ปัญหามาตรการทางกฎหมายในการป้องกันภัยจากการถูกคุกคามทางไซเบอร์

PROBLEMS OF LEGAL MEASURES TO PREVENT FROM CYBER THREATS

[1]สุรชัย พ่วงชูศักดิ์, [2]วิทยา เบ็ญจาธิกุล และ [3]ป้อมฤดี กุมพันธ์

[1]Surachai Phangchoosakdi, [2]Witthaya Benjathikun and [3]Pomrudee Kumpant

มหาวิทยาลัยกรุงเทพธนบุรี, ประเทศไทย

Bangkokthonburi University, Thailand

[1]Attorneyssp@yahoo.com, [2]Law@bkkthon.ac.th, [3]pomkp1989@gmail.com

Received: July 08, 2023; **Revised**: July 29, 2023; **Accepted**: August 24, 2023

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาหาทางแก้ไขประเด็นปัญหาในการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ที่น่าจะยังไม่เพียงพอตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยศึกษาถึงการกำหนดนิยามความหมายทางกฎหมายเกี่ยวกับการกระทำคุกคามทางไซเบอร์ของประเทศไทยเป็นการเฉพาะนั้นเป็นการให้คุ้มครองป้องกันผู้เสียหายที่เป็นเหยื่อจากการถูกคุกคามทางไซเบอร์ด้วยหรือไม่ หน่วยงานที่ช่วยประสานงานการใช้มาตรการการดำเนินคดีเกี่ยวกับการป้องกันจากการถูกกระทำคุกคามทางไซเบอร์มีประสิทธิภาพเพียงพอหรือไม่ และบทลงโทษเกี่ยวกับการกระทำคุกคามทางไซเบอร์เพื่อให้สามารถปฏิบัติงานให้เกิดประสิทธิภาพเต็มที่เหมาะสมหรือไม่ ทั้งนี้เพื่อที่จะนำเสนอแนวทางรูปแบบใหม่มากขึ้นในการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ที่น่าจะมีประสิทธิภาพเพียงพอมากขึ้น ผลการศึกษา 1) พบว่า ประเทศออสเตรเลียมีกฎหมาย Enhancing Online Safety Act 2015 ตามมาตรา 4 และมาตรา 5 ซึ่งมีการกำหนดนิยามของคำว่า การกระทำคุกคามทางไซเบอร์เด็กและเยาวชนไว้โดยเฉพาะเจาะจง 2) พบว่า ประเทศออสเตรเลีย มีหน่วยงานคณะกรรมการการควบคุมความปลอดภัยทางอิเล็กทรอนิกส์ (e-Safety Commissioner) ในการช่วยประสานงานกับตำรวจไซเบอร์ในการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ตามกฎหมาย และ 3) พบว่า ประเทศออสเตรเลีย มี

---

[1] อาจารย์ ดร. สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพธนบุรี

[2] ผู้ช่วยศาสตราจารย์ ดร. สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพธนบุรี

[3] อาจารย์ ดร. สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพธนบุรี

กฎหมาย Enhancing Online Safety Act 2015 มาตรา 46 ที่มีการระบุบทลงโทษทางปกครองที่ให้เสียค่าปรับทางปกครองกับผู้ให้บริการและผู้ใช้บริการที่กระทำความผิดตามกฎหมาย ซึ่งสามารถนำมาแก้ไขและปรับใช้เป็นแนวทางรูปแบบใหม่ในการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ที่สมควรเหมาะสมและเกิดประสิทธิภาพมากขึ้นในกฎหมายประเทศไทย

คำสำคัญ : แนวทางป้องกัน, การกระทำคุกคามทางไซเบอร์, ภัยคุกคามทางไซเบอร์, เหยื่อจากการถูกคุกคามทางไซเบอร์

Abstract

The purpose of this research is to study and find solutions to the problem of preventing cyber threats that are likely to be insufficient according to the Cyber Security Act B.E. 2562 by studying Determining the legal definition of cyber harassment in Thailand specifically provides protection for victims who are victims of cyber harassment or not. Are the agencies that help coordinate the implementation of cyber-attack prosecution measures effective enough and penalties for cyber threats in order to be able to operate with full efficiency or not. In order to introduce more new ways to protect against cyber threats that should be more effective.The results of the study; 1) It was found that Australia has a law Enhancing Online Safety Act 2015 under Sections 4 and 5, which defines the term 2) it was found that Australia There is an electronic safety control committee (e-Safety). Commissioner) to help coordinate with the cyber police in preventing cyber threats according to the law and 3) found that Australia has a law Enhancing Online Safety Act 2015, section 46, which specifies administrative penalties to pay administrative fines. with service providers and service users who violate the law which can be adapted into a new approach to prevent cyber threats in Thailand that is suitable and more effective.

Keywords : Prevention Guidelines, Cyber Threat Actions, Cyber Threats, Victims of Cyber Threats

บทนำ

ปัจจุบันการสื่อสารในโลกปัจจุบันไม่ว่าจะเป็นในรูปแบบของทิศทางเดียวหรือแบบสองทิศทางต่างมีการใช้เทคโนโลยีเป็นสื่อกลางในการสื่อสารโดยมีอินเทอร์เน็ตเป็นเครือข่ายในการเชื่อมโยงเพื่อประโยชน์ต่อชีวิตประจำวันของมนุษย์ โดยมีอุปกรณ์ที่รองรับเทคโนโลยีมาใช้ประกอบไม่ว่าจะเป็นโทรศัพท์สมาร์ทโฟน แทปเลต หรือคอมพิวเตอร์ เป็นต้น โดยมีแนวโน้มในการใช้งานเพิ่มสูงขึ้นตามวิวัฒนาการทางเทคโนโลยี ประโยชน์ของเทคโนโลยีเมื่อเครือข่ายอินเทอร์เน็ตมี

อิทธิพลต่อชีวิตของมนุษย์มากขึ้นด้วยการสร้างพื้นที่เสมือนจริงอย่างพื้นที่ไซเบอร์ (Cyberspace) ซึ่งเป็นพื้นที่ที่มนุษย์หลายล้านคนกระโดดเข้ามาทำกิจกรรมแลกเปลี่ยนข้อมูลข่าวสารซึ่งกันและกันอย่างหนาแน่นผ่านเครือข่ายสังคมออนไลน์ทั้งหลาย เช่น เฟซบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) ไลน์ (Line) เป็นต้น จึงทำให้ผู้ที่เข้ามาใช้งานได้กระทำการที่ละเมิดสิทธิของผู้ใช้งานอย่างหลากหลาย (Mullen et al., 1999, pp. 1244-1249) ไม่ว่าจะด้วยมีเจตนาหรือประมาทเลินเล่อ (Lee, Croninger, Linn, & Chen, 1996, pp. 386-389) ก็ตาม เป็นเหตุทำให้เกิดความเสียหายและเกิดผลกระทบ (กชพรรณ มณีภาค และอุนิษา เลิศโตมรสกุล, 2562, น. 3) กับผู้ใช้งานเช่นกัน (เมธาพันธ์ ประยงค์พันธ์, 2563, น. 4) อันเป็นภัยคุกคามที่มาในรูปแบบออนไลน์ (มูลนิธิส่งเสริมสื่อเด็กและเยาวชน (สสย.), 2563, น. 3) และนอกจากนี้ยังมีการตรวจพบภัยคุกคามในรูปแบบใหม่ ๆ (พรรษาวดี คล้อยระยับ และอุนิษา เลิศโตมรสกุล, 2564, น. 35) เกิดเพิ่มขึ้นบนอุปกรณ์พกพา (พินวา แสนใหม่, 2563, น. 10) และก็ยังมีแนวโน้มว่าภัยคุกคามต่าง ๆ (สุธาเทพ รุณเรศ, 2561, น. 2) ดังกล่าวจะยังคงเพิ่มขึ้นอย่างต่อเนื่อง (อัมพร ธำรงลักษณ์, 2552, น. 35) ซึ่งถือว่าเป็นปัญหาสำคัญ (สาวตรี สุขศรี, 2563, น. 163) จึงทำให้ประเทศไทยได้ออกกฎหมายเพื่อใช้เป็นมาตรการในการป้องกันภัยคุกคามดังกล่าว (รักษ์ษิตา โพธิ์พิทักษ์กุล, 2550, น. 14) คือ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งได้รวบรวมข้อมูลปัญหาที่ใช้เรียกกันมาตั้งแต่ยุคแรกดังเดิมที่ว่า ออนไลน์ บ้าง หรือ ดิจิทัล บ้าง โดยเรียกรวมกันอย่างเป็นทางการโดยใช้คำว่า ไซเบอร์ ซึ่งก็หมายถึง ข้อมูลการสื่อสารที่เกิดจากการใช้บริการระบบอินเทอร์เน็ต ฉะนั้นจึงเกิดนิยามความของคำว่า ภัยคุกคามทางไซเบอร์ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ แต่ถึงอย่างไรก็ตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่ใช้บังคับอยู่นั้น ก็น่าจะยังไม่เพียงพอ เนื่องจากในปัจจุบันก็ยังคงเกิดปัญหาความเสียหายต่าง ๆ ทางไซเบอร์อยู่อีกเป็นจำนวนมากและไม่มีแนวโน้มที่จะลดลง (ปองกมล สุรัตน์, 2561, น. 3) ซึ่งผู้วิจัยมีความเห็นว่า น่าจะยังมีประเด็นปัญหาในการบังคับใช้อยู่ ได้แก่ 1) ภัยคุกคามทางไซเบอร์นั้น นอกจากจะส่งผลกระทบต่อระบบคอมพิวเตอร์แล้ว ก็ยังส่งผลกระทบต่อผู้เสียหายที่เป็นเหยื่อจากการถูกกระทำคุกคามทางไซเบอร์ที่ใช้ในระบบคอมพิวเตอร์ (สำนักเทคโนโลยีสารสนเทศและการสื่อสาร คณะทำงานการจัดการความรู้ สำนักงานเลขาธิการวุฒิสภา, 2559, น. 10) ด้วย ฉะนั้น จึงควรที่จะให้มีการกำหนดนิยามความหมายทางกฎหมายเกี่ยวกับภัยคุกคามทางไซเบอร์ของประเทศไทยเป็นการเฉพาะเพื่อให้คุ้มครองป้องกันผู้เสียหายที่เป็นเหยื่อที่ถูกคุกคามทางไซเบอร์ไว้ด้วยหรือไม่ 2) หน่วยงานที่ใช้มาตรการการดำเนินคดีเกี่ยวกับการป้องกันภัยถูกคุกคามทางไซเบอร์ตามกฎหมายประเทศไทยเพียงพอหรือไม่ และมีจำเป็นต้องมีหน่วยงานที่ช่วยประสานงานการใช้มาตรการการดำเนินคดีเกี่ยวกับการป้องกันจากการถูกกระทำคุกคามทางไซเบอร์หรือไม่ 3) บทลงโทษเกี่ยวกับการป้องกันภัยถูกคุกคามทางไซเบอร์ตามกฎหมายของประเทศไทยมีเพียงพอหรือไม่ จึงทำให้เกิดปัญหาในการใช้วิธีการเพื่อการป้องกันภัยถูกคุกคามทางไซเบอร์ตามกฎหมายที่ไม่สามารถปฏิบัติงานให้เกิดประสิทธิภาพเต็มที่เหมาะสมได้ (Graham, & Wood, 2003, pp. 227-248) ดังนั้น จึงควรศึกษาหาวิธีการใหม่เพื่อนำมาปรับใช้ต่อไป

วัตถุประสงค์ของการวิจัย

1.เพื่อศึกษาให้ทราบว่า ควรที่จะให้มีการกำหนดนิยามความหมายทางกฎหมายเกี่ยวกับภัยการกระทำคุกคามทางไซเบอร์ของประเทศไทยเป็นการเฉพาะเพื่อให้คุ้มครองป้องกันผู้เสียหายที่เป็นเหยื่อไว้ด้วยหรือไม่

2. เพื่อศึกษาให้ทราบว่า หน่วยงานที่ใช้มาตรการการดำเนินคดีเกี่ยวกับการป้องกันภัยถูกคุกคามทางไซเบอร์ตามกฎหมายประเทศไทยมีเพียงพอหรือไม่

3. เพื่อศึกษาให้ทราบว่า บทลงโทษเกี่ยวกับการป้องกันภัยถูกคุกคามทางไซเบอร์ตามกฎหมายของประเทศไทยมีเพียงพอหรือไม่

4. เพื่อศึกษาให้ทราบว่า มีวิธีการใหม่ ๆ ที่จะสามารถนำมาปรับใช้ให้เหมาะสมกับมาตรการการการป้องกันภัยคุกคามทางไซเบอร์ในระบบกฎหมายไทยให้มีประสิทธิภาพมากขึ้นหรือไม่

วิธีการดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพการวิจัย โดยมีเนื้อหาที่เกี่ยวข้องกับแนวทางแก้ไขปัญหามาตรการทางกฎหมายในการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ โดยใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ที่อาศัยการตรวจสอบข้อมูลโดยใช้เทคนิคการตรวจสอบวิเคราะห์ข้อมูลด้วยเทคนิคการวิเคราะห์เนื้อหา (Content Analysis) ตัวบทกฎหมาย เอกสาร รายงาน รวมทั้งงานวิจัยอื่นที่เกี่ยวข้อง

ผลการวิจัย

1. ปัญหาทางกฎหมายในการกำหนดนิยามการกระทำคุกคามทางไซเบอร์ จากผลการศึกษาวิจัยถึงปัญหาทางกฎหมายในการกำหนดนิยามการกระทำคุกคามทางไซเบอร์ พบว่า การกำหนดนิยามความหมายทางกฎหมายการกระทำคุกคามทางไซเบอร์ของประเทศไทยนั้นยังไม่มีการกำหนดเป็นการเฉพาะไว้ (จิตติ ติงศภัทิย์, 2553, น. 1234) เพียงแต่ได้เทียบเคียงปรับใช้กับประมวลกฎหมายอาญา มาตรา 397 คำพิพากษาฎีกาที่ 110/2516 และ คำพิพากษาฎีกา 3711/2557 เพียงนั้น (สาวตรี สุขศรี, 2563, น. 255-256) ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีการกำหนดลักษณะของการคุกคามไว้ว่ามี 2 รูปแบบ คือ 1) การคุกคามต่อข้อมูลอันเป็นสาระสำคัญที่เกี่ยวข้องกับความเสียหายและความมั่นคงของชาติ และ 2) การคุกคามต่อปัจเจกบุคคล พร้อมกับมีบทลงโทษ พระราชบัญญัติว่าด้วยความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ซึ่งมีความเหมือนกันกับนิยามทางกฎหมายของการคุกคามทางไซเบอร์ของประเทศสหรัฐอเมริกา ซึ่งก็ยังไม่มี การกำหนดเป็นการเฉพาะไว้ เพียงแต่มีตัวบทกฎหมาย

กฎหมาย U.S.C Chapter 110A Domestic Violence and Stalking ของประเทศสหรัฐอเมริกา ที่ได้เทียบเคียงปรับใช้กับ มาตรา 2261A ที่กำหนดให้ Stalking เป็นความผิด และมาตรา 2261A (2) ที่บัญญัติให้ครอบคลุมการติดตามรังความออนไลน์หรือระบบสื่อสารอิเล็กทรอนิกส์ด้วยให้มีความผิดด้วย พร้อมกับมีบทกำหนดการถูกคุกคามที่มีความรุนแรงกว่าบทลงโทษประเทศไทย (สาวตรี สุขศรี, 2555, น. 282-320) ซึ่งมีความแตกต่างกับกฎหมายของประเทศออสเตรเลียที่มีกฎหมาย Enhancing Online Safety Act 2015 ตามมาตรา 4 และมาตรา 5 ซึ่งมีการกำหนดนิยามของคำว่า การกระทำคุกคามทางไซเบอร์เด็กเยาวชนไว้โดยเฉพาะเจาะจง (สมยศ เชื้อไทย, 2555, น. 27) และโดยเฉพาะในส่วนของกฎหมาย Enhancing Online Safety Act 2015 มาตรา 5 ที่ได้มีการกำหนดนิยามทางกฎหมายการคุกคามทางไซเบอร์ไว้โดยเฉพาะเจาะจงต่อเด็กชาวออสเตรเลียที่ว่า “การกลั่นแกล้งรังแกทางไซเบอร์ที่เหยื่อเป็นเด็กชาวออสเตรเลีย คือ การกระทำผ่านสื่อสังคมออนไลน์หรือเกี่ยวข้องกับบริการทางอิเล็กทรอนิกส์ โดยบุคคลทั่วไปสามารถเข้าใจได้ว่าเนื้อหาในการกระทำมีผลกระทบต่อเด็กชาวออสเตรเลียอย่างร้ายแรงด้วยวิธีการข่มขู่ คุกคามอย่างร้ายแรง ข่มขวัญทำให้เกิดความกลัวอย่างร้ายแรง รังควานอย่างร้ายแรงหรือทำให้ขายหน้าอย่างร้ายแรง อันเป็นผลกระทบโดยตรงหรือนำมาซึ่งผลกระทบนั้นโดยอ้อม ทำให้สะดวกต่อการตีความนิยามความหมายของการคุกคามทางไซเบอร์เพราะเป็นการระบุไว้เป็นการเฉพาะเจาะจงไว้แล้ว

2. หน่วยงานที่ใช้มาตรการการดำเนินคดีเกี่ยวกับการกลั่นแกล้งคุกคามทางไซเบอร์ จากผลการศึกษาวิจัยโดยวิเคราะห์ถึงหน่วยงานที่ใช้มาตรการการดำเนินคดีเกี่ยวกับการกลั่นแกล้งคุกคามทางไซเบอร์ พบว่า หน่วยงานมาตรการการดำเนินคดีเกี่ยวกับการกลั่นแกล้งคุกคามทางไซเบอร์นั้นประเทศไทยซึ่งมีการจัดตั้งกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี หรือกองบัญชาการตำรวจไซเบอร์ โดยมีอำนาจหน้าที่ไว้อย่างครอบคลุม เช่น เป็นฝ่ายอำนวยการด้านยุทธศาสตร์ให้สำนักงานตำรวจแห่งชาติในการวางแผน ควบคุม ตรวจสอบ ให้คำแนะนำและการเสนอแนะเกี่ยวกับการปฏิบัติงานตามอำนาจหน้าที่ ดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วราชอาณาจักร ซึ่งจะมีการใช้มาตรการจับกุมตัวผู้กระทำผิดมาลงโทษทางอาญาตามกฎหมาย อันเป็นขั้นตอนของกระบวนการยุติธรรมทางอาญาทั่วไป เหมือนกันกับมาตรการของประเทศสหรัฐอเมริกา ซึ่งมีความแตกต่างกันกับมาตรการของประเทศออสเตรเลียที่มีหน่วยงานคณะกรรมการควบคุมความปลอดภัยทางอิเล็กทรอนิกส์ในการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ตามกฎหมาย (e-Safety Commissioner) สามารถนำมาปรับใช้เพื่อมาช่วยที่ทำหน้าที่ประสาน งานกับเจ้าหน้าที่ตำรวจไซเบอร์ในการให้มีการลบโพสต์และโพสต์ขอโทษได้ด้วยความรวดเร็วอันเป็นการเยียวยาจิตใจผู้เสียหายโดยเฉพาะเด็กเยาวชนตามมาตรา 18 และ มาตรา 67 โดยที่เน้นการมีคำสั่งเตือนโดยให้กระทำการลบโพสต์ ขอโทษในสิ่งที่กระทำ ซึ่งหากขัดคำสั่งก็จะมีโทษทางปกครองเป็นค่าปรับแทน โดยจะมีหน่วยงานเพิ่มเติมในการดำเนินการเพื่อประสาน งานและเป็นช่องทางเชื่อมโยงการดำเนินงานให้กับพนักงานเจ้าหน้าที่ เรียกว่า คณะกรรมการควบคุมความปลอดภัยทางอิเล็กทรอนิกส์ e-Safety Commissioner ซึ่งมีอำนาจ

หน้าที่จะทำการประสานงานโดยตรง รับเรื่องร้องเรียน อีกทั้งประสานงานสั่งให้ผู้ให้บริการลบข้อมูล หากเพิกเฉยก็จะถูกดำเนินการฟ้องร้องต่อศาลต่อไป

3. บทลงโทษจากการถูกคุกคามทางไซเบอร์ จากผลการศึกษาวิจัยถึงบทลงโทษจากการถูกคุกคามทางไซเบอร์ พบว่า บทลงโทษตามองค์ประกอบความผิดเกี่ยวกับการคุกคามทางไซเบอร์ของประเทศไทยที่นำมาปรับใช้ตามประมวลกฎหมายอาญา มาตรา 397 ซึ่งมีความเหมือนกันกับกฎหมายของประเทศสหรัฐ อเมริกาที่ใช้กฎหมาย U.S.C Chapter 110A Domestic Violence and Stalking มาตรา 2261A โดยกฎหมายดังกล่าวนั้นมุ่งประสงค์ในการนำตัวผู้กระทำผิดมาลงโทษทางอาญา เพื่อให้มีความยำเกรงต่อกฎหมายด้วยการลงโทษ ซึ่งมีความแตกต่างกับกฎหมายของประเทศออสเตรเลียที่มีกฎหมาย Enhancing Online Safety Act 2015 ซึ่งมีการระบุบทลงโทษทางปกครองที่ให้เสียค่าปรับทางปกครองกับผู้ให้บริการและผู้ใช้บริการที่กระทำความผิดตามกฎหมายตามมาตรา 46 โดยเน้นบทลงโทษโดยการเสียค่าปรับและการทำสาธารณประโยชน์ให้แก่สังคม

4. การนำเสนอวิธีการป้องกันการกระทำคุกคามทางไซเบอร์ใหม่ที่เหมาะสมในการนำมาปรับใช้กับกฎหมายไทย จากผลการศึกษาวิจัยถึงพบว่า มีแนวทางและวิธีการป้องกันการกระทำการคุกคามทางไซเบอร์ใหม่ที่เหมาะสมในการนำมาปรับใช้กับกฎหมายไทย ซึ่งหากมีการนำวิธีการของประเทศออสเตรเลียดังกล่าวข้างต้นนำมาปรับใช้กับกฎหมายไทย ก็น่าที่จะทำให้การตีความนิยามของการกระทำการคุกคามทางไซเบอร์ ซึ่งยังไม่มีนิยามความหมาย ให้สามารถมีนิยามความหมายและขอบเขตองค์ประกอบที่ตีความได้ชัดเจนมากขึ้น อีกทั้งมีหน่วยงานเฉพาะทางไซเบอร์ให้บริการประสานงานโดยตรงที่จะเยียวยาความเสียหายทางจิตใจในการลบโพสต์และโพสต์ขอโทษ และมีบทลงโทษที่มีความเหมาะสมมากขึ้นซึ่งนอกจากการลงโทษทางอาญากับผู้กระทำผิดแล้วยังมีบทลงโทษทางปกครองในการเยียวยาลบโพสต์โดยรวดเร็วและการมีโทษปรับทางปกครองทั้งผู้ให้บริการและผู้กระทำผิดร่วมกันอีกด้วย ซึ่งน่าจะถือได้ว่า เป็นการแก้ไขปัญหามาตรการการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ตามกฎหมายของประเทศไทยอย่างเหมาะสม และสามารถนำไปปฏิบัติงานให้เกิดประสิทธิภาพได้อย่างเต็มที่

อภิปรายผล

1. การกำหนดนิยามความหมายทางกฎหมายการกระทำคุกคามทางไซเบอร์ของประเทศไทยนั้นยังไม่มีการกำหนดเป็นการเฉพาะไว้ เพียงแต่ได้เทียบเคียงปรับใช้กับประมวลกฎหมายอาญา มาตรา 397 เพียงนั้น และก็มีการกำหนดลักษณะของการคุกคามไว้ว่า มี 2 รูปแบบ คือ 1) การคุกคามต่อข้อมูลอันเป็นสาระสำคัญที่เกี่ยวข้องกับความเสียหายและความมั่นคงของชาติ 2) ของการคุกคามต่อปัจเจกบุคคล พร้อมกับมีบทลงโทษพระราชบัญญัติว่าด้วยความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ซึ่งมีความเหมือน กันกับนิยามทางกฎหมายการคุกคามทางไซเบอร์ของประเทศสหรัฐอเมริกา ซึ่งก็ยังไม่มี กำหนดเป็นการเฉพาะ เพียงแต่กฎหมาย U.S.C Chapter 110A Domestic Violence and Stalking ของประเทศสหรัฐอเมริกาได้เทียบเคียงปรับใช้กับ มาตรา

2261A ที่กำหนดให้ Stalking เป็นความผิด และมาตรา 2261A (2) ที่บัญญัติให้ครอบคลุมการติดตามรังควานออนไลน์หรือระบบสื่อสารอิเล็กทรอนิกส์ด้วยให้มีความผิดด้วย พร้อมกับมีบทกำหนดการถูกคุกคามที่มีความรุนแรงกว่าบทลงโทษประเทศไทย ซึ่งก็มีความแตกต่างกันกับกฎหมายของประเทศออสเตรเลียที่มีกฎหมายเฉพาะ คือ Enhancing Online Safety Act 2015 ที่ได้มีการกำหนดนิยามความหมายของการคุกคามทางไซเบอร์ไว้โดยเฉพาะเจาะจง ตามมาตรา 5 ที่ว่า “การกลั่นแกล้งรังแกทางไซเบอร์ที่เหยื่อเป็นเด็กชาวออสเตรเลีย คือ การกระทำผ่านสื่อสังคมออนไลน์หรือเกี่ยวข้องกับบริการทางอิเล็กทรอนิกส์ โดยบุคคลทั่วไปสามารถเข้าใจได้ว่าเนื้อหาในการกระทำมีผลกระทบต่อเด็กชาวออสเตรเลียอย่างร้ายแรงด้วยวิธีการข่มขู่ คุกคามอย่างร้ายแรง ขู่ขวัญทำให้เกิดความกลัวอย่างร้ายแรง รังควานอย่างร้ายแรงหรือทำให้ขายหน้าอย่างร้ายแรง อันเป็นผลกระทบโดยตรงหรือนำมาซึ่งผลกระทบนั้นโดยอ้อม ซึ่งทำให้สะดวกต่อการตีความนิยามความหมายของการคุกคามทางไซเบอร์เพราะเป็นการระบุไว้เป็นการเฉพาะเจาะจงไว้แล้ว

2. หน่วยงานมาตรการการดำเนินคดีเกี่ยวกับการกลั่นแกล้งคุกคามทางไซเบอร์นั้น ประเทศไทยซึ่งมีการจัดตั้งกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี หรือกองบัญชาการตำรวจไซเบอร์ โดยมีอำนาจหน้าที่ไว้อย่างครอบคลุมเช่นเป็นฝ่ายอำนวยการด้านยุทธศาสตร์ให้สำนักงานตำรวจแห่งชาติในการวางแผน ควบคุม ตรวจสอบ ให้คำแนะนำและการเสนอแนะในการปฏิบัติงานตามอำนาจหน้าที่ ดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วราชอาณาจักร ซึ่งจะมีการใช้มาตรการจับกุมตัวผู้กระทำผิดมาลงโทษทางอาญาตามกฎหมาย อันเป็นขั้นตอนของกระบวนการยุติธรรมทางอาญาทั่วไป เหมือนกันกับมาตรการของประเทศสหรัฐอเมริกา ซึ่งจะแตกต่างกันกับมาตรการของประเทศออสเตรเลีย ที่เน้นการมีคำสั่งเตือนโดยให้กระทำการลบโพสต์ ขอโทษในสิ่งที่กระทำ ซึ่งหากขัดคำสั่งก็จะมีโทษทางปกครองเป็นค่าปรับแทน โดยจะมีหน่วยงานเพิ่มเติมในการดำเนินการเพื่อประสานการและเป็นช่องทางในการเชื่อมโยงการดำเนินงานให้กับพนักงานเจ้าหน้าที่ เรียกว่า คณะกรรมการควบคุมความปลอดภัยทางอิเล็กทรอนิกส์ e-Safety Commissioner ซึ่งมีอำนาจหน้าที่ในการช่วยประสานงานโดยตรง รับเรื่องร้องเรียน ประสานงานสั่งผู้ให้บริการลบข้อมูล หากเพิกเฉยคณะกรรมการมีอำนาจในการดำเนินคดีทางปกครองเพื่อเสียค่าปรับทางปกครองตามกฎหมาย

3. องค์ประกอบความผิดเกี่ยวกับการคุกคามประเทศไทย ที่นำมาปรับใช้เทียบเทียบ ตามประมวลกฎหมายอาญา มาตรา 397 มีความเหมือนกันกับประเทศสหรัฐอเมริกาที่ใช้บทกฎหมาย U.S.C Chapter 110A Domestic Violence and Stalking มาตรา 2261A ที่นำมาปรับใช้เทียบเทียบ ซึ่งการพิจารณาองค์ประกอบความผิดนั้นก็เน้นการพิจารณาว่า ครบองค์ประกอบ และไม่จำเป็นต้องมีการกระทำคุกคามซ้ำๆ แต่อย่างใด โดยมีความมุ่งประสงค์ในการนำผู้กระทำผิดมาลงโทษทางอาญา เพื่อให้มีความยำเกรงกฎหมายในการลงโทษ ซึ่งแตกต่างกับประเทศออสเตรเลียต้องพิจารณาองค์ประกอบว่าการกระทำนั้นจะต้องเป็นการกระทำผิดซ้ำๆ ของการกระทำที่ต้องเป็นการกระทำผ่านสื่อทางอิเล็กทรอนิกส์ และเจตนามุ่งร้ายให้ผู้เสียหาย โดยเฉพาะในกลุ่มเด็กชาวออสเตรเลีย ตามกฎหมาย Enhancing Online Safety Act 2015 มาตรา 4 และ 5 ที่ว่า การกลั่น

แกล้งรังแกทางไซเบอร์ที่เหยื่อเป็นเด็กชาวออสเตรเลีย ซึ่งกฎหมายเน้นที่ลงโทษทางปกครอง โดยการพิจารณาบทลงโทษโดยการเสียค่าปรับ ทำสาธารณประโยชน์แก่สังคม

4. การนำผลประโยชน์จากการวิเคราะห์เปรียบเทียบดังกล่าว มาแก้ไขปรับใช้ให้เหมาะสมในการเป็นวิธีการมาตรการใหม่ก็น่าจะทำให้สามารถแก้ไขปัญหาของการใช้วิธีการและมาตรการการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ของประเทศไทยได้อย่างเหมาะสม คือ 1) การนำเพิ่มกฎหมายของประเทศออสเตรเลีย Enhancing Online Safety Act 2015 ที่มีการกำหนดนิยามทางกฎหมายการคุกคามทางไซเบอร์ไว้โดยเฉพาะ เจาะจง ตามมาตรา 4 และมาตรา 5 ดังกล่าวมาแก้ไขปรับใช้ในกฎหมายประเทศไทยโดยเฉพาะในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 2) นำเพิ่มหน่วยงานคณะกรรมการควบคุมความปลอดภัยทางอิเล็กทรอนิกส์ e-Safety Commissioner เช่นของประเทศออสเตรเลียเพื่อมาช่วยทำหน้าที่ประสานงานกับเจ้าหน้าที่ตำรวจไซเบอร์ในการให้มีการลบโพสต์ด้วยความรวดเร็ว 3) เพิ่มบทลงโทษทางปกครองตามกฎหมาย Enhancing Online Safety Act 2015 ประเทศออสเตรเลียที่กฎหมายสามารถ กำหนดให้มีบทลงโทษทางปกครองในกรณีฝ่าฝืนคำสั่งเจ้าหน้าที่ตำรวจไซเบอร์ ฉะนั้น หากนำประโยชน์จากการวิเคราะห์เปรียบเทียบดังกล่าวมาปรับใช้ให้เหมาะสมในการเป็นวิธีการหรือมาตรการใหม่ก็จะทำให้สามารถแก้ไขปัญหาได้อย่างเหมาะสมและมีประสิทธิภาพมากยิ่งขึ้น

ระบบกฎหมายไทยภายใต้มาตรการทางกฎหมายในการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ประเทศไทย ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 นั้นน่าจะยังไม่เพียงพอในการป้องกันภัยจากการถูกคุกคามทางไซเบอร์อยู่ ได้แก่ 1) ภัยคุกคามทางไซเบอร์นั้น นอกจากจะส่งผลกระทบต่อระบบคอมพิวเตอร์แล้ว ก็ยังส่งผลกระทบต่อผู้เสียหายที่เป็นเหยื่อที่ใช้ระบบคอมพิวเตอร์ด้วยแต่ว่ายังไม่มีการกำหนดนิยามความหมายไว้โดยเฉพาะ ฉะนั้น จึงควรที่จะให้มีการกำหนดนิยามความหมายทางกฎหมายเกี่ยวกับการกระทำคุกคามทางไซเบอร์ของประเทศไทยเป็นการเฉพาะเพื่อให้คุ้มครองป้องกันผู้เสียหายที่เป็นเหยื่อไว้ด้วย 2) หน่วยงานที่ใช้มาตรการการดำเนินคดีเกี่ยวกับการป้องกันภัยถูกคุกคามทางไซเบอร์ตามกฎหมายประเทศไทยนั้นมุ่งเน้นในการลงโทษทางอาญาอย่างเดียวซึ่งเป็นการแก้ไขปัญหาทางปลายเหตุ 3) บทลงโทษเกี่ยวกับการกระทำถูกคุกคามทางไซเบอร์ตามกฎหมายของประเทศไทยนั้นเป็นบทลงโทษทางอาญาซึ่งโทษไม่ร้ายแรง และก็ทำให้มีผู้กระทำผิดเพิ่มขึ้นอีก ทำให้เกิดปัญหาในการใช้วิธีการเพื่อการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ตามกฎหมายที่ไม่สามารถปฏิบัติงานให้เกิดประสิทธิภาพได้อย่างเต็มที่เหมาะสมได้ โดยพบว่า ประเทศออสเตรเลียมีกฎหมาย Enhancing Online Safety Act 2015 ตามมาตรา 4 และมาตรา 5 ซึ่งมีการกำหนดนิยามของคำว่า การกระทำคุกคามทางไซเบอร์เด็กเยาวชนไว้โดยเฉพาะเจาะจง และมีคณะกรรมการควบคุมความปลอดภัยทางอิเล็กทรอนิกส์ในการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ตามกฎหมาย (e-Safety Commissioner) ซึ่งสามารถนำมาปรับใช้เพื่อช่วยทำหน้าที่ประสานงานกับเจ้าหน้าที่ตำรวจไซเบอร์ในการให้มีการลบโพสต์และโพสต์ขอโทษได้ด้วยความรวดเร็วอันเป็นการเยียวยาจิตใจของผู้เสียหายโดยเฉพาะเด็กเยาวชนตามมาตรา 18 และ มาตรา 67 และ 3) ตามมาตรา 46

ที่มีการระบุบทลงโทษทางปกครองที่ให้เสียค่าปรับทางปกครองกับผู้ให้บริการและผู้ใช้บริการที่กระทำความผิดตามกฎหมาย ดังนั้น หากมีการนำวิธีการของประเทศออสเตรเลียดังกล่าวนี้นำมาแก้ไขปรับใช้ในการแก้ไขปัญหามาตรการการป้องกันภัยจากการถูกคุกคามทางไซเบอร์ตามกฎหมายของไทยก็น่าจะเป็นการเหมาะสมและสามารถปฏิบัติงานให้เกิดประสิทธิภาพได้มากยิ่งขึ้น

องค์ความรู้ที่ได้จากการศึกษา

1.ข้อดีและประโยชน์ ทำให้การตีความนิยามการกระทำการคุกคามทางไซเบอร์ ซึ่งยังไม่มีนิยามความ ให้สามารถมีนิยามความหมายขอบเขตองค์ประกอบที่ตีความได้ชัดเจน มีหน่วยงานเฉพาะทางไซเบอร์ให้บริการประสานงานโดยตรงที่จะเยียวยาความเสียหายทางจิตใจในการลบโพสต์และโพสต์ขอโทษ และมีบทลงโทษที่มีความเหมาะสมมากขึ้นนอกจากการลงโทษทางอาญากับผู้กระทำผิดแล้ว ก็ยังมีบทลงโทษทางปกครองในการเยียวยาลบโพสต์โดยรวดเร็วและการมีโทษปรับทางปกครองทั้งผู้ให้บริการและผู้กระทำผิดร่วมกันอีกด้วย ซึ่งถือว่า การป้องกันภัยจากการคุกคามทางไซเบอร์ในประเทศไทยแต่ต้นทางสาเหตุ

2.ข้อเสียของการแก้ไขปรับปรุงกฎหมาย เกิดค่าใช้จ่ายงบประมาณในการตั้งหน่วยงานอิสระในการประสานงานดังกล่าวเพิ่มอีกต่างหาก แต่ว่างบประมาณในส่วนนี้ก็ยังคงมีความน่าสนใจในอนาคตเพื่อที่จะเป็นส่วนที่ต่อยอดในการพัฒนาการป้องกันภัยคุกคามทางไซเบอร์ให้เพิ่มประสิทธิภาพมากขึ้น โดยเฉพาะเกี่ยวกับประเด็นปัญหาของการกระทำคุกคามทางไซเบอร์โดยเฉพาะรูปแบบของการปรากฏเว็บไซต์การพนันที่ปัจจุบันมีการเชื่อมต่ออัตโนมัติบนหน้าจออุปกรณ์โทรศัพท์มือถือหรือคอมพิวเตอร์ในขณะกำลังใช้งานอยู่ด้วย การตั้งโปรแกรมอัตโนมัติบนโลกสื่อออนไลน์ที่ส่งผลกระทบเสียหายทางเศรษฐกิจอย่างมาก เพราะถึงแม้ว่าจะมีการตั้งโปรแกรมอัตโนมัติ แต่ว่าการตั้งโปรแกรมดังกล่าวก็ยังคงต้องอาศัยการเชื่อมต่อเครือข่ายอินเทอร์เน็ตอยู่ ซึ่งหน่วยงานนี้ก็ยังสามารถควบคุมดูแลผ่านผู้ให้บริการอินเทอร์เน็ตได้ในส่วนหนึ่ง

เอกสารอ้างอิง

กชพรรณ มณีภาค, และอุนิษา เลิศโตมรสกุล. (2562). *การตกเป็นเหยื่ออาชญากรรมจากการกระทำผิดในโลกอินเทอร์เน็ต: กรณีศึกษาการรังแกกันในโลกไซเบอร์ ในรูปแบบการคุกคามทางเพศ ในเขตกรุงเทพมหานคร. วารสารวิจัยและพัฒนา มหาวิทยาลัยราชภัฏสวนสุนันทา, 11*(2), 3.

จิตติ ติงศภัทิย์. (2553). *คำอธิบายประมวลกฎหมายอาญาภาค 2 ตอน 2 และภาค 3* (พิมพ์ครั้งที่ 7). กรุงเทพฯ: ศูนย์การพิมพ์เพชรรุ่ง.

ปองกมล สุรัตน์. (2561). *การรังแกผ่านโลกไซเบอร์ในมิติสังคมวัฒนธรรม: กรณีศึกษาเยาวชนไทยเจเนอเรชั่น Z.* กรุงเทพฯ: มหาวิทยาลัยศรีนครินทรวิโรฒ.

พรรษาวดี คล้อยระยับ, และอุนิษา เลิศโตมรสกุล. (2564). *การป้องกันการตกเป็นเหยื่อคุกคามทางเพศของเด็กในโลกออนไลน์.* วารสารคุณภาพชีวิตกับกฎหมาย, 17(1), 33-47.

พินวา แสนใหม่. (2563). *การรังแกทางไซเบอร์ สาเหตุและแนวทางการจัดการปัญหา* (วิทยานิพนธ์ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์). สถาบันบัณฑิตพัฒนบริหารศาสตร์, กรุงเทพมหานคร.

มูลนิธิส่งเสริมสื่อเด็กและเยาวชน (สสย.). (2563). *การรักษาความปลอดภัยบนโลกไซเบอร์ (Cybersecurity)* (พิมพ์ครั้งที่ 3). กรุงเทพฯ: วอล์ค ออน คลาวด์.

เมธาพันธ์ ประยงค์พันธ์ และสิริชัย ดีเลิศ. (2563). *ผลกระทบของภัยคุกคามทางโลกออนไลน์ที่ส่งผลต่อผู้ใช้สื่อสังคมออนไลน์.* รายงานการวิจัย. กรุงเทพมหานคร: คณะวิทยาการจัดการ มหาวิทยาลัยศิลปากร.

รักข์ษิตา โพธิ์พิทักษ์กุล. (2550). *มาตรการทางกฎหมายเกี่ยวกับการคุกคามทางอินเตอร์เน็ต* บัณฑิตวิทยาลัย : มหาวิทยาลัยกรุงเทพ,

สมยศ เชื้อไทย. (2555). *หลักกฎหมายกฎหมายมหาชนเบื้องต้น* (พิมพ์ครั้งที่ 8).กรุงเทพฯ:วิญญูชน.

สาวตรี สุขศรี. (2555). *ผลกระทบจากพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น.* กรุงเทพมหานคร: โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชนในมูลนิธิอาสาสมัครเพื่อสังคม.

สาวตรี สุขศรี. (2563). *กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์* (พิมพ์ครั้งที่ 2). กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์.

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร คณะทำงานการจัดการความรู้ สำนักงานเลขาธิการวุฒิสภา. (2559). *องค์ความรู้เรื่องการป้องกันภัยทางคอมพิวเตอร์.* กรุงเทพมหานคร: สำนักเทคโนโลยีสารสนเทศและการสื่อสาร คณะทำงานการจัดการความรู้ สำนักงานเลขาธิการวุฒิสภา.

สุธาเทพ รุณเรศ. (2561). *ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร* บัณฑิตวิทยาลัย : มหาวิทยาลัยธรรมศาสตร,

อัมพร ธำรงลักษณ์. (2552). *การคุกคามทางเพศในโรงเรียนมัธยมศึกษาในเขตกรุงเทพมหานคร: สาเหตุและข้อเสนอทางนโยบาย. วารสารวิชาการ มหาวิทยาลัยราชภัฏบุรีรัมย์, 1*(1),31-47.

Graham, S., & Wood, D. (2003). Digitizing surveillance: Categorization, space, inequality. *Critical Social Policy, 23*(2), 227-248.

Lee, V. E., Croninger, R. G., Linn, E., & Chen, X. (1996). The culture of sexual harassment in secondary schools. *American Educational Research Journal, 33*(2), 383-417.

Mullen, Paul E. et al. (1999). Study of stalker. *The American Journal of Psychiatry, 156*(8), 1244-1249.