มาตรการทางกฎหมายภัยคุกคามทางไซเบอร์

LEGAL MEASURES FOR CYBER THREATS

พันธุ์ทิพย์ นวานุช[1*], อำพล กองเขียว[2] และ ทองเลื่อน วิเชียรผลา[3]
PUNTHIP NAVANUCH[1*], AMPHOL KONGKEAW[2] and THONGLUAN WICHIANPHLA[3]

บทคัดย่อ

ปัจจุบันการพัฒนาด้านเทคโนโลยี กลายเป็นช่องทางในการประกอบอาชญากรรมทางเทคโนโลยีในหลายรูปแบบถือเป็นภัยคุกคามทางไซเบอร์ ซึ่งจากข้อมูลสถิติการแจ้งความเกี่ยวกับอาชญากรรมทางเทคโนโลยี ตั้งแต่วันที่ 1 มีนาคม 2565 ถึงวันที่ 6 กุมภาพันธ์ 2566 มีจำนวนผู้แจ้งความทั้งสิ้น 192,031 คดี รวมความเสียหายถึง 100 ล้านบาท ด้วยเหตุที่เป็นอาชญากรรมที่มีวิวัฒนาการอย่างรวดเร็ว และหลากหลายรูปแบบ จึงเกิดแนวทางที่จะพัฒนา ป้องกันและปราบปรามอาชญากรรมเหล่านี้ โดยมีมาตรการทางกฎหมายหลายฉบับ เข้ามามีบทบาท เช่น กฎหมายมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี กฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ และอื่น ๆ แต่อย่างไรก็ดี แม้จะมีมาตรการทางกฎหมายที่เกี่ยวข้องกับการป้องกันภัยคุกคามทางเทคโนโลยีหลายฉบับ แต่ก็ไม่สามารถป้องกันและปราบปรามได้อย่างมีประสิทธิภาพ จึงมีความจำเป็นต้องพัฒนากฎหมายดังกล่าว รวมทั้งพัฒนาบุคลากรภาครัฐและภาคเอกชนให้มีทักษะ ความรู้ ความสามารถ เท่าทันต่อสถานการณ์อาชญากรรมทางเทคโนโลยีอันเป็นภัยคุกคามทางไซเบอร์

คำสำคัญ : มาตรการทางกฎหมาย ; ภัยคุกคามไซเบอร์

ABSTRACT

Nowadays, technology development became a way to engage in many forms of technological crime. Considered a cyber threat according to statistical data, notification of technological crimes From 1 March 2022 to 6 February 2023, a total of 192,031 cases were reported, totaling 100 million baht in damage due to a rapidly evolving crime. And various forms therefore creating guidelines to develop prevent and suppress. These crimes with many legal measures taking over roles such as law, preventive measures and suppression of technological crimes security, cyber security, and others. However, despite the legal measures related to the prevention of many technological threats. But cannot prevent and subduesuppress effectively. Therefore it is necessary to develop the

[1] ผู้ช่วยศาสตราจารย์ ดร., อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยนอร์ท-เชียงใหม่, Assistant Professor Dr., Faculty of Law, North-Chiangmai University.
[2] อาจารย์, อาจารย์ประจำคณะวิศวกรรมศาสตร์และเทคโนโลยี มหาวิทยาลัยนอร์ท-เชียงใหม่, Lecturer, Faculty of Engineering and Technology, North-Chiangmai University.
[3] ทนายความ, Lawyer, Lawyers Council of Thailand.
[*] Corresponding Author, Email: kungnang2555@hotmail.com
Received: Oct 19, 2023, Revised: Dec 10, 2023, Accepted: Dec 14, 2023

said law. Including the development of government and private personnel to have the same knowledge skills as technological crime situations that are cyber threats.

Keywords: Legal Measures ; Cyber Threats

บทนำ

องค์กรต่างๆ มีการปรับเปลี่ยนกลยุทธ์เพื่อพัฒนาให้เท่าทันสถานการณ์ที่เป็นสากล โดยพัฒนาทางด้านเทคโนโลยีที่มีความล้ำสมัยและขีดความสามารถ ส่งผลให้สามารถเข้าถึงได้อย่างสะดวกรวดเร็วกลายเป็นช่องว่างให้ผู้กระทำความผิดที่แฝงตัวเข้าไปใช้เทคโนโลยีในการประกอบอาชญากรรมในหลากหลายรูปแบบ เช่น การรขอรหัสผ่าน การใช้งานบัญชีอีเมล การแอบอ้างเป็นบุคคลต่างๆ การหลอกว่าจะโอนเงินหรือสิ่งของให้เหยื่อ การโฆษณาปล่อยเงินกู้นอกระบบ การหลอกให้ร่วมลงทุน การหลอกซื้อขายของออนไลน์ (กรฉัตร มารตศรี และคณะ, 2565) การกระทำดังกล่าวนี้เกิดจากการพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเทคโนโลยีที่มีการใช้มากที่สุด คือ การใช้อินเตอร์เน็ต ไม่ว่าจะเป็นการส่งเสริมการศึกษา การสร้างธุรกิจใหม่ๆ ด้านสุขภาพ ตลอดจนการขนส่งคมนาคมโลจิสติกส์ การใช้เทคโนโลยีในการขับเคลื่อนไปสู่เศรษฐกิจดิจิทัล แต่การพัฒนาด้านเทคโนโลยีก็ถือว่ายังมีช่องว่างในการใช้เป็นเครื่องมือในการเกิดภัยคุกคามไซเบอร์ และอาชญากรรมไซเบอร์ (กรกัญญารัก บุญสุขเกิด, 2564)

ไซเบอร์ หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเตอร์เน็ตหรือเครือข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียม และระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

อาชญากรรมไซเบอร์ คือ อาชญากรรมที่กระทำความผิดในระบบคอมพิวเตอร์ หรือการใช้คอมพิวเตอร์เพื่อกระทำความผิด รวมถึงกระทำความผิดในเครือข่ายคอมพิวเตอร์และอุปกรณ์ที่เชื่อมต่อกับเครือข่ายคอมพิวเตอร์ (อัญชลี จวงจันทน์, 2562) โดยอาชญากรรมไซเบอร์มี 2 ลักษณะ คือ การก่ออาชญากรรมที่มีผลต่อวัตถุ เช่น การทำลายข้อมูลซอฟต์แวร์ การเรียกค่าไถ่ทางคอมพิวเตอร์ และการก่ออาชญากรรมที่มีผลต่อจิตใจ เช่น การข่มขู่ให้หวาดกลัว การหลอกให้รัก การฉ้อโกงผ่านอินเตอร์เน็ต ไม่ว่าจะเป็นการหลอกขายสินค้าออนไลน์ การกู้เงินออนไลน์ การหลอกให้ลงทุนในรูปแบบต่างๆ หลอกให้ดาวน์โหลดโปรแกรม หลอกลวงผ่านอีเมล การพนันออนไลน์ เป็นต้น (ปรเมศวร์ กุมารบุญ, 2565) ข้อมูลสถิติการแจ้งความอาชญากรรมทางเทคโนโลยี ตั้งแต่วันที่ 1 มีนาคม 2565 ถึงวันที่ 6 กุมภาพันธ์ 2566 มีจำนวนผู้แจ้งความ 192,031 คดี มีความเสียหายถึง 100 ล้านบาท (สปริงนิวส์, 2565)

สำหรับมาตรการในการป้องกันภัยคุกคามไซเบอร์ได้มีกฎหมายที่เกี่ยวข้องอยู่หลายฉบับ แต่ว่าวิวัฒนาการที่มีหลายรูปแบบของอาชญากรรมไซเบอร์ ซึ่งส่งผลกระทบได้รวดเร็วและเป็นวงกว้าง ตลอดจนมีการพัฒนารูปแบบของอาชญากรรมไปตามความก้าวหน้าทางเทคโนโลยี จึงเป็นที่มาของการรวบรวมมาตรการทางกฎหมายภัยคุกคามไซเบอร์ เพื่อนำไปเป็นแนวทางพัฒนามาตรการป้องกันต่อไป

อาชญากรรมไซเบอร์

เพื่อประโยชน์ในการทำความเข้าใจมาตรการทางกฎหมายภัยคุกคามไซเบอร์ จึงจำเป็นที่จะต้องเริ่มตั้งแต่การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งได้มีการพัฒนาไปพร้อมๆ กับวิวัฒนาการของเทคโนโลยี เพื่อเป็นการรับมือกับอาชญากรรมในรูปแบบใหม่ๆ ที่อาศัยเทคโนโลยีเป็นเครื่องมือในการกระทำความผิด จึงได้มีการพัฒนากฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ โดยคอมพิวเตอร์ที่ถูกใช้ในการกระทำความผิดมี 2 ลักษณะ คือ ถูกใช้เป็นเครื่องมือ และถูกใช้ในฐานะที่เป็นอุปกรณ์หรือช่องทางในการเก็บรักษา รับ-ส่งข้อมูลข่าวสาร ซึ่งในระยะแรกๆ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์จะเป็นเรื่องเกี่ยวกับสิทธิส่วนบุคคลและข้อมูลข่าวสารส่วนบุคคล (ณัฐสุดา อัคราวัฒนา, ม.ป.ป.) และเพื่อเป็นการรับมือกับอาชญากรรมในรูปแบบใหม่ๆ ที่กระทำผ่านทางเทคโนโลยี จึงได้มีการพัฒนากฎหมายอาชญากรรมทางคอมพิวเตอร์และกฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

อาชญากรรมทางเทคโนโลยี หมายความว่า การกระทำหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำ

ความผิดเกี่ยวกับคอมพิวเตอร์เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์บุคคลใดบุคคลหนึ่ง หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้คอมพิวเตอร์เป็นเครื่องมือ (พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566) ทั้งนี้ เพื่อคุ้มครองประชาชนผู้สุจริตซึ่งถูกหลอกลวงจนสูญเสียทรัพย์สินโดยผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ ซึ่งแต่ละวันจะมีผู้ถูกหลอกลวงจำนวนมากและมีมูลค่าความเสียหายสูงมาก และอาชญากรรมที่กระทำความผิดในระบบคอมพิวเตอร์หรือใช้คอมพิวเตอร์เพื่อกระทำความผิด เรียกการกระทำเช่นนี้ว่าอาชญากรรมไซเบอร์

คดีอาชญากรรมไซเบอร์นั้น มีโอกาสเกิดขึ้นได้ตลอดเวลา เพียงแค่ประชาชนสามารถเข้าถึงอินเตอร์เน็ตก็สามารถตกเป็นเหยื่ออาชญากรรม ซึ่งชักจูงใจด้วยความโลภของมนุษย์ ทำให้คดีอาชญากรรมไซเบอร์มีแนวโน้มสูงขึ้น และอาชญากรมักจะพัฒนารูปแบบในการกระทำความผิด เพื่อให้สามารถบรรลุวัตถุประสงค์ในการกระทำความผิดตลอดเวลา

แนวคิดภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยไม่ชอบ โดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ เพื่อมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง (พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562) ส่วนไซเบอร์ หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการใช้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ระบบอินเตอร์เน็ต หรือโครงข่ายโทรคมนาคม

การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ (พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

ภัยคุกคามไซเบอร์นั้น มีวิวัฒนาการหลายรูปแบบซึ่งส่งผลกระทบได้อย่างรวดเร็วและเป็นวงกว้าง โดยไม่จำเป็นต้องใช้ผู้กระทำความผิดจำนวนมาก ซึ่งในปัจจุบันก็มีการกระทำความผิดที่พัฒนารูปแบบมากขึ้นเรื่อยๆ ตามความก้าวหน้าของเทคโนโลยี โดยเริ่มจากการกระทำความผิดต่อสิทธิส่วนบุคคลหรือข้อมูลส่วนบุคคล ในยุคแรกๆ มีการใช้คอมพิวเตอร์เป็นอุปกรณ์ในการเก็บบันทึก ถ่ายทอด และเชื่อมโยงฐานข้อมูลเข้าด้วยกัน ต่อมาจะเป็นการกระทำความผิดโดยใช้คอมพิวเตอร์ในการหลอกลวง โดยอาศัยข้อมูลเปลี่ยนแปลงคอมพิวเตอร์ ซึ่งการกระทำความผิดจะมีวิวัฒนาการคล้ายกันตามการพัฒนาของระบบคอมพิวเตอร์ เริ่มจากการขโมยข้อมูลส่วนบุคคล การขโมยข้อมูลทางการเงินเพื่อปลอมแปลงตัวเลขและยักยอกเงิน การเจาะระบบของหน่วยงานราชการหรือภาคธุรกิจ เช่น การพนันออนไลน์ การหลอกขายของออนไลน์ การขโมยข้อมูลบัตรกดเงิน การเผยแพร่ข้อมูลทางระบบคอมพิวเตอร์ที่ผิดกฎหมาย แก๊งค์คอลเซ็นเตอร์ จะเห็นได้ว่าวิวัฒนาการอาชญากรรมไซเบอร์นี้เป็นภัยคุกคามหนึ่งของประเทศ

ประเภทภัยคุกคามอาชญากรรมไซเบอร์

1. เนื้อหาที่เป็นภัยคุกคาม คือ ภัยคุกคามที่เกิดจากการใช้เผยแพร่ข้อมูลที่ไม่เป็นจริง หรือไม่เหมาะสม เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบหรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามกอนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่างๆ ทางอีเมล ที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณา

2. โปรแกรมไม่พึงประสงค์ คือ ภัยคุกคามที่เกิดจากโปรแกรมที่ถูกพัฒนาขึ้น เพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบเพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมประสงค์ร้ายนี้ติดตั้งอยู่

3. ความพยายามรวบรวมข้อมูลของระบบ คือ ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี ด้วยการเรียกใช้บริการต่างๆ ที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน และการล่อลวงหรือเล่ห์กลต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ

4. ความพยายามจะบุกรุกเข้าระบบ คือ ภัยคุกคามที่เกิดจากความพยายามที่จะบุกรุกเอาเข้าระบบทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะภัยคุกคามนี้รวมถึงความ

พยายามจะบุกรุก เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสด้วยวิธีการสุ่มหรือเดาข้อมูล

5. การบุกรุกหรือเจาะระบบได้สำเร็จ คือ ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก เจาะเข้าระบบได้สำเร็จ และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

6. การโจมตีสภาพความพร้อมใช้งานของระบบ คือ ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่างๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการ จนกระทั่งระบบไม่สามารถให้บริการต่อไปได้

7. การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต คือ ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญหรือเปลี่ยนแปลงแก้ไขข้อมูล

8. การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ คือ ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกง หรือหลอกลวงเพื่อผลประโยชน์ สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศน์ที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าตลอดจนการละเมิดลิขสิทธิ์ (กรกัญญ์ญารัก บุญสุขเกิด, 2564)

ข้อควรระวังป้องกันภัยคุกคาม

1. การหลอกลวง เป็นการหลอกลวงที่ทำได้อย่างแนบเนียนด้วยเทคโนโลยี ด้วยการใช้ปัญญาประดิษฐ์ (AI) ในการสร้างคอนเทนท์ปลอม เช่น การตัดต่อใบหน้าของผู้มีชื่อเสียงเข้าไปแทนหน้าตัวเองในวิดีโอ ทำให้ผู้ไม่ประสงค์ดีสามารถนำคนมีชื่อเสียงไปหลอกลวงผู้อื่นตามความต้องการได้ เนื่องจากปัญญาประดิษฐ์หรือ AI มีความสามารถเก็บข้อมูล ประมวลผลวิเคราะห์และเรียนรู้สิ่งต่างๆ ได้ดี

2. การสร้างความเชื่อ คือ การสร้างข่าวโดยใช้ส่วนหนึ่งของความจริง เพื่อเปลี่ยนแปลงความคิดของคน เช่น การ์ตูนล้อเลียน เสียดสีการเมืองจากเพจต่างๆ ซึ่งข่าวเหล่านี้จะน่าเชื่อถือเพราะมีฐานมาจากความจริง ส่งผลกระทบต่อเป้าหมาย บุคคลหรือองค์กร มักมีเป้าหมายเพื่อดิสเครดิต

3. อธิปไตยไซเบอร์และระบบความปลอดภัยแห่งชาติ คือ อธิปไตยไซเบอร์เกิดขึ้นจากข้อมูลส่วนบุคคลที่สับสนบนโลกออนไลน์ ไม่ว่าจะเป็นแพลตฟอร์มใดก็ตาม เจ้าของแพลตฟอร์มอาจนำไปศึกษาวิเคราะห์เพื่อประโยชน์ในการศึกษาพฤติกรรมของผู้ใช้แต่ละราย เพื่อนำเสนอสินค้าและให้บริการเข้าถึงผู้ใช้โดยตรง นับเป็นการรุกล้ำความเป็นส่วนตัว ซึ่งเรียกว่า อธิปไตยไซเบอร์ (ELEADER อ้างในกัญญ์ญารัก บุญสุขเกิด, 2564)

แนวทางการป้องกันอาชญากรรมทางไซเบอร์

1. ด้านบุคคล

1.1 ควรเพิ่มความระมัดระวังในการใช้บริการอินเทอร์เน็ต เว็บไซต์ หรือโซเชียลมีเดียต่างๆ ไม่ควรเข้าเว็บไซต์แปลกๆ หรือมีความเสี่ยงจะขโมยข้อมูลส่วนบุคคล รวมทั้งควรตั้งโปรไฟล์ให้มีความเป็นส่วนตัว ไม่ควรใช้ข้อมูลส่วนตัวมากเกินไป เช่น Facebook ไม่ควรมีการลงข้อมูลส่วนบุคคล เช่น เลขบัญชี เป็นต้น

1.2 ควรตั้งรหัสความปลอดภัยในอุปกรณ์ทางคอมพิวเตอร์หรือที่ต้องเชื่อมโยงอินเตอร์เน็ตต่าง ๆ รวมทั้งโทรศัพท์มือถือ ควรตั้งรหัสที่คาดเดายาก และไม่ควรใช้รหัสเหมือนกัน เพราะจะง่ายต่อการเจาะข้อมูล

1.3 ควรมีการติดตามข่าวสารที่เกี่ยวกับอาชญากรรมทางไซเบอร์หรือแม้แต่การแชร์ข้อมูล ควรมีการตรวจสอบข้อเท็จจริงก่อนแชร์ต่อสาธารณะ หรือส่งต่อผู้อื่น

2. ด้านภาครัฐและหน่วยงานที่เกี่ยวข้อง

2.1 เสริมสร้างความรู้ให้แก่ประชาชน เช่น การรู้จักปัญหาอาชญากรรมทางไซเบอร์ การให้ความรู้พื้นฐานแก่ประชาชน

2.2 การประชาสัมพันธ์ข้อมูลข่าวสารแก่ประชาชนให้สามารถเข้าถึงได้ง่าย เช่น ข่าวเกี่ยวกับอาชญากรรมทั้งภายในประเทศและภายนอกประเทศ

2.3 การตั้งศูนย์หรือหน่วยงานเฉพาะในการตรวจสอบดูแลเรื่องปัญหาอาชญากรรมทางไซเบอร์ รวมถึงข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัยทางคอมพิวเตอร์

2.4 เสริมความรู้หรือทักษะแก่เจ้าหน้าที่ในเรื่องเกี่ยวกับอาชญากรรมทางไซเบอร์ ความรู้เกี่ยวกับระบบคอมพิวเตอร์ และอื่นๆ ที่เกี่ยวข้อง โดยควรมีการเสริมสร้างทักษะในทุกๆ ปี เพื่อได้ศึกษาพัฒนาการอาชญากรรมทางไซเบอร์และพัฒนาการของเทคโนโลยี

2.5 การวางระบบป้องกันเกี่ยวกับอาชญากรรมทางไซเบอร์ เช่น ระบบการตรวจสอบ ระบบการป้องกันให้กับหน่วยงานภาครัฐและส่งเสริมภาคเอกชน

2.6 ด้านกฎหมาย มีการพัฒนากฎหมายให้ครอบคลุมและทันต่อการพัฒนาของอาชญากรรมทางไซเบอร์ และมีการกำหนดโทษที่เด็ดขาด เหมาะสมกับความผิด

2.7 การพัฒนาระบบ การดำเนินคดีที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ มีหน่วยงานที่ตรวจสอบได้อย่างรวดเร็ว การจับกุม การดำเนินคดี และระบบศาลที่รวดเร็วและมีประสิทธิภาพ

วิธีป้องกันตัวเองให้ปลอดภัยจากอาชญากรรมทางไซเบอร์

อาชญากรรมทางไซเบอร์มีแนวโน้มจะทำความรุนแรงมากขึ้นทุก ๆ ปี องค์กรผู้นำด้านวิจัยและเก็บรวบรวมสถิติด้านนี้คาดการณ์ว่า มูลค่าความเสียหายจากอาชญากรรมทางไซเบอร์อาจพุ่งสูงถึงร้อยละ 15 ต่อปี ดังนั้นทางภาคธุรกิจและผู้บริโภคจึงควรปฏิบัติดังนี้ สำหรับหน่วยงานและองค์กรต่างๆ ควรเร่งดำเนินการอย่างต่อเนื่อง คือ การเก็บบันทึก แบคอัพข้อมูลที่สำคัญของบริษัทเป็นประจำ หากเกิดเหตุฉุกเฉินซึ่งจะได้กู้คืนกลับมาอย่างง่ายดาย นอกจากนี้ควรหมั่นอัพเดตซอฟต์แวร์และระบบปฏิบัติการให้ทันสมัยอยู่เสมอ รวมถึงจัดอบรม ฝึกสอนพนักงานให้รู้เท่าทันภัยออนไลน์ เช่น วิธีสังเกตว่าอีเมลใดเข้าข่ายเป็นกลลวง นอกจากนี้ยังอาจลองพิจารณาทำประกันความเสียหายจากอาชญากรรมทางไซเบอร์ เป็นต้น สำหรับประชาชนทั่วไป สื่อชั้นนำระดับโลกได้ให้คำแนะนำในการป้องกันตัวไว้ เช่น การหมั่นอัพเดตซอฟต์แวร์ทางคอมพิวเตอร์และอุปกรณ์ไอทีอื่นๆ พยายามตั้งพาสเวิร์ดที่คาดเดาได้ยาก และหลีกเลี่ยงการใช้พาสเวิร์ดเก่าซ้ำอีกครั้ง อย่าแชร์ข้อมูลส่วนตัวบนโลกออนไลน์หรือเล่นเกม และ ควิซ ตอบคำถามจากเว็บไซต์ที่ดูไม่น่าเชื่อถือ รวมถึงความระมัดระวังตัวไม่หลงเชื่อหรือคลิกลิ้งค์อะไรง่าย ๆ เป็นต้น (ระบบออนไลน์)

ความมั่นคงปลอดภัยทางไซเบอร์

ความมั่นคงปลอดภัย คือ สถานะที่มีความปลอดภัยไร้กังวล อยู่ในสถานะที่ไม่มีอันตราย และได้รับการป้องกันอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือโดยบังเอิญ องค์กรควรมีความมั่นคงปลอดภัย ดังนี้

1. ความมั่นคงปลอดภัยทางกายภาพ เป็นการป้องกันสิ่งใดๆ ทางกายภาพ ไม่ว่าจะเป็นสิ่งของ สถานที่ หรือพื้นที่ใดๆ ขององค์กร จากการเข้าถึงที่ไม่ได้รับอนุญาตหรือการนำไปใช้ในทางที่ผิด

2. ความมั่นคงปลอดภัยส่วนบุคคล เป็นการป้องกันที่มีส่วนเกี่ยวข้องกับบุคคลหรือกลุ่มคน

3. ความมั่นคงปลอดภัยในการปฏิบัติการ เป็นการป้องกันรายละเอียดต่างๆ ของกิจกรรม

4. ความมั่นคงปลอดภัยในการติดต่อสื่อสาร เป็นการป้องกันสื่อสารที่ใช้ในการติดต่อสื่อสาร รวมถึงเทคโนโลยีที่ใช้และเนื้อหาหรือข้อมูลที่ถูกส่งไปสื่อตามสัญญาณดังกล่าวแล้ว

5. ความมั่นคงปลอดภัยของเครือข่าย เป็นการป้องกันองค์ประกอบการเชื่อมต่อและข้อมูลในเครือข่ายคอมพิวเตอร์

6. ความมั่นคงปลอดภัยของสารสนเทศ เป็นการป้องกันภัยสารสนเทศในระบบคอมพิวเตอร์ (ชฎาพร สิงห์แก้ว, 2564)

กฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติฉบับนี้ตราขึ้น เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการ และการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใดๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จ หรือมีลักษณะลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน จึงมีการกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว

2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ 2 พ.ศ. 2560 การแก้ไขเพิ่มเติมพระราชบัญญัติฉบับนี้ เนื่องจากมีบทบัญญัติบางประการไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในปัจจุบันซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้น ตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็ว โดยมีการกำหนดฐานความผิดขึ้นใหม่และแก้ไขเพิ่มเติมกำหนดเพิ่มเติมฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลายหรือลบล้างข้อมูลคอมพิวเตอร์

3. พระราชบัญญัติว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เพื่อรองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อันเป็นการรองรับนิติสัมพันธ์ต่างๆ ซึ่งแต่เดิมอาจจะจัดทำขึ้นในรูปแบบของหนังสือ ให้เท่าเทียมกับนิติสัมพันธ์รูปแบบอิเล็กทรอนิกส์ รวมตลอดทั้งการลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ และการรับฟังพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

4. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 เหตุผลในการตราพระราชกำหนดฉบับนี้ เนื่องจากปัจจุบันมีการใช้วิธีการทางเทคโนโลยีหลอกลวงประชาชนทั่วไปผ่านอุปกรณ์อิเล็กทรอนิกส์ต่างๆ จนทำให้ประชาชนสูญเสียทรัพย์สินเป็นจำนวนมาก และผู้หลอกลวงได้โอนทรัพย์สินที่ได้จากการกระทำผิดดังกล่าวนั้นผ่านบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลอื่นต่อไปเป็นทอดๆ อย่างรวดเร็ว เพื่อปกปิดหรืออำพรางการกระทำความผิด ซึ่งแต่ละวันประชาชนผู้สุจริตถูกหลอกลวงจำนวนมาก และมีมูลค่าความเสียหายสูง และการหลอกลวงดังกล่าวมีการกระทำที่เกิดขึ้น ส่งผลกระทบต่อประชาชนในวงกว้าง และเป็นอันตรายร้ายแรงต่อระบบเศรษฐกิจของประเทศ เพื่อประโยชน์อันที่จะต้องมีมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีดังกล่าว เพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในเศรษฐกิจของประเทศ

5. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เหตุผลในการตราพระราชบัญญัติฉบับนี้ เนื่องจากปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์อินเตอร์เน็ต โครงข่ายโทรคมนาคมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันอาจกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ เพื่อให้สามารถป้องกันหรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควรกำหนดภารกิจหรือบริการที่มีความสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

6. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ เนื่องจากกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ยังไม่มีบทบัญญัติรองรับในเรื่องตราประทับอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่สามารถระบุถึงตัวผู้กระทำธุรกรรมทางอิเล็กทรอนิกส์ได้ เช่นเดียวกับลายมือชื่ออิเล็กทรอนิกส์ ทำให้เป็นอุปสรรคต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ที่ต้องมีการประทับตราในหนังสือเป็นสำคัญ รวมทั้งยังไม่มีบทบัญญัติที่กำหนดให้สามารถนำเอกสารซึ่งเป็นสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์มาใช้แทนต้นฉบับหรือเป็นพยานหลักฐานในศาลได้ จึงมีการแก้ไขเพิ่มเติมเพื่อให้สอดคล้องกับหลักการดังกล่าว

7. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก จนสร้างความเดือดร้อนรำคาญและความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าทางเทคโนโลยีทำให้การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม จึงได้ตราพระราชบัญญัติฉบับนี้ขึ้นเพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป

บทวิเคราะห์

สืบเนื่องจากการพัฒนาทางเทคโนโลยี ส่งผลให้เกิดการพัฒนาในด้านต่างๆ ตลอดจนเข้ามาเพิ่มความสะดวกสบายในชีวิตประจำวันของคนทั่วไป แต่สิ่งที่ตามมาอย่างหลีกเลี่ยงไม่ได้ คือ อาชญากรรมทางเทคโนโลยีไซเบอร์ เป็นการทุจริตหลอกลวงที่เกิดขึ้นบนโลกอินเตอร์เน็ต และช่องทางออนไลน์ประเภทต่างๆ ไม่ว่าจะเป็นเว็บไซต์ แพลตฟอร์ม โซเชียลมีเดีย หรือแอพพลิเคชั่นบนมือถือ เพื่อแสดงให้เห็นถึงบทบัญญัติที่เป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์โดยตรง เพื่อให้เกิดความชัดเจนและเป็นหลักประกันในการบังคับใช้โดยทำการวิเคราะห์การกำหนดความรับผิดทางอาญากับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

มาตรา 5 “ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกัน การเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ”

มาตรา 7 “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะและมาตรการนั้นมิได้มีไว้

สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ”

มาตรา 8 “ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบ คอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคล ทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

มาตรา 9 “ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

มาตรา 10 “ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

จากบทบัญญัติมาตรา 5 และมาตรา 7 เป็นความผิดฐานเข้าสู่ระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์โดยมิชอบ ซึ่งมีองค์ประกอบความผิด คือ การที่บุคคลใดบุคคลหนึ่ง ผู้ซึ่งไม่มีอำนาจได้เข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตนโดยชอบตามมาตรา 5 ส่วนมาตรา 7 เป็นเรื่องที่บุคคลหนึ่งบุคคลใด ผู้ซึ่งไม่มีอำนาจได้เข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตนโดยเจตนา จะเห็นได้ว่าทั้งสองความผิดนี้แยกกันอย่างชัดเจน โดยแยกเป็นการเข้าถึงระบบคอมพิวเตอร์และการเข้าถึงข้อมูลคอมพิวเตอร์

บทบัญญัติมาตรา 8 เป็นความผิดฐานดักจับข้อมูลคอมพิวเตอร์โดยมิชอบ จึงมีองค์ประกอบความผิด คือ การที่บุคคลหนึ่งบุคคลใด ผู้ซึ่งไม่มีอำนาจได้กระทำด้วยประการใดๆ โดยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อบุคคลทั่วไป อย่างไรก็ดี การดักจับข้อมูลคอมพิวเตอร์ของผู้อื่นนี้จะต้องเป็นข้อมูลที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ ดังนั้นจึงไม่หมายความรวมถึงข้อมูลคอมพิวเตอร์ที่จัดเก็บในรูปแบบซีดีหรือดิสก์เก็ต นอกจากนี้ ยังต้องเป็นข้อมูลคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้หรือไม่ ซึ่งต้องพิจารณาจากข้อเท็จจริงว่าลักษณะการส่งข้อมูลคอมพิวเตอร์ดังกล่าวนั้น ผู้ส่งต้องการให้เป็นเรื่องเฉพาะตนไม่ต้องการให้เปิดเผยข้อมูลนั้นแก่ผู้ใดหรือไม่

บทบัญญัติมาตรา 9 เป็นความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์โดยมิชอบ ซึ่งมีองค์ประกอบความผิด คือ การที่บุคคลหนึ่งบุคคลใด ซึ่งไม่มีอำนาจ ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยเจตนา

ส่วนบทบัญญัติมาตรา 10 เป็นความผิดฐานกระทำโดยมิชอบต่อระบบคอมพิวเตอร์ ซึ่งมีองค์ประกอบความผิด คือ การที่บุคคลหนึ่งบุคคลใด ซึ่งไม่มีอำนาจกระทำการโดยเจตนา เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ

เมื่อพิจารณาถึงสภาพปัญหาอาชญากรรมทางไซเบอร์จะเห็นได้ว่าเปลี่ยนแปลงไปรวดเร็วมากตามการพัฒนาเปลี่ยนแปลงทางเทคโนโลยี ก่อให้เกิดความเสียหายอย่างมหาศาล ส่งผลกระทบในวงกว้างและยังพบว่าการกระทำความผิดในลักษณะนี้สามารถทำจากที่ไหนก็ได้ เพราะเครือข่ายอินเทอร์เน็ตนั้นเชื่อมโยงกันทั่วโลก ดังนั้น จึงมีอาอาชญากรไซเบอร์ที่กระทำความผิดในต่างประเทศ ซึ่งไม่สามารถนำพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งจะใช้บังคับได้ ต้องอาศัยกฎหมายระหว่างประเทศและอนุสัญญาระหว่างประเทศที่ประเทศไทยเข้าร่วมเป็นภาคีสมาชิกอยู่ด้วย ทำให้การบังคับใช้กฎหมายในด้านการป้องกันและปราบปรามการกระทำความผิดในลักษณะที่มีข้อจำกัดและยังไม่เกิดประสิทธิภาพดีเท่าที่ควร

ความผิดเกี่ยวกับความผิดเรื่องการเข้าถึงข้อมูลทางคอมพิวเตอร์โดยมิชอบนี้ยังไปเกี่ยวข้องกับการกระทำข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการทำธุรกรรมอิเล็กทรอนิกส์ ตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551 มาตรา 25 ประกอบมาตรา 3 ตามพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2553 เป็นกฎหมายที่ตราขึ้นมาเนื่องจากปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสาร ได้เข้ามามีบทบาทสำคัญต่อการดำเนินการทั้งภาครัฐและภาคเอกชน โดยมีการทำธุรกรรมทางอิเล็กทรอนิกส์กันอย่างแพร่หลาย จึงมีการส่งเสริมให้มีการบริหารจัดการและรักษาความปลอดภัยของ

ทรัพย์สินสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์เพื่อให้มีการยอมรับและเชื่อมั่นในข้อมูลทางอิเล็กทรอนิกส์มากยิ่งขึ้น ประกอบกับมาตรา 25 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ที่บัญญัติให้ธุรกรรมทางเล็กทรอนิกที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกานี้ ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้ (ธนนท์ทัส สุธริยานิติภักดี, ม.ป.ป.)

อาชญากรรมทางไซเบอร์นี้ นอกจากจะไปเกี่ยวข้องกับมาตรการทางกฎหมายที่กล่าวมาข้างต้นแล้ว ยังไปเกี่ยวข้องกับกฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ ซึ่งเป็นกฎหมายที่รองรับการใช้ลายมือชื่ออิเล็กทรอนิกส์ด้วยกระบวนการใดๆ ทางเทคโนโลยี ให้เสมอด้วยการลงลายมือชื่อธรรมดา อันส่งผลต่อความเชื่อมั่นมากขึ้นในการทำธุรกรรมอิเล็กทรอนิกส์ และที่สำคัญอีกฉบับหนึ่ง คือ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อก่อให้เกิดการรองรับสิทธิและให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจถูกประมวลผล เปิดเผยหรือเผยแพร่ถึงบุคคลจำนวนมากได้ในระยะเวลาอันรวดเร็ว โดยอาศัยพัฒนาการทางเทคโนโลยีจนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ในทางมิชอบอันเป็นการละเมิดต่อสิทธิของข้อมูล ทั้งนี้โดยคำนึงถึงการรักษาดุลยภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัว เสรีภาพในการติดต่อสื่อสาร และความมั่นคงของรัฐ (ณรงค์ กุลนิเทศ, ม.ป.ป.)

สำหรับมาตรการทางกฎหมายภัยคุกคามไซเบอร์ หรือการก่ออาชญากรรมทางคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ มีกฎหมายเกี่ยวข้องที่สำคัญอีกฉบับ คือ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 กฎหมายฉบับนี้มีมาตรการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในประเทศและภายนอกประเทศ และให้อำนาจเจ้าหน้าที่ของรัฐในการตรวจสอบข้อมูลคอมพิวเตอร์ของผู้ที่อาจมีข้อมูลที่เกี่ยวกับภัยคุกคาม พร้อมทั้งกำหนดบทลงโทษผู้ที่ฝ่าฝืนหรือไม่ให้ความร่วมมือ ถือว่าเป็นแนวทางในการป้องกันภัยอาชญากรรมทางไซเบอร์

อย่างไรก็ดี แม้จะมีกฎหมายที่เกี่ยวข้องกับการป้องกันภัยคุกคามอาชญากรรมทางไซเบอร์หลายฉบับ แต่ก็ไม่สามารถป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ได้อย่างมีประสิทธิภาพ เนื่องจากในทางปฏิบัติหน้าที่ของเจ้าพนักงานในกระบวนการพิจารณาคดีเกิดปัญหาในเรื่องพยานหลักฐาน ซึ่งในคดีดังกล่าวนี้จะเป็นพยานหลักฐานทางอิเล็กทรอนิกส์เป็นส่วนใหญ่ ก่อให้เกิดปัญหาและอุปสรรค กล่าวคือลักษณะของพยานหลักฐานดังกล่าวสามารถเปลี่ยนแปลงแก้ไขได้ง่าย และถ้ามีการแก้ไขแล้วจะไม่เหลือร่องรอยอะไรไว้ให้ตรวจสอบเลย นอกจากนี้ยังมีปัญหาการเข้าถึงเพื่อให้ได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ ซึ่งตามกฎหมายรัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2560 มาตรา 336 บุคคลย่อมมีเสรีภาพในการติดต่อสื่อสารถึงกันไม่ว่าทางใด การตรวจหรือการเปิดเผยข้อมูลที่บุคคลสื่อสารถึงกัน รวมถึงการกระทำด้วยประการใดๆ เพื่อให้ล่วงรู้ หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันจะกระทำมิได้ เว้นแต่มีคำสั่งหรือหมายของศาล หรือมีเหตุอื่นตามที่กฎหมายบัญญัติ โดยการได้เข้าถึงเพื่อให้ได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ พนักงานสอบสวนจะประสานกับศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ เป็นหน่วยงานที่อาศัยอำนาจของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในการตรวจสอบและเข้าถึงในระบบคอมพิวเตอร์อันเป็นพยานหลักฐานเกี่ยวกับการกระทำความผิดหรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ทำการถอดรหัสลับ

อย่างไรก็ดี อาชญากรรมทางไซเบอร์มีการแบ่งหน้าที่กันทำ ทำงานกันเป็นทีม มีการติดต่อสื่อสารกันตลอดเวลา เมื่อมีบุคคลใดบุคคลหนึ่งในทีมอาชญากรรมขาดหายไปจากการติดต่อสื่อสาร ก็สงสัยว่าบุคคลนั้นอาจถูกเจ้าหน้าที่ตำรวจจับกุม พยานหลักฐานก็จะถูกทำลายเพื่อลบล้างข้อมูลต่าง ๆ ในคอมพิวเตอร์หรือในมือถือ ทำให้เจ้าหน้าที่ตำรวจไม่สามารถรวบรวมพยานหลักฐานได้ ทำให้เกิดปัญหาในการเข้าถึงเพื่อให้ได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์ (ระบบออนไลน์)

บทสรุป

ความมั่นคงปลอดภัยทางไซเบอร์เป็นเรื่องที่เกี่ยวข้องทั้งภาครัฐและภาคเอกชน หรือภาครัฐเป็นผู้กำหนดนโยบายและกฎระเบียบต่างๆ ส่วนภาคเอกชนมีหน้าที่พัฒนาตามนโยบายดังกล่าว เพื่อให้เกิดเอกภาพในการจัดการกับความมั่นคงปลอดภัยทางไซเบอร์ การรับมือกับภัยคุกคามจึงต้องอาศัยความร่วมมือกับทุกฝ่ายที่เกี่ยวข้อง ซึ่งยุทธศาสตร์ด้านหนึ่งของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม คือการพัฒนาทรัพยากรมนุษย์ด้านดิจิทัล เพื่อให้เกิดความพร้อมด้านบุคลากรในการ

รับมือภัยคุกคามทางไซเบอร์ ในด้านมาตรการทางกฎหมาย มีกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ เช่น กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ในส่วนภาครัฐจะมีสำนักงานตำรวจแห่งชาติหรือกองบังคับการปราบปรามเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) รับผิดชอบงานเกี่ยวกับการป้องกันการสืบสวนการกระทำความผิดทางด้านเทคโนโลยีและสารสนเทศ โดยมุ่งเน้นการกระทำความผิดต่อระบบคอมพิวเตอร์ การใช้คอมพิวเตอร์เป็นเครื่องมือกระทำความผิด และการนำเข้าเผยแพร่ข้อมูลคอมพิวเตอร์สู่ระบบที่เป็นความผิด ตลอดจนการส่งเสริมการสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ภายในสังคม (กิตติ ประเสริฐสุข, 2562)

เอกสารอ้างอิง

[1] กรกัญญ์ญารัก บุญสุขเกิด. (2564). *สถานการณ์และแนวทางการป้องกันอาจชญากรรมไซเบอร์ในประเทศไทย.* คณะสังคมศาสตร์ โรงเรียนนายร้อยตำรวจ.

[2] กรฉัตร มาตรศรี. (2565). *แนวทางการแก้ไขปัญหาและอุปสรรคในการปฏิบัติงานของเจ้าหน้าที่ตำรวจกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กรณีศึกษาการกระทำความผิดฐานฉ้อโกงทางออนไลน์.* คณะอาชญาวิทยาและการบริหารงานยุติธรรม มหาวิทยาลัยรังสิต.

[3] กิตติ ประเสริฐสุข และคณะ. (2562). *ไทยกับความมั่นคงรูปแบบใหม่การค้ามนุษย์การคืนแบบไม่ปกติอาชญากรรมข้ามชาติและความมั่นคงปลอดภัยไซเบอร์.* สถาบันเอเชียตะวันออกศึกษา มหาวิทยาลัยธรรมศาสตร์.

[4] ชฎาภรณ์ สิงห์แก้ว. (2564). *บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม.* คณะรัฐศาสตร์ มหาวิทยาลัยรามคำแหง.

[5] ณรงค์ กุลนิเทศ. (ม.ป.ป.). *รูปแบบและมาตรการแก้ไขปัญหาอาชญากรรมไซเบอร์.* สาขานิติวิทยาศาสตร์ บัณฑิตวิทยาลัย.

[6] ณัฐสุดา อัคราวัฒนา. (ม.ป.ป.). *การกำหนดความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์.* มหาวิทยาลัยธุรกิจบัณฑิต.

[7] ธนนท์ทัส สุธริยานิติภักดี. (ม.ป.ป.). *อาชญากรรมคอมพิวเตอร์ กรณีศึกษามาตรการป้องกันการเข้าถึงข้อมูลทางอินเตอร์เน็ตโดยมิชอบ*

[8] ธนาคารกรุงเทพ จำกัด. (2565). *อาชญากรรมทางไซเบอร์ (Cyber Crime) ภัยคุกคามตัวร้ายในโลกยุคดิจิทัล.* จาก https://www.bangkokbankinnohub.com/th/what-is-cyber-crime/ ค้นเมื่อ 5 กันยายน 2560.

[9] ปรเมศวร์ กุมารบุญ. (2565). เริ่มต้นกับอาชญากรรมไซเบอร์. http://www.gotoknow.org./post/623475.

[10] สปริงนิวส์. (2565). ตำรวจ ปอท. *เปิดสถิติประจำปี 2564 พร้อมเผยแพร่แนวโน้มปีนี้.* https://www.springnews.co.th/spring-life/819659

[11] อัญชลี จวงจันทน์. (2562). *อาชญากรรมไซเบอร์.* สำนักงานเลขาธิการสภาผู้แทนราษฎร.