อาชญากรรมทางเทคโนโลยี: การหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ในประเทศไทย

Technology-Related Crime: Online Fraudulent Transactions of Goods or Services in Thailand

วชิรวิทย์ ทองลิ้ม[1]

กองกำกับการ 1 กองบังคับการปราบปราม กองบัญชาการตำรวจสอบสวนกลาง

1106 ถนนพหลโยธิน แขวงจอมพล เขตจัตุจักร กรุงเทพมหานคร 10900, ประเทศไทย

อีเมลติดต่อ: 6580105924@student.chula.ac.th

Wachirawit Thonglim[2]

Sub-Division 1, Crime Suppression Division, Central Investigation Bureau

1106 Phahonyothin Road, Chomphon, Chatuchak, Bangkok 10900, Thailand

Email: 6580105924@student.chula.ac.th

อุนิษา เลิศโตมรสกุล[3]

สาขาวิชาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา

คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

254 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพมหานคร 10330, ประเทศไทย

อีเมลติดต่อ: unisa.l@.chula.ac.th

Unisa Lerdtomornsakul[4]

Major of Criminology and Criminal Justice, Department of Sociology and Anthropology,

Faculty of Political Science, Chulalongkorn University

254 Phayathai Road, Wangmai, Pathumwan, Bangkok 10330, Thailand

Email: unisa.l@chula.ac.th

Received: January 4, 2025 **Revised**: April 2, 2025 **Accepted:** April 25, 2025

[1] ร.ต.ท., รองสารวัตร.

[2] Pol. Lt., Deputy Inspector.

[3] รองศาสตราจารย์, อาจารย์.

[4] Associate Professor, Lecturer.

บทคัดย่อ

บทความนี้ มีวัตถุประสงค์เพื่อวิเคราะห์สาเหตุของการเกิดอาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ และปัญหาอุปสรรคในการป้องกันปราบปรามอาชญากรรมดังกล่าว โดยเน้นอธิบายรูปแบบลักษณะและประเภทของอาชญากรรมทางเทคโนโลยี โดยเฉพาะการหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ ซึ่งอาชญากรรมดังกล่าวมีความซับซ้อนและถูกพัฒนารูปแบบใหม่ ๆ อยู่ตลอด เนื่องจากเป็นการกระทำความผิดที่เกิดขึ้นบนพื้นที่สมมตผ่านอินเทอร์เน็ต ส่งผลให้การสืบสวนติดตามจับกุมอาชญากรมีความยากลำบากมากขึ้น อีกทั้งการฉ้อโกงโดยการหลอกลวงซื้อขายสินค้าออนไลน์ เป็นอาชญกรรมที่กระทำได้โดยง่าย จึงส่งผลให้อาชญากรรมประเภทดังกล่าวเพิ่มขึ้นอย่างต่อเนื่อง และมีสถิติในการรับแจ้งความสูงสุดเป็นอันดับหนึ่งมาโดยตลอด จากการศึกษาพบว่า สาเหตุของเกิดอาชญากรรมดังกล่าว มีองค์ประกอบ ได้แก่ ผู้กระทำความผิดที่ได้รับแรงจูงใจ เหยื่อที่เหมาะสม และการขาดผู้คุ้มครองที่ดี ซึ่งปัญหาและอุปสรรคในการป้องกันปราบปรามอาชญากรรมประเภทนี้ ได้แก่ ความล่าช้าโดยเฉพาะการทำสำนวนสอบสวน และการรวบรวมพยานหลักฐาน อีกทั้งเจ้าหน้าที่ตำรวจสามารถจับกุมและดำเนินคดีได้เพียงแค่บัญชีม้า ทำให้อาชญากรตัวจริงยังคงลอยนวลส่งผลให้อาชญากรรมยังคงเพิ่มขึ้น

ผลการศึกษาพบว่า การป้องกันปราบปรามอาชญากรรมควรมุ่งตัดองค์ประกอบของสาเหตุการเกิดอาชญากรรมโดยการเพิ่มความรู้ให้ประชาชนและเสริมสร้างมาตรการแก่หน่วยงานรัฐ ให้สามารถสืบสวนและจับกุมอาชญากรได้อย่างมีประสิทธิภาพเมื่อผู้กระทำผิดถูกลงโทษและการป้องกันปราบปรามมีประสิทธิภาพ ย่อมส่งผลให้อาชญากรรมลดลง

คำสำคัญ: อาชญากรรมทางเทคโนโลยี; การหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์; การฉ้อโกงออนไลน์; การป้องกันปราบปรามอาชญากรรม

Abstract

The objective of this paper is to analyse the causes of technology-related crimes, specifically online fraudulent transactions of goods or services. Additionally, it examines the problems and obstacles in the prevention and suppression of these crimes. It focuses on explaining the characteristics and types of technology-related crimes. The crime is complex and constantly evolving in new forms. Since it occurs in cyberspace through the Internet and can be easily committed, resulting in the continuous increase and makes it difficult to investigate and arrest the criminals. The study found that the causes of this crime are motivated offenders, suitable targets, and a lack of capable guardians. In addition, the challenges in preventing and suppressing such crimes include delays in procedures, especially in the investigation and evidence gathering. Furthermore, police officers can only arrest and prosecute mule accounts, which means that real criminals remain scot-free, resulting in an increase in crimes. Therefore,

crime prevention and suppression should focus on cutting out the causes of these crimes by increasing public awareness and strengthening law enforcement measures to be able to investigate and arrest criminals effectively. When offenders are punished, and preventive measures are effective, crime rates will decrease.

Keywords: Technology-Related Crime; Online Fraudulent Transactions of Goods or Services; Online Scams; Crime Prevention and Suppression

1. บทนำ

ปัจจุบันมีเทคโนโลยีได้ถูกพัฒนาให้เข้ามาเป็นส่วนหนึ่งของการดำเนินชีวิตของมนุษย์ ทำให้โลกยุคปัจจุบันเปลี่ยนแปลงไปอย่างก้าวกระโดด เช่น การใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) เทคโนโลยีคลาวด์ (Cloud Computing) ในการเก็บข้อมูล หรือการเชื่อมโยงสิ่งต่าง ๆ ด้วย Internet of Things (IoT) เป็นต้น จะเห็นได้ว่าวิวัฒนาการของเทคโนโลยีถูกพัฒนามาตั้งแต่ยุคอินเทอร์เน็ตจนมาถึงยุคเทคโนโลยีอัจฉริยะ[5] มนุษย์เริ่มเข้าสู่เครือข่ายอินเทอร์เน็ตและพัฒนาเทคโนโลยีเพื่ออำนวยความสะดวกต่าง ๆ จนสามารถเชื่อมต่อกันผ่านเครือข่ายสังคมออนไลน์ (Social Network) และเทคโนโลยีกลายเป็นส่วนหนึ่งของชีวิต เช่น การสื่อสารผ่านสื่อสังคมออนไลน์ (Social Media) การทำธุรกรรมผ่านอินเทอร์เน็ต (E-Commerce) และการจัดเก็บและแบ่งปันข้อมูลต่าง ๆ ซึ่งอาจกล่าวได้ว่า ยุคปัจจุบันเป็นยุคโลกาภิวัตน์ (Globalization) ที่การติดต่อสื่อสารของผู้คนทั่วโลกสามารถเชื่อมต่อและทำกิจกรรมร่วมกันได้อย่างไร้พรมแดน แต่เนื่องด้วยการเชื่อมต่อที่รวดเร็วและสะดวก จึงอาจส่งผลให้การประกอบอาชญากรรมเกิดขึ้นอย่างง่ายดายด้วยเช่นกัน[6]

ยุคโลกาภิวัตน์และการพัฒนาการของอินเทอร์เน็ต ส่งผลกระทบทั้งด้านบวกและด้านลบ ถึงแม้เทคโนโลยีจะช่วยให้การติดต่อสื่อสาร หรือการทำกิจกรรมต่าง ๆ ให้สะดวกและรวดเร็วแล้ว แต่เทคโนโลยีก็ยังถูกอาชญากรใช้เป็นเครื่องมือในการก่ออาชญากรรมได้เช่นกัน เหมือนเหรียญที่มีสองด้านเสมอ หนึ่งในผลกระทบด้านลบ คือการขยายตัวของอาชญากรรม ที่มีพัฒนาการและเปลี่ยนแปลงรูปแบบ เป็นอาชญากรรมข้ามชาติ อาชญากรรมเศรษฐกิจ อาชญากรรมไซเบอร์ อาชญากรรมทางเทคโนโลยี เป็นต้น การใช้เทคโนโลยีเป็นเครื่องมือของอาชญากร ทำให้อาชญากรสามารถดำเนินกิจกรรมที่ผิดกฎหมายจากระยะไกลได้ โดยกระทำความผิดบน Cyber Space หรือพื้นที่สมมติบนโลกออนไลน์ ทำให้อาชญากรรมขยายขอบเขตเป็นวงกว้างและยากต่อการติดตามจับกุม[7] ส่งผลให้อาชญากรรมมีความซับซ้อนและหลากหลายมากขึ้น เช่น การหลอกลวงทางการเงินผ่านระบบธนาคารออนไลน์ การแสวงหาผลประโยชน์ทางเพศจากเด็กและเยาวชนออนไลน์โดยใช้ระบบคอมพิวเตอร์

[5] มนัสนันท์ ด้วงพิทักษ์ และธันย์พัทธ์ ไคร้วานิช, “ชีวิตดิจิทัลในประเทศไทย,” *วารสารกลยุทธ์และความสามารถทางการแข่งขันองค์กร* 1, ฉ. 3 (กันยายน-ธันวาคม 2565): 2-3.

[6] ไพศาล ไกรสิทธิ์, “*ภัยคุกคามจากโลกาภิวัตน์,*” *วารสารวิชาการ มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง* 8, (2548): 109–115.

[7] สาวตรี สุขศรี, “อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญวิทยา,” *วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์* 46, ฉ 2 (มิถุนายน 2560): 415-432.

เป็นเครื่องมือในการกระทำความผิด ดังนั้น จากเดิมที่อาชญากรรมมุ่งก่อความรุนแรงเชิงกายภาพ และเกิดขึ้นตามท้องถนน (Street Crimes) เช่น ลักทรัพย์ วิ่งราวทรัพย์ ชิงทรัพย์ ปล้นทรัพย์ ฆาตกรรม[8] จึงเปลี่ยนแปลงรูปแบบมาเป็นอาชญากรรมที่มุ่งใช้วิธีการปกปิด หลอกลวง ฉ้อโกงเพื่อหวังผลประโยชน์ทางด้านทรัพย์สิน เงินทอง โดยมิได้ใช้กำลังความรุนแรงแต่อย่างใด เรียกได้ว่าเป็นรูปแบบอาชญากรรมเศรษฐกิจ (Economic Crimes)[9] ที่ส่งผลกระทบต่อเศรษฐกิจของชาติโดยตรง (Direct effect on national economy)[10] ซึ่งอาชญากรรมทางเทคโนโลยีเป็นรูปแบบหนึ่งของอาชญากรรมทางเศรษฐกิจ[11] ที่ก่อให้เกิดความเสียหายโดยการใช้เทคโนโลยีหรือคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ซึ่งมีชื่อเรียกแตกต่างกันออกไป แต่ล้วนแล้วมีความหมายเดียวกัน อาทิ อาชญากรรมไซเบอร์ หรืออาชญากรรมคอมพิวเตอร์ เป็นต้น

สำนักงานตำรวจแห่งชาติได้แบ่งประเภทของคดีอาชญากรรมทางเทคโนโลยีไว้ทั้งหมด 14 ประเภท[12] และจากการรวบรวมสถิติข้อมูลการรับแจ้งอาชญากรรมทางเทคโนโลยี หรือรับแจ้งความออนไลน์ สะสมตั้งแต่วันที่ 1 มีนาคม 2565 ถึงวันที่ 31 พฤษภาคม 2567 พบว่ามีจำนวนคดีทั้งสิ้น 569,286 คดี คิดเป็นมูลค่าความเสียหาย 62,366,263,016 บาท ซึ่งคดีประเภท หลอกลวงซื้อขายสินค้าหรือบริการ (ไม่เป็นขบวนการ) มียอดสถิติการรับแจ้งสูงสุดเป็นอันดับ 1 จำนวน 229,998 คดี (42.68%) สร้างความเสียหายกว่า 4,000,579,607 บาท[13] ข้อสังเกตที่สำคัญ คือ ตั้งแต่มีระบบแจ้งความออนไลน์มา คดีฉ้อโกงออนไลน์โดยการหลอกลวงซื้อขายสินค้าหรือบริการ เป็นคดีที่รับแจ้งจำนวนมากที่สุดเป็นอันดับ 1 มาโดยตลอด ซึ่งการฉ้อโกงออนไลน์โดยการหลอกลวงซื้อขายสินค้าหรือบริการ แม้จะไม่ซับซ้อนและไม่ได้สร้างความเสียหายมากในแต่ละคดี แต่เนื่องจากมีจำนวนคดีที่เพิ่มขึ้นต่อเนื่องและเหยื่อสามารถเป็นบุคคลใดก็ได้เพียงแค่ได้เข้าถึงอินเทอร์เน็ต จึงกระทบต่อผู้คนทุกเพศทุกวัย ทำให้เกิดมูลค่าความเสียหายโดยรวมเป็นจำนวนมาก ซึ่งส่งผลกระทบต่อเศรษฐกิจประเทศ การทำงานของตำรวจในป้องกันและปราบปราม และความเชื่อมั่นของประชาชนโดยตรง

เมื่ออาชญากรรมเกิดขึ้นบนโลกออนไลน์ และไม่สามารถระบุตัวตนของอาชญากรได้ อีกทั้งคดีจำนวนมากทำให้เจ้าหน้าที่มีภาระมากขึ้น เมื่อไม่สามารถป้องกันปราบปรามการเกิดอาชญากรรมดังกล่าว มักส่งผลให้ความเชื่อมั่นของคนในสังคมต่อเจ้าหน้าที่ตำรวจลดลง ดังนั้นการศึกษาสาเหตุของการเกิดอาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ จึงมีความสำคัญ และต้องมีการพัฒนาให้

---

[8] ดิเรกฤทธิ์ บุษยธนากรณ์ และสุมนทิพย์ จิตสว่าง, “การเปลี่ยนรูปแบบของอาชญากรรมในศตวรรษที่ 21: ปัญหาอาชญากรรม ลูกผสมในสังคมไทย,” *วารสารสังคมศาสตร์ คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย* 52, ฉ. 1 (มกราคม-มิถุนายน 2556): 1-29.

[9] วนัสนันท์ กันทะวงศ์, “อาชญากรรมเศรษฐกิจ: ศึกษากรณีการตกเป็นเหยื่อการเก็งกำไรอัตราแลกเปลี่ยน เงินตราต่างประเทศ,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชาอาชญาวิทยาและงานยุติธรรม คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2562), 9.

[10] อุนิษา เลิศโตมรสกุล และอัณณพ ชูบำรุง, *อาชญากรรมและอาชญาวิทยา*, พิมพ์ครั้งที่ 2, (กรุงเทพฯ: ศูนย์หนังสือแห่งจุฬาลงกรณ์มหาวิทยาลัย, 2561).

[11] อภิชาติ บวบขม, “อาชญากรรมทางเทคโนโลยี: กฎหมายและแนวทางการป้องกันแบบบูรณาการ,” *Journal of Roi Kaensarn Academi* 8, ฉ. 12 (ธันวาคม 2566): 729.

[12] สำนักงานตำรวจแห่งชาติ, “คำอธิบายลักษณะคดีอาชญากรรมทางเทคโนโลยี ตามความในข้อ 5 ของคำสั่ง ตร. ที่ 182/2566 ลง 17 มี.ค.66,” 17 มีนาคม 2566.

[13] ศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ, “สถิติแจ้งความออนไลน์ ตั้งแต่ 1 มี.ค. 65 – 31 พ.ค. 67,” 2567.

มาตราการป้องกันปราบปรามให้เข้ากับยุคสมัย โดยให้ความรู้และมีเครื่องมืออำนวยความสะดวกให้แก่เจ้าหน้าที่ตำรวจที่เกี่ยวข้อง เพื่อให้การจับกุมและลงโทษผู้กระทำความผิดได้อย่างมีประสิทธิภาพ และนำไปสู่การลดการเกิดอาชญากรรมดังกล่าวได้

2. แนวคิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

จากการศึกษาเรื่องอาชญากรรมทางเทคโนโลยีการหลอกลวงซื้อขายสินค้าหรือบริการทาออนไลน์ในประเทศไทย พบแนวคิดที่เกี่ยวข้อง ดังนี้

2.1 ความหมายของการกระทำความผิดทางเทคโนโลยี

อาชญากรรมทางไซเบอร์ (Cybercrime) หมายถึง การกระทำใด ๆ ที่ฝ่าฝืนต่อบทบัญญัติแห่งกฎหมาย โดยผู้กระทำอาศัยความรู้ด้านเทคโนโลยีคอมพิวเตอร์ในการกระทำความผิด ไม่ว่าลักษณะเป็นการใช้คอมพิวเตอร์เป็นเครื่องมือ หรือมีระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์เป็นเป้าหมาย เพื่อก่อให้เกิดความเสียหาย หรือแสวงหาผลประโยชน์ส่วนตัวโดยมิชอบ[14] ซึ่งปัจจุบันอาชญากรรมดังกล่าวมีชื่อเรียกที่แตกต่างกันออกไป แต่มีความเกี่ยวข้องและสอดคล้องกัน ได้แก่ อาชญากรรมคอมพิวเตอร์ อาชญากรรมทางเทคโนโลยี อาชญากรรมเศรษฐกิจ หรืออาชญากรรมทางไซเบอร์ โดยปัจจุบันอาชญากรรมประเภทนี้เกิดขึ้นหลายรูปแบบ เช่น การโจมตีระบบคอมพิวเตอร์ การแก้ไขหรือขโมยข้อมูลคอมพิวเตอร์ และการหลอกลวงออนไลน์ เป็นต้น อีกทั้งการกระทำความผิดที่มีขอบเขตเป็นวงกว้างและไร้พรมแดน[15] ส่งผลให้การก่ออาชญากรรมของอาชญากรเพียงหนึ่งครั้งอาจส่งผลกระทบไปในหลากหลายพื้นที่ หรือบางครั้งอาจจะส่งผลกระทบต่อหลายประเทศในคราวเดียวกัน[16] จึงอาจนิยามอาชญากรรมลักษณะนี้ได้ว่าเป็นอาชญากรรมข้ามชาติอีกด้วย โดยในบทความนี้ผู้เขียนขอพูดถึงอาชญากรรมไซเบอร์ในลักษณะที่ใช้คอมพิวเตอร์หรือเทคโนโลยีเป็นเครื่องมือในการกระทำความผิด เพื่อก่อให้เกิดความเสียหายแก่ประชาชน ซึ่งทางสำนักงานตำรวจแห่งชาติ และกฎหมายฉบับใหม่ที่ประกาศออกมาเพื่อปรับให้เท่าทันกับยุคสมัยปัจจุบัน เรียกอาชญากรรมประเภทนี้ว่า อาชญากรรมทางเทคโนโลยี

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ได้บัญญัติความหมายของอาชญากรรมทางเทคโนโลยี ไว้ว่า การกระทำหรือพยายามกระทำความผิด ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย การกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ เมื่อวิเคราะห์ตัวบทกฎหมายพบว่าได้มุ่งเน้นไปที่การกระทำความผิดเกี่ยวกับ

---

[14] ธิติรัตน์ สมบูรณ์, “รู้ เข้าใจและตระหนัก อาชญากรรมทางไซเบอร์ (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว,” แก้ไขครั้งล่าสุด 2566, สืบค้นเมื่อ 3 มีนาคม 2568, https://www.chula.ac.th/news/138291/

[15] สาวตรี สุขศรี, “อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญวิทยา,” 420.

[16] Todd Hinnen, “The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet,” *Science and Technology Law Review* 5, no 1 (February 2004) 1-42, Accessed March 3, 2025, https://journals.library.columbia.edu/index.php/stlr/article/view/3636/

คอมพิวเตอร์ โดยใช้คอมพิวเตอร์เป็นเครื่องมือกระทำความผิดฐาน ฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ ซึ่งในความเป็นจริงไม่จำกัดเพียงแค่คอมพิวเตอร์เป็นเครื่องมือ (Computer as a tool) แต่รวมถึงโทรศัพท์มือถือ และอุปกรณ์อื่น ๆ เป็นเครื่องมือช่วยในการกระทำความผิดอีกด้วย[17]

2.2 ลักษณะของอาชญากรรมทางเทคโนโลยี

เมื่ออาชญากรรมได้เปลี่ยนแปลงไปจากที่มุ่งกระทำทางกายภาพไปเป็นอาชญากรรมที่มุ่งกระทำต่อทรัพย์สินของเหยื่อ จึงทำให้เกิดอาชญากรรมรูปแบบใหม่ที่ใช้เทคโนโลยีเป็นเครื่องมือที่ช่วยในการกระทำความผิด อีกทั้งเนื่องจากเป็นอาชญากรรมที่เกี่ยวข้องกับการใช้โครงข่ายอินเทอร์เน็ต และการเชื่อมต่อที่ไร้พรมแดน จึงไม่มีข้อจำกัดเรื่องขอบเขตพื้นที่ในการกระทำความผิด อาชญากรจึงไม่จำเป็นต้องอยู่ในพื้นที่เดียวกันกับเหยื่อ และสามารถเข้าถึงเหยื่อได้โดยอยู่พื้นที่ห่างไกล[18] ซึ่งส่งผลให้เกิดความยุ่งยากในขั้นตอนการสืบสวนรวบรวมพยานหลักฐานของเจ้าหน้าที่ตำรวจ อีกทั้งเทคโนโลยียังช่วยในเรื่องการปกปิดตัวตน ทำให้ยากต่อการติดตามจับกุม เพียงแค่กระทำการผ่านพื้นที่สมมติบนโลกออนไลน์ที่เรียกว่า Cyber Space ทำให้การระบุตัวตนของอีกฝ่ายบนโลกออนไลน์เป็นเรื่องที่ยากหรือไม่สามารถระบุได้ ซึ่งพฤติกรรมที่แสดงออกมาอาจจะสอดคล้องกัน หรือไม่สอดคล้องกันในสองพื้นที่ก็ได้[19] ตัวอย่างเช่น พฤติกรรมที่แสดงออกบนโลกออนไลน์ของบุคคลที่ไม่เคยพบเจอตัวตนจริงมาก่อนอาจแตกต่างกับตัวตนในความเป็นจริง นอกจากนี้ความก้าวหน้าของเทคโนโลยีในปัจจุบันนำไปสู่ความซับซ้อนของอาชญากรรมทางเทคโนโลยี อาชญากรสามารถนำเทคโนโลยีใหม่ ๆ มาใช้เป็นกลอุบายหลอกลวงเหยื่อให้หลงเชื่อ ดังตัวอย่างที่พบเห็นในปัจจุบัน กรณีที่อาชญากรใช้เทคโนโลยี Deep Fake จากปัญญาประดิษฐ์ที่ตัดต่อดัดแปลงใบหน้าเพื่อปกปิดตัวตน และปลอมตัวเป็นเจ้าหน้าที่ตำรวจในคดีประเภท Call Center โดยบางครั้งต้องอาศัยความเชี่ยวชาญเฉพาะด้านและต้องใช้เทคนิคพิเศษในการสืบสวนจับกุมของเจ้าหน้าที่ ซึ่งมีความยุ่งยากและซับซ้อนมากกว่าเดิม จากเหตุผลที่กล่าวมาทำให้การติดตามจับกุมอาชญากรของเจ้าหน้าที่ตำรวจเป็นเรื่องที่ยากขึ้นและใช้เวลานาน เนื่องจากอาชญากรใช้ประโยชน์จากเทคโนโลยี ไม่ว่าจะเป็นการปกปิดตัวตน การกระทำความผิดจากพื้นที่ห่างไกล หรือการใช้เทคโนโลยีเฉพาะทาง ทำให้อาชญากรรมทางเทคโนโลยีเพิ่มขึ้นอย่างต่อเนื่อง และมีจำนวนของอาชญากรและเหยื่อเพิ่มขึ้นอย่างต่อเนื่องเช่นกัน จากที่กล่าวมานี้ข้างต้นทำให้สามารถบ่งบอกถึงลักษณะของอาชญากรรมทางเทคโนโลยี ซึ่งลักษณะของอาชญากรรมไซเบอร์ประกอบด้วย 4 ประการ[20] ได้แก่ 1) ความซับซ้อน, 2) การก่ออาชญากรรมได้จากระยะไกล, 3) ความเป็นนิรนาม และ 4) อาชญากรรมค่อนข้างมีขนาดใหญ่ ด้วยเหตุนี้ การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีจึงจำเป็นต้องพัฒนาเครื่องมือและวิธีการให้ทันสมัยในการสืบสวนและจับกุมเพื่อรับมือกับความท้าทายที่เพิ่มขึ้นในยุคสมัยปัจจุบัน

---

[17] เพ็ญศิริ จันทร์ประทีปฉาย, “มืออาชีพ: ตำรวจไซเบอร์กับภารกิจปราบปรามอาชญากรรมทางเทคโนโลยี,” *สารคดี*, ฉ.14 (มีนาคม 2548).

[18] ธัญพิชชา สามารถ, “การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ,” (วิทยานิพนธ์ปริญญาดุษฎีบัณฑิต สาขาวิชาอาชญาวิทยาและงานยุติธรรม คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2565), 25.

[19] สาวตรี สุขศรี, “อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญวิทยา,” 420.

[20] ธัญพิชชา สามารถ, “การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ,” 18.

2.3 ประเภทของอาชญากรรมทางเทคโนโลยี

โจเซฟ อากาติส (Joseph Aghatise)[21] แบ่งประเภทของอาชญากรรมคอมพิวเตอร์เอาไว้ 2 ประเภท โดยแบ่งจากเป้าหมายของอาชญากรรมว่าเกิดขึ้นต่อคอมพิวเตอร์หรือไม่ หากเป็นประเภทที่คอมพิวเตอร์เป็นเป้าหมาย (Computer as a target) กล่าวคือ อาชญากรรมที่มุ่งโจมตีต่อระบบคอมพิวเตอร์ และต้องใช้เทคนิคเฉพาะด้านในการกระทำความผิด อาชญากรรมลักษณะนี้มีหลากหลายรูปแบบ เช่น Hacker, Virus, Malware หรือ Sniffer เป็นต้น หากคอมพิวเตอร์ไม่ได้เป็นเป้าหมายโดยตรง แต่กลับถูกใช้เป็นเครื่องมือในการกระทำความผิดที่มีมนุษย์เป็นเป้าหมาย เช่นนี้จึงเป็นอีกหนึ่งประเภทที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด (Computer as a tool) ซึ่งไม่จำเป็นต้องอาศัยความรู้หรือเทคนิคเฉพาะทางด้านมากนัก อาชญากรรมประเภทนี้มีหลากหลายรูปแบบ เช่น Cyber-Bullying, Scam หรือ Fake news เป็นต้น การแบ่งประเภทของอาชญากรรมคอมพิวเตอร์ดังกล่าวได้สอดคล้องกับ สาวตรี สุขศรี ซึ่งได้จำแนกประเภทอาชญากรรมไซเบอร์ จากบทบาทของคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิด ดังนี้ 1) การนำคอมพิวเตอร์มาใช้ในการสนับสนุนการก่ออาชญากรรมทั่วไป เช่น การสื่อสารระหว่างอาชญากร หรือการเก็บรักษาข้อมูลที่เกี่ยวข้องกับการกระทำความผิด, 2)การใช้คอมพิวเตอร์เป็นเครื่องมือหลักในการก่ออาชญากรรม ซึ่งอาชญากรรมจะเกิดขึ้นไม่ได้หากไม่มีคอมพิวเตอร์ เช่น การฉ้อโกงออนไลน์ การส่งสแปม หรือ การกลั่นแกล้งทางออนไลน์ และ 3) การที่ระบบหรือข้อมูลคอมพิวเตอร์เป็นเป้าหมายของการก่ออาชญากรรม โดยผู้กระทำความผิดมุ่งโจมตีระบบหรือข้อมูลคอมพิวเตอร์เพื่อสร้างความเสียหาย[22] โดยในส่วนของอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ[23] ได้จำแนกประเภทของอาชญากรรมทางเทคโนโลยีไว้ 14 ประเภท ซึ่งการหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ เป็นหนึ่งประเภทของอาชญากรรมทางเทคโนโลยี และผู้เขียนจะได้กล่าวถึงต่อไป

3. อาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์

จากการศึกษาประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ พบประเด็นที่เกี่ยวข้องดังต่อไปนี้

3.1 กฎหมายที่เกี่ยวข้องกับการฉ้อโกงโดยการหลอกลวงในการซื้อขายสินค้าหรือบริการทางออนไลน์

กฎหมายที่เกี่ยวข้องกับการฉ้อโกงโดยการหลอกลวงในการซื้อขายสินค้าหรือบริการทางออนไลน์ในประเทศไทย มักถูกครอบคลุมภายใต้ประมวลกฎหมายอาญามาตรา 341 ว่าด้วยการฉ้อโกง และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ซึ่งกำหนดโทษสำหรับการหลอกลวงผู้อื่นให้ส่งมอบทรัพย์สินหรือสิ่งของให้โดยการแสดงข้อความอันเป็นเท็จ หรือปิดบังความจริง

[21] Joseph Aghatise, “Cybercrime Definition,” Last modified 2006, Computer Crime Research Center, Accessed March 5, 2025. http://www.crimeresearch.org/articles/joseph06/2/

[22] สาวตรี สุขศรี, *กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์*, พิมพ์ครั้งที่ 2, (กรุงเทพฯ: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2563).

[23] สำนักงานตำรวจแห่งชาติ, “คำอธิบายลักษณะคดีอาชญากรรมทางเทคโนโลยี ตามความในข้อ 5 ของคำสั่ง ตร. ที่ 182/2566 ลง 17 มี.ค.66,”

เมื่อพิจารณาตามองค์ประกอบความผิดฐานฉ้อโกง ผู้กระทำผิดต้องมีเจตนาที่จะหลอกลวงตั้งแต่เริ่มต้น เพื่อให้ได้มาซึ่งทรัพย์สินของผู้เสียหาย โดยการแสดงข้อความอันเป็นเท็จหรือปกปิดความจริง ซึ่งในกรณีการหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ คนร้ายได้ประกาศหรือโฆษณาขายสินค้าโดยมีเจตนาฉ้อฉล และไม่ประสงค์ที่จะส่งมอบสินค้าหรือบริการให้แก่ผู้ซื้อจริงแต่อย่างใด พฤติกรรมดังกล่าวจึงเป็นการกระทำที่เข้าข่ายความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา มาตรา 341[24] ซึ่งกำหนดว่า ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม ผู้นั้นกระทำความผิดฐานฉ้อโกง

นอกจากนี้ การกระทำดังกล่าวยังเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 14 (1)[25] ซึ่งบัญญัติว่า ผู้ใดกระทำความผิดโดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่ น่าจะเกิดความเสียหายแก่ประชาชน ดังนั้น พฤติกรรมของคนร้ายในการประกาศหรือโฆษณาผ่านสื่อออนไลน์ถือเป็นการกระทำความผิดตามกฎหมาย เนื่องจากเป็นการแสดงข้อมูลเท็จเกี่ยวกับสินค้าหรือบริการที่ตนไม่มีความประสงค์ที่จะส่งมอบจริง จึงเป็นการนำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์โดยตรง ส่งผลให้ผู้เสียหายเกิดความเสียหายจากการถูกหลอกลวง ยิ่งไปกว่านั้นหากการกระทำของคนร้ายเป็นการโฆษณา หรือแสดงข้อความอันเป็นเท็จในลักษณะที่ประชาชนทั่วไปสามารถเข้าถึงหรือพบเห็นได้ กล่าวคือ การโพสต์ในลักษณะที่เป็นสาธารณะ ซึ่งบุคคลทั่วไปสามารถพบเห็นและอาจหลงเชื่อได้ การกระทำความผิดเช่นนี้อาจเข้าข่ายเพิ่มโทษ เป็นข้อหาฉ้อโกงประชาชนตามมาตรา 343 ของประมวลกฎหมายอาญาได้อีกด้วย

ดังนั้น พฤติการณ์ของการหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์นั้นไม่เพียงแต่เป็นความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญาเท่านั้น แต่ยังเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อีกด้วย เนื่องจากเป็นการใช้สื่อออนไลน์ในการหลอกลวงและกระทำการที่นำมาซึ่งความเสียหายแก่ผู้เสียหาย ซึ่งในยุคที่การทำธุรกรรมและการซื้อขายสินค้าผ่านช่องทางออนไลน์มีการเติบโตอย่างรวดเร็ว กฎหมายเหล่านี้เป็นเครื่องมือสำคัญในการป้องกันและปราบปรามการฉ้อโกงทางออนไลน์ โดยเฉพาะให้อำนาจในการบังคับใช้กฎหมายแก่เจ้าหน้าที่ในการปกป้องประชาชนจากการถูกหลอกลวง และนำตัวผู้กระทำความผิดมาลงโทษ รวมถึงสร้างความเชื่อมั่นในการทำธุรกรรมทางออนไลน์อีกด้วย

3.2 สาเหตุของการเกิดอาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์

การฉ้อโกงเป็นปัญหาที่พบได้บ่อยในการซื้อขายสินค้าและบริการทางออนไลน์ เมื่อยุคสมัยได้เปลี่ยนแปลงไป ทำให้สังคมเข้าสู่ยุคที่ใช้เทคโนโลยีอำนวยความสะดวก การซื้อขายสินค้าหรือบริการรวมไปถึงการชำระเงินไม่จำเป็นต้องออกไปหน้าร้านค้าเพื่อซื้อสินค้าเหมือนเมื่อก่อน ปัจจุบันการซื้อขายสินค้าจึงสะดวก

[24] ประมวลกฎหมายอาญา, มาตรา 341, ราชกิจจานุเบกษา เล่มที่ 73 ตอนที่ 95 ฉบับพิเศษ (15 พฤศจิกายน 2499): 1.

[25] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, มาตรา 14(1), ราชกิจจานุเบกษา เล่มที่ 134 ตอนที่ 10 ก (24 มกราคม 2560): 24.

รวดเร็วขึ้น อย่างไรก็ตามข้อจำกัดของการซื้อขายสินค้าและบริการทางออนไลน์ คือ การที่ไม่สามารถระบุตัวตนร้านค้าหรือผู้ขายและผู้ซื้อได้ อีกทั้งผู้ซื้อไม่สามารถจับต้องหรือตรวจเช็คสินค้าได้ก่อนทำการซื้อขาย เหตุนี้จึงเป็นความเสี่ยงที่ทั้งผู้ขายและผู้ซื้อสินค้าหรือบริการทางออนไลน์ต้องเผชิญ ถึงแม้จะมีแอพพลิเคชั่นชันที่ทำหน้าที่เป็นตัวกลางในการซื้อขายสินค้าหรือบริการออนไลน์ แต่ด้วยข้อจำกัดบางอย่างทำให้ผู้คนยังเลือกซื้อขายสินค้าหรือบริการออนไลน์กันเองโดยไม่ผ่านตัวกลาง ดังนั้นจึงทำให้ยังคงพบเจอปัญหาฉ้อโกงในลักษณะการซื้อขายสินค้าหรือบริการออนไลน์อย่างต่อเนื่องในปัจจุบัน

สาเหตุของการเกิดอาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์สามารถเกิดจากหลายปัจจัย ไม่ว่าจะเป็นยุคปัจจุบันที่สังคมพัฒนาขึ้น และเทคโนโลยีเป็นประโยชน์ในการดำเนินชีวิต รวมถึงถูกอาชญากรนำมาใช้เพื่อก่ออาชญากรรม อีกทั้งการป้องกันปราบปรามหรือกฎหมายอาจจะไม่ครอบคลุมและตามไม่ทันยุคสมัย จึงทำให้อาชญากรรมทางเทคโนโลยีเกิดขึ้นอย่างต่อเนื่อง ซึ่งทฤษฎีที่นักอาชญาวิทยามักจะนำมาอธิบายถึงสาเหตุการเกิดอาชญากรรมโดยเฉพาะอาชญากรรมไซเบอร์นั้น ได้แก่ ทฤษฎีปกติวิสัย หรือ Routine Activity Theory[26] โดย Cohen and Felson[27] ได้อธิบายทฤษฎีนี้ โดยมีแนวคิดว่าพฤติกรรมหรือกิจวัตรประจำวันของบุคคลสามารถเป็นปัจจัยสำคัญที่สร้างโอกาสในการกระทำความผิดให้แก่อาชญากร โดยมีการวิเคราะห์ว่ากิจกรรมในชีวิตประจำวัน เช่น การเดินทางไปกลับที่ทำงานหรือโรงเรียนอย่างเป็นประจำ การสวมใส่เสื้อผ้าราคาแพง การไปยังร้านค้าที่คุ้นเคย หรือการพกพาของมีค่าราคาแพง เป็นต้น ซึ่งสิ่งเหล่านี้อาจทำให้อาชญากรสังเกตเห็นช่องว่างหรือโอกาสในการกระทำความผิด เนื่องจากอาชญากรสามารถวางแผนและเตรียมการกระทำความผิดได้ ทำให้ลดความเสี่ยงที่จะถูกจับกุม โดยการกระทำซ้ำเดิมหรือการมีรูปแบบชีวิตที่คาดการณ์ได้ง่ายเป็นปัจจัยที่อาชญากรใช้ในการพิจารณาตัดสินใจ ซึ่งทฤษฎีนี้ประกอบไปด้วย 3 องค์ประกอบที่ทำให้เกิดอาชญากรรม โดยที่อาชญากรรมไม่สามารถเกิดขึ้นได้หากขาดองค์ประกอบใดองค์ประกอบหนึ่งไป ซึ่งประกอบด้วย 1) ผู้กระทำความผิดที่ได้รับแรงจูงใจ (Motivated Offenders), 2) เป้าหมายที่เหมาะสม (Suitable Targets) และ 3)การขาดผู้คุ้มครองที่ดี (Absence of Capable Guardians)

ในปัจจุบันอาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ อาชญากรสามารถเป็นบุคคลทั่วไป หรือผู้ใดก็ได้เพียงแค่สามารถใช้เทคโนโลยีในการก่ออาชญากรรม กล่าวคือสามารถใช้อุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ หรือโทรศัพท์มือถือ และผู้นั้นสามารถเข้าถึงเครือข่ายสังคมออนไลน์ผ่านการใช้งานอินเทอร์เน็ต เพียงเท่านี้ก็สามารถเป็นอาชญากรในการหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ได้โดยไม่จำเป็นต้องอาศัยความเชี่ยวชาญ หรือความรู้เฉพาะทางแต่อย่างใด และเนื่องจากอาชญากรรมเกิดขึ้นบนโลกออนไลน์ จึงไม่สามารถระบุตัวตนของผู้ใช้งานอินเทอร์เน็ตที่ทำกิจกรรมผ่าน Cyberspace ได้[28] ด้วยเหตุผลนี้ ทำให้อาชญากรตัดสินใจลงมือกระทำผิด เพราะเมื่อพิจารณาระหว่างผลประโยชน์ทางเศรษฐกิจที่จะได้รับและความเสี่ยงในการถูกจับกุมแล้ว พบว่าประโยชน์ที่จะได้รับ คือ ทรัพย์สินของเหยื่อมี

[26] ธัญพิชชา สามารถ, “การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ,” 58.

[27] Lawrence E. Cohen and Marcus Felson, “Social Change and Crime Rate Trends: A Routine Activity Approach,” *American Sociological Review* 44, no. 4. (August 1979) 588–608.

[28] สาวตรี สุขศรี, “อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญวิทยา,” 420.

ค่ามากกว่าผลเสียที่จะได้รับเมื่อถูกจับกุม เนื่องจากเจ้าหน้าที่ตำรวจต้องใช้ทรัพยากรและเวลาจำนวนมากในการติดตามจับกุมอาชญากรที่กระทำความผิดอาชญากรรมทางเทคโนโลยี ซึ่งในหนึ่งคดีอาจจะใช้เวลาหลายเดือนจนไปถึงหลายปี ดังนั้น การกระทำของอาชญากรเพียงแค่หนึ่งครั้งสามารถหาประโยชน์จากเหยื่อได้หลายรายในเวลาเดียวกัน และได้รับผลตอบแทนจำนวนมาก อีกทั้ง การไร้ตัวตนบนโลกออนไลน์ (Anonymity) ทำให้ความเสี่ยงหรือโอกาสในการถูกจับลดลง[29] จึงทำให้อาชญากรรมสำเร็จอย่างรวดเร็วและไร้ร่องรอย เมื่ออาชญากรต้องการหาประโยชน์จากเหยื่ออยู่ตลอดเวลาอยู่แล้วนั้น ทำให้การหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์เพิ่มขึ้นอย่างต่อเนื่อง โดยมีผู้กระทำความผิดที่ได้รับแรงจูงใจ (Motivated Offenders) อยู่มากมายในสังคมปัจจุบัน อย่างไรก็ตามกิจวัตรของเหยื่อ ได้แก่ การโพสต์ผ่านสื่อสังคมออนไลน์ การซื้อสินค้าหรือบริการผ่านช่องทางออนไลน์ หรือการทำกิจกรรมต่าง ๆ บนโลกออนไลน์ ทำให้เหยื่ออาจจะใช้ชีวิตจนเป็นกิจวัตร และอาจส่งผลให้เกิดช่องว่างหรือแรงจูงใจให้อาชญากรตัดสินใจประกอบอาชญากรรมได้ สอดคล้องกับประเภทของเหยื่อที่ Stephen Schafer ได้แบ่งไว้คือ เหยื่อที่จุดชนวนให้เกิดอาชญากรรม ถึงแม้เหยื่อมิได้กระทำสิ่งใดต่ออาชญากรแต่อาจเป็นเพราะพฤติกรรมของเหยื่อที่เปิดช่อง หรือจูงใจให้อาชญากรกระทำความผิด[30] โดยเหยื่อที่ตกเป็นเป้าหมายมักเป็นผู้ที่มีลักษณะเปราะบางหรือขาดการระมัดระวังเพียงพอ เช่น กลุ่มผู้สูงอายุหรือบุคคลที่ขาดประสบการณ์ด้านการใช้งานอินเทอร์เน็ต อีกทั้งบางกรณีเหยื่อเองที่มีส่วนทำให้เกิดอาชญากรรมขึ้น เนื่องจากมีความประมาทและขาดการพิจารณาอย่างรอบคอบ ในกรณีการหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ การที่ผู้คนส่วนใหญ่มักสั่งซื้อสินค้าออนไลน์จนกลายเป็นกิจวัตรไปแล้ว เมื่อพบเห็นประโยชน์จากซื้อสินค้าออนไลน์ที่มีราคาถูกกว่าท้องตลาด และมีความสะดวกรวดเร็วในการสั่งซื้อสินค้า การชำระเงิน และการจัดส่ง ทำให้ขาดความยั้งคิดก่อนตัดสินใจซื้อสินค้า หรือขาดความตระหนักรู้ว่าการสั่งซื้อสินค้าหรือบริการทางออนไลน์ไม่สามารถระบุตัวตนที่แท้จริงของร้านค้าหรือผู้ขายได้ ซึ่งสอดคล้องกับเป้าหมายที่เหมาะสม (Suitable Targets) ของทฤษฎีปกติวิสัย (Routine Activity Theory)

นอกจากนี้ องค์ประกอบสุดท้าย คือ การขาดผู้คุ้มครองที่ดี (Absence of Capable Guardians) ยังส่งผลให้เกิดอาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ เนื่องจากอาชญากรรมทางเทคโนโลยีเป็นอาชญากรรมรูปแบบใหม่ที่ยังพบช่องว่างทางกฎหมาย หรือกฎหมายยังไม่ครอบคลุม หรือการบังคับใช้ไม่ทันกับยุคสมัย ถึงแม้มีการออกกฎหมายหรือมาตรการใหม่ ๆ เพื่อพัฒนาให้ทันกับการบังคับใช้กฎหมายในยุคปัจจุบัน แต่ยังมีข้อสังเกตุบางประการที่กฎหมายควรแก้ไขหรือปรับปรุงให้มีประสิทธิภาพ เช่น บทลงโทษ หรือความขัดแย้งกันของกฎหมายบางฉบับ เป็นต้น[31] นอกจากนี้ เจ้าหน้าที่ตำรวจซึ่งเป็นผู้มีส่วนในการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยียังขาดความสามารถในการติดตามจับกุมอาชญากรทางเทคโนโลยี เนื่องจากขาดองค์ความรู้ หรือเครื่องมือในการสืบสวน รวบรวมพยานหลักฐานทาง

[29] ปรเมศวร์ กุมารบุญ, “ความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์,” (วิทยานิพนธ์ปริญญาดุษฎีบัณฑิต สาขาวิชาอาชญาวิทยาและงานยุติธรรม คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2563), 63.

[30] ศรีสมบัติ โชคประจักษ์ชัด, *ตำราเหยื่ออาชญากรรม : สิทธิและการช่วยเหลือเยียวยา,* พิมพ์ครั้งที่ 1, (กรุงเทพฯ: คณะรัฐมนตรีและราชกิจจานุเบกษา, 2561).

[31] วนัสนันท์ กันทะวงศ์, “อาชญากรรมเศรษฐกิจ: ศึกษากรณีการตกเป็นเหยื่อการเก็งกำไรอัตราแลกเปลี่ยน เงินตราต่างประเทศ,” 74.

อิเล็กทรอนิกส์[32] อีกทั้ง ปัญหาบัญชีม้าที่อาชญากรใช้ปกปิดเส้นทางการเงิน และการไร้ตัวตนของอาชญากรตัวจริงนั้น เป็นความท้าทายที่เจ้าหน้าตำรวจต้องเผชิญ ส่งผลให้อาชญากรรมทางเทคโนโลยีมีโอกาสเกิดขึ้นอย่างต่อเนื่องกล่าวโดยสรุปได้ว่า สาเหตุของการเกิดอาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ คือ การที่องค์ประกอบทั้งสามเกิดขึ้นครบถ้วน ได้แก่ การขาดผู้คุ้มครองที่ดี (Absence of Capable Guardians) เป้าหมายที่เหมาะสม (Suitable Targets) และผู้กระทำความผิดที่ได้รับแรงจูงใจ (Motivated Offenders) กล่าวคือ การที่กฎหมายและการป้องกันปราบปรามของเจ้าหน้าที่ยังขาดประสิทธิภาพ รวมถึงการขาดความระมัดระวังของเหยื่อที่เลือกซื้อสินค้าจากแหล่งที่ไม่สามารถระบุตัวตนผู้ขายได้ และเน้นเพียงความสะดวกและราคาถูก ทำให้ปัญหายิ่งทวีความรุนแรง เมื่อการป้องกันปราบปรามไม่มีประสิทธิภาพ อาชญากรตัวจริงไม่ถูกนำตัวเข้าสู่กระบวนการยุติธรรม ส่งผลให้อาชญากรรมเพิ่มขึ้นและรูปแบบของการกระทำความผิดถูกพัฒนาอย่างต่อเนื่อง เมื่อผู้คนเห็นว่าอาชญากรเหล่านี้ไม่ถูกจับกุมและได้รับผลตอบแทนสูงจากการกระทำผิด จึงเกิดแรงจูงใจในการเข้าร่วมก่ออาชญากรรมมากยิ่งขึ้น ส่งผลให้อาชญากรรมหลอกลวงซื้อขายออนไลน์กลายเป็นปัญหาอันดับหนึ่งที่ยังเกิดขึ้นอย่างต่อเนื่อง

4. ปัญหาและอุปสรรคในการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์

จากการเติบโตของเทคโนโลยี ทำให้อาชญากรรมได้ถูกพัฒนารูปแบบเป็นอาชญากรรมทางเทคโนโลยี ซึ่งอาชญากรทำการหลอกลวงผู้บริโภค ผ่านการซื้อขายสินค้าหรือบริการบนแพลตฟอร์มออนไลน์ โดยอาชญากรใช้เทคโนโลยีในการกระทำความผิด ทำให้อาชญากรรมทางเทคโนโลยีนั้นสามารถกระทำได้ทุกที่ ผ่านอินเทอร์เน็ต จึงทำให้อาชญากรรมทางเทคโนโลยีเพิ่มขึ้นอย่างรวดเร็ว ส่งผลให้เจ้าหน้าที่ไม่สามารถป้องกันปราบปรามได้อย่างทั่วถึงหรือมีประสิทธิภาพ ปัญหาและอุปสรรคในการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ ได้แก่ การขาดแคลนกำลังพลเจ้าหน้าที่ตำรวจผู้ปฏิบัติงาน โดยเฉพาะพนักงานสอบสวน รวมถึงการขาดองค์ความรู้และความสามารถในการทำสำนวนการสอบสวน หรือการสืบสวนจับกุมผู้ต้องหาอาชญากรรมทางเทคโนโลยี เนื่องจากเป็นอาชญากรรมรูปแบบใหม่ที่ต้องใช้เทคนิคการแกะรอยหรือรวบรวมพยานหลักฐานทางดิจิทัล ซึ่งตามกฎหมายการรวบรวมพยานหลักฐานดังกล่าวจำเป็นต้องอาศัยอำนาจจากเจ้าพนักงานที่รัฐมนตรีแต่งตั้ง ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ นอกจากนี้การรวบรวมพยานหลักฐานยังต้องอาศัยความร่วมมือจากหลายองค์กร เช่น ธนาคาร หรือผู้ให้บริการอินเทอร์เน็ต ซึ่งทำให้ต้องใช้ระยะเวลาในการทำสำนวนการสอบสวน ทำให้เกิดการสะสมของคดีความ กล่าวคือ คดีหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ที่เกิดขึ้นใหม่ทุกวัน ทำให้คดีที่มีอยู่ก่อนหน้านี้ไม่ได้รับการดำเนินการให้เสร็จสิ้นตามกระบวนการที่เหมาะสม จึงนำไปสู่การสะสมของคดีอย่างต่อเนื่องและเพิ่มภาระให้แก่เจ้าหน้าที่ผู้รับผิดชอบ จนกลายเป็นการละเลยหรือทอดทิ้งการดำเนินคดี[33]

[32] กิตติศักดิ์ คุรุนันท์ และทัชชกร แสงทองดี, “แนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย,” *วารสารการบริหารนิติบุคคลและนวัตกรรมท้องถิ่น* 9, ฉ. 6 (มิถุนายน 2566): 180–190.

[33] ณัฐธรณ์ เดชสกุล, “ปัญหาการฉ้อโกงซื้อขายสินค้าทางอินเทอร์เน็ตในประเทศไทย,” *วารสารนวัตกรรมสังคม* 3, ฉ. 1 (มกราคม–มิถุนายน 2563): 137–153.

นอกจากนี้ ปัญหาที่ทำให้อาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ได้พัฒนารูปแบบและเกิดขึ้นอย่างต่อเนื่อง คือ ผู้กระทำผิดตัวจริงซึ่งเป็นผู้ที่เข้าถึงแพลตฟอร์มออนไลน์และทำการหลอกลวงผู้เสียหายไม่ถูกจับกุมหรือดำเนินคดี โดยในทางปฏิบัติเจ้าหน้าที่ผู้บังคับใช้กฎหมายสามารถสืบสวนและจับกุมได้เพียงเจ้าของบัญชีธนาคารที่ปรากฏว่าเป็นผู้รับโอนเงินจากผู้เสียหาย ซึ่งในความเป็นจริงบัญชีเหล่านั้นเป็นเพียงบัญชีม้าที่อาชญากรใช้เป็นกลยุทธ์ในการปกปิดเส้นทางการเงินของตน โดยส่วนใหญ่อาชญากรได้โอนเงินจากบัญชีดังกล่าวไปยังกระเป๋าเงินดิจิทัล หรือสกุลเงินคริปโต ทำให้การติดตามหรืออายัดเงินซับซ้อนมากขึ้น อีกทั้งการสืบสวนคดีเหล่านี้ต้องใช้ทรัพยากรและความรู้เชิงเทคโนโลยีเป็นอย่างมาก รวมถึงการระบุตำแหน่งหรือยืนยันตัวผู้กระทำผิดบนโลกออนไลน์จำเป็นต้องประสานงานกับเจ้าของเว็บไซต์ หรือผู้ให้บริการอินเทอร์เน็ต ซึ่งเป็นกระบวนการที่ใช้เวลานานและซับซ้อนมากเกินกว่าที่จะปราบปรามอาชญากรรมได้อย่างทันท่วงที และอาชญากรมักตั้งฐานปฏิบัติการในต่างประเทศ ทำให้การบังคับใช้กฎหมายข้ามชาติ หรือการขอความร่วมมือด้านข้อมูลคอมพิวเตอร์จากประเทศอื่น ๆ เป็นเรื่องที่ไปได้ยาก หรือแทบจะเป็นไปไม่ได้เลย จึงส่งผลให้อาชญากรตัวจริงไม่ถูกติดตามหรือจับกุม

จากที่กล่าวมาข้างต้น ปัญหาที่ทำให้อาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์เกิดขึ้นในประเทศไทยอย่างต่อเนื่อง คือ ความล่าช้าในการป้องกันและปราบปรามการกระทำความผิด เนื่องจากความล่าช้าจากการขอความร่วมมือระหว่างหน่วยงานเพื่อตรวจสอบการใช้บัญชีม้า ความยากลำบากในการรวบรวมพยานหลักฐาน และเจ้าหน้าที่ขาดความรู้ ความเชี่ยวชาญและกำลังพล จึงทำให้การปราบปรามล่าช้า อีกทั้งผู้กระทำผิดตัวจริงไม่ถูกจับกุมหรือดำเนินคดี เนื่องจากไม่สามารถติดตามตัวได้ ทำให้อาชญากรรมทางเทคโนโลยีมีโอกาสพัฒนาและขยายตัวอย่างต่อเนื่องจนทำให้ปัญหาอาชญากรรมเหล่านี้ทวีความรุนแรงและกลายเป็นปัญหาที่สะสม

5. สรุปผล และข้อเสนอแนะ

จากการศึกษาเรื่องอาชญากรรมทางเทคโนโลยี การหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ในประเทศไทย ผู้เขียนสามรถสรุปผลและมีข้อเสนอแนะดังต่อไปนี้

5.1 สรุปผล

การพัฒนาของเทคโนโลยีได้ส่งผลกระทบทั้งด้านบวกและลบให้สังคมยุคปัจจุบัน แม้เทคโนโลยีจะช่วยอำนวยความสะดวกรวดเร็วในการทำสิ่งต่าง ๆ แต่เทคโนโลยียังถูกใช้เป็นเครื่องมือในการกระทำความผิด โดยเฉพาะอาชญากรรมทางเทคโนโลยีที่ขยายตัวและเปลี่ยนแปลงรูปแบบไปอย่างรวดเร็ว ทำให้อาชญากรสามารถกระทำความผิดจากระยะไกลบนพื้นที่เสมือนจริง หรือ Cyber Space ซึ่งการหลอกลวงซื้อขายสินค้าออนไลน์เป็นหนึ่งในอาชญากรรมที่เกิดขึ้นบ่อย โดยอาชญากรจะนำข้อมูลเท็จโฆษณาสินค้าราคาถูกผ่านแพลตฟอร์มออนไลน์ เมื่อเหยื่อหลงเชื่อและโอนเงินให้กับอาชญากร อาชญากรจะหลบหนีไปอย่างไร้ร่องรอย และใช้บัญชีม้าเพื่อถ่ายโอนเงินเป็นทอด ๆ ทำให้การติดตามเส้นทางการเงินเป็นไปได้ยาก โดยคดีในลักษณะนี้เกิดขึ้นได้ง่าย เนื่องจากอาชญากรไม่จำเป็นต้องมีความเชี่ยวชาญทางเทคโนโลยีสูง เพียงแค่สามารถใช้งานสื่อสังคมออนไลน์เพื่อโพสต์ขายสินค้าได้

นอกจากนี้การปราบปรามและป้องกันอาชญากรรมทางเทคโนโลยีโดยเฉพาะในการทำสำนวนสอบสวนต้องอาศัยทรัพยากรและกำลังพลจำนวนมาก อีกทั้งจำเป็นต้องรวบรวมพยานหลักฐานทางดิจิทัลซึ่งเป็นองค์ความรู้ใหม่ที่ทำได้ยาก และเนื่องจากจำนวนคดีที่เพิ่มขึ้นอย่างต่อเนื่อง ทำให้การดำเนินการทั้งจากฝั่งภาครัฐและเอกชนเกิดความล่าช้า เช่น การประสานงานระหว่างเจ้าหน้าที่ตำรวจกับธนาคารหรือผู้ให้บริการอินเทอร์เน็ต จนไม่สามารถปราบปรามอาชญากรรมทางเทคโนโลยีได้ทันท่วงที อีกทั้งในทางปฏิบัติเจ้าหน้าที่ตำรวจมักไม่สามารถจับกุมตัวผู้กระทำผิดที่แท้จริงได้ เนื่องจากปัญหาการระบุตัวตนและบางครั้งอาชญากรกระทำความผิดจากต่างประเทศ ทำให้เจ้าหน้าที่ตำรวจจับได้เพียงเจ้าของบัญชีธนาคารที่ถูกใช้ในการรับโอนเงินหรือบัญชีม้าเท่านั้น ซึ่งบุคคลเหล่านี้มักไม่เกี่ยวข้องโดยตรงกับการกระทำความผิด ทำให้ผู้กระทำผิดที่แท้จริงยังคงลอยนวลและสามารถพัฒนาวิธีการหลอกลวงใหม่ ๆ ได้อยู่ตลอด ซึ่งเมื่อบุคคลต่าง ๆ เห็นว่าอาชญากรเหล่านี้สามารถกระทำความผิดและยังคงหลบหนีจากการจับกุมได้ แถมยังร่ำรวยจากการกระทำผิด ยิ่งเป็นการกระตุ้นให้เกิดอาชญากรหน้าใหม่เพิ่มขึ้น และไม่มีแนวโน้มที่อาชญากรรมทางเทคโนโลยี ประเภทหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์ลดลงไปจากสังคม

5.2 ข้อเสนอแนะ

อย่างไรก็ตามสาเหตุของการเกิดอาชญากรรมทางเทคโนโลยีประเภทหลอกลวงซื้อขายสินค้าออนไลน์สามารถอธิบายได้ตามทฤษฎีปกติวิสัย (Routine Activity Theory) ซึ่งระบุว่า อาชญากรรมจะเกิดขึ้นเมื่อมีองค์ประกอบสามประการครบถ้วน ได้แก่ ผู้กระทำความผิดที่ได้รับแรงจูงใจ (Motivated Offenders) เป้าหมายที่เหมาะสม (Suitable Targets) และ การขาดผู้คุ้มครองที่มีประสิทธิภาพ (Absence of Capable Guardians) ดังนั้น การป้องกันอาชญากรรมจึงควรมุ่งตัดองค์ประกอบเหล่านี้ ไม่ว่าจะเป็นการเพิ่มความรู้และการตระหนักรู้ให้กับประชาชนเพื่อลดโอกาสในการตกเป็นเหยื่อ โดยการสร้างความตระหนักรู้ในสาธารณชนยังสามารถทำได้ผ่านแคมเปญให้ความรู้ในสื่อสังคมออนไลน์ การจัดอบรมเกี่ยวกับความปลอดภัยไซเบอร์ในโรงเรียน การเผยแพร่ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ผ่านภาคธุรกิจและองค์กรที่เกี่ยวข้อง รวมถึงการสร้างระบบแจ้งเตือนภัยออนไลน์เพื่อให้ประชาชนรับรู้ถึงกลโกงที่เกิดขึ้นล่าสุด นอกจากนี้ ควรมีการส่งเสริมให้ประชาชนมีส่วนร่วมในการรายงานอาชญากรรมทางเทคโนโลยี ผ่านช่องทางที่เข้าถึงได้ง่าย เช่น แอปพลิเคชันแจ้งเหตุ หรือสายด่วนเฉพาะทาง การเสริมสร้างมาตรการป้องกันและปราบปรามให้หน่วยงานรัฐและเอกชนเพื่อเพิ่มประสิทธิภาพในการทำหน้าที่เป็นผู้คุ้มครองที่ดี เช่น การบูรณาการระบบฐานข้อมูลของหน่วยงานที่เกี่ยวข้องเพื่อให้สามารถติดตามพฤติกรรมอาชญากรทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากขึ้น รวมถึงการจัดตั้งศูนย์กลางสำหรับเผยแพร่ข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์ที่สามารถเข้าถึงได้ทั้งประชาชนและหน่วยงานที่เกี่ยวข้อง การใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) และการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) เพื่อช่วยตรวจจับพฤติกรรมที่น่าสงสัยก็เป็นอีกแนวทางหนึ่งที่สามารถช่วยเสริมสร้างมาตรการป้องกันได้อย่างมีประสิทธิภาพ การปรับปรุงกฎหมายให้ทันสมัย การเพิ่มบทลงโทษที่เข้มงวด และการจัดสรรทรัพยากรบุคคลและเครื่องมือที่เหมาะสมให้หน่วยงานที่เกี่ยวข้อง โดยเฉพาะเจ้าหน้าที่ตำรวจเพื่อให้สามารถสืบสวนและจับกุมผู้กระทำผิดได้อย่างมีประสิทธิภาพเมื่อผู้กระทำความผิดตัวจริงถูกดำเนินคดีและเข้าสู่กระบวนการยุติธรรมด้วยความรวดเร็ว รุนแรงและแน่นอน อาชญากรรมทางเทคโนโลยีประเภทนี้ก็จะมีแนวโน้มลดลงในที่สุด

References

Aghatise, J. "Cybercrime Definition," Computer Crime Research Center. Last modified 2006. Accessed March 5, 2025. http://www.crimeresearch.org/articles/joseph06/2/

Apichat Buabkhom. "Technology Crime: Law and Integrated Prevention Approaches." *Journal of Roi Kaensarn Academi* 8, no. 12 (December 2023): 729. [In Thai]

Cohen, L. E., and Felson, M. "Social Change and Crime Rate Trends: A Routine Activity Approach." American Sociological Review 44, no. 4. (August 1979): 588–608.

Direkrit Busayatanakorn and Sumonthip Jitsawang. "Changing Patterns of Crime in the 21st Century: Crime Problems Hybrids in Thai Society." *Journal of Social Sciences, Faculty of Political Science Chulalongkorn University* 52, no. 1 (January-June 2013): 1-29. [In Thai]

Hinnen, Todd. "The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet." Science and Technology Law Review 5, (February 2004): 1-42. Accessed March 3, 2025. https://journals.library.columbia.edu/index.php/stlr/article/view/3636/

Kittisak Kurrunan and Thatchakorn Saengthongdee. "Guidelines for Preventing Cybercrime in Thailand." *Journal of Legal Management and Local Innovation* 9, no. 6 (June 2023): 180-190. [In Thai]

Manatsanun Duangphitak and Thanyapat Khraivanich. "Digital Life in Thailand." *Journal of Organizational Strategy and Competitive Capability* 1, no. 3 (September - December 2022): 2-3. [In Thai]

Natthathon Detsakul. "Problems of Online Fraud in Thailand." *Journal of Social Innovation* 3, no. 1 (January–June 2020): 137–153. [In Thai]

Online Crime Reporting Management Center, Royal Thai Police. "Online Crime Reporting Statistics from March 1, 2022 – May 31, 2024." 2024. [In Thai]

Paisan Kraisit. "Threats from Globalization." Academic Journal of Rajabhat University of Muang Chom Bung 8, (2005): 109–115. [In Thai]

Pensiri Chanpratheepchai. "Professionals: Cyber Police and Their Mission to Suppress Technology Crime." *Documentary*, no. 241 (March 2005). [In Thai]

Porames Kumarnboon. "The Relationship between Anonymity and Cybercrime," Ph.D. Thesis in Criminology and Criminal Justice, Faculty of Political Science, Chulalongkorn University, 2020. [In Thai]

Royal Thai Police. “Explanation of Technology Crime Cases According to Section 5 of Police Order No. 182/2566, March 17, 2023,” 17 March 2023. [In Thai]

Sawatree Suksri. “Computer/Cybercrime and Criminology Theory.” *Journal of Law Thammasat University* 46, no. 2 (June 2017): 415-432. [In Thai]

Sawatree Suksri. The Law on Computer and Cybercrime. 2nd ed. Bangkok: Teaching Materials and Supplementary Documents Project, *Faculty of Law Thammasat University*, 2020. [In Thai]

Srisombat Chokprajakch at. Crime Victimology: Rights and Assistance for Victims. 1st ed. Bangkok: Cabinet and Royal Gazette, 2018. [In Thai]

Thanyapitcha Samart. “Cybercrime Victimization of the Elderly,” Ph.D. Thesis in Criminology and Criminal Justice Faculty of Political Science, Chulalongkorn University, 2023. [In Thai]

Thitirat Somboon. “Know, Understand, and Realize Cybercrime: Preventing Close-to-Home Threats,” Chulalongkorn University News. Last Modified in 2023, Accessed March 3, 2025. https://www.chula.ac.th/news/138291/ [In Thai]

Unisa Lerdtomornsakul and Annop Chubamrung. Crime and Criminology. 2nd ed. Bangkok: Chulalongkorn University Press, 2018. [In Thai]

Wanatsanan Kanthawong. “Economic Crimes: A Case Study of Forex Exchange Speculation Victimization,” Master’s Thesis in Criminology and Criminal Justice, Faculty of Political Science, Chulalongkorn University, 2022. [In Thai]