

**การคุ้มครองสิทธิผู้พักของหอพักเอกชนในกรณีการเก็บรวบรวมข้อมูลสแกนใบหน้าเพื่อ
ควบคุมการผ่านเข้าออก : ศึกษาข้อยกเว้นของความยินยอมตามพระราชบัญญัติคุ้มครอง
ข้อมูลส่วนบุคคล พ.ศ. 2562**

The Protection of The Rights of Resident of Private Dormitory in The Case of Collection
of Biometric Data as A Condition for Entering and Exiting The Dormitory: A Study of
The Application of Exceptions to Consent According to Personal Data Protection Act
B.E.2562

ชาญชัย แสวงศักดิ์¹ และ คณาธิป ทองรวีวงศ์,²
Chanchai Sawangsak¹ and Kanathip Thongrawewong²

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาวิเคราะห์ การตีความ และปรับใช้ ฐานทางกฎหมายตาม มาตรา 24 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในกรณีการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้พักของหอพักเอกชนเพื่อควบคุมการเข้าออก 2) ศึกษาวิเคราะห์ การตีความ และปรับใช้ ฐานทางกฎหมายตาม มาตรา 26 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในกรณีการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้พักของหอพักเอกชนในการควบคุมการเข้าออก งานวิจัยนี้ใช้วิธีวิจัยเชิงคุณภาพในการวิเคราะห์เนื้อหาเปรียบเทียบกับกฎหมายไทยและกฎหมายสหภาพยุโรป

ผลการวิจัยพบว่า 1) กรณีที่ผู้ประกอบการหอพักเอกชนเก็บรวบรวมข้อมูลส่วนบุคคลของผู้พักเพื่อควบคุมการผ่านเข้าออก โดยเป็นข้อมูลส่วนบุคคลทั่วไป เช่น การใช้บัตรอิเล็กทรอนิกส์ อาจอ้างข้อยกเว้นที่ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลตามมาตรา 24 (5) 2) กรณีที่ผู้ประกอบการหอพักเอกชนเก็บรวบรวมข้อมูลผู้พักเพื่อควบคุมการผ่านเข้าออก โดยเป็นประเภทข้อมูลส่วนบุคคลในประเภทการสแกนหน้าหรือภาพจำลองใบหน้า ซึ่งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล จัดเป็น “ข้อมูลชีวภาพ” เป็นกรณีที่ต้องพิจารณาฐานทางกฎหมายตามมาตรา 26 ซึ่งกฎหมายไม่ระบุข้อยกเว้นที่เฉพาะเจาะจงสำหรับกรณีการควบคุมการเข้าออกอาคาร แต่มีข้อยกเว้นที่เกี่ยวข้อง คือมาตรา 26(1) และ มาตรา 26(5) อย่างไรก็ตาม ผลการวิเคราะห์องค์ประกอบและเงื่อนไขตามตัวบทของข้อยกเว้นดังกล่าว ประกอบกับกฎหมายอื่นที่เกี่ยวข้อง เช่น พระราชบัญญัติหอพัก พ.ศ. 2558 พบว่า ผู้ประกอบการหอพักไม่มีหน้าที่หรืออำนาจตามกฎหมายในการเก็บรวบรวมข้อมูลสแกนหน้าหรือข้อมูลชีวภาพของผู้พัก จึงไม่เข้ากรณีข้อยกเว้นที่ไม่ต้องขอความยินยอมตามมาตรา 26 ดังนั้น งานวิจัยนี้จึงมีข้อเสนอแนะปฏิบัติแก่ผู้ประกอบการหอพักว่า 1) หากจะใช้วิธีการเก็บรวบรวมข้อมูลชีวภาพเช่นการสแกนใบหน้าผู้พักห้อง จะต้องขอความยินยอม ซึ่งจะต้องสอดคล้องกับเงื่อนไขตามกฎหมายด้วย 2) การปรับเปลี่ยนมาตรการควบคุมการเข้าออกโดยใช้วิธีการอื่นที่ไม่เก็บรวบรวมข้อมูลชีวภาพ เช่นการใช้คีย์การ์ด

¹ คณะนิติศาสตร์ มหาวิทยาลัยเกษมบัณฑิต; Faculty of Law, Kasem Bhandit University.

² คณะนิติศาสตร์ มหาวิทยาลัยเกษมบัณฑิต; Faculty of Law, Kasem Bhandit University, E-mail:

kanathip.tho@kbu.ac.th

คำสำคัญ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ข้อมูลชีวภาพ การสแกนใบหน้า หอพักเอกชน

ABSTRACT

This research aims to 1) study, analyze, interpret and apply the legal basis according to Section 24 of the Personal Data Protection Act B.E.2562 in the case of collecting personal data of residents of private dormitories to control entry and exit; and 2) study, analyze, interpret and apply the legal basis according to Section 26 of the Personal Data Protection Act in the case of collecting personal data of residents of private dormitories to control entry and exit. This research uses qualitative research methods to analyze the comparative content of Thai law and European Union law.

The research results found that: 1) In the case where private dormitory operators collect personal data of residents to control access, which is general personal information such as the use of electronic cards, they may refer to an exception that does not require consent from the data subject according to Section 24 (5). 2) In the case where private dormitory operators collect face scan of residents to control access, which under the Personal Data Protection Act is classified as biometric data, this is a case that requires consideration of the exception of consent according to Section 26. However, the Act does not specify specific exceptions for controlling building access, but there are related exceptions, namely Sections 26(1) and 26(5). However, the analysis of the elements and conditions according to the text of the aforementioned exceptions, together with other relevant laws, especially the Dormitory Act B.E. 2558 found that dormitory operators do not have the duty or authority by law to collect facial scans or biometric data of residents. Therefore, it does not fall under the exception that does not require consent according to Section 26. Consequently, this research has recommendations for dormitory operators as follows: 1) obtaining consent from residents in case of scanning face for entering the dormitory. 2) Modifying the access control measures by using other methods that do not collect biometric data, such as using key cards.

Keywords: Personal Data Protection Act, Biometric Data, Face Scan, Private Dormitory.

บทนำ

ในเดือน พฤษภาคม พ.ศ.2561 กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ของสหภาพยุโรป ได้แก่ “General Data Protection Regulation” หรือ “GDPR” มีผลใช้บังคับแทนที่ กฎหมายฉบับเดิม คือ “Directive 95/46/EC” ส่งผลกระทบต่อหลายภาคส่วนที่เกี่ยวข้องกับข้อมูลระบุตัวตนของบุคคล (Personal data) ทั้งผู้ประกอบการขนาดใหญ่ กลางและย่อม ผู้เป็นเจ้าของข้อมูลส่วนบุคคล (Kuner, 2018) กฎหมายนี้มีแนวคิดพื้นฐานเกี่ยวกับการคุ้มครองความเป็นอยู่ส่วนตัว (Right to privacy) แต่มีขอบเขตจำกัดเฉพาะในด้านข้อมูลของบุคคล (Solove, 2006) โดยแนวคิดและหลักการปรากฏในความตกลงระหว่างประเทศหลายฉบับ (Voss,

2017) ในส่วนของประเทศไทย ก่อนปี พ.ศ. 2562 ไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ แต่มีกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น กฎหมายคุ้มครองข้อมูลเฉพาะบางภาคส่วนของธุรกิจ เช่น ธุรกิจการเงิน อย่างไรก็ตามในเดือนกุมภาพันธ์ปี พ.ศ. 2562 สภานิติบัญญัติแห่งชาติได้ลงมติเห็นชอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและประกาศในราชกิจจานุเบกษาในเดือนพฤษภาคม พ.ศ. 2562 แม้ว่ากฎหมายนี้ร่างขึ้นโดยอาศัยรูปแบบของกฎหมายสหภาพยุโรปแต่ก็มีหลายประเด็นที่แตกต่างกัน รวมทั้งส่งผลกระทบต่อผู้ประกอบการในหลายแง่มุม เช่น การสร้างต้นทุนในการปฏิบัติตามเงื่อนไขต่าง ๆ ให้สอดคล้องกับกฎหมาย (Compliance cost) (คณาธิป ทองรวิวงศ์, 2564:1) ซึ่งเมื่อพิจารณาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พบว่ากำหนดหลักการที่สำคัญสองส่วนที่อยู่บนแนวคิดแตกต่างกัน (คณาธิป ทองรวิวงศ์, 2564) คือ 1) กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความปลอดภัย ซึ่งอยู่บนพื้นฐานแนวคิดความมั่นคงปลอดภัยของข้อมูลหรือความมั่นคงปลอดภัยสารสนเทศ (Information security) 2) กำหนดให้ผู้ควบคุมข้อมูลต้องอ้างอิงฐานทางกฎหมาย (Legal or lawful basis of processing personal data) ซึ่งอยู่บนพื้นฐานการคุ้มครองสิทธิของเจ้าของข้อมูล เช่น การขอความยินยอมจากเจ้าของข้อมูล หรืออ้างอิงฐานทางกฎหมายอื่นอันเป็นข้อยกเว้นของความยินยอมตามที่กฎหมายระบุไว้ สำหรับงานวิจัยนี้จะศึกษาหลักการส่วนที่สอง กล่าวคือ ในกรณีผู้ประกอบการหรือผู้ให้บริการที่กำหนดให้มีมาตรการรักษาความปลอดภัยในการควบคุมการเข้าออกอาคาร รวมทั้งตรวจสอบสิทธิว่าบุคคลที่เข้าออกเป็นผู้ที่ถูกต้องตามสัญญาหรือไม่ ซึ่งเดิมใช้วิธีการที่ไม่เกี่ยวข้องกับข้อมูลชีวภาพ เช่น การใช้บัตรผ่านเข้าออก หรือ คีย์การ์ด ฯลฯ โดยในปัจจุบันผู้ประกอบการหรือผู้ให้บริการหลายแห่ง จัดซื้ออุปกรณ์และระบบการสแกนใบหน้าหรือม่านตาของผู้พัก การดำเนินการดังกล่าวเป็นการเก็บรวบรวมข้อมูลส่วนบุคคล โดยจัดเป็นประเภท ข้อมูลชีวภาพ (Biometric) ส่งผลให้ผู้ประกอบการหรือผู้ให้บริการอยู่ในสถานะผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ดังกล่าว และมีหน้าที่อ้างอิงฐานทางกฎหมายในการเก็บรวบรวม ใช้เปิดเผยข้อมูลส่วนบุคคล ซึ่งพบว่ามีมาตราที่เกี่ยวข้องคือมาตรา 24 และ มาตรา 26 เป็นต้น ซึ่งโดยหลักจากมาตราดังกล่าว ผู้ประกอบการหรือผู้ให้บริการต้องอาศัยฐานทางกฎหมาย โดยเฉพาะการขอความยินยอม อย่างไรก็ตาม เนื่องจากกฎหมายกำหนดข้อยกเว้นหลายประการที่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องขอความยินยอม แต่ยังไม่ชัดเจนว่าในกรณีของผู้ประกอบการหรือผู้ให้บริการจะสามารถอ้างข้อยกเว้นข้อใด ในการศึกษาวิจัยครั้งนี้ ผู้วิจัยจึงทำการศึกษากฎหมายที่ผู้ประกอบการหรือผู้ให้บริการไม่ขอความยินยอมแต่จะอ้างข้อยกเว้นตามมาตรา 24 มาตรา 26 ในการเก็บรวบรวมข้อมูลการสแกนใบหน้าผู้พักว่าจะสามารถทำได้หรือไม่และอาศัยฐานทางกฎหมายใดเนื่องจากกฎหมายไม่ได้ระบุในกรณีนี้ไว้เป็นการเฉพาะ

วัตถุประสงค์ของการวิจัย

1. ศึกษาวิเคราะห์ การตีความและปรับใช้ ฐานทางกฎหมายตาม มาตรา 24 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในกรณีการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้พักในหอพักเอกชนเพื่อควบคุมการเข้าออกอาคาร

2. ศึกษาวิเคราะห์ การตีความและปรับใช้ ฐานทางกฎหมายตาม มาตรา 26 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในกรณีการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้พักในหอพักเอกชนเพื่อควบคุมการเข้าออกอาคาร

วิธีดำเนินการวิจัย

งานวิจัยนี้เป็นการวิจัยเอกสาร (Documentary Research) ตามกระบวนการดังนี้

1. ข้อมูลที่นำมาวิเคราะห์ ประกอบด้วย ตัวบทกฎหมาย ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป (General Data Protection Regulation หรือ GDPR) แนวปฏิบัติของหน่วยงานกำกับหรือบังคับใช้กฎหมาย วรรณกรรมเกี่ยวกับแนวคิดทฤษฎีทางกฎหมายที่เกี่ยวข้อง รวมทั้งการตีความจากงานวิชาการ งานวิจัย บทความวิชาการ

2. การวิเคราะห์ข้อมูล ใช้วิธีการวิเคราะห์เชิงเนื้อหา (Content Analysis) โดยวิเคราะห์ด้วยทฤษฎีองค์ประกอบ

นิยามการวิจัย

“ผู้พัก” มีความหมายตาม พระราชบัญญัติหอพัก คือ ผู้ซึ่งอยู่ระหว่างการศึกษาในสถานศึกษาในระดับไม่สูงกว่าปริญญาตรีและมีอายุไม่เกินยี่สิบห้าปี

“หอพักเอกชน” มีความหมายตาม พระราชบัญญัติหอพัก คือ หมายความว่า หอพักที่ผู้ประกอบการหอพักเป็นบุคคลทั่วไปซึ่งไม่ใช่สถานศึกษา

“ผู้ประกอบการหอพัก” มีความหมายตามพระราชบัญญัติหอพัก คือ ผู้ได้รับใบอนุญาตประกอบกิจการหอพักตามพระราชบัญญัติหอพัก

ขอบเขตการวิจัย

ขอบเขตในแง่ประเภทของผู้ควบคุมข้อมูลส่วนบุคคล ในการศึกษานี้ได้แก่ หอพัก ตามพระราชบัญญัติหอพัก แบ่งเป็นสองประเภทหลักคือ หอพักสถานศึกษา ซึ่งผู้ประกอบการเป็นสถานศึกษา เช่น หอพักของมหาวิทยาลัย และ หอพักเอกชนซึ่งผู้ประกอบการเป็นบุคคลทั่วไปที่มีใช่สถานศึกษา แต่การศึกษาวินัยครั้งนี้มีขอบเขตเฉพาะหอพักเอกชนที่มีใช่สถานศึกษาเท่านั้น

ขอบเขตในแง่ประเด็นทางกฎหมายเกี่ยวกับข้อมูลส่วนบุคคล เนื่องจากการเก็บรวบรวมข้อมูลชีวภาพของผู้พักในหอพักนั้น มีประเด็นในแง่ฐานทางกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลสองประเด็นหลักคือ 1. การขอความยินยอมอย่างไรชอบด้วยกฎหมาย และ 2 การอ้างข้อยกเว้นของความยินยอมซึ่งในการศึกษานี้จำกัดขอบเขตเฉพาะประเด็นการอ้างข้อยกเว้นของความยินยอมเท่านั้น

กรอบแนวคิดและทฤษฎีของการวิจัย

หัวข้อนี้จะทบทวนกรอบแนวคิดทฤษฎีที่เกี่ยวกับข้อก้ำกับการคุ้มครองข้อมูลชีวภาพซึ่งเป็นข้อมูลส่วนบุคคลของเจ้าของข้อมูลอันเป็นพื้นฐานหลักการของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีหลักสำคัญสองส่วนที่อยู่บนแนวคิดแตกต่างกัน (คณาธิป ทองรวิวงศ์, 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 & Brandeis, 1890) แต่การพิจารณาในแง่ปราศจากการแทรกแซงหรือความลับอาจทำให้สิทธินี้กว้างเกินไป โดยเฉพาะในสภาพสังคมที่มีการติดต่อระหว่างบุคคล ทำให้การไม่ถูกแทรกแซงเป็นไปได้ยาก (Alan, 1967) ต่อมา มีการพัฒนาแนวคิดว่าหมายถึง การจำกัดการเข้าถึงปัจเจกชนโดยบุคคลอื่น (Rubenfield, 1989) ในทางวิชาการ สิทธิดังกล่าวยังคงมีความหมายและขอบเขตกว้าง (Schoeman, 1984) โดยจำแนกได้หลายมิติ รวมถึงการคุ้มครองข้อมูลส่วนบุคคล (Solove, 2006)

ทั้งนี้ตามกฎหมายสหรัฐอเมริกา สิทธิในความเป็นอยู่ส่วนตัว ปรากฏในกฎหมาย คอมมอนลอว์และกฎหมายอื่น เช่นกฎหมายลักษณะละเมิด (Bloustein, 1984) เมื่อพิจารณาในระดับกฎหมายระหว่างประเทศ พบว่า กติการากว่าด้วยสิทธิทางแพ่งและการเมืองของสหประชาชาติ (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 (General Data Protection Regulation หรือ GDPR) มีผลใช้บังคับแทนกฎหมายเดิม (Directive 95/46/EC) โดยมีหลักการสำคัญเช่นเดิมคือ การเก็บรวบรวมใช้เปิดเผยข้อมูลส่วนบุคคลของผู้ที่ต้องอ้างอิงฐานทางกฎหมาย ซึ่งโดยหลักต้องอาศัยฐานความยินยอม เว้นแต่เข้าองค์ประกอบฐานอื่นที่กฎหมายกำหนด

ในส่วนของประเทศไทย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีองค์ประกอบและโครงสร้างหลักตามตัวแบบกฎหมายสหภาพยุโรป โดยเฉพาะอย่างยิ่ง การกำหนดหลักการเกี่ยวกับ “ฐานทางกฎหมาย” (Legal basis) กล่าวคือ การเก็บรวบรวมใช้เปิดเผยข้อมูลส่วนบุคคลของผู้อื่นจะต้องอ้างอิงฐานที่กฎหมายระบุ ซึ่งฐานหลักคือ “ความยินยอม” ตามมาตรา 19 มาตรา 24 มาตรา 26 เป็นต้น ทั้งนี้ ผู้ควบคุมข้อมูลอาจอ้างฐานยกเว้นจากความยินยอมได้ต่อเมื่อเข้ากรณีที่มาตราดังกล่าวระบุไว้เท่านั้น เช่น ประโยชน์โดยชอบด้วยกฎหมายเพื่อการรักษาความปลอดภัยตามมาตรา 24 (5) สำหรับกรณีข้อมูลชีวภาพ เช่น ลายนิ้วมือ ภาพจำลองใบหน้า มีฐานที่กำหนดไว้เฉพาะตามมาตรา 26 จะเห็นได้ว่า กฎหมายกำหนดฐานความยินยอมไว้เป็นหลัก จึงสะท้อนให้เห็นถึงความเชื่อมโยงกับแนวคิดเกี่ยวกับการคุ้มครองสิทธิเจ้าของข้อมูลที่จะสามารถเลือกตัดสินใจเกี่ยวกับข้อมูลส่วนบุคคลของตน โดยในส่วนของข้อยกเว้นที่สามารถเก็บรวบรวมข้อมูลโดยไม่ต้องขอความยินยอมนั้น โดยหลักแล้วเป็นการจำกัดสิทธิจึงต้องตีความอย่างเคร่งครัดเฉพาะที่กฎหมายระบุไว้เท่านั้น

ผลการวิจัย

1. กรณีที่ผู้ประกอบกิจการหอพักเก็บรวบรวมข้อมูลของผู้พักเพื่อควบคุมการผ่านเข้าออก โดยเป็นประเภทข้อมูลส่วนบุคคลทั่วไปที่มีได้ระบุในมาตรา 26 เช่น การใช้บัตรอิเล็กทรอนิกส์ หรือ คีย์การ์ด ซึ่งเชื่อมโยงไปยังข้อมูลระบุตัว เช่น ชื่อ นามสกุลผู้พัก เป็นกรณีที่ต้องพิจารณาฐานทางกฎหมายตามมาตรา 24 ซึ่งผู้ประกอบกิจการหอพักอาจอ้างข้อยกเว้นที่ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลตามมาตรา 24 (5) เนื่องจากการรักษาความปลอดภัยและการตรวจสอบสิทธิผู้พักจัดเป็นประโยชน์โดยชอบด้วยกฎหมาย (Legitimate interest) ของผู้ประกอบกิจการหอพัก อย่างไรก็ตาม ในกรณีที่ผู้ประกอบกิจการหอพักใช้วิธีการเก็บรวบรวมข้อมูลชีวภาพเช่น การสแกนใบหน้า จะไม่สามารถอ้างฐานตามมาตรา 24 (5) เนื่องจากข้อมูลชีวภาพจะต้องพิจารณาฐานที่กำหนดโดยเฉพาะตามมาตรา 26

2. กรณีที่ผู้ประกอบกิจการหอพักเก็บรวบรวมข้อมูลเพื่อควบคุมการผ่านเข้าออก โดยเป็นประเภทข้อมูลส่วนบุคคลในประเภทการสแกนหน้าหรือภาพจำลองใบหน้า (Biometric) เป็นกรณีที่ต้องพิจารณาฐานทางกฎหมายตามมาตรา 26 โดยผู้ประกอบกิจการหอพักอาจอ้างข้อยกเว้นที่ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลตามมาตรา 26 ซึ่งกฎหมายไม่ระบุข้อยกเว้นที่เฉพาะเจาะจงสำหรับกรณีการควบคุมการเข้าออกแต่มีข้อยกเว้นที่เกี่ยวข้องและอาจปรับใช้ได้คือ มาตรา 26 (1) มาตรา 26 (5) อย่างไรก็ตาม จากการวิเคราะห์องค์ประกอบและเงื่อนไขตามตัวบทของข้อยกเว้นประกอบกับกฎหมายเฉพาะสำหรับกิจการนี้ คือ พระราชบัญญัติหอพัก พบว่า ผู้ประกอบกิจการหอพักไม่มีอำนาจหน้าที่ตามกฎหมายในการเก็บรวบรวมข้อมูลสแกนหน้าหรือข้อมูลชีวภาพ จึงไม่เข้ากรณีข้อยกเว้นที่ไม่ต้องขอความยินยอมตามมาตรา 26

สรุปผลและอภิปรายผล

ผลการศึกษาพบว่า ในภาพรวมของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหลักการเกี่ยวกับฐานทางกฎหมาย (Legal Basis) อันเป็นเงื่อนไขของการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้อื่นแตกต่างกันโดยจำแนกตามประเภทข้อมูลส่วนบุคคล กล่าวคือ กรณีข้อมูลส่วนบุคคลทั่วไป จะอยู่ภายใต้มาตรา 24 ที่วางหลักว่าต้องขอความยินยอมจากเจ้าของข้อมูลก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล แต่มีข้อยกเว้น ตามมาตรา 24 (1)-(6) สำหรับกรณีข้อมูลส่วนบุคคลตามมาตรา 26 ซึ่งรวมถึงข้อมูลชีวภาพ เช่น การสแกนใบหน้า จะต้องอาศัยความยินยอมเช่นเดียวกับมาตรา 24 แต่มีข้อยกเว้นเฉพาะตามมาตรา 26 (1)-(5) ดังนั้น ในการวิเคราะห์การตีความและปรับใช้ ฐานทางกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในกรณีที่ผู้ประกอบกิจการหอพักเก็บรวบรวมข้อมูลส่วนบุคคลของผู้พักเพื่อเป็นเงื่อนไขการเข้าออกอาคารอันจัดเป็นวัตถุประสงค์เพื่อการรักษาความปลอดภัยหรือตรวจสอบสิทธิผู้พัก จึงแยกพิจารณาเป็นสองกรณีคือ

กรณีที่หนึ่ง ผู้ประกอบกิจการหอพักเก็บรวบรวมข้อมูลส่วนบุคคลทั่วไปที่มีได้ระบุในมาตรา 26 เช่น การใช้บัตรอิเล็กทรอนิกส์ หรือ คีย์การ์ด ซึ่งเชื่อมโยงไปยังข้อมูลระบุตัวทั่วไป เช่น ชื่อ นามสกุลผู้พัก ดังนี้ ต้องพิจารณาฐานทางกฎหมายตามมาตรา 24 ในส่วนผลการวิจัยตามวัตถุประสงค์ข้อ 1 พบว่าข้อยกเว้นของความยินยอมตามมาตรา 24 อาจนำมาปรับใช้กับกรณีหอพักได้แก่ การอ้างฐานทางกฎหมายตามมาตรา 24 (5) ที่เรียกว่าประโยชน์โดยชอบด้วยกฎหมาย (Legitimate interest) ฐานนี้เทียบเคียงได้กับกฎหมายสหภาพยุโรป (มาตรา 6 (1) (f) , legitimate interests pursued by the controller) ซึ่งต้องประเมินผลกระทบต่อเจ้าของข้อมูล

(Legitimate interest assessment หรือ LIA) จากหลายปัจจัย (European Data Protection Board, 2024) เช่น ประเมินวัตถุประสงค์ (Purpose Test) เช่น ป้องกันการฉ้อโกง (fraud prevention) เพื่อความมั่นคงปลอดภัยของข้อมูลและโครงข่าย (network and information security) (GDPR, Recital 47, Recital 49) และ ยังต้องนำวัตถุประสงค์ดังกล่าวมาซึ่งน้ำหนักกว่ามีความจำเป็น (Necessity) เพียงใด และมีความสมดุลเมื่อเทียบกับผลกระทบต่อเจ้าของข้อมูลหรือไม่ (Balancing Test) (Information Commissioner's Office UK (ICO), 2018) เมื่อพิจารณาวัตถุประสงค์ของการติดตั้งระบบคัดกรองหรือควบคุมคนเข้าออกอาคารที่ประกอบกิจการหอพักแล้วพบว่า โดยทั่วไปหากใช้วิธีการเก็บรวบรวมข้อมูลส่วนบุคคลเช่น การใช้กล้องวงจรปิด (CCTV) การใช้วิธีการแลกเปลี่ยนบัตรเข้าออก หรือการใช้คีย์การ์ด ซึ่งเป็นการเก็บรวบรวมข้อมูลระบุตัวทั่วไป จะตกอยู่ภายใต้ มาตรา 24 และสามารถอ้างฐานประโยชน์โดยชอบด้วยกฎหมายตามมาตรา 24 (5) นี้ได้ ซึ่งหากผู้ประกอบการหอพักดำเนินการตามแนวทางนี้จะสอดคล้องกับการอ้างข้อยกเว้นของความยินยอมตามแนวทาง สหภาพยุโรป (Information Commissioner's Office UK (ICO), 2018) (European Data Protection Board ,2024)

กรณีที่สอง ผู้ประกอบการหอพักเก็บรวบรวมข้อมูลมาตรา 26 เช่น ข้อมูลการสแกนใบหน้าหรือลายนิ้วมือ ไม่สามารถอ้างฐานตามมาตรา 24 (5) แม้ว่าจะเป็นไปเพื่อวัตถุประสงค์ในการรักษาความปลอดภัย และตรวจสอบสิทธิเช่นเดียวกับกรณีหนึ่ง เนื่องจากฐานมาตรานี้ใช้กับกรณีข้อมูลส่วนบุคคลทั่วไป หากเป็นข้อมูลชีวภาพจะต้องพิจารณาฐานเฉพาะตามมาตรา 26

2. ผลการศึกษาพบว่า ในกรณีที่ผู้ควบคุมข้อมูลทำการเก็บรวบรวมข้อมูลประเภทการสแกนใบหน้าตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจัดเป็น “ข้อมูลชีวภาพ” โดยต้องพิจารณาฐานทางกฎหมายตามมาตรา 26 ซึ่งโดยหลักต้องขอความยินยอมจากเจ้าของข้อมูล แต่มาตรานี้กำหนดฐานอันเป็นข้อยกเว้นตามมาตรา 26 (1)-(5) อย่างไรก็ดีตาม ข้อยกเว้นดังกล่าวไม่ได้ระบุเจาะจงถึงกรณีการเก็บรวบรวมข้อมูลเพื่อควบคุมการเข้าออกอาคาร จึงต้องวิเคราะห์การตีความและปรับใช้กฎหมายว่าในกรณีผู้ประกอบการหอพักเก็บรวบรวมข้อมูลส่วนบุคคลประเภทการสแกนใบหน้าของผู้พักเพื่อเป็นเงื่อนไขการเข้าออกอาคารอันจัดเป็นวัตถุประสงค์เพื่อการรักษาความปลอดภัยหรือตรวจสอบสิทธิผู้พักจะปรับใช้ข้อยกเว้นใด ซึ่งเมื่อพิจารณาตัวบทแล้วพบว่าเกี่ยวข้องกับข้อยกเว้นมาตรา มาตรา 26 (1) มาตรา 26 (5) โดยแยกวิเคราะห์ดังนี้

2.1 การอ้างข้อยกเว้นที่ไม่ต้องขอความยินยอม มาตรา 26 (1) เพื่อป้องกันอันตรายต่อชีวิต สุขภาพ ฯลฯ ซึ่งเทียบได้กับฐานประโยชน์สำคัญ (Vital interest) ตามมาตรา 9(2)(c) ของกฎหมายสหภาพยุโรป และจากแนวทางตีความของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสหราชอาณาจักรพบว่า ฐานนี้จำกัดเฉพาะกรณีที่เจ้าของข้อมูลอยู่ในสภาวะไม่สามารถแสดงเจตนายินยอม (Incapable of giving consent) ซึ่งอาจเกิดจากลักษณะทางกายภาพ (Physical) เช่น บาดเจ็บหรือป่วยจนไม่รู้สติตัว หรือไม่สามารถให้ความยินยอมได้ โดยเหตุทางกฎหมาย เช่น เป็นคนไร้ความสามารถ (Information Commissioner's Office UK (ICO), 2018) ดังนั้นในกรณีที่ผู้ประกอบการหอพักกำหนดเงื่อนไขให้ผู้พักต้องเก็บรวบรวมข้อมูลสแกนใบหน้าจึงสามารถผ่านเข้าออก แม้จะอ้างว่าการดำเนินการดังกล่าวเป็นไปเพื่อรักษาความปลอดภัยหรือป้องกันอันตรายต่อชีวิตของผู้พักที่อาจเกิดจากผู้บุกรุกหรืออาชญากรรม แต่หากไม่ปรากฏว่าผู้พักนั้นอยู่ในสภาวะที่ไม่สามารถแสดงเจตนายินยอมได้ ก็ไม่เข้าเงื่อนไขข้อยกเว้นและต้องขอความยินยอม

2.2 การอ้างข้อยกเว้นที่ไม่ต้องขอความยินยอม มาตรา 26 (5) ซึ่งเป็นกรณี “จำเป็นในการปฏิบัติตามกฎหมาย...” เห็นได้ว่า องค์ประกอบเงื่อนไขหลักของมาตรา 26 (5) คือต้องเป็นกรณีที่มีกฎหมายกำหนด จึงต้องวิเคราะห์ว่า มีกฎหมายฉบับใดให้อำนาจหรือกำหนดหน้าที่แก่ผู้ประกอบการหรือพนักงานในการเก็บรวบรวมข้อมูลโดยสแกนหน้าผู้พักหรือไม่ ซึ่งจากการศึกษากฎหมายที่เกี่ยวข้องพบว่ากฎหมายเฉพาะเกี่ยวกับหอพักคือ พระราชบัญญัติหอพัก พ.ศ.2558 กำหนดหน้าที่แก่ผู้ประกอบการหรือผู้จัดการไว้หลายประการ โดยในกรณีที่เกี่ยวข้องกับการควบคุมการเข้าออกและการรักษาความปลอดภัยมีบทมาตราที่เกี่ยวข้องคือ

- มาตรา 59 ผู้ประกอบการหรือหอพักต้องจัดให้มีระเบียบประจำหอพัก ซึ่งต้องมีรายละเอียด เช่น เวลาเข้าออกหอพัก

- มาตรา 62 (2) กำหนดให้ผู้ประกอบการหรือหอพักและผู้จัดการหอพักมีหน้าที่ดูแลรักษาความปลอดภัยด้านสุขลักษณะและอนามัยของหอพักให้เป็นไปตามกฎหมายว่าด้วยการสาธารณสุข

- มาตรา 63 กำหนดให้ผู้จัดการหอพัก ต้องจัดทำทะเบียนผู้พักแต่ละรายส่งให้นายทะเบียน โดยต้องมีรายการ เช่น ชื่อ อายุและเพศของผู้พัก เลขบัตรประจำตัวประชาชน ชื่อบิดามารดาหรือผู้ปกครองของผู้พักลายมือชื่อผู้พัก

- มาตรา 64 กำหนดให้ผู้จัดการหอพักมีหน้าที่ ดูแลไม่ให้บุคคลอื่นที่ไม่ใช่ผู้พักเข้าไปในหอพัก

จากเนื้อหาของตัวบทมาตราที่เกี่ยวข้องเห็นได้ว่า แม้พระราชบัญญัตินี้จะมีบทบัญญัติให้ทำหน้าที่กำหนดระเบียบควบคุมการเข้าออกและดูแลไม่ให้บุคคลอื่นเข้าหอพัก แต่ไม่ได้กำหนดรายละเอียดโดยเจาะจงให้เก็บรวบรวมข้อมูลชีวภาพเช่นการสแกนหน้า นอกจากนี้ กฎหมายกำหนดให้ผู้ประกอบการหรือหอพักมีหน้าที่ส่งข้อมูลผู้พักให้นายทะเบียนตามกฎหมาย แต่ก็มีได้กำหนดให้ต้องส่งข้อมูลการสแกนหน้า สำหรับกรณีที่ผู้ประกอบการหรือหอพักกำหนดเงื่อนไขการเก็บรวบรวมข้อมูลชีวภาพหรือสแกนหน้าในระเบียบของหอพักที่สามารถกำหนดขึ้นได้ตามพระราชบัญญัติหอพัก แต่ระเบียบดังกล่าวก็ไม่ได้มีสถานะเป็นกฎหมายตามนัยของมาตรา 26 (5) ดังนั้นเมื่อนำหลักกฎหมายตามพระราชบัญญัติหอพักมาพิจารณาเงื่อนไขตามมาตรา 26 ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล จะเห็นได้ว่า การอ้างข้อยกเว้นในการเก็บรวบรวมข้อมูลชีวภาพโดยไม่ต้องขอความยินยอมตามมาตรา 26 (5) ต้องตีความโดยเคร่งครัดเนื่องจากเป็นข้อยกเว้นที่จำกัดสิทธิในการให้ความยินยอมของเจ้าของข้อมูล การอ้างมาตรานี้จึงต้องปรากฏว่ามีกฎหมายอื่นที่กำหนดอย่างเจาะจงให้เก็บรวบรวมข้อมูลมาตรา 26 เช่น ประกาศธนาคารแห่งประเทศไทย ที่ สนส.19/2562 ว่าด้วยการพิสูจน์ตัวตนลูกค้าแบบไม่พบเห็นลูกค้าต่อหน้า (Non face to face) กำหนดให้ธนาคารต้องเปรียบเทียบข้อมูลสแกนหน้าลูกค้า (Biometric comparison) เปรียบเทียบกับแนวทางกฎหมายสหภาพยุโรป หรือ General Data Protection Regulation การเก็บรวบรวมข้อมูลสแกนใบหน้าอาจเข้าข้อยกเว้นความยินยอมในกรณีที่มีกฎหมายกำหนดเฉพาะและเพื่อวัตถุประสงค์เจาะจงเกี่ยวกับการปฏิบัติตามกฎหมาย เช่น การปราบปรามอาชญากรรมหรือการบังคับใช้กฎหมายของเจ้าหน้าที่ (European Data Protection Board ,2023) ด้วยเหตุนี้ ผู้ประกอบการหรือหอพักจึงไม่สามารถอ้างมาตรา 26 (5) เป็นข้อยกเว้นของความยินยอมในการเก็บรวบรวมข้อมูลโดยสแกนหน้าผู้พัก

ดังนั้นผลการวิจัยในข้อ 2 จึงชี้ให้เห็นว่า ในกรณีผู้ประกอบการหรือหอพักใช้วิธีการเก็บรวบรวมข้อมูลชีวภาพ เช่น สแกนใบหน้าผู้พักเพื่อการรักษาความปลอดภัยหรือตรวจสอบการผ่านเข้าออกอาคารนั้น จะไม่สามารถอ้างข้อยกเว้นของความยินยอมได้ การตีความนี้สอดคล้องกับการอ้างข้อยกเว้นของความยินยอมตาม

แนวทางการตีความและแนวปฏิบัติของกฎหมายสหภาพยุโรป (European Data Protection Board, 2024) รวมทั้งแนวปฏิบัติของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศที่มีกฎหมายตามแนวทาง GDPR เช่น สหราชอาณาจักร (Information Commissioner's Office UK (ICO), 2018)

ข้อเสนอแนะการวิจัย

1. ข้อเสนอแนะในการบริหารจัดการของผู้ประกอบกิจการหอพักมีว่า หากผู้ประกอบธุรกิจให้เช่าอพาร์ทเมนท์จะใช้มาตรการควบคุมการเข้าออกอาคารด้วยการให้สแกนใบหน้าจะต้องขอความยินยอมจากผู้พักซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลโดยจัดทำเอกสารที่มีรายละเอียดตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้

2. เสนอให้ผู้ประกอบกิจการหอพักลดความเสี่ยงจากข้อพิพาททางกฎหมายโดยใช้วิธีอื่นนอกเหนือจากการสแกนหน้า ม่านตาหรือลายนิ้วมืออันเป็นข้อมูลตามมาตรา 26 เช่นการให้ทางเลือกในการสแกนบัตรหรือiscard

เอกสารอ้างอิง

- คณาธิป ทองรวีวงศ์. (2564ก). *หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล*. กรุงเทพฯ: สำนักพิมพ์นิติธรรม.
- คณาธิป ทองรวีวงศ์. (2564ข). ผลกระทบทางลบอันเกิดจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. *วารสารรัฐศาสตร์ภาคย์ม* 5(16), 42-56
- คณาธิป ทองรวีวงศ์. (2565). *การคุ้มครองสิทธิในการให้ความยินยอมของลูกจ้างจากกรณีนายจ้างขอความยินยอมในการเก็บรวบรวมข้อมูลชีวภาพเพื่อวัตถุประสงค์บันทึกเวลาและตรวจสอบการทำงาน*. รายงานวิจัยฉบับสมบูรณ์. กรุงเทพฯ: มหาวิทยาลัยเกษมบัณฑิต.
- คณาธิป ทองรวีวงศ์ และ ชาญชัย แสงศักดิ์. (2568). *การคุ้มครองสิทธิผู้พักอพาร์ทเมนท์ต่อการเก็บรวบรวมข้อมูลชีวภาพเพื่อควบคุมการเข้าออกอาคาร: ศึกษากรณีความยินยอมของเจ้าของข้อมูล*, รายงานสืบเนื่องการประชุมวิชาการ การประชุมระดับชาติและระดับนานาชาติเบญจมิตรวิชาการ เล่มที่ 5 (มนุษยศาสตร์และสังคมศาสตร์)
- Alan F. W. (1967). *Privacy and Freedom*. New York: Atheneu.
- Arendt, H. (1973). *The Human Condition*. Chicago: University of Chicago Press.
- Bloustein, E. (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.
- Donnelly, J. (1982). "Human Rights and Human Dignity". *The American Law Review*, 76(2): 303-316.
- European Data Protection Board (EDPB) (2024). *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, October 2024*.
- European Data Protection Board (EDPB) (2023). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0, April 2023*.

- Fromholz, J. M. (2000). "The European Union data privacy directive". *Berkeley technology law journal*, 15(1): 460 - 484. *Hall Law Review*, 47(2), pp. 512-535.
- Information Commissioner's Office (ICO), UK (2018). *Guide to the General Data Protection Regulation (GDPR)*. <https://www.ico.org.uk/for-organisations/guide-to-data-protection>
- Kuner, C. (2018). International Organizations and the EU General Data Protection Regulation, *International Organisations Law Review*, 75, 780-798.
- Rubinfeld, J. (1989). "The Right of Privacy". *Harvard Law Review*, 102(4): 737 - 807. *Journal of Communication & Strategy*, 97, 41-58.
- Schoeman. (1984). *Ferdinand, Privacy: Philosophical Dimensions of literature*. "Philosophical Dimensions of privacy: An Anthology", Schoeman, Ferdinand (ed.), UK: Cambridge University Press.
- Solove, D. (January 2006). "A Taxonomy of Privacy". *University of Pennsylvania Law Review*, 154(3), 477 - 560.
- Warren S, & Brandies, D. (1890). "The Right to Privacy". *Harvard Law Review*, 4(5), 193 - 220.