

บทความวิชาการ

การเอาผิดการสะกดรอยตามทางไซเบอร์: ศึกษาเปรียบเทียบกฎหมายไทย
กับสหรัฐอเมริกา อังกฤษและเวลส์ และญี่ปุ่น

Liability for Cyberstalking: A Comparative Study of Thai Law
with the Laws of the United States, England and Wales, and
Japan

ปรุงศักดิ์ เชาวนชาติ ¹

Prungsak Chaowachart ²

มหาวิทยาลัยกรุงเทพ

9/1 หมู่ 5 ถนนพหลโยธิน ตำบลคลองหนึ่ง อำเภอคลองหลวง จังหวัดปทุมธานี 12120

9/1 Moo 5, Phahonyothin Road, Khlong Nueng,

Khlong Luang, Pathum Thani 12120

* Corresponding author E-mail: prungsak_c@bu.ac.th

วันที่รับบทความ : 28 เมษายน 2569 วันที่แก้ไขบทความ : 4 พฤษภาคม 2569

วันที่ตอบรับ : 29 มิถุนายน 2569 วันที่เผยแพร่ : 29 มิถุนายน 2569

¹ อาจารย์ปรุงศักดิ์ เชาวนชาติ, อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ

² Mr.Prungsak Chaowachart, Lecturer at the Faculty of Law, Bangkok University.

บทคัดย่อ

บทความวิชาการฉบับนี้มีวัตถุประสงค์เพื่อศึกษาลักษณะของการสะกดรอยตามทางไซเบอร์ (Cyberstalking) วิเคราะห์มาตรการทางกฎหมายของประเทศไทยเปรียบเทียบกับกฎหมายของสหรัฐอเมริกา อังกฤษและเวลส์ และญี่ปุ่น และเสนอแนวทางการปรับปรุงกฎหมายไทย โดยใช้วิธีการทางนิติศาสตร์เชิงเอกสาร ประกอบกับการเปรียบเทียบกฎหมายเชิงหน้าที่

ผลการศึกษาพบว่า กฎหมายไทยขาดบทบัญญัติเฉพาะ ขาดกลไกคำสั่งคุ้มครองล่วงหน้า และอัตราโทษไม่เหมาะสมกับความรุนแรงของพฤติกรรม ในขณะที่กฎหมายของสามประเทศที่ศึกษามีพัฒนาการก้าวหน้า ทั้งฐานความผิดเฉพาะตาม 18 U.S.C. § 2261A และคดี *Counterman v. Colorado* (2023) ของสหรัฐอเมริกา Stalking Protection Order ของอังกฤษและเวลส์ และพระราชบัญญัติแก้ไขเพิ่มเติม Stalker Regulation Act ของญี่ปุ่น ค.ศ. 2025 ที่ขยายการกำกับดูแลให้ครอบคลุมการใช้อุปกรณ์ Bluetooth Tag ในการติดตามตำแหน่งของผู้เสียหาย

ผู้เขียนเสนอให้เพิ่มมาตรา 309/2 และ 309/3 ในประมวลกฎหมายอาญา เพื่อกำหนดฐานความผิดเฉพาะ และคำสั่งคุ้มครองผู้เสียหายชั่วคราว พร้อมแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้ครอบคลุมการติดตั้งโปรแกรมสอดแนม โดยกำหนดเจตนาในระดับ รู้หรือควรจะได้รู้ เพื่อสร้างสมดุลกับเสรีภาพในการแสดงออกตามรัฐธรรมนูญ และเสนอแนวทางของอังกฤษและเวลส์เป็นต้นแบบหลัก

คำสำคัญ: การสะกดรอยตามทางไซเบอร์, กฎหมายเปรียบเทียบ, คำสั่งคุ้มครองผู้เสียหาย, กฎหมายอาญา

Abstract

This research article examines the nature of cyberstalking, analyses Thailand's existing legal measures, and undertakes a comparative study of the laws of the United States, England and Wales, and Japan, in order to propose reforms to Thai law. The study employs Doctrinal Legal Research combined with Functional Comparative Law methodology.

The findings reveal that Thai law lacks a specific offence, has no pre-emptive protection mechanism, and imposes penalties disproportionate to the gravity of cyberstalking. In contrast, the three comparator jurisdictions have developed more advanced frameworks: the specific federal offence under 18 U.S.C. § 2261A and the recklessness standard established in *Counterman v. Colorado* (2023) in the United States; the Stalking Protection Order regime of England and Wales; and the 2025 amendment to Japan's Stalker Regulation Act, which extends regulation to the use of Bluetooth tracking tags.

The researcher proposes inserting Sections 309/2 and 309/3 into the Thai Penal Code to establish a specific criminal offence and a regime of temporary protection orders for victims, and amending the Computer Crime Act B.E. 2550 to cover the installation of stalkerware. The mens rea element should be set at the level of 'knew or ought to have known' in order to balance victim protection with the constitutional guarantee of freedom of expression. The study recommends adopting the approach of England and Wales as the principal model for reform.

Keywords: cyberstalking, comparative law, protection order, criminal law

1. ความนำ

การพัฒนาของเทคโนโลยีสารสนเทศและเครือข่ายสังคมออนไลน์ได้เปลี่ยนรูปแบบของการสะกดรอยตามไปสู่ การสะกดรอยตามทางไซเบอร์ (Cyberstalking) ซึ่งก่อให้เกิดผลกระทบรุนแรงต่อสภาพจิตใจ ชื่อเสียง และในบางกรณีอาจนำไปสู่ความรุนแรงทางกายภาพหรือการฆาตกรรม (Logan & Walker, 2017) ในประเทศไทยปัญหานี้มีแนวโน้มเพิ่มขึ้น ผู้เสียหายส่วนใหญ่เป็นผู้หญิงและกลุ่มผู้มีความหลากหลายทางเพศ อย่างไรก็ตาม กฎหมายไทยยังไม่มีบทบัญญัติเฉพาะ ต้องอาศัยกฎหมายทั่วไปที่มีได้ครอบคลุมพฤติการณ์ดังกล่าวโดยตรง แม้รัฐบาลได้ตราพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 แต่กฎหมายดังกล่าวมิได้ออกแบบเพื่อจัดการกับการสะกดรอยตามทางไซเบอร์โดยเฉพาะ

เมื่อเปรียบเทียบกับต่างประเทศ พบว่าสหรัฐอเมริกามีฐานความผิดเฉพาะระดับสหพันธรัฐ อังกฤษและเวลส์มีกลไก Stalking Protection Order ที่คุ้มครองผู้เสียหายล่วงหน้า และญี่ปุ่นได้ปรับปรุงกฎหมายให้ครอบคลุมเทคโนโลยีติดตามรูปแบบใหม่ บทความนี้จะมุ่งศึกษาเปรียบเทียบ กฎหมายของประเทศไทยกับสามประเทศข้างต้น เพื่อวิเคราะห์ช่องว่างและเสนอแนวทาง การปรับปรุงมาตรการทางกฎหมายให้สามารถคุ้มครองผู้เสียหายได้อย่างมีประสิทธิภาพ

บทความวิชาการฉบับนี้ใช้วิธีวิจัยทางนิติศาสตร์เชิงเอกสาร (Doctrinal Legal Research) โดยศึกษาวิเคราะห์บทบัญญัติของกฎหมายไทยและกฎหมายต่างประเทศที่เกี่ยวข้อง รวมถึง คำพิพากษาศาลฎีกา ตำราทางวิชาการ บทความวิจัย และเอกสารราชการที่เกี่ยวข้อง ประกอบกับวิธีการเปรียบเทียบกฎหมายเชิงหน้าที่ (Functional Comparative Law) ตามแนวทางของ Zweigert and Kötz (1998) เพื่อเปรียบเทียบมาตรการทางกฎหมายของประเทศไทย กับมาตรการทางกฎหมายของสหรัฐอเมริกา อังกฤษและเวลส์ และญี่ปุ่น โดยมีเกณฑ์การเปรียบเทียบ 4 ประเด็น ได้แก่ (1) ความมีบทบัญญัติเฉพาะ (2) ประสิทธิภาพในการบังคับใช้ (3) กลไกคำสั่งคุ้มครองล่วงหน้า และ (4) ความได้สัดส่วนของอัตราโทษ

2. แนวคิดและทฤษฎีเกี่ยวกับการสะกดรอยตามทางไซเบอร์

2.1 แนวคิดเกี่ยวกับการสะกดรอยตามทางไซเบอร์

คำว่า สะกดรอยตาม (Stalking) ในทางวิชาการหมายถึงพฤติการณ์การกระทำซ้ำ ๆ ของบุคคลหนึ่ง ต่อบุคคลอื่นในลักษณะที่ทำให้ผู้ถูกรบกวนเกิดความหวาดกลัวต่อความปลอดภัยของตนเองหรือบุคคลใกล้ชิด (Mullen et al., 2009) ส่วนการสะกดรอยตามทางไซเบอร์มีลักษณะเฉพาะที่แตกต่างคือ ผู้กระทำสามารถดำเนินการจากระยะไกลและปกปิดตัวตนผ่านกิจกรรมประจำวันบนระบบออนไลน์ (Reyns, 2013) รวมถึงการใช้เทคโนโลยีก้าวหน้า เช่น Stalkerware และอุปกรณ์ติดตามตำแหน่งผ่าน Bluetooth นักวิชาการได้จำแนกประเภทผู้กระทำความผิดเป็น 5 กลุ่ม ได้แก่ Rejected Stalker (ผู้ถูกปฏิเสธความสัมพันธ์) Resentful Stalker (ผู้ต้องการแก้แค้น) Intimacy Seeker (ผู้หลงใหล) Incompetent Suitor (ผู้ขาดทักษะทางสังคม) และ Predatory Stalker (ผู้มีเจตนาทำร้ายทางเพศหรือกายภาพ) การจำแนกประเภทนี้มีนัยสำคัญต่อการกำหนดมาตรการป้องกันและประเมินความเสี่ยง (Mullen et al., 2009)

สำหรับงานวิชาการทางกฎหมายของไทยที่เกี่ยวข้อง ได้แก่ ชญาณิพิมพ์ บัวดิษฐ์ ๒๕๕๑ (2551) ที่ศึกษาความรับผิดชอบทางอาญาของผู้คุกคามผู้อื่นโดยใช้อินเทอร์เน็ต (ชนิดา อร่ามพงษ์ และสุชาติ ธรรมาพิทักษ์กุล, 2557; รักษิชาติ โพธิ์พิทักษ์กุล, 2550) ที่อาศัยกรอบของ Royackers (2000) และเจษฎา การ์นต์ (2566) ที่เสนอเพิ่มมาตรา 309/1 ในประมวลกฎหมายอาญา แม้งานวิจัยดังกล่าว จะมีคุณูปการในการวางพื้นฐานการศึกษาเรื่องการสะกดรอยตามทางไซเบอร์ในประเทศไทย แต่ยังคงมีข้อจำกัดในเชิงขอบเขตและกรอบวิเคราะห์ที่บทความนี้มุ่งเติมเต็ม กล่าวคือ งานส่วนใหญ่ยังคงมุ่งเปรียบเทียบกฎหมายไทยกับกฎหมายของสหรัฐอเมริกาเป็นหลัก โดยยังมิได้ครอบคลุมพัฒนาการของกฎหมายในอังกฤษและเวลส์ และในญี่ปุ่น ซึ่งมีมาตรการสำคัญทั้งในด้านการคุ้มครองผู้เสียหายล่วงหน้าและการรับมือเทคโนโลยีติดตามรูปแบบใหม่ นอกจากนี้ ขอบเขตของการศึกษายังมิได้ขยายไปยังเทคโนโลยีที่เกิดขึ้นภายหลังปี ค.ศ. 2020 เช่น Stalkerware อุปกรณ์ติดตามผ่าน Bluetooth และเทคโนโลยีติดตามตำแหน่งรูปแบบใหม่ ทั้งยังขาด

การวิเคราะห์อย่างเป็นระบบเกี่ยวกับกลไกคำสั่งคุ้มครองผู้เสียหายล่วงหน้า (Stalking Protection Order) และยังมีได้อภิปรายมิติทางรัฐธรรมนูญ โดยเฉพาะการสร้างสมดุลระหว่างการคุ้มครองผู้เสียหาย กับเสรีภาพในการแสดงออกและหลักความได้สัดส่วน อันเป็นช่องว่างทางวิชาการที่บทความนี้มุ่งสำรวจและเติมเต็ม

2.2 ทฤษฎีที่เกี่ยวข้อง

2.2.1 ทฤษฎีการคุ้มครองสิทธิส่วนบุคคล (Right to Privacy)

ทฤษฎีการคุ้มครองสิทธิส่วนบุคคล (Right to Privacy) ตามแนวคิดของ Warren and Brandeis ตั้งอยู่บนหลักว่าบุคคลย่อมมีสิทธิที่จะอยู่อย่างสงบและได้รับความคุ้มครองความเป็นส่วนตัว ในยุคดิจิทัล แนวคิดนี้ขยายไปสู่กรอบสิทธิดิจิทัล (Digital Rights) ที่ได้รับการรับรอง ในตราสารระหว่างประเทศ เช่น ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 ข้อ 12 และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง ค.ศ. 1966 ข้อ 17 ตลอดจนพัฒนาการของกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น General Data Protection Regulation ของสหภาพยุโรป ทฤษฎีนี้จึงเป็นรากฐานในการอธิบายความจำเป็นในการคุ้มครองบุคคลจาก การสะกดรอยตามทางไซเบอร์

2.2.2 ทฤษฎีกิจกรรมประจำวัน (Routine Activity Theory)

ทฤษฎีกิจกรรมประจำวัน (Routine Activity Theory) ของ Cohen and Felson (1979) อธิบายว่า อาชญากรรมเกิดขึ้นเมื่อมีองค์ประกอบสามประการพร้อมกัน คือ ผู้กระทำที่มีแรงจูงใจ (Motivated Offender) ผู้เสียหายที่เหมาะสม (Suitable Target) และการขาดผู้คุ้มครองที่มีศักยภาพ (Absence of Capable Guardian) ในบริบทของไซเบอร์ ผู้คุ้มครองที่มีศักยภาพมิได้จำกัดเฉพาะผู้บังคับใช้กฎหมายหรือผู้ให้บริการแพลตฟอร์ม แต่ยังรวมถึงเทคโนโลยีที่ทำหน้าที่คุ้มครองโดยอัตโนมัติ เช่น ระบบปัญญาประดิษฐ์ที่ตรวจจับการคุกคาม ซอฟต์แวร์ป้องกันไวรัส และระบบตรวจจับ Stalkerware ทฤษฎีนี้สนับสนุนการออกแบบกลไก Stalking Protection Order ที่เพิ่มประสิทธิภาพของผู้คุ้มครองในขั้นก่อนการดำเนินคดีอาญา (Home Office, 2020) โดย

ปัจจัยเสี่ยงในการสะกดรอยตามที่ McEwan et al. (2007) ระบุไว้สามารถใช้เป็นกรอบประเมินผู้ต้องสงสัย

2.2.3 ทฤษฎีการลงโทษเชิงป้องกัน (Deterrence Theory)

ทฤษฎีการลงโทษเชิงป้องกัน (Deterrence Theory) ในทางอาชญวิทยาซึ่งมีรากฐานมาจากการงานของ Cesare Beccaria (1764) และ Jeremy Bentham (1789) เสนอว่า การลงโทษจะมีประสิทธิภาพในการป้องกัน การกระทำผิด เมื่อมีความแน่นอน รวดเร็ว และได้สัดส่วนกับความรุนแรงของการกระทำ ในบริบทของ Cyberstalking ทฤษฎีนี้สนับสนุนการกำหนดฐานความผิดเฉพาะที่ชัดเจน และอัตราโทษที่ได้สัดส่วน เพื่อยับยั้งการกระทำผิดทั้งในระดับบุคคล (Specific Deterrence) และในระดับสังคม (General Deterrence) (Nagin, 2013)

3. กฎหมายที่เกี่ยวข้องกับการคุ้มครองผู้เสียหายจากการสะกดรอยทางไซเบอร์

3.1 มาตรการทางกฎหมายของประเทศไทย

แม้กฎหมายไทยยังไม่มีฐานความผิดเฉพาะเกี่ยวกับการสะกดรอยตามทางไซเบอร์ แต่บทบัญญัติบางประการในกฎหมายปัจจุบันอาจนำมาปรับใช้กับพฤติกรรมดังกล่าวได้ ผู้เขียนจะวิเคราะห์บทบัญญัติของประมวลกฎหมายอาญาที่อาจนำมาปรับใช้กับการสะกดรอยตามทางไซเบอร์ โดยเฉพาะมาตรา 397 มาตรา 392 และมาตรา 326 ถึงมาตรา 328 เพื่อพิจารณาองค์ประกอบความผิดและข้อจำกัดในการใช้บังคับกับพฤติการณ์การสะกดรอยตามในพื้นที่ไซเบอร์

3.1.1 ประมวลกฎหมายอาญา

ประมวลกฎหมายอาญาของไทยมิได้บัญญัติความผิดฐานสะกดรอยตามไว้ โดยเฉพาะ การปรับใช้ในทางปฏิบัติต้องอาศัยบทบัญญัติทั่วไป ได้แก่ มาตรา 397 ที่บัญญัติว่า "ผู้ใดกระทำความผิดใด ๆ ต่อผู้อื่น อันเป็นการรังแก ข่มเหง คุกคาม หรือกระทำให้ได้รับความอับอายหรือเดือดร้อนรำคาญ ต้องระวางโทษปรับไม่เกินห้าพันบาท" และในวรรคสอง วรรคสาม กำหนดอัตราโทษเพิ่มในกรณีกระทำในที่สาธารณะสถาน ต่อ

หน้าธารกำนัล หรือมีลักษณะส่อไปในทางที่จะล่วงเกินทางเพศ หรือกระทำโดยอาศัยอำนาจเหนือผู้ถูกระทำ

เมื่อพิจารณาแยกองค์ประกอบความผิดตามมาตรา 397 จะปรากฏว่า การกระทำอันเป็นองค์ประกอบภายนอก ได้แก่ การรังแก ช่มเหง คุกคาม หรือกระทำให้ผู้อื่นได้รับความอับอายหรือเดือดร้อนรำคาญ องค์ประกอบภายในคือเจตนาทั่วไป (General Intent) ตามมาตรา 59 วรรคหนึ่งและวรรคสองแห่งประมวลกฎหมายอาญา โดยผู้กระทำต้องรู้สำนึกในการกระทำและประสงค์ต่อผลหรือเล็งเห็นผล มิจำเป็นต้องมีเจตนาพิเศษเพื่อสะกดรอยตามทางไซเบอร์ ส่วนผลของการกระทำคือสภาพการถูกรังแกช่มเหง คุกคาม ความอับอายหรือความเดือดร้อนรำคาญที่เกิดแก่ผู้เสียหาย (เกียรติขจร วัจนะสวัสดิ์, 2562; คณิต ณ นคร, 2562; ทวีเกียรติ มีนะกนิษฐ, 2565)

นอกจากนี้ ประมวลกฎหมายอาญา มาตรา 392 บัญญัติให้การทำให้อันเกิด ความกลัวหรือตกใจ โดยการขู่เข็ญเป็นความผิด แต่กำหนดเงื่อนไขให้ต้องมีการขู่เข็ญที่ชัดเจน จึงไม่อาจครอบคลุมพฤติการณ์การติดตามแบบเงียบ ๆ ที่ไม่มีการขู่เข็ญโดยตรง ส่วนมาตรา 326 ถึงมาตรา 328 ความผิดฐานหมิ่นประมาท ใช้บังคับเฉพาะกรณีการใส่ความผู้อื่นต่อบุคคลที่สาม จึงไม่ครอบคลุมการเฝ้าติดตามหรือเก็บข้อมูลผู้เสียหายโดยไม่มีการเผยแพร่ข้อความต่อบุคคลที่สาม

3.1.2 คำพิพากษาศาลฎีกาที่เกี่ยวข้อง

เพื่อทำความเข้าใจขอบเขตการบังคับใช้ของมาตรา 397 ในทางปฏิบัติ ผู้วิจัยได้ศึกษาคำพิพากษาศาลฎีกาสำคัญฉบับหนึ่ง ซึ่งเป็นบรรทัดฐานในการตีความบทบัญญัติดังกล่าว คำพิพากษาศาลฎีกาที่ 1631/2538 วินิจฉัยว่าการกล่าวถ้อยคำในที่ประชุมต่อหน้าผู้อื่น ในลักษณะดูหมิ่นเหยียดหยาม เป็นการรังแกช่มเหงในที่สาธารณะ อันเป็นความผิดตามมาตรา 397 อนึ่ง ตามหลักการตีความของตำราอาญาไทย การกระทำตามมาตรา 397 วรรคสอง ต้องเกิดขึ้นในที่สาธารณะสถาน ต่อหน้าธารกำนัล หรือในสถานที่ที่บุคคลทั่วไปสามารถเข้าถึงได้ (เกียรติขจร วัจนะสวัสดิ์, 2562)

จากการวิเคราะห์คำพิพากษา พบว่าศาลฎีกาตีความมาตรา 397 ภายใต้กรอบของการคุ้มครองความสงบเรียบร้อย ในที่สาธารณะ (Public Order) มากกว่าการคุ้มครองสิทธิความเป็นส่วนตัวส่วนบุคคล (Privacy Right) บทบัญญัติดังกล่าวจึงมีข้อจำกัดสำคัญในการนำมาปรับใช้กับการสะกดรอยตามทางไซเบอร์ ได้แก่ การจำกัดขอบเขตเฉพาะการกระทำทางกายภาพในที่สาธารณะ มิได้ครอบคลุมพฤติกรรมผ่านช่องทางอิเล็กทรอนิกส์ อัตราโทษเพียงปรับไม่เกินห้าพันบาทไม่สะท้อนความรุนแรงของการสะกดรอยตามต่อเนื่อง ขาดองค์ประกอบของการกระทำซ้ำ ๆ (Repeated Course of Conduct) อันเป็นลักษณะสำคัญของการสะกดรอยตาม และไม่มีกลไกคำสั่งคุ้มครองผู้เสียหายล่วงหน้า ช่องว่างเหล่านี้สนับสนุนความจำเป็นในการบัญญัติฐานความผิดเฉพาะตามข้อเสนอเรื่องมาตรา 309/2 และมาตรา 309/3 ที่จะกล่าวถึงในส่วนข้อเสนอแนะ (เจษฎา การันต์, 2566)

3.1.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 มีบทบัญญัติที่สามารถปรับใช้ได้บางกรณี กล่าวคือ มาตรา 14 (1) กำหนดความผิดฐานนำเข้าสู่ข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือเป็นเท็จโดยน่าจะเกิดความเสียหายแก่ประชาชน และมาตรา 16 วรรคหนึ่ง กำหนดความผิดฐานนำเข้าสู่ข้อมูลคอมพิวเตอร์ ที่ปรากฏเป็นภาพของผู้อื่นซึ่งเกิดจากการสร้างขึ้น ตัดต่อ หรือดัดแปลง อย่างไรก็ดีตาม มาตรา 14 (1) มุ่งคุ้มครองประชาชนทั่วไปมากกว่าบุคคลใดบุคคลหนึ่งเฉพาะ และมาตรา 16 ครอบคลุมเฉพาะการติดต่อภาพ มิได้ครอบคลุมการติดตามตำแหน่งผ่านดาวเทียม การใช้ Stalkerware ที่ผู้กระทำความผิดนำเข้าสู่ข้อมูลเข้าสู่ระบบสาธารณะ หรือการสร้าง Deepfake ที่มิได้เผยแพร่สู่สาธารณะ (พรเพชร วิชิตชลชัย, 2552)

3.1.4 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้การคุ้มครองในเชิงป้องกันการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ แต่เป็นกฎหมายว่าด้วยการคุ้มครองข้อมูล มิใช่กฎหมายอาญา ว่าด้วยการสะกดรอยตามโดยตรง โดยโทษอาญาตามมาตรา 79 ครอบคลุมเฉพาะกรณีผู้ควบคุมข้อมูลใช้หรือเปิดเผย ข้อมูลส่วนบุคคลที่อ่อนไหวตามมาตรา 26 โดยมีขอบ จึงไม่ครอบคลุมการเก็บข้อมูลโดยบุคคลธรรมดา เพื่อการสะกดรอยตาม โดยเฉพาะการใช้ Stalkerware เก็บข้อมูลและตำแหน่งของผู้เสียหาย

3.1.5 พระราชบัญญัติคุ้มครองผู้ถูกระทำด้วยความรุนแรงในครอบครัว พ.ศ. 2550

พระราชบัญญัติคุ้มครองผู้ถูกระทำด้วยความรุนแรงในครอบครัว พ.ศ. 2550 มีกลไกคำสั่งคุ้มครองชั่วคราว ที่ศาลออกได้ตามคำร้องของผู้เสียหายหรือพนักงานเจ้าหน้าที่ ซึ่งใกล้เคียงกับ Stalking Protection Order ของอังกฤษและเวลส์ในเชิงโครงสร้าง อย่างไรก็ตาม กฎหมายฉบับนี้ใช้บังคับเฉพาะกรณีความรุนแรงในครอบครัว ตามนิยามในมาตรา 3 ที่จำกัดเฉพาะบุคคลในครอบครัว จึงไม่ครอบคลุมผู้กระทำที่เป็นบุคคลภายนอก เช่น อดีตคู่รักหรือผู้กระทำในรูปแบบ Predatory Stalker ซึ่งเป็นกลุ่มผู้กระทำที่พบบ่อยในบริบทของการสะกดรอยตามทางไซเบอร์

3.1.6 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

ในการพิจารณามาตรการทางกฎหมายของประเทศไทย จำเป็นต้องคำนึงถึงรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ซึ่งมีบทบัญญัติที่เกี่ยวข้องสามมาตรา ได้แก่ มาตรา 32 บัญญัติคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว มาตรา 34 บัญญัติคุ้มครองเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน และการสื่อความหมายโดยวิธีอื่น และมาตรา 26 บัญญัติหลักความได้สัดส่วน (Proportionality Principle) ในการตรากฎหมายที่จำกัดสิทธิและเสรีภาพ

ศาลรัฐธรรมนูญไทยได้พัฒนาหลักความได้สัดส่วนตามมาตรา 26 เป็น Three-Stage Proportionality Test ประกอบด้วย การทดสอบความเหมาะสม (Suitability) ความจำเป็น (Necessity) และความได้สัดส่วนในความหมายแคบ (Proportionality stricto sensu) นอกจากนี้ คำวินิจฉัยศาลรัฐธรรมนูญ ที่ 20/2566 เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มาตรา 14 (1) เป็นบรรทัดฐานสำคัญที่ศาลรัฐธรรมนูญให้ความสำคัญกับหลักกฎหมายต้องชัดเจนแน่นอน (Lex Certa Principle) ซึ่งจะเป็นกรอบในการพิจารณาชอบด้วยรัฐธรรมนูญของร่างฐานความผิดสะกดรอยตามทางไซเบอร์ที่ผู้เขียนเสนอ

3.2 มาตรการทางกฎหมายของต่างประเทศ

ในส่วนของมาตรการทางกฎหมายของต่างประเทศ ในหลายประเทศได้บัญญัติมาตรการเฉพาะเพื่อรับมือกับการสะกดรอยตามและการสะกดรอยตามทางไซเบอร์อย่างเป็นรูปธรรม ทั้งในด้านการกำหนดความผิด การออกคำสั่งคุ้มครองผู้เสียหาย และการปรับกฎหมายให้สอดคล้องกับเทคโนโลยีสมัยใหม่ ผู้เขียนจึงมุ่งศึกษากฎหมายของสหรัฐอเมริกา อังกฤษและเวลส์ และญี่ปุ่น เพื่อเป็นแนวทางทางกฎหมายและนำมาวิเคราะห์เป็นข้อเสนอสำหรับประเทศไทยต่อไป

ต่อไปนี้จะผู้เขียนจะวิเคราะห์มาตรการทางกฎหมายของสามประเทศที่นำมาเปรียบเทียบ ได้แก่ สหรัฐอเมริกา อังกฤษและเวลส์ และญี่ปุ่น เพื่อแสดงให้เห็นพัฒนาการของฐานความผิดเฉพาะ กลไกคำสั่งคุ้มครองล่วงหน้า อัตรโทษ และมาตรฐานองค์ประกอบทางจิตใจที่เป็นต้นแบบสำคัญ สำหรับการปรับปรุงกฎหมายไทย

3.2.1 มาตรการทางกฎหมายของสหรัฐอเมริกา

สหรัฐอเมริกามีฐานความผิดเฉพาะตาม 18 U.S.C. § 2261A ภายใต้ Violence Against Women Act of 1994 (Pub.L. 103-322) ที่ครอบคลุมการใช้ระบบการสื่อสารทางอิเล็กทรอนิกส์ ผู้กระทำความผิดต้องมีเจตนาเฉพาะเจาะจง (Specific Intent) ที่จะฆ่า ทำร้าย คุกคาม ข่มขู่ หรือเฝ้าตรวจสอบผู้อื่น อัตรโทษกำหนดเป็นชั้น โดยโทษพื้นฐานจำคุกไม่เกินห้าปี เพิ่มเป็นจำคุกไม่เกินสิบปี ในกรณีที่ผู้เสียหายได้รับบาดเจ็บ

สาหัส และจำคุกตลอดชีวิตเฉพาะกรณีที่ผู้เสียหายเสียชีวิต อันเป็นผลจากการกระทำ ส่วนกฎหมายของรัฐแคลิฟอร์เนีย ตาม California Penal Code § 646.9 เป็นกฎหมายต่อต้านการสะกดรอยตาม (anti-stalking) ฉบับแรกของสหรัฐอเมริกาที่ตราขึ้นในปี ค.ศ. 1990 ซึ่งต่อมาได้รับการแก้ไขเพิ่มเติมหลายครั้งให้ครอบคลุมการสะกดรอยตามผ่านระบบอิเล็กทรอนิกส์ ทั้งนี้ คำพิพากษา *Counterman v. Colorado* (2023) ที่ศาลฎีกาวินิจฉัยว่าความผิดฐาน True Threats ต้องมีมาตรฐานความรับผิดชอบในระดับประมาทเลินเล่ออย่างร้ายแรง (Recklessness) เป็นบรรทัดฐานสำคัญ สำหรับการออกแบบกฎหมายไทยที่ต้องคำนึงถึงเสรีภาพในการแสดงออก

3.2.2 มาตรการทางกฎหมายของอังกฤษและเวลส์

Protection from Harassment Act 1997 ของอังกฤษและเวลส์ ได้รับการแก้ไขโดย Protection of Freedoms Act 2012 ให้เพิ่มฐานความผิดสะกดรอยตามในมาตรา 2A (โทษจำคุกตามตัวบทไม่เกิน 51 สัปดาห์ ในทางปฏิบัติของศาลแขวงไม่เกิน 6 เดือน) และมาตรา 4A (โทษสูงสุด 10 ปี โดย Policing and Crime Act 2017) จุดเด่นคือมาตรา 2A (3) ระบุพฤติการณ์ตัวอย่างไว้ชัดเจน รวมถึงการเฝ้าตรวจสอบการสื่อสารทางอิเล็กทรอนิกส์ (Crown Prosecution Service, 2025) นอกจากนี้ Stalking Protection Act 2019 ได้สร้างกลไก Stalking Protection Order (SPO) ที่ศาลแขวงสามารถออกได้ตามคำร้องของหัวหน้าตำรวจก่อนการดำเนินคดีอาญา และกำหนดข้อห้ามและข้อบังคับเชิงบวก ระยะเวลาขั้นต่ำสองปี การฝ่าฝืนมีโทษจำคุกสูงสุดห้าปี (Home Office, 2020; Home Office, 2024)

3.2.3 มาตรการทางกฎหมายของประเทศญี่ปุ่น

ประเทศญี่ปุ่นได้ตราพระราชบัญญัติควบคุมการสะกดรอยตาม (Stalker Regulation Act) ใน ค.ศ. 2000 ภายหลังเหตุการณ์ฆาตกรรมในเขตโอเควะ มาตรา 2 นิยาม tsukimatoi-tō ไว้แปดประการ โทษจำคุกไม่เกินหนึ่งปีหรือปรับไม่เกินหนึ่งล้านเยน ในปี ค.ศ. 2025 รัฐสภาญี่ปุ่น (Diet) ได้ตราพระราชบัญญัติแก้ไขเพิ่มเติม Stalker Regulation Act ซึ่งมีผลใช้บังคับในช่วงปลายปีเดียวกัน โดยขยายการกำกับดูแลให้

ครอบคลุมการใช้อุปกรณ์ Bluetooth Tag ในการติดตามตำแหน่งของผู้เสียหาย และให้อำนาจตำรวจในการออกคำเตือน (Keikoku) ได้แม้ไม่มีคำร้องจากผู้เสียหาย (Japan Times, 2025; National Police Agency of Japan, 2025) กลไกที่เป็นเอกลักษณ์คือ Keikoku-Kinshi-meirei (คำเตือน-คำสั่งห้าม) ของตำรวจตามมาตรา 4 และ 5 ที่เป็นการแทรกแซงก่อนยกระดับเป็นคดีอาญา ลดอัตราการลุกลามไปสู่ความรุนแรงทางกายภาพได้อย่างมีประสิทธิภาพ (National Police Agency of Japan, 2022)

4. บทวิเคราะห์เปรียบเทียบมาตรการทางกฎหมายเกี่ยวกับการสะกดรอยตามทางไซเบอร์

จากการศึกษาเปรียบเทียบกฎหมายของทั้งสองประเทศ ผู้เขียนขอเสนอผลการวิเคราะห์ตามกรอบ 4 ประเด็นหลัก ดังต่อไปนี้

4.1 การวิเคราะห์ตามกรอบ 4 ประเด็น: ประสิทธิภาพ บทบัญญัติเฉพาะ กลไกคุ้มครอง และอัตราโทษ

จากการศึกษาเปรียบเทียบกฎหมายของทั้งสองประเทศ ผู้เขียนพบว่าประเทศไทยล่าช้าในทุกมิติเทียบกับสหรัฐอเมริกา อังกฤษและเวลส์ และญี่ปุ่น ทั้งในด้านประสิทธิภาพในการบังคับใช้กฎหมาย ความมีบทบัญญัติเฉพาะ กลไกคำสั่งคุ้มครองล่วงหน้า และอัตราโทษที่ได้สัดส่วน สหรัฐอเมริกามีฐานความผิดเฉพาะตาม 18 U.S.C. § 2261A และมาตรฐาน Recklessness ตามคดี *Counterman v. Colorado* (2023) อังกฤษและเวลส์มี Stalking Protection Order (SPO) ออกได้โดยศาลแขวงตามคำร้องของหัวหน้าตำรวจก่อนการดำเนินคดีอาญา และญี่ปุ่นมีระบบ Keikoku-Kinshi-meirei ที่เป็นการแทรกแซงในขั้นก่อนการดำเนินคดี ในขณะที่ประเทศไทยต้องอาศัย การตีความบทบัญญัติทั่วไปในประมวลกฎหมายอาญา มาตรา 397, 392, 326-328 ที่มีได้ออกแบบเพื่อสะกดรอยตามโดยเฉพาะ อัตราโทษเพียงปรับไม่เกินห้าพันบาทตามมาตรา 397 วรรคหนึ่งไม่ได้สัดส่วนกับความรุนแรง และไม่มีกลไกคำสั่งคุ้มครองล่วงหน้าที่ครอบคลุมการสะกดรอยตามทางไซเบอร์ทั่วไป

เมื่อพิจารณาความเหมาะสมในการประยุกต์ใช้กับประเทศไทย ผู้วิจัยเห็นว่ารูปแบบของอังกฤษและเวลส์ มีความเหมาะสมที่สุดในการเป็นต้นแบบ เนื่องจากมีบทบัญญัติที่ระบุพฤติการณ์ตัวอย่างชัดเจน มี Stalking Protection Order ที่ออกแบบเพื่อการคุ้มครองโดยเฉพาะ และสามารถผสมผสานข้อห้ามและข้อบังคับ เชิงบวกได้ ทั้งนี้ การวางองค์ประกอบทางจิตใจของฐานความผิดใหม่ในระดับ รู้หรือควรจะได้รู้ ทั้งสอดคล้องกับ Recklessness Standard ของระบบ Common Law และเทียบเคียงได้กับเจตนาเล็งเห็นผลตามมาตรา 59 วรรคสองแห่งประมวลกฎหมายอาญา ซึ่งจะสร้างสมดุลระหว่างการคุ้มครองผู้เสียหายกับเสรีภาพในการแสดงออก ตามมาตรา 34 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

4.2 บทสรุปการเปรียบเทียบกฎหมายไทยและต่างประเทศ

จากการวิเคราะห์ข้างต้น ช่องว่างของกฎหมายไทย 3 ประการที่สำคัญ ได้แก่ การขาดฐานความผิดเฉพาะ การขาดกลไกคำสั่งคุ้มครองล่วงหน้า และอัตราโทษไม่ได้สัดส่วน นำไปสู่ข้อเสนอแนะที่จะกล่าวถึงในบทส่งท้าย เพื่อให้กฎหมายไทยสามารถคุ้มครองผู้เสียหายจากการสะกดรอยตามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

5. บทส่งท้าย

บทความวิชาการฉบับนี้สรุปได้ว่า มาตรการทางกฎหมายของประเทศไทยในปัจจุบันยังไม่สามารถคุ้มครองผู้เสียหายจากการสะกดรอยตามทางไซเบอร์ได้อย่างมีประสิทธิภาพ เนื่องจากขาดบทบัญญัติเฉพาะ ขาดกลไกคำสั่งคุ้มครองล่วงหน้า และอัตราโทษไม่เหมาะสมกับความรุนแรงของพฤติการณ์ การศึกษาเปรียบเทียบกับกฎหมายของสหรัฐอเมริกา อังกฤษและเวลส์ และญี่ปุ่น แสดงให้เห็นว่ารูปแบบของกฎหมายอังกฤษมีความเหมาะสมที่สุดในการเป็นต้นแบบ

ผู้เขียนจึงเสนอแนะ ดังต่อไปนี้

1. เพิ่มมาตรา 309/2 ในประมวลกฎหมายอาญา กำหนดความผิดฐานสะกดรอยตามทางไซเบอร์ โดยกำหนดองค์ประกอบในระดับ รู้หรือควรจะได้รู้ และกำหนดอัตราโทษเป็นสองชั้น คือ จำคุกไม่เกินสามปี ปรับไม่เกินหกหมื่นบาท สำหรับกรณีพื้นฐาน และจำคุกไม่เกินสิบปี ปรับไม่เกินสองแสนบาท สำหรับกรณีรุนแรง
2. เพิ่มมาตรา 309/3 ให้ศาลมีอำนาจออกคำสั่งคุ้มครองชั่วคราวตามแบบ Stalking Protection Order ของอังกฤษและเวลส์ และเริ่มต้นด้วยโครงการนำร่องในศาลแขวงเขตกรุงเทพมหานคร
3. แก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพิ่มมาตรา 16/1 ว่าด้วยการติดตั้ง Stalkerware และเพิ่มกระบวนการเร่งด่วนสำหรับการเก็บพยานหลักฐานทางอิเล็กทรอนิกส์
4. ในการวิจัยครั้งต่อไป ควรมีการศึกษาเชิงประจักษ์เกี่ยวกับสถิติคดีในประเทศไทย และศึกษาเปรียบเทียบเพิ่มเติมกับประเทศในภูมิภาคเอเชีย เช่น เกาหลีใต้ สิงคโปร์ และไต้หวัน

6. เอกสารอ้างอิง

- เกียรติขจร วัจนะสวัสดิ์. (2562). คำอธิบายกฎหมายอาญา ภาคทั่วไป (พิมพ์ครั้งที่ 11). พลสยามพรินติ้ง.
- คณิต ฒ นคร. (2562). กฎหมายอาญา ภาคทั่วไป (พิมพ์ครั้งที่ 6). วิญญชน.
- เจษฎา การันต์. (2566). *ปัญหากฎหมายเกี่ยวกับการกำหนดความผิดฐานสะกดรอยตามบุคคลอื่น (Stalking)* [สารนิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยรามคำแหง]. ฐานข้อมูลสารนิพนธ์ มหาวิทยาลัยรามคำแหง. http://www.lawgrad.ru.ac.th/AbstractsFile/6424013051/1727431923097f3b9511ae0f2dee64ce9f4800e73b_abstract.pdf

- ชญาณ์พิมพ์ บัวดิษฐ์เดชา. (2551). *ความรับผิดชอบทางอาญาของผู้คุกคามผู้อื่นโดยใช้อินเทอร์เน็ต*. [วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย]. Chula Digital Collections. <https://digiverse.chula.ac.th/Info/item/dc:22917>
- ชนิดา อร่ามพงษ์ และสุชาติ ธรรมาพิทักษ์กุล. (2557). การกำหนดความผิดและโทษอาชญาฐานคุกคามเฝ้าติดตามและข่มขู่ทางอินเทอร์เน็ต. *วารสารวิชาการมหาวิทยาลัยอีสต์เทิร์นเอเชีย ฉบับสังคมศาสตร์และมนุษยศาสตร์*, 4(2), 148-156.
- ทวีเกียรติ มินะกนิษฐ. (2565). คำอธิบายกฎหมายอาญา ภาคทั่วไป (พิมพ์ครั้งที่ 22). วิญญูชน.
- พรเพชร วิชิตชลชัย. (2552). *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*. สำนักอบรมศึกษากฎหมายแห่งนิติบัณฑิตยสภา.
- รักษิศา โพธิ์พิทักษ์กุล. (2550). *มาตรการทางกฎหมายเกี่ยวกับการคุกคามทางอินเทอร์เน็ต (Cyberstalking)* [วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยกรุงเทพ]. DSpace at Bangkok University. http://dspace.bu.ac.th/bitstream/123456789/886/1/raksita_ppp.pdf
- Beccaria, C. (1764). *On crimes and punishments (Dei delitti e delle pene)*. Livorno: Coltellini.
- Bentham, J. (1789). *An introduction to the principles of morals and legislation*. T. Payne and Son.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588-608.
- Crown Prosecution Service. (2025). *Stalking and harassment: Legal guidance*. <https://www.cps.gov.uk/prosecution-guidance/stalking-orharassment>

- Home Office. (2020). *Stalking protection orders: Statutory guidance for the police. home office*. <https://www.gov.uk/government/publications/stalking-protection-act-statutory-guidance-for-the-police>
- Home Office. (2024). *Stalking protection orders: Review of management information 2019-2024*. <https://www.gov.uk/government/publications/management-information-stalking-protection-orders>
- International Covenant on Civil and Political Rights (ICCPR). (1966, December 16). *United Nations Treaty Series*, 999, 171.
- Logan, T. K., & Walker, R. (2017). Stalking: A multidimensional framework for assessment and safety planning. *Trauma, Violence, & Abuse*, 18(2), 200-222.
- McEwan, T. E., Mullen, P. E., & Purcell, R. (2007). Identifying risk factors in stalking: A review of current research. *International Journal of Law and Psychiatry*, 30(1), 1-9.
- Mullen, P. E., Pathe, M., & Purcell, R. (2009). *Stalkers and their victims* (2nd ed.). Cambridge University Press.
- Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and Justice*, 42(1), 199-263.
- National Police Agency of Japan. (2022). *Outline of the Act on Regulation of Stalking Behaviours. National Police Agency of Japan*. <https://www.npa.go.jp/english/index.html>
- National Police Agency of Japan. (2025). *Notice on the 2025 amendment of the Stalker Regulation Act. National Police Agency of Japan*. <https://www.npa.go.jp/english/index.html>

- Japan Times. (2025, November 11). *Japan adopts bill banning tracker tag use for stalking*. <https://www.japantimes.co.jp/news/2025/11/11/japan/crime-legal/antistalking-law-location-information/>
- Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, 50(2), 216-238. <https://doi.org/10.1177/0022427811425539>
- Royakkers, L. M. M. (2000). The Dutch approach to stalking laws. *California Criminal Law Review*, 3(1), 1-35.
- Zweigert, K., & Kötz, H. (1998). *An introduction to comparative law* (T. Weir, Trans., 3rd ed.). Oxford University Press.