กรอบแนวคิดเชิงระบบคอมพิวเตอร์เพื่อประเมินความเสี่ยงต่อการกระทำผิดกฎหมายที่เกิดขึ้นจากการรังแกบนสื่อสังคมออนไลน์

A Computer-Based Conceptual Framework for Assessing the Risk of Illegal Actions Arising from Cyberbullying

อภิชัย วิลาวรรณ (Apichai Wilawan)[1]
อธิวัฒน์ อภิรัตน์ธนารัฐ (Athiwat Abhiratthanarath)[2]
เชาวลิต ขันคำ (Chouvalit Khancome)[3]
จิรวัฒ ศิริศักดิ์สมบูรณ์ (Chirawat Sirisaksomboon)[4]
[2] ผู้ประพันธ์บรรณกิจ, [1]อาจารย์ประจำคณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏราชนครินทร์
Corresponding Author, Lecturer, Faculty of Humanities and Social Sciences,
Rajabhat Rajanagarindra University
[3]ผู้ช่วยศาสตราจารย์ ดร., อาจารย์ประจำคณะวิทยาศาสตร์ มหาวิทยาลัยรามคำแหง
Assistant Professor Dr., Lecturer, Faculty of Science, Ramkhamhaeng University
[4]อาจารย์ประจำคณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา
Lecturer, Faculty of Political Science and law, Burapha University
E-mail: apichai.wil@mail.rru.ac.th[1] athiwat.abh@mail.rru.ac.th[2]
chouvalit.k@rumail.ru.ac.th[3] chirawat@buu.ac.th[4]

Received: 18 November 2024
Revised: 10 February 2025
Accepted: 12 June 2025

บทคัดย่อ

ในยุคปัจจุบันที่ผู้คนใช้งานสื่อสังคมออนไลน์เป็นส่วนสำคัญของชีวิตประจำวัน อันนำไปสู่ปัญหาการรังแกกันบนสื่อสังคมออนไลน์ในอัตราสูงขึ้นอย่างมีนัยสำคัญ การแสวงหาเครื่องมือที่มีขีดความสามารถตรวจสอบ แจ้งเตือน และประเมินความเสี่ยงต่อการกระทำผิดกฎหมายย่อมมีความสำคัญเป็นอย่างยิ่ง ดังนั้น บทความวิจัยนี้จึงนำเสนอกรอบแนวคิดเชิงระบบคอมพิวเตอร์ใหม่สำหรับใช้ประเมินความเสี่ยงทางกฎหมายที่เกิดขึ้นจากการรังแกบนสื่อสังคมออนไลน์ด้วยการบูรณาการระหว่างศาสตร์กฎหมายและวิทยาการคอมพิวเตอร์ โดยศึกษาพฤติกรรมการรังแกบนสื่อสังคมออนไลน์ในปัจจุบัน นำมา

แจกแจง วิเคราะห์ สังเคราะห์ความเกี่ยวข้องกับการกระทำผิด หรือสุ่มเสี่ยงต่อการกระทำผิดในมาตราใดและกฎหมายที่เกี่ยวข้อง จากนั้นออกแบบกรอบแนวคิดทั่วไปที่ใช้ในการประเมินความเสี่ยงต่อการกระทำผิดกฎหมาย พัฒนาต่อยอดบูรณาการออกแบบกรอบแนวคิดเชิงระบบคอมพิวเตอร์ วิเคราะห์ผลลัพธ์และประเมินความเสี่ยงตามหลักโครงสร้างความรับผิดทางอาญาผสมผสานกับระบบอิงตามกฎที่สร้างชุดของกฎในรูปของเงื่อนไขทางคอมพิวเตอร์ ขีดความสามารถของกรอบแนวคิดใหม่สามารถใช้เป็นตัวแบบประเมินความเสี่ยงต่อการกระทำผิดกฎหมายที่เกี่ยวข้องได้ถึง 4 ระดับ ตรวจสอบได้อย่างน้อย 10 ประเด็น นอกจากนั้นยังสามารถนำไปพัฒนาต่อยอดเป็นโปรแกรมคอมพิวเตอร์เพื่อตรวจสอบ และประเมินความเสี่ยงต่อการกระทำผิดในกฎหมายที่เกี่ยวข้องได้อีกด้วย

คำสำคัญ: การรังแกบนสื่อสังคมออนไลน์, การประเมินความเสี่ยงทางกฎหมาย, โปรแกรมคอมพิวเตอร์, อาชญากรรมคอมพิวเตอร์

Abstract

As social media increasingly permeates daily life, the prevalence of cyberbullying has risen significantly, highlighting the urgent need for tools capable of monitoring, alerting, and assessing associated legal risks. This research article presents a novel, computer-based framework designed to evaluate legal risks arising from cyberbullying through an interdisciplinary approach that integrates legal studies and computer science. Specifically, the study examines contemporary patterns of cyberbullying on social media, categorizes and analyzes these behaviors, and evaluates their potential for legal infringement under relevant statutes. The proposed framework establishes a comprehensive system for assessing legal risks, which is further refined and implemented as a computer-based framework. Analysis and risk assessments are conducted according to principles of criminal liability, utilizing a rule-based system that encodes legal stipulations as computer-based conditions. This innovative framework is capable of evaluating legal risk across four levels of criminal liability and encompasses at least ten issues. Moreover, the framework can be extended into software solutions aimed at monitoring and assessing the risk of legal violations across relevant laws.

Keywords: Cyberbullying, Legal Risk Assessment, Computer Program, Computer Crime

บทนำ

ในยุคปัจจุบัน ผู้คนในสังคมไทยโดยเฉพาะอย่างยิ่งเด็กและเยาวชนต่างใช้งานสื่อสังคมออนไลน์มากขึ้นอย่างมีนัยสำคัญถึงร้อยละ 85.4 (สำนักงานสถิติแห่งชาติ, 2563) ด้วยความสำคัญดังกล่าวนี้ พบว่าเมื่อมีการใช้งานสื่อสังคมออนไลน์มากขึ้นเท่าใด ก็ยิ่งสร้างโอกาสนำไปสู่ปัญหาการรังแกบนสื่อสังคมออนไลน์ (Cyberbullying) อันนำไปสู่การกระทำผิดกฎหมายได้มากขึ้นเพียงนั้น จากสถิติการกระทำผิดทางด้านนี้ของประเทศไทยสูงเป็นอันดับ 5 ของโลก (กองเฝ้าระวังทางวัฒนธรรม, 2564) เมื่อพิจารณาเฉพาะเด็กและเยาวชน จากผลสำรวจของวิมลทิพย์ มุสิกพันธ์ พบข้อมูลว่า กลุ่มเยาวชนร้อยละ 43.1 เคยถูกรังแกบนสื่อสังคมออนไลน์ (กองเฝ้าระวังทางวัฒนธรรม, 2564) ซึ่งสอดคล้องกับผลการวิจัยในปัจจุบัน เช่น Saengcharoensap & Rujiprak (2021), ภูวสิทธิ์ ภูลวรรณ และคณะ (2563) และ ศุภากร หวัง และ สมชาย เตียวกุล (2562) ต่างยืนยันตรงกันว่าในปัจจุบันการรังแกบนสื่อสังคมออนไลน์มีอัตราสูงขึ้นอย่างมีนัยสำคัญ ดังนั้น ปัญหาดังกล่าวจึงถือว่าเป็นปัญหาสำคัญของสังคม เนื่องจากสามารถส่งผลกระทบต่อผู้ถูกกระทำอย่างร้ายแรง เช่น สร้างผลกระทบทางความรู้สึก ทำให้เครียด หวาดระแวง เกิดโรคซึมเศร้าและตัดสินใจฆ่าตัวตาย ทำให้เสียชื่อเสียง สร้างผลกระทบต่อบุคลิกภาพ ทำให้เป็นคนแยกตัวจากสังคม และส่งผลให้มีผลการเรียนตกต่ำ (ปองกมล สุรัตน์, 2561)

การรังแกบนสื่อสังคมออนไลน์สามารถกระทำต่อผู้เสียหายได้อย่างต่อเนื่อง มิหนำซ้ำยังมีร่องรอยการกระทำอยู่ในพื้นที่อินเทอร์เน็ตที่ค่อนข้างถาวรและแพร่กระจายในวงกว้าง นอกจากนั้น ผู้กระทำผิดสามารถสร้างตัวตนแบบนิรนาม ทำให้ผู้เสียหายไม่สามารถระบุตัวผู้กระทำความผิดเพื่อดำเนินคดีได้ (Suarez-Angelino, 2023) ปัจจัยเหล่านี้ส่งผลให้การรังแกบนสื่อสังคมออนไลน์มีแนวโน้มเพิ่มมากขึ้นเรื่อย ๆ โดยเฉพาะในกลุ่มเด็กและเยาวชนที่มีแนวคิดว่า เป็นวิธีระบายอารมณ์โดยไม่ต้องเปิดเผยตัวตน (คุณาธิป ผลทรัพย์, 2563) ซึ่งเมื่อการกระทำเกิดขึ้นบ่อยครั้ง ผู้กระทำจะละเลยความระแวดระวังและซึมซับว่าเป็นเรื่องปกติที่สามารถกระทำได้และไม่ตระหนักถึงผลกระทบของการกระทำต่อผู้ถูกรังแกและความรับผิดทางกฎหมายที่อาจเกิดขึ้นกับตนอันอาจเข้าข่ายผิดกฎหมายฉบับหนึ่งหรือหลายฉบับ เช่น ประมวลกฎหมายอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น

จากผลการศึกษาที่นำเสนอดังกล่าว เป็นที่ประจักษ์ว่า ปัญหาการรังแกบนสื่อสังคมออนไลน์ทั้งผู้ถูกกระทำและผู้กระทำต่างอยู่ในสังคมออนไลน์ ใช้เทคโนโลยีคอมพิวเตอร์ในการกระทำและถูกกระทำ ทั้งนี้อาจรู้หรือไม่รู้ถึงความสุ่มเสี่ยงต่อการกระทำผิดกฎหมาย หรือละเลยไม่ตระหนักรู้ก็เป็นได้ ดังนั้น คณะวิจัยซึ่งมีทั้งนักกฎหมายและนักวิทยาการคอมพิวเตอร์ จึงพิจารณาว่า หากร่วมกันบูรณาการศาสตร์ทั้งทางกฎหมายและวิทยาคอมพิวเตอร์ เพื่อแสวงหาแนวทางแก้ไขปัญหาและคิดค้นเครื่องมือประเมินเชิงคอมพิวเตอร์ที่มีขีดความสามารถใช้ตรวจสอบ หรือประเมินความเสี่ยงต่อการกระทำผิดดังกล่าวขึ้นมาได้ ก็ย่อมทำให้ผู้มีพฤติกรรมรังแกบนสื่อสังคมออนไลน์ตระหนักรู้ว่าการกระทำของตนมีความเสี่ยงหรือผิดต่อ

กฎหมาย อันนำไปสู่การถูกดำเนินคดีได้ ยิ่งในฐานะผู้ถูกกระทำก็ย่อมต้องตระหนักรู้และหาหนทางแก้ไขป้องกันตนเองเช่นกัน หากสร้างเครื่องมือดังกล่าวนี้สำเร็จก็ย่อมนำไปสู่การยับยั้งการกระทำผิด หรือเอาผิดกับผู้กระทำได้ กระทั่งประชาชนทั่วไปก็จะสามารถตระหนักรู้ ระมัดระวังในการใช้สื่อสังคมออนไลน์ ในท้ายที่สุด เครื่องมือดังกล่าวจะนำไปสู่การลดปริมาณการรังแกบนสื่อสังคมออนไลน์ หรือสนับสนุนการรณรงค์และแก้ไขปัญหาสังคมด้านนี้ได้อย่างต่อเนื่อง

ด้วยแนวคิดการแสวงหาแนวทางแก้ไขปัญหาและคิดค้นเครื่องมือดังกล่าว คณะผู้วิจัยได้พัฒนากรอบแนวคิดเชิงระบบคอมพิวเตอร์แบบใหม่ สำหรับประเมินความเสี่ยงทางกฎหมายที่เกิดขึ้นจากการรังแกบนสื่อสังคมออนไลน์ กรอบแนวคิดสร้างขึ้นจากการศึกษาพฤติกรรมการรังแกบนสื่อสังคมออนไลน์ วิเคราะห์ความผิดทางกฎหมายที่เกี่ยวข้อง ออกแบบกรอบแนวคิดในการประเมินความเสี่ยงต่อการกระทำผิดกฎหมายทั้งในมุมมองกรอบแนวคิดแบบทั่วไปและกรอบแนวคิดเชิงระบบคอมพิวเตอร์ กลไกสำคัญของกรอบแนวคิดถูกออกแบบและวิเคราะห์ผลลัพธ์ความเสี่ยงด้วยหลักการทางกฎหมายและแนวคิดเชิงระบบคอมพิวเตอร์เป็นพื้นฐานด้วยเครื่องมือที่ใช้ในการประเมินความเสี่ยงตามหลักโครงสร้างความรับผิดทางอาญา ผสมผสานกับระบบอิงตามกฎ (Rule-Based System) (Pal and Campbell, 1997; Timme and Rietveld, 2019) โดยรวบรวมและจำแนกหมวดหมู่ของผลลัพธ์ที่เป็นไปได้จากการตรวจสอบ แล้วสร้างชุดของกฎในรูปของเงื่อนไข (IF-THEN statements) ที่เกี่ยวข้องกับผลลัพธ์ ประสิทธิภาพของกรอบแนวคิดที่พัฒนาขึ้นสามารถประเมินความเสี่ยงต่อการกระทำผิดกฎหมายที่เกี่ยวข้อง จำนวน 10 ประเด็น ตามประมวลกฎหมายอาญา มาตรา 287, มาตรา 287/2, มาตรา 326, มาตรา 328, มาตรา 392, มาตรา 393, มาตรา 397, พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14, มาตรา 16 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 27 วรรคหนึ่ง วรรคสอง และมาตรา 26 และมาตรา 28* ประเมินระดับความเสี่ยงได้ 4 ระดับ ได้แก่ เสี่ยงต่ำ เสี่ยงปานกลาง เสี่ยงสูง และเสี่ยงสูงมาก กรอบแนวคิดนี้ออกแบบให้สามารถนำไปใช้ได้ทั้งผู้ใช้งานเยาวชนและประชาชนทั่วไป แม้แต่นักคอมพิวเตอร์สามารถนำกรอบแนวคิดไปพัฒนาต่อยอดเป็นซอฟต์แวร์เพื่อใช้เป็นเครื่องมือตรวจสอบประเมินความเสี่ยงต่อการกระทำผิดดังกล่าวได้อย่างดี

วัตถุประสงค์การวิจัย

1. ศึกษาพฤติกรรมการรังแกบนสื่อสังคมออนไลน์
2. วิเคราะห์ความผิดทางกฎหมายที่เกี่ยวข้องกับพฤติกรรมการรังแกบนสื่อสังคมออนไลน์

* ครอบคลุมความผิดเกี่ยวกับการทำให้แพร่หลายซึ่งสื่อลามก, หมิ่นประมาท, ข่มขู่, ดูหมิ่น, คุกคามทำให้เดือดร้อนรำคาญ, นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จหรือลามก, เผยแพร่ภาพตัดต่อ และการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม

3. พัฒนากรอบแนวคิดทั่วไปในการประเมินความเสี่ยงต่อการกระทำผิดกฎหมายที่เกี่ยวข้องกับพฤติกรรมการรังแกบนสื่อสังคมออนไลน์

4. นำเสนอแนวคิดเชิงระบบคอมพิวเตอร์สำหรับประเมินความเสี่ยงต่อการกระทำผิดกฎหมายที่เกิดขึ้นจากการรังแกบนสื่อสังคมออนไลน์

ทบทวนวรรณกรรม

1. พฤติกรรมการรังแกบนสื่อสังคมออนไลน์

นักวิชาการ (กฤษฎา แสงเจริญทรัพย์ และ วีนันท์กานต์ รุจิภักดิ์. 2564; ธวัชชัย ดวงไทย และ สาวิตรี พรหมสิทธิ์, 2565; พินวา แสนใหม่, 2563) อธิบายลักษณะการรังแกบนสื่อสังคมออนไลน์ (cyberbullying) ไว้ในทิศทางเดียวกัน คือ การกระทำที่มุ่งสร้างผลกระทบทางจิตใจและความทุกข์ทรมานต่อผู้ถูกกระทำ โดยใช้การสื่อสารผ่านอุปกรณ์อิเล็กทรอนิกส์หรือสื่อสังคมออนไลน์เป็นเครื่องมือ การรังแกบนสื่อสังคมออนไลน์มีรูปแบบพฤติกรรมที่หลากหลาย คณะวิจัยได้นำรูปแบบการจำแนกประเภทของ ทัศนีย์ ดำเกิงศักดิ์ และ แก้วกัญญา เสวกสุริยวงศ์ (2567); ธวัชชัย ดวงไทย และ สาวิตรี พรหมสิทธิ์. (2565); พินวา แสนใหม่ (2563); มูลนิธิส่งเสริมสื่อเด็กและเยาวชน (2561) และ Willard (2007) มาจัดกลุ่มและจำแนกประเภทใหม่ โดยจัดรวมพฤติกรรมที่เข้าข่ายการกระทำความผิดตามกฎหมายในลักษณะเดียวกันเอาไว้ด้วยกัน ดังนี้ 1) การดูหมิ่น (Insult) เป็นพฤติกรรมดูถูก เหยียดหยาม ด่าทอ หรือสบประมาทผู้อื่น คำประชดคำที่มีความหมายแฝงเป็นการด่าทอ หรือแม้แต่ถ้อยคำที่ล้อเลียนพฤติกรรมและสภาพบกพร่องทางกายของผู้อื่น 2) การหมิ่นประมาท (Denigration/ Dissing) เป็นพฤติกรรมการนินทาว่าร้าย ใส่ร้าย หรือกล่าวถึงผู้อื่นต่อบุคคลที่สามหรือในพื้นที่สาธารณะ 3) การคุกคาม (Harassment) เป็นพฤติกรรมคุมคาม ข่มขู่ ก่อความเดือดร้อนรำคาญ ที่กระทำซ้ำ ๆ ต่อบุคคลที่เป็นเป้าหมายโดยเฉพาะเจาะจง ด้วยวัตถุประสงค์เพื่อสร้างบรรยากาศแห่งความหวาดกลัว ความอับอาย ความเครียด หรือความเดือดร้อน 4) การติดตามรังควานไซเบอร์ (Cyberstalking) เป็นพฤติกรรมการละเมิดความเป็นส่วนตัวที่กระทำซ้ำ ๆ ต่อบุคคลที่เป็นเป้าหมาย ส่งผลให้ผู้ถูกกระทำเกิดความหวาดกลัว ความเครียด หรือรู้สึกไม่ปลอดภัย (สาวตรี สุขศรี, 2563) 5) การเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิ (Doxing/ Outing) เป็นการจงใจเผยแพร่ข้อมูลส่วนบุคคลหรือความลับของผู้อื่น โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ทำให้เจ้าของข้อมูลถูกคุกคาม หรือได้รับความเดือดร้อน (ศักดิกร วัฒนกูล และ จิรวุฒิ ลิปิพันธ์, 2566) 6) การแอบอ้างตัวตนของผู้อื่น (Impersonation/ Fraping) เป็นพฤติกรรมการปลอมเป็นบุคคลอื่นในพื้นที่สื่อสังคมออนไลน์ สร้างความเสียหายแก่ผู้ที่ถูกแอบอ้าง และ 7) การกีดกันออกจากกลุ่ม (Exclusion) เป็นการจงใจกีดกันบุคคลหนึ่งออกจากกลุ่มสนทนากิจกรรมชุมชนออนไลน์ หรือความเป็นเพื่อนในพื้นที่สื่อสังคมออนไลน์ มุ่งให้ผู้ถูกกีดกันรู้สึกโดดเดี่ยว หรือถูกทอดทิ้ง

2. ความเสี่ยงทางกฎหมาย

ความเสี่ยงทางกฎหมาย (Legal Risk) เป็นเรื่องการกระทำที่อาจก่อให้เกิดความรับผิดหรือผลกระทบทางกฎหมายต่อผู้กระทำ กรอบแนวคิดในการประเมินความเสี่ยงทางกฎหมายมักใช้กับองค์กรเพื่อประเมินความเสี่ยงด้านการปฏิบัติตามกฎระเบียบข้อบังคับ (Compliance Risk) ที่นิยมใช้ คือ COSO Enterprise Risk Management (ERM) Frameworks และ ISO 31000 Risk Management Standard ซึ่งเป็นการประเมินความเสี่ยงเชิงคุณภาพบนพื้นฐานของโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) (Society of Corporate Compliance and Ethics & Health Care Compliance Association [SCCE & HCCA], 2020; สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ [สวทช.], 2564) โอกาสที่จะเกิด (Likelihood) เป็นการประเมินความน่าจะเป็น (Probability) โดยประเมินว่า การกระทำในสถานการณ์หนึ่งมีความเสี่ยงที่จะผิดกฎหมายหรือไม่ และความถี่ที่การกระทำนั้นอาจเกิดขึ้น ส่วนผลกระทบ (Impact) เป็นการประเมินความร้ายแรงของความเสียหายหากความเสี่ยงนั้นเกิดขึ้น โดยประเมินว่า มีความรับผิดทางแพ่งและทางอาญามากน้อยเพียงใด มีผลกระทบต่อการเงิน ธุรกิจ ชื่อเสียง ความปลอดภัย หรือการบรรลุเป้าหมายขององค์กรอย่างไร (SCCE & HCCA, 2020) ประเมินอ้างอิงตามมาตรฐานภายในที่กำหนดขึ้นตามบริบทแวดล้อม ตัวแปร และความสามารถในการแบกรับความเสี่ยงของแต่ละองค์กรที่แตกต่างกันไป (SCCE & HCCA, 2020) ผลลัพธ์ที่ได้จากการวิเคราะห์ประเมินโอกาสที่จะเกิดและผลกระทบจะแสดงในรูปของระดับความเสี่ยง (Degree of Risk) โดยทั่วไปจะใช้วิธีประเมินความเสี่ยงเชิงคุณภาพ (Qualitative Legal Risk Assessment) โดยนักกฎหมายเป็นผู้วินิจฉัยประเมินตามวิจารณญาณและความเชี่ยวชาญของนักกฎหมายผู้นั้น อย่างไรก็ดี การประเมินความเสี่ยงในงานวิจัยนี้ คณะวิจัยมุ่งออกแบบให้ประชาชนสามารถใช้ประเมินความเสี่ยงเบื้องต้นด้วยตนเอง (Preliminary Assessment) และสามารถพัฒนาต่อยอดเป็นโปรแกรมคอมพิวเตอร์ได้ คณะวิจัยจึงเลือกพัฒนาเป็นกรอบแนวคิดเชิงระบบคอมพิวเตอร์ที่ใช้ระบบอิงตามกฎเป็นกลไกสำคัญ

3. การวินิจฉัยการกระทำผิดทางอาญา

การวินิจฉัยว่า การกระทำของผู้ใดเป็นความผิดตามกฎหมายอาญาและต้องได้รับโทษหรือไม่ พิจารณาตามหลักโครงสร้างความรับผิดทางอาญาซึ่งเป็นหัวใจสำคัญในการพัฒนากรอบแนวคิดในการประเมินความเสี่ยงต่อการกระทำผิดกฎหมายในงานวิจัยนี้ อันประกอบด้วยหลักเกณฑ์ 3 ประการ 1. การกระทำของผู้นั้นครบองค์ประกอบความผิด คือ เข้าองค์ประกอบในส่วนข้อเท็จจริงครบถ้วน และผู้กระทำมีเจตนาหรือประมาทเลินเล่อ 2. ไม่มีเหตุยกเว้นความผิด หากมีเหตุยกเว้นความผิดแล้ว การกระทำนั้นจะไม่ถือเป็นความผิดทางกฎหมาย และ 3. ไม่มีเหตุยกเว้นโทษ หากมีเหตุยกเว้นโทษ แม้การกระทำจะเป็นความผิด แต่ผู้กระทำย่อมไม่ต้องถูกลงโทษตามกฎหมายในความผิดนั้น

กฎหมายที่กำหนดความผิดทางอาญาครอบคลุมการรังแกบนสื่อสังคมออนไลน์ มี 3 ฉบับ ได้แก่ 1. ประมวลกฎหมายอาญา 2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ 3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งจะอธิบายในส่วนผลการวิจัย

วิธีการวิจัย

การวิจัยนี้ใช้วิธีการวิจัยเชิงเอกสาร (Documentary Research) โดยศึกษาและวิเคราะห์ข้อมูลเกี่ยวกับการรังแกบนสื่อสังคมออนไลน์รวมทั้งกฎหมายที่เกี่ยวข้อง จากนั้น จำแนกแจกแจง วิเคราะห์ สังเคราะห์ความรู้ในเชิงกฎหมาย นำมาพัฒนากรอบแนวคิดทั่วไปในการประเมินความเสี่ยงต่อการกระทำผิดกฎหมาย และพัฒนาต่อยอดในมุมมองเชิงระบบคอมพิวเตอร์ มีรายละเอียดการวิจัยดังนี้

1. รวบรวม ศึกษา จำแนกแจกแจงข้อมูลจากเอกสาร

1) เอกสารขั้นปฐมภูมิ ได้แก่ ประมวลกฎหมายอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2) เอกสารชั้นทุติยภูมิ ได้แก่ หนังสือ บทความในวารสารวิชาการทั้งภาษาไทยและภาษาต่างประเทศ สื่อสิ่งพิมพ์ รวมทั้งข้อมูลจากเว็บไซต์ต่าง ๆ ที่เกี่ยวข้อง

2. วิเคราะห์ข้อมูล

2.1 วิเคราะห์เอกสารที่รวบรวมได้โดยใช้การวิเคราะห์เนื้อหา เพื่อทำความเข้าใจพฤติกรรมการรังแกบนสื่อสังคมออนไลน์ว่ามีกี่ประเภท แต่ละประเภทมีคุณลักษณะและบริบทที่เกี่ยวข้องอย่างไร

2.2 วิเคราะห์เชิงกฎหมาย เพื่อให้ทราบว่าพฤติกรรมการรังแกบนสื่อสังคมออนไลน์ที่ศึกษาเข้าข่ายความผิดตามกฎหมายที่เกี่ยวข้องในมาตราใด และภายใต้องค์ประกอบทางกฎหมายอย่างไร

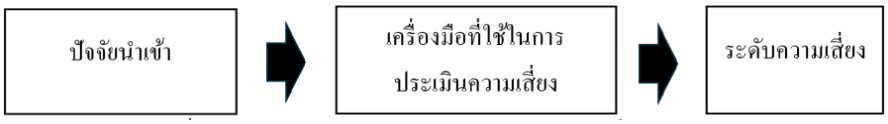
2.3 วิเคราะห์ทำความเข้าใจความเสี่ยงต่อการกระทำผิด หลักการและวิธีการประเมินความเสี่ยง เพื่อเป็นแนวทางในการออกแบบพัฒนากรอบแนวคิดที่เหมาะสมกับการรังแกบนสื่อสังคมออนไลน์

3. การพัฒนากรอบแนวคิดสำหรับประเมินความเสี่ยงต่อการกระทำผิดกฎหมาย

สังเคราะห์ข้อมูลจากการวิเคราะห์เอกสาร โดยเชื่อมโยงข้อมูลที่ได้จากการศึกษาพฤติกรรมการรังแกบนสื่อสังคมออนไลน์ หลักโครงสร้างความรับผิดทางอาญา องค์ประกอบความผิดและบริบทที่เกี่ยวข้อง รวมทั้งหลักการประเมินความเสี่ยง ข้อมูลที่สังเคราะห์จะถูกนำมาใช้พัฒนากรอบแนวคิดสำหรับประเมินความเสี่ยงต่อการกระทำผิดกฎหมาย โดยมีโจทย์ในการพัฒนากรอบแนวคิด คือ 1. เป็นการประเมินความเสี่ยงเบื้องต้นที่ประชาชนทำได้ด้วยตนเอง 2. มีกระบวนการใช้งานที่ง่ายไม่ซับซ้อน 3. มุ่งเป้าประเมินที่ความน่าจะเป็น (Probability) ในการกระทำผิดกฎหมายเพื่อลดพฤติกรรมที่มีความเสี่ยง คณะวิจัยจึงเลือกพัฒนาเป็นกรอบแนวคิดที่ผสมผสานระหว่างความรู้ทางกฎหมายและวิทยาการคอมพิวเตอร์ ซึ่งสามารถนำไปพัฒนาต่อยอดเป็นโปรแกรมคอมพิวเตอร์สำหรับประเมินความเสี่ยงได้

ขั้นตอนและวิธีการพัฒนากรอบแนวคิด

1. ออกแบบกรอบแนวคิดที่เป็นกระบวนการเชิงระบบ โดยมีปัจจัยนำเข้า (Input) เป็นข้อมูลการกระทำที่ต้องการตรวจสอบ นำเข้ามาสู่กระบวนการตรวจสอบ (Process) ด้วยเครื่องมือประเมินความเสี่ยง หลังจากนั้นจะรายงานผลลัพธ์การประเมิน (Output) เป็นระดับความเสี่ยง ตามที่แสดงในภาพที่ 1



ภาพที่ 1 กรอบแนวคิดเชิงระบบสำหรับประเมินความเสี่ยงทางกฎหมาย

2. ออกแบบเครื่องมือประเมินความเสี่ยง ใช้หลักโครงสร้างความรับผิดทางอาญาเป็นฐานในการตรวจสอบและใช้ข้อมูลที่รวบรวมและวิเคราะห์พฤติกรรมการรังแกบนสื่อสังคมออนไลน์ รวมทั้งกฎหมายที่เกี่ยวข้องเป็นฐานข้อมูลของเครื่องมือในการตรวจสอบ การออกแบบดังกล่าวมีขั้นตอนดังนี้

2.1 นำบทบัญญัติกฎหมายที่เกี่ยวข้องมาแยกองค์ประกอบของความผิด ดังตัวอย่างในตารางที่ 1

ตารางที่ 1 ตัวอย่างองค์ประกอบความผิดของบทบัญญัติกฎหมายที่เกี่ยวข้อง

กฎหมาย	องค์ประกอบความผิด							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
287 ป.อ.	ผู้ใด	ทำให้แพร่หลาย	สื่อลามก	เพื่อแสดงอวดแก่ประชาชน				เจตนา
287/2 ป.อ.	ผู้ใด	ทำให้แพร่หลาย	สื่อลามกอนาจารเด็ก	เพื่อแสดงอวดแก่ประชาชน				เจตนา
326 ป.อ.	ผู้ใด	ใส่ความ	ผู้อื่น	ต่อบุคคลที่สาม	เสียชื่อเสียง	ถูกดูหมิ่น	ถูกเกลียดชัง	เจตนา
[…]	[…]	[…]	[…]	[…]	[…]	[…]	[…]	[…]

2.2 สังเคราะห์คุณลักษณะที่สำคัญของพฤติกรรมการรังแกแต่ละประเภทจากคำพิพากษาศาลฎีกา เอกสารวิชาการ และข่าวสารที่เกี่ยวข้อง เช่น ถ้อยคำ บริบทแวดล้อม พื้นที่ที่กระทำ ความสัมพันธ์ระหว่างผู้กระทำและผู้ถูกกระทำ สภาพอารมณ์ และผลกระทบต่อผู้ถูกกระทำ ดังตัวอย่างในตารางที่ 2

ตารางที่ 2 ตัวอย่างการสังเคราะห์ถ้อยคำที่ใช้ในการดูหมิ่น มาตรา 393

ลำดับ	คำดูหมิ่น	แหล่งที่มา	ลำดับ	คำดูหมิ่น	แหล่งที่มา
1	อีสัตว์	ฎ.2220/2518	6	อีหน้าหมา	ฎ.2089/2511
2	อีเหี้ย	ฎ.5257/2548	7	ไอ้หน้าโง่	ฎ.7572/2542
3	อีควาย	ฎ.5257/2548	8	เฮงซวย	ฎ.1623/2551
4	อีดอก	ฎ.2102/2521	9	ตอแหล	ฎ.8919/2552
5	อีหน้าหัวควย	ฎ.1989/2506	[…]	[…]	[…]

2.3 บรรจุคุณลักษณะที่สังเคราะห์ได้ ในรูปแบบฐานข้อมูลในการตรวจสอบแต่ละองค์ประกอบความผิดของมาตรานั้น ๆ โดยสังเคราะห์และออกแบบเครื่องมือทีละมาตราจนครบทั้ง 10 ประเด็น ข้อมูลที่ใช้ในการตรวจสอบ ได้แก่ ใครเป็นผู้กระทำได้บ้าง ใครเป็นผู้ถูกกระทำได้บ้าง มีความสัมพันธ์ระหว่างผู้กระทำและผู้ถูกกระทำที่เป็นองค์ประกอบของความผิดหรือไม่ ลักษณะการกระทำอันเป็น องค์ประกอบของความผิด ถ้อยคำที่เข้าองค์ประกอบความผิด บริบทแวดล้อมที่อาจแสดงถึงเจตนาและบริบทแวดล้อมซึ่งเป็นข้อยกเว้นทำให้การกระทำไม่เป็นความผิด ดังตัวอย่างในตารางที่ 3

ตารางที่ 3 ตัวอย่างเครื่องมือสำหรับใช้ในการตรวจสอบ มาตรา 393

องค์ประกอบ มาตรา 393	**ฐานข้อมูล: ถ้อยคำ ลักษณะการกระทำ และบริบทแวดล้อม**		**ตรวจสอบ Yes/No**
ผู้กระทำ	Any		
ผู้ถูกกระทำ	Any		
ความสัมพันธ์	Any		
ดูหมิ่น	พฤติกรรม	ด่า, ด่าทอ, ว่า, ต่อว่า, ดูถูก, ดูหมิ่น, เหยียดหยาม, หยาม, เหยียด , สบประมาท	
	ถ้อยคำ	สัตว์, ควาย, เหี้ย, ดอก, เปรต, ควย, หมา, หน้าโง่, ต่ำ, ตอแหล, เฮงซวย, ชั่ว [...]	

องค์ประกอบ มาตรา 393	ฐานข้อมูล: ถ้อยคำ ลักษณะการกระทำ และบริบทแวดล้อม	ตรวจสอบ Yes/No
โฆษณา	เว็บบอร์ด, Facebook, Instagram, กลุ่มไลน์, Group Chat, X, Twitter, VK, แชทเกม, Live [...]	
เจตนา	จงใจ, ตั้งใจ, เจตนา, โกรธ, โมโห, ไม่ชอบ, หมั่นไส้, เกลียด, แซว, ไม่ปรากฏข้อมูล	
ข้อยกเว้น	-	

3. ออกแบบผลลัพธ์ความเสี่ยงที่ได้จากการประเมิน ใช้หลักการทางกฎหมายและแนวคิดเชิงระบบคอมพิวเตอร์เป็นพื้นฐาน อาศัยผลลัพธ์ที่ได้จากการตรวจสอบด้วยเครื่องมือประเมินความเสี่ยงตามหลักโครงสร้างความรับผิดทางอาญา ผสมผสานกับระบบอิงตามกฎ (Rule-Based System) (Pal and Campbell, 1997; Timme and Rietveld, 2019) โดยจำแนกหมวดหมู่ของผลลัพธ์ที่เป็นไปได้จากการตรวจสอบแล้วสร้างชุดของกฎในรูปของเงื่อนไข (IF-THEN statements) ที่เกี่ยวข้องกับผลลัพธ์ กฎจะครอบคลุมถึงเงื่อนไข (IF) ที่กำหนดว่าผลลัพธ์ใดอาจนำไปสู่ความเสี่ยงที่ตามมาในระดับใด (THEN) ซึ่งได้กำหนดระดับความเสี่ยงไว้ 4 ระดับ ได้แก่ ความเสี่ยงต่ำ ความเสี่ยงปานกลาง ความเสี่ยงสูง และความเสี่ยงสูงมาก ข้อแนะนำในการตอบสนองต่อความเสี่ยงแต่ละระดับจะแตกต่างกันไป หากมีความเสี่ยงต่ำที่จะเป็นความผิดและถูกดำเนินคดี อาจให้ตอบสนองเพียงเฝ้าระวัง แต่ถ้าความเสี่ยงสูงมากอาจให้ผู้กระทำยุติการกระทำและลบเนื้อหาหรือให้ผู้เสียหายดำเนินคดี ดังแสดงในตารางที่ 4

ตารางที่ 4 เงื่อนไขและระดับความเสี่ยง

กฎ (Rule)	เงื่อนไข (IF)	ระดับความเสี่ยง (THEN)	การตอบสนอง
R1	การกระทำไม่ครบองค์ประกอบข้อเท็จจริง	ต่ำ	เฝ้าระวัง
R2	การกระทำครบองค์ประกอบข้อเท็จจริง (AND) ผู้กระทำไม่มีเจตนา	ปานกลาง	ยุติการกระทำ, แจ้งเตือน
R3	การกระทำครบองค์ประกอบข้อเท็จจริง (AND) ผู้กระทำมีเจตนา (AND) พฤติการณ์มีข้อยกเว้น	สูง	ยุติการกระทำ, แจ้งเตือน, ลบเนื้อหาออก

กฎ (Rule)	เงื่อนไข (IF)	ระดับความเสี่ยง (THEN)	การตอบสนอง
R4	การกระทำครบองค์ประกอบข้อเท็จจริง (AND) ผู้กระทำมีเจตนา (AND) พฤติการณ์ไม่มีข้อยกเว้น	สูงมาก	ยุติการกระทำ, แจ้งเตือน, ลบเนื้อหาออก, ดำเนินคดี

4. นำเสนอแนวคิดเชิงระบบคอมพิวเตอร์สำหรับประเมินความเสี่ยงทางกฎหมายที่เกิดขึ้นจากการรังแกบนสื่อสังคมออนไลน์

ในส่วนนี้ใช้ข้อมูลที่ได้จากการวิเคราะห์และสังเคราะห์ในการนำเสนอแนวคิดเชิงระบบคอมพิวเตอร์ที่สามารถตรวจสอบและประเมินความเสี่ยงต่อการกระทำผิดกฎหมาย โดยใช้กรอบแนวคิดการประเมินความเสี่ยงต่อการกระทำผิดกฎหมายเป็นต้นแบบในการพัฒนา แนวคิดเชิงระบบคอมพิวเตอร์นี้จะถูกออกแบบมาเพื่อให้สามารถนำไปใช้พัฒนาโปรแกรมคอมพิวเตอร์สำหรับป้องกันและลดการรังแกบนสื่อสังคมออนไลน์ โดยการประเมินความเสี่ยงและให้คำแนะนำอย่างเหมาะสม

ผลการวิจัย

ผลการศึกษาที่ได้จากงานวิจัยนี้ แบ่งออกเป็น 3 ส่วน ดังนี้

1. กฎหมายที่เกี่ยวข้องกับพฤติกรรมการรังแกบนสื่อสังคมออนไลน์

จากการศึกษาและวิเคราะห์พฤติกรรมการรังแกบนสื่อสังคมออนไลน์ในงานวิจัยนี้ พบว่ามีกฎหมายที่สามารถนำมาปรับใช้กับพฤติกรรมการรังแกในสื่อสังคมออนไลน์ได้ ดังนี้

1) การดูหมิ่น เหยียดหยาม สบประมาทผู้อื่นบนพื้นที่สาธารณะ เช่น บนสื่อสังคมออนไลน์หรือเว็บไซต์ที่บุคคลทั่วไปสามารถเข้าถึงได้ เป็นความผิดดูหมิ่นโดยการโฆษณาตาม ประมวลกฎหมายอาญา มาตรา 393, การดูหมิ่นด้วยข้อมูลที่เป็นรูปหรือวิดีโอตัดต่อ เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 16, การส่งข้อความหรือข้อมูลดูหมิ่นผู้อื่นเป็นการส่วนตัว เช่น ส่งผ่านกล่องข้อความส่วนตัว (Inbox) หรือส่งจดหมายอิเล็กทรอนิกส์ (e-mail) อาจเข้าข่ายความผิดรังแก คุกคาม ทำให้เดือดร้อนรำคาญ ตามประมวลกฎหมายอาญา มาตรา 397

2) การหมิ่นประมาทโดยการใส่ความผู้อื่นต่อบุคคลที่สามโดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง เป็นความผิดหมิ่นประมาท ตามประมวลกฎหมายอาญา มาตรา 326, ถ้ากระทำบนพื้นที่สื่อสังคมออนไลน์ที่บุคคลทั่วไปสามารถรับรู้ได้ เป็นความผิดหมิ่นประมาทด้วยการ

โฆษณา ตามมาตรา 328, ถ้าใส่ความด้วยภาพหรือวิดีโอลามก อาจเข้าข่ายความผิดตามมาตรา 287, 287/2 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14 (4) และ (5) หากเป็นภาพหรือวิดีโอตัดต่อ จะเข้าข่ายความผิดตามมาตรา 16, ถ้าข้อมูลที่ใส่ความเป็นข้อมูลส่วนบุคคล และผู้กระทำมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล อาจเป็นการเปิดเผยข้อมูลโดยมิชอบ เป็นความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 27 และมาตรา 79

3) การคุกคาม เข้าข่ายความผิดรังแก ข่มเหง คุกคาม ทำให้อับอายหรือก่อความเดือดร้อนรำคาญ ตามประมวลกฎหมายอาญา มาตรา 397, ถ้ามีการข่มขู่ให้หวาดกลัว เป็นความผิดตาม มาตรา 392

4) การติดตามรังควานไซเบอร์ อาจเข้าข่ายความผิดรังแก ข่มเหง คุกคาม ทำให้อับอายหรือก่อความเดือดร้อนรำคาญ ตามประมวลกฎหมายอาญา มาตรา 397, หากมีการข่มขู่ให้หวาดกลัว เป็นความผิดตามมาตรา 392, ถ้ามีพฤติกรรมการตัดต่อรูปหรือวิดีโอแล้วนำไปเผยแพร่ ทำให้อับอาย ย่อมเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 16

5) การเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิ ถ้าเป็นข้อมูลส่วนบุคคลที่ทำให้เจ้าของข้อมูลส่วนบุคคลเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง เป็นความผิดหมิ่นประมาท ตามประมวลกฎหมายอาญา มาตรา 326 หรือ 328 ถ้าผู้กระทำมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล อาจเป็นความผิดตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 27, มาตรา 28 และมาตรา 79 หากข้อมูลเป็นภาพหรือวิดีโอลามก อาจเข้าข่ายความผิดตามประมวลกฎหมายอาญา มาตรา 287, มาตรา 287/2 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14 (4) และ (5)

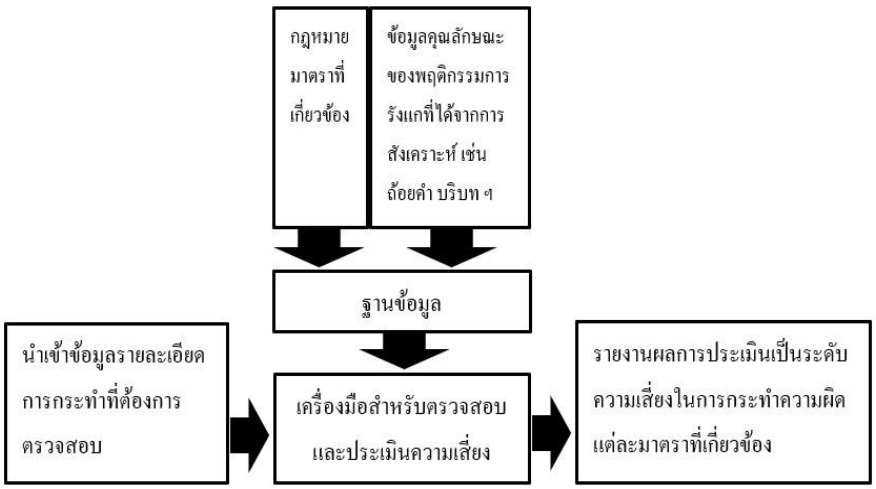
6) การแอบอ้างตัวตนของผู้อื่น ถ้ามีพฤติกรรมการนำเข้าข้อมูลปลอม ซึ่งหมายถึงข้อมูลคอมพิวเตอร์ที่ทำขึ้นโดยผู้ถูกกล่าวอ้างมิได้ให้อำนาจทำ (สุเนติ คงเทพ, 2559) หรือข้อมูลเท็จ อาจเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14 (1) หากใช้ภาพหรือวิดีโอตัดต่อ จะเข้าข่ายความผิดตามมาตรา 16

7) การกีดกันออกจากกลุ่ม จัดเป็นพฤติกรรมการรังแกที่ไม่รุนแรง ไม่เข้าข่ายความผิดฐานใดโดยเฉพาะ แต่ถ้ามีการรังแกประเภทอื่นร่วมกับการกีดกันด้วย ผู้กระทำต้องรับผิดในพฤติกรรมนั้น เมื่อรวบรวมและจำแนกแจกแจง จะได้บทบัญญัติกฎหมายที่นำมาสังเคราะห์เพื่อพัฒนากรอบแนวคิดในการประเมินความเสี่ยงทางกฎหมาย ดังนี้ ประมวลกฎหมายอาญา มาตรา 287, มาตรา 287/2, มาตรา 326, มาตรา 328, มาตรา 392, มาตรา 393 และมาตรา 397 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14 และมาตรา 16 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 27 วรรคหนึ่ง วรรคสอง และมาตรา 28

2. กรอบแนวคิดสำหรับประเมินความเสี่ยงต่อการกระทำผิดกฎหมาย

กรอบแนวคิดสำหรับประเมินความเสี่ยงที่พัฒนาขึ้น ใช้ประเมินความเสี่ยงด้วยขั้นตอนการทำงานเชิงระบบ (System Approach) เริ่มด้วยการนำเข้าข้อมูลการกระทำที่ต้องการตรวจสอบ เข้ามาสู่กระบวนการ

ตรวจสอบว่ามีแนวโน้มเป็นการกระทำความผิดกฎหมายหรือไม่ด้วยเครื่องมือที่ใช้ในการประเมินความเสี่ยง หลังจากนั้นจะรายงานผลลัพธ์การประเมินเป็นระดับความเสี่ยง ดังแสดงในภาพที่ 2



ภาพที่ 2 กรอบแนวคิดสำหรับประเมินความเสี่ยงต่อการกระทำผิดกฎหมายแบบทั่วไป

การประเมินความเสี่ยงโดยเครื่องมือตรวจสอบตามกรอบแนวคิดดังที่กล่าวมานี้ กระทำได้โดย

1. นำข้อมูลรายละเอียดการกระทำที่ต้องการตรวจสอบมาเป็นปัจจัยนำเข้า

2. ตรวจสอบด้วยวิธีการเปรียบเทียบและจับคู่ข้อมูลรายละเอียดการกระทำกับข้อมูลในฐานข้อมูลองค์ประกอบความผิดสำหรับมาตราที่ต้องการประเมินความเสี่ยงโดยเทียบกับฐานข้อมูลทีละองค์ประกอบ ถ้าเทียบแล้วจับคู่ได้กับถ้อยคำ ลักษณะการกระทำ หรือบริบทแวดล้อมในฐานข้อมูลนั้น จะถือว่าการกระทำเข้าองค์ประกอบข้อนั้น ทำเช่นนี้จนครบองค์ประกอบทุกข้อ

3. ประเมินผลลัพธ์ความเสี่ยงตามชุดของกฎที่สร้างไว้

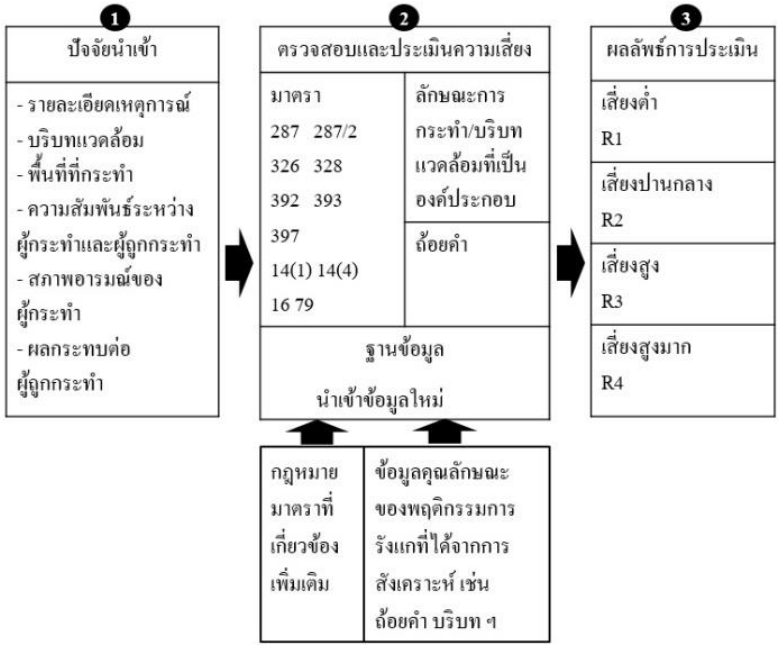
3.1 ถ้าไม่สามารถเทียบจับคู่ได้ในองค์ประกอบข้อเท็จจริงข้อใดเลย หรือเทียบจับคู่ได้เพียงบางข้อแต่ไม่ครบทุกข้อถือว่าการกระทำไม่ครบองค์ประกอบข้อเท็จจริงของมาตรานั้น (กฎ R1) ซึ่งจะแสดงผลลัพธ์เป็นความเสี่ยงระดับต่ำ

3.2 ถ้าเทียบจับคู่กับองค์ประกอบข้อเท็จจริงได้ทุกข้อ จะเทียบบริบทในส่วนเจตนาต่อไป ถ้าเทียบข้อมูลแล้วได้ผลว่าการกระทำไม่มีเจตนา (กฎ R2) จะแสดงผลลัพธ์เป็นความเสี่ยงระดับกลาง

3.3 ถ้าเทียบจับคู่ได้ผลว่าการกระทำมีเจตนาจะเทียบในส่วนข้อยกเว้น ถ้ากฎหมายมาตราที่ตรวจสอบไม่มีข้อยกเว้น (กฎ R4) จะแสดงผลลัพธ์เป็นความเสี่ยงระดับสูงมากทันที

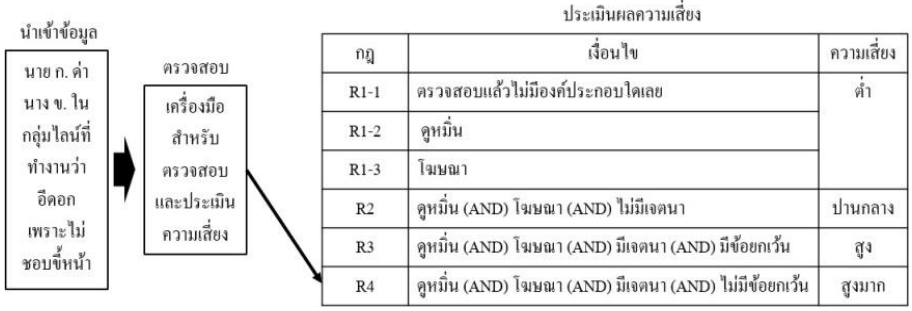
3.4 ถ้ากฎหมายมาตราที่ตรวจสอบมีข้อยกเว้น จะเทียบข้อมูลการกระทำกับข้อยกเว้นอีกครั้งหนึ่ง ถ้าเทียบจับคู่กับข้อยกเว้นได้ (กฎ R3) จะแสดงผลลัพธ์เป็นความเสี่ยงระดับสูง แต่ถ้าไม่สามารถเทียบ

จับคู่กับข้อยกเว้นได้ (กฎ R4) จะแสดงผลลัพธ์เป็นความเสี่ยงระดับสูงมาก ดังขั้นตอนที่แสดงในภาพที่ 3 จากนั้นแสดงตัวอย่างการประเมินความเสี่ยงรายมาตรา ดังตัวอย่างที่ 1 และตัวอย่างที่ 2



ภาพที่ 3 ขั้นตอนการประเมินความเสี่ยงต่อการกระทำผิดกฎหมายแบบทั่วไป

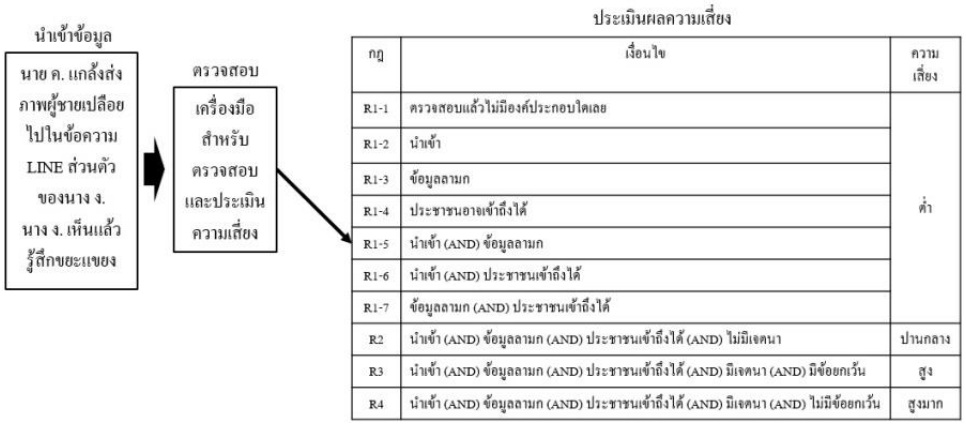
<u>ตัวอย่าง 1</u> การประเมินความเสี่ยงการกระทำผิด ประมวลกฎหมายอาญา มาตรา 393 เช่น นำเข้าข้อมูลการกระทำว่า “นาย ก. ด่านาง ข.ในกลุ่มไลน์ที่ทำงานว่า อีดอก เพราะไม่ชอบขี้หน้า” เมื่อตรวจสอบด้วยเครื่องมือได้ผลว่า นาย ก. เป็นผู้กระทำ ส่วน นาง ข. เป็นผู้ถูกกระทำ การด่าว่าอีดอกเป็นพฤติกรรมและถ้อยคำที่ตรงกับองค์ประกอบ [ดูหมิ่น] พื้นที่การกระทำในกลุ่มไลน์ตรงกับองค์ประกอบ [โฆษณา] การกระทำจึงครบองค์ประกอบข้อเท็จจริง (AND) กระทำไปเพราะมีเจตนา (AND) พฤติการณ์ไม่มี [ข้อยกเว้น] ผลการตรวจสอบเข้ากฎ R4 ซึ่งมีเงื่อนไข (IF) คือ ดูหมิ่น (AND) โฆษณา (AND) มีเจตนา (AND) ไม่มีข้อยกเว้น (THEN) ผลลัพธ์ระดับความเสี่ยงในการกระทำความผิดตามประมวลกฎหมายอาญามาตรา 393 คือ ระดับสูงมาก ดังตัวอย่างในภาพที่ 4



กฎ	เงื่อนไข	ความเสี่ยง
R1-1	ตรวจสอบแล้วไม่มีองค์ประกอบใดเลย	ต่ำ
R1-2	ดูหมิ่น	
R1-3	โฆษณา	
R2	ดูหมิ่น (AND) โฆษณา (AND) ไม่มีเจตนา	ปานกลาง
R3	ดูหมิ่น (AND) โฆษณา (AND) มีเจตนา (AND) มีข้อยกเว้น	สูง
R4	ดูหมิ่น (AND) โฆษณา (AND) มีเจตนา (AND) ไม่มีข้อยกเว้น	สูงมาก

ภาพที่ 4 จำลองการประเมินความเสี่ยง ตามมาตรา 393

ตัวอย่าง 2 การประเมินความเสี่ยงการกระทำผิด พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14 (4) เช่น นำเข้าข้อมูลการกระทำว่า “นาย ค. แกล้งส่งภาพผู้ชายเปลือย ไปในข้อความ LINE ส่วนตัวของนาง ง. นาง ง. เห็นแล้วรู้สึกขยะแขยง” เมื่อตรวจสอบด้วยเครื่องมือได้ผลว่า นาย ค. เป็นผู้กระทำ ส่วน นาง ง. เป็นผู้ถูกกระทำ การส่งภาพตรงกับองค์ประกอบ [นำเข้า] ภาพผู้ชายเปลือยตรงกับองค์ประกอบ [ข้อมูลลามก] พื้นที่การกระทำในข้อความ LINE ส่วนตัว ไม่ตรงกับองค์ประกอบ [ประชาชนอาจเข้าถึงได้] การกระทำไม่ครบองค์ประกอบข้อเท็จจริง ผลการตรวจสอบเข้ากฎ R1 ซึ่งมีเงื่อนไข (IF) คือ ไม่มีองค์ประกอบข้อเท็จจริงข้อใดเลย หรือมีเพียงบางข้อแต่ไม่ครบทุกข้อ (THEN) ผลลัพธ์ระดับความเสี่ยงในการกระทำความผิดตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14 (4) คือ ระดับต่ำ ดังตัวอย่างในภาพที่ 5



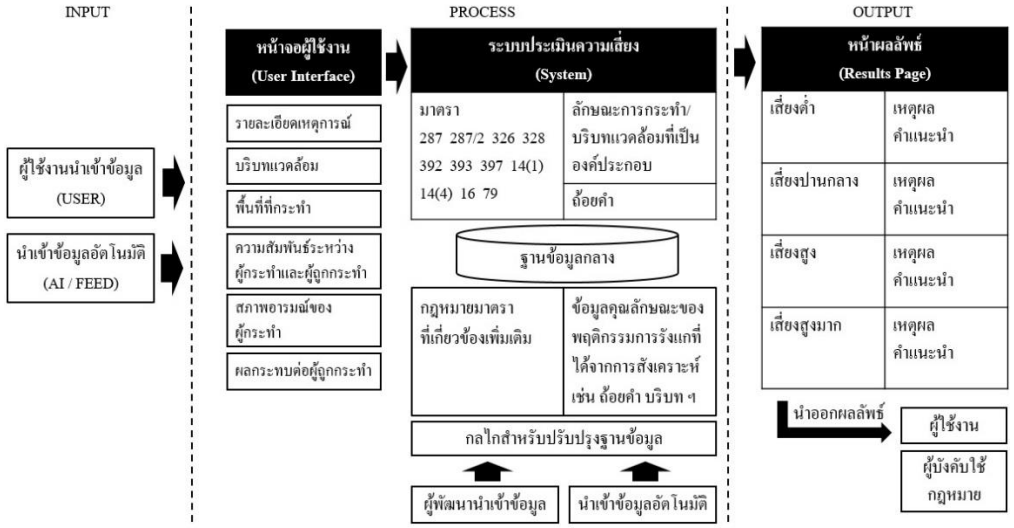
กฎ	เงื่อนไข	ความเสี่ยง
R1-1	ตรวจสอบแล้วไม่มีองค์ประกอบใดเลย	ต่ำ
R1-2	นำเข้า	
R1-3	ข้อมูลลามก	
R1-4	ประชาชนอาจเข้าถึงได้	
R1-5	นำเข้า (AND) ข้อมูลลามก	
R1-6	นำเข้า (AND) ประชาชนเข้าถึงได้	
R1-7	ข้อมูลลามก (AND) ประชาชนเข้าถึงได้	
R2	นำเข้า (AND) ข้อมูลลามก (AND) ประชาชนเข้าถึงได้ (AND) ไม่มีเจตนา	ปานกลาง
R3	นำเข้า (AND) ข้อมูลลามก (AND) ประชาชนเข้าถึงได้ (AND) มีเจตนา (AND) มีข้อยกเว้น	สูง
R4	นำเข้า (AND) ข้อมูลลามก (AND) ประชาชนเข้าถึงได้ (AND) มีเจตนา (AND) ไม่มีข้อยกเว้น	สูงมาก

ภาพที่ 5 จำลองการประเมินความเสี่ยง ตามมาตรา 14 (4)

ผลลัพธ์ความเสี่ยงตามกรอบแนวคิดดังที่กล่าวมาข้างต้น เป็นความเสี่ยงด้านโอกาสที่จะเกิด (Likelihood) โดยเฉพาะ คือ การกระทำที่ตรวจสอบมีโอกาสผิดกฎหมายแต่ละมาตรามากน้อยเพียงใด โดยไม่คำนึงถึงด้านผลกระทบ (Impact) ซึ่งเกี่ยวข้องกับความสามารถในการแบกรับความเสี่ยงในด้านต่าง ๆ ที่แตกต่างกันไปตามปัจจัยของผู้กระทำแต่ละคน กระบวนการตามกรอบแนวคิดนี้จึงสามารถนำไปใช้ได้ทั้งการประเมินความเสี่ยงโดยฝ่ายผู้กระทำและตรวจสอบการกระทำโดยฝ่ายผู้ถูกกระทำ

3. แนวคิดเชิงระบบคอมพิวเตอร์สำหรับประเมินความเสี่ยงต่อการกระทำผิดกฎหมาย

คณะวิจัยนำกรอบแนวคิดสำหรับประเมินความเสี่ยงต่อการกระทำผิดกฎหมายทั่วไป พัฒนาต่อยอดเป็นกรอบแนวคิดเชิงระบบคอมพิวเตอร์ที่สามารถนำไปสู่การพัฒนาโปรแกรมคอมพิวเตอร์ใช้ประเมินความเสี่ยงต่อการกระทำผิดกฎหมาย มีขั้นตอนการทำงานดังแสดงในภาพที่ 6



ภาพที่ 6 แนวคิดเชิงระบบคอมพิวเตอร์สำหรับประเมินความเสี่ยงต่อการกระทำผิดกฎหมาย

แนวทางการนำกรอบแนวคิดสู่โปรแกรมคอมพิวเตอร์

1. การรวบรวมข้อมูลเพื่อนำเข้าสู่ระบบ

ผู้ใช้งานกรอบแนวคิด/ผู้พัฒนาโปรแกรม รวบรวมรายละเอียดของการกระทำผิดในมาตราที่เกี่ยวข้องดังแสดงในผลการวิจัย บริบทต่าง ๆ ที่เกี่ยวข้อง ระบุกฎการประเมินความเสี่ยงให้ละเอียด

2. การออกแบบระบบและโปรแกรม

2.1 ออกแบบโครงสร้างของโปรแกรม โดยเน้นการออกแบบที่สามารถขยายได้ในอนาคต

2.2 ออกแบบหน้าจอผู้ใช้งาน (User Interface) พัฒนาหน้าจอผู้ใช้งานที่ใช้งานง่าย คำนึงถึงความสะดวกในการใช้งานสำหรับประชาชนทั่วไป ช่องป้อนข้อมูลมีให้ผู้ใช้ระบุรายละเอียดเหตุการณ์และบริบทที่เกี่ยวข้อง และอาจสามารถนำเข้าสื่อ เช่น ภาพ วิดีโอ ระบุพื้นที่ที่กระทำ เช่น ข้อความส่วนตัว จดหมายอิเล็กทรอนิกส์ เว็บบอร์ด ระบุความสัมพันธ์ระหว่างผู้กระทำและผู้ถูกกระทำ เช่น คนแปลกหน้า เพื่อน ศัตรู ระบุสภาพอารมณ์ (ถ้ามี) และผลกระทบต่อผู้ถูกกระทำ เช่น เสียชื่อเสียง อับอาย

2.3 ออกแบบหน้าผลลัพธ์ แสดงผลการประเมินความเสี่ยงในรูปแบบที่เข้าใจง่ายและระบุว่าการกระทำมีความเสี่ยงในการละเมิดกฎหมายใดบ้าง พร้อมแสดงคำแนะนำที่เหมาะสม โดยแบ่งระดับความเสี่ยงเป็น 4 ระดับ คือ เสี่ยงต่ำ, เสี่ยงปานกลาง, เสี่ยงสูง และเสี่ยงสูงมาก

3. การพัฒนาโปรแกรม

การพัฒนาโปรแกรม ไม่ว่าจะเป็นแนวคิดแบบออฟไลน์หรือออนไลน์ ต้องมีส่วนระบบส่วนหน้า (Front-End System) ที่ติดต่อกับผู้ใช้งานดังส่วนของการออกแบบ ทั้งหน้าจอส่วนนำเข้าข้อมูลและแสดงผลลัพธ์ที่ตอบสนองทั้งป้อนข้อมูลด้วยมือและด้วยการทำงานป้อนข้อมูลอัตโนมัติตามส่วน เพื่อให้โปรแกรมที่พัฒนาขึ้นสามารถตรวจสอบและวิเคราะห์ข้อมูลนำเข้าได้อย่างถูกต้อง

ส่วนการประมวลผลเบื้องหลัง (Back-End System) แบ่งเป็นส่วนการรับข้อมูลจากส่วนการป้อนข้อมูลนำเข้า เพื่อนำเข้าสู่ส่วนการประเมินความเสี่ยงที่จำเป็นต้องมีอัลกอริทึมการตรวจสอบ วิเคราะห์ถ้อยคำบริบท และความหมายของข้อความ วิเคราะห์เนื้อหา โดยอาศัยฐานข้อมูลของมาตรากฎหมายที่จำเป็นต้องนำเข้าสู่ส่วนประมวลผลให้ครบถ้วนก่อนเป็นเบื้องต้น จากนั้นประเมินความเสี่ยงด้วยระบบอิงตามกฎ (Rule-Based System) ตามกรอบแนวคิดที่นำเสนอไว้ ส่วนประมวลผลเบื้องหลังต้องมีกลไกสำหรับการปรับปรุงฐานข้อมูลและกฎให้ทันสมัยอย่างสม่ำเสมอ ทั้งต้องมีระบบรักษาความปลอดภัยข้อมูล เพื่อให้ผู้ใช้งานมั่นใจว่าข้อมูลที่ป้อนเข้าสู่ระบบจะถูกเก็บรักษาเป็นความลับ

4. การประเมินและปรับปรุง

ในการนำกรอบแนวคิดไปใช้งานจำเป็นอย่างยิ่งต้องมีการประเมินประสิทธิภาพการทำงานของโปรแกรมในด้านต่าง ๆ อยู่เสมอ ไม่ว่าจะเป็นความแม่นยำในการตรวจสอบและประเมินความเสี่ยง ความรวดเร็วในการประมวลผลและการตอบสนองต่อผู้ใช้งาน รวมถึงปรับปรุงฐานข้อมูลอยู่เสมอด้วย

อภิปรายผลและข้อเสนอแนะการวิจัย

จากผลการศึกษา การรังแกบนสื่อสังคมออนไลน์สามารถกระทำผ่านอุปกรณ์อิเล็กทรอนิกส์ได้ง่ายโดยมีรูปแบบพฤติกรรมจำแนกได้ 7 ประเภท กฎหมายที่เกี่ยวกับการรังแกบนสื่อสังคมออนไลน์ มี 3 ฉบับ คือ ประมวลกฎหมายอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีบทบัญญัติครอบคลุมพฤติกรรมการรังแกบนสื่อสังคมออนไลน์เกือบทุกประเภท ยกเว้นการกีดกันออกจากกลุ่ม ซึ่งไม่มีกฎหมายที่สามารถใช้บังคับกับการกระทำได้โดยตรง การรังแกบนสื่อสังคมออนไลน์ครั้งหนึ่งอาจเข้าองค์ประกอบกฎหมายและเป็นความผิดได้หลายฐานความผิดในการกระทำเดียวกันขึ้นอยู่กับบริบทแวดล้อมของการกระทำนั้น การประเมินความเสี่ยงต่อการกระทำผิดกฎหมายจึงมีประโยชน์ในด้านการสร้างความตระหนักรู้ถึงผลของการกระทำและความรับผิดที่อาจเกิดขึ้นทั้งฝ่ายผู้กระทำและฝ่ายผู้ถูกกระทำ

ผลการวิจัยชี้ให้เห็นถึงประโยชน์ของการพัฒนากรอบแนวคิดสำหรับประเมินความเสี่ยงต่อการกระทำผิดกฎหมายซึ่งเป็นเครื่องมือที่ช่วยให้ประชาชนสามารถตรวจสอบและประเมินความเสี่ยงเบื้องต้นได้ด้วยตนเอง โดยนำเอาโครงสร้างความรับผิดทางอาญามาใช้เป็นฐานในการตรวจสอบพฤติกรรมการรังแกบนสื่อสังคมออนไลน์รูปแบบต่าง ๆ ซึ่งช่วยในการประเมินว่า การกระทำมีโอกาสเข้าข่ายการเป็นความผิดตามกฎหมายหรือไม่ การใช้โครงสร้างความรับผิดทางอาญาเป็นพื้นฐานในการตรวจสอบช่วยให้ผู้ใช้สามารถเข้าใจถึงองค์ประกอบความผิดและเหตุยกเว้นความผิดอย่างชัดเจน การใช้ชุดของกฎในรูปของเงื่อนไขเพื่อประเมินระดับความเสี่ยง ช่วยให้สามารถประเมินความเสี่ยงในแต่ละกรณีได้โดยอัตโนมัติ ทำให้เกิดการป้องกันความเสี่ยงในการกระทำที่อาจเข้าข่ายความผิดกฎหมาย

กรอบแนวคิดสำหรับประเมินความเสี่ยงที่พัฒนาขึ้นนี้ สามารถประยุกต์ใช้กับการประเมินความเสี่ยงต่อการกระทำความผิดอาญาตามกฎหมายอื่นได้ โดยปรับปรุงเครื่องมือที่ใช้ในการตรวจสอบในส่วนฐานข้อมูลกฎหมายและพฤติกรรมการกระทำในฐานความผิดที่ต้องการตรวจสอบและประเมิน

อย่างไรก็ตาม การประเมินความเสี่ยงตามกรอบแนวคิดนี้มีข้อจำกัดในเรื่องความแม่นยำต่อรูปแบบการกระทำและบริบทใหม่ในการรังแกที่เกิดขึ้น เนื่องจากขึ้นอยู่กับบริบทและปริมาณฐานข้อมูลที่ใช้ในการวิเคราะห์ ซึ่งอาจไม่ครอบคลุมสถานการณ์ใหม่ ๆ ที่ซับซ้อนทั้งหมด จึงต้องมีการปรับปรุงฐานข้อมูลให้ครอบคลุมและเท่าทันกับการเปลี่ยนแปลงของพฤติกรรมบนสื่อสังคมออนไลน์ รวมถึงแนวทางการตีความและปรับใช้กฎหมายของศาล ดังนั้น หากมีระบบเรียนรู้เชิงลึก (Deep Learning) ที่ทำงานอัตโนมัติด้วยปัญญาประดิษฐ์ จะยิ่งทำให้กรอบแนวคิดมีประสิทธิภาพดีมากยิ่งขึ้น

ข้อจำกัดอีกประการหนึ่ง คือ การประเมินความเสี่ยงตามกรอบแนวคิดนี้ออกแบบให้ประเมินความเสี่ยงจากโอกาสที่การกระทำจะเป็นความผิดเท่านั้น โดยไม่คำนึงถึงด้านผลกระทบที่ผู้กระทำอาจได้รับหากมีการดำเนินการทางกฎหมายเกิดขึ้น ทำให้เหมาะกับการประยุกต์ใช้เพื่อสร้างความตระหนักรู้และหลีกเลี่ยงการกระทำความผิดเท่านั้น แต่ไม่เหมาะสมกับการใช้เพื่อประเมินความเสี่ยงในการดำเนินงานขององค์กรที่ต้องคำนึงถึงความถี่ของการละเมิดกฎหมาย ผลกระทบต่อองค์กร ความสามารถขององค์กรในการจัดการความเสี่ยง เพื่อวางนโยบายที่เหมาะสมกับการขับเคลื่อนองค์กรต่อไป

งานวิจัยนี้แสดงให้เห็นถึงความสำคัญของการบูรณาการความรู้ทางกฎหมายกับวิทยาการคอมพิวเตอร์ และความร่วมมือระหว่างสถานศึกษา หน่วยงานในกระบวนการยุติธรรม กับหน่วยงานที่ด้านเทคโนโลยีสารสนเทศ เพื่อพัฒนานวัตกรรมที่ช่วยแก้ไขปัญหาสังคม การนำกรอบแนวคิดเชิงระบบคอมพิวเตอร์ไปพัฒนาเป็นโปรแกรมสำหรับประเมินความเสี่ยงทางกฎหมาย ย่อมเป็นแนวทางที่น่าสนใจในการลดปัญหาการรังแกบนสื่อสังคมออนไลน์ ทำให้ประชาชนโดยเฉพาะกลุ่มเสี่ยงที่เป็นเยาวชน มีเครื่องมือในการตรวจสอบประเมินความเสี่ยงด้วยตนเองที่อาศัยระบบการทำงานอัตโนมัติของเครื่องคอมพิวเตอร์ อย่างไรก็ตาม โปรแกรมที่จะพัฒนาขึ้นยังต้องมีการทดสอบและปรับปรุงเพื่อให้มั่นใจได้ว่าเครื่องมือนี้สามารถทำงานได้อย่างแม่นยำในสภาพแวดล้อมจริง สามารถรองรับการเปลี่ยนแปลงทั้งในส่วนของกฎหมายและเทคโนโลยีที่เกิดขึ้น และให้คำแนะนำที่เหมาะสมแก่ผู้ใช้งาน

คณะวิจัยมีข้อเสนอแนะจากผลการวิจัย ดังนี้

1. รัฐควรจัดทำเว็บไซต์หรือโปรแกรมประยุกต์สำหรับประชาชนใช้ประเมินความเสี่ยงต่อการกระทำผิดกฎหมายจากการรังแกบนสื่อสังคมออนไลน์ที่อาศัยกรอบแนวคิดและแนวทางพัฒนาจากผลการวิจัยนี้ โดยความร่วมมือระหว่างกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและกระทรวงยุติธรรม

2. หน่วยงานในกระบวนการยุติธรรมและสถาบันการศึกษาสามารถนำผลการวิจัยนี้ไปใช้พัฒนากลยุทธ์เพื่อลดปัญหาการรังแกบนสื่อสังคมออนไลน์ ผ่านการให้ความรู้ด้วยสื่อประชาสัมพันธ์หรือคู่มือเผยแพร่แก่ประชาชนเกี่ยวกับการประเมินความเสี่ยงต่อการกระทำผิดกฎหมายด้วยตนเอง

รายการอ้างอิง

ภาษาไทย

กฤษฎา แสงเจริญทรัพย์ และ วีนันท์กานต์ รุจิภักดิ์. (2564). Cyberbullying ความหมาย และการทบทวนแนวคิดภายใต้บริบทของสังคมไทย. *วารสารกฎหมายและนโยบายสาธารณสุข*, *7*(1), 171-193.

กองเฝ้าระวังทางวัฒนธรรม. (2564). *คู่มือการขับเคลื่อนงานการสร้างภูมิคุ้มกันของสังคมในมิติทางวัฒนธรรม ประจำปีงบประมาณ พ.ศ. 2564*. วันที่ค้นข้อมูล 9 กันยายน 2567, เข้าถึงได้จาก https://surveillance.m-culture.go.th/th/db_53_surveillance_48/24310

คุณาธิป ผลทรัพย์. (2563). *พฤติกรรมการรังแกทางไซเบอร์ของนักศึกษาปริญญาตรี ในเขตภาคตะวันออกของประเทศไทย*. วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยบูรพา.

ทัศนีย์ ดำเกิงศักดิ์ และแก้วกัญญา เสวกสุริยวงศ์. (2567). แนวทางป้องกันการลดพฤติกรรมการกลั่นแกล้งบนโลกไซเบอร์ Cyberbullying โดยใช้มาตรการทางกฎหมาย. *วารสารนิเทศสยามปริทัศน์*, *23*(1).

ธวัชชัย ดวงไทย และสาวิตรี พรหมสิทธิ์. (2565). การประทุษร้ายบนโลกไซเบอร์. *วารสารวิทยาการจัดการมหาวิทยาลัยราชภัฏนครราชสีมา*, *1*(1), 1-15.

ปองกมล สุรัตน์. (2561). สาเหตุและผลกระทบที่เกี่ยวข้องกับการรังแกผ่านโลกไซเบอร์: กรณีศึกษาเยาวชนไทยผู้ถูกรังแก. *วารสารวิชาการ สถาบันเทคโนโลยีแห่งสุวรรณภูมิ*, *4*(1), 260-273.

พินวา แสนใหม่. (2563). *การรังแกทางไซเบอร์ผ่านสื่อออนไลน์ สาเหตุ และแนวทางการจัดการปัญหา*. วิทยานิพนธ์ปริญญามหาบัณฑิต, สถาบันบัณฑิตพัฒนบริหารศาสตร์.

ภูวสิทธิ์ ภูลวรรณ และคณะ. (2563). พฤติกรรมการกลั่นแกล้งออนไลน์ของนักศึกษามหาวิทยาลัยราชภัฏสกลนคร. *วารสารวิจัยสาธารณสุขศาสตร์ มหาวิทยาลัยราชภัฏอุบลราชธานี*, *9*(1), 83-92.

มูลนิธิส่งเสริมสื่อเด็กและเยาวชน. (2561). *การกลั่นแกล้งบนโลกไซเบอร์ (Cyberbullying)*. กรุงเทพฯ: นัชชาวัฒน์.

ศักดิกร วัฒนกูล และจิรวุฒิ ลิปิพันธ์. (2566). อาชญากรรมทางคอมพิวเตอร์ ศึกษากรณีการเปิดเผยข้อมูลส่วนบุคคลในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้อื่น (doxing). *วารสารบัณฑิตศึกษามหาวิทยาลัยธุรกิจบัณฑิตย์*, *12*(1), 192-208.

ศุภากร หวัง และสมชาย เตียวกุล. (2562). การถูกกลั่นแกล้งบนสื่อสังคมออนไลน์ของนักศึกษาสาขาวิทยาศาสตร์สุขภาพ. *วารสารจิตวิทยาคลินิก*, *50*(2), 17-28.

สาวตรี สุขศรี. (2563). *กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์* (พิมพ์ครั้งที่ 2). โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. (2564). *คู่มือการบริหารความเสี่ยงของ สวทช.* วันที่ค้นข้อมูล 9 กันยายน 2567, เข้าถึงได้จาก https://waa.inter.nstda.or.th/stks/pub/2021/20210126-enterprise-risk-management-2564.pdf

สำนักงานสถิติแห่งชาติ. (2563). *สรุปผลที่สำคัญการใช้ไอซีทีของเด็กและเยาวชน พ.ศ. 2563*. วันที่ค้นข้อมูล 9 กันยายน 2567, เข้าถึงได้จาก https://www.nso.go.th/nsoweb/storage/survey_detail/2023/20230721160830_50941.pdf

สุเนติ คงเทพ. (2559). *คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์*. กรุงเทพฯ: บริษัท กรุงสยาม พับลิชชิ่ง จำกัด.

ภาษาอังกฤษ

Pal, K., & Campbell, J. (1997). An application of rule-based and case-based reasoning within a single legal knowledge-based system. *The Data Base for Advances in Information Systems, 28*(4).

Saengcharoensap, K., & Rujiprak, V. (2021). Cyberbullying Among University Students in Thailand. *Thammasat Review, 24*(2), 41-58.

Society of Corporate Compliance and Ethics & Health Care Compliance Association [SCCE & HCCA], (2020). *Compliance Risk Management: Applying the COSO ERM Framework.* Retrieved October 4, 2023, from https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf

Suarez-Angelino, L. (2023). *Cyberbullying: Types, effects, & how to get help. Choosing Therapy*. Retrieved October 4, 2023, from https://www.choosingtherapy.com/cyberbullying/

Timme, I., & Rietveld, R. (2019). *Rule-Based Systems for Decision Support and Decision-Making in Dutch Legal Practice*. A Brief Overview of Applications and Implications. Droit et Societe. 3.

Willard, N. (2007). Educator's Guide to Cyberbullying and Cyberthreats. Retrieved October 4, 2023, from https://www.embracecivility.org/wp-content/uploadsnew/Educators-Guide-Cyber-Safety.pdf