สกสว

POLICY BRIEF

กองทุนส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (ววน.) ร่วมกับ
สำนักงานเลขาธิการสภาผู้แทนราษฎร และ สำนักงานเลขาธิการวุฒิสภา

ปีที่ 12 • ฉบับที่ 16/2566

ข้อเสนอแนะเชิงนโยบายต่อการป้องกันและแก้ไข

การตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ของผู้สูงอายุไทย

PRP
POLICY-RESEARCH PLATFORM

ข้อเสนอแนะเชิงนโยบายต่อการป้องกันและแก้ไข

การตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ของผู้สูงอายุไทย

ประเด็นสำคัญ

- ผู้สูงอายุไทยเกินครึ่งใช้อินเตอร์เน็ต และมากกว่าร้อยละ 80 ใช้โทรศัพท์มือถือ ในขณะเดียวกันก็มีความเสี่ยงต่อภัยไซเบอร์มากกว่ากลุ่มอายุอื่นๆ เนื่องจากเป็นกลุ่มอายุเดียวที่มีค่าเฉลี่ยของดัชนีชี้วัดสุขภาวะทางดิจิทัลอยู่ในระดับที่ต้องพัฒนา
- รูปแบบการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุมี 4 รูปแบบหลัก 1) การตกเป็นเหยื่อในการหลอกลวงให้ลงทุน 2) การตกเป็นเหยื่อการหลอกลวงทางโทรศัพท์เป็นขบวนการหรือแก๊งคอลเซ็นเตอร์ 3) การตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์ และ 4) การตกเป็นเหยื่อการหลอกลวงให้รักทางออนไลน์
- ข้อจำกัดสำคัญในการป้องกันและปราบปรามการกระทำความผิดที่เป็นการหลอกลวงทางไซเบอร์ ประกอบด้วยข้อจำกัดที่เกี่ยวข้องกับความซับซ้อนของการก่ออาชญากรรมโดยอาชญากรมืออาชีพ ข้อจำกัดในการแจ้งความดำเนินคดีของผู้เสียหาย ฐานความผิด ตลอดจนข้อจำกัดในการดำเนินคดีตามกระบวนการยุติธรรม และด้านความร่วมมือกับองค์กรทั้งในและต่างประเทศ

ผู้เขียน

รศ.ดร.รุ่งนภา เทพภาพ

กองบรรณาธิการ

- รศ.ดร.ภาคภูมิ ทิพคุณ
- นางสาวเยาวลัยา อ่อนโพธิ์ทอง
- นางสาวณิศ์ชากมล คงศรี
- นายภัควัฒน์ ภูริพงศ์ธนวัต

จัดทำโดย

- โครงการยกระดับกลไกการเชื่อมโยงงานวิจัยและนวัตกรรมกับฝ่ายนิติบัญญัติ (The Policy-Research Platform : PRP)
- สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.)

สถานที่ติดต่อ

- โครงการยกระดับกลไกการเชื่อมโยงงานวิจัยและนวัตกรรมกับฝ่ายนิติบัญญัติ วิทยาลัยสหวิทยาการ มหาวิทยาลัยธรรมศาสตร์ (ท่าพระจันทร์)

เลขที่ 2 แขวงพระบรมมหาราชวัง เขตพระนคร กรุงเทพฯ 10200

0-2613-2840 0-2623-5250

เกริ่นนำ

อาชญากรรมไซเบอร์ หมายถึง การกระทำผิดที่มีวัตถุประสงค์ทางอาญา โดยมีโครงข่ายคอมพิวเตอร์เข้ามาเกี่ยวข้องในการกระทำความผิด ไม่ว่าจะในฐานะเป็นเครื่องมือหรือเป้าหมาย หรือมีส่วนเกี่ยวข้องกับการกระทำผิดทางอาญา และมีความมุ่งหมายในการกระทำความผิดที่หลากหลายไม่ว่าจะเพื่อผลประโยชน์ทางการเงินในทางส่วนตัว หรือเพื่อคุกคามต่อความมั่นคงของชาติและความสงบเรียบร้อยของประชาชน (นันทวดี คาดคะเน, 2561 อ้างถึงในธัญพิชชา สามารถ, 2565) ลักษณะที่สำคัญของอาชญากรรมไซเบอร์ ประกอบด้วย 1) ความซับซ้อนของการกระทำผิดเนื่องจากเป็นการกระทำผิดโดยใช้ช่องทางอินเตอร์เน็ตหรือพื้นที่ไซเบอร์ที่จับต้องไม่ได้ และผู้กระทำผิดเป็นผู้ที่มีความรู้ความสามารถทำให้อาชญากรรมมีความซับซ้อนมากขึ้น 2) การก่ออาชญากรรมสามารถกระทำได้จากระยะไกล ไม่จำเป็นต้องอยู่ในพื้นที่เดียวกับเหยื่อ ทำให้การแสวงหาหลักฐานและการนำตัวผู้กระทำผิดมาดำเนินคดีมีความยุ่งยากมากขึ้น 3) ความเป็นนิรนาม กล่าวคือ ผู้กระทำผิด/อาชญากรสามารถจะเป็นบุคคลใดก็ได้ และอยู่ที่ใดก็ได้ อีกทั้งมีความสามารถในการปิดบังตัวตนของผู้ใช้งานอินเตอร์เน็ต ทำให้การระบุตัวตนผู้กระทำความผิดเป็นไปได้ยาก และ 4) อาชญากรรมค่อนข้างมีขนาดใหญ่ ซึ่งมักเกิดขึ้นหลายครั้งและมีผู้เสียหายจำนวนมากในวงกว้าง (Bandler & Merzon, 2020 อ้างถึงในธัญพิชชา สามารถ, 2565)

สถานการณ์ปัญหา

การสำรวจของสำนักงานสถิติแห่งชาติ (2565) เผยให้เห็นว่าผู้สูงอายุไทย (อายุ 60 ปีขึ้นไป) จำนวน 13.1 ล้านคน ใช้อินเตอร์เน็ตราว 6.9 ล้านคน (ร้อยละ 52.4) ใช้โทรศัพท์มือถือ 10.8 ล้านคน (ร้อยละ 82.5) โดยผู้สูงอายุในเขตเทศบาล/เขตเมืองจะมีสัดส่วนการใช้อินเตอร์เน็ตและมือถือสูงกว่าผู้สูงอายุที่อยู่นอกเขตเทศบาล/เขตชนบท การสำรวจในไตรมาสที่ 2 ของปี 2566 พบว่า ประชาชนอายุ 50 ปีขึ้นไปร้อยละ 49.7 เคยประสบภัยจากการใช้อุปกรณ์ดิจิทัล โดยถูกรบกวนโดยแก๊งคอลเซ็นเตอร์มากที่สุด ร้อยละ 44.2 รองลงมาคือ ได้รับข่าวปลอม (fake news) ผ่านสื่อสังคมออนไลน์ร้อยละ 19.5 และถูกหลอกจากการซื้อของออนไลน์ ร้อยละ 8.1 (สำนักงานสถิติแห่งชาติ, 2566) นอกจากนี้ ข้อมูลจากศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ ตั้งแต่วันที่ 1 มีนาคม 2565 - 30 กันยายน 2566 พบว่า การหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์ มีผู้เสียหายแจ้งความออนไลน์กว่า 27,509 เรื่อง หรือคิดเป็นร้อยละ 8.20 จากเรื่องการรับแจ้งความทั้งหมด สูงเป็นลำดับที่ 4 รองจากการหลอกลวงซื้อขายสินค้าออนไลน์ หลอกให้โอนเงินเพื่อทำงาน และหลอกให้กู้เงิน โดยมีมูลค่าความเสียหายกว่า 13,952 ล้านบาท สูงเป็นลำดับที่ 1 ของมูลค่าความเสียหายทั้งหมด (MGR Online, 2566) ดัชนีชี้วัดสุขภาวะดิจิทัลของคนไทย (Thailand Cyber Wellness Index) ที่ริเริ่มจัดทำโดย AIS พบว่า กลุ่มผู้สูงอายุวัย 60 ปีขึ้นไป มีความเสี่ยงต่อภัยไซเบอร์มากกว่ากลุ่มอายุอื่นๆ เนื่องจากเป็นกลุ่มอายุเดียวที่มีค่าเฉลี่ยของดัชนีชี้วัดสุขภาวะทางดิจิทัลอยู่ในระดับที่ต้องพัฒนา (AIS, 2566)

รูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ของผู้สูงอายุไทย

ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ หรืออาชญากรรมทางไซเบอร์ในหลายรูปแบบกล่าวคือ (ธัญพิชชา สามารถ, 2565)

▪ การตกเป็นเหยื่อในการหลอกลวงให้ลงทุน

ส่วนใหญ่เป็นการชักชวนจากบุคคลที่รู้จักในกลุ่มไลน์ โดยผู้ชักชวนจะมีประสบการณ์ในการลงทุนและได้รับผลตอบแทนจึงทำให้ผู้สูงอายุหลงเชื่อและร่วมลงทุน ผลจากการถูกกระทำ ทำให้ผู้สูงอายุบางกลุ่มไม่กล้าจะลงทุนอีก แต่บางกลุ่มกลับปรับเปลี่ยนตนเองไปแม่ทีม เพื่อชักชวนผู้อื่นมาลงทุน บางกลุ่มก็ยังคงมองหาการลงทุนใหม่ด้วยความหวังว่าจะได้เงินกลับมา

▪ การตกเป็นเหยื่อการหลอกลวงทางโทรศัพท์เป็นขบวนการหรือแก๊งคอลเซ็นเตอร์

ซึ่งมักเป็นการล่อลวงให้ผู้สูงอายุที่ตกเป็นเหยื่อเกิดความตกใจกลัว เกิดความโลภ หรือหลอกลวงให้เชื่อว่าเป็นบุคคลอื่นแล้วยืมเงิน ทั้งนี้แก๊งคอลเซ็นเตอร์ ถือเป็นอาชญากรรมข้ามชาติที่เป็นภัยคุกคามต่อประเทศไทยในปัจจุบัน (สุมนทิพย์ จิตสว่าง และคณะ, 2563) ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) หรือตำรวจไซเบอร์ รายงานว่ามีรูปแบบการหลอกลวงราว 18 รูปแบบที่กระทำโดยแก๊งคอลเซ็นเตอร์ ในปี 2564 มีรายงานว่ามีความเสียหายจากแก๊งคอลเซ็นเตอร์ถึง 1,600 ล้านบาท นอกจากนี้ศูนย์บริหารการรับแจ้งความคดีออนไลน์ สำนักตำรวจแห่งชาติ ได้รายงานว่า ระหว่างวันที่ 1 มีนาคม 2566-19 สิงหาคม 2566 มีการแจ้งความคดีออนไลน์มากถึง 313,804 เรื่อง (สักรินทร์ นิยมศิลป์ และกาญจนา เทียนลาย, 2566) เพื่อป้องกันและแก้ไขปัญหานี้รัฐบาลไทยได้กำหนดให้มีกฎหมายเฉพาะสำหรับการปราบปรามการหลอกลวงทางออนไลน์ เช่น จัดทำ พ.ร.ก. มาตรการป้องกันและปราบปรามการหลอกลวงทางออนไลน์ โดยเริ่มมีผลบังคับใช้ในวันที่ 17 มีนาคม 2566 ถือเป็นกลไกทางกฎหมายที่มุ่งเป้าไปที่การ **“แก้ไขปัญหาบัญชีม้า”** โดย มีการกำหนดบทลงโทษบัญชีม้า และให้ธนาคารสามารถระงับธุรกรรมที่ต้องสงสัย อย่างไรก็ตามมาตรการดังกล่าวก็ยังไม่เพียงพอที่จะจัดการปัญหาได้อย่างทันท่วงที นอกจากการระงับบัญชียังคงต้องใช้เวลา อีกทั้งกลุ่มมิจฉาชีพก็มีการพัฒนาระบบการทำงานเพื่อหลบเลี่ยงการติดตามของเจ้าหน้าที่อยู่อย่างต่อเนื่องตลาดเวลา (สักรินทร์ นิยมศิลป์ และกาญจนา เทียนลาย, 2566)

รูปแบบการหลอกลวงของแก๊งคอลเซ็นเตอร์มี 4 ลักษณะสำคัญ ได้แก่

1) **การใช้ความโลภของเหยื่อเป็นสิ่งจูงใจ** อาทิ หลอกลวงว่าจะได้รับเงิน/ทรัพย์สินหากมีการดำเนินการตามที่แก๊งคอลเซ็นเตอร์เสนอ เช่น ได้รับคืนภาษี ถูกรางวัล
2) **การใช้ความกลัวของเหยื่อ** โดยจะหลอกลวงผู้เสียหายเกี่ยวกับการเป็นหนี้ และความผิดต่างๆ อาทิ เป็นหนี้บัตรเครดิต หรือมีบัญชีธนาคารพัวพันกับยาเสพติด บัญชีจะต้องถูกอายัดและตรวจสอบโดยหน่วยงานของรัฐที่น่าเชื่อถือ อาทิ สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) เมื่อผู้เสียหายหลงเชื่อก็จะมีการดำเนินการทำธุรกรรมทางการเงินตามที่แก๊งคอลเซ็นเตอร์บอก
3) **การใช้ความไม่รู้หรือขาดความระวังในการปกป้องทรัพย์สินของเหยื่อ** อาทิ การปลอมแปลงหมายเลขโทรศัพท์ของธนาคารและอ้างว่าเป็นเจ้าหน้าที่ของธนาคารขอรหัสผ่าน

เพื่ออัปเดตแอปพลิเคชั่น อ้างว่ารหัสเก่าถูกยกเลิกไป โดยจะชักจูงล่อลวงให้เหยื่อบอกรหัสที่ถูกส่งผ่าน SMS แก่ตน นอกจากนี้ยังมีการหลอกลวงด้วยการนำเสนอขายประกันชีวิต ตลอดจนโปรโมชั่นต่าง ๆ ของธนาคาร

4) **การใช้ความเชื่อ/ความศรัทธาในการหลอกลวงเหยื่อ** อาทิ มีการเปิดเว็ปไซต์/เปิดโปรแกรมเฟซบุ๊คและโฆษณาเพื่อชักชวนเหยื่อให้ร่วมทำบุญ จัดสร้างพระ สร้างวัด จัดงานทำบุญต่างๆ ทำพิธีเสริมดวงชะตา การส่งเลขเด็ด (สุมนทิพย์ จิตสว่าง และคณะ, 2563)

■ การตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์

โดยผู้สูงอายุได้ให้ความไว้วางใจต่อร้านค้าออนไลน์ โดยไม่ได้ตรวจสอบยอดติดตาม หรือโปรไฟล์ร้านว่ามีความน่าเชื่อถือมากน้อยเพียงใด อีกทั้งไม่ได้ตรวจสอบให้ละเอียด รวมถึงการถูกล่อลวงด้วยการส่งเสริมการขายที่จูงใจ อาทิ ราคาต่ำกว่าท้องตลาด มีของแถมมากชิ้น และเทคนิคการตั้งราคาสินค้าไม่สูงมากนัก ทำให้การแจ้งความดำเนินคดีนั้นดูไม่คุ้มค่า

■ การตกเป็นเหยื่อการหลอกลวงให้รักทางออนไลน์ (Romance Scam)

ผู้กระทำผิดจะใช้เทคนิคทางจิตวิทยาในการหลอกลวง เพื่อให้เหยื่อหลงเชื่อและยินยอมให้ทรัพย์สินตามที่ผู้หลอกลวงชักจูง สำหรับผู้สูงอายุแล้ว การวิจัยชี้ให้เห็นว่าผู้กระทำผิดหลอกลวงผู้สูงอายุด้วยความรักความหลง เนื่องจากอยู่ในความเหงาและต้องการคนใกล้ชิดในช่วงวัยเกษียณ ผ่านการสร้างโปรไฟล์ที่น่าเชื่อถือ นอกจากนี้ผู้สูงอายุที่ตกเหยื่อเมื่อรู้ตัวว่าถูกหลอกลวงก็มักจะมีความอับอาย ไม่กล้าไปแจ้งความดำเนินคดี (ธัญพิชชา สามารถ, 2565) นอกจากนี้งานศึกษาของทศพล ทรรศนกุลพันธ์ และคณะ (2562) พบว่า ประเทศไทยมีผู้เสียหายจากพิศวาสอาชญากรรม (Romance Scam) มากขึ้น และไม่มีแนวโน้มที่จะลดลง ในช่วงเดือนมิถุนายน 2561- พฤษภาคม 2562 มีผู้เสียหายและโอนเงินในอาชญากรรมดังกล่าว 322 ราย มูลค่าความเสียหายประมาณ 193 ล้านบาท (ไม่นับรวมคดีที่ถูกร้องเรียนไปยังสถานีตำรวจ และที่เหยื่อไม่กล้าแจ้งความดำเนินคดี) ทั้งนี้ผู้ที่ตกเป็นเหยื่อส่วนใหญ่เป็นหญิงโสด อายุ 40-60 ปี เป็นผู้มีการศึกษาดี หน้าที่การงานมั่นคง มีทรัพย์สิน การวิจัยพบว่า เหยื่อกลุ่มนี้มีไม่ถึงร้อยละ 10 ที่มีการแจ้งความดำเนินคดีเมื่อถูกหลอกลวง ด้วยเหตุผลเกี่ยวกับความอับอายและการขาดความรู้เกี่ยวกับขั้นตอนและสถานที่ของการแจ้งความเมื่อถูกหลอกลวง และเข้าใจว่าการแจ้งความไม่ได้เกิดประโยชน์ เพราะไม่น่าจะดำเนินคดีกับอาชญากรได้ ฉะนั้นอาชญากรรมชนิดนี้จึงไม่มีแนวโน้มลดลง

สาเหตุสำคัญที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์

สาเหตุที่สำคัญ พิจารณาได้ 3 มิติ กล่าวคือ **มิติที่ 1 ตัวผู้สูงอายุเอง** อาทิเช่น ความรู้สึกไม่มั่นคงทางด้านรายได้ของผู้สูงอายุ ฉะนั้นจึงมักหลงเชื่อเมื่อมีผู้มาชักชวนให้ลงทุน เนื่องจากคาดหวังที่จะได้มีเงินมากขึ้นในช่วงบั้นปลายของชีวิต, ความมั่นใจในตนเอง ซึ่งเป็นพัฒนาการของชีวิตที่มีการสะสมประสบการณ์มาอย่างยาวนานในการใช้ชีวิต ฉะนั้นในบางครั้งจึงไม่เห็นความสำคัญของการปรึกษาหารือสมาชิกในครอบครัวก่อนตัดสินใจลงทุน, การขาดความรู้ในเรื่องของการลงทุนการหลอกลวงทางไซเบอร์ ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวง, ภาวะไม่มั่นคงทางอารมณ์ รู้สึกโดดเดี่ยวในช่วงบั้นปลาย จึงมองหาที่พึ่งพิง โดยเฉพาะในกลุ่มที่เป็นเหยื่อของของการหลอกให้รักทางออนไลน์ **มิติที่ 2 ผู้กระทำผิด/ผู้หลอกลวง** กล่าวคือ เป็นกลุ่มบุคคลที่ใกล้กับผู้สูงอายุ เช่น ญาติ เพื่อนฝูง ผู้สูงอายุจึงไว้วางใจ นอกจากนี้หากมิใช่คนใกล้ชิด ก็มักจะเป็นบุคคลที่มีการสร้าง/แสดงภาพลักษณ์น่าเชื่อถือ จูงใจให้ผู้สูงอายุไว้วางใจ ตลอดจนมีเทคนิควิธีในการจูงใจล่อลวงในรูปแบบต่างๆ เช่น การหลอกลวงให้ซื้อของออนไลน์ในราคาที่ไม่สูงและมีการส่งเสริมการตลาดที่จูงใจสูง และ**มิติที่ 3 สภาพแวดล้อม** อาทิ ความคาดหวังที่สังคมมีต่อผู้สูงอายุในฐานะผู้ที่มีประสบการณ์ในการใช้ชีวิตอย่างโชกโชน ทำให้ผู้สูงอายุไม่กล้าเปิดเผยประสบการณ์การตกเหยื่อการหลอกลวงของตนเอง โดยเฉพาะในกลุ่มที่ตกเป็นเหยื่อของการถูกหลอกให้รัก ผู้สูงอายุมักอับอายและไม่กล้าที่จะไปแจ้งความดำเนินคดีกับผู้กระทำผิด นอกจากนี้ความเจริญก้าวหน้าทางเทคโนโลยีเพิ่มโอกาสให้ผู้สูงอายุที่เข้าถึงเทคโนโลยีมีโอกาสถูกหลอกลวงทางไซเบอร์มากยิ่งขึ้น เนื่องจากเห็นโฆษณาชวนเชื่อต่างๆมากขึ้น และในกลุ่มที่ยังไม่คุ้นเคยกับกับเทคโนโลยี ผู้สูงอายุอาจไม่ระมัดระวังทำให้มีการเผยแพร่ข้อมูลส่วนตัวให้กับมิจฉาชีพได้ (ธัญพิชชา สามารถ, 2565)

ข้อจำกัดสำคัญในการป้องกันและปราบปรามการกระทำความผิดที่เป็นการหลอกลวงทางไซเบอร์

ข้อค้นพบจากการศึกษาวิจัยพบว่า การดำเนินการเพื่อป้องกันและปราบปรามการกระทำผิดทาง ไซเบอร์มีข้อจำกัดในการดำเนินการจับกุมผู้กระทำผิด และการดำเนินคดีตามกระบวนการยุติธรรม (ทศพล ทรรศนกุลพันธ์ และคณะ, 2562; สุมนทิพย์ จิตสว่าง และคณะ, 2563) ดังต่อไปนี้

■ ข้อจำกัดอันเนื่องมาจากการเป็นการก่ออาชญากรรม โดยอาชญากรมืออาชีพ

การหลอกลวงทางไซเบอร์ อาทิ พิศวาสอาชญากรรม แก๊งคอลเซ็นเตอร์ มักกระทำโดยอาชญากรมืออาชีพที่มีความรู้ความเชี่ยวชาญ มีทักษะในการประกอบอาชญากรรม มีการแบ่งงานกันอย่างเป็นระบบชัดเจน มีบทเรียนในการฝึกทักษะการหลอกหลวงให้กับสมาชิกในเครือข่าย/แก๊ง มีการศึกษาข้อมูลบริบททางสังคม การเงิน ข้อกฎหมายต่างๆของประเทศที่ต้องการหลอกลวง (สุมนทิพย์ จิตสว่าง และคณะ, 2563)

■ ข้อจำกัดเกี่ยวกับการแจ้งความดำเนินคดีของผู้เสียหาย

เมื่อเกิดเหตุการณ์ขึ้นข้อจำกัดที่สำคัญ คือ ผู้เสียหายไม่ค่อยอยากจะไปยุ่งยากอะไรเกี่ยวกับกระบวนการกฎหมาย เพราะมองว่ายุ่งยาก ใช้เวลายาวนาน และไม่มีความแน่ใจว่าคดีจะคืบหน้าหรือทำให้ได้ทรัพย์กลับมาหรือไม่ อีกทั้งในกลุ่มที่มีสถานะทางสังคมดีก็จะกังวลเรื่องของการเสียชื่อเสียง (ทศพล ทรรศนกุลพันธ์ และคณะ, 2562) นอกจากนี้ผู้เสียหายเองบางส่วนก็ไม่ได้ให้ความร่วมมือกับเจ้าหน้าที่ตำรวจอย่างแท้จริง โดยเฉพาะผู้เสียหายซึ่งเป็นนักท่องเที่ยวที่อาศัยอยู่ในประเทศไทยไม่นาน กรณีของผู้เสียหายที่ตกเป็นเหยื่อของการหลอกให้เล่นพนัน ศาลมักจะเห็นว่าผู้เสียหายเป็นผู้ร่วมกระทำผิดและสมัครใจเล่นเอง จึงมักยกฟ้องในข้อหาฉ้อโกง หากจะมีการลงโทษในข้อหาดังกล่าว จะต้องมีการพิสูจน์ได้อย่างแท้จริงว่าผู้กระทำผิดมีเจตนาหลอกเหยื่อให้มากระทำผิดตั้งแต่แรกซึ่งเป็นการพิสูจน์ที่ยากมาก (สุมนทิพย์ จิตสว่าง และคณะ, 2563)

■ ข้อจำกัดอันเนื่องมาจากฐานความผิด

การตั้งข้อกล่าวหาในการดำเนินคดีการหลอกลวงทางไซเบอร์โดยส่วนใหญ่จะเป็นตั้งข้อหาฉ้อฉลหลอกลวงประชาชน ซึ่งจะต้องมีการดำเนินคดีด้วยการใช้กฎหมายอาญาในการดำเนินคดีและการหลอกลวงเป็นหลัก ซึ่งมีกำหนดโทษที่ไม่สูงมากนัก ทำให้ผู้กระทำผิดสามารถขอประกันตัวจากศาลได้และอาจนำไปสู่การหนีประกันในชั้นศาล ทั้งนี้หากเจ้าหน้าที่ตำรวจตั้งข้อหาในรูปแบบของอาชญากรรมข้ามชาติจะทำให้เจ้าหน้าที่ตำรวจและกระบวนการยุติธรรมสามารถดำเนินคดีได้ตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 ที่มีการกำหนดโทษที่มีความรุนแรงมากขึ้น แต่ก็จะประสบปัญหาความยุ่งยากในการดำเนินการ เนื่องจากเป็นความผิดนอกราชอาณาจักร การสอบสวนกำหนดให้ต้องได้รับมอบอำนาจจากอัยการ อีกทั้งเจ้าหน้าที่ส่วนหนึ่งขาดความรู้ความเข้าใจต่อการดำเนินคดีกับองค์กรอาชญากรรมข้ามชาติรวมทั้งมีปัญหาในการประสานงานระหว่างหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอกประเทศ (สุมนทิพย์ จิตสว่าง และคณะ, 2563)

■ ข้อจำกัดในการดำเนินคดีตามกระบวนการยุติธรรม

ในชั้นของกระบวนการยุติธรรมคดีนี้มักจะหยุดลงในชั้นของพนักงานสอบสวน เนื่องจากลักษณะของการกระทำความผิดที่ไม่สามารถระบุได้อย่างแน่ชัดว่าเป็นการกระทำผิด และผู้กระทำก็ไม่แน่ใจว่าอยู่ในหรือนอกราชอาณาจักร เนื่องจากผู้กระทำผิดมักอำพรางตัวตน ดังนั้นจึงมักมีปัญหาว่าพนักงานสอบสวนในท้องที่ใดควรจะเป็นผู้มีอำนาจสอบสวน เพราะการสอบสวนโดยพนักงานสอบสวนที่ไม่มีอำนาจจะเป็นการสอบสวนที่ไม่ชอบด้วยกฎหมาย พนักงานอัยการไม่มีอำนาจฟ้อง และศาลจะยกฟ้องคดีนี้ในที่สุด ขั้นตอนในการสอบสวนพนักงานสอบสวนจะเริ่มทำการสอบสวนเพื่อให้ได้มาซึ่งผู้กระทำผิด แต่ต้องเผชิญกับอุปสรรคในการรวบรวมพยานหลักฐานของพนักงานสอบสวน 3 กรณี คือ 1) อุปสรรคด้านเวลา 2) อุปสรรคด้านทรัพยากร อาทิ เครื่องมือ กำลังพล งบประมาณ และ 3) อุปสรรคด้านการติดตามตัวผู้กระทำผิด นอกจากนี้หากเจ้าพนักงานตั้งฐานความผิดคดีนี้เป็นคดีฉ้อโกง ย่อมส่งผลให้มีการยอมความได้ ดังนั้นหากผู้เสียหายตัดสินใจถอนคำร้องทุกข์/ยุติการดำเนินคดี เจ้าพนักงานตำรวจก็ไม่สามารถดำเนินคดีนี้ต่อไปได้ ในการแก้ไขจำเป็นต้องดำเนินคดีนี้ในฐานะที่ผู้กระทำผิดเป็นองค์กรอาชญากรรมข้ามชาติ อันจะทำให้คดีนี้กลายเป็นคดีอาญาแผ่นดินและเจ้าพนักงานตำรวจสามารถดำเนินคดีนี้ต่อไปได้แม้ว่าผู้เสียหายจะถอนคำร้องทุกข์/ยุติการดำเนินคดีแล้วก็ตาม การจับกุม พนักงานสอบสวนแทบจะไม่สามารถตามผู้กระทำผิดที่แท้จริงมาลงโทษได้ ทำได้เพียงการสืบเส้นทางการเงินของผู้ร่วมกระทำความผิดที่เป็นเจ้าของบัญชี และนำไปขยายผล แต่ก็มักทำได้ยาก เนื่องจากผู้กระทำผิดมักอาศัยอยู่นอกราชอาณาจักรหรือไม่สามารถหาหลักฐานมายืนยันได้ว่าผู้กระทำผิดคือใคร ขั้นกระบวนการพิจารณาของศาลเมื่อพนักงานสอบสวนไม่สามารถหาพยานหลักฐานมายืนยันจนศาล **“สิ้นสงสัย”** ว่าจำเลยเป็นผู้กระทำผิดที่แท้จริง ศาลก็ต้องปล่อยจำเลยนั้นไป และมิอาจจะมีคำสั่งให้บังคับคดียึดทรัพย์ หรือชดใช้สินไหมทดแทนทางแพ่งได้ (ทศพล ทรรศนกุลพันธ์ และคณะ, 2562)

■ ข้อจำกัดด้านความร่วมมือกับองค์กรทั้งในและต่างประเทศ

การหลอกลวงทางไซเบอร์ เช่น การพิศวาสไซเบอร์ แก๊งคอลเซ็นเตอร์ ถือเป็นการก่ออาชญากรรมในลักษณะขององค์กรอาชญากรรมข้ามชาติ ซึ่งหมายถึงการกระทำผิดโดยละเมิดกฎหมายอาญา ผู้ก่อการกระทำขึ้นในประเทศหนึ่งมีผลเสียหายเชื่อมโยงอีกประเทศหนึ่งหรือ

มากกว่า (สุมนทิพย์ จิตสว่าง และคณะ, 2563) ฉะนั้นจึงจำเป็นที่จะต้องมีการประสานงานกับหน่วยงานทั้งภายในและต่างประเทศในเวลาที่รวดเร็ว แต่ในทางปฏิบัติการประสานงานเต็มไปด้วยความซับซ้อนและต้องใช้เวลา จึงทำให้เกิดความล่าช้าในการดำเนินคดี

ข้อเสนอแนะ

มาตรการเชิงเฝ้าระวังและป้องกันการตกเป็นเหยื่อของการหลอกหลวงทางไซเบอร์ของผู้สูงอายุ

1) การป้องกันการตกเป็นเหยื่อในระดับบุคคล เน้นการส่งเสริมให้ผู้สูงอายุป้องกันตนเองได้จากการถูกหลอกลวงทางไซเบอร์ เป็นต้นว่า สนับสนุนความรู้ความเข้าใจเรื่องการเงินส่วนบุคคลสำหรับผู้สูงอายุ การรักษาข้อมูลและความลับส่วนบุคคล ความรู้การใช้งานอินเตอร์เน็ตและโลกออนไลน์อย่างปลอดภัย ข้อมูลรูปแบบของการหลอกลวงทางไซเบอร์ในรูปแบบต่าง ๆ
2) การป้องกันในระดับชุมชนท้องถิ่น โดยให้ชุมชนเข้ามามีส่วนร่วมในการเฝ้าระวังและป้องกันปัญหา เช่น ร่วมกันรณรงค์ ให้ข้อมูลข่าวสารการหลอกหลวงทางไซเบอร์รูปแบบต่าง ๆ ให้กับผู้สูงอายุ รวมถึงผู้ดูแล และ/หรือคนวัยอื่น ๆ ซึ่งเป็นสมาชิกของชุมชน ทั้งนี้การทำงานในระดับชุมชนท้องถิ่นควรมีเจ้าภาพหลัก อาทิเช่น องค์กรปกครองส่วนท้องถิ่น และ/หรือคณะกรรมการหมู่บ้าน มีการจัดตั้งทีมไซเบอร์ชุมชน เพื่อเป็นหน่วยในการให้คำปรึกษาและให้ความรู้ด้านเทคโนโลยีต่าง ๆ

มาตรการเชิงนโยบายและการปราบปรามผู้กระทำผิด

1) ควรกำหนดให้ภัยคุกคามจากอาชญากรรมทางไซเบอร์เป็นวาระสำคัญของชาติ ควรมีการจัดตั้งกลไก/คณะทำงานระดับสูงแบบ War Room โดยมีนายกรัฐมนตรีเป็นผู้ออกคำสั่ง
2) การบูรณาการความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องเนื่องจากการหลอกลวงทางไซเบอร์ ถือเป็นการกระทำความผิด/อาชญากรรมโดยอาชญากรมืออาชีพ ฉะนั้นจึงจำเป็นที่แต่ละหน่วยงานจักต้องทำงานในเชิงบูรณาการและร่วมมือกันอย่างแข็งขัน ไม่ว่าจะเป็นสำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ (DSI) คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ซึ่งเป็นหน่วยงานกำกับควบคุมดูแลกิจการโทรศัพท์และเครือข่ายผู้ใช้บริการทางโทรศัพท์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ธนาคาร สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) กรมสรรพากร ตลอดจนนักวิชาการ
3) การพัฒนาบุคลากรที่เกี่ยวข้องเพิ่มมากขึ้น (ทั้งจำนวนบุคลากรและทักษะความรู้) ซึ่งเป็นบุคลากรที่มีความเข้าใจอาชญากรรมเกี่ยวกับคอมพิวเตอร์ในภาพรวมทั้งหมด ความรู้เกี่ยวบริบททางเทคโนโลยี (Digital Context) รู้ข้อเท็จจริงทางเทคโนโลยี (Digital Fact) และรู้วิถีทางดิจิทัล (Digital Way)
4) ควรตั้งหน่วยงานเฉพาะเพื่อดำเนินการป้องกันและปราบปราม และใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) ในการตรวจสอบ
5) การเพิ่มบทลงโทษทางกฎหมายและใช้มาตรการยึดทรัพย์และการดำเนินการทางภาษีอากร ควรการกำหนดการเอาผิดทางกฎหมายหนักตาม พ.ร.บ. ป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 กับเครือข่ายผู้การสนับสนุน
6) การทำงานในลักษณะหน่วยงานเดียวกันทั้งโลก (One Team One World) เพื่อตอบสนองต่อการหลอกลวงทางไซเบอร์ในฐานะที่เป็นอาชญากรรมข้ามชาติ จำเป็นต้องอาศัยการทำงานร่วมกันในการป้องกันและปราบปราม การสืบสวน สอบสวน สามารถกระทำได้อย่างมีประสิทธิภาพผ่านการสร้างความร่วมมือระหว่างประเทศในการแลกเปลี่ยนข่าวกรอง การตรวจสอบความร่วมมือและการดำเนินงานที่ตรงกันโดยเฉพาะการก่ออาชญากรรมข้ามชาติเกี่ยวข้องกับหลายประเทศ การช่วยเหลือในการสืบสวนข้อเท็จจริงทางอาญา

มาตรการในการเยียวยาผู้เสียหาย

1) ออกแบบวิธีการร้องทุกข์และดำเนินคดีที่ไม่ต้องเปิดเผยตัวตนหรือเป็นช่องทางร้องเรียนประสานงานออนไลน์ เพื่อลดข้อจำกัดที่เป็นอุปสรรคต่อการเข้าแจ้งความดำเนินคดีต่อผู้กระทำของผู้เสียหายที่มีต้องเป็นเหยื่อของการถูกหลอกหลวงทำให้เกิดความอับอาย
2) พัฒนากระบวนการที่สามารถช่วยเหลือเยียวยาในความเสียหายทางแพ่งและการติดตามทรัพย์สินกลับคืนมาชดใช้สินไหมทดแทน

เอกสารอ้างอิง

- ธัญพิชชา สามารถ. (2565). **การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ**. กรุงเทพฯ: จุฬาลงกรมหาวิทยาลัย. เข้าถึงจาก https://digital.car.chula.ac.th/chulaetd/6716
- ทศพล ทรรศนกุลพันธ์ และคณะ. (2562). **รายงานฉบับสมบูรณ์ โครงการข้อจำกัดของกระบวนการยุติธรรมเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม (Romance Scam) และแนวทางสร้างความตระหนักรู้ให้กับประชาชน**. กรุงเทพฯ: สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.)
- สุมนทิพย์ จิตสว่าง และคณะ. (2563). **รายงานวิจัยฉบับสมบูรณ์ โครงการอาชญากรรมข้ามชาติ: ภัยคุกคามประเทศไทยเกี่ยวกับแก๊งคอลเซ็นเตอร์**. กรุงเทพฯ: สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.)
- สักรินทร์ นิยมศิลป์ และกาญจนา เทียนลาย. (2566). **Policy Brief แก้ปัญหาเชิงรุก “แก๊งคอลเซ็นเตอร์” ในสุขภาพคนไทย**. (2566). นครปฐม: สถาบันวิจัยประชากรและสังคม มหาวิทยาลัยมหิดล.
- สำนักงานสถิติแห่งชาติ.(2565). **สรุปผลที่สำคัญการมีการใช้ไอซีทีของผู้สูงอายุ พ.ศ. 2565**. เข้าถึงจาก https://www.nso.go.th/nsoweb/storage/survey_detail/2023/20230929102632_92912.pdf
- สำนักงานสถิติแห่งชาติ.(2566). **การสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2566 (ไตรมาส 2)**. เข้าถึงจาก https://www.nso.go.th/nsoweb/storage/survey_detail/2023/20230921150748_47692.pdf
- Thai PBS. (2567). **ข้อมูลผู้สูงอายุรั่วไหลเกือบ 20 ล้านชุด ถูกขายในเว็บใต้ดิน**. เข้าถึงจาก https://www.thaipbs.or.th/news/content/336796
- MGR Online. (2566). **เตือนภัยผู้สูงอายุ! ตำรวจไซเบอร์พบถี่ มิจฉาชีพใช้คำหวานหลอกลวงให้ลงทุน ฝากบุตรหลานช่วยดูแลใกล้ชิด**. เข้าถึงจาก https://mgronline.com/crime/detail/9660000092629
- AIS. (2566). **ดัชนีชี้วัดสุขภาวะดิจิทัลของคนไทย (Thailand Cyber Wellness Index)**. เข้าถึงจาก https://sustainability.ais.co.th/storage/update/report/advanc-ebook-thailand-cyber-wellness-th.pdf

PRP POLICY-RESEARCH PLATFORM

โครงการยกระดับกลไกการเชื่อมโยงงานวิจัยและนวัตกรรมกับฝ่ายนิติบัญญัติ
(The Policy-Research Platform : PRP)
เลขที่ 2 แขวงพระบรมมหาราชวัง เขตพระนคร กรุงเทพฯ 10200
โทรศัพท์ : 0-2613-2840 โทรสาร : 0-2623-5250