วิทยาลัยเทคโนโลยีภาคใต้
SOUTHERN COLLEGE OF TECHNOLOGY

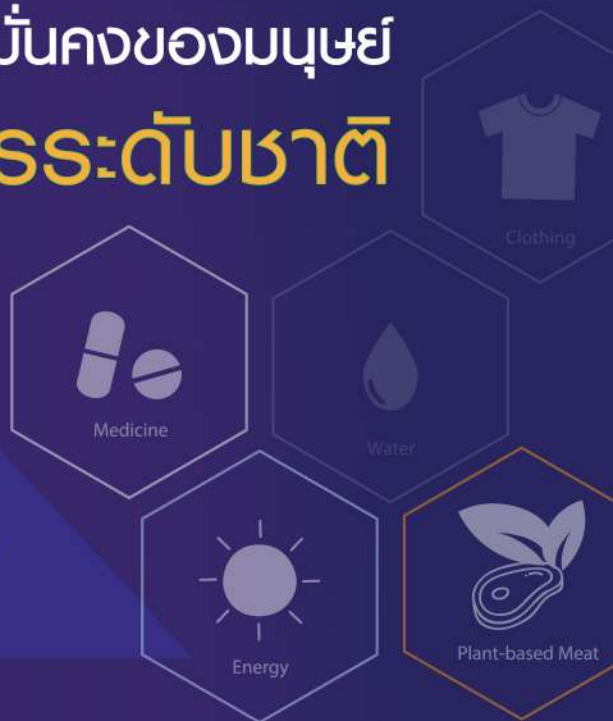
ครั้งที่
13th

Proceedings

# Nouveau Economy for Human Security

## เศรษฐกิจวิถีใหม่เพื่อความมั่นคงของมนุษย์

## การประชุมวิชาการระดับชาติ




ร่วมกับ

# การคุ้มครองสิทธิในการให้ความยินยอมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของบุคคลที่สามในกรณีนายจ้างใช้ระบบจดจำใบหน้าในการบันทึกเวลาทำงานของลูกจ้าง

# Protection of Third Parties’ Right to consent under the Personal Data Protection Act when employers use Facial Recognition Systems to Record Employee’s Work Hours.

**คณาธิป ทองรวีวงศ์**

**Kanathip Thongrawewong**

รองศาสตราจารย์ คณะนิติศาสตร์ และ สถาบันกฎหมายสื่อดิจิทัล มหาวิทยาลัยเกษมบัณฑิต
Associate Professor, Faculty of law and Digital Media Law Institute, Kasembundit University
Corresponding author, e-mail: kanathip.tho@kbu.ac.th

**บทคัดย่อ**

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาวิเคราะห์การอ้างอิงฐานทางกฎหมายอันเป็นข้อยกเว้นของการขอความยินยอมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 ในกรณีที่ผู้ประกอบการนำระบบจดจำใบหน้ามาใช้เก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นนอกเหนือจากลูกจ้าง 2) ศึกษาวิเคราะห์การขอความความยินยอมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 ในกรณีที่ผู้ประกอบการนำระบบจดจำใบหน้ามาใช้เก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นนอกเหนือจากลูกจ้าง และ 3) จัดทำข้อเสนอแนะแนวปฏิบัติสำหรับนายจ้างในการปฏิบัติให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กรณีนำระบบจดจำใบหน้ามาใช้เก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นนอกเหนือจากลูกจ้าง

การวิจัยนี้ใช้วิธีวิจัยเชิงคุณภาพในการวิเคราะห์เนื้อหา เปรียบเทียบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป ผลการวิจัยชี้ให้เห็นว่า 1) แนวปฏิบัติของผู้ประกอบการที่เป็นนายจ้างในการนำระบบจดจำใบหน้า มาใช้เก็บรวบรวมข้อมูลส่วนบุคคลลูกจ้างเพื่อบันทึกเวลางาน นำไปสู่ผลกระทบที่อาจเกิดขึ้นในการเก็บรวบรวมข้อมูลของบุคคลที่สามซึ่งไม่ใช่ลูกจ้าง จึงจะต้องอ้างอิงฐานทางกฎหมายที่แตกต่างกันไปขึ้นอยู่กับวัตถุประสงค์ของการเก็บรวบรวมข้อมูล 2) การใช้ระบบจดจำใบหน้าบุคคลที่สามเพื่อการรักษาความปลอดภัย เพื่อการตลาด ไม่เข้าองค์ประกอบข้อยกเว้นของความยินยอมตามมาตรา 26 และ 3) การขอความยินยอมจากบุคคลที่สามในการใช้ระบบจดจำใบหน้าบุคคลที่สามเพื่อการรักษาความปลอดภัย เพื่อการตลาด ต้องอยู่ภายใต้เงื่อนไขความเป็นอิสระของความยินยอม ซึ่งขึ้นอยู่กับสภาพข้อเท็จจริงและสภาพความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลกับบุคคลที่สามเป็นกรณีไป ผู้วิจัยจึงมีข้อเสนอแนะแก่ผู้ประกอบการในการปรับปรุงแนวปฏิบัติเพื่อให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

**คำสำคัญ**: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ความยินยอม ข้อมูลชีวภาพ ลูกจ้าง ระบบจดจำใบหน้า.

**Abstract**

The purposes of this study were: 1) to study and analyze the exceptions to consent under the Personal Data Protection Act B.E.2562 (PDPA) when employers used facial recognition systems to collect personal data of third parties who were not employees, 2) to analyze legal elements of consent under the PDPA when employers used facial recognition systems to collect personal data of third parties who were not employees, 3) to propose guidelines for employers in order to implement facial recognition systems in compliance with PDPA.

This qualitative research used content analysis by comparative analysis of Personal Data Protection Act B.E. 2562, General Data Protection Regulation of EU (GDPR). It was found that 1.) The practice of employers when used facial recognition systems to record employee’s work hours could cause impact on personal data of third parties who were not employees Therefore, employes shall refer to legal bases under

PDPA which could vary depending on purposes of processing personal data. 2) The collection of third parties personal data by using facial recognition systems for the purposes of security and marketing was not in compliance with exceptions to consent under PDPA. And 3) the consent from third parties for the collection of personal data by using facial recognition systems for the purposes of security and marketing may not in compliance with freely-given consent principles under PDPA depending on case-by-case basis.
The researcher therefore proposed suggestions for employers to adapt their guidelines in order to use facial recognition systems in compliance with PDPA.

**Keywords**: Personal Data Protection Act, Consent, Biometric data, Employee, Facial recognition system.

## บทนำ

ที่มาและความสำคัญของปัญหาในการทำวิจัยสืบเนื่องจาก ในเดือน พฤษภาคม ค.ศ. 2018 กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ของสหภาพยุโรป ( Regulation (EU) 2016/679 (General Data Protection Regulation) ซึ่งต่อไปในบทความนี้จะใช้คำย่อว่า GDPR) มีผลใช้บังคับแทนที่ กฎหมายเดิม (Directive 95/46/EC) ส่งผลกระทบต่อหลายภาคส่วนที่เกี่ยวข้องกับข้อมูลระบุตัวตนของบุคคล (Personal Data) ทั้งผู้ประกอบธุรกิจขนาดใหญ่ กลางและย่อม ผู้เป็นเจ้าของข้อมูลส่วนบุคคล (Kuner, 2018) กฎหมายนี้มีแนวคิดพื้นฐานเกี่ยวกับการคุ้มครองความเป็นอยู่ส่วนตัว (Right to Privacy) แต่มีขอบเขตจำกัดเฉพาะในด้านข้อมูลของบุคคล (Solove, 2006) โดยแนวคิดและหลักการปรากฏในความตกลงระหว่างประเทศหลายฉบับ ในส่วนของประเทศไทย ก่อนปี พ.ศ. 2562 ไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ แต่มีกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น กฎหมายคุ้มครองข้อมูลเฉพาะบางภาคส่วนของธุรกิจ เช่น ธุรกิจการเงิน อย่างไรก็ตามในเดือนกุมภาพันธ์ปี พ.ศ. 2562 สภานิติบัญญัติแห่งชาติได้ลงมติเห็นชอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลก่อนการเลือกตั้งทั่วไปในเดือนมีนาคมเพียงไม่ถึงหนึ่งเดือนและประกาศในราชกิจจานุเบกษาในเดือนพฤษภาคม พ.ศ. 2562 แม้ว่ากฎหมายนี้ร่างขึ้นโดยอาศัยตัวแบบของกฎหมายสหภาพยุโรปแต่ก็มีหลายประเด็นที่แตกต่างกัน รวมทั้งส่งผลกระทบต่อผู้ประกอบการในหลายแง่มุม เช่น การสร้างต้นทุนในการปฏิบัติตามเงื่อนไขต่างๆให้สอดคล้องกับกฎหมาย (Compliance Cost) (คณาธิป ทองรวีวงศ์, 2564) เนื่องจากกฎหมายนี้มีผลบังคับใช้ในเดือนมิถุนายน 2565 และยังไม่มีคำพิพากษาหรือแนววินิจฉัย อีกทั้งตัวบทที่แปลจากกฎหมายสหภาพยุโรปในหลายมาตรายังมีความไม่ชัดเจน ซึ่งเมื่อพิจารณาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พบว่า กำหนดหลักการที่สำคัญสองส่วนที่อยู่บนแนวคิดแตกต่างกัน (คณาธิป ทองรวีวงศ์, 2564) คือ 1. กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความปลอดภัย ซึ่งอยู่บนพื้นฐานแนวคิดความมั่นคงปลอดภัยของข้อมูลหรือความมั่นคงปลอดภัยสารสนเทศ (Information Security) 2. กำหนดให้ผู้ควบคุมข้อมูลต้องอ้างอิงฐานทางกฎหมาย (Legal or lawful basis of processing personal data) ซึ่งอยู่บนพื้นฐานการคุ้มครองสิทธิของเจ้าของข้อมูล เช่น การขอความยินยอมจากเจ้าของข้อมูล หรืออ้างฐานทางกฎหมายอันเป็นข้อยกเว้นของความยินยอม สำหรับงานวิจัยนี้จะศึกษาหลักการส่วนที่สอง ในกรณีนายจ้างที่อยู่ในสถานะผู้ควบคุมข้อมูลของลูกจ้าง และมีหน้าที่อ้างฐานทางกฎหมายในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลลูกจ้าง โดยศึกษาเฉพาะในส่วนแนวปฏิบัติในบันทึกเวลาเข้าออกงานของลูกจ้าง โดยติดตั้งระบบจดจำใบหน้า (Facial Recognition) ซึ่งประกอบด้วยอุปกรณ์บันทึกภาพ ที่จะทำการจับภาพใบหน้า โดยอาจเป็นภาพสามมิติและนำไปวิเคราะห์เปรียบเทียบกับฐานข้อมูลภาพของลูกจ้างที่นายจ้างบันทึกไว้ โดยระบบจะวิเคราะห์ จำแนก หากพบว่าภาพใบหน้าตรงกับฐานข้อมูลจะระบุตัวลูกจ้างและนำไปเชื่อมโยงกับการบริหารจัดการข้อมูลต่างๆ เช่น เพื่อใช้บันทึกเวลางาน ทั้งนี้การดำเนินการดังกล่าวเกิดขึ้นได้แม้ลูกจ้างที่เดินผ่านอุปกรณ์บันทึกภาพไม่ได้มีปฏิสัมพันธ์หรือทำปฏิกิริยาใดกับอุปกรณ์ การดำเนินการดังกล่าวของนายจ้างเป็นการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลซึ่งเป็นภาพจำลองใบหน้าหรือข้อมูลชีวภาพตามมาตรา 26 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีประเด็นปัญหาทางกฎหมายที่สำคัญ เช่น 1. การเก็บรวบรวมภาพจำลองใบหน้าเพื่อบันทึกเวลางานต้องขอความยินยอมจากลูกจ้างตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือสามารถอาศัยข้อยกเว้น ซึ่งประเด็นนี้ผลการศึกษาวิจัยชี้ให้เห็นว่าไม่เข้าองค์ประกอบของข้อยกเว้นตามมาตรา 26 จึงต้องอาศัยความยินยอมจากลูกจ้าง (คณาธิป ทองรวีวงศ์, 2565) และ 2. การเก็บรวบรวมภาพจำลองใบหน้าของบุคคลอื่น โดยในกรณีที่นายจ้างติดตั้งอุปกรณ์บันทึกภาพไว้ในบริเวณทางเข้าออกหรือพื้นที่ซึ่งมีบุคคลอื่นที่ไม่อยู่ในสถานะลูกจ้าง เช่น ลูกค้า ผู้มาติดต่อ หรือ บุคคลที่เคยเป็นลูกจ้างแต่สิ้นสุดสัญญาจ้างด้วยเหตุต่าง ๆ ส่งผลกระทบต่อบุคคลเหล่านี้ในแง่ที่ถูกเก็บรวบรวมข้อมูลไปด้วยและอาจถูกนำไปใช้เปรียบเทียบระบุตัวบุคคล ซึ่งจะอยู่ภายใต้วัตถุประสงค์ที่แตกต่างกับการบันทึกเวลางาน

ลูกจ้าง นำไปสู่ประเด็นว่านายจ้างจะต้องขอความยินยอมจากบุคคลดังกล่าวหรืออาศัยข้อยกเว้นตามกฎหมาย ซึ่งจะได้ศึกษาวิจัยในครั้งนี้ โดยวิเคราะห์เนื้อหา แนวทางตีความตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเปรียบเทียบกับกฎหมายสหภาพยุโรป

## วัตถุประสงค์การวิจัย

1.ศึกษาวิเคราะห์การอ้างอิงฐานทางกฎหมายอันเป็นข้อยกเว้นของการขอความยินยอมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนพ.ศ. 2562 บุคคลในกรณีที่ผู้ประกอบการนำระบบจดจำใบหน้ามาใช้เก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นนอกเหนือจากลูกจ้าง

2.ศึกษาวิเคราะห์การขอความความยินยอมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในกรณีที่ผู้ประกอบการนำระบบจดจำใบหน้ามาใช้เก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นนอกเหนือจากลูกจ้าง

3. จัดทำข้อเสนอแนะแนวปฏิบัติสำหรับผู้ประกอบการในการปฏิบัติให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในกรณีนำระบบจดจำใบหน้ามาใช้เก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นนอกเหนือจากลูกจ้าง

## วิธีการวิจัย

งานวิจัยนี้ใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ศึกษาข้อมูลเอกสาร (Documentary Research) ตามกฎหมายสหภาพยุโรปด้วยการวิเคราะห์เนื้อหาเชิงเปรียบเทียบ (Comparative Analysis) และนำหลักการดังกล่าวมาปรับใช้ในการวิเคราะห์ตีความพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในส่วนหลักการเกี่ยวกับการขอความยินยอมหรืออ้างข้อยกเว้นของความยินยอมในกรณีที่ผู้ประกอบการนำระบบจดจำใบหน้ามาใช้เก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นนอกเหนือจากลูกจ้าง ประชากรและกลุ่มตัวอย่าง วิธีเลือกกลุ่มตัวอย่าง เครื่องมือ การสร้างเครื่องมือ เก็บข้อมูลอย่างไร วิเคราะห์ข้อมูลและสถิติที่ใช้ ซึ่งอาจเป็นวิธีการเชิงคุณภาพหรือปริมาณขึ้นอยู่กับประเภทของงานวิจัย

## กรอบแนวคิดทฤษฎี

หัวข้อนี้จะทบทวนกรอบแนวคิดทฤษฎีที่เกี่ยวกับข้องกับสิทธิในการให้ความยินยอมของเจ้าของข้อมูลอันเป็นพื้นฐานหลักการของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีหลักสำคัญสองส่วนที่อยู่บนแนวคิดแตกต่างกัน (คณาธิป ทองรวีวงศ์, 2564) คือ 1. กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความปลอดภัย ซึ่งอยู่บนแนวคิดความมั่นคงปลอดภัยของข้อมูลหรือความมั่นคงปลอดภัยสารสนเทศ (Information Security) ซึ่งไม่เกี่ยวข้องกับประเด็นการวิเคราะห์ในบทความนี้ 2.กำหนดให้ผู้ควบคุมข้อมูลต้องอ้างอิง “ฐานทางกฎหมาย” (Legal or lawful basis of processing personal data) เช่น การขอความยินยอมจากเจ้าของข้อมูล หรือการอ้างฐานอันเป็นข้อยกเว้นของความยินยอม หลักการส่วนนี้อยู่บนพื้นฐานแนวคิดทฤษฎีเกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นส่วนหนึ่งของแนวคิด “สิทธิในความเป็นอยู่ส่วนตัว” (Right to Privacy) ซึ่งจัดเป็นสิทธิขั้นพื้นฐานของมนุษย์ (Arendt, 1973) กล่าวคือ เป็นสิทธิที่ติดตัวคนมาตั้งแต่กำเนิด จึงอยู่ในกลุ่มของสิทธิมนุษยชน (Donnelly, 1982) บางตำราเรียกว่า สิทธิที่จะอยู่ตามลำพัง (Right to be let alone) กล่าวคือ ปราศจากการแทรกแซงจากบุคคลภายนอก (Warren, Samuel, & Brandies, 1890) แต่การพิจารณาในแง่ปราศจากการแทรกแซงหรือความลับอาจทำให้สิทธินี้กว้างเกินไป โดยเฉพาะในสภาพสังคมที่มีการติดต่อระหว่างบุคคล ทำให้การไม่ถูกแทรกแซงเป็นไปได้ยาก (Alan, 1967) ต่อมามีการพัฒนาแนวคิดว่าหมายถึง การจำกัดการเข้าถึงปัจเจกชนโดยบุคคลอื่น (Rubenfield, 1989) ในทางวิชาการ สิทธิดังกล่าวยังคงมีความหมายและขอบเขตกว้าง (Schoeman, 1984) โดยจำแนกได้หลายมิติ รวมถึงการคุ้มครองข้อมูลส่วนบุคคล (Solove, 2006). ตามกฎหมายสหรัฐอเมริกา สิทธิในความเป็นอยู่ส่วนตัวปรากฏในกฎหมายคอมมอนลอว์และกฎหมายอื่น เช่นกฎหมายลักษณะละเมิด (Bloustein, 1984) เมื่อพิจารณาในระดับกฎหมายระหว่างประเทศ พบว่า กติกาสากลว่าด้วยสิทธิทางแพ่งและการเมืองของสหประชาชาติ (International Covenant on Civil and Political Rights ค.ศ. 1966) รับรองสิทธินี้ไว้ในข้อ 17 สำหรับกฎหมายต่างประเทศที่กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลที่ส่งผลกระทบต่อหลายประเทศ ได้แก่กฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป (Directive 95/46/EC) ซึ่งมีผลผูกพันตามกฎหมายต่อประเทศสมาชิกสหภาพยุโรป (Cate, 1995) โดยหลักสำคัญประการหนึ่งของกฎหมายนี้คือ การวางเงื่อนไขการใช้ การเปิดเผย การโอนข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อจำกัดด้านการโอนข้อมูลออกนอกประเทศ (Fromholz, 2000) ต่อมา ค.ศ. 2018 กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ของสหภาพยุโรป (GDPR) มีผลใช้บังคับแทนกฎหมายเดิม (Directive 95/46/EC) โดยมีหลักการสำคัญเช่นเดิมคือ การเก็บรวบรวมใช้เปิดเผยข้อมูลส่วนบุคคลของผู้อื่นต้องอ้างอิงฐาน

ทางกฎหมาย ซึ่งโดยหลักต้องอาศัยฐานความยินยอม เว้นแต่เข้าองค์ประกอบฐานอื่นที่กฎหมายกำหนด ในส่วนของประเทศไทย ในเดือนกุมภาพันธ์ปี พ.ศ. 2562 สภานิติบัญญัติแห่งชาติลงมติเห็นชอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลก่อนการเลือกตั้งทั่วไปในเดือนมีนาคมเพียงไม่ถึงหนึ่งเดือนและประกาศในราชกิจจานุเบกษาในเดือนพฤษภาคม พ.ศ.2562 กฎหมายนี้มีองค์ประกอบและโครงสร้างหลักตามตัวแบบกฎหมายสหภาพยุโรป ดังนั้น การคุ้มครองสิทธิในการให้ความยินยอมของเจ้าของข้อมูลจึงมีหลักการเฉพาะตามพระราชบัญญัติดังกล่าว โดยบทมาตราที่เกี่ยวข้องและจะนำมาศึกษาในงานวิจัยนี้ประกอบด้วย มาตรา 19 ซึ่งกำหนดหลักเกณฑ์การขอความยินยอม มาตรา 24 มาตรา 27 กำหนดฐานทางกฎหมาย (Legal basis) โดยวางหลักว่าการเก็บรวบรวมข้อมูลส่วนบุคคลต้องขอความยินยอมเว้นแต่จะเข้าข้อยกเว้นที่ระบุไว้ในมาตราเหล่านี้ และมาตรา 26 กำหนดฐานทางกฎหมายโดยเฉพาะสำหรับการเก็บรวบรวมข้อมูลชีวภาพ (Biometric) ซึ่งหมายรวมถึงภาพจำลองใบหน้าและการใช้ระบบจดจำใบหน้า (Facial Recognition)

## ผลการวิจัยและอภิปรายผล

1. จากวัตถุประสงค์การวิจัยข้อ 1 ในการวิเคราะห์การอ้างอิงฐานทางกฎหมายอันเป็นข้อยกเว้นของการขอความยินยอมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 ในกรณีที่ผู้ประกอบการนำระบบจดจำใบหน้ามาใช้เก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นนอกเหนือจากลูกจ้าง ผลการศึกษาพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหลักการเกี่ยวกับฐานทางกฎหมาย (Legal Basis) อันเป็นเงื่อนไขของการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้อื่น ซึ่งจำแนกตามประเภทข้อมูลส่วนบุคคล กล่าวคือ กรณีข้อมูลส่วนบุคคลทั่วไป จะอยู่ภายใต้มาตรา 24 ที่วางหลักว่าต้องขอความยินยอมก่อน แต่มีข้อยกเว้น เช่น การปฏิบัติตามสัญญากับเจ้าของข้อมูล มาตรา 24 (3) ประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูล มาตรา 24 (5) สำหรับกรณีข้อมูลส่วนบุคคลชนิดพิเศษ (Special Categories of Personal data) เช่น ภาพจำลองใบหน้าซึ่งเป็นส่วนหนึ่งของข้อมูลชีวภาพ (Biometric Data) นั้น จะอยู่ภายใต้มาตรา 26 ที่วางหลักว่าต้องขอความยินยอมก่อน แต่มีข้อยกเว้นที่แตกต่างจากมาตรา 24 ซึ่งในที่นี้จะศึกษาเฉพาะข้อยกเว้นที่เกี่ยวข้องกับประเด็นการศึกษาคือ การปฏิบัติตามกฎหมายที่มีวัตถุประสงค์เฉพาะดังระบุในมาตรา 26 (5) โดยมาตรานี้ไม่มีข้อยกเว้นเกี่ยวกับการปฏิบัติตามสัญญาและประโยชน์โดยชอบด้วยกฎหมายดังเช่นมาตรา 24 ทั้งนี้ การที่กฎหมายกำหนดหลักการคุ้มครองข้อมูลชีวภาพเป็นการเฉพาะ เนื่องจากการกระทำต่อข้อมูลชนิดนี้ส่งผลกระทบต่อสิทธิพื้นฐาน (Fundamental Right) โดยอาจเชื่อมโยงไปสู่ผลกระทบในแง่การเลือกปฏิบัติ (Discrimination) ในมิติต่าง ๆ ต่อเจ้าของข้อมูล (GDPR, Recital 51)

ในแง่นี้จะเห็นได้ว่าการนำข้อมูลภาพจำลองใบหน้าซึ่งเป็นเอกลักษณ์เฉพาะของบุคคลไปใช้โดยมิชอบส่งผลให้บุคคลนั้นได้รับผลกระทบในมิติต่าง ๆ เช่น การถูกพรากความเป็นตัวตนไปเนื่องจากการเข้าถึงบริการจำเป็นอาศัยข้อมูลดังกล่าวในการยืนยันตัวตน ดังนั้นกฎหมายจึงกำหนดข้อยกเว้นสำหรับการเก็บรวบรวมข้อมูลชนิดนี้ที่แคบและจำกัดกว่าข้อมูลส่วนบุคคลทั่วไป

อย่างไรก็ตาม เมื่อพิจารณาถึงกรณีนายจ้างใช้อุปกรณ์บันทึกภาพจำลองใบหน้าลูกจ้างแต่ส่งผลกระทบต่อบุคคลที่สามอันเป็นการเก็บรวบรวมข้อมูลด้วยนั้น กฎหมายไม่ได้ระบุถึงกรณีนี้ไว้โดยเฉพาะ จากการศึกษาเนื้อหาและองค์ประกอบของกฎหมาย พบว่า ฐานทางกฎหมายที่เกี่ยวข้องและอาจนำมาปรับใช้ ปรากฏในมาตรา 24 มาตรา 27 และมาตรา 26 โดยแยกพิจารณาได้ตามปัจจัยสองประการคือ สถานะความสัมพันธ์ระหว่างเจ้าของข้อมูลกับผู้ประกอบการ และ วัตถุประสงค์ในการใช้ระบบจดจำใบหน้า ดังนี้

1.1 กรณีบุคคลที่สามซึ่งมีความสัมพันธ์ในฐานะลูกค้าของผู้ประกอบการที่เป็นนายจ้าง หากการเก็บรวบรวมข้อมูลภาพจำลองใบหน้านำไปเปรียบเทียบ จับคู่ วิเคราะห์ จำแนกระบุตัวบุคคล เพื่อนำเสนอสินค้าหรือบริการ หรือ เพื่อการตลาดอื่นๆ ไม่เข้าข้อยกเว้นตามมาตรา 26 และต้องอาศัยความยินยอม หากนำมาใช้เพื่อวัตถุประสงค์ในการให้บริการหรือขายสินค้าตามสัญญาระหว่างกัน ก็ไม่เข้าข้อยกเว้นฐานปฏิบัติตามสัญญามาตรา 24 (3) เพราะข้อมูลภาพจำลองใบหน้าอยู่ภายใต้มาตรา 26 หากการนำภาพจำลองใบหน้าไประบุตัวลูกค้าเพื่อวัตถุประสงค์ในการรักษาความปลอดภัย จะไม่เข้าข้อยกเว้นตามมาตรา 26 และต้องอาศัยความยินยอม ซึ่งต่างกับกรณีการใช้กล้องวงจรปิดเพียงเพื่อบันทึกภาพทั่วไปไม่มีการวิเคราะห์จับคู่ระบุตัวบุคคลจะไม่ใช่ภาพจำลองใบหน้าตามมาตรา 26 และผู้ประกอบการอาจอ้างข้อยกเว้นเพื่อรักษาความปลอดภัยอันเป็นประโยชน์โดยชอบด้วยกฎหมายตามมาตรา 24 (5)

1.2 กรณีบุคคลที่สามเป็นผู้มาติดต่อ (Visitor) ซึ่งไม่มีนิติสัมพันธ์ตามสัญญาใดๆระหว่างกันกับผู้ประกอบการที่เป็นนายจ้าง หากการเก็บรวบรวมข้อมูลภาพจำลองใบหน้าของบุคคลที่สามโดยนำไปเปรียบเทียบ จับคู่ วิเคราะห์ จำแนกระบุตัวบุคคล เพื่อนำเสนอสินค้าหรือบริการ หรือ เพื่อการตลาดอื่น ๆ ไม่เข้าข้อยกเว้นตามมาตรา 26 และต้องอาศัยความยินยอม

หากการนำภาพจำลองใบหน้าไประบุตัวเพื่อวัตถุประสงค์ในการรักษาความปลอดภัย จะไม่เข้าข้อยกเว้นตามมาตรา 26 และต้องอาศัยความยินยอม ซึ่งต่างกับกรณีการใช้กล้องวงจรปิดเพียงเพื่อบันทึกภาพทั่วไปไม่มีการวิเคราะห์จับคู่ระบุตัวบุคคล จะไม่ใช่ภาพจำลองใบหน้าตามมาตรา 26 และผู้ประกอบการอาจอ้างข้อยกเว้นเพื่อรักษาความปลอดภัยอันเป็นประโยชน์โดยชอบด้วยกฎหมายตามมาตรา 24 (5)

1.3 กรณีบุคคลที่สามเป็นบุคคลที่เคยเป็นลูกจ้างของผู้ประกอบการแต่สิ้นสุดสัญญาจ้างแล้ว หากการเก็บรวบรวมข้อมูลภาพจำลองใบหน้าโดยนำไปเปรียบเทียบ จับคู่ วิเคราะห์ จำแนกระบุตัวบุคคล เพื่อนำเสนอสินค้าหรือบริการ หรือ เพื่อการตลาดอื่นๆ ไม่เข้าข้อยกเว้นตามมาตรา 26 และต้องอาศัยความยินยอม หากการนำภาพจำลองใบหน้าไประบุตัวเพื่อวัตถุประสงค์ในการรักษาความปลอดภัย จะไม่เข้าข้อยกเว้นตามมาตรา 26 และต้องอาศัยความยินยอม ซึ่งต่างกับกรณีการใช้กล้องวงจรปิดเพียงเพื่อบันทึกภาพทั่วไปไม่มีการวิเคราะห์จับคู่ระบุตัวบุคคล จะไม่ใช่ภาพจำลองใบหน้าตามมาตรา 26 และผู้ประกอบการอาจอ้างข้อยกเว้นเพื่อรักษาความปลอดภัยอันเป็นประโยชน์โดยชอบด้วยกฎหมายตามมาตรา 24 (5) สำหรับกรณีที่ผู้ประกอบการใช้ระบบจดจำใบหน้าเพื่อป้องกันอดีตลูกจ้างที่ขึ้นบัญชีผู้ไม่พึงประสงค์มิให้เข้ามาในสถานประกอบการนั้นไม่ใช่การปฏิบัติตามกฎหมายและไม่เข้ากรณีการจำเป็นเพื่อใช้สิทธิเรียกร้องตามมาตรา 26 (4) เพราะการใช้ระบบจดจำระบุตัวบุคคลเพื่อป้องกันหรือไม่อนุญาตให้เข้าสถานที่มิได้เกี่ยวข้องและจำเป็นกับการนำข้อมูลนั้นไปดำเนินคดีตามสิทธิเรียกร้องระหว่างกัน

2. จากวัตถุประสงค์การวิจัยข้อ 2 ศึกษาวิเคราะห์การขอความความยินยอมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 ทั้งนี้ ในกรณีที่ผู้ประกอบการนำระบบจดจำใบหน้ามาใช้เก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นนอกเหนือจากลูกจ้าง และเลือกที่จะใช้วิธีการขอความยินยอมจากบุคคลดังกล่าว จึงมีประเด็นการวิเคราะห์ว่า การขอความยินยอมชอบด้วยกฎหมายหรือไม่ ผลการศึกษาพบว่า องค์ประกอบสำคัญคือ ความยินยอมโดยอิสระ (Freely given consent) ซึ่งปรากฏในกฎหมายไทย มาตรา 19 วรรคสี่ว่า “ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม...” ซึ่งเมื่อนำองค์ประกอบของมาตรานี้มาเปรียบเทียบกับกฎหมายสหภาพยุโรปพบว่ามีการอธิบายในส่วนขยายที่ 32 และ 43 (GDPR, recital 32 and 43) และพบว่า หลักการที่คล้ายคลึงกันคือมาตรา 19 กำหนดองค์ประกอบความยินยอมโดยอิสระไว้ในตัวบท ซึ่งเป็นไปตามส่วนขยายที่ 32 ของกฎหมายสหภาพยุโรป แต่ในส่วนที่แตกต่างกันพบว่า มาตรา 19 ไม่ได้กำหนดรายละเอียดหรือเกณฑ์ย่อยในการพิจารณาความเป็นอิสระ ในขณะที่ ส่วนขยายที่ 43 ของกฎหมายสหภาพยุโรป กำหนดเกณฑ์พิจารณาความไม่สมดุลเชิงอำนาจต่อรอง (Imbalance of Power) ซึ่งผู้ควบคุมข้อมูลมีอำนาจต่อรองเหนือกว่าเจ้าของข้อมูล สภาพความสัมพันธ์เช่นนี้ส่งผลทางกฎหมายว่า แม้ผู้ควบคุมข้อมูลจะขอความยินยอมจากเจ้าของข้อมูล ก็ไม่ถือว่าความยินยอมนั้นมีผลเป็นฐานทางกฎหมาย (Valid Legal Ground) นอกจากนี้ ตามแนวทางการตีความของสหภาพยุโรปยังมีการกำหนดเกณฑ์ผลกระทบทางลบ (Negative Consequence) เพื่อนำมาประกอบการพิจารณาว่าความยินยอมเกิดขึ้นโดยอิสระหรือไม่อีกด้วย (European Data Protection Board, 2021) ดังนั้น ผู้วิจัยจะนำเกณฑ์เหล่านี้มาวิเคราะห์ความยินยอมของบุคคลที่สามเพื่อให้ผู้ประกอบการเก็บรวบรวมข้อมูลชีวภาพในกรณีระบบจดจำใบหน้า โดยแยกตามเกณฑ์ดังนี้

2.1 เกณฑ์ความไม่สมดุลเชิงอำนาจต่อรอง (Imbalance of Power) ปรากฏในกฎหมายสหภาพยุโรป (GDPR, Recital 43) กล่าวคือ หากเจ้าของข้อมูลและผู้ควบคุมข้อมูลอยู่บนพื้นฐานความสัมพันธ์ที่มีอำนาจต่อรองไม่เท่าเทียมกันจะส่งผลให้ความยินยอมที่ได้รับจากความสัมพันธ์เช่นนี้ไม่สอดคล้องกับหลักความอิสระ (Article 29 Working party of The European Union, 2011:12) โดยการตีความกฎหมายสหภาพยุโรปยกตัวอย่าง กรณีผู้ควบคุมข้อมูลส่วนบุคคลเป็นหน่วยงานรัฐ (Public authority) และเจ้าของข้อมูลเป็นประชาชน กับ กรณีผู้ควบคุมข้อมูลส่วนบุคคลเป็นนายจ้างและเจ้าของข้อมูลเป็นลูกจ้าง (European Data Protection Board, 2021)

เมื่อนำเกณฑ์นี้มาวิเคราะห์กรณีการเก็บรวบรวมข้อมูลชีวภาพลูกจ้างเพื่อบันทึกเวลางานและตรวจสอบการทำงาน พบว่า พบว่า ไม่สอดคล้องกับหลักความเป็นอิสระ (คณาธิป ทองรวีวงศ์, 2565) อย่างไรก็ตาม แนวทางตีความของสหภาพยุโรปไม่ได้ตีความว่าบุคคลที่สาม เช่น ลูกค้า ผู้มาติดต่อ จัดอยู่ในกรณีความสัมพันธ์เชิงอำนาจต่อรองที่ไม่เท่าเทียมดังเช่นกรณีลูกจ้างกับนายจ้าง การขอความยินยอมจึงอาจสอดคล้องกับเกณฑ์นี้ แต่ยังต้องพิจารณาประกอบกับเกณฑ์ประการที่สองด้วย

2.2 เกณฑ์ผลกระทบทางลบจากการไม่ยินยอมให้เก็บรวบรวมข้อมูล เกณฑ์นี้มีหลักการว่าความยินยอมจะสอดคล้องกับความเป็นอิสระต้องอยู่บนพื้นฐานการมีทางเลือกที่แท้จริง (Real choice) (Article 29 Working party of The European Union, 2011) หากเจ้าของข้อมูลต้องยอมทน (Endure) กับผลกระทบทางลบ (Negative Consequences) อันอาจเกิดขึ้น

หากไม่ยินยอมจะถือว่าเกิดผลกระทบทางลบ ซึ่งมีหลายมิติ เช่น การข่มขู่ บังคับ กดดัน ค่าใช้จ่ายที่เพิ่มขึ้น คุณภาพหรือการบริการที่ลดลง (Downgrade) (European Data Protection Board, 2021)

เมื่อนำเกณฑ์นี้มาวิเคราะห์กรณีการเก็บรวบรวมข้อมูลภาพจำลองใบหน้าตามระบบจดจำใบหน้าของบุคคลที่สามผลทางกฎหมายในแง่ผลกระทบทางลบจะแตกต่างกันไป ขึ้นอยู่กับข้อเท็จจริง ซึ่งแบ่งได้สองกรณีคือ (1) หากสภาพข้อเท็จจริงปรากฏว่าบุคคลที่สามมีความจำเป็นที่จะต้องผ่านเข้าไปในบริเวณที่มีระบบจดจำใบหน้า เช่น ผู้มาติดต่อซึ่งเป็นลูกจ้างของลูกค้าหรือคู่ค้า อันได้รับมอบหมายหรือมีหน้าที่ต้องเข้ามาติดต่อทางธุรกิจ หากไม่ยินยอมให้เก็บรวบรวมข้อมูลอาจทำให้ไม่สามารถปฏิบัติหน้าที่ของตนและส่งผลกระทบต่อการทำงานหรือการประกอบการ ซึ่งจัดเป็นผลกระทบทางลบจากการไม่ยินยอมได้ความยินยอมที่ได้มาในสถานการณ์เช่นนี้ ไม่สอดคล้องกับหลักความยินยอมโดยอิสระ (2) หากสภาพข้อเท็จจริงปรากฏว่าบุคคลที่สามสามารถเลือกที่จะยินยอมหรือไม่ยินยอมให้ใช้ระบบจดจำใบหน้าโดยไม่เกิดผลกระทบทางลบ จะสอดคล้องกับหลักความยินยอมโดยอิสระ

## สรุป

แนวปฏิบัติของผู้ประกอบการที่เป็นนายจ้างในการนำระบบจดจำใบหน้า (Facial recognition) มาใช้เก็บรวบรวมข้อมูลส่วนบุคคลลูกจ้างเพื่อบันทึกเวลางาน นำไปสู่ผลกระทบที่อาจเกิดขึ้นในการเก็บรวบรวมข้อมูลของบุคคลที่สามซึ่งไม่ใช่ลูกจ้าง ซึ่งจะต้องอ้างอิงฐานทางกฎหมายที่แตกต่างจากกรณีลูกจ้าง เมื่อนำปัจจัยสองประการคือ สถานะความสัมพันธ์ และวัตถุประสงค์ในการเก็บรวบรวมข้อมูล มาจำแนกบุคคลที่สามออกเป็นสามกลุ่ม พบว่า

(1) การใช้ระบบจดจำใบหน้าบุคคลที่สามเพื่อการตลาด เพื่อการรักษาความปลอดภัย ไม่เข้าองค์ประกอบข้อยกเว้นของความยินยอมตามมาตรา 26

(2) การขอความยินยอมจากบุคคลที่สามในการใช้ระบบจดจำใบหน้าบุคคลที่สามเพื่อการตลาด เพื่อการรักษาความปลอดภัย ต้องอยู่ภายใต้เงื่อนไขความเป็นอิสระของความยินยอม ซึ่งมีเกณฑ์สำคัญในการพิจารณาสองประการคือ ความสมดุลเชิงอำนาจต่อรอง และ ผลกระทบทางลบจากการไม่ยินยอม โดยการพิจารณาความเป็นอิสระขึ้นอยู่กับสภาพข้อเท็จจริง พฤติการณ์ และสภาพความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลกับบุคคลที่สาม ในแต่ละสถานะ ได้แก่ ลูกค้า คู่ค้า ผู้มาติดต่อ

## ข้อเสนอแนะ

1.ข้อเสนอเชิงการปรับปรุงแนวปฏิบัติตามกฎหมายสำหรับนายจ้างผู้ประกอบการ เสนอการปรับปรุงแนวปฏิบัติเกี่ยวกับการใช้ระบบจดจำใบหน้า เพื่อมิให้เกิดผลกระทบหรือก่อให้เกิดการเก็บรวบรวมข้อมูลบุคคลที่สาม ซึ่งจะส่งผลทางกฎหมายว่า นายจ้างไม่ต้องขอความยินยอมหรืออ้างข้อยกเว้นของความยินยอมตามมาตรา 26 เพราะไม่มีการเก็บรวบรวมข้อมูลชีวภาพ เช่น การติดตั้งอุปกรณ์ดังกล่าวในบริเวณเฉพาะที่เป็นทางเข้าของลูกจ้างเท่านั้น หรือ การจัดให้บุคคลภายนอกผ่านทางเข้าอื่นที่มีการติดตั้งกล้องวงจรปิดทั่วไปที่ไม่มีระบบจดจำใบหน้า

2.ข้อเสนอเชิงการปรับปรุงแนวปฏิบัติตามกฎหมายสำหรับนายจ้างผู้ประกอบการที่ใช้ระบบจดจำใบหน้ากับบุคคลที่สาม เพื่อวัตถุประสงค์ระบุตัวบุคคลและนำไปใช้ทางการตลาด การส่งเสริมธุรกิจ หรือการรักษาความปลอดภัย หรือจัดทำฐานข้อมูลภายในสถานประกอบการ โดยเสนอให้ปรับแนวปฏิบัติการความยินยอมสอดคล้องกับหลักความเป็นอิสระ และป้องกันมิให้เกิดผลกระทบทางลบกับบุคคลที่สามที่ไม่ให้ความยินยอม เช่น การขอความยินยอมจากบุคคลที่สามโดยจัดให้บุคคลที่สามที่ไม่ประสงค์ยินยอมใช้ระบบจดจำใบหน้าได้มีทางเลือกอื่น

## กิตติกรรมประกาศ

ผู้วิจัยขอขอบคุณมหาวิทยาลัยเกษมบัณฑิตที่ให้ทุนอุดหนุนการวิจัยครั้งนี้

## เอกสารอ้างอิง

คณาธิป ทองรวีวงศ์. (2564). *หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล.* กรุงเทพฯ: สำนักพิมพ์นิติธรรม.

คณาธิป ทองรวีวงศ์. (2564:1). ผลกระทบทางลบอันเกิดจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรปและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. *วารสารรัชต์ภาคย์, 15*(38), 42-56.

คณาธิป ทองรวีวงศ์. (2565). *การคุ้มครองสิทธิในการให้ความยินยอมของลูกจ้างจากกรณีนายจ้างขอความยินยอมในการเก็บรวบรวมข้อมูลชีวภาพเพื่อวัตถุประสงค์บันทึกเวลาและตรวจสอบการทำงาน* (รายงานการวิจัย). กรุงเทพฯ: มหาวิทยาลัยเกษมบัณฑิต.

Alan, F. W. (1967). *Privacy and Freedom.* New York: Atheneu.

Arendt, H. (1973). *The Human Condition*. Chicago: University of Chicago Press.

Article 29 Working party of The European Union. (2011). *Opinion 15/2011 on the definition of consent.* (Online) Retrieved November 15, 2020, from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/

Article 29 Working party of The European Union. (2018). *Guidelines on consent under Regulation 2016/679,* (Online) Retrieved November 15, 2020, from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/

Bloustein. (1984). *Privacy as an Aspect of Human Dignity. “Philosophical Dimensions of privacy: An Anthology”, Schoeman, Ferdinand (ed.),* (UK: Cambridge University Press,

Cate, F. H. (1995). “The EU Data Protection Directive, Information Privacy, and the Public Interest”. *Iowa L. Rev, 80*, 431 - 443.

European Data Protection Board (EDPB) Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, 7 July 2021, pp 25-26

Fromholz, J. M. (2000). “The European Union data privacy directive”. *Berkeley Technology Law Journal, 15*(1), 460 - 484.

Information Commissioner’s Office (ICO), UK. (2018). *Guide to the General Data Protection Regulation (GDPR) (Online).* Retrieved November 12, 2020, from www.ico.org.uk/for-organisations/guide-to-data-protection

Donnelly. (1982). “Human Rights and Human Dignity”. *The American Law Review, 76*(2), 303-316.

Rubenfield, J. (1989). “The right of privacy”. *Harvard Law Review, 102*(4), 737 - 807.

Kuner, C. (2018) International Organizations and the EU General Data Protection Regulation*, International Organizations Law Review, 75,* 780-798.

Schoeman. (1984). Ferdinand, Privacy: Philosophical Dimensions of literature. “Philosophical Dimensions of Privacy: An Anthology”, Schoeman, Ferdinand (ed.), UK: Cambridge University Press.

Solove, D. (2006). “A Taxonomy of Privacy”. *University of Pennsylvania Law Review, 154*(3), 477 - 560.

Warren, D.S., & Brandies, D. (1890). “The Right to Privacy”. *Harvard Law Review, 4*(5), 193 - 220.


# SOUTHERN COLLEGE OF TECHNOLOGY

conference.
sct.ac.th

## วิทยาลัยเทคโนโลยีภาคใต้

124/1 ถ.ทุ่งสง-ห้วยยอด ต.ที่วัง อ.ทุ่งสง
จ.นครศรีธรรมราช 80110
โทรศัพท์ 0-7577-0136-7 โทรสาร 0-7553-8031
www.sct.ac.th