Issues in the Definition of Offenses under Section 14 (1), (2), and (3) of the Computer Crime Act B.E. 2550 (2007)

Apiradee Raktham
Dhurakij Pundit University
E-mail: tourlex_narak@hotmail.com
Jirawut Lipipun
Dhurakij Pundit University
E-mail: jirawut.lin@dpu.ac.th

Received	Reviewed	Revised	Accepted
07/08/2025	23/09/2025	04/12/2025	04/12/2025

Abstract

Background and Purpose: The Computer Crime Act B.E. 2550 (2007), particularly Section 14 paragraphs (1), (2), and (3), criminalizes the introduction of false or fake information into a computer system, as well as information affecting national security or related to terrorism. While the Act was enacted to prevent technological misuse, the wording of Section 14 remains ambiguous and lacks sufficient legal precision. Terms such as “false information” and “fake information” are undefined, and broad expressions like “causing public panic” or “harming national security” invite arbitrary interpretation and overbroad application. Such ambiguity undermines the rule of law, the principle of legal certainty, and the protection of fundamental rights.

Objective: This article seeks to examine the substantive scope of offenses under Section 14 (1), (2), and (3) of the Computer Crime Act B.E. 2550 (2007) and to propose legislative reforms that align Thai law with contemporary legal principles emphasizing proportionality, fairness, and clarity.

Methodology: The study adopts a documentary research method, drawing upon the Computer Crime Act B.E. 2550 (2007) and its amendments, relevant Constitutional Court judgments, legal commentaries, academic works, and comparative analyses with international legal standards. The findings are synthesized to develop policy and legislative recommendations for addressing the current ambiguities in the law.

Results: The research reveals that Thai criminal law retains characteristics of centralized interpretive authority and imposes uniform penalties without distinguishing between levels of harm or intent. This approach impedes the realization of justice within the criminal process and creates potential for misuse of Section 14 against individuals expressing political dissent.

Conclusion: It is recommended that Section 14, particularly subsections (1), (2), and (3), be amended to include precise definitions within Section 3 of the Computer Crime Act, differentiate penalties based on the gravity of the offense, and clarify the elements of intent and consequence. Such revisions would strengthen legal certainty, safeguard civil liberties, and promote more equitable and effective law enforcement.

Keyword: Legal Ambiguities; Computer Crime Act; The Stipulation of Criminal Liability under Section 14; Computer-Related Offenses.

ปัญหาขอบเขตการกำหนดความผิดตามมาตรา 14 (1) (2) (3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ.2550

อภิรดี รักษ์ธรรม
มหาวิทยาลัยธุรกิจบัณฑิตย์
อีเมล: tourlex_narak@hotmail.com
จิรวุฒิ ลิปิพันธ์
มหาวิทยาลัยธุรกิจบัณฑิตย์
อีเมล: jirawut.lin@dpu.ac.th

บทคัดย่อ

ภูมิหลังและวัตถุประสงค์: พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยเฉพาะมาตรา 14 วรรคหนึ่ง (1) (2) (3) ที่มีบทบัญญัติเกี่ยวกับการนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลอันเป็นเท็จ ข้อมูลปลอม หรือที่มีความเกี่ยวข้องกับความมั่นคงของรัฐและการก่อการร้าย แม้กฎหมายดังกล่าวมีเจตนารมณ์เพื่อป้องกันอันตรายจากการใช้เทคโนโลยีในทางที่ผิด แต่อย่างไรก็ตาม บทบัญญัติมาตรา 14 กลับมีถ้อยคำที่คลุมเครือและขาดความชัดเจนในทางกฎหมาย เช่น “ข้อมูลปลอม” หรือ “ข้อมูลอันเป็นเท็จ” ซึ่งไม่มีการนิยามไว้ในตัวบทกฎหมายอย่างชัดเจน การใช้ถ้อยคำที่เปิดกว้าง เช่น “ก่อให้เกิดความตื่นตระหนกแก่ประชาชน” หรือ “กระทบต่อความมั่นคงของประเทศ” ยังอาจนำไปสู่การตีความโดยพลการและขยายขอบเขตของความผิดเกินความจำเป็น ส่งผลกระทบต่อหลักนิติรัฐ หลักความมั่นคงแน่นอนทางกฎหมาย (Legal Certainty) และสิทธิขั้นพื้นฐานของประชาชน
วัตถุประสงค์: บทความนี้มีวัตถุประสงค์เพื่อวิเคราะห์ขอบเขตการกำหนดความผิดตามมาตรา 14 (1) (2) (3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และเสนอแนะแนวทางการปรับปรุงกฎหมายไทยให้สอดคล้องกับหลักกฎหมายสมัยใหม่ และเสนอแนะแนวทางแก้ไขปัญหาการตีความและการบังคับใช้กฎหมายเพื่อให้เกิดความชัดเจนและเป็นธรรม
ระเบียบวิธีการศึกษา: การศึกษาครั้งนี้ใช้วิธีการวิจัยเอกสาร ศึกษาจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติม คำอธิบายกฎหมาย คำพิพากษาศาลรัฐธรรมนูญ เอกสารงานวิจัย บทความวิชาการ ตลอดจนหลักการทางกฎหมายอาญาและเปรียบเทียบกับมาตรฐานสากล เพื่อจัดทำข้อเสนอแนะแนวทางแก้ไขปัญหา
ผลการศึกษา: ผลการศึกษาพบว่า กฎหมายไทยยังมีลักษณะรวมศูนย์อำนาจในการตีความและบังคับใช้โทษแบบเดียวกันกับความผิดทุกลักษณะ โดยไม่แยกแยะตามระดับความเสียหายหรือเจตนา ทำให้ไม่สามารถบรรลุเป้าหมายของความยุติธรรมในกระบวนการทางอาญาได้อย่างเต็มที่ อีกทั้งยังเปิดช่องให้เจ้าหน้าที่รัฐใช้บทบัญญัติเหล่านี้ในการดำเนินคดีต่อผู้ที่มีความเห็นต่างทางการเมือง

สรุปผล: ผลการวิจัยชี้ให้เห็นถึงความจำเป็นในการแก้ไขปรับปรุงมาตรา 14 โดยเฉพาะอนุมาตรา (1) (2) (3) ซึ่งควรเพิ่มนิยามศัพท์ให้ชัดเจนในมาตรา 3 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ควรแยกโทษตามลำดับความร้ายแรงของผลกระทบที่เกิดขึ้น และกำหนดโครงสร้างขององค์ประกอบความผิดให้ครอบคลุมถึงเจตนาและผลลัพธ์ของการแสดงเจตนาโดยชัดเจน เพื่อยกระดับคุณภาพในการบังคับใช้กฎหมายมีประสิทธิภาพในอนาคต

คำสำคัญ : ความคลุมเครือของกฎหมาย; พ.ร.บ.คอมพิวเตอร์; การกำหนดความผิดตามมาตรา 14; การกระทำความผิดทางคอมพิวเตอร์

บทนำ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ถูกตราขึ้นเพื่อรองรับการคุ้มครองความมั่นคงปลอดภัยของระบบและข้อมูลคอมพิวเตอร์ อย่างไรก็ดี การบังคับใช้มาตรา 14 (1) (2) และ (3) กลับก่อให้เกิดข้อถกเถียงเกี่ยวกับขอบเขตของการกำหนดความผิด โดยเฉพาะในกรณีที่การนำเข้าข้อมูลคอมพิวเตอร์มีลักษณะเกี่ยวข้องกับการสื่อสารและการแสดงความคิดเห็นในพื้นที่สาธารณะ (วนิดา แสงสารพันธ์, 2556)

ปัญหาสำคัญอยู่ที่การใช้ถ้อยคำซึ่งมีความเปิดกว้างต่อการตีความ เช่น “ข้อมูลคอมพิวเตอร์ปลอมหรือข้อมูลอันเป็นเท็จ” และ “น่าจะเกิดความเสียหาย” อันอาจส่งผลให้บทบัญญัติดังกล่าวถูกนำไปใช้กับพฤติการณ์ที่มีลักษณะเป็นเพียงการแสดงความคิดเห็นหรือการวิพากษ์วิจารณ์เชิงนโยบายมากกว่าการกระทำที่ก่อให้เกิดอันตรายในเชิงกฎหมายอาญา (วรเจตน์ ภาคีรัตน์, 2564)

บทความนี้มีวัตถุประสงค์เพื่อศึกษาขอบเขตการกำหนดความผิดตามมาตรา 14 (1) (2) และ (3) โดยวิเคราะห์องค์ประกอบความผิดและแนวทางการตีความของศาลไทยควบคู่กับการศึกษาเชิงเปรียบเทียบกฎหมายต่างประเทศ เพื่อนำไปสู่ข้อเสนอแนะเชิงโครงสร้างและเชิงการบังคับใช้ที่สอดคล้องกับหลักกฎหมายอาญามากยิ่งขึ้น

วัตถุประสงค์การศึกษา

บทความนี้มีวัตถุประสงค์เพื่อวิเคราะห์ขอบเขตการกำหนดความผิดตามมาตรา 14 (1) (2) (3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และเสนอแนะแนวทางการปรับปรุงกฎหมายไทยให้สอดคล้องกับหลักกฎหมายสมัยใหม่ และเสนอแนะแนวทางแก้ไขปัญหาการตีความและการบังคับใช้กฎหมายเพื่อให้เกิดความชัดเจนและเป็นธรรม

ขอบเขตการวิจัย

บทความนี้มุ่งเน้นการวิเคราะห์ ปัญหาขอบเขตการกำหนดความผิดเกี่ยวกับการนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ ตามมาตรา 14 (1) (2) (3) ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยมีขอบเขตดังนี้

1. ศึกษาขอบเขตการกำหนดความผิดตามมาตรา 14 (1) (2) (3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

2. ศึกษาองค์ประกอบความผิด และแนวทางการตีความของศาลไทยเกี่ยวกับมาตรา 14 (1) (2) (3) โดยศึกษาจากแนวคำพิพากษาของศาลตั้งแต่การประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จนถึงปัจจุบัน

3. ศึกษากฎหมายและแนวปฏิบัติในประเทศไทย โดยอาจเปรียบเทียบกับหลักกฎหมายของสหพันธ์สาธารณรัฐเยอรมนี สหรัฐอเมริกา และสาธารณรัฐสิงคโปร์ เพื่อเป็นแนวทางในการตีความ หรือการกำหนดนิยามและการบังคับใช้กฎหมายเพื่อให้เกิดประสิทธิภาพในการบังคับใช้และยังรักษาไว้ซึ่งเสรีภาพในการแสดงออกของบุคคล

การทบทวนวรรณกรรม

จากการทบทวนวรรณกรรมที่เกี่ยวข้อง สามารถแยกความแตกต่างระหว่างพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2560 ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มีโครงสร้างส่วนใหญ่เหมือนกับพระราชบัญญัติฯ ปี 2550 เพียงแต่มีการปรับปรุงตัวบทและเพิ่มเติมเนื้อหาในบางส่วน เพื่อให้เกิดความชัดเจนในการบังคับใช้ (เอกสารประกอบการพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับที่...) พ.ศ.. บรรจุระเบียบวาระการประชุมสภานิติบัญญัติแห่งชาติครั้งที่ 26/2559 วันพฤหัสบดีที่ 28 เมษายน 2559) โดยสามารถสรุปความแตกต่างได้ตามตารางดังต่อไปนี้

ตารางเปรียบเทียบความแตกต่างของพระราชบัญญัติฯปี 2550 กับปี 2560

หัวข้อ	พระราชบัญญัติฯ ปี 2550	พระราชบัญญัติฯ ปี2560
การหมิ่นประมาทออนไลน์	**มาตรา 14** (1) การนำเข้ามูลเท็จไม่ว่าทั้งหมดหรือบางส่วนที่ทำให้เกิดความเสียหายแก่ผู้อื่นต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ	**มาตรา 8** เพิ่มบทบัญญัติในมาตรา14 (1)เดิม ได้แก่ การนำเข้าข้อมูลเท็จไม่ว่าทั้งหมดหรือบางส่วน ที่ทำให้เกิดความเสียหายแก่ผู้อื่น อันมิใช่การกระทำความผิดฐานหมิ่น

		ประมาทตามประมวลกฎหมายอาญา ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ
การนำเข้าข้อมูลเท็จที่มีผลต่อความมั่นคงของประเทศ	**มาตรา 14 (2)** การนำเข้าข้อมูลเท็จที่น่าจะก่อให้เกิด - ความเสียหายต่อความมั่นคงของประเทศ - ความตื่นตระหนกแก่ประชาชน	**มาตรา 8** เพิ่มนิยามของมาตรา 14 (2) การนำเข้าข้อมูลเท็จที่น่าจะก่อให้เกิด - ความเสียหายต่อความมั่นคงปลอดภัยของประเทศ - ความปลอดภัยสาธารณะ - ความมั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ - ความตื่นตระหนกแก่ประชาชน

ปัญหาที่เกิดจากการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม พ.ศ. 2560 กฎหมายดังกล่าวเป็นกฎหมายที่มีจุดมุ่งหมายในการควบคุมและปราบปรามการกระทำผิดที่เกิดขึ้นในโลกที่เทคโนโลยีมีการเปลี่ยนแปลงเป็นอย่างมาก เช่น การเผยแพร่ข้อมูลเท็จ การโจรกรรมข้อมูล การละเมิดความมั่นคงของชาติ และการกระทำผิดเกี่ยวกับการใช้ระบบคอมพิวเตอร์

เครื่องมือการวิจัย

การศึกษาครั้งนี้ใช้วิธีการวิจัยเอกสาร ศึกษาจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติม คำอธิบายกฎหมาย คำพิพากษาศาลรัฐธรรมนูญ เอกสารงานวิจัย บทความวิชาการ ฐานข้อมูลสาธารณะ ตลอดจนหลักการทางกฎหมายอาญาและเปรียบเทียบกับมาตรฐานสากล เพื่อจัดทำข้อเสนอแนะแนวทางแก้ไขปัญหา

การเก็บรวบรวมข้อมูล

การศึกษาครั้งนี้มีวัตถุประสงค์เพื่อวิเคราะห์แนวโน้มการดำเนินคดีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยเฉพาะมาตรา 14 (1) (2) และ (3) ซึ่งเป็น

บทบัญญัติว่าด้วยความผิดที่เกี่ยวข้องกับ “เนื้อหาข้อมูลคอมพิวเตอร์” (content-related offences) เพื่อทำความเข้าใจลักษณะการบังคับใช้กฎหมายในทางปฏิบัติและผลกระทบต่อหลักนิติรัฐ รวมถึงเสรีภาพในการแสดงความคิดเห็นของประชาชน

1. แนวทางและขอบเขตของการเก็บข้อมูล

การเก็บข้อมูลอาศัยแนวทางการวิจัยเชิงคุณภาพควบคู่กับการวิเคราะห์เชิงปริมาณ โดยมุ่งรวบรวมข้อมูลจากคดีจริงที่มีการดำเนินการภายใต้มาตรา 14 (1) (2) และ (3) ในช่วงระหว่างปี พ.ศ. 2550–2554 ซึ่งเป็นระยะเริ่มต้นของการบังคับใช้กฎหมายดังกล่าว ทั้งนี้ การเลือกช่วงเวลาดังกล่าวมีเหตุผลสำคัญคือ เป็นช่วงเวลาที่สะท้อนแนวทางการตีความและการใช้บทบัญญัติมาตรา 14 ในทางปฏิบัติอย่างหลากหลาย ทั้งในคดีที่เกี่ยวข้องกับการหมิ่นประมาทออนไลน์ การเผยแพร่ข้อมูลเท็จ และคดีที่มีลักษณะกระทบต่อความมั่นคงของรัฐ

2. แหล่งข้อมูลและวิธีการรวบรวม

(1) จากการวิเคราะห์ในส่วนของคำพิพากษาและคำฟ้องคดีที่ปรากฏในฐานข้อมูลจากคำพิพากษาของศาล หรือฐานข้อมูลสาธารณะ เช่น ฐานข้อมูลคดีของโครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw) หรือรายงานของศูนย์ทนายความเพื่อสิทธิมนุษยชน (TLHR) โดยเฉพาะคดีที่ระบุข้อกล่าวหาภายใต้มาตรา 14 (1), 14 (2) หรือ 14 (3)

(2) จากการวิเคราะห์ในส่วนของเอกสาร รายงาน และงานวิจัยที่มีการเก็บข้อมูลเชิงสถิติและเชิงวิเคราะห์เกี่ยวกับการดำเนินคดีตามพระราชบัญญัติคอมพิวเตอร์ฯ อาทิเช่น รายงาน “Computer Crime?” ของ iLaw (2555) หรือ รายงานสถิติของสำนักงานจัดการข้อมูลและสถิติด้านกระบวนการยุติธรรม (OJA) ซึ่งแสดงแนวโน้มจำนวนคดีหมวด “ความผิดเกี่ยวกับคอมพิวเตอร์” รายปี เพื่อใช้เทียบแนวโน้มโดยรวมกับข้อมูลเชิงลึกจากรายงาน iLaw หรือรายงานของ Freedom House และ TLHR ที่ให้ข้อมูลเชิงคุณภาพเกี่ยวกับลักษณะคดีและแนวทางการตีความของศาลในคดีซึ่งมีลักษณะเป็นการจำกัดเสรีภาพในการแสดงความคิดเห็น

การวิเคราะห์ข้อมูล

จากการศึกษาคำพิพากษาศาลฎีกาและสถิติการดำเนินคดีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในช่วงปี พ.ศ. 2550–2554 พบว่า การบังคับใช้มาตรา 14 (1) (2) และ (3) มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะมาตรา 14 (1) ซึ่งถูกใช้มากที่สุดในคดีที่เกี่ยวกับการหมิ่นประมาทออนไลน์และการเผยแพร่ข้อมูลอันเป็นเท็จที่กระทบชื่อเสียงบุคคล (โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw), Computer Crime?, 2555)

ขณะที่มาตรา 14 (2) และ (3) ถูกนำมาใช้ในคดีที่เกี่ยวข้องกับ “ความมั่นคงของรัฐ” และ “ข้อมูลอันอาจก่อให้เกิดความตื่นตระหนกแก่ประชาชน” ซึ่งมักมีความเกี่ยวข้องกับการแสดงความ

คิดเห็นทางการเมือง ศาลฎีกามีแนวโน้มตีความองค์ประกอบของคำว่า “ข้อมูลเท็จ” และ “ความมั่นคง” อย่างจำกัดมากขึ้น เพื่อป้องกันไม่ให้เกิดการใช้กฎหมายเกินขอบเขต (คำพิพากษาฎีกาที่ 2148/2562 และคำพิพากษาฎีกา ที่ 5793/2567)

ดังนั้น การวิจัยนี้ต้องการชี้ให้เห็นความจำเป็นในการแก้ไขปรับปรุงมาตรา 14 โดยเฉพาะอนุมาตรา (1) (2) (3) ยังคงเป็นประเด็นสำคัญที่ควรได้รับการปรับปรุงให้ชัดเจนมากขึ้น ซึ่งควรเพิ่มนิยามศัพท์ให้ชัดเจนในมาตรา 3 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และควรแยกโทษตามลำดับความร้ายแรงของผลกระทบที่เกิดขึ้น และกำหนดโครงสร้างขององค์ประกอบความผิดให้ครอบคลุมถึงเจตนาและผลลัพธ์ของการแสดงเจตนาโดยชัดเจน เพื่อให้สอดคล้องกับหลักความได้สัดส่วน (proportionality) และการคุ้มครองสิทธิมนุษยชนตามรัฐธรรมนูญและกติการะหว่างประเทศ เพื่อให้การบังคับใช้กฎหมายมีประสิทธิภาพมากยิ่งขึ้น

ผลการวิจัย

จากการศึกษาสภาพปัญหา และผลกระทบด้านการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในแต่ละวัตถุประสงค์ ดังนี้

1. ปัญหาขอบเขตการกำหนดความผิดตามมาตรา 14 (1) (2) (3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ผลการศึกษาพบว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยเฉพาะมาตรา 14 (1) (2) และ (3) มีเจตนารมณ์ในการป้องกันการนำข้อมูลเท็จหรือข้อมูลปลอมเข้าสู่ระบบคอมพิวเตอร์ รวมถึงการคุ้มครองประโยชน์สาธารณะด้านความมั่นคง อย่างไรก็ดี บทบัญญัติดังกล่าวใช้ถ้อยคำที่มีลักษณะคลุมเครือและมิได้กำหนดนิยามไว้โดยชัดแจ้ง เช่น “ข้อมูลปลอม” หรือ “ข้อมูลอันเป็นเท็จ” ส่งผลให้การตีความและการบังคับใช้กฎหมายแตกต่างกันในทางปฏิบัติและเปิดพื้นที่ให้เกิดการใช้ดุลพินิจอย่างกว้างขวาง (วนิดา แสงสารพันธ์, 2556)

นอกจากนี้ ถ้อยคำในส่วนของ “ความมั่นคงของประเทศ” และ “ความตื่นตระหนกแก่ประชาชน” ตามมาตรา 14 (2) ยังขาดความแน่นอนในเชิงนิยาม ซึ่งอาจส่งผลกระทบต่อหลักความมั่นคงแน่นอนของกฎหมาย อันเป็นองค์ประกอบสำคัญของหลักนิติรัฐตามรัฐธรรมนูญแห่งราชอาณาจักรไทย (วรพจน์ วิศรุตพิชญ์, 2540) เนื่องจากประชาชนไม่อาจคาดหมายขอบเขตของความรับผิดทางอาญาได้อย่างชัดเจน

สำหรับมาตรา 14 (3) ซึ่งเชื่อมโยงการนำเข้าข้อมูลกับความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือการก่อการร้ายตามประมวลกฎหมายอาญา พบว่ามีปัญหาเชิงโครงสร้างด้านกระบวนการยุติธรรม กล่าวคือ บทบัญญัติมิได้ระบุเงื่อนไขที่ชัดเจนว่าการประเมินสถานะของข้อมูลดังกล่าวต้องอาศัยคำพิพากษาถึงที่สุดในความผิดมูลฐานก่อนหรือไม่ ส่งผลให้เกิดความไม่แน่นอนในการ

บังคับใช้กฎหมาย (คณาธิป ทองรวีวงศ์, 2567) นอกจากนี้ การตีความมาตรา 14 (1) (2) (3) อย่างกว้างขวางยังมีผลกระทบต่อ เสรีภาพในการแสดงความคิดเห็นของประชาชน ซึ่งเป็นสิทธิขั้นพื้นฐานตามรัฐธรรมนูญมาตรา 34 และตามข้อ 19 ของอนุสัญญาระหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) โดยพบว่าในหลายกรณีมีการนำมาตรา 14 มาใช้ดำเนินคดีต่อผู้ที่แสดงความคิดเห็นทางการเมืองหรือเผยแพร่ข้อมูลที่วิพากษ์วิจารณ์รัฐบาล แม้ว่าข้อมูลนั้นจะไม่เป็นเท็จในสาระสำคัญก็ตาม (International Commission of Jurists, 2021) สะท้อนถึงการใช้กฎหมายดังกล่าวเป็นเครื่องมือในการจำกัดสิทธิเสรีภาพมากกว่าการคุ้มครองความมั่นคงของรัฐ

ในภาพรวม ข้อค้นพบในส่วนนี้สะท้อนให้เห็นลักษณะของปัญหาเชิงโครงสร้างของบทบัญญัติมาตรา 14 ซึ่งเป็นพื้นฐานสำคัญต่อการพิจารณาแนวทางการตีความและการปรับใช้กฎหมายในทางปฏิบัติในลำดับถัดไป

2. วิเคราะห์องค์ประกอบความผิด และแนวทางการตีความของศาลไทยเกี่ยวกับมาตรา 14 (1) (2) และ (3) โดยศึกษาจากแนวคำพิพากษาของศาลตั้งแต่การประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จนถึงปัจจุบัน

ผลการศึกษาพบว่า มาตรา 14 (1) (2) และ (3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นบทบัญญัติหลักที่ใช้กำหนดความรับผิดจากการนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยแม้อนุมาตราแต่ละข้อจะมีองค์ประกอบความผิดเฉพาะแตกต่างกัน แต่ล้วนมีจุดร่วมสำคัญคือการประเมินลักษณะของข้อมูลและผลกระทบที่อาจเกิดขึ้นต่อบุคคลหรือสาธารณะ จากการศึกษาคำพิพากษาของศาลไทยตั้งแต่เริ่มใช้กฎหมายจนถึงปัจจุบัน พบแนวโน้มการตีความที่ให้น้ำหนักกับ “ความเป็นไปได้ของผลเสียหาย” มากกว่าการพิสูจน์ผลที่เกิดขึ้นจริง และมีการขยายความหมายขององค์ประกอบบางประการโดยเฉพาะคำว่า “ข้อมูลอันเป็นเท็จ” ในลักษณะกว้าง (Werle, 2005)

ในส่วนของมาตรา 14 (1) แนวคำพิพากษาของศาลมิได้จำกัดขอบเขตของคำว่า “ข้อมูลอันเป็นเท็จ” เฉพาะข้อมูลที่เป็นเท็จในสาระสำคัญทั้งหมด หากแต่ครอบคลุมถึงข้อมูลที่มีบางส่วนไม่ตรงต่อข้อเท็จจริงและอาจก่อให้เกิดความเข้าใจผิดแก่สาธารณะ (คำพิพากษาศาลฎีกาที่ 2534/2565) ขณะที่มาตรา 14 (2) ศาลได้พิจารณาผลกระทบในเชิงโครงสร้างของความเสียหายเป็นสำคัญ โดยถือว่าการกระทำที่มีลักษณะ *น่าจะ* กระทบต่อความมั่นคงของรัฐหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชนย่อมเพียงพอให้ความผิดสำเร็จแล้ว โดยไม่จำเป็นต้องปรากฏผลเสียหายที่เกิดขึ้นจริงในทุกกรณี (TLHR, 2565) จากแนวคำพิพากษาดังกล่าวจะเห็นว่า ศาลมักตีความ “ข้อมูลเท็จ” อย่างกว้างโดยไม่จำกัดเฉพาะข้อมูลเท็จที่เป็นสาระสำคัญเท่านั้น แต่รวมถึงข้อความหรือความคิดเห็นที่อาจก่อให้เกิดความเข้าใจผิดแก่สาธารณะแนวทางนี้จึงถูกวิพากษ์โดยนักวิชาการว่าอาจขัดต่อหลัก “nullum crimen sine

lege”ที่กำหนดให้การกระทำเป็นความผิดได้ต่อเมื่อมีกฎหมายบัญญัติไว้อย่างชัดเจน (Gerhard Werle, 2005,)

สำหรับมาตรา 14 (3) จากแนวคำพิพากษาปรากฏว่า ศาลให้น้ำหนักกับเจตนาและบทบาทของผู้เผยแพร่ข้อมูลเป็นหลัก โดยวินิจฉัยว่าการที่บุคคลมีอำนาจควบคุมหรือดูแลเนื้อหาที่มีลักษณะเชื่อมโยงกับความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือการก่อการร้ายตามประมวลกฎหมายอาญา ย่อมถือเป็นการ “นำข้อมูลเข้าสู่ระบบคอมพิวเตอร์” ได้ แม้ยังไม่ปรากฏผลในเชิงประจักษ์ แนวทางการตีความดังกล่าวสะท้อนข้อจำกัดเชิงโครงสร้างของบทบัญญัติในการกำหนดกฎเกณฑ์ทางกฎหมายที่มีความแน่นอนและเป็นเอกภาพ อันเป็นประเด็นที่มีนัยสำคัญต่อการประเมินความสอดคล้องของมาตรา 14 กับหลักความมั่นคงแน่นอนทางกฎหมายและหลักนิติรัฐ และอาจถูกใช้จำกัดเสรีภาพในการแสดงความคิดเห็นของประชาชน (วรเจตน์ ภาคีรัตน์, 2564; International Commission of Jurists, 2021)

3. แนวทางปรับปรุงกฎหมายและแนวปฏิบัติในประเทศไทย โดยอาจเปรียบเทียบกับหลักกฎหมายของสหพันธ์สาธารณรัฐเยอรมนี สหรัฐอเมริกา และสาธารณรัฐสิงคโปร์ เพื่อเป็นแนวทางในการตีความ หรือการกำหนดนิยามและการบังคับใช้กฎหมายเพื่อให้เกิดประสิทธิภาพในการบังคับใช้และยังรักษาไว้ซึ่งเสรีภาพในการแสดงออกของบุคคล สามารถแยกพิจารณาได้ดังนี้

การกำหนดความผิดตามมาตรา 14 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นประเด็นที่ได้รับความสนใจในเชิงทฤษฎีกฎหมายอาญา เนื่องจากบทบัญญัติดังกล่าวใช้ถ้อยคำที่มีลักษณะเปิดกว้างและมิได้กำหนดนิยามขององค์ประกอบความผิดไว้อย่างชัดเจน การศึกษาตามกรอบหลักนิติรัฐ หลักความชัดเจนแน่นอนของกฎหมาย ทฤษฎีองค์ประกอบความรับผิดทางอาญา และทฤษฎีความเหมาะสมในการกำหนดความผิด จึงมีความสำคัญต่อการทำความเข้าใจข้อจำกัดเชิงโครงสร้างของบทบัญญัติดังกล่าวสามารถแยกพิจารณาได้ดังนี้

3.1 หลักนิติรัฐและหลักความชัดเจนแน่นอนของกฎหมาย

หลักนิติรัฐกำหนดให้กฎหมายอาญาต้องมีความชัดเจน แน่นอน และสามารถคาดหมายผลทางกฎหมายได้ล่วงหน้า เพื่อให้ประชาชนทราบขอบเขตของการกระทำที่อาจก่อให้เกิดความรับผิด (คณิต ณ นคร, 2560) อย่างไรก็ดี มาตรา 14 (1)–(3) ใช้ถ้อยคำสำคัญ เช่น “ข้อมูลเท็จ” “ข้อมูลปลอม” “น่าจะเกิดความเสียหาย” และ “ความมั่นคงของรัฐ” โดยมิได้กำหนดนิยามหรือเกณฑ์การตีความไว้ในตัวบท ส่งผลให้เกิดความไม่แน่นอนในการบังคับใช้กฎหมายและเปิดโอกาสให้เกิดการตีความที่แตกต่างกันในทางปฏิบัติ (วนิดา แสงสารพันธ์, 2556)

3.2 ทฤษฎีองค์ประกอบความรับผิดทางอาญา (Elements Theory)

ตามแนวคิดของ Andrew Ashworth โครงสร้างความรับผิดทางอาญาต้องประกอบด้วยการกระทำ เจตนา ความสัมพันธ์เชิงเหตุและผล และผลเสียหายที่พิสูจน์ได้จริง (Ashworth, 2013) อย่างไร

ก็ดี การกำหนดองค์ประกอบความผิดตามมาตรา 14 โดยใช้เกณฑ์ “น่าจะเกิดความเสียหาย” แสดงถึงการลงโทษโดยไม่ต้องพิสูจน์ผลเสียหายที่เกิดขึ้นจริง ซึ่งไม่สอดคล้องกับกรอบแนวคิดเรื่องความรับผิดทางอาญาที่อาศัยความเสียหายเชิงประจักษ์เป็นฐาน (อภิรัตน์ เพ็ชรศิริ, 2562)

3.3 ทฤษฎีความเหมาะสมในการกำหนดความผิดและหลักความได้สัดส่วน

Douglas Husak เสนอว่าการกำหนดความผิดอาญาควรอยู่ภายใต้หลัก minimal criminalization และต้องมีผลเสียหายที่ตรวจสอบได้จริงรองรับ เพื่อหลีกเลี่ยงปัญหา overcriminalization (Husak, 2008) เมื่อพิจารณามาตรา 14 พบว่าการกำหนดความผิดโดยอาศัยความเสียหายเชิงคาดการณ์หรือความตื่นตระหนกของประชาชน ยังไม่สอดคล้องกับหลักการดังกล่าว อีกทั้งการกำหนดโทษที่มีระดับใกล้เคียงกันในอนุมาตราที่มีความร้ายแรงแตกต่างกัน ยังสะท้อนปัญหาในเชิงสัดส่วนของโทษที่บังคับใช้ (ภรณี ตัณฑชุณห์, 2557)

3.4 การประเมินองค์ประกอบมาตรา 14 (1) (2) และ (3) ตามกรอบทฤษฎีสากล

เมื่อวิเคราะห์องค์ประกอบความผิดของมาตรา 14 ทั้งสามอนุมาตราตามกรอบของ Ashworth และ Husak พบว่า มาตรา 14 (1) และ (2) กำหนดความรับผิดโดยไม่ต้องพิสูจน์ผลเสียหายที่เกิดขึ้นจริง และอาศัยผลกระทบเชิงสมมุติฐานเป็นฐานในการลงโทษ ขณะที่มาตรา 14 (3) ซึ่งเกี่ยวข้องกับความมั่นคงของรัฐ มิได้กำหนดเกณฑ์การพิสูจน์ระดับความร้ายแรงของผลกระทบไว้อย่างชัดเจน ส่งผลให้ขอบเขตความรับผิดขึ้นอยู่กับดุลพินิจในการตีความเป็นสำคัญ ซึ่งก่อให้เกิดข้อจำกัดในเชิงความแน่นอนของกฎหมาย

3.5 หลักการคุ้มครองสิทธิและเสรีภาพในการแสดงความคิดเห็นในบริบทกฎหมายคอมพิวเตอร์

ภายใต้หลักนิติรัฐ การจำกัดสิทธิและเสรีภาพต้องไม่กระทบต่อสาระสำคัญของสิทธิ และต้องเป็นไปตามหลักความได้สัดส่วน (รัฐธรรมนูญแห่งราชอาณาจักรไทย, 2560, มาตรา 26) เสรีภาพในการแสดงความคิดเห็นซึ่งได้รับการคุ้มครองตาม ICCPR มาตรา 19 อนุญาตให้จำกัดสิทธิได้เฉพาะเท่าที่จำเป็นและได้สัดส่วน (ICCPR, 1966) และในทัศนะของ Eric Barendt เสรีภาพในการแสดงออกเป็นกลไกที่รองรับการวิพากษ์วิจารณ์รัฐและเป็นรากฐานของระบบประชาธิปไตย ด้วยเหตุนี้การจำกัดต้องทำด้วยความเคร่งครัดและไม่เกินความจำเป็น (Eric Barendt , 2005, หน้า 14) การที่มาตรา 14 ใช้ถ้อยคำที่เปิดช่องให้ตีความกว้างจึงมีความเสี่ยงอย่างมากต่อการบังคับใช้ที่ไม่สอดคล้องกับหลักสากล เช่น การเอาผิดจาก “ความตื่นตระหนก” แม้ยังไม่ปรากฏอันตรายจริง ซึ่งเข้าข่ายการใช้มาตรการทางอาญาโดยไม่อาศัยความเสียหายที่สามารถพิสูจน์ได้

นักวิชาการด้านสิทธิมนุษยชนและองค์กรระหว่างประเทศได้ชี้ให้เห็นว่า การใช้บทบัญญัติที่มีถ้อยคำกว้างในกฎหมายคอมพิวเตอร์อาจนำไปสู่การจำกัดเสรีภาพเกินความจำเป็น โดยเฉพาะในกรณีที่การแสดงออกมิได้ก่อให้เกิดอันตรายที่พิสูจน์ได้จริง (Barendt, 2005; International Commission of

Jurists, 2021) ปัญหาดังกล่าวสะท้อนให้เห็นถึงความท้าทายในการกำหนดและบังคับใช้บทบัญญัติมาตรา 14 ให้สอดคล้องกับหลักกฎหมายอาญาสมัยใหม่ หลักนิติรัฐ และมาตรฐานสิทธิมนุษยชนสากล

ดังนั้น การบังคับใช้กฎหมายคอมพิวเตอร์ที่กระทบต่อสิทธิเสรีภาพต้องยึดหลักการตีความบทบัญญัติที่มีโทษทางอาญาอย่างเคร่งครัด โดยจำเป็นต้องแสดงให้เห็นอันตรายหรือความเสียหายที่พิสูจน์ได้จริง มิใช่ตีความโดยอาศัยความกลัวหรือผลเชิงสมมุติฐาน การรักษาสมดุลระหว่างความมั่นคงของรัฐและสิทธิของประชาชนจึงเป็นเงื่อนไขสำคัญในการทำให้มาตรา 14 ไม่ขัดต่อหลักนิติรัฐ หลักสิทธิมนุษยชนสากล และหลักการลงโทษที่ได้สัดส่วนของโทษอาญา

3.6 เปรียบเทียบกับหลักกฎหมายของสหพันธ์สาธารณรัฐเยอรมนี สหรัฐอเมริกา และสาธารณรัฐสิงคโปร์

มาตรา 14 วรรคหนึ่ง (1) (2) (3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ใช้การ “นำข้อมูลเข้าสู่ระบบคอมพิวเตอร์” เป็นหลักในการพิจารณาของการเอาผิด โดยอาศัยลักษณะของเนื้อหาข้อมูล เช่น “ข้อมูลคอมพิวเตอร์ปลอม” “ข้อมูลคอมพิวเตอร์อันเป็นเท็จ” หรือข้อมูลที่เกี่ยวกับความมั่นคงแห่งราชอาณาจักรและการก่อการร้ายเป็นตัวกำหนดขอบเขตความผิด (คณาธิป ทองรวีวงศ์, 2567, หน้า 120)

อย่างไรก็ดี ถ้อยคำสำคัญจำนวนมากกลับไม่มีนิยามในมาตรา 3 เช่น “ข้อมูลคอมพิวเตอร์ปลอม” “ข้อมูลคอมพิวเตอร์อันเป็นเท็จ” “ความมั่นคงปลอดภัยของประเทศ” หรือ “ความตื่นตระหนกแก่ประชาชน” ส่งผลให้การตีความต้องอาศัยดุลพินิจอย่างกว้างขวาง และทำให้ประชาชนไม่สามารถคาดหมายได้อย่างแน่นอนว่าพฤติการณ์ใดจะถูกนับเป็นความผิดอาญา อันเป็นปัญหาต่อหลักความมั่นคงแน่นอนทางกฎหมายและหลักนิติรัฐ (วรเจตน์ ภาคีรัตน์, 2564, หน้า 312–322; วรพจน์ วิศรุตพิชญ์, 2540, หน้า 1) ยิ่งไปกว่านั้น มาตรา 14 (3) ยังมีการโยงไปยังความผิดเกี่ยวกับความมั่นคงและการก่อการร้ายในประมวลกฎหมายอาญาโดยตรง โดยไม่กำหนดเงื่อนไขว่าต้องมีคำพิพากษาถึงที่สุดหรือไม่ จึงทำให้ผู้ถูกกล่าวหาสามารถถูกดำเนินคดีในฐานะเกี่ยวข้องกับความมั่นคงได้ตั้งแต่ระดับ “ข้อมูล” ที่อาจยังไม่ผ่านการวินิจฉัยเนื้อหาความผิดตามประมวลกฎหมายอาญา (คณิต ณ นคร, 2560, หน้า 65–69) ซึ่งกระทบหลักสันนิษฐานไว้ก่อนว่าบริสุทธิ์และหลักการไม่กำหนดโทษโดยไม่มีความแน่นอนของกฎหมาย (Gerhard Werle, 2005, หน้า 35)

เมื่อเทียบกับหลักทฤษฎีกฎหมายอาญาที่เน้นให้มีการกำหนดความผิดอย่างชัดเจน ทั้งในด้านการกระทำ เจตนา และผลกระทบที่พิสูจน์ได้ (อภิรัตน์ เพ็ชรศิริ, 2562, หน้า 83–90) จะเห็นชัดว่ามาตรา 14 (1) (2) (3) มีปัญหาเชิงโครงสร้าง ที่สมควรนำมาเปรียบเทียบกับกฎหมายต่างประเทศเพื่อปรับปรุงให้สอดคล้องกับมาตรฐานสากลมากขึ้น

3.6.1 การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของสหพันธ์สาธารณรัฐเยอรมนี

3.6.1.1 การแยกฐานความผิดตามผลประโยชน์ที่คุ้มครอง

ประมวลกฎหมายอาญา (Strafgesetzbuch: StGB) ของเยอรมนีแยกความผิดตาม “ผลประโยชน์ที่กฎหมายคุ้มครอง” อย่างชัดเจน ไม่ใช้กฎหมายบทเดียวครอบคลุมความรับผิดทั้งทางทรัพย์สิน ระบบข้อมูล ความมั่นคง และความสงบเรียบร้อยทางการเมืองเหมือนมาตรา 14 (1) (2) (3) ของไทย (Gerhard Werle, 2005, หน้า 35)

ตัวอย่างเช่น มาตรา 263a StGB ว่าด้วย “Computer Fraud” กำหนดความผิดจากการใช้ หรือแทรกแซงระบบประมวลผลข้อมูลโดยมิชอบ เพื่อให้ได้มาซึ่งประโยชน์ทางทรัพย์สิน โดยต้องมี (1) การกระทำต่อระบบคอมพิวเตอร์ (2) เจตนาทุจริต (3) ความเสียหายต่อทรัพย์สินของผู้อื่น มาตรา 263a จึงกำหนดเงื่อนไขของความรับผิดกับ “การใช้ระบบเป็นเครื่องมือฉ้อโกง” และ “ผลกระทบทางทรัพย์สิน” ไม่ใช่เพียงความเป็นเท็จของข้อมูลในเชิงนามธรรมเท่านั้น (Ashworth, 2013, หน้า 80–83)

ส่วนมาตรา 267 StGB ว่าด้วยการปลอมแปลงเอกสาร ขยายความคุ้มครองไปถึงเอกสารอิเล็กทรอนิกส์ โดยพิจารณาว่าข้อมูลนั้นมีสถานะเป็น “หลักฐานทางกฎหมาย” หรือไม่ การปลอมเอกสารดิจิทัลจึงถูกพิจารณาจากคำว่า “เอกสาร” ที่มีนิติฐานะที่ชัดเจนไม่ใช่ข้อมูลทุกประเภทในระบบคอมพิวเตอร์จะเป็นเอกสารที่ที่ต้องรับผิดทางกฎหมาย (Gerhard Werle, 2005, หน้า 35) ต่างจากกฎหมายคอมพิวเตอร์ของไทยที่ใช้คำว่า “ข้อมูลคอมพิวเตอร์อันเป็นเท็จ” ครอบคลุมข้อมูลทุกชนิดและอาจเป็นความผิดได้

3.6.1.2 ความผิดเกี่ยวกับระบบคอมพิวเตอร์และโครงสร้างพื้นฐาน

มาตรา 303b StGB กำหนดความผิดฐาน “Computer Sabotage” โดยเน้นการคุ้มครองความปลอดภัยของระบบและโครงสร้างพื้นฐานของรัฐหรือเอกชน เช่น การทำให้ระบบหยุดชะงัก การทำลายข้อมูล หรือการขัดขวางการทำงานของระบบที่สำคัญต่อเศรษฐกิจหรือความมั่นคงของประเทศ (คณาธิป ทองรวีวงศ์, 2567, หน้า 120)

โครงสร้างของมาตรา 303b StGB แยกระดับความร้ายแรงตามผลกระทบที่เกิดขึ้น เช่น กรณีกระทบต่อระบบทั่วไปจะมีโทษเบากว่ากรณีกระทบต่อโครงสร้างพื้นฐานสำคัญ ซึ่งอาจกำหนดโทษจำคุกสูงตั้งแต่ 3 ปี ไปจนถึงจำคุกถึง 10 ปี การจัดโครงสร้างเช่นนี้สะท้อนการใช้หลักความได้สัดส่วนของโทษอย่างจริงจัง ต่างจากมาตรา 14 ของไทยที่กำหนดโทษใกล้เคียงกันแม้พฤติการณ์และผลกระทบจะต่างกันมาก (เกียรติขจร วัจนะสวัสดิ์, 2562, หน้า 2)

3.6.1.3 ความสงบเรียบร้อยกับเสรีภาพการแสดงความคิดเห็น

กรณีการแสดงออกของประชาชนในหลาย มาตรา 130 StGB ว่าด้วย “Incitement to Hatred” กำหนดความผิดเฉพาะกรณีที่ข้อความหรือการสื่อสารมีลักษณะเป็นการยุยงให้เกิดความเกลียดชังหรือความรุนแรงต่อกลุ่มบุคคล เช่น กลุ่มชาติพันธุ์หรือศาสนา และมีผลจริงต่อความสงบ

เรียบร้อยของสังคม ไม่ได้เอาผิดข้อมูลเท็จหรือความคิดเห็นทุกประเภท (Gerhard Werle, 2005, หน้า 35)

ขณะเดียวกัน Basic Law มาตรา 5 รับรองเสรีภาพในการแสดงความคิดเห็น การรับข้อมูลข่าวสาร และเสรีภาพของสื่อ โดยกำหนดให้การจำกัดสิทธิทำได้เฉพาะตามกฎหมายทั่วไปที่เคารพสิทธิและศักดิ์ศรีของผู้อื่น (วรพจน์ วิศรุตพิชญ์, 2540, หน้า 1) เมื่อเทียบกับกฎหมายไทยจะเห็นว่า เยอรมนีวางฐานตามรัฐธรรมนูญรองรับเสรีภาพไว้ก่อน แล้วจึงใช้บทกฎหมายอาญาเฉพาะกรณีที่มีอันตรายต่อประโยชน์สาธารณะอย่างแท้จริงที่จะต้องรับผิดทางกฎหมาย

3.6.2 การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของสหรัฐอเมริกา

3.6.2.1 Computer Fraud and Abuse Act (CFAA)

ในสหรัฐอเมริกา กฎหมายหลักด้านอาชญากรรมทางคอมพิวเตอร์คือ Computer Fraud and Abuse Act (CFAA) บัญญัติไว้ที่ 18 U.S.C. § 1030 โดยมีหลักในการพิจารณาการกระทำความผิดจากการเข้าถึงระบบคอมพิวเตอร์ที่ได้รับการคุ้มครองโดยไม่ได้รับอนุญาต หรือการใช้สิทธิการเข้าถึงเกินขอบเขตที่ได้รับอนุญาต รวมทั้งการก่อให้เกิด “ความเสียหาย” ต่อระบบ หรือข้อมูล เช่น การล่มของระบบ หรือความเสียหายเชิงเศรษฐกิจ (International Commission of Jurists, 2021, หน้า 14–15)

CFAA จึงมุ่งเน้น “พฤติการณ์การเข้าถึงและการใช้ระบบ” มากกว่าการควบคุมตัวเนื้อหาของข้อมูล การกระทำจะเป็นความผิดก็ต่อเมื่อมีผลกระทบที่พิสูจน์ได้ ไม่ใช่เพียงการโพสต์ข้อมูลที่รัฐเห็นว่าไม่ถูกต้องหรือเป็นเท็จ (Herbert L. Packer, 1968, pp. 296–300) แนวคิดนี้สอดคล้องกับหลักการที่ว่า กฎหมายอาญาควรเป็นมาตรการสุดท้าย (ultima ratio) และไม่ควรถูกใช้กับการแสดงออกทั่วไปที่ไม่ก่อให้เกิดอันตรายที่แท้จริงต่อสังคม

3.6.2.2 First Amendment กับการจำกัดบทลงโทษทางอาญา

สหรัฐอเมริกายังมีกรอบของกฎหมายรัฐธรรมนูญที่เข้มข้นทาง First Amendment ซึ่งให้การคุ้มครองเสรีภาพในการพูด การพิมพ์ และการชุมนุม โดยเฉพาะอย่างยิ่งความเห็นทางการเมืองหรือประเด็นสาธารณะ ศาลจะใช้มาตรฐานที่เข้มงวดในการพิจารณากฎหมายที่จำกัดการแสดงความคิดเห็น หากรัฐไม่อาจพิสูจน์ความจำเป็นและความได้สัดส่วนของการลงโทษได้ กฎหมายนั้นจะถูกวินิจฉัยว่าขัดต่อกฎหมายรัฐธรรมนูญ (International Commission of Jurists, 2021, หน้า 14–15) ในทางปฏิบัติ ปัญหาข้อมูลเท็จหรือข้อมูลที่บิดเบือนมักถูกพิจารณาด้วยกฎหมายเฉพาะเรื่อง เช่น กฎหมายหมิ่นประมาท กฎหมายเลือกตั้ง หรือกฎหมายโฆษณาเท็จ มากกว่าที่จะใช้กฎหมายคอมพิวเตอร์เป็นฐานเอาผิดต่อ “ข้อมูลเท็จ” โดยตรง ซึ่งแตกต่างจากกฎหมายคอมพิวเตอร์มาตรา 14 ของไทยซึ่งเปิดช่องให้การแสดงออกบนสื่อสังคมถูกนำมาฟ้องในฐานะ “การนำข้อมูลเท็จเข้าสู่ระบบคอมพิวเตอร์” ได้โดยง่าย (วนิดา แสงสารพันธ์, 2556, หน้า 25–27)

3.6.3 การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของสาธารณรัฐสิงคโปร์

3.6.3.1 การแยกกฎหมายคอมพิวเตอร์กับกฎหมายข้อมูลเท็จ

สาธารณรัฐสิงคโปร์มีทั้งกฎหมายเกี่ยวกับการโจมตีระบบและการเข้าถึงโดยมิชอบ เช่น Computer Misuse Act และกฎหมายเฉพาะสำหรับการควบคุม “ข้อมูลเท็จทางออนไลน์” คือ Protection from Online Falsehoods and Manipulation Act 2019 (POFMA) ซึ่งเป็นตัวอย่างสำคัญของการแยกฐานความผิดตามลักษณะผลประโยชน์ที่คุ้มครอง (คณาธิป ทองรวีวงศ์, 2567, หน้า 120)

ภายใต้กฎหมาย (POFMA) มาตรา 2 ให้นิยาม ให้นิยาม “statement of fact” ไม่รวมถึงความคิดเห็น จึงไม่เข้าข่ายเป็น “false statement of fact” ที่ถูกลงโทษหรือสั่งแก้ไขภายใต้กฎหมายนี้ เว้นแต่จะเป็นความเห็นที่แฝงข้อเท็จจริงอันเป็นเท็จที่พิสูจน์ได้ว่าก่อให้เกิดอันตรายตามมาตรา 4 (Protection from Online Falsehoods and Manipulation Act, 2019, s. 2–4) แนวทางนี้ทำให้กฎหมายสามารถจัดการกับ “ข้อมูลเท็จที่มีอันตราย” โดยไม่กระทบกระเทือนต่อเสรีภาพของ “การแสดงความคิดเห็นโดยสุจริต” ทั้งหมดนี้ต่างจากมาตรา 14 ของไทยที่ไม่ได้แยกความเห็นกับข้อเท็จจริงไว้อย่างชัดเจน (วนิดา แสงสารพันธ์, 2556, หน้า 25–27)

3.6.3.2 ลำดับมาตรการการลงโทษทางอาญา

ภายใต้กฎหมาย (POFMA) ยังออกแบบมาเพื่อให้รัฐใช้มาตรการขั้นเบา เช่น คำสั่งให้เผยแพร่ข้อความแก้ไข (correction notice) หรือคำสั่งให้ลบข้อมูลเป็นอันดับแรกก่อนเข้าสู่การลงโทษทางอาญาในกรณีที่มีความร้ายแรงหรือมีการฝ่าฝืนคำสั่ง (Protection from Online Falsehoods and Manipulation Act, 2019, s. 11–17) การวางลำดับมาตรการเช่นนี้สะท้อนหลักการจำกัดการใช้โทษทางอาญาไว้เป็นทางเลือกสุดท้ายเพื่อป้องกันการล่วงล้ำสิทธิเสรีภาพเกินความจำเป็น (Douglas Husak, 2008, หน้า 121)

ในทางเปรียบเทียบ มาตรา 14 (1) (2) (3) ของไทยไม่มีมาตรการการตรวจสอบเป็นขั้นเป็นตอนจากขั้นตอนระดับเบาไปหาหนัก หากเห็นว่าข้อมูลเป็นเท็จหรือข้อมูลปลอมหรือเห็นว่าน่าจะเป็นภัย ก็สามารถนำไปสู่การดำเนินคดีอาญาได้ทันที จึงมีความเสี่ยงสูงที่อาจกระทบต่อเสรีภาพการแสดงความคิดเห็นและสิทธิในการรับรู้ข้อมูลข่าวสารของประชาชน (International Commission of Jurists, 2021, หน้า 14–15)

สรุปผลการวิจัย

1. การศึกษาขอบเขตการกำหนดความผิดตามมาตรา 14 (1) (2) และ (3)

ผลการศึกษาพบว่า มาตรา 14 (1) (2) และ (3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 กำหนดความผิดโดยใช้ถ้อยคำที่มีความเปิดกว้าง เช่น “ข้อมูลคอมพิวเตอร์

อันเป็นเท็จ” “ข้อมูลคอมพิวเตอร์ปลอม” และ “น่าจะเกิดความเสียหาย” โดยมิได้กำหนดนิยามหรือเกณฑ์การตีความไว้อย่างเป็นระบบ ส่งผลให้ขอบเขตของความผิดต้องอาศัยการตีความในทางปฏิบัติเป็นสำคัญ ลักษณะดังกล่าวทำให้บทบัญญัติมีความยืดหยุ่นในการบังคับใช้สูง และเกี่ยวข้องโดยตรงกับความสามารถในการคาดหมายผลทางกฎหมายของบุคคลภายใต้หลักความมั่นคงแน่นอนของกฎหมายในระบบนิติรัฐ (วนิดา แสงสารพันธ์, 2556; วรเจตน์ ภาคีรัตน์, 2564) ทั้งนี้ ข้อค้นพบในส่วนนี้เป็นฐานข้อมูลสำคัญสำหรับการพิจารณาแนวทางในการกำหนดขอบเขตและนิยามขององค์ประกอบความผิดให้มีความชัดเจนยิ่งขึ้นในทางกฎหมาย

2. การศึกษาองค์ประกอบความผิดและแนวทางการตีความของศาลไทย

จากการศึกษาคำพิพากษาของศาลไทยพบว่า แนวทางการตีความมาตรา 14 (1) (2) และ (3) มีจุดร่วมคือการให้น้ำหนักกับองค์ประกอบ “การนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์” เป็นฐานของความรับผิด ขณะที่องค์ประกอบเกี่ยวกับลักษณะของข้อมูลและผลแห่งการกระทำถูกพิจารณาโดยการให้ใช้ดุลพินิจตามข้อเท็จจริงของแต่ละคดี โดยในมาตรา 14 (1) ศาลตีความคำว่า “ข้อมูลอันเป็นเท็จ” ครอบคลุมถึงข้อมูลที่อาจก่อให้เกิดความเข้าใจคลาดเคลื่อนแก่สาธารณชน ส่วนมาตรา 14 (2) และ (3) ศาลให้ความสำคัญกับพฤติการณ์ที่ “น่าจะ” ก่อให้เกิดผลกระทบต่อประโยชน์ที่กฎหมายมุ่งคุ้มครอง แม้ยังไม่ปรากฏผลเสียหายที่เกิดขึ้นจริง แนวทางดังกล่าวสะท้อนรูปแบบการกำหนดความรับผิดที่เน้นการประเมินความเสี่ยงของผลกระทบมากกว่าผลลัพธ์ที่เกิดขึ้นแล้ว ซึ่งเป็นข้อมูลสำคัญต่อการพิจารณาความเหมาะสมขององค์ประกอบความผิดและเกณฑ์การตีความในลำดับถัดไป (วรเจตน์ ภาคีรัตน์, 2564)

3. การศึกษากฎหมายและแนวปฏิบัติเปรียบเทียบกับกฎหมายต่างประเทศ

ผลการศึกษาเชิงเปรียบเทียบกับกฎหมายของสหพันธ์สาธารณรัฐเยอรมนี สหรัฐอเมริกา และสาธารณรัฐสิงคโปร์ พบว่า ระบบกฎหมายดังกล่าวมีการจัดโครงสร้างความผิดเกี่ยวกับคอมพิวเตอร์โดยแยกฐานความผิดตามผลประโยชน์ที่กฎหมายมุ่งคุ้มครองอย่างชัดเจน และให้ความสำคัญกับการกำหนดองค์ประกอบความผิดและระดับโทษให้สอดคล้องกับลักษณะและความร้ายแรงของผลกระทบที่เกิดขึ้นจริง เมื่อเปรียบเทียบกับกฎหมายไทย พบว่ามาตรา 14 (1) (2) และ (3) ยังคงรวมหลายลักษณะของพฤติการณ์ไว้ในบทบัญญัติเดียว และกำหนดอัตราโทษในระดับใกล้เคียงกัน ข้อค้นพบเชิงเปรียบเทียบดังกล่าวจึงเป็นฐานสำหรับการพิจารณาแนวทางการปรับโครงสร้างบทบัญญัติและการบังคับใช้กฎหมายให้เหมาะสมกับบริบทของกฎหมายไทยในส่วนต่อไป

ข้อเสนอแนะ

จากผลการอภิปรายพบว่าบทบัญญัติมาตรา 14 (1) (2) และ (3) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 มีประเด็นเชิงโครงสร้างและแนวทางการตีความที่เกี่ยวข้องกับ

ความชัดเจนของขอบเขตความผิดและการบังคับใช้กฎหมาย ข้อเสนอแนะจึงสามารถนำเสนอในเชิงนิติวิธีเป็นลำดับดังต่อไปนี้

1. ข้อเสนอแนะเชิงกฎหมายว่าด้วยการกำหนดขอบเขตของบทบัญญัติ

ควรมีการกำหนดนิยามที่ใช้เป็นฐานของความผิดในมาตรา 14 ให้มีความชัดเจนมากยิ่งขึ้น โดยเฉพาะถ้อยคำที่ใช้เป็นเกณฑ์หลักในการกำหนดความผิด เช่น “ข้อมูลคอมพิวเตอร์อันเป็นเท็จ” “ข้อมูลคอมพิวเตอร์ปลอม” และ “น่าจะเกิดความเสียหาย” ซึ่งปัจจุบันยังมิได้มีการกำหนดนิยามหรือหลักเกณฑ์รองรับไว้อย่างชัดเจนในตัวบทกฎหมาย เพื่อให้การตีความมีทิศทางที่แน่นอนและเอื้อต่อความสามารถในการคาดหมายผลทางกฎหมายของบุคคล นอกจากนี้ การจัดโครงสร้างฐานความผิดตามลักษณะของพฤติการณ์และผลประโยชน์ที่กฎหมายมุ่งคุ้มครอง อาจช่วยให้การกำหนดอัตราโทษมีความสอดคล้องกับระดับความร้ายแรงของการกระทำได้อย่างเหมาะสม

2. ข้อเสนอแนะว่าด้วยการตีความและการบังคับใช้กฎหมาย

ควรให้ความสำคัญกับการตีความบทบัญญัติที่มีโทษทางอาญาโดยการตีความมาตรา 14 ควรเป็นไปตามหลักการตีความกฎหมายอาญาอย่างเคร่งครัด โดยให้ความสำคัญกับความหมายของถ้อยคำตามตัวบทและโครงสร้างของบทบัญญัติเป็นหลัก เพื่อจำกัดการขยายขอบเขตของความผิดให้อยู่ภายในกรอบที่กฎหมายบัญญัติไว้อย่างชัดแจ้ง

สำหรับคดีที่เกี่ยวข้องกับการเผยแพร่ข้อมูลหรือการสื่อสารผ่านระบบคอมพิวเตอร์ ควรพิจารณาบริบทของการสื่อสารในสังคมดิจิทัลควบคู่กับข้อเท็จจริงแห่งคดี โดยแยกแยะระหว่างข้อมูลเท็จในเชิงข้อเท็จจริง กับการแสดงความคิดเห็นหรือการนำเสนอทรรศนะ ทั้งนี้เพื่อให้การบังคับใช้มาตรา 14 เป็นไปตามขอบเขตของความผิดที่กฎหมายมุ่งหมายจะควบคุม

3. ข้อเสนอแนะเชิงบูรณาการว่าด้วยการประยุกต์แนวทางเชิงเปรียบเทียบ

จากผลการศึกษาเชิงเปรียบเทียบ การแยกฐานความผิดเกี่ยวกับคอมพิวเตอร์ตามผลประโยชน์ที่กฎหมายคุ้มครองอย่างชัดเจน เป็นแนวทางที่ช่วยเพิ่มความเป็นระบบของบทบัญญัติ การประยุกต์แนวคิดดังกล่าวให้เหมาะสมกับโครงสร้างของกฎหมายไทย อาจสนับสนุนให้การกำหนดองค์ประกอบความผิดและอัตราโทษตามมาตรา 14 (1) (2) และ (3) มีความชัดเจนและสอดคล้องกับหลักกฎหมายอาญามากยิ่งขึ้น

เอกสารอ้างอิง

เกียรติขจร วัจนะสวัสดิ์. (2562). *คำอธิบายรายวิชากฎหมายอาญา ภาค 1 เล่ม 1* (พิมพ์ครั้งที่ 11). กรุงเทพฯ: กรุงสยาม พับลิชชิ่ง.

คณิต ณ นคร. (2559). *กฎหมายอาญา ภาคความผิด* (พิมพ์ครั้งที่ 12). กรุงเทพฯ: สำนักพิมพ์วิญญูชน.

คณาธิป ทองรวีวงศ์. (2567). *กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1: ภาคกรอบแนวคิด*

ทฤษฎีและโครงสร้างฐานความผิด ภาคความผิดต่อความมั่นคงปลอดภัยของระบบและข้อมูลคอมพิวเตอร์. กรุงเทพฯ: สำนักพิมพ์นิติธรรม.

วรเจตน์ ภาคีรัตน์. (2564). *คำสอนว่าด้วยรัฐและหลักกฎหมายมหาชน* (พิมพ์ครั้งที่ 3). กรุงเทพฯ: สำนักพิมพ์อ่านกฎหมาย.

อภิรัตน์ เพ็ชรศิริ. (2562). *ทฤษฎีอาญา ทฤษฎีโทษ และกระบวนการขั้นพื้นฐาน* (พิมพ์ครั้งที่ 4). กรุงเทพฯ: สำนักพิมพ์วิญญูชน.

บรรจง วงค์สุนะ. (2567). ปัญหาทางกฎหมายของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 14. *Journal of Roi Kaensarn Academi*, 10, 1894–1904.

วนิดา แสงสารพันธ์. (2556). ขอบเขตของเสรีภาพในการแสดงความคิดเห็นภายใต้ข้อจำกัดของกฎหมาย. *วารสารผู้ตรวจการแผ่นดิน*, 2(2), 20–27.

ภรณี ตัณฑชุณห์. (2557). *ความเหมาะสมในการกำหนดความผิดทางอาญา: ศึกษากรณีปัญหาการล้มกีฬาตามกฎหมายไทย* (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต). มหาวิทยาลัยธรรมศาสตร์.

International Commission of Jurists. (2021). *Curtailing free expression and information online in Thailand*. Geneva: International Commission of Jurists.