ทัศนมิติว่าด้วยสิทธิความเป็นส่วนตัวบนสื่อสังคมและกลไกปกป้อง*

Perspectives on Social Media Privacy Rights and Protection Mechanisms

ณัฐพล ยิ้มยวน (Nathapol Yimyuan)**

วศิณ ชูประยูร (Vasin Chooprayoon)***

*วิทยานิพนธ์หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต

**นักศึกษาปริญญาโท, หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต, E-mail: nathapol.y@rsu.ac.th

***ผู้ช่วยศาสตรจารย์, ผู้อำนวยการหลักสูตรการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต, E-mail: vasin@rsu.ac.th

ได้รับบทความ: 16 มี.ค. 63 / แก้ไขปรับปรุง: 19 พ.ย. 63 / อนุมัติให้ตีพิมพ์: 9 ธ.ค. 63 / เผยแพร่ออนไลน์: 17 ธ.ค. 63

DOI: 10.14456/rilj.2020.13

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษา 1) สิทธิความเป็นส่วนตัวบนสื่อสังคม และ 2) กลไกปกป้องความเป็นส่วนตัวบนสื่อสังคม การวิจัยนี้เป็นการวิจัยเชิงปริมาณ ใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง ซึ่งเป็นบุคลากรสายสนับสนุนของมหาวิทยาลัยรังสิต จำนวน 263 คน สถิติที่ใช้ในการวิเคราะห์ข้อมูล ได้แก่ ก) สถิติพื้นฐาน (การแจกแจงความถี่ ร้อยละ ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน) และ ข) สถิติเชิงอนุมาน ได้แก่ การวิเคราะห์ความแปรปรวน 3 ทาง (3-Way ANOVA) และการวิเคราะห์ความแปรปรวนร่วม (ANCOVA) ผลการทดสอบสมมติฐาน พบว่า ก) ระดับความรู้ความเข้าใจเกี่ยวกับการถูกละเมิดความเป็นส่วนตัวผ่านสื่อสังคม ขึ้นกับอิทธิพลร่วมของช่วงระยะเวลาในการใช้สื่อสังคมในรอบวันกับการตอบสนองต่อคำสั่งงานของผู้บังคับบัญชา

ข) การตอบสนองต่อคำสั่งงานของผู้บังคับบัญชาขึ้นกับอิทธิพลร่วมระดับความรู้ความเข้าใจเกี่ยวกับการถูกละเมิดความเป็นส่วนตัวผ่านสื่อสังคม ค) การใช้ฟังก์ชันระบุพิกัดของตนเอง ณ สถานที่ต่างๆ ฟังก์ชันการโพสต์และการแบ่งปันข้อมูลในรูปแบบไม่เป็นสาธารณะ และการตั้งค่าเพื่อกำหนดบุคคลให้สามารถค้นหาบัญชีสื่อสังคมของตัวตน ขึ้นกับระดับการศึกษา ง) การใช้ฟังก์ชันระบุพิกัดของตนเอง ณ สถานที่ต่างๆ และการใช้ฟังก์ชันการยืนยันตัวตนแบบสองชั้นขึ้นกับอายุงาน จ) การใช้ฟังก์ชันการเปิดบัญชี การเชื่อมโยงระหว่างแอปพลิเคชันสื่อสังคมต่างๆ อาทิ Facebook, Instagram, Twitter ขึ้นกับอายุงาน และ ฉ) การใช้ฟังก์ชันการตั้งค่าเพื่อกำหนดบุคคลให้สามารถค้นหาบัญชีสื่อสังคมของตัวตน ขึ้นกับเพศสภาพ

คำสำคัญ: สื่อสังคม สิทธิความเป็นส่วนตัว กลไกปกป้องความเป็นส่วนตัว

Abstract

This research aimed to study 1) Social media privacy rights, and 2) Privacy protection mechanisms on social media. The study was a quantitative research using questionnaires as research tools for gathering data from 263 respondents, supporting officers working at Rangsit University. Statistics used for analyzing empirical data from the returned questionnaires were a) basic statistics: frequency, percentage, mean, standard deviation; b) inferential statistics for testing hypotheses: 3-way ANOVA (analysis of variance) and ANCOVA (analysis of covariance). The test resulted that a) levels of knowledge and understandings on social media privacy and its violation of privacy rights influenced by periods of daily use of social media and responding to the chief's commands; b) responding to the chief's commands influenced by the levels of knowledge and understandings on social media privacy and its violation of privacy rights; c) capability to set up GPS, security post and sharing, two levels of confirmation identities depending on levels of education; d) GPS setting and two levels of confirmation identities depending on work experiences; e) personal account setting, linkage among Facebook, Instagram, Twitter depending on work experiences, f) using the settings function to determine individual searching for its own social media accounts depends on gender.

Keywords: Social Media, Privacy Rights, Privacy Protection Mechanisms

บทนำ

สื่อสังคมเป็นสื่อออนไลน์ที่มีบริบทครอบคลุมการนำเสนอทั้งในส่วนเนื้อหา ภาพ วีดิทัศน์ ดนตรี ฯลฯ สื่อสังคมสามารถตอบสนองผู้ใช้ได้แบบมีปฏิสัมพันธ์ทันที แอปพลิเคชันสื่อสังคมที่ได้รับความนิยมในปัจจุบันได้แก่ เฟซบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) ไลน์ (Line) ลิงค์กิดอิน (LinkedIn) ฯลฯ สื่อสังคมเหล่านี้ได้สร้างความสัมพันธ์ระหว่างเพื่อน กลุ่ม และชุมชน ก่อให้เกิดความสัมพันธ์เชื่อมโยงครอบคลุมทั้งโลก ผู้ใช้สามารถเข้าถึงได้ตลอดเวลาผ่านอุปกรณ์ดิจิทัลต่างๆ อาทิ สมาร์ตโฟน แท็ปเล็ต แล็ปท็อป ผ่านระบบเครือข่ายอินเทอร์เน็ต และเป็นกระแสของโลกในปัจจุบัน ซึ่ง รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 กำหนดให้การเข้าถึงอินเทอร์เน็ตเป็นสิทธิขั้นพื้นฐานของพลเมือง

อัตราผู้ใช้สื่อสังคมเพิ่มขึ้นอย่างต่อเนื่อง จุดประสงค์ในการใช้มีความหลากหลาย อาทิ เพื่อติดตามความเคลื่อนไหวหรือพฤติกรรมของบุคคล เพื่อผลประโยชน์ในการขยายตลาดด้วยการใช้ข้อมูลลูกค้าจากแหล่งต่างๆ การรวบรวมหมายเลขโทรศัพท์ ที่อยู่จดหมายอิเล็กทรอนิกส์ หมายเลขบัตรเครดิต และข้อมูลส่วนตัวอื่นๆ เป็นประจักษ์พยานที่แสดงให้เห็นการละเมิดสิทธิความเป็นส่วนตัวที่เกิดขึ้นในสังคมปัจจุบันผ่านสื่อสังคม

มหาวิทยาลัยรังสิต เป็นมหาวิทยาลัยเอกชนที่มีชื่อเสียงได้รับการจัดอันดับโดย Webometrics Ranking of World Universities (2019) เป็นอันดับที่ 23 ของมหาวิทยาลัยทั้งหมดในประเทศไทย มีหลักสูตรหลากหลาย มุ่งผลิตบัณฑิตให้มีความรู้ความสามารถ มีคุณภาพ มีศีลธรรม และคุณธรรม พร้อมที่จะนำความรู้ ความสามารถ และทักษะ ไปพัฒนาประเทศต่อไป บุคลากรสายสนับสนุนของมหาวิทยาลัยรังสิต เป็นกลไกสำคัญอันหนึ่งที่จะขับเคลื่อน ให้เป็นไปตามยุทธศาสตร์ เป้าหมาย นโยบาย แผน พันธกิจ และกระบวนการทำงานของมหาวิทยาลัยได้อย่างสัมฤทธิ์ผล

จากการศึกษานำร่องด้วยการสุ่มสัมภาษณ์บุคลากรสายสนับสนุนจำนวนหนึ่งของมหาวิทยาลัยรังสิต พบว่า บุคลากรสายสนับสนุนและผู้บริหารทุกระดับและทุกหน่วยงานนิยมใช้แอปพลิเคชันสื่อสังคมผ่านอุปกรณ์ดิจิทัลต่างๆ เพราะสะดวกรวดเร็วในการสื่อสารภายใน ซึ่งทั้งสองฝ่ายยอมรับได้ถ้าการสื่อสารนั้นเกิดขึ้นในเวลาปฏิบัติงานปกติ แต่หากเป็นการใช้สื่อสังคมเพื่อสั่งการนอกเวลาทำการ หรือในวันหยุด/วันลา ทำให้บุคลากรสายสนับสนุนรู้สึกว่าเป็นการไม่เคารพสิทธิความเป็นส่วนตัวซึ่งกันและกัน และเข้าข่ายละเมิดสิทธิมนุษยชนขั้นพื้นฐาน

ผลการศึกษานำร่องดังกล่าวทำให้ผู้วิจัยประสงค์จะศึกษาเกี่ยวกับระดับความรู้เกี่ยวกับความเป็นส่วนตัวผ่านสื่อสังคมและกลไกปกป้องการละเมิดความเป็นส่วนตัวของบุคลากรสายสนับสนุนมหาวิทยาลัยรังสิต เพื่อให้บุคลากรสายสนับสนุนและผู้บริหารทุกระดับและทุกหน่วยงานได้ตระหนักถึงประเด็นปัญหาดังกล่าว ในการใช้สื่อสังคมที่เหมาะสม ผู้วิจัยคาดหวังเป็นอย่างยิ่งว่า ผลการวิจัยจะเป็นองค์ความรู้เบื้องต้นในการพัฒนาแนวทางการใช้สื่อสังคมในการสื่อสารระหว่างเพื่อนร่วมงานและผู้บริหารทุกระดับชั้น และในทุกหน่วยงานได้อย่างเหมาะสม

วัตถุประสงค์การวิจัย

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาระดับความรอบรู้เกี่ยวกับความเป็นส่วนตัวบนสื่อสังคม และกลไกปกป้องความเป็นส่วนตัวบนสื่อสังคมของบุคลากรสายสนับสนุนมหาวิทยาลัย

สื่อสังคม

สื่อสังคมคือการสื่อสารอิเล็กทรอนิกส์ในรูปแบบเว็บไซต์เพื่อสร้างเครือข่ายสังคม และการโพสต์ข้อความขนาดสั้นหรือ Microblogging ซึ่งผู้ใช้จะสร้างสรรค์ชุมชนออนไลน์เพื่อแบ่งปันข้อมูล ความคิด ข้อความส่วนตัว และเนื้อหาอื่นๆ ในหลากรูปแบบ อาทิ วีดิทัศน์ (Merriam-Webster, 2019) นอกจากนี้ ยังมีนักวิชาการท่านอื่นๆ ได้อธิบายความหมายของสื่อสังคม เช่น Kietzmann, Hermkens, McCarthy, & Silvestre (2011) และ Oba, & Wildman (2015) อธิบายว่าสื่อสังคมคือเทคโนโลยีที่ใช้คอมพิวเตอร์เป็นสื่อกลางในการปฏิสัมพันธ์ซึ่งกันและกัน เป็นเทคโนโลยีที่อำนวยความสะดวกในการสร้างสรรค์และแบ่งปันสารสนเทศ ความคิด ความสนใจในอาชีพ และการแสดงความคิดเห็นในรูปแบบอื่นๆ ผ่านชุมชนเสมือนและเครือข่าย และ Hudson (2018) อธิบายว่าสื่อสังคมคือเว็บไซต์และแอปพลิเคชันที่ออกแบบมาเพื่อให้ผู้คนสามารถแบ่งปันเนื้อหาได้อย่างรวดเร็ว มีประสิทธิภาพ และตามเวลาจริง นักวิชาการจำนวนมากระบุว่าสื่อสังคมเป็นแอปพลิเคชันบนสมาร์ทโฟนหรือแท็บเล็ต จึงอาจกล่าวโดยสรุปได้ว่า สื่อสังคมคือนวัตกรรมดิจิทัลที่เป็นสื่อกลางในการสื่อสารระหว่างผู้ใช้ผ่านระบบเครือข่ายอินเทอร์เน็ต Kietzmann, Hermkens, McCarthy, & Silvestre (2011) อธิบายเพิ่มเติมว่าสื่อสังคมมีฟังก์ชันจำนวน 7 หน่วยการทำงานแบบรังผึ้ง พร้อมอธิบายนัยสำคัญของแต่ละหน่วย ดังรูปที่ 1

รูปที่ 1 ฟังก์ชันของสื่อสังคมและนัยสำคัญของฟังก์ชันสื่อสังคม (Kietzmann, Hermkens, McCarthy, & Silvestre, 2011)

จากรูปที่ 1 แสดงหน่วยการทำงานของสื่อสังคมจำนวน 7 หน่วย คือ ตัวตน การสนทนา การแบ่งปัน การแสดงตัวตน ความสัมพันธ์ ชื่อเสียง และกลุ่ม แต่ละหน่วยจะทำให้สามารถแกะรอยและตรวจสอบมุมมองเฉพาะของผู้ใช้ และนัยต่างๆ หน่วยการเหล่านี้เป็นกรอบแนวคิดที่จะช่วยให้เข้าใจถึงความแตกต่างของระดับความสามารถในการจัดโครงแบบสื่อสังคมได้

ความเป็นส่วนตัว

จากการทบทวนวรรณกรรม พบว่าทฤษฎีความเป็นส่วนตัวของ Westin (1967) อธิบายว่ามนุษย์ต้องการความเป็นส่วนตัวไปพร้อมๆ กับความต้องการด้านอื่นๆ ความเป็นส่วนตัวจะช่วยปรับอารมณ์เกี่ยวกับการปฏิสัมพันธ์ระหว่างบุคคลในรอบวัน เป็นกระบวนการที่ไม่หยุดนิ่ง เป็นโอกาสในการปลดปล่อยอารมณ์ เป็นวิธีการในการตระหนักรู้ในตนเอง เป็นการกำหนดขอบเขตการสื่อสารระหว่างบุคคลที่ได้รับการปกป้องและแบ่งปันข้อมูลส่วนบุคคลแก่บุคคลที่เชื่อถือได้ ในขณะที่ทฤษฎีของ Altman (1975) กำหนดว่า ความเป็นส่วนตัวประกอบด้วยคุณสมบัติ 5 ประการ คือ 1) เป็นกระบวนการพลวัตของการควบคุมขอบเขตระหว่างบุคคล 2) มีระดับความต้องการความเป็นส่วนตัวและการกระทำจริง 3) ไม่ใช่ฟังก์ชันทางเดียวหากแต่สัมพันธ์กับระดับความเป็นส่วนตัว คือระดับความเป็นส่วนตัวที่เหมาะสม

(ความต้องการเท่ากับระดับการกระทำจริง) ความเป็นส่วนตัวสูง (การกระทำจริงมากกว่าความต้องการ) และความเป็นส่วนตัวน้อย (ความต้องการมากกว่าความเป็นจริง) 4) ความเป็นส่วนตัวมีสองทิศทาง เกี่ยวข้องกับข้อมูลนำเข้าจากแหล่งหนึ่ง และกลายเป็นผลลัพธ์ให้แก่แหล่งอื่น และ 5) ความเป็นส่วนตัวมีได้ทั้งในระดับบุคคลและกลุ่ม (Altman 1975; Margulis 1977) นอกจากนี้ ทฤษฎี CPM ของ Petronio (2002) เป็นทฤษฎีว่าด้วยการจัดการความเป็นส่วนตัวในการสื่อสาร ในทฤษฎี CPM กำหนดขอบเขตความเป็นส่วนตัวไว้ทั้งในระดับเปิดกว้าง สนิทสนม และความลับ ซึ่งการจัดการขอบเขตความเป็นส่วนตัวของบุคคลและกลุ่มต้องมีการประสานงานระหว่างบุคคล และในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 34 กำหนดให้คนไทยมีเสรีภาพ ในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น และมาตรา 36 กำหนดให้มีเสรีภาพในการติดต่อสื่อสารถึงกันไม่ว่าในทางใดๆ รวมทั้ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ประกาศใช้ด้วยเหตุผลที่ว่าเพื่อคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล

กลไกปกป้องความเป็นส่วนตัว

ในการปกป้องความเป็นส่วนตัวบนสื่อสังคม มีนักวิชาการหลายท่านได้เสนอกลไกปกป้องที่ผู้ใช้สื่อสังคมต้องตระหนักและเรียนรู้ อาทิ Siciliano (2014); Kumar, Saravanakumar, & Deepa (2016); Concordia Social Media Team (2017) กลไกปกป้องดังกล่าว ได้แก่ การจำกัดการมองเห็นของผู้ใช้คนอื่นๆ (การตั้งค่าความเป็นส่วนตัว) การควบคุมวิธีการให้ผู้ใช้คนอื่นๆ พบเจ้าของบัญชีผู้ใช้ การสกัดกั้นการแท็กรูปภาพ การแจ้งเตือนการล็อกอิน การสกัดกั้นผู้ใช้ที่เป็นสแปม การควบคุมบุคคลที่จะส่งข้อความมาถึงผู้ใช้เจ้าของบัญชีสื่อสังคม การตระหนักรู้ว่าเมื่อโพสต์ทุกอย่างบนอินเทอร์เน็ต สิ่งที่โพสต์นั้นจะตรึงถาวรอยู่บนอินเทอร์เน็ต (สารสนเทศที่แบ่งปันอาจเชื่อมโยงไปยังบุคคลอื่น) การคัดกรองก่อนตกลงยอมรับบุคคลเป็นเพื่อน การระมัดระวังการคลิกลิงค์ใดๆ ที่เพื่อนๆ ส่งมาให้ การปิดใช้งานฟังก์ชัน GPS การไม่ตั้งค่าล็อกอินอัตโนมัติ การเปลี่ยนพาสเวิร์ดอย่างสม่ำเสมอ การปิดบัญชีเก่าเมื่อไม่ใช้แล้ว

ขอบเขตของการวิจัย

1. ขอบเขตด้านประชากรของการวิจัย ได้แก่ บุคลากรสายสนับสนุนในส่วนงานต่างๆ ในมหาวิทยาลัยรังสิต จำนวน 1,313 คน (สำนักงานบุคคล มหาวิทยาลัยรังสิต, 2560)

2. ขอบเขตด้านตัวแปร

2.1 ตัวแปรอิสระ ได้แก่

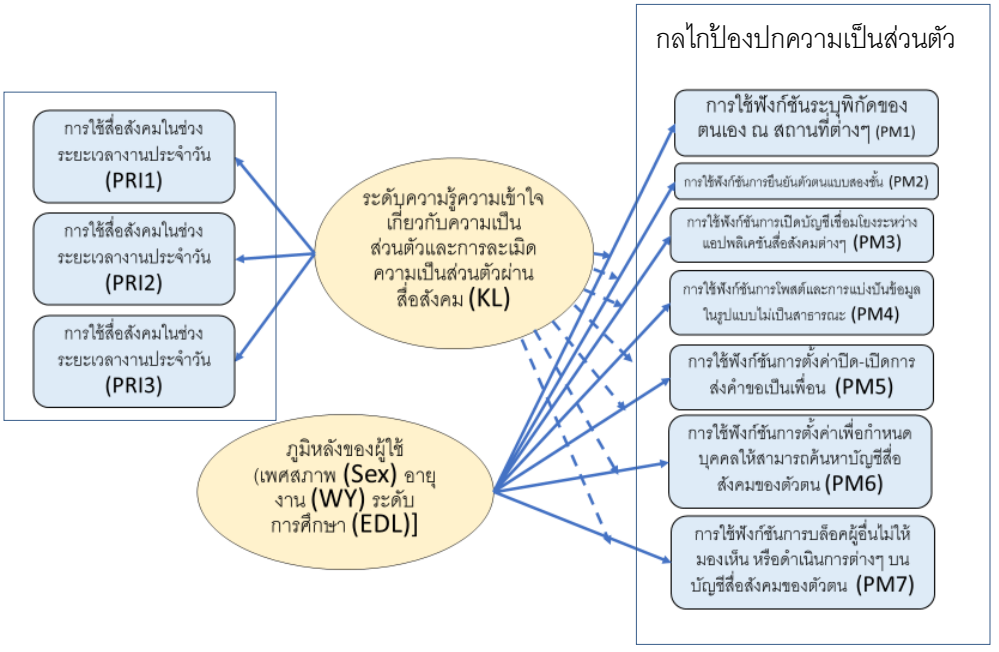
ก) ภูมิหลังของผู้ตอบแบบสอบถาม ได้แก่ เพศสภาพ อายุงาน ตำแหน่งงาน ระดับการศึกษา และหน่วยงานที่สังกัด

ข) ประสบการณ์การถูกละเมิดความเป็นส่วนตัวผ่านสื่อสังคม

2.2 ตัวแปรตาม ได้แก่ กลไกปกป้องความเป็นส่วนตัวบนสื่อสังคม ระดับความรู้ความเข้าใจเกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัวผ่านสื่อสังคม

กรอบแนวคิดของการวิจัย

จากการทบทวนแนวคิดและทฤษฎีที่เกี่ยวข้อง ผู้วิจัยได้พัฒนาเป็นกรอบการวิจัย ดังรูปที่ 1



รูปที่ 2 กรอบแนวคิดของการวิจัย

จากรูปที่ 2 ตัวแปร KL ที่ปรากฏในกรอบของการวิจัย หมายถึง ระดับความรู้ความเข้าใจเกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัวผ่านสื่อสังคม 3 ระดับ คือ ระดับความรู้น้อย ความรู้ปานกลาง ความรู้มาก เป็นตัวแปรควบคุมไม่ให้ส่งผลต่อการใช้กลไกปกป้องความเป็นส่วนตัวที่เป็นผลมาจากการมีภูมิหลังที่แตกต่างกันของผู้ใช้

สมมติฐานของการวิจัย

ผู้วิจัยได้กำหนดสมมติฐานไว้ทั้งสิ้น 14 สมมติฐาน ตามกรอบการวิจัย ดังต่อไปนี้

สมมติฐานกลุ่มที่ 1 เป็นการทดสอบว่าระดับความรู้ความเข้าใจเกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัวผ่านสื่อสังคม (KL) 3 ระดับ คือ ระดับความรู้น้อย ความรู้ปานกลาง ความรู้มาก เป็นผลมาจาก การใช้สื่อสังคมในช่วงระยะเวลางานประจำวัน (PRI1) การปฏิบัติงานนอกเวลาหลังจากได้รับคำสั่งของผู้บังคับบัญชาผ่านสื่อสังคม (PRI2) และ วิธีการตอบสนองต่อคำสั่งของผู้บังคับบัญชาผ่านสื่อสังคม (PRI3) หรือไม่ ผู้วิจัยทดสอบสมมติฐานในกลุ่มนี้ด้วยการวิเคราะห์ความแปรปรวน 3 ทาง (3-Way ANOVA) นำค่าเฉลี่ยของตัวแปร PRI1-3 เปรียบเทียบกัน เพื่อหาความแตกต่างของค่าเฉลี่ยระหว่างตัวแปรทั้งสามดังกล่าว เพื่อพิจารณาว่าตัวแปรทั้งสามมีอิทธิพลร่วมกันต่อระดับความรู้ (KL) หรือไม่

สมมติฐานกลุ่มที่ 2 เป็นการทดสอบว่าการใช้กลไกปกป้องความเป็นส่วนตัวบทสื่อสังคมเป็นผลมาจากภูมิหลังที่แตกต่างกันของบุคลากรสายสนับสนุนหรือไม่ โดยควบคุมตัวแปรระดับความรู้ความเข้าใจเกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัวผ่านสื่อสังคม (KL) ไม่ให้ส่งผลแทรกซ้อนเข้ามาในระหว่างการทดสอบ ผู้วิจัยทดสอบสมมติฐานในกลุ่มนี้ด้วยการวิเคราะห์ความแปรปรวนร่วม (ANCOVA) เพื่อทดสอบว่ากลไกปกป้องความเป็นส่วนตัวทั้ง 7 ฟังก์ชัน เป็นผลมาจากการมีระดับการศึกษา อายุงาน และเพศสภาพที่แตกต่างกันหรือไม่ โดยควบคุมไม่ให้ระดับความรู้เกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัวผ่านสื่อสังคม (KL) เข้ามามีอิทธิพลร่วม

เครื่องมือการวิจัย

ผู้วิจัยกำหนดตัวบ่งชี้ตัวแปรและตัวอย่างข้อคำถาม เพื่อนำไปสู่การพัฒนาแบบสอบถาม แบบสอบถามที่พัฒนาแล้วเสร็จได้นำไปตรวจสอบความเที่ยงตรงเชิงเนื้อหา และความเที่ยงตรงเชิงโครงสร้าง โดยผู้ทรงคุณวุฒิจำนวน 5 ท่านเป็นผู้ตรวจสอบความเที่ยงตรงดังกล่าว จากนั้นนำผลการประเมินไปคำนวณหาค่าดัชนีความสอดคล้อง ของข้อคำถามกับวัตถุประสงค์และคำถามการวิจัย ผลการคำนวณบ่งชี้ว่าแบบสอบถามมีค่าดัชนีความสอดคล้องทั้งฉบับเท่ากับ 0.80 แสดงว่าแบบสอบถามที่พัฒนาขึ้นมานี้มีความเที่ยงตรงทั้งในเชิงโครงสร้างและเนื้อหา ผู้วิจัยได้นำแบบสอบถามที่ปรับปรุงแล้วนี้ไปทดลองใช้กับผู้ตอบแบบสอบถามที่ไม่ใช่ตัวอย่างของการวิจัยนี้จำนวน 30 คนจากนั้น ได้นำคำตอบจากกลุ่มทดลองดังกล่าวไปคำนวณหาค่าความเชื่อมั่น (r) ด้วยสูตร K-R 20 ของ Kuder, & Richardson (1937) เพราะข้อคำถามในแบบสอบถามเป็นแบบถูก-ผิด หรือ ด้วยเห็น-ไม่เห็นด้วย ซึ่งเป็นข้อคำถามแบบ Dichotomous ผลการคำนวณพบว่าข้อคำถามทุกข้อในแบบสอบถามระหว่าง 0.20 ถึง 0.80 ซึ่งเป็นไปตามเกณฑ์ กล่าวคือแบบสอบถามมีความเชื่อมั่นที่ยอมรับได้ เนื้อหาในแบบสอบถามประกอบด้วย 3 ตอน คือ ตอนที่ 1 คุณลักษณะทางประชากรศาสตร์ของผู้ตอบแบบสอบถาม ตอนที่ 2 ระดับความรู้เกี่ยวกับการถูกละเมิดความเป็นส่วนตัวผ่านสื่อสังคม ตอนที่ 3 กลไกปกป้องความเป็นส่วนตัวบนสื่อสังคม

การกำหนดขนาดกลุ่มตัวอย่างและการสุ่มตัวอย่าง

กลุ่มตัวอย่างของการวิจัยในครั้งนี้คือบุคลากรสายสนับสนุนในมหาวิทยาลัยรังสิต จำนวน 307 คน จากจำนวนประชากรรวมทั้งสิ้น 1,313 คน (สำนักงานบุคคล มหาวิทยาลัยรังสิต, 2560) ใช้เทคนิคการสุ่มแบบมีความน่าจะเป็น (Probability Random Sampling) ด้วยวิธีการสุ่มตามระดับชั้นภูมิ กล่าวคือ ชั้นภูมิที่ 1 บุคลากรสายสนับสนุน สังกัดวิทยาลัย/คณะ/สถาบัน จำนวน 534 คน เมื่อคำนวณสัดสวนแล้วจะมีผู้ตอบ 125 คน ชั้นภูมิที่ 2 บุคลากรสายสนับสนุนสังกัดสำนัก/ศูนย์ จำนวน 779 คน เมื่อคำนวณสัดสวนแล้วจะมีผู้ตอบ 182 คน ในการเข้าถึงผู้ตอบแบบสอบถามในแต่ละชั้นภูมิ ผู้วิจัยใช้การสุ่มแบบง่าย (Simple Random Sampling) ด้วยการใช้โปรแกรมคอมพิวเตอร์สำเร็จรูปออนไลน์ในการสุ่มตัวเลขสุ่มจากตัวเลขระหว่าง 1 ถึง n ตามขนาดกลุ่มตัวอย่างในแต่ละชั้นภูมิ ซึ่งผู้วิจัยมีรายชื่อของประชากรทั้ง 2 ชั้นภูมิเรียงลำดับตามรหัสบุคลากร จากนั้นผู้วิจัยจึงแจกแบบสอบถามไปยังตัวอย่างที่สุ่มได้ดังกล่าว โดยใช้เวลา 2 เดือน ในการเก็บรวบรวมข้อมูล ได้รับแบบสอบถามกลับคืน รวมทั้งสิ้น 263 ฉบับ คิดเป็นร้อยละ 85.67 ซึ่งเพียงพอต่อการนำไปวิเคราะห์ข้อมูล

ภูมิหลังของผู้ตอบแบบสอบถาม

ผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง มีอายุงานที่ปฏิบัติงานในมหาวิทยาลัยรังสิต ตั้งแต่ 20 ปี ขึ้นไป และไม่ใช่ผู้บริหารหน่วยงาน ส่วนใหญ่สำเร็จการศึกษาระดับปริญญาตรี และปฏิบัติงานในสำนักงานและศูนย์ต่างๆ และไม่มีประสบการณ์การถูกละเมิดความเป็นส่วนตัวผ่านสื่อสังคม

สรุปผลการวิจัย

ข้อค้นพบจากการวิจัยจำแนกเป็น 3 ส่วนสำคัญ ดังนี้

ส่วนที่ 1 ระดับความรู้เกี่ยวกับความเป็นส่วนตัวความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัวผ่านสื่อสังคมของบุคลากรสายสนับสนุนมหาวิทยาลัยรังสิต

ในส่วนนี้ ผู้วิจัยกำหนดข้อคำถามเพื่อชี้วัดระดับความรู้ความเข้าใจจำนวน 14 ข้อคำถาม เป็นข้อคำถามแบบถูก-ผิด คะแนนเต็ม 14 คะแนน ดังนี้

1) มหาวิทยาลัยไม่สามารถนำข้อมูลส่วนตัวของบุคลากรไปใช้ประโยชน์ไม่ว่าในทางใดๆ

2) บุคลากรมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน เพื่อสะท้อนการบริหารงานของผู้บังคับบัญชาอย่างตรงไปตรงมา

3) การเปิดเผยข้อมูลการสื่อสารระหว่างบุคลากรกับผู้บังคับบัญชาผ่านสื่อสังคมสามารถกระทำได้

4) บุคลากรสามารถใช้วิธีการใดๆ ก็ได้เพื่อให้ได้มาซึ่งข้อมูลที่เพื่อนร่วมงานสื่อสารกันเกี่ยวกับตนเอง

5) มหาวิทยาลัยมีสิทธิโดยชอบธรรมในการเข้าถึงข้อมูลการติดต่อสื่อสารของบุคลากรทั้งทางจดหมายอิเล็กทรอนิกส์และสื่อสังคมใดๆ เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์

6) ในกรณีเกิดหรือคาดว่าจะเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ขึ้นในระบบสารสนเทศของมหาวิทยาลัย ถือว่าเป็นหน้าที่ของทุกหน่วยงานที่จะต้องมีแนวทาง มาตรการ หรือแผนปฏิบัติการรองรับ

7) มหาวิทยาลัยมีหน้าที่จัดระบบข้อมูลส่วนบุคคลของบุคลากร เพื่อให้การคุ้มครองข้อมูลข่าวสารส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและปลอดภัย

8) มหาวิทยาลัยสามารถเปิดเผยข้อมูลข่าวสารส่วนตัวของบุคลากร โดยไม่จำเป็นต้องได้รับความยินยอมเป็นลายลักษณ์อักษรจากบุคลากร

9) มหาวิทยาลัยไม่ให้สิทธิแก่บุคลากรในการตรวจสอบ/แก้ไขข้อมูลข่าวสารส่วนบุคคลของตนเองในระบบสารสนเทศ เพราะมีผู้บริหารระบบคอยกำกับดูแลแก้ไขอยู่แล้ว

10) กรณีที่ลาออก หรือถูกให้ออก หรือเกษียณอายุงาน มหาวิทยาลัยจะต้องล้างข้อมูลข่าวสารเกี่ยวกับบุคลากรออกจากระบบสารสนเทศของมหาวิทยาลัยทันที

11) หน่วยงานต่างๆ ในมหาวิทยาลัยสามารถส่งจดหมายอิเล็กทรอนิกส์ถึงบุคลากรโดยไม่เปิดโอกาสให้บุคลากรสามารถบอกเลิก หรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับ

12) การบิดเบือนหรือปลอมแปลงข้อมูลทั้งหมดหรือบางส่วน หรือเป็นเท็จแล้วนำเข้าสู่ระบบคอมพิวเตอร์ สามารถกระทำได้อย่างถูกต้องตามกฎหมายถ้าได้รับการยินยอมจากผู้บริหารระบบ

13) บุคลากรสามารถฟ้องร้องเพื่อนร่วมงานได้ตามกฎหมาย ถ้าเพื่อนร่วมงานแอบเข้าถึงข้อมูลคอมพิวเตอร์ของหน่วยงานโดยมิชอบ

14) ประชาชนไทยทุกคนสามารถเข้าถึงข้อมูลด้านการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในทางเศรษฐกิจของประเทศได้ทุกเมื่อ

ผลการทดสอบพบว่าบุคลากรสายสนับสนุน มหาวิทยาลัยรังสิต ทำคะแนนเฉลี่ยได้ 7.62 คะแนน (ค่าเบี่ยงเบนมาตรฐานเท่ากับ 1.92 ส่วนใหญ่ทำคะแนนได้ในช่วงระหว่าง 7-9 คะแนน เมื่อจำแนกคะแนนออกเป็น 3 กลุ่ม พบว่าบุคลากรมีระดับความรู้เกี่ยวกับความเป็นส่วนตัวและการถูกละเมิดความเป็นส่วนตัวผ่านสื่อสังคมในระดับปานกลาง ตามรายละเอียดการจำแนกกลุ่มดังต่อไปนี้

กลุ่มที่ 1 มีความรู้น้อย ช่วงคะแนน 3.00-6.33 มีจำนวน 70 คน

กลุ่มที่ 2 มีความรู้ปานกลาง ช่วงคะแนน 6.43-9.67 มีจำนวน 109 คน

กลุ่มที่ 3 มีความรู้มาก ช่วงคะแนน 9.68-13.00 มีจำนวน 84 คน

<u>ส่วนที่ 2 กลไกดิจิทัลเพื่อปกป้องความเป็นส่วนตัวบนสื่อสังคม</u>

ผลการวิจัยบ่งชี้ว่า บุคลากรสายสนับสนุน มหาวิทยาลัยรังสิต มีทั้งที่ใช้และไม่ใช้กลไกปกป้องความเป็นส่วนตัวบนสื่อสังคม ดังตารางที่ 1

ตารางที่ 1 การมีกลไกดิจิทัลเพื่อปกป้องความเป็นส่วนตัวบนสื่อสังคม

กลไกปกป้อง	การใช้งาน			
	ไม่เคย		เคย	
	ความถี่	ร้อยละ	ความถี่	ร้อยละ
1. ฟังก์ชันระบุพิกัดตนเอง ณ สถานที่ต่างๆ	60	22.81	203	77.19
2. ฟังก์ชันการยืนยันตัวตนแบบสองชั้น	127	48.29	136	51.71
3. ฟังก์ชันการเปิดบัญชีเชื่อมโยงระหว่างแอปพลิเคชันสื่อสังคมต่างๆ อาทิ Facebook, Instagram, Twitter	91	34.60	172	65.40
4. ฟังก์ชันการโพสต์และการแบ่งปันข้อมูลในรูปแบบไม่เป็นสาธารณะ	60	22.81	203	77.19
5. ฟังก์ชันการตั้งค่าปิด-เปิด การส่งคำขอเป็นเพื่อน	62	23.57	201	76.43
6. ฟังก์ชันการตั้งค่าเพื่อกำหนดบุคคลให้สามารถค้นหาบัญชีสื่อสังคมของตน	103	39.16	160	60.84
7. ฟังก์ชันการบล็อกผู้อื่นไม่ให้มองเห็น หรือดำเนินการต่างๆ บนบัญชีสื่อสังคมของตน	72	27.38	191	72.62

จากตารางที่ 1พบว่าบุคลากรสายสนับสนุนส่วนใหญ่เคยใช้กลไกปกป้องข้อที่ 1 และ 4 มากที่สุด รองลงมาคือข้อที่ 5, 7 และ 3 ตามลำดับ กลไกปกป้องข้อ *2* และ 6 เป็นกลไกที่ไม่เป็นที่นิยมใช้มากที่สุด รองลงมาคือกลไกข้อที่ *3* และ *7* ตามลำดับ

ส่วนที่ 3 ผลการทดสอบสมมติฐาน

ผลการทดสอบสมมติฐานกลุ่มที่ 1 พบว่า ระดับความรู้ความเข้าใจเกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัวผ่านสื่อสังคม (KL) ไม่ขึ้นกับช่วงระยะเวลาในการใช้สื่อสังคมในรอบวัน (PRI1) ช่วงเวลาในการสั่งงานผ่านสื่อสังคมของผู้บังคับบัญชา (PRI2) และการตอบสนองต่อคำสั่งงานของผู้บังคับบัญชา (PRI3) อีกทั้งไม่ขึ้นกับอิทธิพลร่วมของช่วงระยะเวลาในการใช้สื่อสังคมในรอบวัน (PRI1) และช่วงเวลาในการสั่งงานผ่านสื่อสังคมของผู้บังคับบัญชา (PRI2) รวมทั้งไม่ขึ้นกับอิทธิพลร่วมของช่วงเวลาในการสั่งงานผ่านสื่อสังคมของผู้บังคับบัญชา (PRI2) และการตอบสนองต่อคำสั่งงานของผู้บังคับบัญชา (PRI3) หากแต่ขึ้นกับอิทธิพลร่วมของช่วงระยะเวลาในการใช้สื่อสังคมในรอบวัน (PRI1) และการตอบสนองต่อคำสั่งงานของผู้บังคับบัญชา (PRI3) ดังผลลัพธ์การทดสอบด้วยเทคนิคทางสถิติ 3-way ANOVA ในตารางที่ 2

ตารางที่ 2

ความแปรปรวน	Type III Sum of Squares	องศาอิสระ	ค่าเฉลี่ยยกกำลังสอง	F	p-value
Corrected Model	82.178[a]	34	2.417	1.262	.163
Intercept	223.763	1	223.763	116.821	.000
PRI1	6.653	2	3.326	1.737	.178
PRI2	4.245	3	1.415	.739	.530
PRI3	7.881	5	1.576	.823	.534
PRI1* PRI2	4.028	4	1.007	.526	.717
PRI1* PRI3	30.565	6	5.094	2.660	.016
PRI2* PRI3	13.615	6	2.269	1.185	.315
PRI1* PRI2 * PRI3	14.153	7	2.022	1.056	.393
Error	436.720	228	1.915		
Total	2490.000	263			
Corrected Total	518.897	262			

ผลการทดสอบสมมติฐานกลุ่มที่ 2 พบว่าบุคลากรสายสนับสนุนมหาวิทยาลัยรังสิตที่มีระดับการศึกษาต่ำกว่าปริญญาตรี ปริญญาตรี หรือสูงกว่าปริญญาตรี มีกลไกปกป้องความเป็นส่วนตัวด้วยการใช้ฟังก์ชันระบุพิกัดของตนเอง ณ สถานที่ต่างๆ ต่างกัน (PM1) ดังผลลัพธ์การทดสอบด้วยสถิติ ANCOVA (ตารางที่ 3)

ตารางที่ 3

ฟังก์ชันระบุพิกัดของตนเอง ณ สถานที่ต่างๆ (PM1)					
ความแปรปรวน	Type III Sum of Squares	**องศาอิสระ**	**ค่าเฉลี่ยยกกำลังสอง**	F	p-value
Corrected Model	1.768[a]	2	.884	5.159	.006
Intercept	124.113	1	124.113	724.438	.000
EDL	1.768	2	.884	5.159	.006
Error	44.544	260	.171		
Total	203.000	263			
Corrected Total	46.312	262			

ผู้วิจัยได้ควบคุมตัวแปรระดับความรู้เกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัว (KL) ด้วยการทดสอบว่าระดับความรู้ดังกล่าวมีอิทธิพลต่อการมีกลไกปกป้องความเป็นส่วนตัวด้วยการใช้ฟังก์ชันระบุพิกัดของตนเอง ณ สถานที่ต่างๆ ต่างกัน (PM1) หรือไม่ และมีอิทธิพลคงที่หรือไม่ ผลการทดสอบพบว่า ความสัมพันธ์ระหว่างการมีกลไกปกป้องความเป็นส่วนตัวด้วยการใช้ฟังก์ชันระบุพิกัดของตนเอง ณ สถานที่ต่างๆ (PM1) กับระดับการศึกษา (EDL) ไม่ต่างกัน เมื่อมีระดับความรู้ (KL) ต่างกัน แสดงว่า มีอิทธิพลคงที่ (ตารางที่ 4) จึงสามารถวิเคราะห์ต่อไปด้วย ANCOVA ได้ (ตารางที่ 5)

ตารางที่ 4

ฟังก์ชันระบุพิกัดของตนเอง ณ สถานที่ต่างๆ					
ความแปรปรวน	Type III Sum of Squares	**องศาอิสระ**	**ค่าเฉลี่ยยกกำลังสอง**	F	p-value
Corrected Model	3.402[a]	5	.680	4.075	.001
Intercept	7.181	1	7.181	43.006	.000
EDL	1.663	2	.831	4.979	.008
KL	1.442	1	1.442	8.634	.004
EDL * KL	.910	2	.455	2.725	.067
Error	42.910	257	.167		
Total	203.000	263			
Corrected Total	46.312	262			

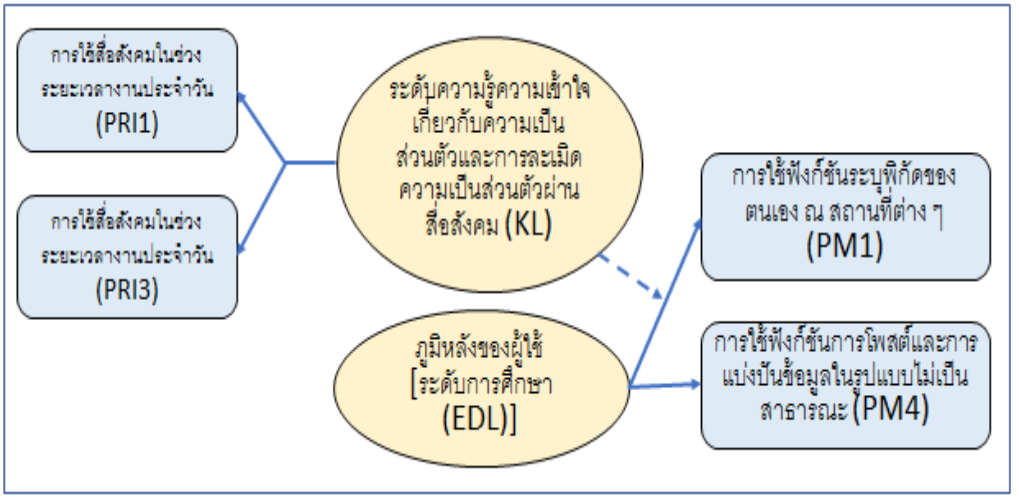
ตารางที่ 5

ฟังก์ชันระบุพิกัดของตนเอง ณ สถานที่ต่าง ๆ					
ความแปรปรวน	Type III Sum of Squares	**องศาอิสระ**	**ค่าเฉลี่ยยกกำลังสอง**	F	p-value
Corrected Model	2.492[a]	3	.831	4.909	.002
Intercept	11.659	1	11.659	68.912	.000
KL	.724	1	.724	4.279	.040
EDL	1.674	2	.837	4.948	.008
Error	43.820	259	.169		
Total	203.000	263			
Corrected Total	46.312	262			

จากตารางที่ 5 สรุปได้ว่าการมีกลไกปกป้องความเป็นส่วนตัวด้วยการใช้ฟังก์ชันระบุพิกัดของตนเอง ณ สถานที่ต่างๆ ต่างกัน (PM1) ขึ้นอยู่กับระดับความรู้เกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัว (KL) และระดับการศึกษา (EDL) ของบุคลากรสายสนับสนุนมหาวิทยาลัยรังสิตอย่างมีนัยสำคัญทางสถิติ ที่ระดับ .05 (p-value=.040 และ.008 ตามลำดับ)

การทดสอบกลไกปกป้องความเป็นส่วนตัวที่เหลือ (PM2-PM7) ว่าเป็นผลมาจากภูมิหลังของบุคลากรโดยที่ไม่มีระดับความรู้ความเข้าใจ (KL) เข้ามาแทรกซ้อนนั้น ผู้วิจัยดำเนินการทดสอบด้วยเทคนิคทางสถิติดังที่กล่าวรายละเอียดไว้ข้างต้นทุกประการ ผลการทดสอบสรุปได้ว่า ฟังก์ชันการโพสต์และการแบ่งปันข้อมูลในรูปแบบไม่เป็นสาธารณะ (PM4) ขึ้นกับระดับการศึกษา (EDL) การมีกลไกปกป้องความเป็นส่วนตัวด้วยการใช้ฟังก์ชันระบุพิกัดของตนเอง ณ สถานที่ต่างๆ ต่างกัน(PM1) ขึ้นอยู่กับระดับความรู้เกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัว (KL) และระดับการศึกษา (EDL) ของบุคลากรสายสนับสนุนมหาวิทยาลัยรังสิต

จากการทดสอบสมมติฐาน ผู้วิจัยได้พัฒนาเป็นแผนภาพความสัมพันธ์ระหว่างระดับความรู้ความเข้าใจเกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัวผ่านสื่อสังคม (KL) ภูมิหลังของผู้ใช้ เพศสภาพ (Sex) อายุงาน (WY) ระดับการศึกษา (EDL) ประสบการณ์การถูกละเมิดความเป็นส่วนตัวผ่านสื่อสังคม (PRI1, PRI2, PRI3) และ กลไกปกป้องความเป็นส่วนตัวบนสื่อสังคม (PM1, PM2, PM3, PM4, PM5, PM6, PM7) ดังรูปที่ 2



รูปที่ 3 ความสัมพันธ์ระหว่าง ประสบการณ์การถูกละเมิดความเป็นส่วนตัวผ่านสื่อสังคม (PRI1, PRI2, PRI3) กับ KL และความสัมพันธ์ของ ภูมิหลังของผู้ใช้ (EDL) และ KL กับ กลไกปกป้องความเป็นส่วนตัว (PM1 และ PM4)

การอภิปรายผลการวิจัย

จากการทดสอบสมมติฐาน จะเห็นว่าระดับความรู้ความเข้าใจเกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัวผ่านสื่อสังคม (KL) ไม่ได้เป็นผลมาจากช่วงระยะเวลาในการใช้สื่อสังคมในรอบวัน (PRI1) ช่วงเวลาในการสั่งงานผ่านสื่อสังคมของผู้บังคับบัญชา (PRI2) และการตอบสนองต่อคำสั่งงานของผู้บังคับบัญชา (PRI3) ที่เป็นเช่นนี้อาจเป็นเพราะบุคลากรมีความรู้ความเข้าใจในประเด็นการละเมิดความเป็นส่วนตัวในระดับปานกลาง (คะแนนเฉลี่ย 7.62 จากคะแนนเต็ม 14) จึงมีความเป็นไปได้ที่จะไม่ตระหนักหรือไม่ให้ความสนใจว่าตนเองถูกละเมิดความเป็นส่วนตัว โดยผู้บังคับบัญชาผ่านการใช้สื่อสังคมสั่งงานนอกเวลาทำการทั้งก่อนเริ่มงาน และหลังเลิกงาน โดยไม่รู้ตัว (ร้อยละ 84.03 ถูกสั่งงานนอกเวลาการ) นั่นหมายความว่าบุคลากรต้องปรับอารมณ์ในการปฏิสัมพันธ์กับผู้บังคับบัญชาไม่ให้เกิดความรู้สึกต่อต้านการสั่งงานนอกเวลาทำการ ซึ่งสอดคล้องกับแนวคิดของ Westin (1967) ที่อธิบายว่าความต้องการความเป็นส่วนตัวของมนุษย์จะช่วยปรับอารมณ์เกี่ยวกับการปฏิสัมพันธ์ระหว่างบุคคลในแต่ละวันให้ราบรื่น นอกจากนี้ ผู้วิจัยได้นำตัวแปร PRI1 และ PRI2 ไปทดสอบเพื่อหาอิทธิพลร่วมว่าจะส่งผลต่อ KL หรือไม่ และพบว่าทั้งสองตัวแปรต่างไม่มีอิทธิพลร่วมใดๆ ต่อ KL อาจเป็นเพราะบุคลากร

ไม่ตระหนัก หรือไม่ให้ความสนใจว่าตนเองถูกละเมิดความเป็นส่วนตัวดังกล่าว นอกจากนี้ อิทธิพลร่วมของ PRI2 และ PRI3 ไม่ส่งผลต่อ KL เช่นเดียวกัน ด้วยเหตุที่ว่าบุคลากรมีการสื่อสารด้วยความกระตือรือร้นและรับทราบคำสั่งและปฏิบัติทันที โดยไม่สนใจว่าตนเองจะถูกละเมิดความเป็นส่วนตัวจากผู้บังคับบัญชาหรือไม่ อาจกล่าวได้ว่า ไม่วิตกกังวลกับประเด็นความเป็นส่วนตัวและการถูกละเมิดความเป็นส่วนตัวผ่านสื่อสังคมเท่าใดนัก ซึ่งเป็นข้อค้นพบที่แตกต่างไปจากข้อค้นพบในงานวิจัยของ Buettner (2015) ที่ชี้ว่าความวิตกกังวลเกี่ยวกับความเป็นส่วนตัวมีผลต่อการใช้นวัตกรรม อาทิ วิตกว่าข้อมูลส่วนตัวจะถูกผู้อื่นนำไปใช้ในทางที่ผิด กลัวผู้อื่นรับรู้เรื่องราวส่วนตัว นอกจากนี้ ผลการวิจัยยังชี้ว่า PRI1 และ PRI3 มีอิทธิพลร่วมกันต่อ KL กล่าวคือถ้าใช้สื่อสังคมในช่วงเวลางานและได้รับสั่งงานจากผู้บังคับบัญชาในช่วงเวลางานก็อาจไม่ตระหนักรู้ว่าตนถึงละเมิดความเป็นส่วนตัว แต่จะเริ่มกังวลเมื่อผู้บังคับบัญชาสั่งงานนอกเวลาทำการ ซึ่งตรงกับแนวคิดของ Smith, & Kidder (2010) ที่ชี้ว่าสิทธิความเป็นส่วนตัวของแต่ละบุคคลต้องได้รับการพิจารณา ซึ่งองค์กรควรพัฒนาแนวทางการใช้เว็บเครือข่ายสังคมในกระบวนการประยุกต์งานตามประเด็นด้านจริยธรรม กฎหมาย และแนวปฏิบัติที่ดี

ผลการทดสอบสมมติฐานยังชี้ให้เห็นว่าระดับความรู้เกี่ยวกับความเป็นส่วนตัวและการละเมิดความเป็นส่วนตัว (KL) และระดับการศึกษา (EDL) สามารถอธิบายความผันแปรการมีกลไกปกป้องความเป็นส่วนตัวด้วยการใช้ฟังก์ชันระบุพิกัดของตนเอง ณ สถานที่ต่างๆ ต่างกัน (PM1) ที่เป็นเช่นนี้อาจเป็นเพราะว่าการใช้ฟังก์ชันดังกล่าว ต้องใช้เทคนิควิธีที่ซับซ้อนพอสมควรในการกำหนดพิกัดและต้องอาศัยขั้นตอนวิธีหลายขั้นตอน ถ้าผู้ใช้ไม่มีความรู้ความเข้าใจในประเด็นความเป็นส่วนตัวและกลไกปกป้องความเป็นส่วนตัว อาจจะไม่ใช้หรือใช้ฟังก์ชันนี้อย่างขาดความระมัดระวัง และ/หรืออาจกระตือรือร้นเรียนรู้ที่จะใช้ นอกจากนี้ยังพบว่าฟังก์ชันการโพสต์และการแบ่งปันข้อมูลในรูปแบบไม่เป็นสาธารณะ (PM4) ขึ้นกับระดับการศึกษา (EDL) เช่นเดียวกัน อย่างไรก็ดี ในภาพรวมงานวิจัยนี้ชี้ว่าบุคลากรสายสนับสนุนของมหาวิทยาลัยรังสิตใช้ฟังก์ชันต่างๆ ของสื่อสังคมเป็นกลไกปกป้องความเป็นส่วนตัวของตน สอดคล้องกับแนวคิดของ Potter (2014) ที่ระบุว่าสังคมได้ก้าวมาถึงจุดที่ต้องให้ความสำคัญกับการทำความรู้ความเข้าใจในประเด็นความเป็นส่วนตัวบนสื่อแบบรู้เท่าทัน ถ้ามีระดับการรับรู้ต่ำก็อาจทำให้เกิดความเสี่ยงที่จะเป็นภัยคุกคามสำคัญต่อผู้ใช้สื่อดังกล่าว นอกจากนี้ Timm, & Duven (2008) ได้ชี้ว่าความเป็นส่วนตัวในเครือข่ายสังคมนั้นคือสารสนเทศส่วนบุคคลเป็นสิ่งสำคัญที่สาธารณะชนทั่วไปจะเข้าถึงโดยเสรีมิได้ การที่บุคลากรสายสนับสนุนใช้กลไกปกป้องความเป็นส่วนตัวเป็นส่วนมากนั้นอาจเป็นเพราะมีระดับการตระหนักถึงความเป็นส่วนตัวสูงขึ้น สอดคล้องกับงานวิจัยของ O'Brien, & Torre (2012); Madden, & Smith (2010) ที่ว่าผู้ใช้สื่อสังคมโดยเฉพาะ Facebook มีการตระหนักถึง ความเป็นส่วนตัวในระดับสูง และเป็นไปในทิศทางเดียวกันกับ Magolis, & Briggs (2016) ที่ว่าผู้ใช้สื่อสังคมจะมีวิธีการในการกำหนดค่า

ความเป็นส่วนตัวแตกต่างกัน รวมทั้ง Nyoni, & Velempini (2018) ระบุว่าร้อยละ 88 ของผู้ใช้สื่อสังคมโดยเฉพาะ Facebook ทราบวิธีในการกำหนดค่าต่างๆ เพื่อป้องกันข้อมูลของตน

ข้อเสนอแนะในการนำผลการวิจัยไปประยุกต์ใช้

จากคะแนนระดับความรู้ความเข้าใจในประเด็นความเป็นส่วนตัวและกลไกปกป้องความเป็นส่วนตัวของบุคลากรสายสนับสนุนที่มีระดับคะแนนเฉลี่ยเพียง 7.62 คะแนน จากคะแนนเต็ม 14 คะแนน สะท้อนว่าบุคลากรดังกล่าวมีระดับความรู้ความเข้าใจในระดับปานกลาง สะท้อนว่ามีการตระหนักรู้ประเด็นความเป็นส่วนตัวไม่มากนักรวมทั้งข้อค้นพบอื่นๆ จากงานวิจัยนี้ ผู้วิจัยได้นำไปเป็นประเด็นสนทนากลุ่มร่วมกับผู้ทรงคุณวุฒิจำนวน 5 ท่าน ผนวกเข้ากับข้อเสนอแนะของ Dey, & Mondal (2019) ได้ข้อเสนอแนะว่ามหาวิทยาลัยรังสิตควรสร้างเสริมการตระหนักรู้ถึงประเด็นความเป็นส่วนตัวบนสื่อสังคมให้เกิดขึ้นแก่บุคลากรผ่านแนวทางต่างๆ ดังนี้

1) กำหนดข้อมูลที่มหาวิทยาลัยต้องเก็บรวบรวม ประมวลผล ปกปิด และ/หรือเผยแพร่สู่สาธารณะ

2) กำหนดนโยบายความเป็นส่วนตัวที่สะท้อนถึงความตั้งใจและวัตถุประสงค์ในการรวบรวมข้อมูลส่วนบุคคลของบุคลากร

3) สร้างกลไกในการรักษาความมั่นคงปลอดภัยสารสนเทศ อาทิ การแจ้งเตือนหากมีการใช้อุปกรณ์อื่นนอกเหนือจากอุปกรณ์ปกติของบุคลากรเพื่อเข้าสู่ข้อมูลของบุคลกร การแจ้งเตือนหากผู้ที่ไม่ได้รับอนุญาตเข้าถึง ทำลาย จัดเก็บ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคลากร

4) มีความโปร่งใสในการใช้ข้อมูล บุคลากรสามารถตรวจสอบได้

5) กำหนดบทบัญญัติว่าด้วยการบำรุงรักษาข้อมูลให้มีความถูกต้องแม่นยำ

6) การกำหนดแนวปฏิบัติเรื่องความเป็นส่วนตัวที่บุคลากรต้องปฏิบัติตาม

ในส่วนบุคลากร ควรป้องกันความเป็นส่วนตัวมิให้ถูกละเมิด ดังนี้

1) ตระหนักถึงบรรทัดฐานความเป็นส่วนตัวและการยินยอม

2) พัฒนาตนให้มีความรู้ในการประมวลผลข้อมูลและการส่งผ่านข้อมูล

3) สร้างทางเลือกในการแบ่งปันเนื้อหาส่วนบุคคลโดยมิถูกผู้อื่นละเมิด

4) จำกัดการประมวลผลเนื้อหา

5) กำหนดทางเลือกที่เหมาะสมในการคงไว้และเปิดเผยข้อมูล

6) ดัดแปลงแก้ไข้เนื้อหาที่แบ่งปันมิให้ไปละเมิดผู้อื่น

7) มีแนวปฏิบัติที่ดีในการรักษาความมั่นคงปลอดภัยสารสนเทศ

.....

เอกสารอ้างอิง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. (2562). *การคุ้มครองข้อมูลส่วนบุคคล*. สืบค้นจาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560. (2560). สิทธิและเสรีภาพของปวงชนชาวไทย. สืบค้นจาก http://www.ratchakitcha.soc.go.th /DATA/PDF/2560/A/040/1.PDF

สำนักงานบุคคล มหาวิทยาลัยรังสิต. (2560). สถิติบุคลากรสายสนับสนุน มหาวิทยาลัยรังสิต (เอกสารอัดสำเนา).

Altman, I. (1975). *The environment and social behavior: privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Pub.

Buettner, R. (2015). Analyzing the problem of employee internal social network site avoidance: Are users resistant due to their privacy concerns? *Proceedings of the 2015 48th Hawaii International Conference on System Sciences* (pp.1819-1826). Hawaii: IEEE. Doi: 10.1109/HICSS.2015.

Concordia Social Media Team. (2017). 10 ways to protect yourself on social media. Retrieved from https://www.concordia.ca/cunews/main/stories/2017/11/21/ stay-safe-on-social-media.html.

Dey, K., & Mondal, P. (2019). Privacy awareness among the academic social network users. *Library Philosophy and Practice (e-journal).* (2905), 1-19 Retrieved from https: //digitalcommons.unl.edu/libphilprac/2905.

Hudson, M. (2018). *What is social media? The Balance Small Business.* Retrieved from https://www.thebalancesmb.com/what-is-social-media-2890301

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons, 54*(3), 241-251.

Kuder, G. F., & Richardson, M. W. (1937). The theory of the estimation of test reliability. *Psychometrika, 2*(3), 151–160.

Kumar, S., Saravanakumar, K., & Deepa, K. (2016). On Privacy and security in social media – a comprehensive study. *Procedia Computer Science, 78*, 114 – 119. Retrieved from https://www.sciencedirect .com/ science/article/pii/S1877050916000211.

Madden, M. K., & Smith, A. W. (2010). *Reputation management and social media: How people monitor their identity and search for others others online*. Washington D.C.: Pew Internet & American Life Project. Retrieved from https://www.pewinternet.org/2010/05/ 26/ reputation-management-and-social-media/

Magolis, D., & Briggs, A. (2016). A phenomenological investigation of social networking privacy awareness through a media literacy lens. *Journal of Media Literacy Education*, 8 (2), 22-34. Retrieved from https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1167 &contest=jmle

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues 33*(3), 5-21.

Merriam-Webster. (2019). *Social media*. Retrieved from https://www.merriam- webster.com/ dictionary/social%20media

Nyoni. P., & Velempini. M. (2018). Privacy and user awareness on Facebook. *South African Journal of Science, 114*(5-6). 1-5. Retrieved from https://dx.doi.org/10.17159/sajs.2018/20170103

O'brien, D., & Torres, A. M. (2012). Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management. 31* (2): 63-97.

Obar, J. A., & Wildman, S. (2015). Social media definition and the governance challenge: an introduction to the special issue. *Telecommunications Policy,* 39 (9): 745–750. doi: 10.1016/j.telpol.2015.07.014

Petronio, S. (2011). Road to developing communication privacy management theory: narrative in progress, please stand by. *The Journal of Family Communication, 4*(3-4), 193-207.

Potter, W. J. (2014). *Medialiteracy* (7 th.). Los Angeles, CA: Sage.

Siciliano, R. (2014). *10 Tips to protect yourself on social networks*. Retrieved February 21, 2019, from https://safr.me/blog/2014/05/13/10-tips-to-protect-yourself-on-social-networks/

Smith, W. P., & Kidder, D. L. (2010). You've been tagged! (Then again, maybe not): Employers and Facebook. *Business Horizons, 53*(5), 491-499.

Timm, D. M., & Duven, C. J. (2008). Privacy and social networking sites. *New Directions for Student Services* (124): 89-101.

Webometrics Ranking of World Universities. (2019), Retrieved from http://www.webometrics.info /en/search/ Rankings/Rangsit%20UNiversity%20type%3Apais.

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.