การศึกษาปัญหาและอุปสรรคของกฎหมายและนโยบาย ที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

PROBLEMS AND OBSTACLES OF LAWS AND POLICIES RELATED TO THE PREVENTION AND SUPPRESSION ON TECHNOLOGICAL CRIMES

[1]ประดิษฐ์ จันทมูลตรี, [2]ธันย์ธรณ์เทพ แย้มอุทัย และ [3]สุรชัย พ่วงชูศักดิ์

[1]Pradit Janthamooltree, [2]Thundthornthep Yamoutai and

[3]Surachai Phuangchoosakdi

[1]มหาวิทยาลัยกรุงเทพธนบุรี, ประเทศไทย

[1]Bangkokthonburi University, Thailand

[1]ty.naja@hotmail.com, [2]thundthornthep@gmail.com

[3]Attorneyssp@yahoo.com

Received: October 26, 2024; **Revised** :November 15, 2024; **Accepted** :December 28,2024

บทคัดย่อ

บทความวิจัยเรื่องการศึกษาปัญหาและอุปสรรคของกฎหมายและนโยบายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีนี้ มีวัตถุประสงค์เพื่อศึกษาหาทางแก้ปัญหาประเด็นอุปสรรคของกฎหมายและนโยบายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีซึ่งน่าจะยังไม่เพียงพอ ซึ่งจากการศึกษาพบว่า 1) มีปัญหาอุปสรรคในการตีความหมายของคำว่า “สแปม” ซึ่งยังไม่มีในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 รวมทั้งกฎหมายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของหน่วยงานต่างๆ ฉะนั้นคำว่า“สแปม”จึงได้ใช้นิยามความเทียบเคียงคำว่า “จดหมายทางธุรกรรมหรือจดหมายอิเล็กทรอนิกส์เพื่อการพาณิชย์”

---

[1]อาจารย์ สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพธนบุรี

[2]อาจารย์ สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพธนบุรี

[3]อาจารย์ ดร. สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพธนบุรี

แทนซึ่งน่าจะยังคงไม่เพียงพอ จึงทำให้การกระทำผิดในการจารกรรมข้อมูลในคอมพิวเตอร์โดยวิธีการดูดข้อมูลคอมพิวเตอร์ทางออนไลน์หรือที่เรียกว่าสแปมยังคงพบมากขึ้นและทำให้เกิดคดีอาชญากรรมทางเทคโนโลยีเพิ่มขึ้นในประเทศไทยอย่างต่อเนื่อง ซึ่งถือเป็นสาเหตุสำคัญที่เป็นอุปสรรคของกฎหมายและนโยบายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของประเทศไทย ดังนั้น ผู้ศึกษาจึงเห็นควรศึกษาแนวทางในการตีความหมายของคำว่า “สแปม”ซึ่งต้องอยู่ภายใต้แนวคิดอนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรปหรืออนุสัญญา กรุงบูดาเปสต์ และต้องอยู่ในแนวทางกฎหมายของต่างประเทศด้วย อาทิเช่น แนวทางกฎหมายที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ของสหรัฐอเมริกามาตรา 18 ประมวลกฎหมายอาญา (18 U.S.C) และประมวลกฎหมายอาญาประเทศเยอรมัน มาตรา 202a และ 202b ที่ให้นิยามความไปทำนองเดียวกันว่า ผู้ใดกระทำการใดๆ ที่ทำให้ได้รับข้อมูลในคอมพิวเตอร์ผู้อื่นแล้วเผยแพร่ซึ่งน่าจะทำให้เจ้าของข้อมูลอาจได้รับอันตรายเสียหายได้ในอนาคตก็ย่อมถือว่า การกระทำผิดจารกรรมข้อมูลคอมพิวเตอร์ ซึ่งถือได้ว่า เป็นคำที่มีลักษณะความหมายที่มีความใกล้เคียงกับคำว่า “สแปม” ที่ถูกเรียกในการใช้ดูดข้อมูลคอมพิวเตอร์ทางออนไลน์ของผู้อื่นโดยมิชอบด้วยกฎหมาย

คำสำคัญ: การจารกรรมข้อมูลในระบบคอมพิวเตอร์, อนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรป, สแปม

Abstract

The Research article on the study of problems and obstacles in laws and policies related to the prevention and suppression of technological crimes. The objective is to study and find solutions to the problems of legal and policy obstacles related to measures to prevent and suppress technological crimes, which are likely to be insufficient. The study found that 1) there are obstacles in interpreting the meaning of the word "spam" which does not yet exist in the Computer Crime Act (No. 2) B.E. 2017, including laws related to measures. Prevent and suppress technological crimes of various agencies. Therefore, the word "spam" has been used to define similar to the word "spam". Instead, “transactional mail or commercial electronic mail” is likely still inadequate. As a result, the offense of computer espionage by means of online computer data extraction, also known as spam, is still more common and has led to an increase in technological crime cases in Thailand continuously. This is considered an

important cause that is an obstacle to laws and policies related to the prevention and suppression of technological crimes in Thailand. Therefore, the researcher deems it necessary to study guidelines for interpreting the meaning of the word “Spam” which must fall under the concept of the Council of Europe Computer Crime Convention or the Budapest Convention. And must be within the legal guidelines of foreign countries as well, such as the legal guidelines related to computer crimes of the United States, Section 18 of the Criminal Code (18 U.S.C) and the German Criminal Code, Sections 202a and 202b, which define the same thing as Whoever does anything That causes data to be received on other people's computers and distributed, which is likely to cause the owner of the data to be harmed in the future is considered. Computer espionage offenses which can be considered It is a word whose meaning is similar to the word "spam" which is used to illegally extract other people's online computer data.

Keywords: Computer espionage, Council of Europe Cybercrime Convention, Spam

บทนำ

ปัญหาและอุปสรรคของกฎหมายและนโยบายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีนี้ ซึ่งจากสถิติประวัติคดีอาชญากรรมทางเทคโนโลยีนั้น มีอัตราการเพิ่มขึ้นอย่างรวดเร็ว เฉพาะแต่มูลค่าความเสียหายทางแพ่งที่เกี่ยวเนื่องกับอาญา ช่วงวันที่ 1-29 กุมภาพันธ์ 2567 พบว่า มีจำนวน 21,506 เรื่อง มูลค่าความเสียหายรวม 2,493,842,459 บาท เฉลี่ย 85,944,568 บาทต่อวัน (กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, 2567) ซึ่งมูลเหตุที่มาของความเสียหายนั้นเป็นการส่งสแปมเพื่อดูดข้อมูลของผู้เสียหายมาเตรียมการก่อนแล้วจึงใช้วิธีการหลอกลวงในรูปแบบต่างทางออนไลน์ ฉะนั้นจึงต้องหาทางแก้ปัญหาประเด็นสาเหตุหลักสำคัญโดยเฉพาะการตีความหมายคำว่า “สแปม”เพื่อให้ครอบคลุมถึงผู้กระทำผิดที่ใช้เทคโนโลยีในการดูดข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบด้วยกฎหมาย ซึ่งประเทศไทยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 1) แต่พบว่า 1) การตีความหมายคำว่า “สแปม” ยังไมมีในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 1) ซึ่งยังต้องนำนิยามความอื่นมาเทียบเคียงตีความแทน ได้แก่ คำว่า “จดหมายทางธุรกรรมหรือจดหมายอิเล็กทรอนิกส์เพื่อการพาณิชย์” 2) แนวทางในการตีความหมายการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูล

คอมพิวเตอร์อันเป็นเท็จ ตามมาตรา 14 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560 ประเทศไทยนั้นมุ่งเน้นในส่วนที่ว่าน่าจะเกิดความเสียหายต่อระบบคอมพิวเตอร์อันเป็นการคุ้มครองแต่เฉพาะระบบคอมพิวเตอร์เป็นหลัก ซึ่งมีความแตกต่างจากแนวทางการตีความหมายของการนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ภายใต้อนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรป หรืออนุสัญญา กรุงบูดาเปสต์ ที่มุ่งเน้นในส่วนที่ว่า ผู้กระทำผิดได้กระทำการดูดข้อมูลเผยแพร่โดยการปล่อยนำข้อมูลคอมพิวเตอร์อันผิดกฎหมายเข้าสู่ระบบคอมพิวเตอร์ในเครื่องคอมพิวเตอร์ของผู้อื่น ซึ่งผู้ศึกษาเห็นว่า กรณีดังกล่าวนี้การตีความหมายการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ ตามมาตรา 14 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 น่าจะยังไม่เพียงพอ และก็น่าจะศึกษาในส่วนประเด็น ได้แก่ 1) ควรมีการตีความหมายคำว่า “สแปม” ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 หรือไม่ 2) แนวทางการตีความหมายของคำว่า “สแปม” น่าจะนำแนวทางของอนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรป หรืออนุสัญญากรุงบูดาเปสต์ และแนวทางของตัวบทกฎหมายต่างประเทศนำมาเปรียบเทียบปรับปรุงแก้ไขนำเสนอในการตีความหมายหรือไม่ เพื่อให้สอดคล้องกับการแก้ไขประเด็นปัญหาอุปสรรคดังกล่าวต่อไป

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาถึงปัญหาและอุปสรรคในการตีความหมายของคำว่า “สแปม” ซึ่งยังไม่มีในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

2. เพื่อศึกษาแนวทางการตีความหมายของคำว่า “สแปม” ภายใต้อนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรป หรืออนุสัญญากรุงบูดาเปสต์ เพื่อนำมาเปรียบเทียบปรับปรุงแก้ไขนำเสนอในการตีความหมายของประเทศไทย

3. เพื่อที่จะนำผลการศึกษาการตีความคำว่า “สแปม” ที่ได้จากการศึกษาวิจัยนำไปเสนอปรับปรุงแก้ไขเพิ่มเติมในการตีความหมายในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เพื่อให้สอดคล้องกับนโยบายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของหน่วยงานต่างๆ ที่เกี่ยวข้องให้มีประสิทธิภาพสูงสุดต่อไป

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้ใช้กระบวนการวิจัยเชิงคุณภาพ (Qualitative research process) มีเนื้อหาที่เกี่ยวข้องกับแนวทางในการตีความหมายของคำว่า “สแปม” ซึ่งยังไม่มีในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 โดยวิจัยศึกษาจากข้อมูลของเว็บไซค์หน่วยงานต่างที่เกี่ยวข้อง ในส่วนใหญ่เป็นข้อมูลในแบบเอกสารทางออนไลน์ที่เกี่ยวกับการป้องกันและปราบปรามปัญหาอาชญากรรมทางเทคโนโลยี ไม่ว่าจะเป็นบทความ หนังสือ วารสารต่างๆ แนวคิดที่มาของอนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรปหรืออนุสัญญา กรุงบูดาเปสต์ ตัวบทกฎหมายตามประมวลกฎหมายของประเทศไทยและต่างประเทศ ข้อมูลคดี มาตรการการป้องกันและปราบปรามปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทยและต่างประเทศเพื่อนำมาเปรียบเทียบกับมาตรการการป้องกันและปราบปรามประเทศไทย

ผลการวิจัย

1. ปัญหาและอุปสรรคในการตีความหมายของคำว่า “สแปม” นั้นไม่มีในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 รวมทั้งกฎหมายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของหน่วยงานต่างๆ ซึ่งคำว่า “สแปม” ได้ใช้นิยามความหมายเทียบเคียงกับคำว่า “จดหมายทางธุรกรรมหรือจดหมายอิเล็กทรอนิกส์เพื่อการพาณิชย์” แทนซึ่งน่าจะยังคงไม่เพียงพอ จึงทำให้การกระทำผิดในการจารกรรมข้อมูลในคอมพิวเตอร์โดยวิธีการดูดข้อมูลคอมพิวเตอร์ทางออนไลน์หรือที่เรียกว่าสแปมยังคงพบมากขึ้นและทำให้เกิดคดีอาชญากรรมทางเทคโนโลยีเพิ่มขึ้น (กุลนิดา ผาตินาวิน, 2564) ในประเทศไทยอย่างต่อเนื่อง

2. แนวทางการตีความหมายของคำว่า “สแปม”ภายใต้อนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรป หรืออนุสัญญากรุงบูดาเปสต์ เน้นในส่วนที่ว่า ผู้กระทำผิดได้กระทำการดูดข้อมูลเผยแพร่โดยการปล่อยนำข้อมูลคอมพิวเตอร์อันผิดกฎหมายเข้าสู่ระบบคอมพิวเตอร์ในเครื่องคอมพิวเตอร์ของผู้อื่น ซึ่งน่าจะเป็นความหมายใกล้เคียงของคำว่า “สแปม” เปรียบเทียบกับแนวทางกฎหมายที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ของสหรัฐอเมริกา ซึ่งกำหนดไว้ในมาตรา 18 ประมวลกฎหมายอาญา (18 U.S.C) กำหนดโทษการโจรกรรมข้อมูล ปลอมแปลงเอกลักษณ์บุคคล แฮกกิ้งบุกรุกล่วงล้ำระบบคอมพิวเตอร์ โดยตามมาตรา 1030 (a)(1) ผู้ใดเข้าถึงคอมพิวเตอร์เพื่อกระทำการจารกรรมข้อมูลคอมพิวเตอร์ ต้องระวางโทษไม่เกิน 10 ปี และ/หรือ ปรับตาม

มาตรา 1030(c)(1) ประกอบ มาตรา 1030(a)(2) การบุกรุกเข้าคอมพิวเตอร์ ได้แก่ การแฮกกิ้ง เป็นต้น เป็นผลให้เกิดการเปิดเผยข้อมูลรัฐ เครดิต การเงิน หรือสารสนเทศ ต้องระวางโทษ 1 ปี และ/หรือปรับตามมาตรา 1030(c)(2)(A) ซึ่งพบว่า การกระทำการใดๆ ที่ทำให้ได้รับข้อมูลในคอมพิวเตอร์ผู้อื่นแล้วเผยแพร่ ซึ่งน่าจะทำให้เจ้าของข้อมูลอาจได้รับอันตรายเสียหายได้ในอนาคตก็ย่อมถือว่า เป็นการกระทำผิดฐานจารกรรมข้อมูลคอมพิวเตอร์หรือสแปมแล้ว ซึ่งก็น่าจะถือเป็นความหมายที่น่าจะมีความใกล้เคียงกับการตีความหมายของคำว่า “สแปม” อันสามารถนำมาแก้ไขเพิ่มนิยามความหมายไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ของประเทศไทยได้

3. ผลการศึกษาการตีความหมายของคำว่า “สแปม” น่าจะหมายถึงการกระทำการใดๆ ที่ทำให้ได้รับข้อมูลในคอมพิวเตอร์ผู้อื่นแล้วเผยแพร่ซึ่งน่าจะทำให้เจ้าของข้อมูลอาจได้รับอันตรายเสียหายได้ในอนาคต ซึ่งหากนำความหมายดังกล่าวนี้นำไปเสนอปรับปรุงแก้ไขเพิ่มเติมในการตีความหมายในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ก็น่าจะทำให้การตีความหมายของคำว่า “สแปม” สอดคล้องกับนโยบายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของหน่วยงานต่างๆ ที่เกี่ยวข้องและทำให้มีประสิทธิภาพในการป้องกันและปราบปรามได้อย่างมีประสิทธิภาพมากขึ้นต่อไปในอนาคต

อภิปรายผล

จากการศึกษาปัญหาและอุปสรรคในการตีความหมายของคำว่า “สแปม” ซึ่งยังไม่มีในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 รวมทั้งกฎหมายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของหน่วยงานต่างๆ มีประเด็นที่สามารถนำมาอธิปรายผลได้ ดังนี้

1. คำว่า “สแปม” ได้ใช้นิยามความหมายเทียบเคียงกับคำว่า “จดหมายทางธุรกรรมหรือจดหมายอิเล็กทรอนิกส์เพื่อการพาณิชย์” แทน ซึ่งน่าจะยังคงไม่เพียงพอ เนื่องจากมีคดีเกี่ยวกับการหลอกลวงทางไซเบอร์ออนไลน์ เกิดปัญหาเรื่องการสืบสวนสอบสวนในคดีอาญาและปัญหาเรื่องการรับฟังพยานอิเล็กทรอนิกส์ ปัญหาเรื่องการพิสูจน์ข้อเท็จจริง เนื่องจากการกระทำผิดออนไลน์นั้นไม่สามารถรู้ตัวการผู้ที่กระทำผิด เพราะผู้กระทำสามารถใช้รหัสของผู้อื่นมาใช้แทนรหัสตนเองเพื่อหลบหนีการกระทำผิดได้ (ตวงพร จุลตามระ, 2561) ซึ่งถือเป็นวิธีการที่สลับซับซ้อน (วิรมณ ดาวดวง, 2564) จึงทำให้การกระทำผิดในการจารกรรมข้อมูลในคอมพิวเตอร์โดยวิธีการดูดข้อมูล

คอมพิวเตอร์ทางออนไลน์หรือที่เรียกว่าสแปมยังคงพบมากขึ้นและทำให้เกิดคดีอาชญากรรมทางเทคโนโลยีเพิ่มขึ้น (นัทธมน เพชรกล้า,2562) ในประเทศไทยอย่างต่อเนื่อง

2. แนวทางการตีความหมายของคำว่า “สแปม”ตามแนวทางของภายใต้อนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรป หรืออนุสัญญากรุงบูดาเปสต์ เน้นในส่วนที่ว่าผู้กระทำผิดได้กระทำการดูดข้อมูลเผยแพร่โดยการปล่อยนำข้อมูลคอมพิวเตอร์อันผิดกฎหมายเข้าสู่ระบบคอมพิวเตอร์ในเครื่องคอมพิวเตอร์ของผู้อื่น ซึ่งน่าจะเป็นความหมายใกล้เคียงของคำว่า “สแปม” เปรียบเทียบกับแนวทางของประเทศสหรัฐอเมริกา รัฐเวอร์จิเนีย มีแนวคิดกำหนดไว้ในประมวลกฎหมายอาญา ว่าด้วยคอมพิวเตอร์ซึ่งอธิบายว่าการบริการทางคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์เป็นสิ่งที่สามารถขโมยได้และได้บัญญัติให้การกระทำทำนองเดียวกับ Lund ลงในบัญญัติกฎหมายว่าด้วยการลักทรัพย์ของรัฐ (วีระพงษ์ บุญโญภาส, 2557) และก็ยังมีกฎหมายที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ของสหรัฐอเมริกา ซึ่งกำหนดไว้ใน มาตรา 18 ประมวลกฎหมายอาญา (18 U.S.C) กำหนดโทษการโจรกรรมข้อมูล ปลอมแปลงเอกลักษณ์บุคคล เฮกกิ้ง บุกรุกล่วงล้ำระบบคอมพิวเตอร์ โดยตามมาตรา 1030 (a)(1) ผู้ใดเข้าถึงคอมพิวเตอร์เพื่อกระทำการจารกรรมข้อมูลคอมพิวเตอร์ ต้องระว่างโทษไม่เกิน 10 ปี และ/หรือ ปรับตามมาตรา 1030(c)(1) ประกอบ มาตรา 1030(a)(2) การบุกรุกเข้าคอมพิวเตอร์ ได้แก่ การแฮกกิ้ง เป็นต้นเป็นผลให้เกิดการเปิดเผยข้อมูลรัฐ เครดิต การเงิน หรือสารสนเทศ ต้องระวางโทษ 1 ปี และ/หรือ ปรับตามมาตรา 1030(c)(2)(A) และประมวลกฎหมายอาญาของประเทศเยอรมนี ได้กำหนดในส่วนที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ ไว้ใน มาตรา 202a ว่า ผู้ใดกระทำการโจรกรรมข้อมูลต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับ สำหรับการได้มาซึ่งข้อมูลโดยผิดกฎหมาย หรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ทั้งข้อมูลที่อยู่ระหว่างสื่อสารหรือข้อมูลที่ถูกจัดเก็บไว้แล้ว ประกอบมาตรา 202b ว่า ผู้ใดกระทำการหลอกลวงทางอินเตอร์เน็ต (phishing) รวมถึงการดักจับข้อมูลต้องระวางโทษจำคุกไม่เกิน 2 ปี หรือปรับ ซึ่งพบว่า แนวทางมาตราการป้องกันและปราบปรามสอดคล้องกันว่า ผู้ใดกระทำการใดๆ ที่ทำให้ได้รับข้อมูลในคอมพิวเตอร์ผู้อื่นแล้วเผยแพร่ซึ่งน่าจะทำให้เจ้าของข้อมูลอาจได้รับอันตรายเสียหายได้ในอนาคตก็ย่อมถือว่า การกระทำผิดจารกรรมข้อมูลคอมพิวเตอร์หรือสแปมแล้ว ซึ่งก็น่าจะถือเป็นความหมายที่น่าจะมีความใกล้เคียงกับการตีความหมายของคำว่า “สแปม” อันสามารถนำมาแก้ไขเพิ่มนิยามความหมายไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ของประเทศไทยได้

3. ผลการศึกษาการตีความหมายของคำว่า “สแปม” ความหมายน่าจะหมายถึงการกระทำการใดๆ ที่ทำให้ได้รับข้อมูลในคอมพิวเตอร์ผู้อื่นแล้วเผยแพร่ซึ่งน่าจะทำให้เจ้าของข้อมูลอาจได้รับอันตรายเสียหายได้ในอนาคต ซึ่งหากนำความหมายดังกล่าวนี้นำเสนอไปปรับปรุงแก้ไข

เพิ่มเติมในการตีความหมายในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ก็น่าจะทำให้การตีความหมายของคำว่า “สแปม” สอดคล้องกับนโยบายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของหน่วยงานต่างๆ ที่เกี่ยวข้อง โดยเฉพาะการสืบสวนสอบสวนของเจ้าหน้าที่ เพื่อนำตัวผู้ที่กระทำความผิดซึ่งใช้ความรู้ความสามารถทางเทคโนโลยีมาดำเนินคดี (กุลนิดา ผาตินาวิน, 2564) เพราะการกระทำผิดที่เกี่ยวกับเทคโนโลยี ก็น่าจะต้องใช้คำที่ตีความหมายในทำนองที่คลอบคลุมการใช้เทคโนโลยีให้เกิดความเสียหายด้วยเช่นเดียวกัน (นันทวดี คาดคะเน, 2561) ซึ่งสอดคล้องกับแนวคิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (Hi-Tech Crime) (เพ็ญศิริ จันทร์ประทีปฉาย, 2548) สถานการณ์ในปัจจุบันทำให้มีประสิทธิภาพในการป้องกันและปราบปรามมากขึ้นต่อไป

องค์ความรู้ที่ได้จากการศึกษา

ประเทศไทยสามารถนำคำนิยามความที่มีความใกล้เคียงกันกับคำว่า “สแปม” มาแก้ไขปัญหาอุปสรรคป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยการนำมาปรับปรุงแก้ไขเพิ่มเติมในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 หรือกฎหมายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ซึ่งเดิมได้ใช้นิยามความเทียบเคียงคำว่า “จดหมายทางธุรกรรมหรือจดหมายอิเล็กทรอนิกส์เพื่อการพาณิชย์” แทนซึ่งน่าจะยังคงไม่เพียงพอ จึงทำให้การกระทำผิดในการจารกรรมข้อมูลในคอมพิวเตอร์โดยวิธีการดูดข้อมูลคอมพิวเตอร์ทางออนไลน์หรือที่เรียกว่าสแปมยังคงพบมากขึ้นและทำให้เกิดคดีอาชญากรรมทางเทคโนโลยีเพิ่มขึ้นในประเทศไทยอย่างต่อเนื่อง โดยการใช้คำโดยเฉพาะเจาะจงว่าผู้ใดกระทำการใดๆ ที่ทำให้ได้รับข้อมูลในคอมพิวเตอร์ผู้อื่นแล้วเผยแพร่ซึ่งน่าจะทำให้เจ้าของข้อมูลอาจได้รับอันตรายเสียหายได้ในอนาคต” เพื่อให้สามารถตีความถึงผู้ที่กระทำความผิดซึ่งใช้ความรู้ความสามารถทางเทคโนโลยีมากขึ้น อันน่าจะสอดคล้องกับอนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรป หรืออนุสัญญากรุงบูดาเปสต์ และกฎหมายที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ของต่างประเทศ อาทิเช่น ประเทศสหรัฐอเมริกา และประเทศเยอรมัน อันจะส่งให้เกิดประสิทธิภาพในใช้มาตรการในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของประเทศไทยเพิ่มขึ้น

ข้อดีประโยชน์และข้อเสียของการแก้ไขปรับปรุงนิยามความหมาย

ข้อดีและประโยชน์ ทำให้มีการตีความนิยามความหมายของคำว่า “สแปม” ได้อย่าง

สอดคล้องเหมาะสมกับเจตนารมณ์แนวคิดอนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรป หรืออนุสัญญา กรุงบูดาเปสต์ และยังทำให้เกิดประสิทธิในการใช้มาตรการในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีระหว่างประเทศไทยกับต่างประเทศเพิ่มขึ้น(กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, 2564) เนื่องจากว่า มีแนวคิดมุมมองกฎหมายที่เหมือนคล้ายไปในทำนองเดียวกัน ซึ่งหากว่า มีความต้องการที่จะต้องขอความช่วยเหลือร่วมมือในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีระหว่างประเทศก็ย่อมที่จะทำให้ความช่วยเหลือร่วมกันกันเกิดประสิทธิภาพมากขึ้นในระดับสากล (กัลยา ชินาธิวร, 2562)

ข้อเสีย อาจทำให้ต้องเสียค่าใช้จ่ายเพิ่มขึ้นเนื่องจากต้องมีหน่วยงานที่ช่วยเหลือในการวิเคราะห์สอบสวนข้อเท็จจริงเกี่ยวกับรูปแบบของการสแปมต่างๆ เพิ่มขึ้นด้วย เพราะว่า การสแปมนั้นเป็นการกระทำผิดที่สามารถเปลี่ยนรูปแบบขึ้นได้ตลอดเวลาขึ้นอยู่กับการพัฒนาโปรแกรมเทคโนโลยีความพิวเตอร์ (กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี, 2566) ฉะนั้น หากมีการเพิ่มเติมในการตีความนิยามคำว่า “สแปม” นี้แล้ว ก็น่าจะต้องเกิดค่าใช้จ่ายเพิ่มขึ้นในการตั้งหน่วยงานเจ้าหน้าที่เพื่อรองรับการพัฒนาเทคโนโลยีที่เกี่ยวกับการ สแปม เพื่อให้รู้เท่าทันกับการกระทำผิดที่ผู้กระทำผิดมีความรู้ในการใช้เทคโนโลยีสมัยใหม่

เอกสารอ้างอิง

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี. (2564). *สถิติการเข้าแจ้งความร้องทุกข์ ศูนย์บริการประชาชนในปี พ.ศ. 2564.* กองบัญชาการตำรวจสอบสวนกลาง, สำนักงานตำรวจแห่งชาติ.

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี. (2566). *รายงานสถิติการหลอกลวงทางออนไลน์ที่ผู้เสียหายแจ้งความออนไลน์.* กรุงเทพฯ: สำนักงานตำรวจแห่งชาติ.

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี. (2567). *รายงานสถิติการหลอกลวงทางออนไลน์ที่ผู้เสียหายแจ้งความออนไลน์.* กรุงเทพฯ: สำนักงานตำรวจแห่งชาติ.

กัลยา ชินาธิวร (2562). *ปัจจัยความสำเร็จของสิงคโปร์ กรณีศึกษาเพื่อประกอบการพัฒนาแนวทางการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทยรายงานการศึกษาส่วนบุคคล,* กระทรวงการต่างประเทศ

กุลนิดา ผาตินาวิน (2564). *ปัญหาการนำสืบพยานหลักฐานข้อมูลอิเล็กทรอนิกส์ในคดีอาญา.* บัณฑิตวิทยาลัย : มหาวิทยาลัยธุรกิจบัณฑิต.

ตวงพร จุลตามระ (2561). *ปัญหาการนำสืบพยานหลักฐานข้อมูลอิเล็กทรอนิกส์ในคดีอาญา ศึกษากรณี ข้อมูลที่ได้จากระบบการรับส่งข้อความทันที.* บัณฑิตวิทยาลัย : มหาวิทยาลัยธุรกิจบัณฑิต.

นัทธมน เพชรกล้า. (2562). *การศึกษาสถานการณ์ของอาชญากรรมไซเบอร์ในประเทศไทย. โครงการพัฒนานักบริหารการเปลี่ยนแปลงรุ่นใหม่ รุ่นที่ 11.* กรุงเทพฯ: สถาบันส่งเสริมการบริหารกิจการบ้านเมืองที่ดี.

นันทวดี คาดคะเน (2561). *ปัญหาในการปราบปรามอาชญากรรมไซเบอร์ภายใต้กฎหมายระหว่างประเทศ.* บัณฑิตวิทยาลัย : มหาวิทยาลัยธรรมศาสตร์.

เพ็ญศิริ จันทร์ประทีปฉาย. (2548). *มืออาชีพ: ตำรวจไซเบอร์กับภารกิจปราบปรามอาชญากรรมทางเทคโนโลยี.* วารสารสารคดี, 21, (241).

วิรมณ ดาวดวง (2564). *ปัญหาการรวบรวมพยานหลักฐานเพื่อดำเนินคดีอาชญากรรมไซเบอร์.* บัณฑิตวิทยาลัย : มหาวิทยาลัยธรรมศาสตร์.

วีระพงษ์ บุญโญภาส และคณะ (2557). *อาชญากรรมทางเศรษฐกิจ.*กรุงเทพฯ สำนักพิมพ์นิติธรรม.

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, รายงานการประชุมครั้งที่ 2/ 2561 (20 ธันวาคม 2561).

American Criminal Code (18 U.S.C) Council of Europe Computer Crime Convention or Budapest Convention

German Criminal Code Sections 202a and 202b