การศึกษารูปแบบการจัดเก็บและบริหารข้อมูลอัตลักษณ์บุคคล เพื่อนำมาประยุกต์ใช้ในศาลยุติธรรม[1]

A Study of the Model of Collecting and Managing Identity Data for Apply in the Courts of Justice[2]

ณัฐณิชา คะชา[3]

คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

2 ถนนพระจันทร์ แขวงพระบรมมหาราชวัง เขตพระนคร กรุงเทพมหานคร 10200, ประเทศไทย

อีเมลติดต่อ: chuleecha.c@coj.go.th

Nuthnicha Cachar[4]

Faculty of Law, Thammasat University

2 Prachan Road, Phra Barom Maha Ratchawang, Phra Nakhon, Bangkok 10200, Thailand

Email: chuleecha.c@coj.go.th

Received: April 18, 2023 **Revised:** July 25, 2023 **Accepted:** August 3, 2023

บทคัดย่อ

บทความนี้ มีวัตถุประสงค์เพื่อวิเคราะห์ความเหมาะสมว่าศาลยุติธรรมควรนำข้อมูลอัตลักษณ์บุคคลที่อยู่ในรูปแบบของเทคโนโลยีไบโอเมตริกมาจัดเก็บ บริหารจัดการ และประยุกต์ใช้งานในส่วนของการระบุตัวตนหรือพิสูจน์และยืนยันตัวตนหรือไม่ ซึ่งหากพิจารณาแล้วเห็นว่าเหมาะสมก็ต้องดำเนินการวิเคราะห์หาแนวทางในการสร้างนวัตกรรมการทำงานแบบใหม่พร้อมทั้งสรรหาเครื่องมือที่จำเป็นเพื่อนำมาใช้สนับสนุนการปฏิบัติงานของทุกหน่วยงานในศาลยุติธรรม

จากการศึกษาพบว่า เทคโนโลยีไบโอเมตริกมีคุณสมบัติที่สามารถใช้ในการระบุตัวตน พิสูจน์ตัวจริงหรือพิสูจน์อัตลักษณ์ได้เป็นอย่างดี ซึ่งเมื่อนำเทคโนโลยีนี้มาประยุกต์ใช้งานจะทำให้ระดับการรักษาความปลอดภัยในการเข้าถึงทรัพยากรต่าง ๆ ขององค์กรมีเพิ่มมากยิ่งขึ้น นอกจากนี้ ยังสามารถนำมาประยุกต์ใช้งานร่วมกับ

---

[1] ได้รับทุนสนับสนุนการศึกษาเต็มจำนวนจากสำนักงานศาลยุติธรรม, ประจำปี 2560.

[2] Full Scholarship from Office of the Judiciary, 2017.

[3] นักวิจัยอิสระด้านกฎหมาย.

[4] Independent Legal Researcher.

การทำงานของศาลยุติธรรมได้อีกหลากหลายด้าน เพื่อให้การปฏิบัติงานของศาลยุติธรรมโดยรวมมีประสิทธิภาพเพิ่มมากขึ้นได้อีกด้วย แต่อย่างไรก็ตาม การนำไปใช้งานควรคำนึงถึงรูปแบบข้อมูลไบโอเมตริกที่เลือกใช้ในแต่ละงานควรมีความเหมาะสมทั้งในด้านคุณสมบัติและราคา รูปแบบและคุณภาพของข้อมูลไบโอเมตริกที่จัดเก็บไว้ต้องเป็นไปตามมาตรฐานสากลเพื่อให้เกิดความแม่นยำเวลาใช้งานและสามารถนำไปเชื่อมโยงเพื่อใช้ประโยชน์ร่วมกับหน่วยงานอื่นได้ ควรมีนโยบายในการบริหารจัดการข้อมูลให้เป็นไปตามกฎหมายหรือระเบียบข้อบังคับที่เกี่ยวข้อง มีระบบบริหารจัดการความเสี่ยงและรักษาความมั่นคงปลอดภัยในการเข้าถึงข้อมูล ควรให้ความรู้ผนวกกับการสร้างจิตสำนึกแก่บุคลากรในองค์กรให้ระมัดระวังการละเมิดข้อมูลส่วนบุคคลหรือสิทธิส่วนบุคคลของผู้อื่น และสุดท้ายคือ ประโยชน์ที่องค์กรได้รับควรมีความคุ้มค่าเมื่อเทียบกับมูลค่าเงินงบประมาณที่ใช้ลงทุน

คำสำคัญ: การจัดเก็บและบริหารข้อมูล; อัตลักษณ์บุคคล; ศาลยุติธรรม

Abstract

The purpose of this article is the Court of Justice should use identity information in the form of biometric technology to store, manage, and apply in the area of identification or identity verification and authentication. If considered appropriate, analysis must be conducted to find approaches to creating innovative work methods, as well as necessary instruments to support operation of all Court of Justice agencies.

The study found that in addition to biometric technology, features may be used to identify, authenticate, and verify identity to boost security levels when accessing different organizational resources. There are also applications in conjunction with other aspects of Court of Justice work, making overall performance more efficient. Yet implementation should specify that biometric data format chosen for each task should cohere with features and price. Stored biometric data format and quality must meet international standards to ensure accuracy at time of use and be linkable for use by other agencies. Policy should manage data according to relevant laws or regulations with a risk management system and data access security. Knowledge should be combined with awareness-raising among organizational personnel to prevent personal data or privacy rights violations. Ultimately, organizational benefits receive should match the investment cost.

Keywords: Collecting and managing data; Identification’; Courts of Justice

1. บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

หลังจากเกิดสถานการณ์การระบาดครั้งใหญ่ของเชื้อไวรัสโคโรนาสายพันธุ์ใหม่ทั่วโลก หรือที่รู้จักกันในชื่อว่า โควิด-19 ตั้งแต่ปลายปี พ.ศ. 2562 จนถึงทุกวันนี้ เป็นเหตุให้ทุกคนจำเป็นต้องเว้นระยะห่างทางสังคมกับบุคคลรอบข้างตามนโยบายป้องกันการแพร่กระจายของโรค อีกทั้งต้องปรับวิธีมีปฏิสัมพันธ์กับผู้อื่นในสังคม จนกระทั่งทุกคนเคยชินและพบข้อดีของการทำธุรกรรมในลักษณะนี้ว่ามีความสะดวกรวดเร็ว ลดค่าใช้จ่ายและเวลา ประชาชนส่วนใหญ่ในปัจจุบันจึงสามารถใช้งานระบบอิเล็กทรอนิกส์ในชีวิตประจำวันได้เป็นอย่างดี ด้วยเหตุนี้ โลกจึงมีนวัตกรรมดิจิทัลแบบใหม่เกิดขึ้นตลอดเวลา เพราะทุกประเทศต่างเร่งพัฒนาศักยภาพด้านเทคโนโลยีของตนเพื่อได้เปรียบในการแข่งขันด้านเศรษฐกิจกับประเทศอื่น รวมถึงมีภาพลักษณ์ของประเทศที่ดีเพื่อดึงดูดประเทศอื่นให้เข้ามาลงทุน

แต่ในบางครั้งหากโชคร้ายระบบก็อาจทำงานผิดพลาดได้ ซึ่งสามารถเกิดขึ้นได้จากหลายสาเหตุ เช่น เกิดจากการวิเคราะห์ออกแบบหรือพัฒนาระบบในส่วนที่เชื่อมต่อกับโครงสร้างหลักของเทคโนโลยีภายในเวลาที่เร่งรีบเกินไปจนเกิดข้อผิดพลาดและทำให้เกิดช่องโหว่ของระบบ หรือการออกแบบลำดับขั้นตอนการใช้งานระบบและการบริหารจัดการข้อมูลยังไม่ดีพอ หรือแม้กระทั่งความผิดพลาดของมนุษย์เนื่องจากผู้ใช้งานบางคนยังไม่คุ้นชินกับการใช้งานหรือไม่มีความรู้ความเข้าใจเกี่ยวกับลักษณะการทำงานของเทคโนโลยีนี้เพียงพอก็อาจเป็นอีกสาเหตุหนึ่งที่มีปริมาณไม่แพ้กัน ในที่นี้ขอยกตัวอย่าง เช่น เทคโนโลยีทางการเงิน (Financial Technology) ปัจจุบันกำลังเป็นที่นิยมอย่างมากเพราะทำให้การโอนเงินหรือธุรกรรมด้านการเงินอื่น ๆ สามารถทำได้อย่างสะดวกรวดเร็วผ่านโทรศัพท์มือถือแบบสมาร์ทโฟนของเจ้าของบัญชี ทำให้ผู้ใช้งานสามารถใช้ชีวิตอย่างสะดวกสบายขึ้นเป็นอย่างมากนั้น หากมองจากมุมของผู้ที่เคยเห็นโครงสร้างการพัฒนาระบบจะเข้าใจดีว่าเบื้องหลังของเทคโนโลยีนี้มีความซับซ้อนเป็นอย่างมาก หากเกิดช่องโหว่ของระบบด้วยสาเหตุใดก็ตามที่กล่าวถึงแล้วข้างต้นก็อาจจะเป็นช่องทางให้มิจฉาชีพฉวยโอกาสนี้เข้าถึงบัญชีเพื่อขโมยเงินหรือทรัพย์สินบนระบบดิจิทัลได้อย่างรวดเร็ว ซึ่งปัจจุบันจะเห็นได้ว่ามิจฉาชีพออนไลน์จะมีการใช้กลวิธีหลากหลายรูปแบบ เช่น การสร้างเว็บไซต์ปลอมวิธีการคือหลอกให้เจ้าของบัญชีกรอกข้อมูลสำคัญลงไปแล้วจึงนำข้อมูลเหล่านั้นไปสวมรอยทำธุรกรรมแทน[5] การแอบดักข้อมูลสำคัญของเจ้าของบัญชีผ่านเครือข่ายคอมพิวเตอร์ปลอมที่มิจฉาชีพสร้างขึ้น หรือกรณีคอลเซ็นเตอร์ (Call Center) ที่หลอกให้ผู้รับสายแจ้งข้อมูลส่วนตัวให้ทราบเพื่อใช้เป็นข้อมูลในการเดารหัสผ่าน จากนั้นจึงให้กดลิงค์ธนาคารปลอมเพื่อแอบติดตั้งโปรแกรม ควบคุมอุปกรณ์จากระยะไกลจนสามารถเข้าถึงโทรศัพท์มือถือของเหยื่อและควบคุมเองได้ เป็นต้น จากปัญหาที่ยกมาเป็นตัวอย่างนี้ จะเห็นได้ว่าเรื่องนี้ไม่ได้กระทบเพียงแค่กลุ่มธุรกิจธนาคารเพียงอย่างเดียว แต่กลับส่งผลกระทบต่อองค์กรอื่นทั้งภาครัฐและเอกชน

[5] บรรณศักดิ์ ยุวมิตร, “Phishing คืออะไร ป้องกันอย่างไร,” แก้ไขครั้งล่าสุด 2564, สืบค้นเมื่อ 13 มิถุนายน 2565, https://www.cyfence.com/article/what-is-phishing/

ในลักษณะเป็นลูกโซ่ซึ่งรวมถึงกระบวนการยุติธรรมด้วย อันจะเห็นได้จากกรณีตัวอย่างข้างต้นนี้ จะทำให้คดีที่เจ้าของบัญชีถูกดูดเงินออกไปจากบัญชียังคงเกิดขึ้นตลอดเวลา ทำให้มีคดียื่นฟ้องต่อศาลแทบทุกวันซึ่งส่งผลให้ทุกหน่วยงานในกระบวนการยุติธรรมจำเป็นต้องปฏิบัติงานหนักขึ้นตามปริมาณคดีที่ไหลเข้าสู่กระบวนการยุติธรรมตลอดเวลา

จากสถานการณ์ที่เกิดขึ้น ทำให้หน่วยงานที่มีภารกิจเกี่ยวข้องกับเรื่องนี้จำเป็นต้องเร่งวิเคราะห์หาสาเหตุและแนวทางแก้ไขปัญหา พร้อมแนวทางที่จะป้องกันปัญหาในอนาคตโดยเร็วที่สุด และสำหรับกรณีนี้ธนาคารแห่งประเทศไทยได้ประกาศนโยบายการดำเนินงานเพื่อรักษาความปลอดภัย ซึ่งก็คือแนวปฏิบัติการใช้เทคโนโลยีชีวิมิติ (Biometric Technology) ในการให้บริการทางการเงิน โดยแจ้งผู้ให้บริการทางการเงินที่อยู่ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทยทุกแห่งต้องดำเนินการเพิ่มระบบการยืนยันตัวตนด้วยใบหน้าตามแนวปฏิบัตินี้ให้แล้วเสร็จโดยเร็วที่สุดเท่าที่จะเป็นไปได้เพื่อป้องกันความสูญเสียที่อาจจะเกิดขึ้นมากไปกว่านี้ โดยการนำเทคโนโลยีไบโอเมตริกมาประยุกต์ใช้เพิ่มเติมนอกเหนือจากการใช้รหัสผ่านแบบเดิมนี้จะเกิดปัจจัยในการยืนยันตัวตนรูปแบบใหม่ที่มิจฉาชีพไม่สามารถเข้าถึงข้อมูลหรือปลอมแปลงได้ วิธีนี้เป็นการใช้หลักการเปรียบเทียบข้อมูลไบโอเมตริก (Biometric Comparison) กับแหล่งข้อมูลที่เชื่อถือได้ (Trusted Source) เช่น ภาพใบหน้าของลูกค้าซึ่งไปยืนยันตัวตนที่สาขาของธนาคารไว้แล้ว หรืออาจใช้ภาพจากบัตรประจำตัวประชาชนหรือหนังสือเดินทางบนแอพลิเคชั่น (Mobile Banking) ซึ่งการที่จะเลือกใช้แหล่งข้อมูลจากที่ใดนั้นจะขึ้นอยู่กับนโยบายของธนาคารแห่งประเทศไทยขณะนั้น[6] โดยขั้นตอนการยืนยันตัวตนด้วยใบหน้าจะปรากฏขึ้นเฉพาะในกรณีที่ลูกค้าต้องการขอเปิดบัญชี หรือเจ้าของบัญชีประสงค์จะทำรายการโอนเงินมากกว่า 50,000 บาทต่อ 1 รายการ หรือมูลค่ารวมกันทุก ๆ 200,000 บาท ในรอบระยะเวลา 1 วัน หรือการขอปรับเพิ่มวงเงินทำธุรกรรมต่อวันให้โอนได้เกินกว่า 50,000 บาท ผ่านสมาร์ทโฟน[7] และถ้าหากจะยกตัวอย่างที่ใกล้ตัวที่สุด ก็คงจะหนีไม่พ้นการยืนยันตัวตนเพื่อเข้าใช้งานสมาร์ทโฟนของทุกคนนั่นเอง จากประโยชน์ซึ่งสามารถเห็นได้ชัดเจนนี้ ทำให้เทคโนโลยีไบโอเมตริกเป็นที่ยอมรับว่ามีประโยชน์อย่างมากและนำมาประยุกต์ใช้กับระบบต่าง ๆ ได้หลากหลายวิธี

ดังนั้น เมื่อกล่าวถึงการนำไบโอเมตริกมาประยุกต์ใช้งานในกระบวนการยุติธรรมนั้น เป็นที่ทราบกันดีว่ามีหลายหน่วยงานที่ใช้งานไบโอเมตริกผ่านมุมมองของนักนิติวิทยาศาสตร์มาเป็นระยะเวลานานแล้ว เนื่องด้วยคุณสมบัติที่มีความเป็นเอกลักษณ์และสามารถชี้ไปถึงตัวบุคคลที่เป็นเจ้าของอัตลักษณ์ได้ด้วยหลักการทางวิทยาศาสตร์ ทำให้หน่วยงานของรัฐหลายแห่งที่มีภารกิจหลักในการสืบหา หรือยืนยันตัวบุคคลสามารถใช้ข้อมูลไบโอเมตริกที่เก็บได้จากสถานที่เกิดเหตุหรือที่ปรากฏอยู่ในเอกสารประจำตัวที่ค้นได้จากตัวของผู้ต้องสงสัยเป็นข้อมูลสำคัญในการปฏิบัติงานได้เช่นกัน ซึ่งข้อมูลที่ได้นี้อาจเป็นลายนิ้วมือ หรือภาพใบหน้าที่ได้จากกล้องวงจรปิดภายในบริเวณนั้นก็ได้ แต่หากเมื่อได้กล่าวถึงศาลยุติธรรมซึ่งถือว่าเป็นองค์กรสำคัญของกระบวนการยุติธรรมนั้น จากประสบการณ์ทำงานของผู้เขียนตลอดระยะเวลาที่ผ่านมาเห็นว่าศาลยุติธรรมยังไม่มีการจัดเก็บและนำข้อมูล

[6] ธนาคารแห่งประเทศไทย, “แนวปฏิบัติการใช้เทคโนโลยีชีวมิติในการให้บริการทางการเงิน,” แก้ไขครั้งล่าสุด 2563, สืบค้นเมื่อ 29 สิงหาคม 2563, https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2563/ThaiPDF/25630177.pdf/

[7] ธนาคารแห่งประเทศไทย, “คำถาม-คำตอบ เรื่อง มาตรการจัดการภัยทุจริตทางการเงินของ ธปท.,” แก้ไขครั้งล่าสุด 2566, สืบค้นเมื่อ 12 เมษายน 2566, https://www.bot.or.th/content/dam/bot/documents/th/news-and-media/news/2023/QA_n1066t.pdf/

ดังกล่าวมาประยุกต์ใช้เพื่อสนับสนุนการพิจารณาพิพากษาคดีอย่างเป็นรูปธรรมและเป็นมาตรฐานเดียวกันทั่วประเทศ หรือหากใช้ก็เป็นเพียงบางศาลที่มีเขตอำนาจใกล้กับชายแดน โดยมีวัตถุประสงค์เพื่อพิสูจน์ตัวตนของผู้ต้องหาหรือจำเลยที่เป็นบุคคลต่างด้าว และใช้งานได้เพียงในศาลของตนเท่านั้น ดังนั้นหากศาลยุติธรรมมีฐานข้อมูลไบโอเมตริกซึ่งอาจเกิดจากการจัดเก็บขึ้นใหม่เอง หรือเชื่อมโยงข้อมูลกับหน่วยงานอื่นแล้วจะสามารถนำมาประยุกต์ใช้ให้เกิดประโยชน์ได้จริงหรือไม่

กรณีศึกษาที่จะยกขึ้นมาต่อไปนี้เป็นเหตุการณ์ที่เกิดขึ้นจริง คือการจับฝาแฝดผิดตัว คดีนี้เกิดขึ้นเมื่อ พ.ศ. 2555 โดยตำรวจได้รับการร้องเรียนจากมารดาของฝาแฝดทั้งสองว่าตำรวจดำเนินคดีผิดคน ซึ่งเรื่องนี้เริ่มมาจากการที่ตำรวจได้จับกุมบุตรชายที่เป็นแฝดผู้น้องในข้อหาทำร้ายร่างกายผู้อื่นจนบาดเจ็บสาหัส แต่แท้ที่จริงแล้วผู้ที่ก่อคดีคือแฝดผู้พี่ ขณะนั้นแฝดผู้น้องต้องถูกคุมขังแทนแฝดผู้พี่นานกว่าหนึ่งปี และถึงแม้ในภายหลังมารดาจะนำแฝดผู้พี่เข้ามอบตัวแล้ว ตำรวจก็ไม่ได้รับตัวไว้ โดยอ้างว่าคดีความนี้ได้ล่วงเลยมาจนกระทั่งศาลมีคำพิพากษาให้จำคุกเป็นเวลา 4 ปี เรียบร้อยแล้ว ดังนั้นหลังจากที่กรณีดังกล่าวถูกเผยแพร่ผ่านสื่อมวลชน ประกอบกับพนักงานสอบสวนเจ้าของคดีได้ชี้แจงภายหลังว่า ตนได้ทำการสอบสวนแฝดผู้น้องแล้ว ขณะนั้นเขายอมรับว่าเขาคือแฝดผู้พี่รวมถึงมีใบประกันสังคมของแฝดผู้พี่ติดตัวเขาอยู่ในวันที่เข้าจับกุม ทำให้พนักงานสอบสวนเข้าใจว่าจับกุมผู้ต้องหาถูกคนแล้ว และพนักงานสอบสวนได้ส่งใบประกันสังคมให้อัยการเพื่อเป็นหลักฐานประกอบการสั่งฟ้อง แต่ไม่ได้มีการตรวจสอบลายนิ้วมือผู้ต้องหาเพื่อเปรียบเทียบ ทำให้เกิดเสียงวิพากษ์วิจารณ์ถึงความหละหลวมในการปฏิบัติหน้าที่ของตำรวจ รวมไปถึงตั้งคำถามถึงความเชื่อมั่นในกระบวนการยุติธรรมทั้งระบบ ด้วยสาเหตุนี้เองภายหลังจากที่ผู้บัญชาการตำรวจแห่งชาติในขณะนั้นได้สั่งให้มีการตรวจเปรียบเทียบอัตลักษณ์บุคคลอีกครั้ง พบว่า ลายพิมพ์นิ้วมือที่หัวแม่มือขวาของแฝดคนที่กำลังถูกคุมขังอยู่ในเรือนจำ เมื่อเทียบกับข้อมูลลายพิมพ์นิ้วมือของแฝดผู้น้องจากทะเบียนราษฎรของกรมการปกครองแล้วนั้น ผลการตรวจสอบพบว่า ลักษณะของลายนิ้วมือที่ได้จากตัวจำเลยในเรือนจำ มีลักษณะพิเศษตรงกับลายพิมพ์นิ้วมือที่ระบุชื่อของน้องชายฝาแฝดถึง 15 จุด แต่ไม่ตรงกับลายพิมพ์นิ้วมือที่ระบุชื่อของพี่ชายฝาแฝด จึงทำให้ยืนยันได้ว่า บุคคลที่ถูกคุมขังในเรือนจำในขณะนั้นคือน้องชายฝาแฝด ไม่ใช่พี่ชายฝาแฝดที่ก่อคดีตัวจริง[8] จากกรณีที่เกิดขึ้นนี้ หากพนักงานสอบสวนปฏิบัติตามขั้นตอนเพื่อพิสูจน์อัตลักษณ์เสียก่อน หรือหากศาลยุติธรรมสามารถตรวจสอบอัตลักษณ์บุคคลระหว่างกระบวนการพิจารณาคดีได้ ก็อาจลดโอกาสผิดพลาดที่จะทำให้เกิดจุดด่างพร้อยบนภาพลักษณ์ของกระบวนการยุติธรรมและแก้ไขปัญหาได้เร็วกว่านี้ กรณีนี้จึงกลายเป็นประเด็นที่ทำให้ผู้เขียนมีความสนใจ และเป็นที่มาของการศึกษาเพื่อหาแนวทางในการนำไบโอเมตริกมาประยุกต์ใช้ให้เกิดประโยชน์ต่อศาลยุติธรรมของประเทศไทย

ซึ่งคำว่า “ไบโอเมตริก” นั้นเป็นการนำเทคโนโลยีด้านชีวภาพผนวกเข้ากับความรู้ทางการแพทย์และคอมพิวเตอร์เข้าด้วยกัน โดยใช้คุณลักษณะทางสรีรวิทยาหรือคุณลักษณะทางพฤติกรรมของแต่ละบุคคลซึ่งมีความเป็นเอกลักษณ์และสามารถเทียบวัดหรือนับออกมาเป็นจำนวนได้มาผนวกเข้ากับหลักการทางสถิติเพื่อใช้ในการจดจำบุคคล หรือจำแนกแต่ละบุคคลออกจากกัน ซึ่งคำศัพท์อื่นที่มีความหมายเดียวกันหรือ

[8] ทีมข่าวรายงานพิเศษ, “คลี่ปมปริศนา: ไขคดีจับแฝดผิดตัว,” คอลัมน์ ข่าวอาชญากรรม, *คมชัดลึก*, 14 กรกฎาคม 2556, สืบค้นเมื่อ 1 พฤษภาคม 2561, http://www.komchadluek.net/news/crime/163380/

ใกล้เคียงมากกับคำว่าไบโอเมตริกนี้สามารถพบเห็นจากบทความอื่น ๆ โดยทั่วไปได้อีกหลายคำ ยกตัวอย่างเช่น คุณลักษณะทางชีวมิติ ข้อมูลทางชีวภาพ หรือข้อมูลอัตลักษณ์บุคคล เป็นต้น แต่ในบทความนี้จะใช้คำว่า ไบโอเมตริก เพื่อความเข้าใจที่ตรงกันทั้งบทความ

ในการพิสูจน์ความเป็นตัวตนด้วยเทคโนโลยีไบโอเมตริกในมนุษย์นั้นจะใช้วิธีตรวจสอบจากสิ่งที่มีเอกลักษณ์หรือลักษณะเฉพาะที่ชัดเจนและสามารถบ่งบอกความเป็นตัวตนของผู้นั้นได้ โดยลักษณะเฉพาะสามารถแบ่งออกได้สองรูปแบบ ได้แก่ ลักษณะเฉพาะทางกายภาพหรือสรีรวิทยา (Physiological Biometrics) เป็นสิ่งที่สามารถวัดได้โดยตรงจากส่วนต่าง ๆ ทั้งภายในและภายนอกของร่างกายของมนุษย์ อาทิ ใบหน้า (Facial) ม่านตา (Iris) ลายนิ้วมือ (Fingerprint) ลักษณะฝ่ามือ (Hand Geometry) เส้นเลือดในนิ้ว ในมือ หรือในแขน (Finger Vein, Hand Vein or Arm Vein) จอรับภาพ (Retina) หรือลักษณะเส้นเลือดในลูกตา (Eye vein) ใบหู (Ear) ลักษณะรูปแบบอุณหภูมิของใบหน้า (Thermal Face) ลักษณะของฟัน (Dental Characteristic) กลิ่นกาย (Body Odor) และ ดีเอ็นเอ (DNA) และลักษณะเฉพาะทางพฤติกรรม (Behavioral Characteristics) เป็นสิ่งที่สามารถวัดได้จากลักษณะทางพฤติกรรมหรือการกระทำของแต่ละบุคคล เช่น เสียง (Voice) การกดแป้นพิมพ์หรือวิธีใช้เมาส์ (Mouse Activity or Key Stroke Movement) การเดิน (Gait) หรือการลงลายมือชื่อ (Signature) เป็นต้น ดังนั้นจุดเด่นของเทคโนโลยีไบโอเมตริกคือการที่สามารถยืนยันได้ว่าบุคคลนี้เป็นตัวจริงหรือไม่ (Verification) หรือสามารถระบุได้ว่าบุคคลคนนี้คือใคร (Identification) โดยไบโอเมตริกทุกแบบมีหลักการทำงานพื้นฐาน 5 ขั้นตอน ดังนี้ 1) การรวบรวมข้อมูลไบโอเมตริก (Capture) เป็นขั้นตอนการรวบรวมอัตลักษณ์ของบุคคลด้วยอุปกรณ์รับข้อมูล (Sensor) และแปลงให้อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์เพื่อให้ได้มาซึ่งข้อมูลไบโอเมตริกตั้งต้น เช่น การรวบรวมภาพใบหน้าด้วยกล้องดิจิทัล จากนั้นคัดแยกเฉพาะส่วนที่เป็นใบหน้าออกจากภาพพื้นหลังแล้วปรับความเอียง แสงเงา ให้เหมาะสมกับการนำไปประมวลอัตลักษณ์, 2) การประมวลอัตลักษณ์ (Signal Processing) เป็นขั้นตอนการประมวลข้อมูลไบโอเมตริกตั้งต้นให้กลายเป็นข้อมูลไบโอเมตริกอ้างอิงเพื่อให้พร้อมต่อการนำไปเปรียบเทียบกับข้อมูลไบโอเมตริกที่ต้องการพิสูจน์หรือยืนยัน โดยข้อมูลไบโอเมตริกที่ผ่านขั้นตอนนี้แล้วจะไม่สามารถแปลงกลับไปเป็นข้อมูลไบโอเมตริกตั้งต้นได้ เช่น การประมวลผลภาพใบหน้าจะเริ่มจากการค้นหาดวงตาของมนุษย์ก่อน จากนั้นจะตรวจจับจุดสังเกตบนใบหน้า เช่น คิ้ว ปาก จมูก รูจมูก และม่านตา เมื่อระบบสรุปว่าพบบริเวณใบหน้าแล้ว ก็จะทำการคำนวณจากระยะห่างระหว่างจุดสังเกตสำคัญจำนวนมากเพื่อหาลักษณะเฉพาะที่สำคัญและเป็นเอกลักษณ์ เช่น ดวงตา หางคิ้ว ความกว้างริมฝีปาก หากเป็นลายนิ้วมือก็จะใช้จุดสังเกตบนลายนิ้วมือ (Minutiae), 3) การเก็บข้อมูล (Data storage) เป็นขั้นตอนการจัดเก็บข้อมูลไบโอเมตริกอ้างอิงไว้ในระบบจัดเก็บและเชื่อมโยงเข้ากับข้อมูลอื่นของเจ้าของข้อมูล เช่น ชื่อ-นามสกุล เลขประจำตัวประชาชน, 4) การเปรียบเทียบอัตลักษณ์ (Comparison) เป็นขั้นตอนการเปรียบเทียบระหว่างข้อมูลไบโอเมตริกที่ต้องการระบุ พิสูจน์ หรือยืนยันตัวตน กับข้อมูลไบโอเมตริกอ้างอิงที่เก็บไว้ภายในองค์กรหรือแหล่งข้อมูลที่เชื่อถือได้ โดยแสดงผลการเปรียบเทียบเป็นระดับความเชื่อมั่นการเป็นบุคคลเดียวกัน ซึ่งมีการใช้งานใน 2 ลักษณะ คือ การระบุตัวตน (Identification) คือ การนำข้อมูลไบโอเมตริกของบุคคลมาเปรียบเทียบตัวบุคคลกับข้อมูลไบโอเมตริกอ้างอิงที่บุคคลนั้นได้ลงทะเบียนไว้ และบันทึกอยู่ในระบบจัดเก็บแล้ว ซึ่งเป็นขั้นตอนที่ผู้ขอใช้งานต้องแสดงตัวตน เพื่อระบุว่าตนเองเป็นบุคคลที่มีข้อมูลอยู่ในระบบจัดเก็บข้อมูลนี้หรือไม่ ซึ่งจะมีการเปรียบเทียบในลักษณะ 1: เอ็น คอมแพชั่น (One to Many Matching Process) คือ การหาบุคคลนี้

จำนวน 1 คน จากในฐานข้อมูลทั้งหมดจำนวนคน และการพิสูจน์อัตลักษณ์หรือการยืนยันตัวตน (Authentication) คือ การนำข้อมูลไบโอเมตริกของบุคคลมาเปรียบเทียบกับแหล่งข้อมูลที่เชื่อถือได้ เพื่อพิสูจน์และยืนยันว่าเป็นบุคคลนั้นตามที่อ้างถึงจริงหรือไม่ เช่น กระบวนการรู้จักผู้ใช้บริการ (KYC) ในการเปิดบัญชีเงินฝากเป็นการเปรียบเทียบข้อมูลไบโอเมตริกที่ได้จากการถ่ายภาพคนที่กำลังทำธุรกรรมในเวลานี้ทันที กับข้อมูลไบโอเมตริกอ้างอิงแบบรูปใบหน้าที่บันทึกไว้ในบัตรประจำตัวประชาชน ซึ่งจะมีลักษณะแบบ 1 ต่อ 1 คือ จะเริ่มจากการค้นหาจากชื่อ-สกุลหรือเลขบัตรประจำตัวประชาชนที่ตรงกันก่อน เมื่อพบแล้วจึงเปรียบเทียบข้อมูลลักษณะบนใบหน้าจากทั้งสองรูปว่าคนที่กำลังขอทำรายการธุรกรรมในเวลานี้คือนายบี ทดสอบ จริงหรือไม่ โดยชื่อ-สกุล เลขบัตรประจำตัวประชาชน หรือรูปใบหน้า ล้วนแล้วแต่เป็นปัจจัยที่ใช้ในการยืนยันตัวตน และ 5) การตัดสินใจ (Decision) เป็นขั้นตอนสุดท้ายที่จะแสดงผลลัพธ์จากการเปรียบเทียบอัตลักษณ์ของบุคคล โดยเปรียบเทียบค่าคะแนนความเชื่อมั่นที่ยอมรับได้ (Threshold) กับค่าคะแนนความเชื่อมั่นจากการเปรียบเทียบอัตลักษณ์ของบุคคล เพื่อตัดสินใจว่าเป็นบุคคลนั้นจริงหรือไม่[9]

1.2 วัตถุประสงค์

1.2.1 เพื่อให้เข้าใจถึงลักษณะของอุปกรณ์รับสัญญาณ (Sensor) หลักการทำงานของเทคโนโลยี ข้อดีและข้อด้อยของเทคโนโลยีไบโอเมตริกแต่ละแบบที่นิยมใช้งานในปัจจุบัน และทราบว่าปัจจุบันมีการนำไบโอเมตริกไปประยุกต์ใช้ในหน่วยงานภาครัฐ ณ ต่างประเทศและประเทศไทยอย่างไรบ้าง ทั้งในด้านของการใช้งานทั่วไป ตลอดจนด้านที่เกี่ยวข้องกับกระบวนการยุติธรรม

1.2.2 เพื่อให้ตระหนักถึงอุปสรรคหรือข้อจำกัดด้านต่าง ๆ ของการประยุกต์ใช้ไบโอเมตริกในระบบจัดเก็บข้อมูลอัตลักษณ์บุคคลที่ใช้ในหน่วยงานภาครัฐของต่างประเทศและประเทศไทย และนำมาวิเคราะห์เพื่อป้องกันหรือแก้ไขปัญหาข้อขัดข้องต่อไป

1.2.3 เพื่อสร้างแนวทางในการนำเทคโนโลยีไบโอเมตริกมาประยุกต์ใช้งานภายในศาลยุติธรรม โดยแบ่งออกเป็น การใช้งานใช้ร่วมกับระบบงานศาลอิเล็กทรอนิกส์ (E-Court) ในด้านที่เกี่ยวกับพิจารณาพิพากษาคดี และการประยุกต์ใช้ร่วมกับระบบบริหารสำนักงานอิเล็กทรอนิกส์ (E-Office) ในด้านที่เกี่ยวกับงานธุรการ

1.2.4 เพื่อสร้างแนวทางรองรับการเชื่อมโยงข้อมูลอัตลักษณ์บุคคลของศาลยุติธรรมกับหน่วยงานอื่นในกระบวนการยุติธรรม กรณีที่หน่วยงานมีข้อตกลงร่วมกัน

1.3 ขอบเขตการวิจัย

การศึกษานี้ มุ่งศึกษาวิเคราะห์ให้เข้าใจในลักษณะและหลักการทำงานของเทคโนโลยีไบโอเมตริกแต่ละรูปแบบที่นิยมใช้งานในปัจจุบัน เพื่อให้ทราบถึงข้อดีและข้อด้อยของเทคโนโลยีแต่ละรูปแบบและสามารถเลือกใช้เทคโนโลยีรูปแบบที่เหมาะสมกับสภาพแวดล้อมของโครงการที่จะจัดทำได้ จากนั้นจึงค้นคว้าหาข้อมูลเพื่อเป็นกรณีศึกษาเกี่ยวกับโครงการที่มีการจัดเก็บข้อมูลอัตลักษณ์บุคคลโดยใช้เทคโนโลยีไบโอเมตริกในหน่วยงานภาครัฐทั้งของต่างประเทศและในประเทศไทย โดยเฉพาะอย่างยิ่งระบบที่เป็นของหน่วยงานในกระบวนการยุติธรรม

[9] ธนาคารแห่งประเทศไทย, “คำถาม-คำตอบ เรื่อง มาตรการจัดการภัยทุจริตทางการเงินของ ธปท.,” แก้ไขครั้งล่าสุด 2566, สืบค้นเมื่อ 12 เมษายน 2566, https://www.bot.or.th/content/dam/bot/documents/th/news-and-media/news/2023/QA_n1066t.pdf/

1.4 ระเบียบวิธีวิจัย หรือวิธีการศึกษา

การศึกษานี้ เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) ใช้วิธีเชิงพรรณนา (Descriptive Research) โดยดำเนินการวิจัยจากการค้นคว้าเอกสาร (Documentary Research) เพื่อหาหลักการ แนวคิด และทฤษฎีที่เกี่ยวข้องจากแหล่งข้อมูลทุติยภูมิ (Secondary Data) ได้แก่ หนังสือ บทความ กฎหมาย เอกสารประกอบการประชุมหรือสัมมนา งานวิจัยต่างๆ ที่เกี่ยวข้อง ทั้งรูปเล่มและแบบออนไลน์ ศึกษาการใช้งานไบโอเมตริกและกฎหมายที่เกี่ยวข้องขององค์กรต่าง ๆ ทั้งต่างประเทศและประเทศไทย

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ทราบถึงหลักการทำงาน ลักษณะเฉพาะ ข้อดีและข้อด้อย ประโยชน์และข้อควรระวังในการใช้งานเทคโนโลยีไบโอเมตริกแต่ละรูปแบบที่มีอยู่ในปัจจุบัน รวมถึงสามารถวิเคราะห์ออกแบบแนวทางการนำเทคโนโลยีไบโอเมตริกมาประยุกต์ใช้เพื่อสนับสนุนการปฏิบัติงานของศาลยุติธรรม

1.5.2 ทราบถึงความสำคัญของสิทธิส่วนบุคคลหรือความกังวลของประชาชนในสังคมที่มีต่อการถูกละเมิดข้อมูลส่วนบุคคลจากหน่วยงานภาครัฐในประเทศของตนเอง ส่งผลให้เกิดความระมัดระวังในการวิเคราะห์ออกแบบโครงการหรือระบบต่าง ๆ ด้วยความรอบคอบอยู่เสมอ ทั้งนี้ เพื่อไม่ให้เกิดการละเมิดสิทธิของบุคคลหรือเป็นเหตุให้ประชาชนในสังคมเกิดความกังวล อันจะเป็นการทำลายภาพลักษณ์ที่ดีของศาลยุติธรรม

1.5.3 ศาลยุติธรรมมีแนวทางการจัดเก็บข้อมูลอัตลักษณ์บุคคลด้วยเทคโนโลยีไบโอเมตริกมาประยุกต์ใช้กับภารกิจของของศาลยุติธรรมที่ปลอดภัยและมีประสิทธิภาพ ทั้งในด้านที่สนับสนุนการปฏิบัติงานธุรการของหน่วยงาน และด้านที่เกี่ยวข้องกับกระบวนการพิจารณาพิพากษาคดีของศาลยุติธรรม

2. ผลการศึกษาวิจัย

จากการศึกษาเรื่องการศึกษารูปแบบการจัดเก็บและบริหารข้อมูลอัตลักษณ์บุคคลเพื่อนำมาประยุกต์ใช้ในศาลยุติธรรม พบประเด็นดังต่อไปนี้

2.1 แนวคิดในการนำข้อมูลอัตลักษณ์บุคคลที่อยู่ในรูปแบบไบโอเมตริกมาประยุกต์ใช้งานเพื่อสนับสนุนกระบวนการพิจารณาพิพากษาคดีของศาลยุติธรรมในประเทศไทย

2.1.1 การพัฒนาระบบบริหารและระบุอัตลักษณ์บุคคลตามหมายจับของศาลยุติธรรมด้วยระบบรู้จำ ไบโอเมตริกอัตโนมัติ เพื่อสนับสนุนการปฏิบัติงานของเจ้าพนักงานตำรวจศาล

เจ้าพนักงานตำรวจศาล (Court Marshal) มีอำนาจหน้าที่ในการรักษาความปลอดภัยและคุ้มครองข้าราชการฝ่ายตุลาการศาลยุติธรรม รวมถึงติดตามจับกุมผู้ต้องหาหรือจำเลยที่ได้รับการปล่อยตัวชั่วคราว แล้วหลบหนีหรือผู้ที่ไม่ปฏิบัติตามหมายเรียกหรือคำสั่งศาล[10] และปฏิบัติงานร่วมกับตำรวจในการดำเนินการจับกุมเพื่อเข้าสู่กระบวนการศาล[11] ดังนั้นเพื่อให้เจ้าพนักงานตำรวจศาลติดตามจับกุมกลุ่มคนดังกล่าวได้สะดวกยิ่งขึ้น

[10] ศูนย์รักษาความปลอดภัย สำนักงานศาลยุติธรรม, “มารู้จักเจ้าพนักงานตำรวจศาลกันเถอะ,” แก้ไขครั้งล่าสุด 2563, สืบค้นเมื่อ 20 กรกฎาคม 2563, https://ojso.coj.go.th/th/content/category/detail/id/45/iid/198955/

[11] สำนักกฎหมายและวิชาการศาลยุติธรรม สำนักงานศาลยุติธรรม, “รายงานสรุปผลการรับฟังความคิดเห็นในการประเมินผลสัมฤทธิ์พระราชบัญญัติเจ้าพนักงานตำรวจศาล พ.ศ. 2562,” แก้ไขครั้งล่าสุด 2565, สืบค้นเมื่อ 3 ธันวาคม 2565, https://law survey.coj.go.th/Documents/result043.pdf/

ผู้เขียนจึงมีแนวคิดจัดทำโครงการพัฒนาระบบบริหารและระบุอัตลักษณ์บุคคลตามหมายจับของศาลยุติธรรมด้วยระบบรู้จำไบโอเมตริกอัตโนมัติ โดยระบบดังกล่าวจะจัดเก็บข้อมูลของผู้มีหมายจับสองส่วนได้แก่ ส่วนข้อมูลพื้นฐาน (Identity) อันได้แก่ ชื่อ นามสกุล หมายเลขบัตรประชาชน วันเดือนปีเกิด และอื่น ๆ เป็นต้น และส่วนของข้อมูลไบโอเมตริก คือ ลายนิ้วมือ และรูปใบหน้า ซึ่งแหล่งที่มาของข้อมูลไบโอเมตริกที่จะใช้ในระบบนั้นศาลอาจเป็นผู้จัดเก็บเอง หรือเชื่อมโยงข้อมูลจากหน่วยงานอื่นที่มีข้อมูลเก็บไว้แล้วก็ได้ เช่น กองทะเบียนประวัติอาชญากร สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ เพื่อให้ลดขั้นตอนปฏิบัติงาน แต่อย่างไรก็ตามหากศาลประสงค์จะจัดเก็บเองศาลควรมีการจัดทำข้อบังคับประธานศาลฎีกาเพื่อกำหนดแนวปฏิบัติให้ชัดเจนและเป็นไปในทางเดียวกันทุกศาล เช่น ให้เจ้าหน้าที่จัดเก็บข้อมูลเมื่อศาลมีคำสั่งอนุญาตให้ปล่อยชั่วคราว และจัดเก็บตามขั้นตอนที่ระบุไว้ ซึ่งขั้นตอนการจัดเก็บหรือการวัดคุณภาพของข้อมูลควรอ้างอิงตามข้อเสนอแนะมาตรฐานของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ส่วนวิธีการนำไปใช้นั้น อาจศึกษาแนวปฏิบัติทั้งจากต่างประเทศและในประเทศ เช่น กองพิสูจน์หลักฐานกลางและศูนย์พิสูจน์หลักฐาน 1-10 ของกองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ เพื่อวิเคราะห์หาแนวทางที่เหมาะสมกับการปฏิบัติงานของเจ้าพนักงานตำรวจศาลต่อไป

2.1.2 การพิสูจน์ตัวผู้ต้องหาหรือจำเลยว่าเป็นบุคคลเดียวกับที่หน่วยงานอื่นส่งตัวมายังศาล

สืบเนื่องมาจากประเด็นของการจับแฝดผิดคนก่อนหน้านี้ การพิสูจน์อัตลักษณ์ของผู้ต้องหาหรือจำเลยว่าเป็นบุคคลเดียวกับที่ตำรวจหรืออัยการส่งมาในคดีอาญานั้น ๆ หรือไม่นั้น เป็นสิ่งที่ทำได้ เนื่องจากตำรวจมีข้อมูลอัตลักษณ์บุคคลที่เป็นลายนิ้วมือพร้อมรูปถ่ายของจำเลยอยู่แล้ว ส่วนวิธีการอาจใช้การเชื่อมโยงข้อมูลสำหรับพิสูจน์อัตลักษณ์ของจำเลยว่าบุคคลที่อัยการสั่งฟ้องนั้นเป็นบุคคลในคดีจริง ประกอบกับกองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ ได้มีการจัดซื้อจัดจ้างโครงการขยายและพัฒนาระบบตรวจสอบลายพิมพ์นิ้วมืออัตโนมัติ (Automatic Fingerprint Identification System: AFIS) โดยมีวัตถุประสงค์ที่จะพัฒนาและปรับปรุงระบบให้ดีขึ้น รองรับปริมาณข้อมูลเพิ่มขึ้น รวมถึงมีแนวคิดที่จะเก็บภาพใบหน้าและม่านตาเพิ่มเติมอีกทั้งยังมีหัวข้อการพัฒนาระบบเชื่อมโยงเพื่อรองรับการเชื่อมโยงกับหน่วยงานภายนอก จากขอบเขตโดยละเอียดของงาน (TOR) จะเห็นได้ว่ามีโอกาสเป็นไปได้ที่กระบวนการยุติธรรมจะสามารถใช้ข้อมูลไบโอเมตริกร่วมกับกองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติในอนาคต

2.1.3 การพิสูจน์ตัวตนของจำเลยในคดีอาญาที่ต้องโทษประหารชีวิต

ตามระเบียบกระทรวงยุติธรรมว่าด้วยหลักเกณฑ์และวิธีการประหารชีวิตนักโทษ พ.ศ. 2546 ข้อ 5 ได้แจ้งวิธีพิสูจน์ตัวตนของจำเลยในคดีอาญาที่กำลังจะประหารชีวิตไว้ว่า ให้เรือนจำถ่ายรูปพร้อมบันทึกข้อมูลและตำหนิรูปพรรณของจำเลยไว้ รวมถึงจัดทำแผ่นพิมพ์ลายนิ้วมือของจำเลย แล้วให้ส่งรูปถ่ายไปยังผู้พิพากษาตัดสินเพื่อยืนยันว่าเป็นรูปถ่ายของจำเลยซึ่งต้องประหารชีวิตจริงพร้อมลงนามรับรองรูปถ่ายไว้ที่ด้านหน้าของรูปถ่ายทุกรูปก่อนส่งคืนกรมราชทัณฑ์เพื่อเตรียมการประหารชีวิตบุคคลนั้นต่อไป ซึ่งในความเป็นจริงแล้วมีโอกาสน้อยนักที่ผู้พิพากษาซึ่งพิจารณาคดีในศาลชั้นต้นจะสามารถจดจำใบหน้าจำเลยได้ เพราะกระบวนการจนถึงชั้นฎีกาจนถึงการขอพระราชทานอภัยโทษจะใช้เวลาหลายปี หากเมื่อถึงเวลาแล้วผู้พิพากษาที่ตัดสินไม่รับรองภาพถ่ายบุคคลนั้นกระบวนการจะเป็นอย่างไรต่อไป ดังนี้แล้ว แนวทางการแก้ไขปัญหานี้ควรเริ่มด้วย

กระบวนการจัดเก็บข้อมูลจำเลยทันทีที่ศาลชั้นต้นอ่านคำพิพากษาของศาลชั้นต้นให้จำเลยมีโทษประหารชีวิต โดยให้ถ่ายรูปจำเลย จัดทำแผ่นพิมพ์ลายนิ้วมือหรือเก็บข้อมูลด้วยวิธีอื่น รวมทั้งจัดทำบันทึกประวัติและตำหนิรูปพรรณไว้ และควรมีการจัดทำข้อบังคับประธานศาลฎีกาเพื่อสร้างแนวปฏิบัติในเรื่องดังกล่าวที่ชัดเจน

2.2 ตัวอย่างแนวคิดในการนำข้อมูลอัตลักษณ์บุคคลที่อยู่ในรูปแบบไบโอเมตริกมาประยุกต์ใช้เพื่อสนับสนุนงานธุรการของศาลยุติธรรมในประเทศไทย

2.2.1 การเพิ่มฟังก์ชั่นในแอปพลิเคชันโทรศัพท์มือถือ (Mobile Application) ของศาลยุติธรรมให้เข้าใช้งานด้วยไบโอเมตริกได้

หากศาลยุติธรรมพัฒนาแอปพลิเคชันโทรศัพท์มือถือ (Mobile Application) ที่ให้บริการประชาชนหรือบุคลากรภายในหน่วยงานเพิ่มเติม โดยนำข้อมูลไบโอเมตริกไปใช้ในการยืนยันตัวตนเพื่อเข้าใช้งานแทนการพิมพ์ชื่อผู้ใช้งานและรหัสผ่าน โดยผูกแอปพลิเคชัน (Application) ที่ติดตั้งบนโทรศัพท์มือถือกับข้อมูลลายนิ้วมือ ม่านตา หรือใบหน้า ที่เก็บไว้แล้วบนโทรศัพท์มือถือของแต่ละคนจะทำให้เข้าถึงข้อมูลได้สะดวกรวดเร็วยิ่งขึ้น ไม่จำเป็นต้องเข้าใช้งานด้วยรหัสผ่านที่ยาวและยุ่งยาก

2.2.2 การใช้ข้อมูลไบโอเมตริกในการรับส่งไฟล์เอกสารที่ต้องรักษาความลับ

ในศาลยุติธรรมมีการรับส่งไฟล์ที่ข้อมูลเป็นความลับอยู่หลายแบบและส่งไปมาหลายขั้นตอน เช่น ข้อมูลร่างคำพิพากษา หรือคำสั่งของศาลสูง หรือร่างคำพิพากษาหรือคำสั่งที่ต้องส่งตรวจตามระเบียบราชการฝ่ายตุลาการศาลยุติธรรม ว่าด้วยการรายงานคดีสำคัญในศาลชั้นต้นและศาลชั้นอุทธรณ์ต่อประธานศาลฎีกา และการรายงานคดีและการตรวจสำนวนคดีในสำนักงานอธิบดีผู้พิพากษาภาค พ.ศ. 2562 เป็นต้น จึงควรมีโครงการพัฒนาระบบรับส่งไฟล์ร่างคำพิพากษาหรือคำสั่งแบบอิเล็กทรอนิกส์ ที่สามารถเข้ารหัส ถอดรหัส และรับหรือส่งไฟล์ได้ด้วยการใช้ไบโอเมตริกยืนยัน เพื่อให้มีหลักฐานว่ามีผู้รับและส่งเมื่อวันและเวลาใด พร้อมประทับวัน เวลา และเวอร์ชั่นของไฟล์ตามลำดับ ทำให้เพิ่มประสิทธิภาพของการปฏิบัติงานภายในศาลให้เป็นไปโดยสะดวกรวดเร็วและปลอดภัยยิ่งขึ้น

3. สรุปผล และข้อเสนอแนะ

จากการศึกษาเรื่อง การศึกษารูปแบบการจัดเก็บและบริหารข้อมูลอัตลักษณ์บุคคลเพื่อนำมาประยุกต์ใช้ในศาลยุติธรรม ผู้ศึกษาสามารถสรุปผลและมีข้อเสนอแนะดังนี้

3.1 สรุปผล

จากการศึกษา เรื่อง การศึกษารูปแบบการจัดเก็บและบริหารข้อมูลอัตลักษณ์บุคคลเพื่อนำมาประยุกต์ใช้ในศาลยุติธรรมพบว่า เทคโนโลยีไบโอเมตริกมีคุณสมบัติที่ใช้ในการระบุตัวตน หรือพิสูจน์อัตลักษณ์ได้เป็นอย่างดี เหมาะสมต่อการนำมาประยุกต์ใช้งานภายในศาลยุติธรรมซึ่งสามารถทำได้หลากหลายรูปแบบ เนื่องจากเป็นเครื่องมือที่สามารถเพิ่มระดับการรักษาความปลอดภัยในการเข้าถึงทรัพยากรต่าง ๆ ของหน่วยงาน และทำให้การปฏิบัติงานของศาลยุติธรรมโดยรวมมีความรวดเร็วและประสิทธิภาพเพิ่มมากขึ้น แต่การดำเนินการ

ควรคำนึงถึงรูปแบบข้อมูลไบโอเมตริกที่เลือกใช้ในแต่ละงานควรมีความเหมาะสมทั้งในด้านคุณสมบัติและราคา รูปแบบและคุณภาพของข้อมูลไบโอเมตริกที่จัดเก็บไว้ต้องเป็นไปตามมาตรฐานสากลเพื่อให้เกิดความแม่นยำเวลาใช้งานและสามารถนำไปเชื่อมโยงเพื่อใช้ประโยชน์ร่วมกับหน่วยงานอื่นได้ ควรมีนโยบายในการบริหารจัดการข้อมูลให้เป็นไปตามกฎหมายหรือระเบียบข้อบังคับที่เกี่ยวข้อง มีระบบบริหารจัดการความเสี่ยงและรักษาความมั่นคงปลอดภัยในการเข้าถึงข้อมูล ควรให้ความรู้ผนวกกับการสร้างจิตสำนึกแก่บุคลากรในองค์กรให้ระมัดระวังการละเมิดข้อมูลส่วนบุคคลหรือสิทธิส่วนบุคคลของผู้อื่น และประโยชน์ที่องค์กรได้รับควรมีความคุ้มค่าเมื่อเทียบกับมูลค่าเงินงบประมาณที่ใช้ลงทุน

3.2 ข้อเสนอแนะ

จากการศึกษาเรื่อง การศึกษารูปแบบการจัดเก็บและบริหารข้อมูลอัตลักษณ์บุคคลเพื่อนำมาประยุกต์ใช้ในศาลยุติธรรม ผู้เขียนเห็นควรเสนอแนะหากจะใช้เทคโนโลยีการจัดเก็บและบริหารข้อมูลอัตลักษณ์บุคคลในหน่วยงาน ต้องคำนึงถึงความปลอดภัยของข้อมูล โดยมีการกำหนดแนวทางปฏิบัติที่ชัดเจนว่าหน่วยงานจะรักษาความปลอดภัยของคลังข้อมูลประเภทนี้อย่างไร เนื่องจากข้อมูลไบโอเมตริกเป็นข้อมูลอัตลักษณ์เฉพาะบุคคลที่บางอย่างไม่สามารถเปลี่ยนแปลงได้ตลอดชีวิต เช่น ลายนิ้วมือหรือม่านตา ประกอบกับในปัจจุบันประเทศไทยมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่กำหนดโทษทั้งทางแพ่งและอาญาในอัตราโทษสูงมากหากเกิดการรั่วไหลของข้อมูล ดังนั้นการนำข้อมูลนี้ไปใช้งานจึงควรคำนึงถึงการบริหารจัดการความเสี่ยงและรักษาความมั่นคงปลอดภัยในการเข้าถึงคลังข้อมูลให้มากเท่าที่จะเป็นไปได้

References

Bank of Thailand. “Guidelines for the Use of Biometric Technology in Financial Services.” Last modified July 22, 2020. Accessed August 29, 2020. https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2563/ThaiPDF/25630177.pdf/ [In Thai]

Bank of Thailand. “Questions and Answers on Measures to Manage Financial Corruption Threats of the BoT.” Last modified March 29, 2023. Accessed April 12, 2023. https://www.bot.or. th/content/dam/bot/documents/th/news-and-media/news/2023/QA_n1066t.pdf/ [In Thai]

Bansak Yuwamit. “What is Phishing? How to Prevent It.” Last modified May 8, 2021. Accessed June 13, 2022. https://www.cyfence.com/article/what-is-phishing/ [In Thai]

Office of Law and Judiciary Academics Office of the Judiciary. “Report Summarizing the Results of Listening to Opinions on the Evaluation of the Achievement of the Court Police Officers Act B.E. 2562.” Last modified July 18, 2022. Accessed December 3, 2022. https://lawsurvey.coj.go.th/Documents/result043.pdf/ [In Thai]

Security Center Office of the Courts of Justice. “Let’s Get to Know the Court Police Officers.” Last modified June 24, 2020. Accessed July 20, 2020. https://ojso.coj.go.th/th/content/category/detail/id/45/iid/198955 [In Thai]

Special Report News Team. “Unraveling the Mystery: Solving the Case of the Wrong Twin.” Crime News Column, Komchadluek, July 14, 2013. Accessed July 1, 2018. http://www.komchadluek.net/news/crime/163380/ [In Thai]