้ใช้ที่มีสิทธิใช้ระบบ ไม่ให้เข้าใช้ระบบ จำนวนของ False Reject ถ้าคำนวณออกมาเป็นเปอร์เซนต์ จะเรียกว่า อัตราการปฏิเสธผิดพลาด (False Reject Rate หรือ FRR) ระบบสแกนลายนิ้วมือปัจจุบันมีการใช้เช่นกับ เครื่องคอมพิวเตอร์แบบ Tablet ส่วนระบบสแกนฝ่ามือจะ ปลอมได้ยากกว่าการสแกนลายนิ้วมือ และระบบสแกนฝ่ามือ จะมีการตรวจอุณหภูมิ ตรวจระยะความยาวของนิ้วเป็นการ เช็คข้อมูลเพิ่มเติมมากขึ้น ส่วนระบบสแกนรูม่านตานั้น ปัจจุบันยังไม่ได้รับความนิยมเท่าไรนัก แต่ระบบที่ได้รับความ นิยมมากขึ้นคือระบบสแกนหน้า โดยใช้กล้องวีดีโอถ่ายภาพ หน้าคน (Face Recognition) ที่จะเดินผ่านประตูแล้วบันทึก รูปหน้าลงฐานข้อมูลคอมพิวเตอร์ ซึ่งได้แก่ข้อมูลระยะห่าง ระหว่างดวงตา ความลึกของเบ้าตา ความกว้าง ความยาว ของจมูก ลักษณะของโหนกแก้ม และ โครงหน้า รูปร่างของปาก กราม และคาง

สำหรับเทคโนโลยีการสแกนลายนิ้วมือที่นิยมใช้ ในปัจจุบัน ดร.ศรัณย์ สัมฤทธิ์เดชขจร[2] นักวิจัยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค) บอกว่า โดยทั่วไปแล้วอาจแบ่งได้ 3 ลักษณะได้แก่ เซ็นเซอร์ประจุไฟฟ้า (Capacitive Sensor) เซ็นเซอร์อุณภูมิ (Themal Sensor) และเซ็นเซอร์แสง (Optical Sensor) เทคโนโลยีสองแบบแรกผู้ใช้ต้องแตะไปที่เซ็นเซอร์โดยตรง ทำให้อายุการใช้งานสั้น และมีปัญหาเรื่องการบำรุงรักษา โดยในต่างประเทศที่มีอากาศหนาวจะเกิดไฟฟ้าสถิตย์ทำลายเซ็นเซอร์ได้ ขณะที่ระบบแสง จะทนกว่าและมีคุณสมบัติรวมของเทคโนโลยีอื่นมาไว้ด้วย หลักการทำงานของเซ็นเซอร์แสง คือการสะท้อนกลับหมด ของแสงด้วยการอาศัยแสงสีแดงส่องลายนิ้วมือที่วางอยู่บน เลนส์สะท้อนกลับ ตัวหัวเซ็นเซอร์เช่นเดียวกับการใช้นิ้วจับ แก้วที่มีน้ำอยู่ภายใน ซึ่งการสะท้อนของแสงทำให้เรามอง ลายนิ้วมือได้อย่างชัดเจน

ผลสรุปทางวิทยาศาสตร์กล่าวว่า มนุษย์ชาติจำนวน 600 ล้านคน เมื่อผ่านมาเป็นระยะเวลา 300 ปี จะมีโอกาส ที่ลายนิ้วมือซ้ำกันเพียง 1 คู่ ในส่วนของทารกเมื่ออยู่ในครรภ์ มารดาเป็นเวลา 7 เดือน ก็มีลายนิ้วมือเป็นของตัวเอง ครั้นเมื่อโตใหญ่ขึ้นเป็นผู้ใหญ่ลายนิ้วมือก็ไม่ได้เปลี่ยนแปลง เมื่อพบอุบัติเหตุกับลายนิ้วมือร่างกายก็จะซ่อมแซมส่วนที่ สึกหรอได้ ดังนั้น ธรรมชาติของลายนิ้วมือจึงเป็นเอกลักษณ์ ของแต่ละบุคคล ซึ่งเป็นที่ยอมรับของนานาชาติต่อความเป็น เอกลักษณ์ของลายนิ้วมือ

ลักษณะการทำงานของเทคโนโลยีชีวมาตร (Biometrics Technology) นั้น จะมีการแปลคุณลักษณะเฉพาะ ส่วนบุคคลผ่านเข้าไปทางอุปกรณ์นำเข้าข้อมูล (Input) และ แปลงเป็นรหัสดิจิทัล เพื่อทำการเปรียบเทียบกับรหัสดิจิทัล ที่ถูกจัดเก็บไว้ในคอมพิวเตอร์ ถ้ารหัสดิจิทัลในคอมพิวเตอร์นั้นไม่สัมพันธ์กับ (Match) รหัสคุณลักษณะส่วนบุคคล

คอมพิวเตอร์นั้นก็จะปฏิเสธการเข้าถึงข้อมูลนั้นทันที เทคโนโลยีชีวมาตรที่ได้รับความนิยมอย่างแพร่หลายในปัจจุบัน มีหลายประเภท ในหนังสือของการี่ บี เชลลี่[3] (Gary B. Shelly) ได้เขียนเอาไว้คือ เครื่องสแกนลายพิมพ์นิ้วมือ, ระบบเครื่อง จดจำใบหน้า, เครื่องพิมพ์ลายเส้นบนฝ่ามือ, ระบบการพิสูจน์ หรือจดจำเสียง, ระบบการตรวจพิสูจน์ลายเซ็น, ระบบการจดจำ ม่านตา, ระบบการพิสูจน์ดีเอ็นเอ (DNA) ซึ่งมีรายละเอียดดังนี้ คือ : (1) เครื่องสแกนลายพิมพ์นิ้วมือ (Fingerprint Scanner) ซึ่งราคาปัจจุบันประมาณ 100 ดอลล่าร์สหรัฐ โดย สามารถนำเอาเทคโนโลยีนี้ไปใช้ภายในบ้าน หรือในธุรกิจขนาด เล็ก บางบริษัทซื้อเครื่องคอมพิวเตอร์ชนิดที่มีเครื่องพิมพ์ ลายนิ้วมือติดกับแป้นพิมพ์มาด้วย เพื่อให้พนักงานพิมพ์ ลายนิ้วมือแทนการเข้าชื่อผู้ใช้ (User Name) และรหัสผ่าน (Password) ก่อนเข้าใช้งานคอมพิวเตอร์, โน้ตบุ๊คคอมพิวเตอร์ หรือแม้กระทั่งการเข้าสู่เว็บไซต์ ตามร้านขายของชำ และ ร้านขายปลีก ในปัจจุบันมีการนำเอาเครื่องสแกนลายพิมพ์ นิ้วมือเข้าไปใช้กันเป็นจำนวนมาก โดยเฉพาะเกี่ยวกับเรื่องการ ชำระเงิน ไม่ว่าลูกค้าจะอยู่ที่ไหน ลูกค้าสามารถผ่านการพิมพ์ ลายนิ้วมือลงบนเครื่องพิมพ์ลายนิ้วมือ เสร็จแล้วก็จะมีการ เชื่อมโยงไปในเรื่องทฤษฎีการเลือกชำระเงินว่าผู้ใช้เลือกใช้ รูปแบบไหน ซึ่งระบบจะมีการตรวจสอบบัญชีของลูกค้า รวมทั้ง สินเชื่อบัตรเครดิตของลูกค้าได้ด้วย



รูปภาพที่ 1 และรูปภาพที่ 2 เครื่องสแกนลายนิ้วมือตรวจสอบ การพิสูจน์ตัวตนของนักท่องเที่ยว การตรวจจับใบหน้า การสแกนลายพิมพ์นิ้วมือ และการสแกนม่านตา (Iris) เพื่อ การทำธุรกรรมด้านการเงิน เช่น บัตร ATM (Gary B. Shelly 2007:567)

(2) ระบบเครื่องจดจำใบหน้า (A Face Recognition Systems) โดยระบบจะดึงรูปภาพของใบหน้า และทำการเปรียบเทียบกับรูปภาพจริงของผู้ใช้ที่ถูกต้องตามกฎหมายระบบการจดจำใบหน้านี้ถูกพัฒนาขึ้นมาใช้เพื่อรักษาความปลอดภัยของผู้ที่เดินเข้าออกในห้องทำงาน, การดำเนินการกับ ผู้กระทำผิดทางกฎหมาย, การตรวจตรารักษาความปลอดภัย และใช้จดจำใบหน้าของบุคคลที่ผ่านเข้าออกตามสนามบิน เพื่อป้องกันความปลอดภัย เครื่องโน้ตบุ๊คคอมพิวเตอร์บางชนิดใช้เทคโนโลยีนี้เพื่อรักษาความปลอดภัยของคอมพิวเตอร์ เครื่องคอมพิวเตอร์จะไม่สามารถทำงานได้หากผู้ใช้คนนั้นไม่มีสิทธิ์โดยชอบด้วยกฎหมาย เทคโนโลยีนี้มีความชาญฉลาดมาก มันสามารถที่จะจดจำคนได้ทั้งคนที่สวมแว่นตา และไม่ได้สวม แว่นตา คนที่ไปทำศัลยกรรมตกแต่งใบหน้าหรือคนที่สวมใส่ เครื่องประดับ และแม้กระทั่งคนที่ปรับเปลี่ยนทรงผมใหม่ หรือ ใส่วิกผมปลอมก็ตาม (3) เครื่องพิมพ์ลายเส้นบนฝ่ามือ (A Hand Geometry) อุปกรณ์ชนิดนี้ จะทำการวัดสัณฐาน และขนาดของเส้นลายมือบนฝ่ามือของแต่ละบุคคล ซึ่งจะมี ลายเส้นที่แตกต่างกันไป ราคาของเครื่องสแกนพิมพ์

ลายฝ่ามือ นี้ ราคาประมาณ 1,000 ดอลล่าร์สหรัฐ บางองค์กรหรือบาง มหาวิทยาลัย ใช้อุปกรณ์ชนิดนี้เพื่อลงเวลาการเข้าทำงานของ พนักงาน ซึ่งเป็นเสมือนระบบการรักษาความปลอดภัยไปในตัว ใช้ตรวจสอบนักศึกษาที่เข้าไปใช้ห้องสันทนาการหรือแม้กระทั่ง ในสถานที่รับเลี้ยงเด็ก และโรงพยาบาลก็ใช้เทคโนโลยีนี้สำหรับ ตรวจสอบผู้ปกครองที่มารับเด็กและบุตรของตน (http://news.bbc.co.uk) (4) ระบบการพิสูจน์หรือจดจำเสียง (A Voice Verification System) ระบบนี้จะทำการเปรียบ เทียบเสียงพูดสดจริงกับรูปแบบของเสียงที่ถูกจัดเก็บเอาไว้ ว่าตรงกันหรือไม่ บางองค์กรใช้เทคโนโลยีนี้ลงเวลาการเข้า ทำงาน และมีอีกหลายบริษัทใช้เทคโนโลยีนี้ในการเข้าถึงแฟ้ม ข้อมูลและเครือข่ายคอมพิวเตอร์ที่เสี่ยงต่อความเสียหายได้ง่ายหรือแฟ้มข้อมูลที่เป็นความลับขององค์กร สถาบัน การเงินบางแห่งใช้เพื่อรักษาความปลอดภัยเกี่ยวกับการประมวลรายการทางธุรกิจของธนาคารผ่านโทรศัพท์ (Telephone Banking) (5) ระบบการตรวจพิสูจน์ลายเซ็น (A Signature Verification System) เทคโนโลยีนี้ใช้การจดจำรูปร่าง เส้นสายลายเซ็นซึ่งเซ็นโดยใช้ปากกาพิเศษหรือปากกาสำหรับ รับข้อมูลเข้าสู่คอมพิวเตอร์ (Tablet) โดยจะวัดจากแรงกด และอารมณ์ในการเซ็น (6) ระบบการจดจำม่านตา (Iris Recognition System) เป็นระบบรักษาความปลอดภัยที่มี ประสิทธิภาพสูงมาก โดยจะมีกล้องสำหรับถ่ายรูปม่านตาของคน และอ่านจดจำบันทึกเปรียบเทียบรูปแบบของม่านตา ที่ถูกจัดเก็บไว้ในคอมพิวเตอร์เช่นเดียวกับการพิมพ์ลายนิ้วมือ ระบบการจดจำม่านตามีราคาแพงมาก ส่วนใหญ่มักใช้ในการ รักษาความปลอดภัยในหน่วยงานของรัฐบาล ในกองทัพ รวมถึงสถาบันทางด้านการเงิน ในมลรัฐเท็กซัสมีการใช้ เทคโนโลยีนี้ในการทำบัตร ATM ให้กับลูกค้าและสามารถ เบิกถอนเงินสดได้อย่างรวดเร็ว (7) ระบบการพิสูจน์ดีเอ็นเอ (DNA) ในหน่วยงาน งานเทคนิคการแพทย์ โรงพยาบาล ค่ายบางระจัน (4) ได้อธิบายเกี่ยวกับดีเอ็นเอไว้ว่า DNA ย่อมา จาก Deoxyribonucleic Acid ซึ่งเป็นสารพันธุกรรม ซึ่งพบ อยู่ในนิวเคลียสของเซลล์ทุกเซลล์ในร่างกาย DNA ที่อยู่ใน นิวเคลียสจะได้รับถ่ายทอดครึ่งหนึ่งมาจากพ่อและอีกครึ่งหนึ่ง จากแม่ DNA จะไม่ซ้ำกันยกเว้นในกรณีแฝดที่มาจากไข่ และอสุจิตัวเดียวกันหรือที่เรียกว่าแฝดแท้นั่นเอง และพี่น้อง พ่อแม่เดียวกันก็จะไม่มี DNA ที่ไม่เหมือนกันด้วย เรานำ เอาความไม่เหมือนกันนี้เอามาใช้ประโยชน์ทางด้านนิติเวชได้ ซึ่งนิยมกันเอามาใช้ในการพิสูจน์ตัวบุคคลนั้นเอง ทีนี้เราจะ รู้ได้อย่างไรว่าใครเป็นใคร ประการแรกเราต้องเก็บตัวอย่าง DNA ของผู้ที่ต้องการจะพิสูจน์เสียก่อน ซึ่งสามารถเก็บตัวอย่าง ได้หลายชิ้นส่วน เช่น เลือด เนื้อเยื่อ, กระดูก, เส้นผม หรือ แม้แต่ฟัน จากนั้นเราก็เก็บตัวอย่าง DNA จากพ่อและแม่ มาทำการ Match ข้อมูลหรือการเทียบข้อมูลนั้นเอง ตรวจวิเคราะห์ DNA สิ่งสิ่งตรวจที่นิยมคือ เลือดครบ ส่วนเจาะใส่สารกันเลือดแข็ง (EDTA BLOOD) ส่วนของ DNA ที่นำมาทำการศึกษาวิเคราะห์ ได้แก่ (1) Chromosomal DNA หรือ Nuclear DNA (nDNA): เทคนิคการวิเคราะห์มีตั้งแต่การ วิเคราะห์ลายพิมพ์นิ้วมือของ nDNA และส่วน VNTRs ปัจจุบันนำเทคนิคการเพิ่มขยาย DNA ด้วย Polymerase Chainreaction ร่วมกับการวิเคราะห์ความหลากหลายอัลลีล ของ Dna ที่มีลำดับเบสซ้ำ ๆ หรือ Short Tandem Repeats ซึ่งมีกระจายอยู่ทั่วทุกโครโมโซมเพื่อพิสูจน์บุคคล และพิสูจน์ ความเป็นพ่อ แม่ ลูกการวิเคราะห์ Short Tandem Repeats (STRs) ที่อยู่บน Y-chromosome ใช้สำหรับการพิสูจน์พ่อ ลูก และเครือญาติทางพ่อ แต่ไม่อาจใช้พิสูจน์ความเป็น ครอบครัว พ่อ แม่ ลูก (2) Mitochondrial DNA (mtDNA) เป็น DNA นอกนิวเคลียส อยู่ใน Mitochondria ใช้ประโยชน์ เพื่อการพิสูจน์แม่ ลูก และเครือญาติทางแม่ ไม่อาจพิสูจน์ ความเป็นครอบครัว พ่อ แม่ ลูก อย่างไรก็ตามแม้ว่าการพิสูจน์ บุคคลใน

ปัจจุบันมุ่งเน้นการตรวจวิเคราะห์ DNA แต่การตรวจ บุคคลทางกายภาพ เช่น ลายนิ้วมือจากสถานที่เกิดเหตุ ลายนิ้วมือจากศพ มีข้อได้เปรียบการตรวจ DNA โดยเฉพาะ กรณีการพิสูจน์คู่แฝดจากไข่ใบเดียวกัน เนื่องจากการตรวจ DNA ในคู่แฝดซึ่งตรวจด้วยทุกเทคนิคที่ใช้กันในปัจจุบันไม่ สามารถแยกหรือบอกความแตกต่างของคู่แฝดไข่ใบเดียวกันได้

รูปภาพที่ 3 การเสวนาประชาชน เรื่อง "การเก็บข้อมูลชีวมาตร (Biometrics) ของหน่วยงานรัฐกับการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ" (https://www.spu.ac.th/activities:2019)

บทความในวารสาร CIO World & Business ฉบับเดือนสิงหาคม พ.ศ. 2562 สุพล พรหมมาพันธุ์[5] เขียนไว้ว่าเมื่อวันศุกร์ที่ 12 กรกฎาคม พ.ศ. 2562 เวลา 13.30-16.30 น. ที่ผ่านมา สมาคมความมั่นคงปลอดภัยสารสนเทศและคณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม ร่วมกันจัด เสวนาประชาชน เรื่อง "การเก็บข้อมูลชีวมาตร (Biometrics) ของหน่วยงานรัฐกับการละเมิดสิทธิส่วนบุคคลและผลกระทบ ต่อความมั่นคงของประเทศ" โดยมีวิทยากรและผู้ร่วมเสวนา คือ อาจารย์ปริญญา หอมอเนก ประธานและผู้ก่อตั้ง, ACIS Professional Center Co., Ltd. (ACIS), นพ.สุธี ทุวิรัตน์ กรรมการสมาคมความมั่นคงปลอดภัยสารสนเทศ พล.อ.บรรเจิด เทียนทองดี, พล.อ.เจิดวุธ คราประยูร, และ พ.ต.อ.ญาณพล ยั่งยืน ณ ห้องพัชรกิติยาภา อาคารเฉลิมพระบารมี 50 ปี ซอยศูนย์วิจัย ถ.เพชรบุรีตัดใหม่ กรุงเทพฯ

อาจารย์ปริญญา หอมอเนก[6] กล่าวว่าในประเทศ ไทย พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ปี 2562 ประกาศใช้แล้ว เมื่อวันที่ 24 พฤษภาคม พ.ศ. 2562 ถ้าเป็นข้อมูลอีเมล, Facebook รั่วไหล ยังสามารถแก้ไขได้ด้วยการเปลี่ยน Password แต่ถ้าเป็นข้อมูลเหล่านี้รั่วไหล แล้วจะทำอย่างไร เช่น ลายพิมพ์นิ้วมือ ฝ่ามือ ใบหน้า เรตินา ม่านตา (Iris) ลายเซ็น ดีเอ็นเอ เสียง เป็นต้น ซึ่งข้อมูล เหล่านี้รั่วไหลแล้วไม่สามารถนำกลับมาได้ แก้ไขได้ยากด้วย ข่าวล่าสุด Facebook ได้ประกาศว่าออกหนุนเงินสกุล Libra แม้กระทั่งคนที่เคยได้รับรางวัลโนเบล ก็ยังไม่เชื่อมั่นว่าข้อมูล จะไม่รั่วไหล อ.ปริญญา ยังได้กล่าวถึงกระบวนการในการเข้าถึง เทคโนโลยีการเก็บข้อมูลมี 3 รูปแบบที่มีความแตกต่างกัน คือ (1) การระบุตัวตน (Identification) อันหมายถึงการระบุตัวตน ว่าคุณเป็นใคร ซึ่งเป็นการระบุตัวตนผ่านชื่อผู้ใช้ (Username), ความปลอดภัยของหมายเลขไอดี (Security ID), สมาร์ทการ์ด (Smart Card) และพีไอวี (PIV) (2) การตรวจสอบรับรอง (Authentication) เป็นการพิสูจน์ตรวจสอบว่าคุณเป็นใคร ผ่านชื่อผู้ใช้/คำสั่งผสมรหัสผ่าน

(Username/Password Combo), หรือ PIN, OTP หรือการเก็บข้อมูลทางชีวมาตร (Biometrics Data) ซึ่งเป็นลักษณะเฉพาะของแต่ละบุคคล หรืออัตลักษณ์ เช่น ลายพิมพ์นิ้วมือ เรตินา ม่านตา ใบหน้า เป็นต้น ปัจจุบันมีการใช้ไบโอเมทริกซ์นี้กันอย่างแพร่หลาย เช่น การสแกนลายพิมพ์นิ้วมือเพื่อปลดล็อกปุ่มโทรศัพท์, การสแกน ใบหน้าเข้าทำงาน และห้องประชุม (3) การอนุญาต (Authorization) หมายถึงการได้รับอนุญาตจากผู้ที่เป็นเจ้าของข้อมูล ในการเก็บข้อมูลความเป็นส่วนตัวของประชาชนนั้น หน่วยงาน ของรัฐต้องมีการรับรองความปลอดภัยที่แน่นอนยั่งยืนว่าข้อมูลเหล่านั้นต้องไม่รั่วไหล ถ้าคุณเดินทางไปเซิ่นเจิ้น เมื่อเข้าสู่เมือง จะมีกล้องจับเก็บข้อมูลตลอด บางคนกลัวมากจะกระโดดตึกตายก็มี และมีการประท้วงเกี่ยวกับเรื่องนี้ที่ประเทศฮ่องกงด้วย เช่นกัน ความจริงแล้วการจัดเก็บข้อมูลสามารถทำได้ แต่เราไม่รู้ว่าเขาเอาข้อมูลของเราไปขายหรือเปล่า สรุปประเด็นเป็น 2 ข้อ คือ (1) ปัจจุบันเทคโนโลยีไปไกลมากที่เรียกว่า Disruptive Technologies for Value Economy ต้องรู้เท่าทัน (2) เรื่องของคน การจัดเก็บข้อมูลของคนต้องดูว่าเขาเอาไปทำ อะไร เมื่อคุณเก็บข้อมูลไปแล้วมีการรักษาความปลอดภัย ที่ดีหรือไม่ การจัดเก็บข้อมูลต้อง Concern เรื่องของ Privacy ด้วย การจัดเก็บข้อมูล “ถ้าเก็บข้อมูลเพื่อความมั่นคงของ ประเทศสามารถทำได้ แต่คุณต้องไม่ให้ข้อมูลรั่วไหลนะ ถ้าไม่ชัวร์จริงอย่าเก็บดีกว่า” ถ้าคุณเก็บข้อมูลของใครแล้ว ควรลบทิ้ง พ.ร.บ.ความมั่นคงไซเบอร์ ห้ามล่ม, พ.ร.บ.ข้อมูลส่วนบุคคล ห้ามรั่ว ถ้าข้อมูลรั่ว มีคนจะเล่นงานคุณ

นพ.สุธี ทุวิรัตน์ กล่าวว่า มี 2 เรื่องหลัก คือ (1) หนังสือเดินทาง (Passport) รุ่นใหม่ของประเทศไทย โดยกระทรวงการต่างประเทศ ซึ่งแต่เดิมมีการเก็บข้อมูลทั้ง ภาพถ่าย และลายพิมพ์นิ้วมือสิบนิ้ว แต่ต่อไปนี้จะมีการ เก็บข้อมูลชีวมาตรม่านตา (Iris) ด้วย ซึ่งทางกระทรวงฯ ได้ให้เหตุผลว่าการเก็บข้อมูลชีวมาตรดังกล่าวเป็นคุณลักษณะความปลอดภัยสูงสุดในการป้องกันการปลอมแปลงหนังสือเดินทาง ซึ่งแตกต่างจากประเทศอื่น เช่น สหรัฐอเมริกาเก็บเฉพาะข้อมูล ภาพถ่ายอย่างเดียว ไม่ให้เก็บลายพิมพ์นิ้วมือ ในสหภาพยุโรป เก็บเฉพาะภาพถ่ายและลายพิมพ์นิ้วมือเพียง 2 นิ้ว เช่น ประเทศเยอรมันนี มีการเก็บม่านตา ส่วนประเทศเนเธอร์แลนด์ เก็บลายพิมพ์นิ้วมือ เป็นต้น สำนักงานตรวจคนเข้าเมือง (สตม.) เวลามีคนเดินทางไปต่างประเทศเขาจะดำเนินการตรวจ 2 เรื่อง คือ (1) ตรวจเอกสาร โดยเอา Passport มาสแกน เพื่อให้รู้ว่า คนนี้คือใคร (Identification) (2) ระบบอิเล็กทรอนิกส์ (Chip) คือการนำเอาข้อมูลในเอกสารมาตรวจสอบว่าตรงกันไหม ซึ่งเป็นการยืนยันตัวตนที่แน่นอน (Authentication) ตอนนี้ใครจะไปทำหนังสือเดินทางจะต้องถูกเก็บ 3 อย่าง คือ (1) รูปถ่าย (2) ลายพิมพ์นิ้วมือ และ (3) ม่านตา ซึ่งคนที่มา จัดเก็บข้อมูลนั้นเป็นบริษัทเอกชนที่มีการเข้ามาประมูลงานได้ จากภาครัฐและได้ไปในราคาถูก ๆ ซึ่งเอกชนเหล่านี้ในแต่ละปี มีการเปลี่ยนแปลงไป แล้วแต่ว่าใครจะประมูลได้ ซึ่งตรงนี้ ข้อมูลคนทำหนังสือเดินทางอาจจะรั่วไหล และอาจถูกสวมรอยได้ (2) การลงทะเบียนซิมโทรศัพท์ด้วยวิธีอัตลักษณ์ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และ กิจการโทรคมนาคมแห่งชาติ (กสทช.) มีนโยบายการให้ ลงทะเบียนซิมโทรศัพท์ทั้งการตรวจสอบใบหน้าและสแกน ลายพิมพ์นิ้วมือทั่วประเทศ เมื่อเก็บข้อมูลเหล่านี้ไปแล้วมั่นใจได้อย่างไรว่าข้อมูลไม่รั่วไหล แม้กระทั่งข้อมูลบัตรประชาชน ของบุคคลสำคัญหลายคนถูกนำไปลงทะเบียนซ้ำกันหลายครั้ง ต่อไปอาจมีผลกระทบต่อการเลือกตั้ง เมื่อก่อนมีการใช้ บัตรประชาชนในการเลือกตั้ง แต่ต่อไปจะมีการใช้ e-Vote ในการเลือกตั้ง เมื่อข้อมูลถูกนำไปเก็บไว้ในฐานข้อมูล ถ้าข้อมูล เหล่านั้นถูกแฮกจะเกิดอะไรขึ้นกับผลการเลือกตั้ง สรุปคือ รัฐอยากควบคุมข้อมูลส่วนบุคคล, บริษัทธุรกิจ อยากได้ข้อมูล ของลูกค้า ข้อมูลส่วนบุคคลในโลกออนไลน์ถูกนำไปวิเคราะห์

หาผลประโยชน์ ควรมีการปกป้องข้อมูลด้วยวิธีการที่ปลอดภัย ด้วย มี 2 กรณีตัวอย่าง คือ กรณีแรก สายการบินบริติช แอร์เวย์ ในเครือบริษัทอินเตอร์เนชั่นแนล แอร์ไลน์สกรุ๊ป (IAG) ถูกสำนักงานคณะกรรมาธิการข้อมูลของสหราชอาณาจักร (ICO) ลงโทษปรับเงินเป็นจำนวน 183.39 ล้านปอนด์ (ประมาณ 7,069,820,000 บาท) สืบเนื่องจากกรณีการรั่วไหลของข้อมูล ทางการเงิน และข้อมูลลูกค้าของบริษัทเมื่อปีที่แล้ว (https://thestandard.co) กรณีที่สอง คือ โรงแรมแมริออท (Marriot) อินเตอร์เนชั่นแนล เครือธุรกิจโรงแรมรายใหญ่ที่สุดในโลก โดนแฮ็กเกอร์เจาะระบบล้วงข้อมูลลูกค้า 500 ล้านคน นับตั้งแต่ ปี 2014 และอาจต้องจ่ายค่าปรับสูงถึง 200 ล้านดอลลาร์ (https://www.posttoday.com) สำหรับในประเทศไทย อาจจะเข้าข่ายผิด พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตราที่ 6 มีโทษจำคุก และโทษปรับทางปกครอง 5 ล้านบาท คณะกรรมการก็มีความผิดด้วย

ขณะที่เวทีเสวนาประชาชนอันประกอบด้วย นพ.สุธี ทุวิรัตน์, พล.อ.บรรเจิด เทียนทองดี, พล.อ.เจิดวุธ คราประยูร, และ พ.ต.อ.ญาณพล ยั่งยืน สรุปความว่า การจัดเก็บข้อมูล ชีวมาตรนั้นมีทั้งข้อดีและข้อเสีย สำหรับข้อดี คือเมื่อเกิดปัญหาอาชญากรรมขึ้น สมัยก่อนตามจับผู้ร้ายได้ยากมาก เพราะหา หลักฐานไม่ค่อยมี และมีการพิมพ์ลายนิ้วมือไว้นี้พอเป็นแนวทางที่จะช่วยได้ในการสืบพยานหลักฐาน แต่ส่วนใหญ่คนที่ทำไว้ก็เป็นจำพวกพ่อค้าที่ทำดอกไม้เพลิง พอจะหาคนทำผิดก็หายาก เนื่องจากคนที่ทำลายพิมพ์นิ้วมือไว้ก็ยังไม่เคยมี ประวัติอาชญากรรม เวลาจะหาข้อมูลจับผู้ร้ายก็ต้องไปพิสูจน์ ว่าใครใส่แหวนนิ้วไหน ดังนั้นการจัดเก็บข้อมูลส่วนบุคคลเอา ไว้ในการทำบัตรประชาชนก็ถือว่ายังมีประโยชน์ แต่ไม่ใช่เก็บข้อมูลทุกอย่าง รหัสผ่าน (Password) อีเมล์ เมื่อถูกแฮกไป ก็ยังสามารถเปลี่ยนได้ แต่ม่านตาเปลี่ยนไม่ได้ ในสหภาพยุโรปเขาเก็บข้อมูลโดยให้สแกนนิ้วเพียงแค่ 2 นิ้ว ส่วนที่เหลือเอาไว้ ใช้ประโยชน์อย่างอื่น จะเกิดอะไรขึ้นหากต่อไปมีการโคลนนิ่งมนุษย์ การเก็บข้อมูลของหน่วยงานรัฐควรต้องมีการออกแบบ ให้ชัดเจนว่าจะเก็บข้อมูลอะไรบ้าง ไม่ใช่เก็บทุกอย่าง เพราะตอนนี้ทำบัตรประชาชน, ทำหนังสือเดินทาง, ทำใบขับขี่ ก็เก็บข้อมูลกันหมดทั้งรูปถ่าย ลายพิมพ์นิ้วมือ ใบหน้า ม่านตา ต่อไปอาจมีการเก็บถึงเรื่องดีเอ็นเอ (DNA) ด้วย เพราะอาจเสี่ยง ต่อการละเมิดสิทธิส่วนบุคคล ต้องบอกประชาชนให้ชัดเจนว่า มีความจำเป็นอะไรต้องเก็บข้อมูลชีวมาตรเหล่านี้ ถ้าพลาด ข้อมูลรั่วไหลเพียง 1 % ย่อมมีผลเสีย ส่งผลกระทบต่อประชาชน ท้ายสุด นพ.สุธี ทุวิรัตน์ ได้มีข้อเสนอแนะในการ เสวนา ครั้งนี้ คือ (1) รัฐควรจะหลีกเลี่ยงการบังคับเก็บข้อมูลชีวมาตรของประชาชน เก็บเท่าที่จำเป็นจริง ๆ (2) รัฐควรจะต้อง กำกับดูแลมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ และคุ้มครองข้อมูลส่วนบุคคลของข้อมูลชีวมาตรอย่างมี ธรรมาภิบาล เปิดเผย โปร่งใส (3) รัฐไม่ควรจะยอมให้เอกชน เข้ามาบริหารจัดการฐานข้อมูลชีวมาตร และ (4) รัฐต้องมี มาตรการเยียวยาแก้ไขเจ้าของข้อมูลที่เกิดการรั่วไหล ทั้งหมด ทั้งมวลนี้หากทางรัฐได้เห็นความสำคัญเหล่านี้ จึงนับได้ว่าจะ เป็นประโยชน์ต่อประชาชนและประเทศชาติโดยแท้จริง

ข่าวล่าสุด นายแพทย์สุธี ทุวิรัตน์[7] กรรมการสมาคม ความมั่นคงปลอดภัยระบบสารสนเทศ หรือ TISA เปิดเผยกับ “ฐานเศรษฐกิจ” ว่ากรณีธนาคารแห่งประเทศไทย (ธปท.) กำลัง ผลักดันให้มีการใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) โดยการเอาเทคโนโลยีชีวมาตร (Biometric) เช่น การจดจำใบหน้า ลายนิ้วมือ หรือม่านตา มาใช้ในการพิสูจน์ ยืนยันตัวบุคคลในการทำธุรกรรมทางการเงิน (Biometric Payment) กำลังส่งผลกระทบต่อเงินฝากธนาคารคนไทย และมีโอกาสถูกแฮกเกอร์สวมรอยถอนหรือสั่งโอนไปจนเกลี้ยงบัญชีโดยไม่รู้ตัว ทั้งยังไม่สามารถที่จะเรียกร้องความ

รับผิดชอบ จากธนาคารได้ “ปัจจุบันมีการบังคับเก็บข้อมูลชีวมาตร ประชาชน ได้แก่ ภาพถ่ายใบหน้า ลายนิ้วมือ 10 นิ้ว โดยหน่วยงานรัฐ เช่น การทำบัตรประชาชน หนังสือเดินทาง ลงทะเบียนซิมมือถือ นอกจากนี้กระทรวงการต่างประเทศกำหนดให้มีการเก็บข้อมูลม่านตาเพิ่มเติม โดยข้อมูลเหล่านี้ถูก เก็บไว้ในฐานข้อมูลของเอกชนผู้รับสัมปทานภาครัฐ หากมีการ รั่วไหลข้อมูลหรือเจ้าหน้าที่รัฐนำข้อมูลไปใช้ไม่ถูกต้อง จะส่งผล ให้คนไทยทั้งประเทศมีความเสี่ยงที่จะถูกแอบอ้าง สวมรอย ตัวบุคคลถอนเงินในบัญชีธนาคารจนหมดตัวและยังมีโอกาส ที่จะถูกแอบอ้างสวมรอยตัวบุคคลทำธุรกรรมทางดิจิทัลอื่น ๆ ล่าสุดทางสมาคมฯ ได้ยื่นหนังสือเกี่ยวกับข้อวิตกกังวลถึงการ เก็บข้อมูลชีวมาตรส่วนบุคคลในความรับผิดชอบของหน่วยงานรัฐไปยัง พล.อ.ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี โดยประเด็นปัญหาสำคัญ คือ 1. การจัดเก็บข้อมูลชีวมาตรของประชาชนโดยหน่วยงานรัฐ ที่ไม่ได้มีการพิจารณาถึงเหตุผล และความจำเป็นอย่างรอบคอบและรอบด้าน รวมทั้งไม่ได้มีการพิจารณาถึงผลกระทบต่อเจ้าของข้อมูลกรณีที่เกิดการ รั่วไหลหรือถูกละเมิด 2. การที่หน่วยงานรัฐให้เอกชนเข้ามา เป็นผู้บริหารจัดการฐานข้อมูลชีวมาตรของประชาชน, 3. การไม่มีมาตรการเยียวยาบุคคลผู้เป็นเจ้าของข้อมูลชีวมาตร ที่อยู่ในความควบคุมของหน่วยงานรัฐกรณีเกิดการรั่วไหลหรือ ถูกละเมิด, 4. การไม่มีมาตรการกำกับดูแลที่มีธรรมาภิบาล เปิดเผยและโปร่งใส บังคับใช้กับหน่วยงานรัฐที่บังคับเก็บข้อมูล ส่วนบุคคลประชาชน โดยเฉพาะอย่างยิ่งข้อมูลชีวมาตร และ 5. การจัดเก็บข้อมูลชีวมาตรของประชาชน โดยไม่มีมาตรฐาน การรักษาความมั่นคงปลอดภัยเพียงพอ สุ่มเสี่ยงข้อมูลรั่วไหล และทำให้ไม่สามารถเอาชีวมาตรมาใช้พิสูจน์ยืนยันตัวตนทำ ธุรกรรมอิเล็กทรอนิกส์ เช่น ไม่สามารถใช้ชีวมาตรยืนยัน ตัวบุคคลในการชำระเงินออนไลน์ หรือการลงคะแนนเลือกตั้ง อิเล็กทรอนิกส์ในอนาคตอันใกล้ เนื่องจากข้อมูลที่รั่วไหลจะถูก นำมาใช้แอบอ้างสวมรอยตัวบุคคลทำธุรกรรมทางดิจิทัลไป ตลอดชีวิต สำหรับข้อเสนอแนะ คือ 1. จัดตั้งคณะทำงาน เพื่อรวบรวมข้อมูลการบังคับเก็บข้อมูลชีวมาตรของประชาชน 2. ศึกษาว่าประกาศบังคับเก็บข้อมูลชีวมาตรของหน่วยงานรัฐแต่ละแห่งเป็นไปโดยชอบธรรมและมีอำนาจตามกฎหมาย หรือไม่ และใช้อำนาจรัฐขัดกับบทบัญญัติเรื่องการคุ้มครอง สิทธิและเสรีภาพประชาชนตามรัฐธรรมนูญหรือไม่

การประยุกต์ใช้เทคโนโลยีชีวมาตร หรือไบโอ-เมทริกซ์ ปัจจุบันมีนิยมใช้งานกันอย่างแพร่หลาย ตัวอย่างเช่น ทีมข่าวอาชญากรรม[8] ของ MGR Online เมื่อวันที่ 14 กันยายน พ.ศ. 2562 ได้รายงานข่าวเรื่อง “สตม.โชว์ศักยภาพ ไบโอเมทริกซ์ 3 วัน จับพาสปอร์ตปลอม 8 ราย” ความว่า วันนี้ (24 ก.ย.) เวลา 16.00 น. ที่สำนักงานตรวจคนเข้าเมือง (สตม.) พล.ต.ท.สมพงษ์ ชิงดวง ผบช.สตม. พร้อมด้วย พล.ต.ต.ภาคภูมิภิภัทฒ์ สัจจพันธุ์ รอง ผบช.สตม. พล.ต.ต. อิทธิพล อิทธิสารรณชัย รอง ผบช.สตม. พ.ต.อ.เกติ์ฉกาจ นิลประดับ รอง ผบก.ตม.2 ร่วมกันแถลงผลการระดม กวาดล้างอาชญากรรมและกวดขันจับกุมคนต่างด้าวที่เข้ามา อยู่ในราชอาณาจักรโดยผิดกฎหมายหรือที่มีพฤติกรรมจะ เข้ามากระทำความผิดทางอาญาหรือก่อความเดือดร้อนวุ่นวาย ให้บังเกิดผลอย่างเป็นรูปธรรม โดยระหว่างวันที่ 11-13 กันยายน กองกำกับการสืบสวนปราบปราม กองบังคับการ ตรวจคนเข้าเมือง 2 มีผลการจับกุมคดีสำคัญ ๆ จำนวน 8 ราย โดยเมื่อวันที่ 11 ก.ย. ที่ผ่านมา เวลาประมาณ 08.20 น. จับกุม ครอบครัวชาวอิหร่านทั้ง 3 ราย ใช้หนังสือเดินทางประเทศ กรีซปลอม เพื่อใช้ในการเดินทางไปขอลี้ภัยที่ประเทศอังกฤษ โดยผู้เป็นพ่ออ้างว่าติดต่อนายหน้าชาวอิหร่านเพื่อจัดหา เอกสารเดินทาง ค่าใช้จ่ายประมาณ 50,000 ยูโร หรือประมาณ 1,700,000 บาท โดยต้องชำระล่วงหน้า 20,000 ยูโร ที่ประเทศ อิหร่าน และ

เดินทางมารับหนังสือเดินทางที่ประเทศตุรกี ได้ชำระส่วนที่เหลืออีก 30,000 ยูโร ก่อนจะเดินทางมาประเทศ ไทยเพื่อใช้หนังสือเดินทางปลอมเล่มดังกล่าวในการเดินทาง ต่อมาเวลาประมาณ 12.20 น. ของวันเดียวกันสามารถจับกุม ชายชาวอิหร่าน อายุ 34 ปี ผู้ต้องหาชาวอิหร่าน โดยใช้หนังสือ เดินทางประเทศกรีซปลอมเพื่อใช้ในการเดินทางไปขอลี้ภัยที่ ประเทศอังกฤษเช่นกัน โดยรายนี้ติดต่อนายหน้ารับหนังสือ เดินทางที่ประเทศตุรกี และเสียค่าใช้จ่ายจำนวน 4,000 ยูโร หรือประมาณ 136,000 บาท โดยหนังสือเดินทางจำนวน 2 ใน 4 เล่ม ระบบไบโอเมทริกซ์แจ้งเตือนว่าเป็นหนังสือเดินทาง ที่ถูกขโมยจากฐานข้อมูลของอินเตอร์โพล ทางตำรวจ กก.สส.ปป.บก.ตม.2 จึงทำการแจ้งข้อหาชาวอิหร่านทั้ง 4 รายนี้ ในข้อหา “ใช้หรือมีไว้ใช้ซึ่งหนังสือเดินทางปลอมฯ (หนังสือ เดินทางประเทศกรีซปลอม)” นำส่ง พนักงานสอบสวน สภ.ท่าอากาศยานสุวรรณภูมิดำเนินคดี จากนั้นวันที่ 12 ก.ย. ที่ผ่านมา เวลาประมาณ 08.30 น. จับกุม 2 ผู้ต้องหาหญิง ชาวปาเลสไตน์ ได้โดยสารเครื่องบินมาจากกรุงอาบูดาบี ใช้หนังสือเดินทางประเทศสวีเดนหน้าเหมือนในการเดินทาง เข้าประเทศ เพื่อแฝงตัวเป็นนักท่องเที่ยว ก่อนที่จะใช้หนังสือ เดินทางหน้าเหมือนเดินทางไปขอลี้ภัยยังประเทศที่สาม โดยทั้ง 3 ราย ติดต่อนายหน้าที่ประเทศอิหร่าน มีค่าใช้จ่าย คนละ 12,500 ยูโร (หรือประมาณคนละ 375,000 บาท ซึ่งชำระ ล่วงหน้าคนละ 2,500 ยูโร หรือประมาณคนละ 75,000 บาท เมื่อครั้งติดต่อรับเล่ม และจะชำระส่วนที่เหลือเมื่อสามารถ เดินทางไปยังไประเทศที่สามสำเร็จ โดยระบบไบโอเมทริกซ์ อ่านค่าความเหมือนเปรียบเทียบภาพถ่ายจากชิพที่ฝังอยู่ในหนังสือเดินทางอีพาสปอร์ตกับภาพผู้โดยสาร พบว่ามีเปอร์เซ็นต์ ความเหมือนกันนั้นมีค่าต่ำ ผู้โดยสารมีใบหน้า หู ตา จมูก และปาก แตกต่างจากภาพที่จัดเก็บในชิพ ทางตำรวจ กก.สส. ปป.บก.ตม.2 จึงจับกุมผู้ต้องหาทั้ง 3 ราย พร้อมแจ้งข้อหา “ใช้หนังสือเดินทางของผู้อื่นโดยมิชอบในประการที่น่าจะก่อให้ เกิดความเสียหายต่อผู้อื่นหรือประชาชน” นำส่งพนักงาน สอบสวน สภ.ท่าอากาศยานสุวรรณภูมิ ดำเนินคดี และวันที่ 13 ก.ย. ที่ผ่านมา เวลาประมาณ 09.30 น. จับกุมชายชาว ไนจีเรีย อายุ 31 ปี ใช้หนังสือเดินทางแอฟริกาใต้ปลอม เดินทางมาจากประเทศตุรกี เปลี่ยนเครื่องที่ประเทศกาตาร์ ก่อนที่จะเดินทางเข้าประเทศไทย เพื่อแฝงตัวเป็นนักท่องเที่ยว ก่อนที่จะใช้หนังสือเดินทางปลอม เพื่อลักลอบไปทำงานใน ประเทศเกาหลีใต้ รับหนังสือเดินทางจากนายหน้าชาว แอฟริกาใต้ เสียค่าดำเนินการประมาณ 600 เหรียญสหรัฐ หรือประมาณ 18,000 บาท โดยระบบไบโอเมทริกซ์ สามารถ ตรวจสอบหน้าข้อมูลส่วนบุคคลด้วยแสงต่าง ๆ เช่น แสงยูวี แสงอินฟาเรด พบความผิดปกติของหน้าข้อมูลส่วนบุคคล เล่มดังกล่าว ตำรวจ กก.สส.ปป.บก.ตม.2 จับกุมชายคน ดังกล่าวในข้อหา “ใช้หรือมีไว้ใช้ซึ่งหนังสือเดินทางปลอมฯ (หนังสือเดินทางประเทศกรีซปลอม)” นำส่ง พนักงานสอบสวน สภ.ท่าอากาศยานสุวรรณภูมิดำเนินคดีต่อไป

ในรายงานเรื่อง “ไบโอเมทริกซ์” สุพาวรรณ์ กุศลครออง[9] ได้เขียนถึงการประยุกต์ใช้ไบโอเมทริกซ์ไว้ใน sites.google.com สามารถนำไปประยุกต์ใช้ได้หลายแนวทาง คือ (1) การควบคุม ใช้ในการควบคุมการเข้าออกสถานที่/หรือ การใช้ตรวจสอบเวลาทำงานการเข้าออกสถานที่หวงห้ามในปัจจุบัน มักจะใช้บัตรผ่าน หรือใช้รหัสผ่าน หรือแม้แต่การใช้ยามเฝ้า ซึ่งการป้องกันแบบนี้สามารถถูกลักลอบได้ง่าย เช่นบัตรผ่าน หรือรหัสผ่าน อาจหาย ลืม หรือแม้แต่ให้คนอื่นยืมใช้ได้ ส่วนยามเฝ้าก็ขึ้นอยู่กับความเข้มงวดของยามแต่ละคน ความบกพร่องของระบบที่ใช้กันอยู่ในปัจจุบันจึงมีอยู่มาก การนำเอา ไบโอเมทริกซ์มาช่วยเช่น การผ่านเข้าออกโดยใช้การ สแกนลายพิมพ์นิ้วมือ, ใช้การตรวจสอบรูปหน้า, หรือแม้แต่ การใช้การตรวจสอบลักษณะของเรตินาภายในดวงตา จึงเป็น ทางออกที่ดีกว่าการใช้งานที่เป็นอยู่ในปัจจุบัน (2) การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย เครื่องคอมพิวเตอร์ แบบ Notebook หลายรุ่น มีการนำเอาเทคโนโลยี Biometrics ประเภทลายนิ้วมือเพื่อมาช่วย Authentication การใช้ งานเครื่องคอมพิวเตอร์ซึ่งค่อนข้างมีประโยชน์มากสำหรับบุคคล ที่ต้องการความปลอดภัยในการรักษาข้อมูล เพราะถึงแม้ว่า เครื่องคอมพิวเตอร์จะถูกขโมย แต่ผู้ที่ขโมยไปก็ไม่สามารถนำไปใช้งานได้ โดยการใช้ลายนิ้วมือมาช่วยมีอยู่หลัก ๆ สองประเภท คือเครื่องคอมพิวเตอร์ Notebook ที่มีตัวตรวจ จับลายนิ้วมืออยู่ในตัวเครื่องอยู่แล้ว และประเภทที่ใช้ PC Card ที่มีตัวตรวจจับลายนิ้วมืออยู่ ใส่เข้าไปในช่อง PC Card ของเครื่องคอมพิวเตอร์ Notebook โดยที่ลายนิ้วมือจะเป็นการ ใช้ทดแทนการใช้รหัสผ่าน (Password) นั่นเอง นอกจากนี้ การใช้งานคอมพิวเตอร์ระบบเครือข่าย จะต้องให้ผู้ใช้ใส่รหัส ผ่านก่อนการใช้งานทุกครั้ง แต่เนื่องจากรหัสผ่านสามารถถูก คาดเดาหรือขโมยหรือถูกยืมไปใช้ได้ง่าย ดังนั้นการใช้ Biometrics มาเป็นตัวเข้ารหัสการใช้งานของผู้ใช้ระบบเครือข่ายจึงเป็นสิ่งที่สามารถยืนยันได้อย่างแท้จริงว่าผู้ที่ใช้ระบบเครือข่ายอยู่ คือผู้ที่มีสิทธิในการใช้งานได้จริง (3) การใช้งานของสถาบันการเงินในปัจจุบันการตรวจสอบตัวบุคคลเป็นสิ่งที่เป็นพื้นฐาน ที่สำคัญของการทำธุรกิจของสถาบันทางการเงิน การใช้การตรวจสอบลายเซ็น ลายนิ้วมือ บัตรประจำตัว หรือแม้แต่ รหัสผ่าน ล้วนแต่เป็นสิ่งที่ง่ายต่อการปลอมแปลงและเป็น ปัญหาที่สถาบันการเงินต้องพบเจอกับกลโกงต่าง ๆ ที่ทำให้เกิด ความเสียหาย ดังนั้นการนำเอาเทคโนโลยีทางด้านไบโอเมทริกซ์ มาใช้เป็นสิ่งประกอบเพิ่มเติมในการตรวจสอบตัวบุคคล จึงเป็น สิ่งที่ได้รับความสนใจเป็นอย่างมากจากสถาบันทางการเงิน ทั้งทางด้านการช่วยในการเบิกถอนเงินทั้งที่ผ่านทางเคาน์เตอร์ และทั้งที่ผ่านทางเครื่อง ATM นอกจากนี้การใช้เทคโนโลยี ไบโอเมทริกซ์ในการตรวจสอบผู้ใช้บัตรเครดิตก็จะเป็นการ ช่วยลดการปลอมแปลง หรือการลักลอบใช้บัตรเครดิตของ ผู้อื่น และในทางกลับกันก็ยังช่วยลดการปฏิเสธความ รับผิดชอบของผู้ใช้งานเอง เพราะมีหลักฐานที่แน่นอนในการ ระบุตัวบุคคลที่เชื่อถือได้ (4) การใช้งานด้านการระบุตัว อาชญากร การระบุตัวอาชญากรที่ทำการตรวจสอบลายนิ้วมือ หรือการชี้ตัวโดยพยาน ซึ่งสามารถนำเอา Biometrics มาช่วยในการตรวจสอบลายนิ้วมือโดยอัตโนมัติ AFIS (Auto- mated Fingerprint Identification System) ระบบนี้ นอกจากจะให้ทางตำรวจตรวจลายนิ้วมือที่พบในที่เกิดเหตุ กับฐานข้อมูลลายนิ้วมืออาชญากรที่มีอยู่แล้ว ระบบ AFIS ยังสามารถเป็นแหล่งข้อมูลให้กับทางองค์กรทางเอกชนในการ ค้นหาประวัติการทำผิดกฎหมายของผู้สมัครงานหรือบุคคลากรภายในองค์กรได้อีกด้วย (5) งานทะเบียนราษฎร์จะเห็นได้ว่า ในยุคปัจจุบันประเทศไทยเองก็ได้มีการพัฒนางานทะเบียน ราษฎร์ให้มีความทันสมัยและมีความสะดวกสบายและมีความ รวดเร็วมากยิ่งขึ้น ส่วนหนึ่งก็ได้มีการนำเทคโนโลยี Biometrics ร่วมกับเทคโนโลยีทางคอมพิวเตอร์ เพื่อมาใช้กับการระบุ ยืนยันตัวบุคคลในการ

มาติดต่องานทะเบียนราษฎร์ ซึ่งจะทำ ให้เกิดความคล่องตัวมากยิ่งขึ้น อย่างเช่น ในการต่ออายุ บัตรประชาชน ก็สามารถทำแบบออนไลน์ได้ที่สำนักงานเขต หรืออำเภอที่ใดก็ได้ เนื่องจากจะมีการยืนยันตัวบุคคลและ เชื่อมโยงเป็นระบบเครือข่ายเดียวกันทั้งประเทศ เป็นต้น (6) การพิสูจน์ลายเซ็น โดยจะมีเครื่องตรวจสอบลายเซ็น (Signature Verification System) เทคโนโลยีนี้ใช้การจดจำลักษณะ ของลายเซ็น เส้นสายลายเซ็นซึ่งเซ็นโดยใช้ปากกาพิเศษหรือ ปากกาสำหรับรับข้อมูลเข้าสู่คอมพิวเตอร์ (Tablet) โดยจะวัด จากแรงกด จังหวะความหนักเบาของลายเซ็น และอารมณ์ ในการเซ็น การพิสูจน์ลายเซ็นในปัจจุบันยิ่งได้รับการยอมรับ มากขึ้น โดยในหลายประเทศได้มีการออกกฎหมายมารองรับ โดยเฉพาะการทำธุรกิจพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) และการเซ็นเอกสารการปฏิบัติงานต่าง ๆ ในประเทศไทย ได้มีการออกพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ปี พ.ศ. 2544 โดยมีปรากฏอยู่ในมาตราที่ 4 ซึ่งเป็นการกำหนด นิยามความตอนหนึ่งว่า “ลายมือชื่ออิเล็กทรอนิกส์” หมายความ ว่า อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้น ให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูล อิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับ
ข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคล ผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับ ข้อความในข้อมูลอิเล็กทรอนิกส์นั้น และในมาตราที่ 9 ความว่า ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูล อิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า (1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่า เจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ (2) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้ โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลง ของคู่กรณี และบล็อกเกอร์ชื่อ Pornaka abobee111[10] ได้เขียนไว้ใน Bloggang เกี่ยวกับการนำไบโอเมทริกซ์มาใช้ ด้านการค้าคือ (7) การนำมาใช้ในธุรกิจการค้า มีนำเทคโนโลยี Biometrics มาใช้กับธุรกิจการค้า เป็นการนำเทคโนโลยี Biometrics ที่ได้นำข้อมูลทางกายภาพของบุคคลทำงานร่วมกับเทคโนโลยีระบบคอมพิวเตอร์ ในกิจการธุรกิจร้านค้า หรือ ร้านสะดวกซื้อ ห้างสรรพสินค้า เพื่อใช้ในการชำระเงินช่วยไม่ให้เสียเวลาในการรอคิวที่จุดชำระเงิน เพราะลูกค้าไม่ต้อง พกเงินสดอีกต่อไป การทำงานก็คือ ลูกค้าจะต้องเลือก ลงทะเบียนกับร้านค้าก่อนเพื่อที่จะเก็บรวบรวมข้อมูลของลูกค้า เอาไว้ ที่เรียกระบบนี้ว่า Touch to Pay เมื่อลงทะเบียนกับ ร้านค้าเรียบร้อยก็สามารถซื้อสินค้าได้ทุกอย่าง จากนั้นเมื่อมา จุดชำระเงินก็แค่วางนิ้วมือเพื่อให้เครื่องอ่านลายนิ้วมือสำหรับ การชำระเงินแบบ Biometrics แล้วใส่รหัสผ่านและเลือกวิธี การชำระเงินตามที่ได้ลงทะเบียนไว้ตอนแรก ซึ่งระบบก็จะทำ การอ่านข้อมูลพร้อมกับหักเงินของคุณโดยอัตโนมัติ

รูปภาพที่ 5 และรูปภาพที่ 6 แสดงการใช้เทคโนโลยีชีวมาตรเพื่อตรวจสอบการเข้าถึงและการใช้บัตร ATM ทางด้านการเงินและ เครื่องสแกนลายพิมพ์นิ้วมือ เพื่อใช้เข้า-ออกในการทำงาน (Gary B. Shelly 2007:567 and https://www.bloggang.com 2020)

ดังนั้นจะเห็นได้ว่าการพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมาตร (Biometrics Technology) นั้นมีความสำคัญเป็น อย่างมาก โดยเฉพาะอย่างยิ่งการนำไปประยุกต์ใช้ในการ ทำงานด้านต่าง ๆ ไม่ว่าจะเป็นระบบธนาคาร การจัดทำหนังสือ เดินทาง (Passport) การจัดทำทะเบียนราษฎร์ เป็นต้น หากมี การจัดเก็บข้อมูลของประชาชนไม่มากจนเกินไปก็มีประโยชน์ อย่างมาก เพราะจะช่วยในเรื่องของรักษาความมั่นคงปลอดภัย ในการทำงาน ตลอดจนในเรื่องของความสะดวกสบาย แต่ถ้า หากว่าทางหน่วยงานของรัฐและเอกชนมีการจัดเก็บข้อมูล ทางชีวมาตรหลายอย่างมากเกินไป คือ ทั้งลายพิมพ์นิ้วมือ ภาพถ่ายการสแกนใบหน้า การสแกนม่านตา เป็นต้น อีกทั้งยังเปิดโอกาสให้บริษัทเอกชนเข้ามาประมูลการจัดเก็บ ข้อมูลชีวมาตรด้วย และบริษัทเอกชนเหล่านั้นก็มีการผลัด เปลี่ยนหมุนเวียนกันไป สุดแล้วแต่ใครจะประมูลได้ ซึ่งวิธีการ เช่นว่านี้อาจเป็นการเสี่ยงต่อการละเมิดสิทธิส่วนบุคคลแล้ว ยังเสี่ยงต่อการที่มีข้อมูลรั่วไหลอีกด้วย หากไม่มีมาตรการ การรักษาความปลอดภัยที่ดี ซึ่งถ้าหากมีการรั่วไหลของข้อมูล ขึ้นมาจริง ๆ อาจมีการขโมยอัตลักษณ์หรือการสวมรอยจาก แฮกเกอร์ในการก่ออาชญากรรมทางไซเบอร์ โดยเฉพาะ อาชญากรรมทางด้านการเงิน เช่น อาจมีการถอน หรือสั่งจ่าย เงินไปจนหมดบัญชี หรือผู้ที่เป็นเจ้าของบัญชีไม่สามารถสั่งจ่าย ชำระเงินทางบัญชีออนไลน์ได้

เอกสารอ้างอิง

1. สุธี ทุวิรัตน์, เทคโนโลยีระตัวตน “ชีวมาตร” น่ากลัวหรือไม่, มติชนออนไลน์, สืบค้นเมื่อวันที่ 20 กุมภาพันธ์ 2563 จาก https://www.matichon.co.th/news-monitor/news_1679649
2. ศรัณย์ สัมฤทธิ์เดชขจร, ไบโอเมทริกซ์ (Biometric) คืออะไร, สืบค้นเมื่อวันที่ 13 กุมภาพันธ์ 2563 จาก http://www.hitop.co.th/bio-metric.html
3. การี่ บี. เซลลี่ (Gary B. Shelly), Discovering Computers 2008 A Gateway to Information Web Enhance “Discovering Computers 2006: A Gateway to Information Web Enhanced Introductory” Thomson Course Technology, 2008:263.
4. งานเทคนิคการแพทย์ โรงพยาบาลค่ายบางระจัน, DNA ในการพิสูจน์พ่อ แม่ ลูก, สืบค้นเมื่อวันที่ 13 กุมภาพันธ์ 2563 จาก http://www.govesite.com/labkhai/activities.php?aid=20131113205702WaeJq3q
5. สุพล พรหมมาพันธุ์, การเก็บข้อมูลชีวมาตรของหน่วยงานรัฐกับความเสี่ยงที่อาจมีการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ, วารสาร CIO World & Business, August 2019:60-1.
6. ปริญญา หอมอเนก, สไลด์การประกอบการบรรยายเก็บข้อมูลชีวมาตร (Biometrics) ของหน่วยงานรัฐกับการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ, 2562.
7. สุธี ทุวิรัตน์, ยื่นร้องนายก หวั่นล้วงตับ สแกนใบหน้า, หนังสือพิมพ์ฐานเศรษฐกิจ, หน้า 1 ฉบับที่ 3,495 วันที่ 11-14 สิงหาคม พ.ศ. 2562. สืบค้นเมื่อวันที่ 13 กุมภาพันธ์ 2563 จาก https://www.thansettakij.com/content/407027
8. ทีมข่าวอาชญากรรม, “สตม.โชว์ศักยภาพไบโอเมทริกซ์ 3 วัน จับพาสปอร์ตปลอม 8 ราย” MGR Online สืบค้นเมื่อวันที่ 20 กุมภาพันธ์ 2563 จาก https://mgronline.com/crime/detail/9620000088608

9. สุพาวรรณ์ กุศลครออง, ไบโอเมทริกซ์, สืบค้นเมื่อวันที่ 20 กุมภาพันธ์ 2563 จาก https://sites.google.com/site/bixometrik/bi-xo-metrik
10. Pornaka abeo111, Biometrics Technology, สืบค้นเมื่อวันที่ 21 กุมภาพันธ์ 2563 จาก https://www.bloggang.com/m/viewdiary.php?id=pornaka&group=9