แนวทางการป้องกันอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ออนไลน์โดยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคม
(ฉบับสมบูรณ์)

นางสาว ขวัญชนก ศรีภมร

เอกัตศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรมหาบัณฑิต
สาขาวิชากฎหมายเศรษฐกิจ
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2565

หัวข้อเอกัตศึกษา	แนวทางการป้องกันอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ออนไลน์โดยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคม
โดย	นางสาวขวัญชนก ศรีภมร
รหัสประจำตัว	648 01920 34
หลักสูตร	ศิลปศาสตรมหาบัณฑิต สาขาวิชากฎหมายเศรษฐกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
หมวดวิชา	กฎหมายธุรกิจทั่วไป
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ ดร.ณัชพล จิตติรัตน์
ปีการศึกษา	2565

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้เอกัตศึกษาฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรมหาบัณฑิต สาขาวิชากฎหมายเศรษฐกิจ

ลงชื่อ.....อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ ดร.ณัชพล จิตติรัตน์)

บทคัดย่อ

เนื่องจากสภาพสังคมของประเทศไทยในปัจจุบันได้มีการอาศัยเทคโนโลยีในการดำรงชีวิตประจำวันมากขึ้นโดยเฉพาะอย่างยิ่งการติดต่อสื่อสารที่มีการพัฒนาและเจริญก้าวหน้าไปอย่างรวดเร็วโดยมีรูปแบบการติดต่อสื่อสารผ่านช่องทางที่หลากหลายจนทำให้เกิดช่องว่างในการหลอกลวงของแก๊งคอลเซ็นเตอร์ซึ่งส่งผลกระทบทางด้านการเงินต่อเศรษฐกิจในประเทศไทยเป็นอย่างมาก

จากการค้นคว้ากฎหมายที่เกี่ยวข้องเกี่ยวกับเรื่องแก๊งคอลเซ็นเตอร์ ผู้วิจัยพบว่าในประเทศไทยได้มีการบังคับใช้กฎหมายที่ใช้ในการปราบปรามโดยการกำหนดความผิดทางอาญาซึ่งยังไม่รวมถึงมาตรการการป้องกันอาชญากรรมโดยความร่วมมือของเอกชนประกอบกับบริบทต่างๆที่ทำให้การบังคับกฎหมายดังกล่าวยังไม่มีประสิทธิภาพเท่าที่ควรจึงทำให้ไม่สามารถจับกุมและกวาดล้างได้อย่างสมบูรณ์เนื่องจากมิจฉาชีพเหล่านี้มักมีที่อยู่ไม่เป็นหลักแหล่งและรูปแบบการหลอกลวงมีวิธีที่ซับซ้อนมากขึ้นทำให้ยากต่อการสืบสาวต้นตอประกอบกับบทกฎหมายที่ใช้ในการปราบปรามซึ่งผู้วิจัยมองว่าเป็นการแก้ปัญหาทางปลายเหตุ เนื่องจากบทกฎหมายที่เกี่ยวข้องมักเป็นบทกฎหมายทางอาญา การที่จะสามารถลงโทษผู้กระทำความผิดดังกล่าวได้จะต้องเกิดเหตุการณ์ขึ้นแล้วเท่านั้น ดังนั้นการที่จะนำตัวผู้กระทำความผิดมาลงโทษแทบจะไม่ได้มีผลอะไรที่ทำให้แก๊งคอลเซ็นเตอร์ลดน้อยลง ดังนั้นประเทศไทยจึงควรหันมาให้ความสำคัญกับการป้องกันและกำกับดูแลก่อนที่จะเกิดเหตุเสียมากกว่า เพราะการหาแนวทางในการป้องกันตั้งแต่ต้นจะสามารถช่วยลดความเสียหายได้ไม่มากก็น้อยและเป็นการสร้างความตื่นตัวให้กับประชาชน (Public Awareness Raising) ในการระมัดระวังแก๊งคอลเซ็นเตอร์ในปัจจุบัน

ปัญหาการจับกุมและการบังคับใช้กฎหมายในการปราบปรามดังกล่าวก็เป็นปัญหาหลักของต่างประเทศเช่นเดียวกับประเทศไทย ดังนั้นในเมื่อขั้นตอนในการจับกุมหรือปราบปรามเป็นขั้นตอนที่ทำได้ยากในทางปฏิบัติ จากการศึกษาของผู้วิจัยพบว่าในต่างประเทศมักจะเน้นการบังคับใช้แผนปฏิบัติการเชิงรุกและมาตรการทางกฎหมายที่ใช้การป้องกันแก๊งคอลเซ็นเตอร์เพื่อที่จะช่วยบรรเทาความเสียหายให้กับประชาชนมากกว่าการเน้นการปราบปรามและวิธีที่จะช่วยการป้องกันได้ดีคือการให้ภาคส่วนที่เกี่ยวข้องกับอุตสาหกรรมโทรคมนาคมเป็นตัวดักจับความผิดปกติของหมายเลข

โทรศัพท์เนื่องจากแก๊งคอลเซ็นเตอร์ส่วนใหญ่มักใช้หมายเลขโทรศัพท์ที่ผิดกฎหมายหรือหมายเลขโทรศัพท์ที่ไม่มีคนใช้งานโดยใช้เทคโนโลยีในการแปลงหมายเลขและแอบอ้างเป็นหน่วยงานหรือบุคคลที่น่าเชื่อถือ ดังนั้นถ้าในส่วนของต้นทางคือกิจการโทรคมนาคมสามารถทำการตรวจสอบหรือตรวจพบตั้งแต่แรกจะทำให้ประชาชนเกิดความสูญเสียลดน้อยลง ซึ่งจากการที่ต่างประเทศหันมาสนใจการป้องกันมากกว่าปราบปรามพบว่าสถิติการสูญเสียของประชาชนลดลงอย่างมีนัยสำคัญ ดังนั้นการออกมาตรการทางกฎหมายในการป้องกันหมายเลขโทรศัพท์ที่มีความผิดปกติไม่ว่าจะเป็นจัดให้แผนปฏิบัติการที่เป็นรูปธรรม การพิสูจน์และยืนยันตัวตน การตรวจสอบและแบ่งปันข้อมูลโทรศัพท์ที่กระทำผิดระหว่างหน่วยงานภาครัฐและเอกชนโดยเฉพาะอย่างยิ่งการสร้างความตระหนักรู้ให้ประชาชนแม้ว่าจะไม่ได้ช่วยลดปริมาณการโทรเข้ามาหลอกลวงประชาชนแต่ช่วยให้ลดความสูญเสียทางด้านการเงินได้อย่างมากเนื่องจากประชาชนได้ตระหนักถึงการหลอกลวงและมีความรู้ในการตัดสินใจว่าหมายเลขโทรศัพท์ดังกล่าวที่โทรเข้ามาเป็นการหลอกลวงหรือไม่

แม้ว่าประเทศไทยจะมีสำนักงาน กสทช. ที่มีอำนาจทางกฎหมายในการออกประกาศในเรื่องต่างๆเพื่อใช้บังคับกับผู้ให้บริการโทรคมนาคมที่ต้องปฏิบัติตามไม่ว่าจะเป็นเรื่องการพิสูจน์และยืนยันตัวตนหรือเรื่องอื่นๆก็ตาม ในส่วนการออกประกาศในการจัดให้มีการตรวจสอบยืนยันตัวตนแต่วัตถุประสงค์หลักคือการรักษาสิทธิของผู้ใช้บริการโดยที่ผู้ให้บริการไม่สามารถขัดขวางได้ซึ่งทำให้ขั้นตอนและวิธีการต่างๆอาจจะยังคงมีช่องโหว่อยู่บ้างเนื่องจากประกาศฉบับไม่ได้เน้นการป้องกันกรณีที่ผู้บริโภคจะถูกหลอกลวงจากการสวมสิทธิการย้ายหมายเลขโทรศัพท์ ด้วยเหตุนี้ผู้วิจัยจึงเห็นว่าในเมื่อสำนักงาน กสทช. ได้รับอำนาจจากกฎหมายในการออกประกาศแล้ว สำนักงาน กสทช.ควรออกประกาศเกี่ยวกับวิธีการยืนยันตัวตนเพื่อป้องกันการหลอกลวงทางโทรศัพท์โดยเฉพาะแยกเป็นอีกหนึ่งฉบับ เพื่อจะได้นำมาปรับขั้นตอนและวิธีการพิสูจน์ยืนยันตัวตนให้เหมาะสมกับการป้องกันการหลอกลวงทางโทรศัพท์ นอกจากนี้ควรผลักดันให้ภาครัฐส่งเสริมการนำเทคโนโลยีมาใช้ในการเชื่อมต่อฐานข้อมูลกับผู้ให้บริการโทรคมนาคมในการตรวจสอบหมายเลขโทรศัพท์เพื่อที่จะได้ทำการตรวจจับหรือปิดกั้นการใช้งานหมายเลขได้อย่างทันท่วงทีและส่งเสริมการร่วมกันทำงานแบบบูรณาการโดยรวมเป็นฐานข้อมูลส่วนกลางไม่แยกส่วนเนื่องจากในปัจจุบันผู้ให้บริการโทรคมนาคมแต่ละเครือข่ายยังคงทำงานแยกเป็นอิสระรวมไปถึงขั้นตอนในการตรวจสอบหมายเลขที่ต้องผ่านกระบวนการและใช้เวลาค่อนข้างมาก ทำให้บางครั้งการจำกัดการเข้าถึงหมายเลขโทรศัพท์เหล่านั้นอาจไม่ทันการประกอบกับเพื่อลดความเป็นอิสระของหน่วยงานทั้งภาครัฐและภาคเอกชนให้น้อยลง

กิตติกรรมประกาศ

เอกัตศึกษาฉบับนี้สำเร็จลุล่วงได้ด้วยความกรุณาเป็นอย่างยิ่งจากผู้ช่วยศาสตราจารย์ ดร.ณัชพล จิตติรัตน์ ที่ได้ให้ความกรุณารับเป็นอาจารย์ที่ปรึกษาเอกัตศึกษาให้กับผู้เขียนและได้คำแนะนำข้อคิดเห็นต่าง ๆ ที่เป็นประโยชน์ต่อการจัดทำเอกัตศึกษาฉบับนี้ให้สมบูรณ์ ตลอดจนตรวจทานและปรับปรุงแก้ไขข้อบกพร่องต่าง ๆ ด้วยความเอาใจใส่อย่างดียิ่ง ผู้เขียนขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ผู้เขียนขอขอบพระคุณบิดา มารดาและครอบครัว รวมถึงคณาจารย์ทุกท่าน เพื่อน ๆ พี่ ๆ น้อง ๆ หลักสูตรศิลปศาสตรมหาบัณฑิต สาขาวิชากฎหมายเศรษฐกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัยที่ให้การสนับสนุน ให้ความช่วยเหลือและเป็นกำลังใจสำคัญให้แก่ผู้เขียนจนทำให้เอกัตศึกษาฉบับนี้สำเร็จลุล่วงไปด้วยดี

ผู้เขียนหวังเป็นอย่างยิ่งว่าเอกัตศึกษาฉบับนี้จะก่อให้เกิดประโยชน์แก่บุคคลทั่วไปที่สนใจศึกษา หากมีข้อผิดพลาดประการใด ผู้เขียนกราบขออภัยและขอน้อมรับไว้แต่เพียงผู้เดียว

สารบัญ

สารบัญรูปภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

อาชญากรรมทางเทคโนโลยีถือเป็นเหตุการณ์ทางสังคมที่สามารถเกิดขึ้นได้ตลอดเวลาในยุคปัจจุบัน โดยเฉพาะอย่างยิ่งเมื่อเทคโนโลยีเข้ามามีบทบาทและแทรกซึมการดำรงชีวิตประจำวันอีกทั้งการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็วของเทคโนโลยีทำให้เกิดสภาวะโลกไร้พรมแดน (Globalization) การติดต่อสื่อสารหรือการทำธุรกรรมต่างๆสามารถทำได้อย่างสะดวกและมีความคล่องตัวสูง โดยไม่ว่าจะอยู่ที่ไหนบนโลกก็สามารถทำธุรกรรมหรือติดต่อสื่อสารกันได้ง่ายมากขึ้นยกตัวอย่างเช่น ด้านการเงินการลงทุนหรือแม้กระทั่งการซื้อสินค้าหรือบริการเพียงแค่คลิกผ่านหน้าจอก็สามารถสั่งซื้อสินค้าได้ทันที เป็นต้น ในเมื่อมีข้อดีแล้วย่อมมีข้อเสียเกิดขึ้นคือเกิดการแทรกซึมของขบวนการอาชญากรรมในรูปแบบต่างๆโดยในปัจจุบันเหล่ามิจฉาชีพมักจะนิยมใช้เทคโนโลยีเป็นสื่อกลางทำให้การใช้กฎหมายบังคับเป็นไปได้ยาก เนื่องจากสืบหาที่มาของต้นตอได้ยากส่งผลให้รูปแบบอาชญากรรมมีความหลากหลายและมีวิธีการที่ซับซ้อนมากขึ้น พฤติกรรมดังกล่าวจึงเป็นที่มาของคำว่า“อาชญากรรมทางเทคโนโลยี” หรือ“อาชญากรรมไซเบอร์”[1] ซึ่งอาชญากรรมทางเทคโนโลยีคือการนำเทคโนโลยีหลากหลายรูปแบบและซับซ้อนมาใช้ผสมกับการกระทำความผิด ในบางครั้งมีการดำเนินการเป็นเครือข่ายข้ามประเทศโดยมีลักษณะเกี่ยวข้องกับการฟอกเงินและการฉ้อโกงประชาชน ทั้งนี้ลักษณะของอาชญากรรมดังกล่าวสามารถนำไปสู่อาชญากรรมข้ามชาติได้ซึ่งส่งผลกระทบต่อประชาชนเป็นวงกว้างและสร้างความเสียหายแก่ระบบเศรษฐกิจในประเทศเป็นจำนวนมหาศาล

ในประเทศไทย มักเกิดอาชญากรรมทางเทคโนโลยีหลายรูปแบบและจากตัวอย่างเหตุการณ์ที่ผ่านมาพบว่าสามารถเกิดขึ้นได้ทั้งกับประชาชนหรือแม้องค์กรของภาครัฐ เช่น การที่กระทรวงสาธารณสุขของประเทศไทยโดนแฮกข้อมูลผู้ป่วยในปี2563หรือเหตุการณ์โรงพยาบาลสระบุรีถูก

[1] พิมพ์ผกา ทรายข้าว, Cybercrime หรือ Computer Crime, [ออนไลน์], 2564, แหล่งที่มา https://www.nsm.or.th/other-service/671-online-science/knowledge-inventory/sci-vocabulary/sci-vocabulary-information-technology-museum/4267-cybercrime.html [3 มีนาคม 2565]

โจมตีด้วย Ransomware หรือที่เรียกว่า มัลแวร์เรียกค่าไถ่[2] โดยการล็อกรหัสไฟล์ข้อมูลทั้งหมดเพื่อแลกกับเงินจำนวนหนึ่งนอกจากนี้ยังมีคดีในส่วนของภาคประชาชนที่ตกเป็นเหยื่อโดยไม่รู้ตัว เช่น เหตุการณ์ประชาชนถูกตัดเงินผ่านบัตรเครดิตและบัตรเดบิตทั้งที่ไม่ได้ทำธุรกรรม[3] โดยที่บัญชีธนาคารเหล่านั้นได้ผูกกับแอพพลิเคชั่นต่างๆไว้ได้แก่ แอปเปิลสโตร์ กูเกิ้ลเพลย์สโตร์ เป็นต้น ทำให้มีประชาชนเดือดร้อนและสร้างความเสียหายเป็นจำนวนมาก โดยการตัดเงินดังกล่าวมีต้นทางการแฮกข้อมูลมาจากต่างประเทศและส่วนใหญ่เกิดกับร้านค้าออนไลน์ที่จดทะเบียนในต่างประเทศ

อาชญากรรมอีกรูปแบบที่มักเกิดขึ้นซ้ำๆและมีความเสียหายเป็นวงกว้างและเป็นปัญหาอยู่ในสังคมไทยมานานเนื่องจากยังไม่สามารถแก้ไขได้ตรงจุดประกอบกับในปัจจุบันได้กลับมาระบาดในสังคมไทยอีกครั้งนั่นคือ “แก๊งคอลเซ็นเตอร์”

แก๊งคอลเซ็นเตอร์ คือ ขบวนการหลอกลวงทางโทรศัพท์โดยการสร้างสถานการณ์ต่างๆให้เหยื่อเชื่อใจเพื่อที่จะหลอกล่อเอาประโยชน์จากเหยื่อ โดยในปีพ.ศ. 2565 จากสถานการณ์ระบาดของโควิด19 แก๊งคอลเซ็นเตอร์ได้กลับมาระบาดในสังคมไทยเป็นวงกว้างและสร้างความเสียหายนับไม่ถ้วนประกอบกับวิธีการหลอกลวงเหยื่อรูปแบบใหม่และซับซ้อนมากยิ่งขึ้นทำให้ประชาชนทั่วไปตกเป็นเหยื่อได้ง่าย โดยรูปแบบการหลอกลวงของแก๊งคอลเซ็นเตอร์ที่เป็นที่นิยมมากที่สุดในปัจจุบันคือปลอมตัวเป็นหน่วยงานหรือบุคคลที่น่าเชื่อถือโดยใช้วิธีการที่เรียกว่า ฟิชชิ่ง[4] ในรูปแบบของ Vishing[5] ที่ย่อมาจากคำว่า “Voice” และ “Phishing” คือการหลอกลวงผ่านทางโทรศัพท์ เช่น การปลอมตัวเป็นพนักงานของไปรษณีย์ไทย บริษัทขนส่งเอกชน ศาล สถานีตำรวจ เป็นต้น โดยมีวิธีการหลอกลวงที่ประชาชนส่วนใหญ่โดนหลอกลวง คือ โทรศัพท์ไปหาเหยื่อและแอบอ้างเป็นหน่วยงานต่างๆโดยมีวิธีการพูดโน้มน้าวใจในเรื่องต่างๆให้เหยื่อคล้อย

---

[2] ไทยรัฐออนไลน์, รพ.สระบุรีโดนมัลแวร์เรียกค่าไถ่ ระบบคอมฯ พัง ต้องซักประวัติใหม่ทำล่าช้า, [ออนไลน์], 2563, แหล่งที่มา https://www.thairath.co.th/news/local/central/1926639 [22 [10 มีนาคม 2565]

[3] BBC News, บัตรเครดิต-เดบิต: แบงก์ชาติ- ส.ธนาคารไทย พบเหตุถูกตัดเงินผิดปกติ เกิดจากธุรกรรมกับร้านค้าออนไลน์, [ออนไลน์], 2564, แหล่งที่มา _ https://www.bbc.com/thai/thailand-58950301 [10 มีนาคม 2565]

[4] The Chapt, Phishing คืออะไร? รู้ทันการโจรกรรมบนโลกไซเบอร์ ปี 2022, [ออนไลน์], 2565, แหล่งที่มา https://thechapt.com/phishing/ [10 มีนาคม 2565]

[5] บรรณศักดิ์ ยุวมิตร, Phishing คืออะไร ป้องกันอย่างไร, [ออนไลน์], 2563, แหล่งที่มา https://www.cyfence.com/article/what-is-phishing/ [10 มีนาคม 2565]

ตามและหลงเชื่อ ยกตัวอย่างเช่น หลอกเหยื่อว่ามีคดีความติดตัวต้องไปยื่นเรื่องต่อศาลคดีความจึงจะจบและหลอกให้เหยื่อโอนเงินเป็นค่าปฏิบัติการการดำเนินคดี หรือ อ้างว่ามีพัสดุผิดกฎหมายตกค้าง เป็นต้น นอกจากนี้แก๊งคอลเซ็นเตอร์ยังสามารถใช้การหลอกลวงแบบฟิชชิ่งในรูปแบบอื่น คือ การใช้ Short Message Service หรือที่เรียกกันว่า “SMS” เป็นการส่งข้อความหลอกลวงผ่านทางโทรศัพท์ เช่น หลอกลวงโดยการส่งผ่านข้อความมือถือโดยในข้อความนั้นมีเนื้อหาที่มุ่งเน้นเกี่ยวกับการเงินหรือการลงทุนที่ดึงดูดให้เหยื่อสนใจโดยที่ทิ้งเบอร์โทรศัพท์เอาไว้ให้เหยื่อติดต่อสอบถามและหลอกให้เหยื่อโอนเงินจนหมดบัญชี หรืออ้างว่ามาจากสถาบันการเงินโดยที่หลอกลวงเหยื่อว่าบัญชีเงินฝากมีปัญหาให้โทรติดต่อด่วน เป็นต้น และคดีล่าสุดที่เป็นข่าวใหญ่เมื่อเดือนพฤศจิกายน 2565[6] โดยเป็นแผนกวาดล้างกลุ่มนายทุนจีนผิดกฎหมายและได้สืบสาวไปยังต้นตอพบว่าผู้ต้องหาชาวจีนรายดังกล่าวไม่สามารถพูดภาษาไทยได้แต่กลับมีบัตรประชาชนไทย ซึ่งจากการสอบสวนพบว่าเป็นบัตรประชาชนปลอม นอกจากนี้ได้ตรวจสอบพบบันทึกการเข้าออกประเทศจากพาสปอร์ตของผู้ต้องหาที่ได้ทำการยึดไว้พบว่ามีการเดินทางเข้าออก ไทย-กัมพูชา 25 ครั้ง และ เข้า-ออก มาเลเซียอีก 12 ครั้งและยังพบความเชื่อมโยงกับกลุ่ม "คิงโรมัน" ซึ่งเป็นขบวนการ "แก๊งคอลเซ็นเตอร์" ที่ใช้ประเทศไทยเป็นที่พักอาศัยอีกด้วย

ด้วยเหตุที่ดังกล่าวที่เกิดขึ้น ผู้วิจัยจึงเล็งเห็นถึงความสำคัญของปัญหาเนื่องจากการระบาดของแก๊งคอลเซ็นเตอร์ได้สร้างความเสียหายต่อระบบเศรษฐกิจของประเทศไทยและสร้างความรำคาญให้กับประชาชนผู้บริสุทธิ์ซึ่งไม่มีท่าทีว่าจะสามารถกำจัดได้ นอกจากนี้การแอบอ้างเป็นหน่วยงานต่างๆของมิจฉาชีพทำให้ความน่าเชื่อถือขององค์กรธุรกิจลดน้อยลงและยังสร้างความหวาดระแวงให้กับประชาชนว่าหน่วยงานที่โทรเข้ามาเป็นหน่วยงานจริงหรือไม่ ประกอบกับประเทศไทยไม่ได้มีแนวทางในการป้องกันปัญหาอย่างชัดเจน ดังนั้นผู้เขียนเห็นว่าจึงควรศึกษารูปแบบและลักษณะการกระทำความผิดของแก๊งคอลเซ็นเตอร์ ประกอบกับศึกษาแนวทางในการป้องกันเพื่อที่จะนำมาประยุกต์ใช้กับประเทศไทยและเพื่อบรรเทาความเดือดร้อนและความเสียหายที่เกิดกับประชาชนโดยการผ่อนหนักเป็นเบาในเรื่องอาชญากรรมทางเทคโนโลยีโดยเปรียบเทียบว่าประเทศไทยควรมีการพัฒนากระบวนการใดให้มีประสิทธิภาพในการรับมือกับเหตุการณ์ที่อาจจะเกิดขึ้น นอกจากนี้ยังเพื่อบรรเทาความเสียหายในภาคเศรษฐกิจและ ภาค

[6] ข่าวอาชญากรรม, ขยายผลจับ "นายทุนจีน" ปลอมบัตร ปชช.ไทย ล่าสุดพบ เอี่ยว "แก๊งคอลเซ็นเตอร์", [ออนไลน์], 2565, แหล่งที่มา https://www.komchadluek.net/news/crime/535195 [30 พฤศจิกายน 2565]

ประชาชนไม่ให้ถูกหลอกหรือเป็นเหยื่อในอาชาญากรรมที่เกิดขึ้นในรูปแบบเดิมรวมทั้งหามาตรการที่เหมาะสมกับประเทศไทยมากที่สุด

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาปัจจัยและผลกระทบที่เกิดขึ้นจากแก๊งคอลเซ็นเตอร์
2. เพื่อศึกษารูปแบบการหลอกลวงของแก๊งคอลเซ็นเตอร์ที่กระทบต่อความน่าเชื่อถือของหน่วยงานภาครัฐและเอกชนในประเทศไทย
3. เพื่อเปรียบเทียบแนวทางการป้องกันและมาตรการทางกฎหมายที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ของประเทศไทยและต่างประเทศ
4. เพื่อให้หน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องกับเรื่องแก๊งคอลเซ็นเตอร์เข้ามามีส่วนร่วมในการร่วมมือกันหาแนวทางป้องกันแก๊งคอลเซ็นเตอร์อย่างมีประสิทธิภาพ

1.3 สมมติฐานของการศึกษา

แม้ประเทศไทยจะมีการปราบปรามอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์โดยการกำหนดความผิดทางอาญาและการใช้นโยบายทางอาญาของรัฐ แต่อย่างไรก็ตามการดำเนินการดังกล่าวยังไม่รวมถึงมาตรการในการป้องกันอาชญากรรมของภาคส่วนอุตสาหกรรมโทรคมนาคมดังนั้นจึงควรมีการแก้ไขเพิ่มเติมกฎหมายโดยการนำแนวทางและมาตรการป้องกันในส่วนของอุตสาหกรรมโทรคมนาคมของประเทศออสเตรเลียและประเทศสหราชอาณาจักรมาปรับใช้เพื่อจะก่อให้เกิดผลในการป้องกันอาชญากรรมประเภทดังกล่าวได้มากขึ้น

1.4 ขอบเขตการศึกษา

ศึกษาปัจจัย รูปแบบการหลอกลวง และผลกระทบที่เกิดจากแก๊งคอลเซ็นเตอร์โดยจำกัดเฉพาะกรณีในดินแดนของรัฐ ที่ส่งผลต่อความน่าเชื่อถือของหน่วยงานภาครัฐและภาคเอกชน รวมไปถึงการใช้อำนาจทางกฎหมายของภาครัฐในการที่ให้ภาคเอกชนเข้ามีบทบาทในการร่วมมือกันเสนอและศึกษาหาแนวทางการป้องกัน โดยเปรียบเทียบระหว่างแนวทางการป้องกันของประเทศไทยและต่างประเทศและสามารถวิเคราะห์ถึงความเหมาะสมและความครอบคลุมถึงแนวทางที่เหมาะสมอันจะสามารถนำมาปรับปรุงและบังคับใช้กฎหมายให้มีความเหมาะสมและมีประสิทธิภาพ

1.5 วิธีการดำเนินศึกษา

งานวิจัยฉบับนี้ทำการศึกษาและค้นคว้ารวบรวมข้อมูลแบบเชิงคุณภาพ โดยใช้วิธีการศึกษาค้นคว้าจากเอกสาร (Documentary Research) ซึ่งได้ทำการรวบรวมตลอดจนถึงวิเคราะห์ข้อมูลเอกสารที่เกี่ยวข้องในรูปของสื่อประเภทหนังสือ บทความ บทบัญญัติของกฎหมาย และสื่อประเภทข้อมูลอิเล็กทรอนิกส์โดยใช้อินเตอร์เน็ตเป็นเครื่องช่วยค้นคว้าและได้นำข้อมูลเหล่านั้นมาศึกษาเรียบเรียงและวิเคราะห์เพื่อหาข้อสรุปของการวิจัยให้มีประสิทธิภาพมากที่สุด

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ทราบถึงปัจจัยและผลกระทบที่เกิดขึ้นจากแก๊งคอลเซ็นเตอร์
2. ได้ทราบถึงรูปแบบการหลอกลวงของแก๊งคอลเซ็นเตอร์ที่กระทบต่อความน่าเชื่อถือของหน่วยงานภาครัฐและเอกชนในประเทศไทย
3. ได้วิเคราะห์และเปรียบเทียบแนวทางการป้องกันและมาตรการทางกฎหมายที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ของประเทศไทยและต่างประเทศ
4. สามารถเสนอให้หน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องกับเรื่องแก๊งคอลเซ็นเตอร์เข้ามามีส่วนร่วมในการร่วมมือกันหาแนวทางการป้องกันแก๊งคอลเซ็นเตอร์อย่างมีประสิทธิภาพ

บทที่ 2
แนวคิดและทฤษฎีที่เกี่ยวข้อง

เมื่อขึ้นชื่อว่าอาชญากรรมแล้ว ไม่ว่าจะเป็นอาชญากรรมประเภทไหนก็ถือว่าเป็นการกระทำความผิดกฎหมายที่สามารถส่งผลกระทบต่อชีวิต เสรีภาพและทรัพย์สิน อย่างไรก็ตามอาชญากรรมสามารถแบ่งได้หลายประเภทขึ้นอยู่กับเจตนาที่อาชญากรเหล่านั้นเลือกทำ ได้แก่ อาชญากรรมยาเสพติด อาชญากรรมทางเพศ เป็นต้น แต่มีอาชญากรรมประเภทหนึ่งที่ไม่เพียงแต่อาศัยการเปลี่ยนแปลงและพัฒนาที่รวดเร็วของเทคโนโลยีในโลกปัจจุบันมาเป็นเครื่องมือกระทำความผิดและสร้างความเสียหายให้กับระบบเศรษฐกิจเป็นจำนวนมหาศาล แต่ยังทำให้เกิดอาชญากรรมข้ามชาติได้อีกด้วย นั่นคือ อาชญากรรมทางเทคโนโลยี หรือ อาชญากรรมทางคอมพิวเตอร์

อาชญากรรมทางเทคโนโลยีในปัจจุบัน หากไม่นับความผิดฐานหมิ่นประมาทแล้ว จากสถิติในปี 2564 ล่าสุดที่กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีออกมาเปิดเผย[7] พบว่า อาชญากรรมที่เกิดขึ้นบ่อยๆมีด้วยกัน 2 รูปแบบหลักๆ คือการแฮกข้อมูลและการฉ้อโกงออนไลน์ซึ่งพบว่าอาชญากรรมใน 2 รูปแบบนี้ คนร้ายมักอาศัยโอกาสจากเทคโนโลยีใหม่ๆมาเอื้อประโยชน์ในการกระทำความผิด หรือปกปิดตัวตนไม่ให้เจ้าหน้าที่ตำรวจสามารถสืบสวนหาตัวคนร้ายได้โดยง่าย โดยใช้ช่องทางต่างๆ เช่น การปกปิดตัวตนโดยนำภาพหรือชื่อบุคคลอื่นมาสร้างบัญชีในสื่อสังคมออนไลน์ปลอม หรือการปกปิดที่อยู่ไอพี (ip address) หรือการซื้อบัญชีธนาคารจากผู้ที่รับจ้างเปิดบัญชีธนาคารที่เรียกว่าบัญชีม้า เป็นต้น ซึ่งเป็นการสร้างความยุ่งยากให้กับเจ้าหน้าที่ในการสืบสวนหาตัวผู้กระทำความผิดมาดำเนินคดีตามกฎหมาย เนื่องจากถือเป็นภัยคุกคามและมีความร้ายแรงระดับประเทศและสามารถสังเกตได้ว่ากระบวนการการก่ออาชญากรรมดังกล่าวมักทำในรูปแบบของเครือข่ายและมีการแฝงตัวมากับธุรกิจหรือแฝงตัวเป็นบุคคลอื่นทำให้มีคนตกเป็นเหยื่ออย่างมากมาย ในปี 2565 อาชญากรรมทางเทคโนโลยีที่ระบาดมากที่สุดในสังคมไทยและทำให้ภาครัฐต้องออกมาให้ความรู้และเตือนประชาชนตั้งแต่ต้นปีที่ผ่านมานั่นคือ แก๊งคอลเซ็นเตอร์ ซึ่งส่วนใหญ่จะใช้วิธีการในการกระทำความผิดแบบ ฟิชชิ่ง (Phishing)

---

[7] ข่าวช่อง 8, ด่าทอ ให้ร้าย ผ่านโซเชียล อันดับ 1 อาชญากรรมไซเบอร์ปี 64, [ออนไลน์] , 2565, แหล่งที่มา https://www.thaich8.com/news_detail/104021 [11 พฤษภาคม 2565]

ฟิชชิ่ง (Phishing) หมายถึง การโจรกรรมทางออนไลน์ที่อาชญากรมักกระทำการปลอมแปลงหน้าเว็บไซต์ เอกสาร ข้อมูลสำคัญ อีเมล หรือแม้กระทั่งเสียงให้ดูเหมือนเป็นบุคคลหรือองค์กรที่น่าเชื่อถือ โดยแก๊งคอลเซ็นเตอร์ในปัจจุบันส่วนใหญ่ได้ใช้วิธีฟิชชิ่งเพิ่มเข้ามาในการหลอกลวงเหยื่อเพิ่มเติมจากที่ปกติใช้ ระบบ Voice Over Internet Protocol (VOIP)[8] ที่เป็นการนำรูปแบบโทรศัพท์ด้วยเสียงผ่านเครือข่ายอินเทอร์เน็ตซึ่งสามารถเลือกเบอร์ได้ว่าจะให้เบอร์อะไรเป็นเบอร์ที่แสดงกับทางปลายทางที่ติดต่อเพื่อให้ผู้รับเกิดความสับสนและเข้าใจผิด เมื่อเข้าใจผิดจึงเกิดการหลงเชื่อและนำไปสู่การฉ้อโกงได้

2.1 ความหมายและแนวคิดของอาชญากรรมทางเทคโนโลยี (Cybercrime)

ในปัจจุบันยังไม่มีนักวิชาการที่ได้ให้คำนิยามของคำว่า “อาชญากรรมทางเทคโนโลยี” หรือ “อาชญากรรมคอมพิวเตอร์” ไว้อย่างชัดเจน แต่จากการศึกษาผู้วิจัยสามารถสรุปจากงานเขียนต่างๆ ที่ได้สืบค้นเพิ่มเติมว่าอาชญากรรมทางเทคโนโลยี หมายถึง การกระทำความผิดต่อกฎหมายผ่านช่องทางเทคโนโลยีโดยอาศัยคอมพิวเตอร์หรืออุปกรณ์ต่างๆในการเชื่อมโยงเครือข่ายทำให้เหยื่อได้รับความเสียหายและส่งผลต่อระบบเศรษฐกิจของประเทศเป็นวงกว้างซึ่งการกระทำความผิดดังกล่าวมีรูปแบบที่แตกต่างกันออกไป

อาจารย์ปริญญา หอมเอนก ได้กล่าวว่า[9] “อาชญากรรมทางไซเบอร์ ไม่มีพรมแดน กลายเป็นอาชญากรรมข้ามชาติ และพัฒนาไปเป็นองค์กรอาชญากรรมข้ามชาติ คนร้ายใช้วิทยาการที่ก้าวหน้า การจัดการกับปัญหานี้จึงไม่ใช่เรื่องง่ายและยังต้องไปอาศัยความร่วมมือกับผู้เชี่ยวชาญด้านอื่นๆตามประเภทของอาชญากรรมอีกด้วย”

พ.ต.ท.พัฒนะ ศุกรสุต ผู้เชี่ยวชาญเฉพาะด้านคดีพิเศษ กรมสอบสวนคดีพิเศษ หรือ DSI ได้ให้คำนิยามใหม่ว่า[10] “ Smart โจร เป็นอาชญากรที่ฉลาดมากขึ้น สามารถใช้เทคโนโลยีที่ล้ำหน้ากว่า

---

[8] ผู้จัดการออนไลน์, กสทช.กำชับค่ายมือถือตัดไฟแต่ต้นลม บล็อกเบอร์แก๊งคอลเซ็นเตอร์ไม่ให้โทร.เข้าไทย, [ออนไลน์], 2565, แหล่งที่มา https://mgronline.com/cyberbiz/detail/9650000005777 [10 พฤษภาคม 2565]

[9] สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (องค์การมหาชน), ผู้เชี่ยวชาญ มั่นใจ ชีวิตวิถีใหม่ อยู่ภายใต้ภัยคุกคามทางไซเบอร์ แนะทุกหน่วยงานต้องออกแบบระบบที่ทำงานได้แม้ถูกโจมตี, [ออนไลน์], 2563, แหล่งที่มา : https://www.tijthailand.org/th/highlight/detail/cybercrime-covid-19 [15 พฤษภาคม 2565]

[10] เรื่องเดียวกัน

เจ้าหน้าที่ไปหลายก้าวจึงไม่ควรประเมินความสามารถของคนกลุ่มนี้ต่ำเกินไปและยังเป็นอาชญากรรมที่ไม่มีเชื้อชาติ ไม่มีขอบเขตของประเทศจึงยากลำบากต่อการติดตาม เมื่อการกระทำผิดกฎหมายในประเทศหนึ่งเกิดขึ้นจากอีกประเทศหนึ่ง ทำให้การบังคับใช้กฎหมายมีความซับซ้อนมากขึ้นในแต่ละครั้งต้องไปดูว่ามีสนธิสัญญาระหว่างกันหรือไม่และมีรายละเอียดในการส่งผู้ร้ายข้ามแดนเข้ามาเกี่ยวข้อง”

ศาสตราจารย์พิเศษ ดร.กิตติพงษ์ กิตยารักษ์ ได้กล่าวสรุปไว้ว่า[11] “อาชญากรรมไซเบอร์เป็นปัญหาใหญ่ต่อการพัฒนาไปสู่ความเป็น “พลเมืองดิจิทัล” จึงต้องการความร่วมมือจากทุกฝ่ายที่ต้องรับมือให้ได้ในทุกมิติ ตั้งแต่การรับมือกับความหลากหลายของรูปแบบอาชญากรรมที่ซับซ้อนมากขึ้น โอกาสในการก่ออาชญากรรมผ่านเครือข่ายอินเทอร์เน็ตทำได้ง่าย สะดวก แนบเนียน และป้องกันยากขึ้น ส่วนประเด็นเรื่องกฎหมายจะต้องพิจารณาให้มีความหลากหลายและทันสมัยมากขึ้นและต้องคำนึงถึงประสิทธิภาพในการบังคับใช้กฎหมายด้วยเพราะฝ่ายอาชญากรสามารถก่อเหตุได้โดยไม่มีพรมแดน ไม่ต้องมีข้อตกลง ไม่ต้องมีสนธิสัญญา ในขณะที่ฝ่ายเจ้าหน้าที่ซึ่งรวบรวมพยานหลักฐานกลับมีข้อจำกัดทั้งเรื่องพรมแดน ความร่วมมือระหว่างประเทศ เช่น การส่งพยานหลักฐาน ต้องมีกระบวนการในการร่วมมือที่ซับซ้อน”

2.2 รูปแบบอาชญากรรมทางเทคโนโลยีของแก๊งคอลเซ็นเตอร์

ปัจจุบันวิธีการหลอกลวงของแก๊งคอลเซ็นเตอร์มีหลากหลายรูปแบบและได้พัฒนาตามเทคโนโลยีที่เปลี่ยนแปลงไป โดยส่วนมากจะนิยมใช้การฟิชชิ่งเข้ามาเป็นเครื่องมือช่วยหลอกล่อเหยื่อ ซึ่งการหลอกลวงแบบฟิชชิ่งยังมีรูปแบบที่แตกต่างกันออกไปโดยสามารถแบ่งชื่อเรียกออกไปตามรูปแบบการโจมตีได้อีก 8 รูปแบบ ดังต่อไปนี้

2.2.1 Phishing emails[12] คือ การส่งอีเมลหลอกลวงต่าง ๆ โดยอาจจะใช้ความสัมพันธ์ของบุคคล สถาบันการเงินหรือตำแหน่ง เช่น CEO เจ้าของบริษัทหรือเจ้าหน้าที่ธนาคาร เพื่อให้ผู้ที่ได้รับอีเมลไม่สงสัยและเพิ่มความน่าเชื่อถือ ซึ่งเนื้อหาในอีเมลนั้นเป็นการหลอกล่อผู้ใช้งานให้กรอก

---

[11] สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (องค์การมหาชน), ผู้เชี่ยวชาญ มั่นใจ ชีวิตวิถีใหม่ อยู่ภายใต้ภัยคุกคามทางไซเบอร์ แนะทุกหน่วยงานต้องออกแบบระบบที่ทำงานได้แม้ถูกโจมตี, [ออนไลน์], 2563, แหล่งที่มา : https://www.tijthailand.org/th/highlight/detail/cybercrime-covid-19 [15 พฤษภาคม 2565]

[12] บรรณศักดิ์ ยุวมิตร, Phishing คืออะไร, [ออนไลน์], 2564, แหล่งที่มา https://www.cyfence.com/article/what-is-phishing/ [1 มิถุนายน 2565]

ข้อมูลส่วนตัวต่าง ๆ เช่น รหัสผ่าน หรือส่งโปรแกรมให้ติดตั้งลงเครื่องคอมพิวเตอร์ตามที่แฮกเกอร์ต้องการ

2.2.2 Spear Phishing[13] คือ เป็นการโจมตีแบบมีกลุ่มเป้าหมายเฉพาะเจาะจง โดยมิจฉาชีพต้องทำการค้นคว้าข้อมูลส่วนตัวของกลุ่มที่ต้องการโจมตีเพื่อสร้างความน่าเชื่อถือในอีเมลนั้นมากยิ่งขึ้น ซึ่งฟิชชิ่งรูปแบบนี้มักสร้างความเสียหายให้กับองค์กรบริษัทได้มาก เนื่องจากกลุ่มมิจฉาชีพมักจะปลอมตัวเป็นพนักงานบริษัทนั้นและสร้างอีเมลปลอมเพื่อให้ดูน่าเชื่อถือหรือปลอมเป็นคนที่รู้จักและหลอกให้โอนเงินมา เช่น ปลอมเป็นเพื่อนในเฟซบุ๊กแล้วทำการทักแชทไปขอยืมเงิน เป็นต้น ตัวอย่างดังกล่าวก็ถือเป็น Spear Phishing เช่นเดียวกัน

2.2.3 Whaling Phishing[14] คือ การโจมตีที่มีกลุ่มเป้าหมายเฉพาะเจาะจงที่เป็นบุคคลสำคัญ โดยมีลักษณะคล้ายกับ Spear Phishing แต่มีรูปแบบที่ซับซ้อนมากกว่า เป้าหมายของ Whalingจะเล็งไปที่บุคคลเพียงคนเดียวและมักจะเป็นบุคคลที่มีตำแหน่งงานอยู่ในระดับสูง เช่น ผู้จัดการ (Manager) หรือ ซีอีโอ (Chief Executive Officer - CEO) เป็นต้น

2.2.4 Vishing Phishing หรือที่รู้จักกันในนาม Voice Phishing[15] คือ การหลอกล่อล้วงข้อมูลผ่านทางเสียง โดยแฮกเกอร์จะใช้วิธีการปลอมตัวแล้วโทรศัพท์เข้ามาเพื่อขอข้อมูลส่วนบุคคลไป เช่น โทรมาแอบอ้างเป็นเจ้าหน้าที่ธนาคารแล้วขอเลขบัตรเครดิตหรือเลขบัตรประชาชน หรือ โทรมาหาเหยื่อแล้วแอบอ้างว่าเป็นพนักงานขององค์กรที่น่าเชื่อถือและทำการหลอกล่อให้เหยื่อโอนเงิน เป็นต้น ซึ่งจะเห็นได้ว่าวิธี Voice Phishing เป็นวิธีที่แก๊งคอลเซ็นเตอร์นิยมใช้กันมากที่สุด โดยจะทำการกล่าวต่อไปอย่างละเอียดในหัวข้อถัดไป

---

[13] วสันต์ ลิ่วลมไพศาล, Spear Phishing ภัยธุรกิจสร้างความเสียหายได้มากกว่าที่คิด, [ออนไลน์], 2564, แหล่งที่มา https://www.mfec.co.th/th/cto-brief/spear-phishing-%E0%B8%A0%E0%B8%B1%E0%B8%A2%E0%B8%98%E0%B8%B8%E0%B8%A3%E0%B8%81%E0%B8%B4%E0%B8%88%E0%B8%AA%E0%B8%A3%E0%B9%89%E0%B8%B2%E0%B8%87%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B9%80%E0%B8%AA/ [1 มิถุนายน 2565]

[14] ศูนย์ไซเบอร์กองทัพอากาศ, "Phishing" ภัยออนไลน์ที่ไม่ควรมองข้าม !!!, [ออนไลน์], 2565, แหล่งที่มา https://cyber.rtaf.mi.th/publish/page.aspx?id=912 [3 มิถุนายน 2565]

[15] เรื่องเดียวกัน

2.2.5 Smishing Phishing[16] คือ การหลอกลวงผ่านทางข้อความสั้น SMS โดยผู้ส่งจะพยายามโน้มน้าวให้ผู้อ่านคลิกเปิดลิงก์ที่แนบมากับข้อความ SMS เพื่อเข้าสู่หน้าเว็บไซต์ปลอมที่ถูกสร้างเตรียมเอาไว้ ซึ่งในเว็บดังกล่าวก็จะมีช่องให้กรอกข้อมูลส่วนตัวที่สำคัญ เช่น เลขบัตรประชาชน เลขบัญชีธนาคาร เป็นต้น ซึ่งวิธีนี้ก็เป็นอีกหนึ่งวิธีที่แก๊งคอลเซ็นเตอร์เลือกใช้ควบคู่ไปกับวิธี Voice Phishing

2.2.6 Angler Phishing[17] คือ การหลอกลวงโดยการสังเกตพฤติกรรมทางโซเชียล โดยแฮกเกอร์จะเฝ้าจับตาพฤติกรรมการใช้งาน social media ของเหยื่อ แล้วสวมรอยเป็นเจ้าหน้าที่มาหลอกลวงเหยื่อให้หลงเชื่อ เช่น ถ้าเรามีการทวิตข้อความบ่นค่ายมือถือ มิจฉาชีพก็จะปลอมตัวมาเป็นตัวแทนของค่ายมือถือนั้นและทำการหลอกลวงเหยื่อ เป็นต้น

2.2.7 CEO Fraud Phishing[18] คือ การหลอกลวงโดยใช้บุคคลสำคัญเป็นตัวล่อซึ่งเทคนิคนี้มีความคล้ายคลึงกับเทคนิค Whaling Phishing โดยเป้าหมายของแฮกเกอร์ คือ ซีอีโอ หรือคนที่อยู่ในระดับผู้บริหาร (Management Level) ที่เป็นบุคคลสำคัญขององค์กรแต่วิธีการโจมตีนั้นจะรุนแรงกว่ามาก หลักการสำคัญคือจะใช้บุคคลสำคัญเป็นตัวล่อให้ผู้อื่นหลงเชื่อเพื่อกระทำการอย่างใดอย่างหนึ่ง เช่น ปลอมตัวเป็น CEO จากนั้นก็ส่งอีเมลออกไปในนามของ CEO ให้กับลูกน้องหรือผู้ที่เกี่ยวข้องอื่นๆ เพื่อขอให้ผู้รับอีเมลทำการโอนเงินหรือส่งข้อมูลสำคัญที่เป็นความลับของบริษัทกลับมาให้

2.2.8 Search Engine Phishing[19] คือ การหลอกลวงที่สร้างความน่าเชื่อถือจากเครื่องมือค้นหาโดยที่จะวางเหยื่อล่อเป้าหมายผ่านผลลัพธ์การค้นหาของเครื่องมือค้นหา (Search Engine) หรือบริการค้นหาเว็บไซต์ ได้แก่ Google เป็นต้น ซึ่งแฮกเกอร์จะสร้างเว็บไซต์ที่ยื่นข้อเสนอต่างๆ จากนั้นก็อาศัยเทคนิคการปรับแต่งเครื่องมือค้นหาหรือที่เรียกว่า "SEO (Search Engine Optimization)" ในการทำให้เว็บปลอมที่สร้างขึ้นมาติดอยู่ในผลลัพธ์การค้นหาที่สูงเพื่อทำให้เหยื่อหลงเชื่อก่อนจะเข้าไปกรอกข้อมูลสำคัญๆ

---

[16] ศูนย์ไซเบอร์กองทัพอากาศ, "Phishing" ภัยออนไลน์ที่ไม่ควรมองข้าม !!!, [ออนไลน์], 2565, แหล่งที่มา https://cyber.rtaf.mi.th/publish/page.aspx?id=912 [3 มิถุนายน 2565]

[17] เรื่องเดียวกัน

[18] เรื่องเดียวกัน

[19] เรื่องเดียวกัน

จากประเภทของอาชญากรรมทางเทคโนโลยีข้างต้นที่กล่าวมาได้สร้างภัยคุกคามที่สำคัญต่อประชาชนโดยข้อมูลของผู้ใช้นับล้านถูกขโมยภายในไม่กี่ปีที่ผ่านมา นอกจากนี้ยังได้สร้างความเสียหายอย่างมากต่อระบบเศรษฐกิจของหลายประเทศ นั่นจึงเป็นสาเหตุว่าทำไมจึงควรที่จะส่งเสริมและให้ความรู้กับตัวเองและผู้อื่นเกี่ยวกับมาตรการป้องกันที่สามารถทำได้เพื่อปกป้องตัวเองในฐานะบุคคลหรือในฐานะธุรกิจ เพราะเพื่อป้องกันภัยคุกคามที่ยิ่งใหญ่ที่สุดต่อทุกอาชีพ ทุกอุตสาหกรรม และทุกบริษัทในโลก

2.3 ทฤษฎีที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ออนไลน์

อาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ในแต่ละประเทศย่อมมีการใช้รูปแบบที่แตกต่างกันออกไปขึ้นอยู่กับบริบทของประเทศนั้น แต่ส่วนใหญ่มักมีจุดประสงค์เดียวกันคือการหลอกลวงเหยื่อเพื่อนำมาสู่การฉ้อโกงเงิน

2.3.1 ความหมายและลักษณะของแก๊งคอลเซ็นเตอร์ออนไลน์

แก๊งคอลเซ็นเตอร์ออนไลน์ คือ อาชญากรรมทางเศรษฐกิจรูปแบบหนึ่งที่มีลักษณะเป็นการฉ้อโกงประชาชนโดยมีรูปแบบการหลอกลวง ปลอมแปลงโดยใช้กลไกต่างๆหลอกล่อให้เหยื่อตายใจไม่ว่าจะวิธีใดก็ตามซึ่งส่วนใหญ่มักเป็นการโทรหลอกลวงเหยื่อ ประกอบกับในปัจจุบันที่เทคโนโลยีสามารถใช้อินเทอร์เน็ตเพื่อโทรจากทั่วทุกมุมโลก ในต่างประเทศจะรู้จักกันในนาม Phone Scammer หรือ Vishing Phishing

ในประเทศไทยจากการรายงานของศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ เปิดเผยว่า[20]ประเทศไทยพบการใช้โทรศัพท์เพื่อหลอกลวงมากกว่า 6.4 ล้านครั้ง โดยเพิ่มขึ้นกว่าร้อยละ 270 จากปี 2563 และในไทยพบการส่งข้อความขนาดสั้นหรือเอสเอ็มเอส (SMS) หลอกลวงเพิ่มขึ้นถึงร้อยละ 57 และในปี 2564 ที่ผ่านมา มีผู้เสียหายเข้าแจ้งความกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กว่า 1,600 คน มูลค่าความเสียหายสูงกว่า 1,000 ล้านบาท นับแต่เดือนมกราคมถึง 15 กุมภาพันธ์ 2565

---

[20] อาริยา สุขโต วิทยากรชำนาญการพิเศษ กลุ่มงานบริการวิชาการ 2 สำนักวิชาการ, ภัยอาชญากรรมแก๊งคอลเซ็นเตอร์, [ออนไลน์], 2565, แหล่งที่มา https://library.parliament.go.th/th/radioscript/rr2565-jul7 [13 ตุลาคม 2565]

ลักษณะของแก๊งคอลเซ็นเตอร์ คือ เป็นกลุ่มมิจฉาชีพที่มีรูปแบบการทำงานเป็นขบวนการซึ่งมีการแบ่งหน้าที่ชัดเจนส่วนใหญ่มักอาศัยช่องทางความตื่นกลัวและความโลภของคนเป็นปัจจัยหลักในการหลอกลวง และกลุ่มเป้าหมายที่เป็นที่นิยมของมิจฉาชีพ ได้แก่ เหยื่อมักจะเป็นผู้สูงวัยที่ไม่เข้าใจในเทคโนโลยีมากพอ ข้าราชการเกษียณที่มีเงินเก็บสะสม หรือแม้กระทั่งข้าราชการระดับสูง เป็นต้น การทำงานของแก๊งคอลเซ็นเตอร์มีการอัปเดตข้อมูลตามเทรนในช่วงระยะเวลานั้นตลอดเวลาซึ่งจะทำให้เห็นว่าการหลอกลวงแต่ละครั้งจะเปลี่ยนเรื่องราวไปเรื่อย ๆ มีการทำ “บัญชีม้า” หรือการรับจ้างเปิดบัญชีเพื่อให้โอนเงินเป็นทอด ๆ ตามรอยได้ยาก รวมไปถึงใช้วิธีแลกเงินเป็นคริปโตเคอเรนซี่หรือบิทคอยน์

กระบวนการของแก๊งคอลเซ็นเตอร์สามารถเกิดขึ้นและเชื่อมโยงได้มากกว่า 1 ประเทศ เช่น แก๊งคอลเซ็นเตอร์ที่หลอกลวงคนไทยอาจมีศูนย์ดำเนินงานอยู่ที่ประเทศกัมพูชา เป็นต้น ส่วนใหญ่จะมีนายทุนใหญ่เป็นชาวต่างชาติและมีทีมงานจากหลากหลายประเทศซึ่งหนึ่งในนั้นก็มีคนไทยที่ไม่ว่าจะถูกหลอกให้ไปทำงานหรือจงใจก็ตาม โดยในสถิติได้มีคนไทยจำนวนมากร้องขอความช่วยเหลือผ่านทางสถานเอกอัครราชทูตไทยในกรุงพนมเปญ โดยระบุว่าถูกหลอกลวงให้ไปทำงานและถูกกักขังอยู่ในฝั่งกัมพูชา จนทำให้สถานทูตไทยในกัมพูชาถึงกับต้องออกประกาศเตือนคนไทยที่หลบหนีเข้าไปทำงานผิดกฎหมายในกัมพูชา

รูปภาพที่ 1[21] ประกาศเตือนการเดินทางไปทำงานในกัมพูชาโดยผิดกฎหมาย

รูปภาพที่ 2[22] ประกาศการเดินทางไปทำงานในกัมพูชาโดยผิดกฎหมาย

[21] สถานเอกอัครราชทูต ณ กรุงพนมเปญ, ประกาศเตือน การเดินทางไปทำงานในกัมพูชาโดยผิดกฎหมาย, [ออนไลน์], 2564, แหล่งที่มา https://phnompenh.thaiembassy.org/th/content/ประกาศเตือน-การเดินทางไปทำงานในกัมพูชาโดยผิดกฎหมาย [1 ตุลาคม 2565]

[22] เรื่องเดียวกัน

2.3.2 องค์ประกอบการกระทำความผิดของแก๊งคอลเซ็นเตอร์

จากการศึกษาการกระทำความผิดหรือปฏิบัติการแก๊งคอลเซ็นเตอร์ในปัจจุบันและจากข้อมูลเชิงลึกของ พลตำรวจตรี พันธนะ นุชนารถ[23] ผู้กำกับการสืบสวนสอบสวนสำนักงานตำรวจคนเข้าเมืองและทีมงานซึ่งปฏิบัติการอยู่ในชุด PCT ปราบปรามแก๊งคอลเซ็นเตอร์ ได้ให้ข้อมูลว่า กระบวนการแก๊งคอลเซ็นเตอร์มักจะตั้งเป็นหน่วยงานและมีการแบ่งหน้าที่ในแต่ละแผนกโดยจะแบ่งทีมงานเป็นทีมเพื่อรับผิดชอบในเรื่องต่าง ๆ ได้แก่

1. ทีมคิดสตอรี่ ทีมนี้จะเป็นการคิดสตอรี่เรื่องราวที่จะใช้ในการหลอกลวงรวมไปถึงการวางสคริปต์หรือบทพูดที่ใช้ในการหลอกล่อเหยื่อ
2. ทีมจิตวิทยา เป็นกลุ่มที่มีความรู้ความเข้าใจเรื่องจิตวิทยาและพฤติกรรมมนุษย์ ทีมนี้จะคอยกลั่นกรอง “เรื่องราว” ว่า เรื่องราวแบบไหนที่เหยื่อฟังแล้วจะหลงเชื่อได้ง่าย ซึ่งโดยส่วนใหญ่จะใช้เรื่องราวที่ทำให้เกิดความกลัวหรือเกิดความเชื่อใจคนที่หลอกลวง
3. ทีมเทรนนิ่ง เป็นทีมที่มีไว้เพื่ออบรมเครือข่ายคอลเซ็นเตอร์ในรูปแบบที่สมัครใจและหลอกให้มาทำงาน เพื่อให้คนที่เข้ามาทำงานใหม่เข้าใจถึงวิธีการหลอกลวงตลอดจนถึงเทคนิค กลยุทธ์และวิธีพูดคำพูดต่างๆ
4. ทีมหาเหยื่อ หมายถึง ทีมที่คอยหาคนที่มารับงานโดยอาจจะเป็นการหลอกคนอื่นอีกที สิ่งที่สำคัญคือต้องเป็นคนชาติเดียวกับเป้าหมายที่จะหลอกลวง
5. ทีมหา “บัญชีม้า” หรือที่เรียกว่าบัญชีทางผ่านเพื่อรับโอนเงินระหว่างเหยื่อและมิจฉาชีพ เป็นการโกงเงินบนโลกออนไลน์ที่ต้องใช้บัญชีธนาคารหรือการซื้อขายของผิดกฎหมาย โดยจะดำเนินการโอนเงินเข้าสู่เครือข่ายทันทีที่หลอกลวงสำเร็จ ทำให้ตำรวจสืบหาเส้นทางทางการเงินได้ยาก

[23] Nation Online, เปิดคู่มือ “รับมือแก๊งคอลเซ็นเตอร์” พร้อม "เปิดโปงขบวนการข้ามชาติ", [ออนไลน์], 2565, แหล่งที่มา https://www.nationtv.tv/news/378864640 [13 ตุลาคม 2565]

รูปภาพที่ 3[24] เปิดคู่มือ “รับมือแก๊งคอลเซ็นเตอร์” พร้อม "เปิดโปงขบวนการข้ามชาติ"

2.3.3 ปัจจัยที่ทำให้เกิดปัญหาการหลอกลวงโดยแก๊งคอลเซ็นเตอร์ออนไลน์

จากที่กล่าวมาข้างต้น พฤติกรรมของแก๊งคอลเซ็นเตอร์นั้นสามารถนำทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) มาวิเคราะห์ถึงปัจจัยในการเกิดแก๊งคอลเซ็นเตอร์ออนไลน์ได้เนื่องจากเป็นทฤษฎีที่อธิบายถึงสาเหตุหรือองค์ประกอบของการเกิดอาชญากรรมได้อย่างชัดเจนและเข้าใจง่าย ซึ่งสามารถนำไปใช้การแก้ไขปัญหาทั้งด้านการป้องกันและการปราบปรามอาชญากรรมได้อย่างมีประสิทธิภาพ

ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory)[25] เป็นทฤษฎีที่อธิบายถึงสาเหตุที่เกิดจากปัจจัยต่างๆหรือองค์ประกอบของการเกิดอาชญากรรมโดยประกอบด้วย 3 ด้าน ได้แก่

1. ผู้กระทำผิดหรือคนร้าย (Criminals) หมายถึง ผู้ที่มีความต้องการ (Desire) จะก่อเหตุลงมือกระทำผิด

2. เหยื่อ (Victims)หรือเป้าหมาย (Target) หมายถึง บุคคล สถานที่หรือวัตถุที่ผู้กระทำผิดหรือคนร้าย มุ่งหมายกระทำต่อหรือมีเป็นเป้าหมายที่ต้องการลงมือกระทำก่อนหน้าอยู่แล้ว

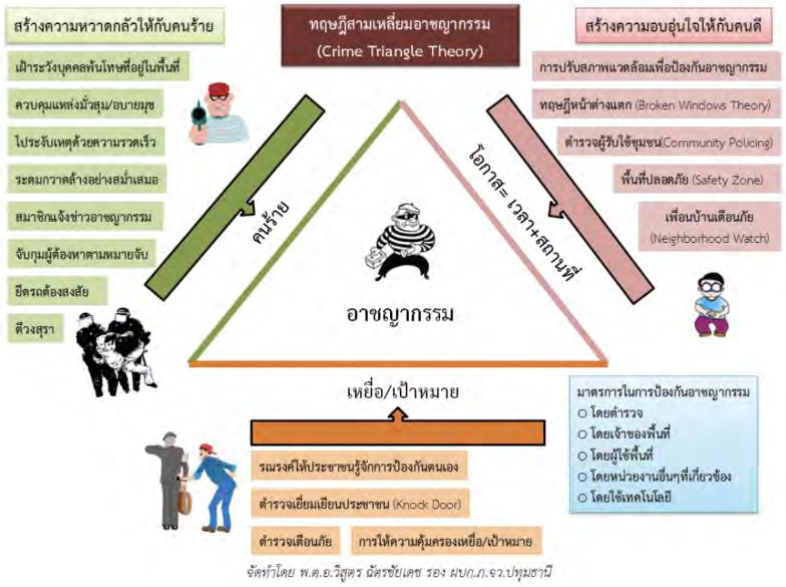
---

[24] Nation Online, เปิดคู่มือ “รับมือแก๊งคอลเซ็นเตอร์” พร้อม "เปิดโปงขบวนการข้ามชาติ", [ออนไลน์], 2565, แหล่งที่มา https://www.nationtv.tv/news/378864640 [13 ตุลาคม 2565]

[25] สุพิศาล ภักดีนฤบาล, 4 Dimensions การบริหารงานสืบสวน : กองบังคับการปราบปราม, ครั้งที่พิมพ์ 2 (นนทบุรี : กรีนแอปเปิ้ล กราฟฟิคปริ้นติ้ง จำกัด, 2556), หน้า 144

3. โอกาส (Opportunity) หมายถึง ช่วงเวลา (Time) และรวมไปถึงสถานที่ (Place) ที่เหมาะสมที่ผู้กระทำผิดหรือคนร้าย มีความสามารถที่จะลงมือกระทำผิดหรือก่ออาชญากรรม

รูปภาพที่ 4[26] Dimensions การบริหารงานสืบสวน : กองบังคับการปราบปราม



ดังนั้นจะเห็นได้ว่าเมื่อครบ 3 องค์ประกอบเมื่อไหร่ อาชญากรรมก็จะเกิดขึ้นทันที ซึ่งปัจจัยการกระทำผิดของแก๊งคอลเซ็นเตอร์ ผู้วิจัยสามารถวิเคราะห์ได้ดังนี้

ด้านที่ 1 ผู้กระทำผิดหรือคนร้าย (Criminals) การที่คนคนนึงจะยอมกระทำความผิดกฎหมายนั้นต้องมาสาเหตุและแรงจูงใจในการกระทำผิดดังกล่าว ซึ่งจากการศึกษาของผู้วิจัยพบว่าแรงจูงใจที่สำคัญที่จะทำให้เกิดกระทำความผิดนั้นส่วนใหญ่คือ เงิน

(ก) ค่าตอบแทนที่สูง

สิ่งหนึ่งที่สร้างแรงจูงใจให้คนนิยมกระทำความผิดและหลบหนีเข้าไปทำงานอย่างผิดกฎหมายคือค่าตอบแทนที่สูงจากนายทุนใหญ่ซึ่งส่วนใหญ่เป็นชาวต่างชาติ ปกติแล้วแก๊งคอลเซ็นเตอร์มักจะตั้งสำนักงานภายนอกประเทศไทยเพื่อทำให้การสืบสวนและจับกุมเป็นไปได้ยาก โดยที่ประเทศยอดฮิตที่ใช้ในการตั้งสำนักงานคือ

[26] สุพิศาล ภักดีนฤบาล, 4 Dimensions การบริหารงานสืบสวน : กองบังคับการปราบปราม, ครั้งที่พิมพ์ 2 (นนทบุรี : กรีนแอปเปิ้ล กราฟฟิคปริ้นติ้ง จำกัด, 2556), หน้า 144

ประเทศกัมพูชา เนื่องจากเป็นประเทศที่สามารถหลบหนีเข้าเมืองผ่านดินแดนธรรมชาติได้ ดังนั้นจึงทำให้ทางการไทยมีการทำ MOU[27] ร่วมกันกับประเทศกัมพูชาเพื่อทำให้กระบวนการปราบปรามเป็นไปอย่างมีประสิทธิภาพและรวดเร็วมากยิ่งขึ้น แม้ว่าการทำ MOU ดังกล่าวจะไม่ได้มีผลผูกพันทางกฎหมายแต่เนื่องจากสถานทูตไทยหรือผู้ช่วยทูตตำรวจไทยไม่สามารถเข้าไปให้ความช่วยเหลือคนไทยในกัมพูชาได้โดยตรงจึงต้องอาศัยฝ่ายกัมพูชาในการส่งตัวผู้กระทำความผิดดังกล่าวกลับมารับโทษในประเทศไทย

(ข) ปัญหาความยากจน

ปัญหาความเหลื่อมล้ำและความยากจนเป็นปัญหาของไทยมานานประกอบกับสถานการณ์โควิด-19ที่ทำให้คนมีทางเลือกในการอยู่รอดไม่มากนัก ดังนั้นทางเลือกไหนที่สามารถทำให้ดำรงชีวิตต่อไปได้จึงไม่ยากที่จะกระทำความผิด จะเห็นได้ว่ามีคนไทยจำนวนมากที่หลบหนีผ่านช่องทางธรรมชาติไปประเทศเพื่อนบ้านเพื่อไปทำงานอย่างผิดกฎหมายซึ่งหนึ่งในนั้นคือทำงานให้กับแก๊งคอลเซ็นเตอร์แล้วมาหลอกคนไทยด้วยกันเอง

จะเห็นได้ว่าค่าตอบแทนที่สูงและปัญหาความยากจนเป็นเพียงปัจจัยเบื้องต้นของผู้กระทำผิดที่ก่อให้เกิดอาชญากรรมขึ้น ดังนั้นจึงต้องพยายามลดหรือควบคุมจำนวนผู้กระทำผิด โดยมุ่งเน้นใช้ทฤษฎีบังคับใช้กฎหมาย (Law Enforce Theory) เช่น การเพิ่มบทลงโทษเพื่อตัดมูลเหตุจูงใจในการกระทำผิดเป็นสำคัญ เป็นต้น ประกอบกับการประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อที่จะแก้ไขปัญหาได้ตรงจุดและเพื่อลดปัญหาการว่างงาน

ด้านที่ 2 เหยื่อ (Victims) หรือเป้าหมาย (Target) จากการวิเคราะห์พบว่า ลักษณะของเหยื่อที่แก๊งคอลเซ็นเตอร์มักใช้เป็นเป้าหมายในการหลอกลวง ได้แก่

[27] ทัน LINE ไทยคู่ฟ้า, ครม. ไฟเขียว ร่าง MOU ไทย – กัมพูชา ผนึกกำลังปราบแก๊ง Call Center และ Hybrid Scam ข้ามแดน, [ออนไลน์], 2565,แหล่งที่มา https://www.thaigov.go.th/news/contents/details/56680 [11 ตุลาคม 2565]

1. คนยากจน คนตกงาน หรือคนที่อยากมีฐานะทางการเงินที่ดีขึ้น ซึ่งแน่นอนว่าเป้าหมายกลุ่มนี้สามารถใช้บทสนทนาเรื่องการเงินเป็นหลักโดยใช้วิธีจิตวิทยาเข้าช่วยทำการโน้มน้าวเหยื่อและกระตุ้นทำให้เกิดความโลภ
2. คนมีฐานะหรือมีเงินเก็บซึ่งส่วนใหญ่อยู่กับบ้าน เช่น แม่บ้าน จากการสำรวจและการเข้ามาแจ้งความของเหยื่อพบว่ากลุ่มคนเหล่านี้ไม่ค่อยติดตามข่าวสาร โดยแก๊งคอลเซ็นเตอร์จะใช้หมายเลขโทรศัพท์เป็นหมายเลขโทรศัพท์จริงของหน่วยงานที่แอบอ้างแต่ใช้เทคโนโลยีแปลงสัญญาณโทรศัพท์เป็นหมายเลขโทรศัพท์ที่ไม่สามารถติดต่อกลับได้เพื่อให้ยากต่อการติดตามจับกุมหรือเป็นหมายเลขที่ยาวกว่าปกติทั่วไปเพื่อให้เหยื่อหลงเชื่อว่าเป็นการติดต่อมาจากหน่วยงานจริง ๆ

ดังนั้นจากเหตุการณ์ข้างต้น ประชาชนเองต้องตระหนักรู้และอัพเดตข้อมูลข่าวสารต่างๆเพื่อป้องกันการตกเป็นเหยื่อของแก๊งคอลเซ็นเตอร์ออนไลน์ ในขณะที่ภาครัฐต้องรณรงค์และเปิดเผยข้อมูล กระบวนการหลอกลวงของแก๊งคอลเซ็นเตอร์เพื่อให้ประชาชนได้ทราบและถ้าเกิดเหตุการณ์ที่ทำให้ตกเป็นเหยื่อแล้ว ประชาชนสามารถไปร้องเรียนได้ที่หน่วยงานใดและมีวิธีอย่างไรในการจัดการกับเหตุการณ์เหล่านั้น

ด้านที่ 3 โอกาส (Opportunity)โอกาสในที่นี้หมายถึง เวลาและสถานที่ที่เหมาะสมในการก่ออาชญากรรม ในส่วนโอกาสของแก๊งคอลเซ็นเตอร์นั้นสามารถเกิดขึ้นได้ตลอดเวลาเนื่องจากเป็นการใช้เทคโนโลยีในการก่อเหตุทำให้มิจฉาชีพไม่ต้องรอว่าเมื่อไหร่จะถึงโอกาสในการหลอกลวง

2.3.4 ผลกระทบที่เกิดขึ้นจากอาชญากรรมทางเทคโนโลยีจากการหลอกลวงของแก๊งคอลเซ็นเตอร์

การระบาดของแก๊งคอลเซ็นเตอร์ก่อให้เกิดผลกระทบอย่างมีนัยสำคัญต่อด้านต่างๆในประเทศไทยไม่ว่าจะเป็นภาคธุรกิจหรือประชาชนเองที่ต้องเผชิญกับแก๊งคอลเซ็นเตอร์ ดังนั้นผู้วิจัยจึงทำการสรุปผลกระทบในด้านต่างๆมา 3 ด้าน

(ก) ผลกระทบด้านเศรษฐกิจ

แน่นอนว่าการหลอกลวงของแก๊งคอลเซ็นเตอร์แม้จะเป็นการหลอกทีละเล็กทีละน้อยหรือเหยื่อบางรายก็ถูกหลอกด้วยมูลค่ามหาศาล แต่เมื่อนำความเสียหายที่เกิดขึ้นมารวมกันแล้ว

พบว่าการหลอกลวงนั้นได้สร้างมูลค่าความเสียหายไว้อย่างมหาศาลและไม่สามารถทำการยับยั้งหรืออายัดได้ทันท่วงทีเนื่องจากส่วนใหญ่ใช้บัญชีม้าในการถอนเงินออกไป ซึ่งจากการเปิดตัวเลขของธนาคารแห่งประเทศไทย[28] พบว่า ในปี 2564 คนไทยถูกแก๊งคอลเซ็นเตอร์หลอกถึง 6.4 ล้านครั้งซึ่งเพิ่มจากปี 2563 ถึง 270% และมีมูลค่าความเสียหายรวมมากกว่า 1500 ล้านบาท

(ข) ผลกระทบด้านสังคม

เนื่องจากการหลอกลวงของแก๊งคอลเซ็นเตอร์ได้สร้างมูลค่าความเสียหายอย่างมาก ทำให้เหยื่อบางรายโดนหลอกจนหมดตัวและมักจะประสบกับความเครียด เหยื่อบางรายมีภาวะหนี้สินจนนำไปสู่ปัญหาสุขภาพจิตตามมาหรือบางรายคิดสั้นฆ่าตัวตายเพราะสูญเงินที่เก็บมาทั้งชีวิตซึ่งส่วนใหญ่มักจะเป็นเหยื่อผู้สูงอายุ แม่บ้านหรือพ่อบ้านที่มีเงินเก็บ โดยบุคคลเหล่านั้นไม่ทันต่อเทคโนโลยีและกลไกการหลอกลวงทำให้สามารถตกเป็นเหยื่อได้โดยง่าย

(ค) ผลกระทบกับหน่วยงานภาครัฐและเอกชน

เนื่องจากหน่วยงานทั้งภาครัฐและเอกชนต่างก็ถูกการแอบอ้าง ถูกใช้ชื่อเสียงและความน่าเชื่อถือของหน่วยงานตนเองในการหลอกลวง ซึ่งส่งผลกระทบต่อตัวขององค์กรเองเนื่องจากได้รับความน่าเชื่อถือจากลูกค้าหรือประชาชนน้อยลง เพราะประชาชนขาดความมั่นใจว่าสายที่โทรเข้ามาเป็นการโทรมาจากหน่วยงานจริงหรือแก๊งคอลเซ็นเตอร์ ยกตัวอย่างเช่น บริษัท โกลบอล เพาเวอร์ ซินเนอร์ยี่ จำกัด (มหาชน) หรือ GPSC[29] แจ้งว่าถูกมิจฉาชีพแอบอ้างนำชื่อ โลโก้บริษัทและการปลอมแปลงข้อมูลเอกสารของกลุ่มบริษัทไปใช้เพื่อหลอกลวงให้โอนเงินเปิดเครดิต โดยคาดหวังให้อนุมัติปล่อยสินเชื่อออนไลน์ บริษัทจึงต้องออกมาชี้แจงว่ากลุ่มบริษัทไม่มีนโยบายในการดำเนินการในลักษณะดังกล่าวแต่อย่างใดและอยู่ระหว่างดำเนินการทางกฎหมายกับบุคคลที่แอบอ้างนำชื่อและโลโก้บริษัทไปใช้ดังกล่าว หรือจะเป็นกรณีของบริษัทขนส่งต่างๆที่ถูกแอบอ้างนำชื่อเสียงไปใช้โดยทางไม่

---

[28] ทีมพัฒนาและวิเคราะห์ข้อมูล ฝ่ายนโยบายระบบการชำระเงิน, Financial Fraud : กลโกงทางการเงินใกล้ตัวกว่าที่คิด, [ออนไลน์], 2565, แหล่งที่มา https://www.bot.or.th/Thai/PaymentSystems/Publication/payment_insight/Documents/Bi-monthly_report_Vol14-2022_April.pdf [30 ตุลาคม 2565]

[29] ประชาชาติธุรกิจออนไลน์, แก๊งคอลเซ็นเตอร์โทรไม่หยุด เอกชนเสียหาย ประกาศดำเนินคดีขั้นสุด, [ออนไลน์], 2565, แหล่งที่มา https://www.prachachat.net/general/news-917443 [30 ตุลาคม 2565]

ชอบ จะเห็นได้ว่า2ตัวอย่างข้างต้น สร้างความเสียหายให้กับบริษัทเนื่องจากความน่าเชื่อถือลดน้อยลง ดังนั้นการที่จะกู้ชื่อเสียงและความน่าเชื่อถือกลับคืนมานั้นถือเป็นบททดสอบสำคัญของบริษัทแม้ว่าการกระทำดังกล่าวจะไม่ได้เกิดจากตัวบริษัทเองก็ตาม

2.4 ทฤษฎีการลงโทษทางอาญา

การลงโทษ (Punitive) คือการกระทำที่ก่อให้เกิดผลร้ายต่อตัวผู้กระทำความผิดซึ่งผลร้ายนั้น อาจจะเกิดขึ้นกับร่างกาย จิตใจ หรือทรัพย์สิน[30] เพื่อทำให้ผู้กระทำความผิดเกิดการเกรงกลัวรวมไปถึงการเป็นตัวอย่างบทเรียนให้ผู้อื่นเพื่อที่จะไม่กระทำผิดในลักษณะดังกล่าวรวมไปถึงหยุดการกระทำหรือพฤติกรรมที่ไม่สมควรและผิดกฎหมาย

ในประเทศไทยกฎหมายอธิบายว่าการลงโทษทางอาญาจะเกิดขึ้นได้ก็ต่อเมื่อมีการกระทำผิดหรือมีการกระทำที่จะเป็นความผิด โดยที่การกระทำนั้นต้องมีกฎหมายบัญญัติไว้ให้เป็นความผิดตามหลักที่ว่า "ไม่มีความผิด ไม่มีโทษ โดยไม่มีกฎหมาย" ซึ่งหมายถึงว่าความรับผิดนั้นจะต้องเป็นไปตามที่กฎหมายได้บัญญัติไว้และมีการกำหนดบทลงโทษไว้แล้ว ดังนั้นการกระทำใดที่เห็นว่ามีผลกระทบต่อสังคมจะถูกบัญญัติให้เป็นความผิดและกำหนดบทลงโทษไว้ แต่อย่างไรก็ตามการลงโทษใช่ว่าจะมีผลไปในทางบวกเสมอไปแม้ว่าประเทศไทยได้กำหนดลักษณะการลงโทษทางอาญาไว้แล้ว ได้แก่ การประหารชีวิต การจำคุก การกักขัง การปรับ และการริบทรัพย์สิน[31] แต่ก็ยังมีการเกิดอาชญากรรมขึ้นตลอดโดยจะสังเกตเห็นได้จากอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ออนไลน์ ที่แม้ว่ากฎหมายจะมีการกำหนดบทลงโทษไว้แต่ก็ไม่ได้ทำให้ผู้กระทำผิดเกิดความเกรงกลัวแต่อย่างใดซึ่งในปัจจุบันก็ยังมีลักษณะการกระทำความผิดดังกล่าวอยู่เรื่อยๆ

2.4.1 ทฤษฎีการลงโทษเพื่อการปราบปราม

แนวคิดและทฤษฎีการลงโทษทางอาญาเป็นสิ่งที่มีมาแต่เดิมและได้มีการพัฒนาขึ้นเป็นลำดับ จากเดิมที่มุ่งเน้นการลงโทษเพื่อแก้แค้นทดแทนให้เกิดความหลาบจำเพียงอย่างเดียวก็ได้มีการนำเอาแนวคิดในการมุ่งแก้ไขพฤติกรรมของผู้กระทำความผิดเข้ามาใช้ด้วย ซึ่งก่อให้เกิดวิธีการและมาตรการต่างๆที่นำมาใช้เพื่อให้เกิดความเหมาะสมกับผู้กระทำความผิด

---

[30] อัจฉรียา ชูตินันทน์, อาชญาวิทยาและทัณฑวิทยา, (กรุงเทพมหานคร : สำนักพิมพ์วิญญูชน, 2561) หน้า 206

[31] พระราชบัญญัติให้ใช้ประมวลกฎหมายอาญา พ.ศ. 2499 , มาตรา 18

แต่ละราย โดยเฉพาะอย่างยิ่งผู้กระทำความผิดที่สามารถฟื้นฟูแก้ไขพฤติกรรมให้กลับตัวเป็นคนดีคืนสู่สังคมได้และผู้ที่กระทำความผิดเล็กน้อยหรือกระทำความผิดโดยปราศจากความชั่วดังนั้นในการลงโทษผู้กระทำความผิดอาญาจึงจำเป็นต้องพิจารณาทฤษฎีการลงโทษทางอาญาประกอบด้วย ซึ่งแต่ละทฤษฎีมีรูปแบบและวัตถุประสงค์ในการลงโทษทางอาญาที่แตกต่างกันไป โดยทฤษฎีการลงโทษทางอาญาที่ปรากฏอยู่มีดังต่อไปนี้

2.4.1.1 ทฤษฎีการลงโทษเพื่อเป็นการแก้แค้นตอบแทน (Retribution)

เป็นทฤษฎีการลงโทษที่เก่าแก่ที่สุด โดยมีความคิดมาจากการแก้แค้น คือ เมื่อบุคคลใดกระทำความผิด บุคคลนั้นต้องได้รับโทษที่สาสมให้สมกับการกระทำที่ได้ทำไว้และผู้กระทำความผิดจะต้องได้รับการลงโทษเทียบเท่ากับความเจ็บปวดและความทรมานที่ผู้เสียหายได้รับ จะเห็นว่าวิธีการลงโทษตามทฤษฎีนี้ค่อนข้างใช้ความรุนแรงและทารุณจึงมักจะถูกกัดค้านในสังคมปัจจุบัน ต่อมาสำนักกฎหมายคลาสสิกได้เปลี่ยนแนวคิดในการลงโดยไม่ให้ใช้การลงโทษแบบทรมานแต่ให้จำนวนความหนักเบาของโทษต้องได้สัดส่วนกับความผิด ส่วนเหตุผลการลงโทษยังยึดหลักว่าผู้กระทำผิดสมควรได้รับโทษเพราะทุกคนมีเจตจำนงอิสระวิธีการลงโทษเพื่อแก้แค้นทดแทนมีวิธีการลงโทษหลายทาง[32]

ทฤษฎีนี้มีพื้นฐานความคิดมาจากลัทธิเจตจำนงเสรีที่เรียกว่า Free will ซึ่งมีความเชื่อเป็นพื้นฐานว่ามนุษย์มีเหตุผลมีอิสระเสรีภาพที่จะคิดรวมไปถึงมีเสรีภาพที่จะกระทำการใด ๆ ภายใต้ความคิดความเชื่อและการตัดสินใจของตนเองรวมทั้งความสามารถของบุคคลในการในการใช้เหตุผลและมนุษย์ย่อมมีเหตุผลเป็นของตนเอง ดังนั้นมนุษย์จึงต้องรับผิดชอบต่อการกระทำของตนเองที่ได้กระทำลงไปหากเป็นการกระทำที่ดีย่อมได้รับผลตอบแทนแต่หากเป็นการกระทำที่ไม่ดีหรือเป็นกระทำการที่ฝ่าฝืนต่อกฎเกณฑ์ของสังคมย่อมสมควรได้รับการตำหนิหรือได้รับการลงโทษจากสังคมอย่างหลีกเลี่ยงไม่ได้ การที่สังคมลงโทษเขาเพราะเหตุผลที่มาจากการกระทำของเขาเองไม่ใช่องค์ประกอบอื่น ดังนั้นวัตถุประสงค์ของการลงโทษตามทฤษฎีนี้คือการลงโทษเพื่อแก้แค้นทดแทน[33]

---

[32] สัญญพงศ์ ลิ่มประเสริฐ และ สุธีราภรณ์ แสงจันทร์ศรี และ อนิสา มานะทน. การลงโทษผู้กระทำผิดทางอาญา. รายงานประชุมวิชาการระดับชาติ มหาวิทยาลัยรังสิต ประจำปี 2562, หน้า 1489. ณ คณะนิติศาสตร์ มหาวิทยาลัยรังสิต ปทุมธานี ประเทศไทย, 26 เมษายน 2562

[33] ณัฐธ์วัฒน์ สุทธิโยธิน, “กฎหมายอาญาและอาชญาวิทยาชั้นสูง ทฤษฎีการลงโทษ หน่วยที่6 สาขาวิชานิติศาสตร์,” (กรุงเทพฯ : มหาวิทยาลัยสุโขทัยธรรมาธิราช) หน้า 12

2.4.2 ทฤษฎีการลงโทษเพื่อการป้องกัน

แม้ว่าบทลงโทษอาญาโดยส่วนใหญ่จะมีวัตถุประสงค์เพื่อปราบปรามการกระทำความผิดแต่ก็ไม่เพียงพอดังนั้นจึงจำเป็นต้องมีทฤษฎีที่เกี่ยวกับบทลงโทษในการใช้มาตรการป้องกันเข้ามาเกี่ยวข้องเพื่อเป็นการป้องกันคุ้มครองสังคมรวมไปถึงเป็นการวางมาตราการป้องกันไม่ให้ความผิดเกิดขึ้นซ้ำ

2.4.2.1 ทฤษฎีอรรถประโยชน์ (Utilitarian theory)

เป็นทฤษฎีที่มองว่าการลงโทษเป็นสิ่งที่ร้ายแรงแต่ถ้าก็มีความจำเป็นในการลงโทษดังกล่าวเพื่อป้องกันสังคมจากการกระทำที่ผิดและสิ่งที่เป็นอันตรายต่อการอาศัยอยู่ร่วมกันในสังคมก็ควรที่จะมีบทลงโทษ ดังนั้น ทฤษฎีนี้จะเน้นถึงวิธีการป้องกันไม่ให้เกิดการกระทำความผิดอาญาขึ้นในอนาคตอีกเนื่องจากแนวความคิดของทฤษฎีนี้มองว่าลักษณะของมนุษย์คือการแสวงหาความพอใจและหลีกเลี่ยงความเจ็บปวด ดังนั้น สังคมจึงควรมีการดำเนินการตามหลักประโยชน์สูงสุดเพื่อมนุษย์ทุกคนโดยการกำหนดโทษทางอาญาให้สอดคล้องกับสัดส่วนความร้ายแรงของความเสียหายที่เกิดขึ้นในสังคม[34] โดยวัตถุประสงค์หลักของทฤษฎีนี้คือ เพื่อข่มขู่หรือยับยั้ง (Deterrence) ดังนั้นการพิจารณาลงโทษผู้กระทำความผิด ไม่ได้พิจารณาถึงสิ่งที่ผู้กระทำความผิดได้กระทำมาแล้ว แต่เป็นการลงโทษเพื่อป้องกันไม่ให้ผู้กระทำความผิดและบุคคลอื่นในสังคมเกิดความคิดที่จะกระทำความผิดซ้ำอีกและเพื่อให้การลงโทษทางอาญามีความชอบมากยิ่งขึ้น โดยโทษดังกล่าวจะต้องสามารถข่มขู่ขับและยับยั้งผู้คนในสังคมที่คิดที่จะกระทำความผิดเพื่อไม่ให้กล้าที่จะกระทำความผิดได้ เช่น การนำโทษประหารชีวิตมาใช้ลงโทษผู้กระทำความผิดที่หนัก เป็นต้น

การลงโทษควรจะมีไว้เพื่อเป็นการป้องกัน โดยการใช้แนวคิดเรื่องการข่มขู่ยับยั้ง (Deterrence) ดังนั้น วัตถุประสงค์ของการลงโทษตามทฤษฎีข่มขู่หรือยับยั้งจึงแบ่งออกเป็น 2 ประการ[35]

---

[34] ปราโมทย์ เสริมศีลธรรม, “หลักเกณฑ์ในการกำหนดโทษทางอาญา ภายใต้โครงการสนับสนุนสารสนเทศเพื่อการทำงานของสมาชิกรัฐสภา” (กรุงเทพฯ : สถาบันพระปกเกล้า, 2564) หน้า 16

[35] ณัฐธ์วัฒน์ สุทธิโยธิน, “กฎหมายอาญาและอาชญาวิทยาชั้นสูง ทฤษฎีการลงโทษ หน่วยที่6 สาขาวิชานิติศาสตร์,” (กรุงเทพฯ : มหาวิทยาลัยสุโขทัยธรรมาธิราช) หน้า 21

1. การลงโทษเพื่อข่มขู่ยับยั้งโดยเฉพาะหรือป้องกันโดยเฉพาะ (Specific Deterrence) เป็นการลงโทษผู้กระทำผิดรายบุคคลเพื่อยับยั้งไม่ให้กระทำผิดซ้ำ โดยถือเป็นการป้องกันโดยเฉพาะ (Specific Prevention)

2. การลงโทษเพื่อข่มขู่ยับยั้งโดยทั่วไปหรือป้องกันโดยทั่วไป (General Deterrence) เป็นการลงโทษผู้กระทำผิดเพื่อเป็นตัวอย่างให้สังคมทั่วไปเห็น เพื่อที่จะได้เกรงกลัวโทษจากการกระทำผิดและไม่คิดที่จะกระทำผิดขึ้นอีก ถือเป็นการป้องกันโดยทั่วไป (General Prevention)

2.4.2.2 ทฤษฎีการลงโทษเพื่อแก้ไขฟื้นฟู (Rehabilitation)

เป็นทฤษฎีที่มีความเชื่อพื้นฐานว่า การลงโทษควรมีเพื่อการแก้ไขฟื้นฟูผู้กระทำผิดให้กลับตัวเป็นคนดีเพื่อไม่ให้ผู้กระทำผิดกลับมากระทำผิดซ้ำรวมทั้งพยายามที่จะช่วยให้ผู้กระทำผิดกลับคืนสู่สังคมได้ตามปกติดังนั้นจึงต้องมีการให้การเรียนรู้และการอบรมให้เพียงพอที่ให้ผู้กระทำผิดกลับไปใช้ชีวิตในสังคมตามปกติ เช่น การฝึกอาชีพ รวมทั้งการพยายามช่วยให้ผู้กระทำผิดไม่รู้สึกมีปมด้อยจากการที่ได้รับการลงโทษ

จะเห็นได้ว่าทฤษฎีนี้เน้นความเป็นเหตุเป็นผล เน้นการศึกษาเชิงประจักษ์ มีการนำความรู้ทางด้านสังคมศาสตร์มาใช้มาใช้ในวงการนิติศาสตร์เพื่อศึกษาถึงสาเหตุแห่งการกระทำผิด ดังนั้นการลงโทษตามทฤษฎีการลงโทษเพื่อแก้ไขฟื้นฟูและมีวัตถุประสงค์เพื่อที่จะศึกษาทำความเข้าใจสาเหตุแห่งการกระทำผิดโดยเน้นตัวบุคคลผู้กระทำผิดและสภาพแวดล้อมเพื่อที่จะหาทางแก้ไขผู้กระทำผิดมากกว่าที่จะลงโทษ การทำให้ผู้กระทำผิดกลับไปสู่สังคมของตนเองได้[36]

---

[36] ณัฐฐ์วัฒน์ สุทธิโยธิน, “กฎหมายอาญาและอาชญาวิทยาชั้นสูง ทฤษฎีการลงโทษ หน่วยที่6 สาขาวิชานิติศาสตร์,” (กรุงเทพฯ : มหาวิทยาลัยสุโขทัยธรรมาธิราช) หน้า 21

2.5 แนวความคิดเกี่ยวกับการกำกับดูแลอุตสาหกรรมโทรคมนาคมและการป้องกันอาชญากรรมแก๊งคอลเซ็นเตอร์

เนื่องจากการระบาดของแก๊งคอลเซ็นเตอร์มีความเกี่ยวเนื่องกับอุตสาหกรรมโทรคมนาคม ดังนั้นการศึกษาแนวคิดที่เกี่ยวกับการกำกับดูแลกิจการโทรคมนาคมรวมไปถึงแนวคิดในการป้องกันอาชญากรรมแก๊งคอลเซ็นเตอร์จึงมีความสำคัญและจำเป็นที่จะต้องมีการศึกษาทำความเข้าใจเกี่ยวกับการกำกับดูแลโทรคมนาคมและบทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้องเพื่อที่จะสะท้อนให้เห็นถึงภาพรวมปัญหาหรือข้อจำกัดในการกำกับดูแล

2.5.1 วัตถุประสงค์ของการกำกับดูแลอุตสาหกรรมโทรคมนาคม

การกำกับดูแลกิจการโทรคมนาคมเกิดขึ้นครั้งแรกในประเทศสหรัฐอเมริกาและประเทศแคนาดา[37] กิจการโทรคมนาคมถือเป็นบริการสาธารณะขั้นพื้นฐานที่ทุกประเทศจำเป็นต้องมีแม้ว่าในปัจจุบันกิจการดังกล่าวจะเป็นการบริหารโดยภาคเอกชน แต่ในบทบาทของภาครัฐก็ยังต้องมีการกำกับดูแลเพื่อให้ความมั่นใจกับประชาชนว่าการให้บริการของกิจการโทรคมนาคมจะเป็นประโยชน์ต่อประชาชนและเป็นธรรมมากที่สุด รวมถึงการออกใบอนุญาตประกอบกิจการอย่างโปร่งใสซึ่งในปัจจุบันภาครัฐได้ผ่อนคลายมาตรการกำกับดูแลมากขึ้นเพื่ออำนวยความสะดวกในการใช้งานให้กับประชาชนให้สอดคล้องกับความต้องการที่จะให้ประชาชนเข้าถึงบริการโทรคมนาคมได้อย่างครอบคลุม แต่การผ่อนคลายดังกล่าวได้เกิดช่องว่าในการแทรกซึมของขบวนการอาชญากรรมซึ่งหนึ่งในนั้นคือแก๊งคอลเซ็นเตอร์ได้

กิจการโทรคมนาคมของประเทศไทยรวมถึงต่างประเทศมีการเปลี่ยนแปลงอย่างรวดเร็วเนื่องจากความก้าวหน้าของเทคโนโลยี ทำให้ต้องเปิดตลาดและส่งเสริมการแข่งขันให้เอกชนเข้ามาเป็นผู้ประกอบการ โดยภาครัฐมีหน้าที่ในการกำกับดูแลและเหตุผลสำคัญว่าทำไมจะต้องมีการกำกับดูแลกิจการโทรคมนาคม สาเหตุก็คือการเปิดตลาดที่เสรีมากขึ้น ซึ่งภาครัฐเองก็มีหน้าที่ในการควบคุมการประกอบกิจการของภาคเอกชนเหล่านั้น นอกจากการควบคุมแล้วยังก่อให้เกิดหน่วยงานอิสระจากผู้ให้บริการ เช่น FCC ของประเทศ

---

[37] พิมพ์พชา ปิยะเกศินและพัชรี พิชญุษากรและอโนชา หงส์บุรินทร์และทิพย์สุรางค์ วาทิตต์พันธุ์และอาจารย์อภิญญา บัณฑิตวุฒิสกุล , ความรู้ทั่วไปเกี่ยวกับการกำกับดูแลกิจการโทรคมนาคมและการออกใบอนุญาตประกอบกิจการโทรคมนาคม, ครั้งที่พิมพ์ 1 (กรุงเทพฯ : แอ๊ปป้า พริ้นติ้ง กรุ๊ป จำกัด, 2552), หน้า 3

สหรัฐอเมริกา OFCOM ของประเทศสหราชอาณาจักร ACMA ของประเทศออสเตรเลีย รวมถึงประเทศไทยเองก็มีสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือที่เรียกว่า กสทช นั่นเอง โดยทิศทางของกิจการโทรคมนาคมของประเทศต่างๆจะไปในแนวทางเดียวกันคือการส่งเสริมให้มีการแข่งขันกันอย่างสมบูรณ์แต่ยังคงมีแนวทางกำกับดูแลซึ่งการกำกับดูแลในแต่ละประเทศจะมีความแตกต่างกันเนื่องจากขึ้นอยู่กับบริบทของประเทศนั้นๆ

การกำกับดูแลกิจการโทรคมนาคมมีผลมาจากข้อกำหนดที่ 5 ในเอกสารการอ้างอิง (Reference Paper) ขององค์การการค้าโลกเรื่อง Telecommunication Services[38] ที่ได้กล่าวไว้ว่า หน่วยงานในการกำกับดูแลต้องแยกออกจากผู้ให้บริการโทรคมนาคมและต้องไม่มีความรับผิดต่อผู้ให้บริการโทรคมนาคมรายใดรายหนึ่ง การตัดสินใจและขั้นตอนที่ใช้โดยหน่วยงานกำกับดูแลจะต้องไม่ลำเอียงต่อผู้เข้าร่วมตลาดทั้งหมด สำหรับประเทศไทยได้มีนโยบายการเปิดให้กิจการโทรคมนาคมภาคเอกชนได้เข้ามาประกอบการอย่างเสรีตามนโยบายที่ประเทศไทยทำไว้กับองค์การการค้าโลกและได้ยกเลิกการผูกขาดการให้บริการของหน่วยงานภาครัฐ โดยการส่งเสริมให้ภาคเอกชนได้ทำการค้าอย่างเสรีภายใต้การกำกับดูแลของ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ซึ่งถูกจัดตั้งตามพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการ วิทยุกระจายเสียง วิทยุโทรทัศน์และกิจการโทรคมนาคม พ.ศ. 2553 ที่จะทำการกล่าวอย่างละเอียดในบทถัดไป

2.5.2 หลักการพื้นฐานในการกำกับดูแลกิจการโทรคมนาคม

จากการสืบค้นเกี่ยวกับแนวคิดในการกำกับดูแลกิจการโทรคมนาคมในประเทศต่างๆ รวมถึงประเทศไทย ผู้วิจัยพบว่าไม่ได้มีหลักเกณฑ์ตายตัวในการใช้กำกับดูแลเนื่องจากต่างประเทศก็ต่างบริบทกันซึ่งการออกกฎเกณฑ์หรือข้อบังคับในการกำกับดูแลกิจการโทรคมนาคมก็จะขึ้นอยู่กับสภาพแวดล้อมหรือสังคมในประเทศนั้น ดังนั้น ผู้วิจัยจะขอทำการสรุปในภาพกว้างว่าหลักการพื้นฐานในการกำกับดูแลกิจการโทรคมนาคมที่ควรมีและประกอบด้วยอะไรบ้าง

---

[38] Telecommunications Services: Reference Paper, Negotiating group on basic telecommunications, [Online], 1996, Source https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm [2022, November 25]

(ก) การกำกับดูแลกิจการโทรคมนาคมต้องมีการกำหนดนโยบายและแนวทางการดำเนินงานให้ชัดเจนไม่ว่าจะเป็นการออกเป็นกฎหมายให้สอดคล้องกับบริบทของประเทศนั้นๆเพื่อที่จะได้กำหนดให้ผู้ให้บริการโทรคมนาคมได้อำนวยความสะดวกแก่ประชาชน

(ข) การเข้าแทรกแซงจากทางภาครัฐอย่างมีประสิทธิภาพโดยที่ไม่ให้ผู้ประกอบการรายใดรายหนึ่งมีอำนาจเหนือตลาดมากเกินไป

(ค) สนับสนุนให้มีการแข่งขันอย่างเสรีและเป็นธรรมของผู้ประกอบการ เพื่อเพิ่มคุณภาพในการให้บริการและเพิ่มศักยภาพของตัวผู้ประกอบการเอง

(ง) การกำหนดกฎเกณฑ์ กติกา ระเบียบ ข้อบังคับเกี่ยวกับการประกอบธุรกิจในเรื่องต่อไปนี้

- การให้บริการโทรคมนาคมที่ได้มาตรฐาน
- มีการกำหนดราคาที่สมเหตุสมผลและประชาชนเข้าถึงได้ง่าย
- ประชาชนต้องสามารถเข้ารับบริการโทรคมนาคมแม้จะอยู่ในพื้นที่ห่างไกล

(จ) ผู้ประกอบการต้องจัดทำรายงานผลการดำเนินงานและการกำกับดูแลต่อหน่วยงานที่กำกับดูแล

(ฉ) มีหน่วยงานที่รับผิดชอบในด้านโทรคมนาคมโดยเฉพาะ ซึ่งสามารถเป็นหน่วยงานอิสระที่อยู่ภายใต้การควบคุมของรัฐหรือไม่ก็ได้

2.5.3 การกำกับดูแลกิจการโทรคมนาคมและแนวทางการป้องกันอาชญากรรม

หลักการการกำกับดูแลกิจการโทรคมนาคมตามที่ได้กล่าวไปแล้วเบื้องต้นนั้นจะเห็นได้ว่า หลักโดยทั่วไปไม่ได้กล่าวถึงการป้องกันอาชญากรรมทางเทคโนโลยีเนื่องจาก หลักการดังกล่าวเป็นหลักการที่เน้นการควบคุมการประกอบกิจการของผู้ให้บริการโทรคมนาคมเป็นส่วนใหญ่ประกอบกับในอดีต อาชญากรรมทางเทคโนโลยีไม่ได้เป็นสิ่งที่เกิดขึ้นซึ่งแตกต่างจากปัจจุบัน เพราะในโลกปัจจุบันเทคโนโลยีเข้ามามีบทบาทเพิ่มมากกว่าในอดีต การพัฒนาอย่างรวดเร็วของเทคโนโลยีทำให้หน่วยงานกำกับดูแลกิจการโทรคมนาคมในปัจจุบันเริ่มหันมาสนใจว่าจะมีแนวทางการปฏิบัติหรือข้อบังคับอย่างให้ให้กิจการเหล่านั้นปฏิบัติตามเพื่อ

บรรเทาความเสี่ยงและความเสียหายที่อาจเกิดขึ้นกับภาคประชาชนรวมถึงภาคธุรกิจเองที่ตกเป็นผู้เสียหายจากเหล่าอาชญากรรมเหล่านั้น

แม้ว่าในปัจจุบันประเทศไทยยังไม่ได้มีข้อปฏิบัติหรือแนวทางการกำกับดูแลอย่างตายตัวว่าหน่วยงานไหนเป็นผู้รับผิดชอบถ้าเกิดเหตุการณ์การหลอกลวงจากเหล่าอาชญากรต่างๆ แต่จากการศึกษาพบว่าภาครัฐเองก็ได้เกิดการตื่นตัวในการหาวิธีการและข้อปฏิบัติต่างๆที่ผู้ประกอบการโทรคมนาคมจะต้องปฏิบัติเพื่อที่จะเป็นหนึ่งในวิธีการลดความเสียหายและอุดช่องว่างต่างๆที่เกิดขึ้น ซึ่งในปัจจุบันสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช) ก็ได้มีการจัดทำรายงานผลการกำกับดูแลกิจการโทรคมนาคมเป็นรายไตรมาสประจำทุกปี[39] ซึ่งในส่วนของรายงานก็จะประกอบไปด้วยหัวข้อใหญ่ๆดังต่อไปนี้

1. การออกใบอนุญาตในกิจการโทรคมนาคม
2. การขอพาดสายสื่อสารโทรคมนาคม
3. สภาพตลาดโทรคมนาคมในปัจจุบัน
4. ภารกิจด้านการทดสอบมาตรฐานคุณภาพการให้บริการโทรศัพท์เคลื่อนที่
5. ประเด็นการรับเรื่องร้องเรียนและคุ้มครองผู้ใช้บริการ
   ซึ่งในการร้องเรียนนี้ไม่ได้รวมถึงการร้องเรียนของผู้บริโภคที่ได้ทำการร้องเรียนเรื่องการโดนหลอกลวงจากอาชญากรรมแก๊งคอลเซ็นเตอร์ ส่วนใหญ่จะเป็นเรื่องร้องเรียนในแง่ของคุณภาพและมาตรฐานของการให้บริการ หรือ การคิดค่าบริการที่ไม่เป็นธรรม เสียมากกว่า

ดังนั้นจะเห็นได้ว่าการกำกับดูแลกิจการโทรคมนาคมในประเทศไทย ยังไม่มีประเด็นการป้องกันอาชญากรรมทางเทคโนโลยีและการกำหนดขั้นตอนปฏิบัติต่างๆที่ใช้ในการป้องกันอาชญากรรมยังไม่ชัดเจนเท่าที่ควรเหมือนกับของต่างประเทศที่ผู้วิจัยได้ทำการศึกษาและจะทำการกล่าวในบทที่ 4 ต่อไป

[39] รายงานข้อมูลการกำกับดูแลกิจการโทรคมนาคม ไตรมาส 1 ปี 2565

บทที่ 3
แนวทางการป้องกันและการกำกับดูแลของกิจการโทรคมนาคมเพื่อป้องกันแก๊งคอลเซ็นเตอร์ในประเทศไทย

ปัจจุบันแก๊งคอลเซ็นเตอร์ได้เข้ามามีบทบาทและกระทบในด้านเศรษฐกิจของประเทศไทยเป็นอย่างมากเนื่องจากการหลอกลวงดังกล่าวทำให้เกิดความสูญเสียทางการเงิน แม้ว่าในซึ่งในปัจจุบันประเทศไทยมีการกำหนดความผิดทางอาญาที่มีการบังคับใช้ไว้อยู่แล้ว ได้แก่ ความผิดฐานฉ้อโกงประชาชนซึ่งถือเป็นความผิดมูลฐานตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 3 และการปกปิดซ่อนเร้นเงินหรือและทรัพย์สินในรูปแบบต่างๆ อันเป็นการฟอกเงินตามมาตรา 5 หรือจะเป็นการนำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลที่นำเข้าในระบบคอมพิวเตอร์เป็นข้อมูลที่บิดเบือนหรือเป็นข้อมูลเท็จไม่ว่าทั้งหมดหรือบางส่วนโดยข้อมูลเหล่านั้นทำให้เกิดความเสียหายแก่ประชาชนซึ่งจะผิดตามมาตรา 14 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 นอกจากนี้ยังมีบทลงโทษทางอาญาเพื่อให้ผู้ที่หลอกลวงรับผิดในการกระทำที่ก่อให้เกิดความเสียหายต่างๆ ตามมาตรา 341 คือการหลอกลวงผู้อื่นด้วยการแสดงข้อความ อันเป็นเท็จหรือปกปิดข้อความจริง มาตรา 342 การกระทำความผิดฐานฉ้อโกง และ 343 แสดงข้อความอันเป็นเท็จต่อประชาชน หรือด้วยการปกปิดความจริงซึ่งควรบอกให้แจ้งแก่ประชาชน ประมวลกฎหมายอาญา ทั้งนี้แม้ว่ากฎหมายมีความพยายามในการป้องกันอาชญากรรมประเภทดังกล่าวและมีบทลงโทษต่างๆซึ่งรวมไปถึงบทลงโทษทางอาญาที่ได้บังคับใช้อยู่ในปัจจุบันที่ได้ทำการกล่าวไปข้างต้น โดยเป็นการกำหนดโทษที่ให้อาชญากรเกรงกลัวและเป็นการดำเนินการปรามปรามอาชญากรรมภายหลังจากที่เกิดขึ้นแล้ว แต่ก็ยังไม่มีประสิทธิภาพจากการบังคับใช้กฎหมายต่างๆมากนักซึ่งจะเห็นได้จากตามข่าวและสถิติการแจ้งความของประชาชนยังคงเกิดความสูญเสียทางการเงินอยู่อย่างต่อเนื่องประกอบกับประเทศไทยในปัจจุบันยังขาดขั้นตอนและการใช้มาตรการการป้องกันที่เหมาะสมในเบื้องต้น

3.1 บทกฎหมายที่ใช้ปราบปรามแก๊งคอลเซ็นเตอร์ออนไลน์ในปัจจุบัน

แม้ว่าในปัจจุบันจะมีการบังคับใช้บทกฎหมายกับผู้กระทำความผิดหรือแก๊งคอลเซ็นเตอร์ออนไลน์ที่แต่กฎหมายดังกล่าวมักจะเป็นกฎหมายที่สามารถใช้บังคับหลังจากเกิดเหตุการณ์ขึ้นแล้วเท่านั้นซึ่งทำให้ในบางครั้งไม่สามารถทำการยับยั้งและป้องกันได้อย่างทันท่วงที

3.1.1 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542

เป็นการใช้กฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมและรวมไปถึงการกำหนดมาตรการในการดำเนินการเกี่ยวกับทรัพย์สินตามกฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามการฟอกเงินประกอบกับหลักการของกฎหมายดังกล่าวที่มีการยึดหรืออายัดทรัพย์สินนั้นเป็นเพียงมาตรการชั่วคราวเพื่อประกันให้มีการริบทรัพย์สินหรือเพื่อใช้เป็นพยานหลักฐานในการพิสูจน์ความผิดในการดำเนินคดีต่างๆ

จากการศึกษาของผู้วิจัยเห็นว่าภายใต้พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มีความเกี่ยวข้องกับความผิดแก๊งคอลเซ็นเตอร์ด้วยกันอยู่ 2 กรณี คือ

(ก) การฉ้อโกงประชาชนซึ่งถือเป็นความผิดมูลฐาน[40]

(ข) การเปลี่ยนสภาพทรัพย์สินที่เกี่ยวกับการกระทำความผิดโดยการปกปิดซ่อนเร้นทรัพย์สิน ไม่ว่าจะเป็นการปกปิดที่มาของทรัพย์สินหรือมีการอำพรางลักษณะที่แท้จริงการได้มารวมถึงการใช้ ครอบครอง โอนซึ่งทรัพย์สินที่เกี่ยวกับการกระทำความผิด[41]

3.1.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

การนำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ซึ่งเป็นข้อมูลที่บิดเบือนหรือเป็นข้อมูลเท็จไม่ว่าทั้งหมดหรือบางส่วนโดยข้อมูลเหล่านั้นทำให้เกิดความเสียหายแก่ประชาชน[42] ในกรณีของแก๊งคอลเซ็นเตอร์ เช่น การโทรมาหลอกลวงให้ผู้เสียหายเข้าเว็บไซต์ที่เป็นของอาชญากรเองซึ่งภายในเว็บไซต์นั้นมีการใช้ข้อมูลที่ผิดๆโดยการแอบอ้างเป็นเว็บไซต์การลงทุน เป็นต้น

3.1.3 ประมวลกฎหมายอาญา

แม้ว่าในปัจจุบันจะมีการบังคับใช้กฎหมายและมีบทลงโทษทางอาญากับผู้กระทำความผิดแก๊งคอลเซ็นเตอร์ ไม่ว่าจะเป็นกรณีของการกระทำความผิดฐานฉ้อโกงโดยอาศัยองค์ประกอบต่างๆในการหลอกลวง เช่น นำความอ่อนแอทางจิตใจของเหยื่อมาเป็น

---

[40] พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 3 (3)

[41] พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 5

[42] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 14

เครื่องมือในการหลอกลวง เป็นต้น[43] หรือการแสดงข้อความที่ไม่เป็นความจริงและปกปิดความจริงที่ควรบอกให้ประชาชนรู้และการหลอกลวงดังกล่าวทำให้ได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวง[44]

ซึ่งบทกฎหมายทั้งหมดที่ทำการกล่าวมาข้างต้นทางผู้วิจัยมองว่าเป็นการแก้ปัญหาทางปลายเหตุ เนื่องจากการที่จะสามารถลงโทษผู้กระทำความผิดดังกล่าวจากบทกฎหมายข้างต้นที่ได้กล่าวมาจะต้องเกิดเหตุการณ์ขึ้นแล้วเท่านั้นประกอบกับการลงโทษผู้กระทำผิดจะต้องประกอบด้วยองค์ประกอบต่างๆเนื่องจากเป็นการลงโทษทางอาญาดังนั้นการที่จะนำตัวผู้กระทำความผิดมาลงโทษแทบจะไม่ได้มีผลอะไรที่ทำให้แก๊งคอลเซ็นเตอร์ลดน้อยลง ดังนั้นประเทศไทยจึงควรหันมาให้ความสำคัญกับการมาตรการการป้องกันและกำกับดูแลก่อนที่จะเกิดเหตุเสียมากกว่า เพราะการหาแนวทางในการป้องกันตั้งแต่ต้นจะสามารถช่วยลดความเสียหายได้ไม่มากก็น้อยและเป็นการสร้างความตื่นตัวให้กับประชาชนในการระมัดระวังแก๊งคอลเซ็นเตอร์ในปัจจุบันประกอบกับในปัจจุบันประเทศไทยยังขาดมาตรการการป้องกันที่เหมาะสม ซึ่งการที่จะป้องกันได้ตั้งแต่ต้นทางจำเป็นจะต้องอาศัยหน่วยงานที่เกี่ยวข้องกับหมายเลขโทรศัพท์มือถือที่ที่เป็นเสมือนต้นน้ำในการวางแนวทางการป้องกันต่างๆ ดังนั้นจึงต้องอาศัยผู้ที่มีอำนาจหน้าที่ตามกฎหมายในการดูแลเรื่องดังกล่าวคือ สำนักงาน คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.)

3.2 หน่วยงานที่เกี่ยวข้องกับการกำกับดูแลแก๊งคอลเซ็นเตอร์ของประเทศไทย

จากการค้นคว้าพบว่า การระบาดของแก๊งคอลเซ็นเตอร์ในประเทศไทยได้ก่อความรำคาญให้กับประชาชนและสร้างความเสียหายจำนวนมาก ทางสำนักงานตำรวจแห่งชาติจึงได้มีการเชิญทั้งหน่วยงานภาครัฐโดยมีหน่วยงานหลักคือสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) และหน่วยงานภาครัฐอื่นๆประกอบกับหน่วยงานภาคเอกชนได้แก่ ผู้ให้บริการโทรคมนาคม มาร่วมกันหารือและหาทางออกเกี่ยวกับแก๊งคอลเซ็นเตอร์นี้เนื่องจากต้องอาศัยความร่วมมือในหลายภาคส่วนหรือคณะทำงานพหุภาคี 11

---

[43] ประมวลกฎหมายอาญา พ.ศ. 2499 มาตรา 342

[44] ประมวลกฎหมายอาญา พ.ศ. 2499 มาตรา 341 , 343

หน่วยงานที่ได้ทำการเกริ่นไปในตอนต้น โดยหน่วยงานต้องร่วมกันหาแนวในการป้องกันและสร้างความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องในการหาแนวทางการป้องกันแก๊งคอลเซ็นเตอร์ โดยสามารถแบ่งหน่วยงานในการกำกับดูแลที่เกี่ยวข้องในเรื่องของแก๊งคอลเซ็นเตอร์ได้ดังต่อไปนี้

3.2.1 หน่วยงานภาครัฐที่เกี่ยวข้อง

หน่วยงานภาครัฐที่เข้ามามีบทบาทและเกี่ยวข้องกับเรื่องแก๊งคอลเซ็นเตอร์มีด้วยกันหลายหน่วยงาน ซึ่งแต่ละหน่วยงานจะมีหน้าที่ที่เป็นอิสระต่อกัน โดยผู้วิจัยจะขอยกมาเฉพาะหน่วยงานที่มีคำสำคัญ ดังต่อไปนี้

1. สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช) เป็นหน่วยงานหลักที่มีหน้าที่ในการกำกับดูแลกิจการโทรคมนาคมโดยตรง โดยอาศัยอำนาจของรัฐธรรมนูญแห่งราชอาญาจักรไทย พ.ศ.2560 มาตรา 60 ซึ่งได้กล่าวไว้ว่าภาครัฐต้องจัดให้มีองค์กรอิสระในการรับผิดชอบและกำกับการดำเนินงานในการจัดให้มีการใช้ประโยชน์จากคลื่นซึ่งหนึ่งในนั้นคือธุรกิจโทรคมนาคมโดยที่ประชาชนต้องได้รับประโยชน์สูงสุด[45] กล่าวโดยสรุปคือรัฐธรรมนูญได้ให้อำนาจกับองค์กรอิสระซึ่งต้องเป็นองค์กรของภาครัฐในการกำกับดูแลกิจการโทรคมนาคมต่างๆ เพื่อก่อให้เกิดประโยชน์สูงสุดแก่ประชาชน นอกจากนี้ยังมีมาตรา274[46] ที่ให้อำนาจโดยตรงแก่คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติตามพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553 ซึ่งถือเป็นกฎหมายประกอบรัฐธรรมนูญ โดยที่คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติถือเป็นองค์กรอิสระภายใต้มาตรา 60 วรรค 3 และคณะรัฐมนตรีสามารถดำเนินการแก้ไขพระราชบัญญัติได้ตามอำนาจของรัฐธรรมนูญที่ได้ให้ไว้นอกจากนี้ยังกำหนดรายละเอียดของการคุ้มครองประชาชนไม่ให้ถูกเอารัดเอาเปรียบจากผู้ประกอบการและการดำเนินการใดๆที่จะกระทบต่อสิทธิและ

[45] รัฐธรรมนูญแห่งราชอาญาจักรไทย พ.ศ.2560 มาตรา 60 วรรค3

[46] รัฐธรรมนูญแห่งราชอาญาจักรไทย พ.ศ.2560 มาตรา 274

เสรีภาพของประชาชนไว้ด้วย[47] นอกจากจะมีการแก้ไขความในรัฐธรรมนูญฉบับ พ.ศ. 2560 เกี่ยวกับคลื่นความถี่แล้วยังส่งผลต่อกฎหมายประกอบรัฐธรรมนูญนั่นคือ พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการ วิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม (ฉบับที่ 3) พ.ศ. 2562 ซึ่งเป็นการแก้ไขครั้งที่ 3 นับจากการมี พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553 การแก้ไขครั้งที่ 3[48] มีการเพิ่มเติมเกี่ยวกับการเริ่มกระบวนการสรรหากรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติรวมทั้งวาระการดำรงตำแหน่งของกรรมการติดตาม ซึ่งการประเมินผลการปฏิบัติงานไม่มีความชัดเจนตลอดจนกระบวนการจัดทำงบประมาณรายจ่ายประจำปีของสำนักงาน กสทช. ที่ใช้บังคับอยู่ในปัจจุบันยังเป็นอุปสรรคต่อการปฏิบัติงานทำให้การบริหารงบประมาณเกิดความล่าช้าประกอบกับเทคโนโลยีการสื่อสารโดยใช้คลื่นความถี่ได้พัฒนาขึ้นทำให้ต้องมีการปรับปรุงการอนุญาตให้ใช้คลื่นความถี่ขึ้นใหม่เพื่อให้การใช้คลื่นความถี่เกิดประโยชน์สูงสุด นอกจากนั้นเพื่อประโยชน์ในการแจ้งเหตุฉุกเฉินที่ต้องการความช่วยเหลือของประชาชนเลยทำให้มีการกำหนดหมายเลขโทรศัพท์ฉุกเฉินแห่งชาติเพื่อให้การรับแจ้งเหตุฉุกเฉินมีประสิทธิภาพสูงสุดจึงจำเป็นต้องมีการแก้ไขเกิดขึ้น[49] โดยที่มีข้อสังเกตคือ พระราชบัญญัติฉบับนี้ทำให้สำนักงานกสทช. มีอำนาจเบ็ดเสร็จในการบริหารจัดการสิทธิการเข้าใช้วงโคจรดาวเทียมสามารถจัดการและจัดเก็บผลประโยชน์รวมไปถึงการออกใบอนุญาต กำกับดูแลช่องสัญญาณและคลื่นความถี่ของดาวเทียมต่างชาติได้อีกด้วย โดยทำหน้าที่อำนวยการแทนหน่วยงานของรัฐทั้งในประเทศและต่างประเทศ

---

[47] รัฐธรรมนูญแห่งราชอาญาจักรไทย พ.ศ.2560 มาตรา 60 วรรค3

[48] พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการ วิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม (ฉบับที่ 3) พ.ศ. 2562, หมายเหตุ

[49] พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการ วิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม (ฉบับที่ 3) พ.ศ. 2562

ดังนั้นจึงสามารถสรุปได้ว่า สำนักงานกสทช. เป็นหน่วยงานภาครัฐที่เป็นหน่วยงานหลักในการควบคุมและกำกับดูแลผู้ให้บริการโทรคมนาคม ซึ่งรวมไปถึงเรื่องแก๊งคอลเซ็นเตอร์ออนไลน์ ซึ่งโดยส่วนตัวผู้วิจัยมีความเห็นว่า สำนักงาน กสทช.สามารถกำหนดเกณฑ์ในการหาทางกำกับดูแลเรื่องแก๊งคอลเซ็นเตอร์ได้เนื่องจากมีอำนาจในการออกระเบียบวิธีปฏิบัติต่างๆให้กับผู้ประกอบกิจการโทรคมนาคมในการหาแนวทางการป้องกันรวมถึงขั้นตอนการอุดช่องว่างของเหล่าอาชญากรรมต่างๆ เหมือนของประเทศออสเตรเลียที่จะทำการกล่าวในบทถัดไปว่าประเทศออสเตรเลียมีแนวทางในการป้องกันแก๊งคอลเซ็นเตอร์อย่างไรเพื่อบรรเทาความเสียหายจากหนักให้เป็นเบา นอกจาก สำนักงาน กสทช. ที่เป็นหน่วยงานหลักแล้ว ยังมีหน่วยงานภาครัฐอื่นๆที่เกี่ยวข้องในการร่วมกันหาแนวทางการป้องกันแก๊งคอลเซ็นเตอร์ โดยแต่ละหน่วยงานจะมีหน้าที่เฉพาะแตกต่างกันออกไป ดังนี้

2. สำนักงานตำรวจแห่งชาติ มีหน้าที่รับแจ้งความและรับเรื่องร้องเรียนต่างๆ ประกอบกับในปัจจุบันได้เปิดให้มีการแจ้งความผ่านระบบออนไลน์ โดยประชาชนสามารถแจ้งผ่านทางเว็บไซต์ www.thaipoliceonline.com หรือปรึกษาปัญหาได้ที่เบอร์ด่วน 1441 ซึ่งภายในเว็บไซต์ดังกล่าวได้มีคู่มือในการใช้ระบบและเบอร์สายด่วนไว้ให้ประชาชนสามารถโทรติดต่อได้ตลอด 24 ชั่วโมง[50]

3. กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บช.สอท). ทำหน้าที่รับผิดชอบคดีเกี่ยวกับอาชญากรรมทางเทคโนโลยีเป็นหลัก[51]

4. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ภายใต้การกำกับดูและของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) มีหน้าที่กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ซึ่งในปัจจุบันได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือที่เรียกว่า PDPA ซึ่งทางรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อ

---

[50] ผู้จัดการออนไลน์, เปิดขั้นตอนแจ้งความออนไลน์ thaipoliceonline.com รับเฉพาะคดีอาชญากรรมทางเทคโนโลยี, [ออนไลน์], 2565, แหล่งที่มา https://mgronline.com/onlinesection/detail/9650000021035 [22 ตุลาคม 2565]

[51] สุภาพิชญ์ ถิระวัฒน์, กองบัญชาการตำรวจไซเบอร์, [ออนไลน์], 2564, แหล่งที่มา https://library.parliament.go.th/th/radioscript-rr2564-nov1 [17 ตุลาคม 2565]

เศรษฐกิจและสังคม มองว่าหลังจากการประกาศใช้ PDPA ไปคาดว่าปัญหาแก๊งคอลเซ็นเตอร์จะลดลง[52]

5. ธนาคารแห่งประเทศไทย (ธปท.) ในส่วนของธนาคารแห่งประเทศไทยนั้นจะมีบทบาทและหน้าที่ในการควบคุมบัญชีม้า ซึ่งในปัจจุบันก็ยังไม่มีวิธีที่สามารถกำจัดบัญชีม้าได้อย่าง100เปอร์เซ็นต์เนื่องจากความยากของการสืบสวนและการปกปิดตัวตนที่ไม่ให้เชื่อมโยงไปถึงผู้กระทำความผิดได้[53]

6. สมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์ และสภาองค์กรของผู้บริโภค

7. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หน้าที่หลักคือ เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

3.2.2 ความร่วมมือจากหน่วยงานเอกชนที่มีส่วนเกี่ยวข้อง

หน่วยงานเอกชนที่มีส่วนร่วมในกับปัญหาแก๊งคอลเซ็นเตอร์ของประเทศไทยส่วนใหญ่มักจะได้รับผลกระทบโดยตรงและเป็นส่วนหนึ่งใน 11 หน่วยงานคณะทำงานพหุภาคี โดยหน่วยงานเอกชนประกอบไปด้วย

1. ผู้ให้บริการโทรคมนาคม หมายถึง บริษัทผู้ให้บริการเครือข่ายโทรศัพท์มือถือ โดยบริษัทต่างๆมักจะส่งตัวแทนของบริษัทเข้ามาร่วมหารือในการร่วมกันหาแนวทางในการป้องกันอาชญากรรมทางเทคโนโลยี

2. บริษัท Gogolook ประเทศไทย คือบริษัทผู้พัฒนาแอปพลิเคชันฮูส์คอลล์ (Whoscall) ที่ในปัจจุบันสามารถช่วยบรรเทาให้ประชาชนตระหนักรู้ว่าเบอร์ที่ทำการโทรเข้ามาเป็นเบอร์ของมิจฉาชีพหรือไม่

---

[52] ไทยรัฐออนไลน์, หวัง PDPA ลดแก๊งคอลเซ็นเตอร์, [ออนไลน์], 2565, แหล่งที่มา https://www.thairath.co.th/business/economics/2429726 [22 ตุลาคม 2565]

[53] พิมพ์ธัญญา ฆ้องเสนาะ, บัญชีม้า, [ออนไลน์], 2565, แหล่งที่มา https://library.parliament.go.th/th/radioscript/rr2565-may6 [19 ตุลาคม 2565]

3.3 แนวทางการป้องกันแก๊งคอลเซ็นเตอร์ของประเทศไทย

จากสถานการณ์แก๊งคอลเซ็นเตอร์ระบาดในประเทศไทยได้สร้างความตื่นตัวให้กับภาครัฐรวมไปถึงภาคเอกชนอย่างมาก เนื่องจากได้สร้างความเสียหายให้กับประชาชนเป็นจำนวนมากซึ่งในปัจจุบันประเทศไทยยังไม่มีการกำหนดแนวทางที่แน่ชัดและเป็นรูปธรรมในการวางแผนปฏิบัติการ (Action Plan) การป้องกันแก๊งคอลเซ็นเตอร์ดังกล่าวเหมือนของต่างประเทศซึ่งในต่างประเทศจะเน้นมาตรการเชิงรุก คือ เน้นการป้องกันมากกว่าแก้ไขและมีการกำหนดแผนปฏิบัติการอย่างชัดเจนเป็นรูปธรรมและมีตัวชี้วัดแผนปฏิบัติการนั้น ซึ่งหนึ่งในประเทศที่ผู้วิจัยได้ทำการศึกษาและเห็นสมควรว่าควรจะนำมาเป็นตัวอย่างให้กับประเทศไทยนั่นคือ ประเทศออสเตรเลีย โดยประเทศออสเตรเลียมีการกำหนดและวางแผนปฏิบัติการการป้องกันหรือที่เรียกว่า The Combating Scams Action Plan ที่จะทำการกล่าวถึงในบทถัดไปอย่างละเอียด โดยแผนปฏิบัติการดังกล่าวเป็นการร่วมมือของทางภาครัฐและภาคเอกชนซึ่งก็คือผู้ให้บริการโทรคมนาคมในการร่วมมือกันและวางแผนการป้องกันการหลอกลวงของแก๊งคอลเซ็นเตอร์ อีกหนึ่งประเทศคือประเทศอังกฤษที่มีการวางแผนปฏิบัติการป้องกันการหลอกลวง ที่เรียกว่า Nuisance calls and messages Update to ICO / Ofcom joint action plan เป็นแผนปฏิบัติการร่วมมือขององค์กรภาครัฐและเอกชนเช่นเดียวกัน ดังนั้นเมื่อเกิดเหตุการณ์ขึ้นกับประชาชน ประชาชนสามารถไปติดต่อและเข้าถึงหน่วยงานที่เกี่ยวข้องได้ทันท่วงทีและบางรายสามารถทำการยับยั้งและอายัติบัญชีได้ก่อนที่มิจฉาชีพจะถอนเงินออกไป แต่ในทางกลับกันประเทศไทยส่วนใหญ่จะเน้นที่การจับกุมหลังจากที่เกิดผู้เสียหายแล้วมากกว่าการวางแผนป้องกัน แม้ว่าในประเทศไทยในปัจจุบันจะมีแอปพลิเคชันฮูส์คอลล์ (Whoscall) ที่ใช้ในการตรวจสอบหมายเลขโทรศัพท์ว่าสายที่โทรเข้ามานั้นเป็นสายของมิจฉาชีพหรือไม่ แต่ก็ทำได้แค่เช็คเบื้องต้นเท่านั้น โดยแอปพลิเคชันดังกล่าวได้รับการพัฒนาจาก บริษัท gogolook ซึ่งเป็นบริษัทพัฒนาแอปพลิเคชันสัญชาติไต้หวันที่โดดเด่นทางด้านเทคโนโลยีในการป้องกันการทุจริต (Anti-Fraud Technology) และมีฐานข้อมูลที่ใหญ่ที่สุดในภูมิภาคเอเชียตะวันออกและเอเชียตะวันออกเฉียงใต้ โดยมีข้อมูลเบอร์โทรศัพท์มากกว่า 1.6 พันล้านหมายเลข[54]

---

[54] Mobileocta_Admin, Gogolook ปั้น Whoscall แพลตฟอร์มต่อต้านการฉ้อโกงแห่งแรกในประเทศไทย ปกป้องคนไทยไม่ให้ตกเป็นเหยื่อการใช้โทรศัพท์และข้อความหลอกลวง, [ออนไลน์], 2565, แหล่งที่มา https://www.mobileocta.com/gogolook-creates-whoscall-the-first-anti-fraud-platform-in-thailand/ [25 พฤศจิกายน 2565]

ในปัจจุบันคณะทำงานพหุภาคี 11 หน่วยงานที่เกี่ยวข้องกับการแก้ไขปัญหาคอลเซ็นเตอร์ในประเทศไทยได้ทำการเสนอต่อบอร์ด กสทช ว่าให้ที่ประชุม กสทช. พิจารณากำหนดในเงื่อนไขท้ายใบอนุญาตให้ผู้ประกอบการโทรศัพท์เคลื่อนที่ทุกรายสร้างระบบหรือแอปพลิเคชันที่ให้ประชาชนสามารถเลือกสมัครบริการปฏิเสธไม่รับสายที่โทรมาจากต่างประเทศได้รวมถึงมีมาตรการในการแก้ไขปัญหาและประสานงานกับบริษัทเครือข่ายมือถือเพื่อหาวิธีเตือนให้ผู้ใช้โทรศัพท์ให้ตระหนักถึงการโทรเข้าของมิจฉาชีพโดยหากเป็นเลขหมายที่โทรมาจากต่างประเทศหรือโทรผ่านระบบอินเทอร์เน็ต ทางค่ายมือถือจะโชว์เป็นเครื่องหมายบวกบนหมายเลขโทรศัพท์[55] (ตัวอย่างรูปที่5) เพื่อแจ้งเตือนผู้รับสาย ดังนั้น ในส่วนของประชาชนต้องมีการสร้างความตระหนักรู้ต่อปัญหาร่วมกัน มีสติและคอยติดตามข่าวสารด้านอาชญากรรมในยุคดิจิทัลเพื่อป้องกันตัวเองในการตกเป็นเหยื่อ โดย11หน่วยงานดังกล่าวประกอบไปด้วย[56] กสทช. ผู้แทนกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ก.ดีอีเอส) ผู้แทนคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผู้แทนธนาคารแห่งประเทศไทย (ธปท.) ผู้แทนกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บช.สอท). ผู้แทนประกอบการโทรศัพท์เคลื่อนที่รายใหญ่ทั้ง 4 ราย (AIS TRUE DTAC และ NT) ผู้แทนสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์ และผู้แทนสภาองค์กรของผู้บริโภค

---

[55] ปฐมพงศ์ ศรีแสงจันทร์, คณะทำงานพหุภาคีแก้ไขปัญหาคอลเซ็นเตอร์เสนอบอร์ด กสทช. ขีดเส้นตายให้โอเปอเรเตอร์ทุกรายสร้างระบบให้ประชาชนเลือกสมัครบริการปฏิเสธไม่รับสายที่โทรมาจากต่างประเทศ เพื่อลดความเดือดร้อนจากปัญหาดังกล่าวโดยเร็วที่สุด, [ออนไลน์], 2565, แหล่งที่มา https://www.nbtc.go.th/News/Press-Center/55326.aspx?lang=th-th [25 พฤศจิกายน 2565]

[56] ข่าวเศรษฐกิจ, กสทช.ฟัน ‘ค่ายมือถือ’ วันละล้านไร้น้ำยาปราบคอลเซ็นเตอร์, [ออนไลน์], 2565, แหล่งที่มา https://www.bangkokbiznews.com/business/1014117 [27 พฤศจิกายน 2565]

รูปภาพที่ 5[57] สำรวจเบอร์อันตราย ห้ามรับสาย ห้ามโทรกลับ ก่อนสูญเงิน

สำนักงานตำรวจแห่งชาติได้เปิดเผยว่า[58] ตัวเลขของผู้เสียหายแจ้งความผ่านระบบ โดยเป็นการเปิดศูนย์รับแจ้งความออนไลน์เมื่อวันที่ 1 มี.ค.- 10 พ.ค.65 ที่ผ่านมา พบว่ามีจำนวนการแจ้งความเสียหายเข้ามา 22,426 คดี มูลค่าความเสียหายเฉลี่ยกว่า 1,500 ล้านบาทต่อเดือน และมีการแจ้งความเฉลี่ยวันละ 300 คดี ส่วนใหญ่เป็นการหลอกลวงด้านการเงินที่มีคดีที่มีความเชื่อมโยงกันถึง 5,079 คดี จากตัวเลขดังกล่าวจะเห็นได้ว่า ประเทศไทยได้มีการสูญเสียในระบบเศรษฐกิจอย่างมหาศาล ถ้าทำการปล่อยไว้จะทำให้มีประชาชนได้รับความเสียหายเพิ่มขึ้นอีกเท่าตัว

จะเห็นได้ว่า ประเทศไทยยังไม่มีแผนปฏิบัติการที่ใช้สำหรับเป็นแนวทางการป้องกันที่เป็นรูปธรรม ซึ่งส่วนใหญ่จะสามารถสังเกตุได้จากตามหน้าข่าวว่าเป็นกระบวนการกวาดล้างและเป็นการปราบปรามเสียมากกว่า ประกอบกับหน่วยงานหลักในการกำกับดูแลยังขาดมาตรการที่ชัดเจนในการ

---

[57] Workpoint TODAY, สำรวจเบอร์อันตราย ห้ามรับสาย ห้ามโทรกลับ ก่อนสูญเงิน, [ออนไลน์], 2562, แหล่งที่มา https://workpointtoday.com/%E0%B8%AB%E0%B9%89%E0%B8%B2%E0%B8%A1%E0%B8%A3%E0%B8%B1%E0%B8%9A%E0%B8%AA%E0%B8%B2%E0%B8%A2-%E0%B8%AB%E0%B9%89%E0%B8%B2%E0%B8%A1%E0%B9%82%E0%B8%97%E0%B8%A3%E0%B8%81%E0%B8%A5%E0%B8%B1%E0%B8%9A/ [11 พฤศจิกายน 2565]

[58] 7HDร้อนออนไลน์, ผบ.ตร. นัดถกหน่วยงานภาครัฐและเอกชน ร่วมมือออกมาตรการจัดการแก๊งคอลเซ็นเตอร์, [ออนไลน์], 2565, แหล่งที่มา https://news.ch7.com/detail/569172 [9 พฤศจิกายน 2565]

แก้ไขปัญหารวมไปถึงการแบ่งแยกหน้าที่ในการจัดการกับปัญหาดังกล่าวยังมีความคลุมเครือ ดังนั้น ผู้วิจัยเห็นว่าประเทศไทยควรจัดทำแผนปฏิบัติการการป้องกันและบรรเทาการเกิดแก๊งคอลเซ็นเตอร์ที่ชัดเจน เพื่อป้องกันเหตุการณ์ก่อนที่จะเกิดเหตุการณ์ขึ้น เนื่องจากในปัจจุบันภาครัฐของประเทศไทยมีการประชุมเรื่องคอลเซ็นเตอร์อยู่ตลอดเวลาและมีการจัดทำ MOU ต่างๆ แต่การที่จัดทำ MOU นั้นไม่ได้เป็นเครื่องมือที่สามารถใช้บังคับได้เนื่องจาก MOU ไม่ได้มีผลตามกฎหมายโดยตรง รวมไปถึงเพื่อความเป็นรูปธรรมและสามารถวัดผลได้ดังเช่นประเทศออสเตรเลียที่จะทำการกล่าวในบทถัดไป

3.4 ประกาศและหลักเกณฑ์ต่างๆที่เกี่ยวข้องกับการใช้บริการโทรศัพท์ภายใต้การกำกับดูแลของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ

หลังจากที่สำนักงาน กสทช มีอำนาจจากกฎหมายในการควบคุมดูแลกิจการโทรคมนาคมต่างๆ ส่งผลให้มีมาตรการและออกหลักเกณฑ์มาเพื่อใช้บังคับกับผู้ให้บริการโทรคมนาคมโดยมีจุดประสงค์คือเพื่อให้สามารถดำเนินการไปได้อย่างเหมาะสมสอดรับกับสถานการณ์และการเปลี่ยนแปลงของเทคโนโลยีรวมไปถึงการคุ้มครองสิทธิของผู้บริโภค โดยหลักเกณฑ์สำคัญๆที่ทางผู้วิจัยเห็นว่ามีความเกี่ยวเนื่องกับเรื่องแก๊งคอลเซ็นเตอร์ มีดังต่อไปนี้

3.4.1 ประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่

ประกาศฉบับนี้เกี่ยวกับการที่ผู้ใช้บริการต้องการย้ายค่ายโทรศัพท์แต่ต้องการใช้หมายเลขเดิม อธิบายให้เข้าใจง่ายคือ การย้ายค่ายเบอร์เดิม โดยหัวใจสำคัญของประกาศฉบับนี้เพื่อป้องกันสิทธิของผู้ใช้บริการและคุ้มครองผลประโยชน์ของผู้ใช้บริการในการที่จะเปลี่ยนผู้ให้บริการโดยที่ผู้ให้บริการไม่สามารถทำการขัดขวางผู้ใช้บริการในการเปลี่ยนผู้ให้บริการได้ยกเว้นกรณีหมายเลขนั้นได้มาโดยไม่ชอบด้วยกฎหมาย หรือ เลขหมายนั้นอยู่ในระหว่างการดำเนินคดี นอกจากนี้หัวใจสำคัญคือผู้ให้บริการรายใหม่และรายเดิมต้องร่วมกันตรวจสอบข้อมูลของผู้ใช้บริการเพื่อเป็นการยืนยันสถานะความเป็นเจ้าของหมายเลขและตรวจสอบยืนยันสถานภาพและเงื่อนไขอื่นใดกับผู้ให้บริการรายเดิม โดยผู้ให้บริการต้องดำเนินการให้เสร็จภายใน 2 วันนับแต่วันที่ผู้ใช้บริการได้ยื่นคำขอเว้นแต่เอกสารต่างๆจะไม่

ครบถ้วน[59] โดยสำนักงาน กสทช.ได้ใช้อำนาจ[60] ในการออกประกาศฉบับนี้ เพื่อเป็นการควบคุมวิธีการปฏิบัติงานของผู้ให้บริการรายเดิมและรายใหม่ให้ปฏิบัติตามประกาศอย่างเคร่งครัด

3.4.1.1 หลักเกณฑ์การโอนย้ายผู้ให้บริการโทรศัพท์เคลื่อนที่ของผู้ใช้บริการโทรศัพท์เคลื่อนที่ ตามประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่

วัตถุประสงค์ของหลักเกณฑ์ฉบับนี้คือพัฒนาการให้บริการและกระบวนการโอนย้ายผู้ให้บริการโทรศัพท์และรักษาสิทธิของผู้ใช้บริการในการครอบครองและใช้งานหมายเลขโทรศัพท์โดยผู้ให้บริการโทรคมนาคมมีหน้าที่ในการปฏิบัติตามโดยการประชาสัมพันธ์เผยแพร่หลักเกณฑ์นี้ให้ประชาชนทั่วไปสามารถเข้าใจโดยง่าย ดำเนินการเพื่อให้สามารถเรียกไปยังหมายเลขที่ถูกโอนย้ายและส่วนสำคัญคือผู้ให้บริการจะต้องร่วมกันตรวจสอบการดำเนินการตามหลักเกณฑ์ฉบับนี้ให้ถูกต้องครบถ้วน และ ร่วมกันพิจารณาถึงข้อดี ข้อเสีย ปัญหาอุปสรรคต่างๆ เพื่อเสนอต่อสำนักงาน กสทช. ในการแก้ไขปรับปรุงการดำเนินการโอนย้ายและการบริการผู้ให้บริการให้ดียิ่งขึ้นไปโดยการแก้ไขปรับปรุงในแต่ละคราวนั้นให้ดำเนินการเป็นระยะที่เหมาะสม เนื่องจากการที่ผู้ให้บริการโทรคมนาคมปฏิบัติและตรวจสอบตามเกณฑ์ที่กำหนด จะสามารถอุดช่องว่างหรือการเกิดอาชญากรรมได้ในบางส่วนเนื่องจากลูกค้าจะถูกการตรวจสอบและการยืนยันตัวตนก่อนที่จะมีการจัดส่งซิมการ์ดให้[61] โดยหลักเกณฑ์ฉบับนี้เป็นไปตามประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมาย

---

[59] ประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่

[60] พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553 มาตรา 27 ,มาตรา 81 และ พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มาตรา 12 วรรค 4

[61] หลักเกณฑ์การโอนย้ายผู้ให้บริการโทรศัพท์เคลื่อนที่ของผู้ใช้บริการโทรศัพท์เคลื่อนที่ ตามประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่ (MNP Porting Process Manual) ฉบับตามมติ กสทช. ครั้งที่ 15/2564 เมื่อวันที่ 11 สิงหาคม 2564

โทรศัพท์เคลื่อนที่ โดยที่ผู้ให้บริการต้องจัดทำรายละเอียดหลักเกณฑ์การโอนย้ายผู้ให้บริการโทรศัพท์เคลื่อนที่เพื่อที่จะเสนอแผนต่อสำนักงาน กสทช. ต่อไป[62]

(ก) บทบาทหน้าที่ของผู้ให้บริการรายใหม่

โดยทางผู้วิจัยจะขอทำการเน้นและสรุปเพียงประเด็นหน้าที่ของผู้ให้บริการรายใหม่ในหลักเกณฑ์ฉบับนี้เนื่องจากผู้ให้บริการรายใหม่จะเป็นผู้ที่มีภาระหน้าที่ในการพิสูจน์ยืนยันตัวตนในการดำเนินการข้อมูลและเอกสารหลักฐาน ซึ่งทางผู้วิจัยมองว่าผู้ให้บริการรายใหม่เปรียบเสมือนปลายทางที่สามารถดักจับความผิดปกติหากเกิดกรณีการหลอกหลวงโดยมิจฉาชีพหรือการใช้เบอร์โทรศัพท์โดยไม่ถูกกฎหมาย โดยที่ผู้ให้บริการรายใหม่ต้องให้ผู้ใช้บริการให้รายละเอียดข้อมูลคำขอโอนย้าย ซึ่งสามารถเป็นรูปแบบกระดาษหรือรูปแบบอิเล็กทรอนิกส์ก็ได้

- กรณีผู้ใช้บริการเป็นบุคคลธรรมดา ผู้ใช้บริการจะต้องให้ข้อมูลและเอกสารต่างๆอย่างน้อยดังนี้ 1.บัตรประชาชน หนังสือเดินทาง(กรณีชาวต่างชาติ) หรือบัตรที่ออกโดยหน่วยงานราชการ 2.หมายเลขโทรศัพท์ที่ผู้ใช้บริการขอโอนย้าย 3.รหัสแสดงตนที่ผู้ใช้บริการได้รับจากผู้ให้บริการรายเดิม โดยผู้ให้บริการรายใหม่ต้องมีการพิสูจน์และยืนยันตัวบุคคลของผู้ใช้บริการด้วยระบบอัตลักษณ์[63]
- กรณีผู้ใช้บริการเป็นนิติบุคคล ให้ดำเนินการยื่นคำขอโอนย้าย ณ ศูนย์ให้บริการของผู้ให้บริการรายใหม่เท่านั้น โดยผู้ให้บริการรายใหม่จะต้องเรียกดูเอกสารของผู้ใช้บริการประกอบด้วยข้อมูลอย่างน้อยดังนี้ 1.บัตรประจำตัวประชาชนของผู้มีอำนาจกระทำการแทนนิติบุคคลหรือบัตรที่หน่วยงานราชการออกให้ กรณีผู้มีอำนาจกระทำการ

[62] ประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่ ข้อ12

[63] หลักเกณฑ์การโอนย้ายผู้ให้บริการโทรศัพท์เคลื่อนที่ของผู้ใช้บริการโทรศัพท์เคลื่อนที่ ตามประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่ (MNP Porting Process Manual) ฉบับตามมติ กสทช. ครั้งที่ 15/2564 เมื่อวันที่ 11 สิงหาคม 2564

แทนนิติบุคคลไม่ใช่คนไทยให้ใช้หนังสือเดินทาง หรือกรณีผู้มีอำนาจกระทำการแทนนิติบุคคลได้มอบอำนาจให้บุคคลอื่นกระทำการแทนให้ใช้สำเนาเอกสารข้างต้น ซึ่งลงลายมือชื่อรับรองสำเนาถูกต้องแล้ว 2. หนังสือรับรองนิติบุคคล 3.สำเนาใบแจ้งหนี้ที่ได้มีการชำระค่าใช้บริการแล้ว 4.หนังสือมอบอำนาจสำเนาบัตรประจำตัวประชาชนของผู้มอบอำนาจและบัตรประจำตัวประชาชนของผู้รับมอบอำนาจ ในกรณีให้บุคคลอื่นยื่นคำขอแทน 5.หมายเลขโทรศัพท์เคลื่อนที่ ที่ผู้ใช้บริการขอโอนย้าย 6.รหัสแสดงตนที่ผู้ใช้บริการได้รับจากผู้ให้บริการรายเดิม[64]

จะเห็นได้ว่าการจัดเก็บข้อมูลเพื่อนำมาใช้ในการยืนยันตัวตนไม่ว่าจะเป็นลูกค้าบุคคลธรรมดาหรือนิติบุคคล ผู้ให้บริการรายใหม่มีหน้าที่ในการตรวจสอบเอกสาร จัดทำ และจัดเก็บข้อมูลหลักฐานของผู้ใช้บริการตามที่ได้กล่าวไปข้างต้น โดยจัดทำในรูปแบบอิเล็กทรอนิกส์ให้ครบถ้วนและให้ถือว่าผู้ใช้บริการได้แสดงเจตนาในการยื่นขอโอนย้ายผู้ให้บริการโดยสมบูรณ์และให้เริ่มดำเนินการโอนย้ายผู้ให้บริการตามขั้นตอนการโอนย้าย (Porting Process) ของหลักเกณฑ์ฉบับนี้ต่อไป

[64] หลักเกณฑ์การโอนย้ายผู้ให้บริการโทรศัพท์เคลื่อนที่ของผู้ใช้บริการโทรศัพท์เคลื่อนที่ ตามประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่ (MNP Porting Process Manual) ฉบับตามมติ กสทช. ครั้งที่ 15/2564 เมื่อวันที่ 11 สิงหาคม 2564

รูปภาพที่ 6[65] วิธีย้ายค่ายมาเป็นครอบครัว AIS

(ข) ช่องทางการยื่นคำขอต่อผู้ให้บริการรายใหม่

ผู้ใช้บริการต้องทำการยื่นคำขอย้ายหมายเลขต่อผู้ให้บริการรายใหม่โดยสามารถยื่นได้ ณ จุดให้บริการโอนย้ายโดยผู้ให้บริการ ซึ่งประกอบไปด้วย

- ศูนย์บริการลูกค้าหรือจุดให้บริการของผู้ให้บริการรายใหม่ซึ่งจุดนั้นต้องได้รับการแต่งตั้งจากผู้ให้บริการรายใหม่เพื่อจำหน่ายสินค้าและบริการ ทำการตลาดและจุดให้บริการนั้นต้องแสดงสัญลักษณ์ทางการค้าของผู้ให้บริการรายใหม่ โดยจุดให้บริการดังกล่าวต้องปฏิบัติตามเกณฑ์และมีความรับผิดชอบร่วมกันเสมือนผู้ให้บริการรายใหม่
- ช่องทางออนไลน์ ได้แก่เว็บไซต์ แอปพลิเคชัน ของผู้ให้บริการรายใหม่ โดยลูกค้าจะเป็นคนดำเนินการโอนย้ายด้วยตนเองซึ่งผู้ให้บริการรายใหม่ต้องเป็นคนจัดทำวิธีการ ขั้นตอนและกระบวนการพิสูจน์ยืนยันตัวตนโดยวิธีการดังกล่าวต้องผ่านการตรวจสอบจาก สำนักงาน กสทช.

[65] Knowledge Center, วิธีย้ายค่ายมาเป็นครอบครัว AIS, [ออนไลน์], แหล่งที่มา https://aiscallcenter.ais.co.th/ikm/acc/index.php?kmid=KM1020179 [29 ตุลาคม 2565]

- จุดให้บริการอื่นๆที่ได้รับการอนุญาตจาก สำนักงาน กสทช. โดยลูกค้าจะเป็นผู้ดำเนินการโอนย้ายด้วยตนเองแต่จุดบริการนั้นต้องมีเงื่อนไขดังต่อไปนี้คือ

1. เป็นนิติบุคคลที่ตั้งขึ้นตามกฎหมายไทย
2. มีการทำสัญญาและได้รับแต่งตั้งอย่างเป็นทางการจากผู้ให้บริการ
3. มีระบบการสื่อสารข้อมูลที่เชื่อมต่อโดยตรงกับผู้ให้บริการรายใหม่ทุกราย
4. มีระบบและอุปกรณ์การให้บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่ผ่านระบบธุรกรรมอิเล็กทรอนิกส์ด้วยระบบอ่านบัตรประจำตัวประชาชน (Card Reader)
5. มีระบบรักษาความปลอดภัยของข้อมูลที่เพียงพอโดยจุดให้บริการต้องไม่มีการจัดเก็บข้อมูลของผู้ใช้บริการไว้ที่ตนเองแต่ให้มีการส่งข้อมูลโดยตรงไปที่ผู้ให้บริการรายใหม่โดยทันที ประกอบกับในปัจจุบันได้มีการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
6. จุดให้บริการนั้นต้องมีการกำหนดเวลาทำการให้ชัดเจนและการพฤติกรรมการบริการหรือการโฆษณาต้องไม่เข้าข่ายการกีดกันทางการแข่งขันกับผู้บริการรายอื่นๆ

ทั้งนี้เมื่อผู้ใช้บริการได้ทำการยื่นคำขอเรียบร้อยแล้ว ผู้ใช้บริการสามารถรับซิมการ์ดใหม่โดยติดต่อผู้ให้บริการรายใหม่ ณ ศูนย์บริการลูกค้าของผู้ให้บริการรายใหม่หรือจุดให้บริการอื่นๆตามที่ได้กำหนดไว้ข้างต้น กรณีที่ผู้ใช้บริการยื่นคำขอผ่านช่องทางออนไลน์และประสงค์จะให้ผู้ให้บริการจัดส่งซิมการ์ด ผู้ให้บริการสามารถจัดส่งซิมการ์ดให้ตามความประสงค์ของผู้ใช้บริการ โดยผู้ให้บริการต้องจัดให้ผู้ใช้บริการทำการยืนยันตัวตนก่อนเปิดใช้หมายเลขทั้งนี้ผู้ให้บริการจะต้องนำเสนอรายละเอียดวิธีการ ขั้นตอน และ กระบวนการพิสูจน์และยืนยันตัวบุคคลซึ่งวิธีดังกล่าวต้องผ่านการทดสอบจากสำนักงาน กสทช[66]

[66] หลักเกณฑ์การโอนย้ายผู้ให้บริการโทรศัพท์เคลื่อนที่ของผู้ใช้บริการโทรศัพท์เคลื่อนที่ ตามประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่ (MNP Porting Process Manual) ฉบับตามมติ กสทช. ครั้งที่ 15/2564 เมื่อวันที่ 11 สิงหาคม 2564

จะเห็นได้ว่าไม่ว่าผู้ใช้บริการจะส่งคำขอโอนย้ายหมายเลขผ่านช่องทางใด ผู้ให้บริการรายใหม่จะต้องทำการพิสูจน์และยืนยันตัวตน หรือ จัดให้มีวิธีการให้ผู้ใช้งานยืนยันตัวตนก่อนการเปิดใช้งานซิมการ์ดเสมอ

3.4.2 ประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง การลงทะเบียนและการจัดเก็บข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่

เนื่องจากการระบาดของแก๊งคอลเซ็นเตอร์ได้สร้างความเสียหายให้กับภาคเศรษฐกิจในประเทศไทยซึ่งปัจจัยที่ทำให้ยังไม่สามารถปราบปรามได้คือเบอร์โทรศัพท์ที่เปลี่ยนแปลงไปเรื่อยๆ ดังนั้นสำนักงาน กสทช.จึงมีคำสั่งคุมเข้มล่าสุดว่า บัตรประชาชน 1 ใบ สามารถลงทะเบียนเบอร์โทรศัพท์ได้ไม่เกิน 5 หมายเลขต่อ1ผู้ให้บริการ แต่หากที่จะต้องมีเบอร์โทรศัพท์มากกว่า 5 หมายเลขจะต้องไปทำการแสดงตนและยืนยันตัวตนที่จุดให้บริการของผู้ให้บริการโทรคมนาคมรวมไปถึงร้านค้าตัวแทนจำหน่าย (ตู้ลูก)[67]เพื่อเป็นการป้องกันไม่ให้มิจฉาชีพนำซิมการ์ดไปใช้ในการหลอกลวงประชาชนให้เกิดความเดือดร้อนและก่อให้เกิดความเสียหายเสียทรัพย์ตามที่ปรากฏเป็นปัญหากว้างขวางในปัจจุบัน โดยที่ผู้ให้บริการโทรคมนาคมต้องดำเนินการปฏิบัติให้เป็นไปตามประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง การลงทะเบียนและการจัดเก็บข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่[68] ซึ่งคำสั่งของสำนักงาน กสทช.ล่าสุดมีวัตถุประสงค์เพื่อที่จะให้ผู้ประกอบกิจการโทรคมนาคมได้มีความเคร่งคัดในการปฏิบัติตามกฎเกณฑ์ดังกล่าว

---

[67] สยามรัฐออนไลน์, สกัดแก๊งคอลเซ็นเตอร์ "กสทช." จ่อปรับ 1 ล้านบาท ค่ายมือถือไม่จัดการลงทะเบียนซิมการ์ด, [ออนไลน์], 2565, แหล่งที่มา https://siamrath.co.th/n/363170 [3 พฤศจิกายน 2565]

[68] ประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง การลงทะเบียนและการจัดเก็บข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่

รูปภาพที่ 7[69] ค่ายมือถือหวั่น กสทช.ถูกปรับวันละล้าน เข้มงวดร้านลูกตู้ลงทะเบียนซิม 1 คน 1 ค่ายไม่เกิน 5 เบอร์

การเก็บเอกสารในการยืนยันตัวตนของบุคคลธรรมดาในประกาศดังกล่าว จะเน้นไปที่บัตรประชาชนหรือหนังสือเดินทางฉบับจริงกรณีที่เป็นชาวต่างชาติ โดยมีใจความสำคัญของประกาศฉบับนี้คือถ้าผู้ใช้บริการไม่แจ้งรายละเอียดและปฏิเสธไม่ให้เอกสารหลักฐานซึ่งเป็นข้อมูลในการลงทะเบียนผู้ใช้บริการและการพิสูจน์และยืนยันตัวบุคคล จุดให้บริการและผู้ให้บริการสามารถปฏิเสธการลงทะเบียนผู้ใช้บริการและการเปิดให้บริการ ได้โดยจะต้องแจ้งเหตุผลแห่งการปฏิเสธการให้บริการนั้นให้ผู้ใช้บริการได้รับทราบ หน้าที่หลักของผู้ให้บริการคือตรวจสอบความถูกต้องของเอกสารหลักฐานที่ใช้ในการลงทะเบียนรวมทั้งพิสูจน์และยืนยันตัวบุคคล ด้วยความรอบคอบและรัดกุมให้เป็นไปตามข้อกำหนดและ

[69] ผู้จัดการออนไลน์ ,ค่ายมือถือหวั่น กสทช.ถูกปรับวันละล้าน เข้มงวดร้านลูกตู้ลงทะเบียนซิม 1 คน 1 ค่ายไม่เกิน 5 เบอร์, [ออนไลน์], 2565, แหล่งที่มา https://mgronline.com/onlinesection/detail/9650000078487 [15 พฤศจิกายน 2565]

แนวทางการปฏิบัติ[70] ซึ่งประกาศฉบับนี้เป็นไปตามการให้อำนาจของสำนักงาน กสทช. ในการออกระเบียบ ประกาศ หรือคำสั่งต่างๆ[71]

ทางผู้วิจัยมีความเห็นว่าเห็นด้วยกับออกประกาศดังกล่าวมาเพื่อป้องกันการใช้หมายเลขเบอร์โทรศัพท์ในการหลอกลวงประชาชน เนื่องจากถ้าผู้ให้บริการไม่ปฏิบัติตามตามข้อกำหนดในการพิสูจน์ยืนยันตัวตนและการจัดเก็บเอกสารที่ผู้ให้บริการโทรคมนาคมร้องขอ ผู้ให้บริการโทรคมนาคมสามารถปฏิเสธได้ทันที

3.5 บทลงโทษที่เกี่ยวข้องกับการที่ผู้ประกอบกิจการโทรคมนาคมไม่ทำตามหลักเกณฑ์ที่สำนักงาน กสทช. กำหนด

เนื่องจากทางสำนักงาน กสทช. มีอำนาจหน้าที่ในการออกกฎเกณฑ์ต่างๆตามที่กฎหมายได้ให้อำนาจไว้[72] ดังนั้นผู้ประกอบกิจการโทรคมนาคมต้องปฏิบัติตามประกาศหรือหลักเกณฑ์ต่างๆ ถ้าเกิดการฝ่าฝืนอาจจะมีโทษปรับทางปกครองได้[73] เนื่องจากถือเป็นการกระทำที่ฝ่าฝืนและไม่ปฏิบัติตามกฎหมาย

1. ในกรณีผู้ให้บริการโทรคมนาคมทำการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหรือคำสั่งเกี่ยวกับการอนุญาตและกำกับดูแลการประกอบกิจการ จะต้องเสียค่าปรับทางปกครองไม่ต่ำกว่า 20,000 บาทต่อวันแต่ไม่เกินอัตราร้อยละ 1.1 ของรายได้ก่อนหักค่าใช้จ่ายอันเกิดจากการประกอบกิจการ โทรคมนาคมของผู้รับใบอนุญาตภายใต้ใบอนุญาตประกอบกิจการโทรคมนาคมตามแบบใบอนุญาตนั้นๆ โดยคิดจากรายได้ในปีก่อนหน้า[74]

2. ในกรณีผู้ให้บริการโทรคมนาคมทำการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหรือคำสั่งเกี่ยวกับการคุ้มครองผู้บริโภคหรือประโยชน์สาธารณะ ต้องเสียค่าปรับทางปกครองไม่

---

[70] ประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง การลงทะเบียนและการจัดเก็บข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่

[71] พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553 มาตรา 27 ,มาตรา 81 และ พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มาตรา 50

[72] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2560 มาตรา 60 วรรค3 และมาตรา 274

[73] ประกาศสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่อง กำหนดหลักเกณฑ์การบังคับทางปกครองในกิจการโทรคมนาคม ข้อ.4

[74] ประกาศสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่อง กำหนดหลักเกณฑ์การบังคับทางปกครองในกิจการโทรคมนาคม ข้อ.10 (1) , ภาคผนวก ก ข้อ 4 , 15.12 , 15.13 , 15.14

ต่ำกว่า 60,000 บาทต่อวัน แต่ไม่เกินอัตราร้อยละ 0.3 ของรายได้ก่อนหักค่าใช้จ่ายอันเกิดจากการประกอบกิจการโทรคมนาคม[75] ซึ่งรวมไปถึงการที่ผู้รับใบอนุญาตไม่ปฏิบัติตามมาตรการคุ้มครองผู้ใช้บริการเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม[76]

จะเห็นได้ว่า หากผู้ให้บริการโทรคมนาคมไม่ปฏิบัติตามกฎระเบียนที่สำนักงาน กสทช. กำหนด ไม่ว่าจะเข้าเรื่องอะไรก็ตามผู้ให้บริการโทรคมนาคมจะต้องถูกลงโทษตามโทษปรับทางปกครองตามที่กฎหมายได้กำหนด

ดังนั้นผู้วิจัยจะขอทำการสรุปในบทที่ 3 นี้ว่า แม้ว่าประเทศไทยในปัจจุบันจะมีการบังคับใช้กฎหมายเกี่ยวกับการลงโทษของผู้ที่กระทำความผิดที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์อยู่แล้วก็ตาม ซึ่งบทกฎหมายดังกล่าวเป็นกฎหมายที่มีโทษทางอาญาและถึงแม้ว่ากฎหมายมีความพยายามในการปราบปรามอาชญากรรมประเภทด้วยโทษดังกล่าวประกอบกับมีการใช้บทลงโทษต่างๆ แต่การที่จะสามารถใช้บทลงโทษดังกล่าวได้นั้นต้องเป็นการใช้ภายหลังจากที่เกิดเหตุกาณ์อาชญากรรมเกิดขึ้นแล้วทำให้ประเทศไทยยังประสบปัญหาความสูญเสียทางด้านการเงินในระบบเศรษฐกิจอยู่อย่างต่อเนื่องและจำนวนอาชญากรก็ไม่ได้เกรงกลัวกับบทลงโทษที่บังคับใช้อยู่ในปัจจุบัน ทั้งนี้ทางผู้วิจัยจึงเล็งเห็นว่าในเมื่อกฎหมายที่บังคับใช้ในการจับกุมและดำเนินคดีที่ถือเป็นการลงโทษแบบปลายทางยังไม่มีสามารถจัดการปัญหาแก๊งคอลเซ็นเตอร์ได้เท่าที่ควร ประเทศไทยควรหันมาให้ความสำคัญกับแนวทางในการป้องกันและกำกับดูแลตั้งแต่ต้นทางซึ่งเป็นอีกทางเลือกหนึ่งที่ในปัจจุบันประเทศไทยยังขาดรวมไปถึงการวางแผนปฏิบัติการป้องกันที่เป็นรูปธรรม ชัดเจน รวมถึงการใช้อำนาจทางกฎหมายในการป้องกันที่เหมาะสมซึ่งการที่จะป้องกันได้ตั้งแต่ต้นทางต้องอาศัยหน่วยงานที่เกี่ยวข้องกับหมายเลขโทรศัพท์มือถือที่เป็นเสมือนต้นน้ำในการวางแนวทางการป้องกันต่างๆ ดังนั้นจึงต้องอาศัยผู้ที่มีอำนาจหน้าที่ตามกฎหมายในการดูแลเรื่องดังกล่าวคือ สำนักงาน คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) และในปัจจุบันประเทศไทยได้มีการเชิญหน่วยงานที่มีส่วนเกี่ยวข้องกับเรื่องแก๊งคอลเซ็นเตอร์ทั้งภาครัฐและภาคเอกชนมา

---

[75] ประกาศสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่อง กำหนดหลักเกณฑ์การบังคับทางปกครองในกิจการโทรคมนาคม ข้อ.10 (3) , ภาคผนวก ค ข้อ 8

[76] พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มาตรา 50

ประชุมเพื่อหารือแนวทางต่างๆ แต่ก็ไม่ได้มีการจัดทำเป็นแผนที่เป็นรูปธรรมทำให้ไม่สามารถติดตามผลได้ ดังนั้นเพื่อที่จะแก้ปัญหาดังกล่าวผู้วิจัยจึงจะทำการศึกษาแนวทางการป้องกันของต่างประเทศเพื่อที่จะนำมาปรับใช้ให้เข้ากับบริบทของประเทศไทยเอง โดยจะทำการกล่าวอย่างละเอียดในบทต่อไป

บทที่ 4
กระบวนการในการป้องกันและการกำกับดูแลของกิจการโทรคมนาคมเพื่อป้องกันแก๊งคอลเซ็นเตอร์ของประเทศออสเตรเลียและประเทศสหราชอาณาจักร

ผู้วิจัยได้ทำการค้นคว้าข้อมูลวิธีการในการปราบปรามและป้องกันแก๊งคอลเซ็นเตอร์ของประเทศออสเตรเลียและประเทศสหราชอาณาจักรแล้วนำมาเปรียบเทียบกับประเทศไทยเพื่อพิจารณาว่ามาตรการของประเทศไทยนั้นเพียงพอหรือไม่ ยังขาดหลักการอะไรที่สำคัญบ้าง ที่จะสามารถหามาตรการในการบรรเทาความเสียหายจากการก่ออาชญากรรมทางเศรษฐกิจได้อย่างทันกาลและมีประสิทธิภาพ

4.1 แนวทางการป้องกันและความร่วมมือกันจากภาครัฐและเอกชน

ไม่เพียงแต่ประเทศไทยที่ประสบปัญหากับแก๊งคอลเซ็นเตอร์ประเทศเดียว แม้แต่ประเทศที่พัฒนาแล้วอย่างประเทศออสเตรเลียและประเทศอังกฤษก็ประสบปัญหานี้ไม่ต่างจากประเทศไทยซึ่งสร้างความสูญเสียด้านการเงินให้กับประชากรที่ถูกหลอกลวงและส่งผลกระทบต่อระบบเศรษฐกิจให้กับประเทศดังกล่าวเป็นจำนวนมาก ด้วยปัญหาที่เกิดขึ้นทำให้รัฐบาลของแต่ละประเทศหันมาให้ความสำคัญกับการแก้ปัญหารวมไปถึงวิธีการในการปราบปรามและป้องกันแก๊งคอลเซ็นเตอร์ ซึ่งจากการค้นคว้าพบว่าทั้ง2ประเทศจะเน้นมาตรการการป้องกันที่ได้รับอำนาจจากกฎหมายในการมาบังคับใช้กับผู้ให้บริการโทรคมนาคมซึ่งเป็นต้นทางในการดักจับความผิดปกติของหมายเลขโทรศัพท์

4.1.1 ประเทศออสเตรเลีย

เนื่องจากประเทศออสเตรเลียประสบปัญหาแก๊งคอลเซ็นเตอร์ออนไลน์ที่มีหลากหลายรูปแบบโดยเฉพาะอย่างยิ่งการหลอกลวงทางโทรศัพท์ยังคงเป็นวิธีที่พบได้บ่อยที่สุดที่มิจฉาชีพกำหนดเป้าหมายไปที่เหยื่อ และถือว่าวิธีการหลอกลวงทางโทรศัพท์เป็นวิธีที่ประสบความสำเร็จมากที่สุดในแง่ของจำนวนเงินที่สูญเสียไป จากรายงาน Targeting Scams report ในปี 2020[77] ของหน่วยงาน Australian Competition and Consumer Commission หรือในภาษาไทยเรียกว่า คณะกรรมาธิการด้านการแข่งขันและผู้บริโภคแห่งออสเตรเลีย ซึ่งมีหน้าที่รับผิดชอบการรับรองผู้ให้บริการและบังคับใช้กฎ CDR (สิทธิในข้อมูลผู้บริโภค) พบว่าจำนวนตัวเลข

[77] Australian Competition and Consumer Commission, Targeting Scams report 2020, June 2021, P.20

ความสูญเสียจากการหลอกลวงทางโทรศัพท์ปี 2020 ในช่วงของการระบาดโควิด-19 ประกอบกระแสของคริปโทเคอเรนซี่ที่อยู่ในช่วงขาขึ้น ณ เวลานั้น ทำให้พบว่าการหลอกลวงทางโทรศัพท์เพิ่มขึ้น 48% เมื่อเทียบกับปี 2019 และมีการสูญเสียจากการหลอกลวงทางโทรศัพท์เพิ่มขึ้นเป็นมากกว่า 48 ล้านดอลลาร์ โดยวิธียอดฮิตของเหล่ามิจฉาชีพที่ใช้ในการหลอกลวงเหยื่อ 3 อันดับแรก คือ โทรศัพท์ อีเมล และข้อความ ซึ่งเป็นวิธีการติดต่อ 3 อันดับแรกที่มิจฉาชีพใช้หลอกลวงและติดต่อกับประชาชนในปี 2020

อย่างไรก็ตาม แม้ว่าออสเตรเลียจะเผชิญปัญหาแก๊งคอลเซ็นเตอร์ออนไลน์ไม่ต่างกับประเทศไทย แต่จากที่ผู้วิจัยได้ทำการค้นคว้าพบว่าออสเตรเลียมีการจัดทำแผนปฏิบัติการ (Action Plan) ที่เป็นรูปธรรมและมีแนวทางในการป้องกันที่มาจากความร่วมมือของภาครัฐและเอกชนซึ่งแนวทางดังกล่าวสามารถลดปัญหาของตัวเลขการสูญเสียได้อย่างมีนัยสำคัญแม้ว่าจำนวนคอลเซ็นเตอร์ที่โทรเข้ามาป่วนจะยังมีอยู่เรื่อยๆและมีแนวโน้มที่จะมากขึ้นก็ตาม ดังนั้นผู้วิจัยจึงขอนำแนวทางการป้องกันของประเทศออสเตรเลียมาศึกษาเพื่อที่จะสามารถนำมาปรับใช้กับประเทศไทยได้ต่อไป

4.1.1.1 หน่วยงานที่มีส่วนเกี่ยวข้องจากภาครัฐ

หน่วยงานภาครัฐที่มีส่วนเกี่ยวข้องและมีหน้าที่ความรับผิดชอบโดยตรงเกี่ยวกับปัญหาแก๊งคอลเซ็นเตอร์ออนไลน์ ทางผู้วิจัยขอทำการกล่าวถึงเฉพาะหน่วยงานที่มีความรับผิดชอบหลัก ดังต่อไปนี้

1. ACMA (Australian Communication and Media Authority)[78] เป็นองค์กรภาครัฐที่กำกับดูแลกิจการแพร่ภาพกระจายเสียง อินเทอร์เน็ต วิทยุ สื่อสาร และโทรคมนาคม รวมไปถึงมีหน้าที่ควบคุมการสื่อสารและบริการสื่อในออสเตรเลียและเป็นผู้พิจารณาเงื่อนไขใบอนุญาต (license conditions) การประกอบการกิจการแพร่ภาพกระจายเสียงประเภท ต่างๆ ตามที่ได้อำนาจในพระราชบัญญัติการให้บริการแพร่ภาพกระจายเสียง พ.ศ. 2535 (the Broadcasting Services Act 1992 หรือเรียกสั้นๆ ว่า BSA)

[78] ชนัญสรา อรนพ ณ อยุธยา และ พิมลพรรณ ไชยนันท์, "โครงการพัฒนาและส่งเสริมแนวทางการกำกับดูแลกันเองขององค์กรวิชาชีพ ด้านกิจการกระจายเสียงและกิจการโทรทัศน์", (ศูนย์ศึกษานโยบายสื่อ คณะนิเทศศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย,2559) หน้า 23

ซึ่งถ้าเปรียบเทียบในประเทศไทยคือ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) นอกจากนี้ ACMA ได้กำหนดให้มีการควบคุมระบบการซื้อขายสินค้าและบริการผ่านระบบโทรศัพท์ ซึ่งจะต้องได้รับการยินยอมจากผู้รับเท่านั้น จึงจะมีสิทธิส่งข้อความและหากไม่ทำตามข้อกำหนดผู้บริโภคมีสิทธิที่จะร้องเรียนมาที่ ACMA ได้ทันที ซึ่งทางผู้วิจัยมองว่าข้อกำหนดเหล่านี้ยังไม่มีความชัดเจนในประเทศไทย โดยบทบาทหลักของ ACMA คือเมื่อมีคำสั่งมาจากรัฐมนตรี ACMA ต้องมีหน้าที่ในการกำหนดมาตรฐานอุตสาหกรรมโดยต้องบังคับใช้กับผู้ให้บริการโทรคมนาคมและมีหน้าที่จัดการกับที่เกี่ยวข้องกับกิจกรรมโทรคมนาคมเหล่านั้น[79]

2. ACCC (Australian Competition and Consumer Commission) คือ คณะกรรมการด้านการแข่งขันและผู้บริโภคแห่งออสเตรเลียซึ่งเป็นหน่วยงานของรัฐที่ทำหน้าที่ให้ความคุ้มครองผู้บริโภคโดยเฉพาะ มีหน้าที่สืบสวนสอบสวนคำร้องเรียนของผู้บริโภคซึ่งเกี่ยวข้องกับผู้บริโภคส่วนรวม หลังจากได้รับเรื่องร้องเรียนแล้ว กรณีที่เป็นปัญหาเล็กน้อย ACCC มีอำนาจสั่งให้ผู้ผลิตหรือผู้ขายกระทำการอย่างใดอย่างหนึ่ง นอกจากนี้ยังมีอำนาจให้ผู้ผลิตกระทำการหรือไม่กระทำการอย่างใดได้โดยไม่ต้องขออำนาจจากศาลและมีอำนาจสั่งลงโทษปรับผู้ผลิตได้ โดยหน่วยงานนี้สามารถเปรียบได้กับประเทศไทยคือ สำนักงานคณะกรรมการคุ้มครองผู้บริโภคของประเทศไทย[80]

---

[79] The Telecommunication Act 1997, subsection 125AA (1)

[80] รังสรรค์ โรจน์ชีวิน, มนตรี จิตร์วิวัฒน์, ดิลก เสริมวิริยะกุล, สมชาติ เลิศลิขิตวรกุล, ชัชวาล วิบุลสันติ และหฤทัย ประพุทธนิติสาร, “กฎหมายคุ้มครองผู้บริโภค และการดำเนินคดีคุ้มครองผู้บริโภค ประเทศออสเตรเลีย ศึกษาเกี่ยวกับกรณี การกระทำในทางการค้าทำให้ผู้บริโภคเกิดความเข้าใจผิด หรือหลอกลวงผู้บริโภคทางการค้า การเอาเปรียบผู้บริโภคที่มีความด้อยหรือความเสียเปรียบในทางการค้า หลักประกันผู้บริโภค การเยียวยาและอำนาจการบังคับใช้ของ ACCC การพิจารณาคดีผู้บริโภคโดยช่องทางพิเศษ การนำอิเล็กทรอนิกส์และเทคโนโลยีมาใช้ในการดำเนินกระบวนพิจารณาคดีของศาล”, การฝึกอบรมหลักสูตร “กฎหมายเกี่ยวกับวิธีพิจารณาความแพ่งชั้นสูง” ณ มหาวิทยาลัยนิวเซาท์เวลส์ ประเทศออสเตรเลีย, สำนักการต่างประเทศ

3. ACSC (Australian Cyber Security Centre) คือศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติของออสเตรเลีย เป็นหน่วยงานของรัฐบาล โดยมีหน้าที่คือ รักษาความปลอดภัยในโลกไซเบอร์ให้กับประชาชนและเป็นผู้นำในการตอบสนองต่อการดำเนินงานของรัฐบาลออสเตรเลียต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ จัดทำระเบียบการดำเนินงานและทรัพยากรด้านความปลอดภัยทางไซเบอร์แห่งชาติ ศึกษาและตรวจสอบภัยคุกคามทางไซเบอร์[81]
4. Scamwatch คือ หน่วยงานเฉพาะที่จัดตั้งขึ้นมาใหม่และอยู่ภายใต้การกำกับดูแลของ The ACCC (Australian Competition and Consumer Commission) ซึ่งเป็นหน่วยงานของรัฐที่ทำหน้าที่ให้ข้อมูลแก่ประชาชนในเรื่องการหลอกลวงทุกรูปแบบและแนะนำวิธีหลีกเลี่ยงเพื่อป้องกันตนเองจากการตกเป็นเหยื่อ ภารกิจหลักของ Scamwatch คือการเผยแพร่เอกสาร ข้อเท็จจริง รายงานประจำปีเกี่ยวกับรูปแบบการหลอกลวงเพื่อให้ประชาชนได้รับรู้อย่างทันท่วงที และสามารถให้ประชาชนแจ้งหรือรายงานการหลอกลวงได้ผ่านทางเว็บไซต์ https://www.scamwatch.gov.au/ [82]

4.1.1.2 ความร่วมมือจากภาคเอกชน

ในปัจจุบัน หน่วยงานรัฐบาลของประเทศออสเตรเลียได้พยายามขอความร่วมมือจากภาคเอกชน ซึ่งส่วนใหญ่จะเป็นผู้ประกอบกิจการเครือข่ายโทรศัพท์รายต่างๆ โดยให้เข้ามามีส่วนร่วมในการวางแผนวิธีการป้องกันไม่ให้ประชาชนตกเป็นเหยื่อ โดยมีการจัดตั้ง Communications Alliance (CA) หรือที่เรียกว่า พันธมิตรทางการสื่อสาร ซึ่งเป็นการรวมตัวของผู้ให้บริการโทรคมนาคมในประเทศออสเตรเลียเพื่อร่วมกันจัดทำ Code of Conduct ด้านการคุ้มครองผู้บริโภค ซึ่งเป็นส่วนหนึ่งของการกำกับดูแลกันเอง (self-regulation)

---

[81] ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักข่าวกรองแห่งชาติ, ออสเตรเลียเริ่มปิดกั้นข้อความหลอกลวงที่อ้างว่ามาจากหน่วยงานของรัฐบาล, [ออนไลน์], 2564, แหล่งที่มา https://www.nia.go.th/cyber/cyberpage/588/ [13 พฤศจิกายน 2565]

[82] โสภิดา วีรกุลเทวัญ, แนวทางการจัดการกับปัญหาการส่งข้อความสั้นหรือโทรศัพท์ที่ไม่พึง ประสงค์ (spam) และหลอกลวง (scam) ต่อผู้บริโภคในต่างประเทศ , หน้า 2

4.1.2 ประเทศสหราชอาณาจักร

จากการศึกษาแนวทางในการป้องกันแก๊งคอลเซ็นเตอร์ของประเทศสหราชอาณาจักรพบว่า สหราชอาณาจักรได้เผชิญกับปัญหาการหลอกลวงของแก๊งคอลเซ็นเตอร์มานานโดยมีรูปแบบ เช่น การหลอกลวงโดนผ่านการตลาดของการขายสินค้า เป็นต้น ซึ่งสร้างความรำคาญและความสูญเสียกับประชาชนอย่างต่อเนื่อง จึงทำให้ปี 2013 หน่วยงานภาครัฐได้ทำการจัดทำแผนปฏิบัติอย่างเป็นรูปธรรมในการวางแผนการป้องกันเพื่อจัดการกับอันตรายต่อผู้บริโภคที่เกิดจากการโทรและข้อความหลอกลวงดังกล่าว โดยแผนที่จัดทำคือ Nuisance calls and messages Update to ICO - Ofcom joint action plan ซึ่งมีการจัดทำเป็นประจำทุกปีตั้งแต่ปี 2013 จนถึงปัจจุบัน[83] ดังนั้นผู้วิจัยจึงขอนำแนวทางการป้องกันของประเทศสหราชอาณาจักรมาศึกษาเพิ่มเติมเพื่อที่จะสามารถนำมาปรับใช้กับประเทศไทยได้ต่อไป

4.1.2.1 หน่วยงานที่มีส่วนเกี่ยวข้องจากภาครัฐ

หน่วยงานภาครัฐที่มีส่วนเกี่ยวข้องและมีหน้าที่ความรับผิดชอบโดยตรงเกี่ยวกับปัญหาแก๊งคอลเซ็นเตอร์ออนไลน์ ทางผู้วิจัยขอทำการกล่าวถึงเฉพาะหน่วยงานที่มีความรับผิดชอบหลัก ดังต่อไปนี้

1. Ofcom (Office of Communications) เป็นหน่วยงานอิสระภายใต้การกำกับดูแลของรัฐบาล โดยอาศัยอำนาจของพระราชบัญญัติการสื่อสาร ค.ศ. 2003 (The Communication Act 2003) ซึ่งจะสังเกตได้ว่ามีลักษณะเหมือนกับ กสทช ในประเทศไทย และ ACMA ในประเทศออสเตรเลียโดย Ofcom ทำหน้าที่กำกับดูแลกิจการสื่อสารของสหราชอาณาจักรที่ประกอบด้วยกิจการโทรทัศน์ กิจการวิทยุรวมไปถึงกิจการโทรคมนาคมระบบสาย กิจการโทรคมนาคมเคลื่อนที่และกิจการไปรษณีย์ โดยในปี 2017 และ 2018 ทาง Ofcom ได้ทำการออกกลยุทธ์ในด้านต่างๆที่ครอบคลุมถึงการปกป้องคุ้มครองผู้บริโภคซึ่งจะถูกกำหนดเป็นยุทธศาสตร์ด้วย โดยการปกป้องคุ้มครองจะเน้น

[83] Ofcom, Tackling nuisance calls and messages, [Online], 2021, Source https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/tackling-nuisance-calls-messages [2022, December 21]

การคุ้มครองผู้บริโภคจากภัยคุกคามรูปแบบต่างๆ ซึ่งรวมไปถึงการแก้ไขปัญหาเกี่ยวกับการรบกวนทางโทรศัพท์ด้วยการร่วมติดตาม ตรวจสอบ และป้องกันปัญหาการรบกวนทางโทรศัพท์กับผู้ให้บริการและหน่วยงานที่เกี่ยวข้อง[84]

2. ICO (The Information Commissioner's Office) หรือแปลเป็นไทยได้ว่า สำนักงานคณะกรรมาธิการด้านข้อมูลข่าวสาร เป็นองค์กรผู้ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ และเป็นผู้นำในการจัดการกับการโทรขายทางโทรศัพท์ที่สร้างความรำคาญให้กับประชาชน รวมไปถึงสายการโทรเข้าด้วยข้อความการตลาดอัตโนมัติและข้อความการหลอกลวงต่างๆ นอกจากนี้ยังมีความรับผิดชอบในการรักษารายชื่อหมายเลขโทรศัพท์ของบุคคลและธุรกิจที่ต้องการยกเลิกการรับสายการตลาดสดที่ไม่พึงประสงค์หรือแฟกซ์การตลาดที่ไม่พึงประสงค์
3. Action Fraud เป็นศูนย์ที่รับรายงานการฉ้อโกงและอาชญากรรมไซเบอร์เป็นการเฉพาะ เนื่องด้วยการติดตามสถานการณ์ที่ส่งผลกระทบแก่ผู้บริโภคอย่างใกล้ชิดที่ถูกจัดตั้งเมื่อปี 2005 ซึ่งการฉ้อโกงและอาชญากรรมกรรมเทคโนโลยีต่างๆที่เกิดขึ้นในดินแดนของสหราชอาณาจักรจะถูกรายงานไปยัง Action Fraud จากนั้นรายงานเหล่านี้จะได้รับการวิเคราะห์โดย National Fraud Intelligence Bureau (NFIB)[85] ซึ่งประชาชนสามารถรายงานการถูกหลอกลวงได้ที่ https://www.actionfraud.police.uk/ โดยภายในเว็บไซต์จะมีการให้ข้อมูลแก่ประชาชนในเรื่องการหลอกลวงทุกรูปแบบและแนะนำวิธีหลีกเลี่ยงเพื่อป้องกันตนเองจากการตกเป็นเหยื่อ

4.1.2.2 ความร่วมมือจากเอกชน

แม้ว่าประเทศสหราชอาณาจักรจะมีการทำแผนปฏิบัติการอย่างเป็นรูปธรรมในปี 2013 แต่การที่ภาครัฐได้ทำความร่วมมือกับภาคเอกชนเกิดขึ้นเมื่อใน

---

[84] จิตสุภา ฤทธิผลิน, “ทิศทางและนโยบายการกำกับดูแลกิจการกระจายเสียง และกิจการโทรทัศน์ในยุคของการหลอมรวมสื่อ : กรณีศึกษาเปรียบเทียบยุทธศาสตร์ ของ FCC และ OFCOM,” (วิทยานิพนธ์ของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ,2560), หน้า 253

[85] โชคสุข กรกิตติชัย, “สหราชอาณาจักรบริเตนใหญ่และไอร์แลนด์เหนือ กับการป้องกันและปราบปรามการทุจริต,” เอกสารวิชาการอิเล็กทรอนิกส์ สำนักวิชาการ สำนักงานเลขาธิการสภาผู้แทนราษฎร (สิงหาคม 2565) หน้า 13

ปี 2018 เมื่อทาง Ofcom ได้มีการดำเนินการบังคับใช้ตามเป้าหมายที่วางไว้ ไม่ว่าจะเป็นการทำงานร่วมกับผู้ให้บริการโทรคมนาคมเพื่อป้องกันการโทรหลอกลวงที่รบกวนประชาชน การแบ่งปันข้อมูลระหว่างกันซึ่งรวมไปถึงพันธมิตรระหว่างประเทศของสหราชอาณาจักรเพื่อที่จะจัดการกับการหลอกลวงดังกล่าวโดยหน่วยงานที่บังคับใช้กฎหมายด้วยความรับผิดชอบในการจัดการกับการหลอกลวงและการฉ้อโกง และการทำงานร่วมกันระหว่างหน่วยงานกำกับดูแลและหน่วยงานอื่นๆ เพื่อยับยั้งและลงโทษองค์กรหรือบุคคลที่กระทำความผิดจากการโทรและส่งข้อความที่ก่อกวน[86] นอกจากนี้ยังมีการร่วมมือซึ่งอาศัยความสมัครใจของแต่ละภาคส่วนเข้ามาร่วมกันหาแนวทางป้องกันรวมไปถึงทำการจัดตั้งหน่วยงานเฉพาะส่วนขึ้นมา นั่นคือ หน่วยงาน Stop Scams UK

Stop Scams UK เป็นหน่วยงานที่ภาคเอกชนจัดตั้งขึ้นโดยมีลักษณะไม่แสวงหาผลกำไร แต่เพื่อเป็นการทำงานร่วมกันโดยนำผู้นำในอุตสาหกรรมของธุรกิจที่มีความรับผิดชอบจากทั่วทั้งภาคการธนาคาร โทรคมนาคม และเทคโนโลยี เช่น ธนาคารHSBC ผู้นำเทคโนโลยีGoogle Microsoft ผู้ให้บริการโทรคมนาคม KCOM เป็นต้น มารวมตัวกันเพื่อช่วยหยุดการหลอกลวงที่ต้นทาง ซึ่ง Stop Scams UK ได้ทำการก่อตั้งขึ้นเมื่อปี 2020 และปัจจุบันมีสมาชิกอยู่ 18 หน่วยงาน โดยจุดประสงค์หลักของการก่อตั้งคืออำนวยความสะดวกในการพัฒนาและหาทางป้องกันในทางเทคนิคที่จะช่วยป้องกันอันตรายและความสูญเสียที่เกิดจากการหลอกลวงดังนั้นการหลอกลวงเกือบทั้งหมดที่เกี่ยวข้องกับภาคการธนาคาร เทคโนโลยี และโทรคมนาคมตั้งแต่สองแห่งขึ้นไป Stop Scams UK จะนำธุรกิจจากภาคส่วนสำคัญทั้งสามส่วนนี้มารวมกันเพื่อสร้างแนวทางการแก้ปัญหาแบบองค์รวมและรวมไปถึงการพัฒนาระบบที่จำเป็นในการดักจับความผิดปกติที่อาจจะเกิดจากการหลอกลวงได้[87]

---

[86] The Information Commissioner's Office (ICO) and Ofcom Nuisance calls and messages, Update to ICO-Ofcom joint action plan 2019, 7 March 2019

[87] Stop Scams UK, WORKING TOGETHER TO STOP SCAMS AT SOURCE, [Online], 2022, Source https://stopscamsuk.org.uk/about-stop-scams-uk [2022, December 10]

4.2 แผนปฏิบัติการเชิงรุกและนโยบายที่ใช้โดยอาศัยความร่วมมือจากภาครัฐและเอกชน

จากการศึกษาพบว่า ไม่ว่าจะเป็นประเทศออสเตรเลียหรือประเทศสหราชอาณาจักรทั้ง 2 ประเทศจะเน้นการออกมาตรการป้องกันแก๊งคอลเซ็นเตอร์ตั้งแต่ต้นทางมากกว่ามาตรการการปราบปราม ดังนั้นจะเห็นได้ว่าทั้ง 2 ประเทศจะมีการจัดทำแผนปฏิบัติการที่เป็นรูปธรรมเพื่อนำมาเป็นแนวทางในการปฏิบัติของผู้ให้บริการโทรคมนาคมและหน่วยงานที่เกี่ยวข้อง

4.2.1 ประเทศออสเตรเลีย

เนื่องจากประเทศออสเตรเลียเป็นประเทศที่เผชิญกับปัญหาของแก๊งคอลเซ็นเตอร์ ซึ่งทางรัฐบาลของออสเตรเลียได้มองเห็นถึงปัญหาดังกล่าวว่ามีผลกระทบทางสังคมและเศรษฐกิจที่สำคัญต่อชาวออสเตรเลียโดยขนาดและผลกระทบของแก๊งคอลเซ็นเตอร์ได้เพิ่มขึ้นเรื่อยๆ ทำให้ประชาชนคาดหวังให้ทางภาครัฐดำเนินการหรือหาทางในการป้องกันไม่ว่าทางใดก็ทางหนึ่ง โดยที่ภาครัฐของออสเตรเลียได้มีแนวคิดว่าการหาแนวทางป้องกันไม่ให้เกิดย่อมดีกว่าการที่เกิดขึ้นแล้วและมาตามจับกุมทีหลัง แนวคิดนี้จึงทำให้ภาครัฐได้ออกแผนปฏิบัติการ (Action plan) ต่างๆในการป้องกันประชาชนจากการถูกหลอกลวงของคอลเซ็นเตอร์

ในปี 2018 ACMA (Australian Communication and Media Authority) ได้จัดทำโปรเจคที่ชื่อว่า “Scam Technology Project”[88] เป็นโปรเจคในการสำรวจวิธีแก้ปัญหาเพื่อจัดการกับการโทรศัพท์หลอกลวงประชาชนบนเครือข่ายโทรคมนาคมของออสเตรเลียประกอบกับทางภาครัฐจะพิจารณาถึงสิ่งที่สามารถทำได้เพื่อขัดขวางกิจกรรมการหลอกลวงทางโทรศัพท์ของแก๊งคอลเซ็นเตอร์ โดยในโปรเจคนี้ ACMA มุ่งเน้นการร่วมมือกันระหว่างภาครัฐและภาคเอกชน ได้แก่ ACCC (Australian Competition and Consumer Commission) และ ACSC (Australian Cyber Security Centre) ซึ่งเป็นผู้เชี่ยวชาญในอุตสาหกรรมด้านโทรคมนาคม รัฐบาล หน่วยงานกำกับดูแลในต่างประเทศ รวมไปถึงผู้ให้บริการโทรคมนาคมของประเทศออสเตรเลีย เพื่อช่วยให้โปรเจคนี้บรรลุเป้าหมาย

---

[88] Australian Competition and Consumer Commission, Targeting Scam Report of the ACCC on scams activity 2020, June 2021

The Combating Scams Action Plan[89] เกิดขึ้นเมื่อปี 2019 หลังจากที่ ACMA ได้ริเริ่ม Scam Technology Project โดยในแผนปฏิบัติการจะเน้นการป้องกันการหลอกลวงทางโทรศัพท์และได้มีจุดประสงค์หลักของการจัดทำแผนปฏิบัติการคือ ลดปริมาณการหลอกลวงของคอลเซ็นเตอร์ทุกรูปแบบรวมไปถึง Wangiri scam[90] ซึ่งเป็นหนึ่งในรูปแบบมิจฉาชีพทางโทรศัพท์ที่กำลังแพร่ระบาดโดยมีลักษณะคือ มิจฉาชีพมักใช้หมายเลขต่างประเทศโทรเข้ามาและวางสายหลังจากการที่หมายเลขปลายทางดังครั้งที่หนึ่ง ถ้าเหยื่อโทรกลับจะส่งผลให้มีค่าบริการพิเศษสำหรับผู้โทรและผู้หลอกลวงจะพยายามให้ผู้โทรอยู่ในโทรศัพท์ให้นานที่สุด เช่น มีการเล่นเพลงค้างไว้หรือมีเสียงอัตโนมัติพูดเชิญชวนให้เหยื่อฟัง เป็นต้น นอกจากนี้แผนปฏิบัติการดังกล่าวมีจุดประสงค์เพื่อนำเสนอ 3 ประเด็นหลักในการลดอัตราการหลอกลวงทางโทรศัพท์โดยอาศัยความร่วมมือระหว่างผู้มีส่วนได้ส่วนเสีย คืออุตสาหกรรมโทรคมนาคม (ผู้ให้บริการโทรคมนาคม)และหน่วยงานภาครัฐบาลได้ทำงานร่วมกันเพื่อดำเนินการให้บรรลุเสร็จสิ้นในปี 2020

[89] Australian Competition and Consumer Commission, Targeting Scam Report of the ACCC on scams activity 2020, June 2021

[90] พี่กวาง, เตือนภัย! "Wangiri Fraud" มิจฉาชีพแนวใหม่ Missed Call ให้เราเสียเงิน!, [ออนไลน์], 2561, แหล่งที่มา https://www.dek-d.com/teentrends/49294/ [11 พฤศจิกายน 2565]

รูปภาพที่ 8[91] What is Wangiri Fraud and how does it impact telecom operators?

แม้ว่าแผนปฏิบัติการนี้จะเน้นการหาทางออกให้กับผู้ประกอบการอุตสาหกรรมโทรคมนาคม แต่การหาทางออกมักจะไม่มีประสิทธิภาพเท่าที่ควรถ้าปราศจากการร่วมมือของทางภาครัฐที่จะช่วยทำการส่งเสริม แบ่งปันข้อมูลระหว่างอุตสาหกรรมโทรคมนาคม ต่างอุตสาหกรรมรวมไปถึงรัฐบาล ซึ่งทางรัฐบาลจะต้องทำการสนับสนุนการประสานงานเชิงกลยุทธ์เพื่อที่จะทำให้การรับรู้ของผู้บริโภคดีขึ้นและการบังคับใช้กฎระเบียบเป็นไปตามแผนที่วางไว้ นอกจากนี้เพื่อที่จะให้บรรลุแผนปฏิบัติการนี้ ผู้ให้บริการโทรคมนาคมจำเป็นต้องดำเนินการตามกฎระเบียบใหม่ๆที่จะเกิดขึ้นเพื่อดำเนินการป้องกันหมายเลยโทรศัพท์ที่ทำการหลอกลวง โดยภาระผูกพันที่บังคับใช้โดย ACMA ส่วนใหญ่จะเกี่ยวกับการรับรองการใช้รหัสสายเรียกเข้า (CLI) ที่ถูกต้องตามกฎหมาย โดย ACMA ได้ทำการเสนอแผนปฏิบัติการ 3 แผน[92] หลักเพื่อให้เป็นไปตามวัตถุประสงค์ต่อการจัดตั้งของโครงการ ได้แก่ แผนที่1 คือ การจัดตั้งคณะทำงานเฉพาะกิจระหว่างรัฐบาลและอุตสาหกรรมโทรคมนาคม แผนที่2 คือ

[91] Nithin Gangadharan, What is Wangiri Fraud and how does it impact telecom operators?, [Online], 2019, Source: https://www.subex.com/blog/What-is-wangiri-fraud-how-does-it-impact-for-telecom-operators/ [2022, November 13]

[92] Australian Communication and Media Authority, Combating scams Action plan summary, November 2019, Page 7

การพัฒนาภาระผูกพันที่บังคับใช้ใหม่สำหรับผู้ให้บริการโทรคมนาคมและแผนที่3 คือ การริเริ่มดำเนินโครงการลดการหลอกลวงโดยอาศัยเทคโนโลยีต่างๆ

แผนปฏิบัติการ 1 คือ จัดตั้งคณะทำงานเฉพาะกิจด้านการดำเนินการหลอกลวงโดยใช้การโทรศัพท์เป็นเครื่องมือและจัดให้มีการประสานงานระหว่างรัฐบาลและอุตสาหกรรมผู้ให้บริการโทรคมนาคมในการร่วมมือกันกำกับดูแลด้านกลยุทธ์ต่างๆในการลดการหลอกลวงทางโทรคมนาคม รวมไปถึงการวิเคราะห์ความคิดเห็นของฝ่ายต่างๆเพื่อพิจารณาประกอบกับบริบทภายในประเทศและหาแนวทางระหว่างประเทศเพื่อขัดขวางการขบวนการหลอกลวง โดยมี ACMA ซึ่งได้รับอำนาจจาก the Broadcasting Services Act 1992 และ พระราชบัญญัติ the Telecommunications Act 1997 เป็นหน่วยงานหลักในการดูแลแผนปฏิบัติการนี้ซึ่งจากการวิเคราะห์ของ ACMA มีความเห็นว่า การร่วมมือกันและระหว่างภาครัฐและเอกชนเป็นปัจจัยสำคัญที่ช่วยส่งเสริมกิจกรรมและทำให้เกิดการลดลงของการหลอกลวงโดยมิจฉาชีพ การที่ภาครัฐของทางออสเตรเลียจัดให้มีแผนนี้ขึ้นมาเนื่องจากเห็นว่า ปี 2015 ในสหราชอาณาจักร (UK) มีหน่วยงานกำกับดูแลด้านโทรคมนาคม (Ofcom) ได้จัดตั้งคณะทำงานเชิงกลยุทธ์เพื่อจัดการกับความรำคาญและการหลอกลวงทางโทรศัพท์โดยได้อาศัยความร่วมมือกับกลุ่มผู้ให้บริการโทรคมนาคมรายใหญ่ 9 ราย และได้ดำเนินการตามแผนริเริ่มในการลดการหลอกลวงที่ประสบความสำเร็จหลายประการตั้งแต่นั้นมา[93]

ดังนั้น แผนปฏิบัติการนี้จึงเป็นการแนะนำให้จัดตั้งคณะทำงานด้านการป้องกันและกำกับดูแลที่นำโดย ACMA ซึ่งประกอบด้วยตัวแทนจากอุตสาหกรรมโทรคมนาคมและหน่วยงานรัฐบาลที่เกี่ยวข้อง พร้อมด้วยผู้สังเกตการณ์จากภาคส่วนอื่นๆ เพื่อเป็นทำการดำเนินการจัดตั้งคณะทำงานเฉพาะกิจทันที

แผนปฏิบัติการ 2 คือ พัฒนาการบังคับใช้ข้อตกลงสำหรับผู้ให้บริการโทรคมนาคมเพื่อให้ง่ายต่อการตรวจจับ ติดตาม ปิดกั้นการใช้งาน และขัดขวางมิจฉาชีพ โดยแผนปฏิบัติการนี้อาศัยอำนาจของหน่วยงาน ACMA ให้ผู้ให้บริการโทรคมนาคมเป็นหน่วยงานหลักในการดำเนินการเพื่อที่จะ

(ก) แชร์ข้อมูลเบอร์โทรศัพท์ของมิจฉาชีพภายในกลุ่มอุตสาหกรรมบริษัทผู้ให้บริการเครือข่ายด้วยกันเองโดยไม่ผิดกฎหมาย หลังจากที่ทางภาครัฐได้มีการบังคับใช้ข้อตกลงกับผู้ให้บริการโทรคมนาคมพบว่าการแชร์ข้อมูลเบอร์โทรศัพท์ของมิจฉาชีพส่งผลให้

[93] Ofcom, Nuisance calls and messages - Update to ICO-Ofcom joint action plan, 2019, viewed 23 August 2019.

หน่วยงานรัฐบาลและหน่วยงานบังคับใช้กฎหมายหลายแห่งได้รับรายงานกิจกรรมการหลอกลวงของแก๊งคอลเซ็นเตอร์เพิ่มมากขึ้นซึ่งการแบ่งปันข้อมูลรายงานการหลอกลวงในวงกว้างจะช่วยให้ผู้ให้บริการโทรคมนาคมสามารถปรับปรุงการระบุและทำการปิดกั้นการใช้งานเบอร์โทรศัพท์ได้อย่างทันท่วงทีและมากยิ่งขึ้น[94] โดยบริษัท Telstra ซึ่งเป็นบริษัทโทรคมนาคมของออสเตรเลียที่ให้บริการเครือข่ายโทรคมนาคม อินเทอร์เน็ตรวมไปถึงกิจการโทรทัศน์ ได้เปิดเผยว่า หลังจากที่เริ่มมีการแชร์ข้อมูลเบอร์โทรศัพท์ของมิจฉาชีพสามารถทำการระบุเบอร์โทรที่ทำการหลอกลวงมากกว่า 2.9 ล้านครั้งและปิดกั้นการใช้งานได้สำเร็จในเดือนกรกฎาคม 2019[95]

(ข) ป้องกันการโทรเข้าจากต้นทางในประเทศที่ผู้โทรไม่มีสิทธิ์ในการใช้หมายเลขและลดปริมาณสายของการโทรเข้าโดยใช้เบอร์ต่างประเทศโดยให้ผู้ให้บริการโทรคมนาคมสามารถระบุสายการโทรเข้านั้นเป็นเบอร์ที่ผิดกฎหมาย เช่น การปิดกั้นการใช้งาน Wangiri scam ที่มีต้นทางมาจากจากเครือข่ายทั่วโลก

(ค) จัดให้มีการใช้และอัพเดตเทคโนโลยีการกรอง SMS

(ง) จัดให้มีการให้คำแนะนำและให้ข้อมูลแก่ลูกค้า

(จ) เผยแพร่และประชาสัมพันธ์ตามช่องทางโซเชียลมีเดียต่างๆ ได้แก่ เฟซบุ๊ก ทวิตเตอร์ อินสตราแกรมโดยให้ประชาชนเข้าถึงและสามารถศึกษาลักษณะการหลอกลวงทางโทรศัพท์ในรูปแบบต่างๆเพื่อสร้างความตระหนักรู้และวิธีการจัดการเมื่อตนเองตกเป็นเหยื่อ โดยสามารถดาวน์โหลดไฟล์รูปภาพได้จากเว็บไซต์ของ ACMA และสามารถนำไปใช้ประชาสัมพันธ์ต่อได้

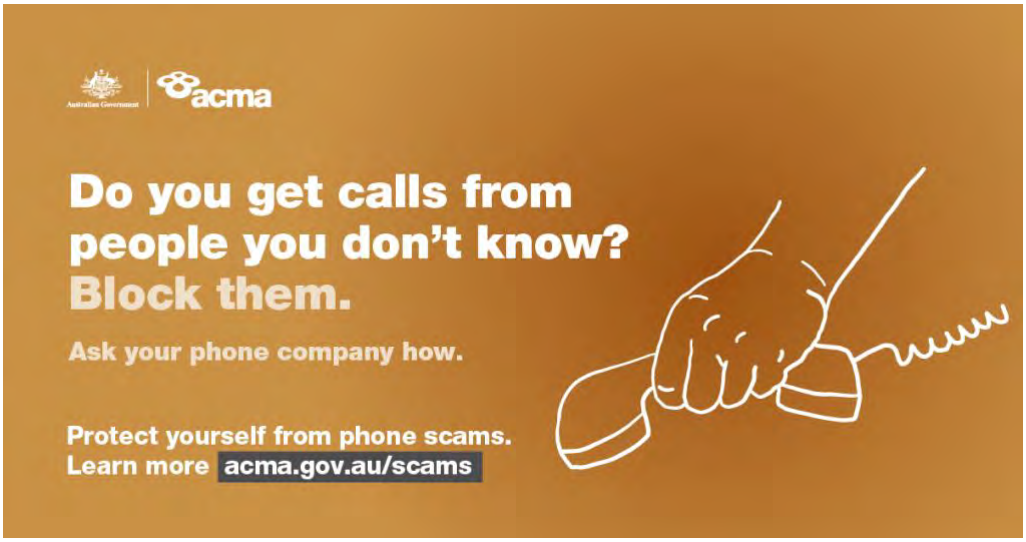
(ฉ) เตรียมการสร้างความตระหนักรู้ของประชาชนและการคุ้มครองข้อมูลจะถูกพิจารณาภายใต้ทิศทางของ the Telecommunications (Industry Standard for Mobile Number Pre- Porting Additional Identity Verification) Direction 2019 ที่กำหนดให้ ACMA กำหนดมาตรฐานอุตสาหกรรมเพื่อใช้มาตรการยืนยันตัวตนก่อนการ

[94] Australian Communication and Media Authority, Combating scams Action plan summary, November 2019

[95] Andrew Penn, Tackling the changing face of our customer, [Online], 2019, Source : https://www.linkedin.com/pulse/tackling-changing-face-our-customer-andrew-penn/ [2022, November 13]

โอนย้ายผู้ให้บริการโทรศัพท์เคลื่อนที่ของผู้ใช้บริการโทรศัพท์ให้ได้รับการปรับปรุงอย่างเหมาะสมที่สุด

รูปภาพที่ 9 ตัวอย่างของโปสเตอร์รูปภาพตามเว็บไซต์ที่ได้อ้างอิงในเชิงอรรถที่44
Phone scam educational resources



แผนปฏิบัติการ 3 คือ การริเริ่มดำเนินโครงการลดการหลอกลวงโดยอาศัยเทคโนโลยีต่างๆ แผนปฏิบัติการนี้อยู่ในการดูแลของผู้ให้บริการโทรคมนาคมเป็นหลัก ซึ่งถือเป็นความร่วมมือของภาคเอกชนในการยับยั้งและป้องกัน โดยที่ ACMAจะทำงานร่วมกับภาคอุตสาหกรรมและผู้มีส่วนได้ส่วนเสียหลักเพื่ออำนวยความสะดวกในการทดลองและเพื่อหาวิธีในในการปรับใช้ตั้งแต่ระยะสั้นไปจนถึงระยะยาว ซึ่งแผนนี้ประกอบไปด้วย

(ก) มีการพัฒนาและทดลองใช้ “Do Not Originate List (DNO)” การระบุรายการ DNO ดังกล่าวอาจช่วยลดการนำชื่อเสียงของแบรนด์ที่น่าเชื่อถือมาใช้เพื่อกระทำการหลอกลวงและช่วยลดผลกระทบต่อบุคคลที่สาม การทดลองใช้ DNO เกิดขึ้นเนื่องจากบริษัทที่มีชื่อเสียงและมีความน่าเชื่อถือรวมไปถึง ATO (Australian Taxation Office) หรือในภาษาไทยเรียกว่ากรมสรรพกรออสเตรเลียซึ่งเป็นหน่วยงานของรัฐได้ตกเป็นเป้าหมายของการหลอกลวงโดยการใช้หมายเลขเบอร์โทรศัพท์ของหน่วยงานต่างๆปลอมแปลงเพื่อที่จะทำให้เหยื่อหลงเชื่อว่าหมายเลขที่โทรนั้นมาจากหน่วยงานจริงที่สามารถตรวจสอบได้และมีความน่าเชื่อถือโดย การทดลองใช้รายการ DNO นี้ ได้มีการสำรวจแนวทางแก้ปัญหากับผู้ให้

บริการเครือข่ายโทรศัพท์เพื่อที่จะทำการปิดกั้นการใช้งานเบอร์โทรที่ใช้หลอกลวงโดยใช้ CLI (Calling Line Identification or caller ID) ซึ่งสามารถตรวจสอบได้ว่ากำลังถูกใช้โดยมิจฉาชีพหรือไม่ เพื่อที่จะคืนความมั่นใจให้กับผู้บริโภคในการรับสายโทรศัพท์จากแบรนด์ที่เชื่อถือได้รวมไปถึงการทดสอบความเป็นไปได้ในอนาคตสำหรับการเปิดตัวในวงกว้างซึ่งรวมถึง SMEsและผู้บริโภคที่มีการใช้ตัวเลขดังกล่าว

(ข) สามารถระบุและปิดกั้นการใช้งาน Wangiri scam ได้ เนื่องจากลักษณะของ Wangiri ค่อนข้างมีลักษณะเฉพาะคือเป็นการโทรที่มีปริมาณมากและมีระยะเวลาสั้น ๆ ทำให้เหยื่อเกิดความสงสัยและเกิดการโทรกลับ ดังนั้นการหาทางแก้ไขปัญหาโดยการนำเทคโนโลยีมาใช้ในการระบุและปิดกั้นการใช้งานเบอร์โทรดังกล่าว

(ค) การปิดกั้นการรับส่งข้อมูล เนื่องจากปริมาณของเบอร์โทรศัพท์ที่ทำการหลอกลวงในออสเตรเลียมีจำนวนมากซึ่งส่วนใหญ่เบอร์โทรดังกล่าวมีต้นทางมาจากนอกประเทศออสเตรเลียและมีการสั่งการผ่านเว็บไซต์ที่ซับซ้อนของการกำหนดเส้นทางการโทรและการรับส่งข้อมูลตาม IP

ทั้ง 3 แผนปฏิบัติการนี้ ACMA ได้มีการอัพเดตความคืบหน้าของการวางแผนปฏิบัติการเป็นประจำทุกปีตามตารางที่ผู้วิจัยได้ทำการสรุปด้านล่างดังนี้

แผนปฏิบัติการ	**หน่วยงานที่ดูแล (หลัก)**	**สถานะงานและความคืบหน้า**
แผนปฏิบัติการ 1	ACMA	มีการประชุมของคณะทำงานที่จัดตั้งขึ้นจำนวน 3 ครั้งในปี 2020 และจะจัดให้มีการประชุมในปี 2021 และ 2022 อย่างต่อเนื่อง
แผนปฏิบัติการ 2	ผู้ให้บริการโทรคมนาคม และ ACMA	1.มีการเผยแพร่ข้อมูลให้ประชาชนสามารถศึกษาเกี่ยวกับรูปแบบการหลอกลวงทางโทรศัพท์เพื่อสร้างความตระหนักรู้ให้กับประชาชนและสามารถหาวิธีจัดการเมื่อตนตกเป็นเหยื่อได้อย่างทันท่วงที

		2.ก่อให้เกิด “Reducing Scams Call Industry Code” ซึ่งมีผลบังคับใช้ในปี 2020 โดยจะกล่าวในหัวข้อถัดไป
แผนปฏิบัติการ 3	ผู้ให้บริการโทรคมนาคม	ผู้ให้บริการโทรคมนาคมได้ทดลองริเริ่มดำเนินโครงการลดการหลอกลวงโดยอาศัยเทคโนโลยีต่างๆ และสามารถปิดกั้นการใช้งานหมายเลขโทรศัพท์ได้มากกว่า 30 ล้านครั้งในปี 2020

4.2.2 ประเทศสหราชอาณาจักร

จากการศึกษาแนวทางในการป้องกันแก๊งคอลเซ็นเตอร์ในส่วนของภาคอุตสาหกรรมโทรคมนาคมของประเทศสหราชอาณาจักรพบว่า สหราชอาณาจักรมีการจัดทำแผนปฏิบัติอย่างเป็นรูปธรรมในการวางแผนการป้องกันเพื่อจัดการกับอันตรายต่อผู้บริโภคที่เกิดจากการโทรและข้อความหลอกลวง โดยแผนที่จัดทำคือ Nuisance calls and messages Update to ICO - Ofcom joint action plan ซึ่งจัดทำครั้งแรกเมื่อปี 2013 และได้ทำการทบทวนและปรับปรุงแผนปฏิบัติการทุกปีเพื่อให้สอดคล้องกับบริบทหรือการกระทำของเหล่าอาชญากรรมที่เปลี่ยนแปลง โดยแผนปฏิบัติการดังกล่าวได้เกิดจาก ICO และ Ofcom ซึ่งหน่วยงาน ICO จะเป็นผู้นำในการแก้ปัญหาหมายเลขโทรศัพท์ที่ทำการโทรติดต่อเพื่อทำการตลาดในรูปแบบของไฟล์เสียงที่ได้มีการบันทึกไว้หรือที่เรียกว่าข้อความอัตโนมัติรวมไปถึงการเสนอขายแบบใช้พนักงานในการโฆษณาทางการตลาด และรวมถึงข้อความและอีเมลที่สร้างความรำคาญ โดย ICO มีหน้าที่ดำเนินการบังคับใช้กฎหมายกับองค์กรที่ละเมิดกฎที่เกี่ยวข้อง ในส่วนของ Ofcom เป็นผู้นำในดูแลหมายเลขโทรศัพท์ที่ได้ทำการเปิดหมายเลขแต่ไม่มีการใช้งาน ซึ่งสามารถสรุปได้ว่าแผนปฏิบัติการเน้นการทำงานร่วมกันระหว่าง ICO Ofcom บริษัทโทรคมนาคม และองค์กรอื่น ๆ โดยให้ความช่วยเหลือด้านการวิจัยและทางเทคนิคตลอดจนคำแนะนำแก่ผู้บริโภค

แผนปฏิบัติการฉบับล่าสุดที่ทาง Ofcom ได้ทำการเผยแพร่คือ Nuisance calls and messages Update to ICO / Ofcom joint action plan 2021 โดยภายในแผนปฏิบัติการล่าสุดนี้ได้มีการอัพเดตความคืบหน้าของแผนปฏิบัติการปีก่อนๆ ซึ่งผู้วิจัยจะขอทำการสรุปประเด็นที่เกี่ยวโยงกับเรื่องแก๊งคอลเซ็นเตอร์ ได้แก่

1. ดำเนินการตามเป้าหมายกับบุคคลหรือบริษัทที่ไม่ปฏิบัติตามกฎของ ICO ที่เน้นการก่อก่วนของการโฆษณาการตลาดผ่านการโทรศัพท์และข้อความรวมไปถึงหมายเลขที่ได้รับการจัดสรรแล้วแต่ไม่เคยถูกนำมาใช้
2. สร้างความตระหนักและจัดการกับกลโกงที่นำเหตุการณ์ไวรัสโคโรนา (โควิด-19) มาใช้ในการหลอกลวง
3. เน้นการทำงานร่วมกับผู้ให้บริการโทรคมนาคมเพื่อปรับปรุงวิธีที่รบกวนและป้องกันการโทรรบกวนและการโทรเพื่อที่จะพยายามหลอกลวง
4. เน้นการลงโทษองค์กรและบุคคลที่ก่อเหตุรำคาญโดยทำงานร่วมกับหน่วยงานกำกับดูแลและหน่วยงานบังคับใช้กฎหมายอื่นๆ
5. แบ่งปันข้อมูลระหว่างผู้ให้บริการโทรคมนาคมรวมถึงพันธมิตรระหว่างประเทศและหน่วยงานที่บังคับใช้กฎหมายเกี่ยวกับความรับผิดชอบในการจัดการกับการหลอกลวงและการฉ้อโกง

แผนปฏิบัติการดังกล่าวมีการเก็บข้อมูลสำคัญที่ใช้ในการใช้วิเคราะห์ความคืบหน้าและประสิทธิภาพของแผนปฏิบัติการ คือ มีการวิจัยการติดตามการโทรรบกวน (Nuisance calls tracking research) ซึ่งโดยปกติแล้ว Ofcom จะทำการวิจัยการติดตามเกี่ยวกับประสบการณ์การโทรที่ก่อความรำคาญของประชาชนจำนวน สามครั้งต่อปี โดยในงานวิจัยนี้ Ofcom จะทำการสัมภาษณ์กับประชาชนที่ได้รับสายรบกวนทางโทรศัพท์บ้านหรือโทรศัพท์มือถือส่วนตัว การวิจัยนี้จะดำเนินการผ่านการสัมภาษณ์แบบตัวต่อตัวของกลุ่มตัวอย่างประชาชนในสหราชอาณาจักรที่เป็นตัวแทนระดับประเทศ[96]

ในปัจจุบัน แผนปฏิบัติการยังเน้นการทำงานระหว่าง Ofcom และบริษัทผู้ให้บริการโทรคมนาคมและหน่วยงานกำกับดูแลอื่น ๆ โดยตั้งเป็นกลุ่มคณะทำงานเพื่อทำความเข้าใจแนวโน้มที่อาจเกิดขึ้นในการหลอกลวงรวมไปถึงหาวิธีในการยับยั้ง โดยทำให้เกิดแนวความคิดริเริ่มเพื่อช่วยบริษัทโทรคมนาคมในการระบุหมายเลขโทรศัพท์ที่ไม่ถูกต้องและปิดกั้นการใช้งานการโทรที่มีมาจากหมายเลขเหล่านี้ โดยทาง Ofcom เป็นหน่วยงานหลักในคณะทำงานเชิงกลยุทธ์ที่ประกอบด้วย

[96] The Information Commissioner's Office (ICO) and Ofcom Nuisance calls and messages, Update to ICO-Ofcom joint action plan 2021, 23 March 2021

บริษัทผู้ให้บริการโทรคมนาคม 11 แห่ง ซึ่งถ้าได้เป็นสมาชิกแล้ว สมาชิกของกลุ่มจะต้องทำการส่งข้อมูลให้กับ Ofcom ในแต่ละเดือนโดยสรุปหมายเลขโทรศัพท์ที่แต่ละหน่วยงานได้รับการร้องเรียน ทาง Ofcomจะทำการรวบรวมข้อมูลทั้งหมดและแบ่งปันให้กับสมาชิกของกลุ่ม

ภายใต้การบังคับใช้อำนาจของ Ofcom ผู้ให้บริการโทรคมนาคมจะต้องดำเนินการตามขั้นตอนที่เหมาะสมในการตรวจสอบและระบุหมายเลขโทรศัพท์ที่ทำการหลอกลวงเพื่อเป็นการป้องกันไม่ให้เชื่อมต่อถึงประชาชนได้[97] โดยรายการหมายเลขโทรศัพท์ที่ต้องทำการแบ่งปันข้อมูลระหว่างสมาชิกของกลุ่ม มีดังต่อไปนี้

ก. หมายเลขโทรศัพท์ที่อยู่นอกเหนือของการกำหนดหมายเลขของ The National Telephone Numbering Plan ให้ถือว่าเป็นหมายเลขโทรศัพท์ผิดกฎหมาย

ข. หมายเลขโทรศัพท์ที่ได้ถูกการรายงานเข้ามาและได้มีการตรวจสอบกับแหล่งข้อมูลอื่นๆ ว่าเป็นเบอร์โทรศัพท์ที่น่าสงสัย

ค. Do not originate list คือ หมายเลขโทรศัพท์ที่อยู่ในรายการดังกล่าวโดยหมายเลขเหล่านี้เป็นหมายเลขที่องค์กรอื่นๆของภาครัฐได้มีการแบ่งปันการใช้ข้อมูล ซึ่งลักษณะของหมายเลขเหล่านี้คือเป็นหมายเลขที่ได้รับการจัดสรรแล้วแต่ไม่เคยถูกนำมาใช้สำหรับการโทรออกดังนั้นหมายเลขกดังกล่าวจึงเป็นช่องว่างให้มิจฉาชีพสามารถเปลี่ยนการแสดงชื่อของสายที่โทรเข้าบนหน้าจอโทรศัพท์ (CLI) เพื่อซ่อนตัวตนหรือเลียนแบบหมายเลขของบริษัทจริงเพื่อหลอกล่อให้คนคิดว่าการโทรนั้นมาจากแหล่งที่เชื่อถือได้ เช่น ธนาคาร เป็นต้น

Ofcom ได้มีการขอความร่วมมือให้บริษัทโทรคมนาคมจำนวน 9 บริษัททำการสรุปงานที่มาตราการต่างๆที่ใช้ในการกำจัดการหลอกลวงและแผนการรับมือในอนาคต ซึ่งบริษัทโทรคมนาคมส่วนใหญ่ได้ให้ความร่วมมือกับทาง Ofcom โดยได้มีการดำเนินกิจกรรมต่างๆ เพื่อปกป้องผู้บริโภคจากการหลอกลวงทางโทรศัพท์ ข้อความ และอีเมล โดยนโยบายส่วนใหญ่ของผู้ให้บริการโทรคมนาคม มีดังต่อไปนี้

1. เน้นการเผยแพร่ข้อมูลเกี่ยวกับกลโกงและให้การสนับสนุนเพิ่มเติมกับผู้บริโภคในกรณีที่ตกเป็นเหยื่อ

[97] The General Conditions of Entitlement, C6

2. ผู้ให้บริการโทรคมนาคมบางรายมีการพัฒนาและนำเทคโนโลยีมาใช้การพัฒนาระบบเพื่อให้สามารถตรวจจับหมายเลขโทรศัพท์ที่ทำการหลอกลวงได้ง่ายมากขึ้น เช่น มีการปิดกั้นการเข้าถึงข้อความที่มีลักษณะไม่ปลอดภัย เป็นต้น
3. มีการฝึกอบรมเกี่ยวกับการหลอกลวงรูปแบบต่างๆให้กับพนักงานของบริษัทและได้จัดตั้งทีมภายในที่เชี่ยวชาญสำหรับการตรวจสอบการหมายเลขโทรศัพท์ที่ทำการหลอกลวง

จากแผนปฏิบัติการข้างต้นที่เกิดจากการบังคับใช้กฎหมายรวมไปถึงการขอความร่วมมือจากภาคเอกชนที่ได้รับความร่วมมืออย่างเป็นระบบ ทำให้ ICO และ Ofcom สรุปว่าการบังคับใช้เป้าหมายต่างๆประสบความสำเร็จมากขึ้นเนื่องจากมีการประสานงานระหว่างหน่วยงานกำกับดูแลกับภาคอุตสาหกรรมโทรคมนาคมและภาคส่วนต่างที่เกี่ยวข้อง ส่งผลให้การพิจารณาแนวโน้มระยะยาวในช่วง 5 ปีที่ผ่านมาจำนวนการร้องเรียนลดลงอย่างมีนัยสำคัญ[98]

4.3 มาตรการทางกฎหมายที่เกี่ยวข้อง

จากที่กล่าวไปข้างต้นว่าทั้ง 2 ประเทศจะเน้นการป้องกันดังนั้นมาตรการทางกฎหมายที่เกี่ยวข้องและนำมาบังคับใช้จะเป็นการนำทฤษฎีที่เกี่ยวกับบทลงโทษในการใช้มาตรการป้องกันเข้ามาเกี่ยวข้องโดยมีจุดประสงค์หลักคือเพื่อเป็นการป้องกันคุ้มครองสังคมรวมไปถึงการป้องกันไม่ให้ความผิดเกิดขึ้นซ้ำ

4.3.1 ประเทศออสเตรเลีย

หลังจาก ACMA มีการวางแผนปฏิบัติการ The Combating Scams Action Plan ในปี 2019 ที่ได้กล่าวไปข้างต้น ซึ่งประกอบไปด้วย 3 แผนหลักๆ ทำให้เกิดการบังคับใช้กฎหมายและมาตรฐานอุตสาหกรรมใหม่ขึ้นเพื่อให้เป็นไปตามแผนปฏิบัติการที่ได้วางไว้ โดยประกอบด้วย

[98] The Information Commissioner's Office (ICO) and Ofcom Nuisance calls and messages, Update to ICO-Ofcom joint action plan 2021, 23 March 2021

4.3.1.1 Telecommunications (Mobile Number Pre- Porting Additional Identity Verification) Industry Standard 2020

เป็นมาตรฐานอุตสาหกรรมที่จัดทำขึ้นและเป็นไปตามทิศทางภายใต้มาตรา 125AA(1) ของพระราชบัญญัติ Telecommunication Act 1997[99] และเป็นการจัดทำเพื่อให้สอดคล้องและเป็นการต่อยอดจาก Telecommunications (Industry Standard for Mobile Number Pre-Porting Additional Identity Verification) Direction 2019 ซึ่งเป็นเรื่องเกี่ยวกับการยืนยันตัวตนของผู้ใช้บริการ[100] โดยมาตรา 125AA(1) ดังกล่าวกล่าวไว้ว่า ACMA ต้องจัดให้มีมาตรฐานอุตสาหกรรมที่ใช้กับอุตสาหกรรมโทรคมนาคมซึ่งประกอบด้วย ผู้ให้บริการโทรคมนาคมรวมไปถึงบริการโทรคมนาคมสาธารณะและจัดการกับเรื่องที่เกิดขึ้นและมีความเกี่ยวข้องกับกิจกรรมโทรคมนาคม[101] ซึ่งเนื้อหาของมาตรฐานอุตสาหกรรมใหม่ที่เกิดขึ้นนี้เกี่ยวข้องกับการวางข้อกำหนดการยืนยันตัวตนเพิ่มเติมเพื่อบังคับใช้กับผู้ให้บริการโทรคมนาคมเพื่อให้เป็นไปตามวัตถุประสงค์ โดยได้ประกาศใช้เมื่อวันที่ 30 เมษายน 2020 และถือเป็น Code of Conduct ที่ต้องปฏิบัติตามหากเป็นผู้ให้บริการโทรคมนาคม วัตถุประสงค์ของมาตรฐานอุตสาหกรรมนี้คือป้องกันการโอนย้ายหมายเลขโทรศัพท์โดยไม่ได้รับอนุญาตประกอบกับการลดอันตรายต่อลูกค้าที่อาจเกิดจากการย้ายหมายเลขโทรศัพท์โดยไม่ได้รับอนุญาตและเพื่อปรับปรุงข้อกำหนดในการยืนยันตัวตนในการย้ายหมายเลขโทรศัพท์มือถือโดยสามารถเข้าถึงอุปกรณ์มือถือที่เชื่อมโยงกับหมายเลขบริการมือถือนั้นได้โดยตรงและทันทีและยังลดความสามารถของนักต้มตุ๋นในการหลอกลวงและการฉ้อโกงในการโอนย้ายอุปกรณ์เคลื่อนที่

มาตรฐานอุตสาหกรรมนี้มีข้อกำหนด**เพิ่มเติม**เกี่ยวกับการยืนยันตัวตนก่อนการย้ายข้อมูลดังนี้

1. ก่อนที่จะเริ่มการโอนย้ายหมายเลขโทรศัพท์ ผู้ให้บริการโทรคมนาคมจะต้องใช้กระบวนการยืนยันตัวตนเพิ่มเติมอย่างน้อยหนึ่งกระบวนการเพื่อยืนยันว่าบุคคลที่ยื่นคำขอย้ายหมายเลขคือผู้ถือสิทธิ์ในการใช้งานหมายเลขโทรศัพท์ที่จะย้าย

---

[99] Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020

[100] Telecommunications (Industry Standard for Mobile Number Pre-Porting Additional Identity Verification) Direction 2019

[101] The Telecommunication Act 1997, subsection 125AA(1)

(ก) ผู้ให้บริการโทรศัพท์สามารถยืนยันว่าบุคคลที่ยื่นคำขอสามารถเข้าถึงอุปกรณ์มือถือที่ใช้ร่วมกับหมายเลขโทรศัพท์ที่จะย้ายได้โดยตรงและทันที

- ในกรณีที่ผู้ใช้บริการทำการร้องขอการโอนหมายเลข ณ ศูนย์บริการหรือบริเวณร้านค้า ทางด้านศูนย์บริการหรือร้านค้าที่เป็นตัวแทนของผู้ให้บริการโทรคมนาคมต้องดำเนินการโทรไปที่หมายเลขโทรศัพท์ในขณะที่อยู่ในร้านและตรวจสอบว่ามือถือของลูกค้ามีการรับสายผ่านอุปกรณ์ที่ใช้กับหมายเลขบริการมือถือนั้น
- ในกรณีการยืนยันตัวตนด้วยเสียง ถ้าในกรณีของลูกค้า ผู้ให้บริการโทรคมนาคมที่รับสายจะทำการโทรกลับหมายเลขบริการมือถือที่จะย้ายเพื่อยืนยันว่าบุคคลที่ทำการยื่นคำขอนั้นเป็นเจ้าของและมีสิทธิ์ในการใช้งานจริง หรือ ตัวแทนที่ได้รับอนุญาตของลูกค้า ผู้ให้บริการโทรคมนาคมที่รับสายจะโทรกลับหมายเลขบริการมือถือที่จะย้ายเพื่อยืนยันว่าบุคคลที่ทำการยื่นคำขอนั้นเป็นตัวแทนที่ได้รับอนุญาตของลูกค้าจริง
- การยื่นคำขอผ่านช่องทางออนไลน์ ผู้ให้บริการโทรคมนาคมต้องทำการยืนยันโดยการตรวจสอบรหัสการยืนยันที่ลูกค้าหรือตัวแทนที่ได้รับอนุญาตของลูกค้าได้รับ โดยรหัสยืนยันดังกล่าวต้องไม่มีการซ้ำกัน

(ข) การใช้รหัสยืนยันที่ไม่ซ้ำกัน (unique verification code) ซึ่งส่งโดยผู้ให้บริการโทรคมนาคมที่ได้รับผ่านข้อความ SMS ไปยังหมายเลขโทรศัพท์ที่จะย้ายและทางฝั่งผู้ให้บริการโทรคมนาคมจะได้รับการยืนยันทันทีผ่านข้อความ SMS ว่าลูกค้าหรือตัวแทนที่ได้รับอนุญาตของลูกค้าได้รับรหัสยืนยันที่ไม่ซ้ำกันนั้น

(ค) มีการใช้ข้อมูลไบโอเมตริกซ์อย่างน้อยหนึ่งรูปแบบ ตัวอย่างของข้อมูลไบโอเมตริกซ์ เช่น ใบหน้า ลายนิ้วมือ เป็นต้น

(ง) ในกรณีที่ลูกค้าเป็นธุรกิจรายใหญ่และต้องการที่จะทำการย้ายหมายเลขภายใต้สัญญากับผู้ให้บริการโทรคมนาคม โดยผู้ให้บริการโทรคมนาคมดังกล่าวต้องยืนยันว่าบุคคลที่ยื่นคำขอเป็นตัวแทนที่ได้รับอนุญาตของลูกค้าธุรกิจรายใหญ่และบุคคลที่

ยื่นคำขอนั้นสามารถเข้าถึงหมายเลขหลักที่เกี่ยวข้องกับลูกค้าธุรกิจรายใหญ่ได้โดยตรงและทันที

2. ในกรณีที่ผู้ให้บริการโทรคมนาคมไม่สามารถยืนยันได้ว่าบุคคลที่ยื่นคำขอเป็นผู้ถือสิทธิ์ของหมายเลขโทรศัพท์ที่จะย้ายผ่านกระบวนการใดกระบวนการหนึ่งที่อธิบายไว้ในข้อ 1 ข้างต้น ผู้ให้บริการโทรคมนาคม อาจดำเนินการยืนยันตัวตนเพื่อยืนยันว่าบุคคลที่ยื่นคำขอเป็นผู้ถือสิทธิ์ในการใช้หมายเลขโทรศัพท์จริงๆโดยสามารถใช้กระบวนการใดกระบวนการหนึ่งต่อไปนี้

(ก) เรื่องการใช้เอกสาร ผู้วิจัยสามารถสรุปได้ดังนี้ เอกสารที่สามารถใช้นำมายืนยันตัวตนได้ต้องเป็นเอกสารประเภทราชการที่ทางการออสเตรเลียเป็นผู้ออก และ/หรือ เอกสารที่หน่วยงานที่น่าเชื่อถือเป็นผู้ออกให้ซึ่งมีเงื่อนไขคือ สามารถนำเอกสารประเภทราชการออกให้จำนวน 2 ฉบับ หรือ เอกสารประเภทราชการออกให้จำนวน 1 ฉบับและเอกสารประเภทหน่วยงานที่น่าเชื่อถือออกให้จำนวน 2 ฉบับมาใช้ในการยืนยันตัวตน ในส่วนของชนิดเอกสาร ทางผู้วิจัยจะขอยกตัวอย่างของเอกสารในบางส่วนเท่านั้น

เอกสารที่ออกโดยราชการ ได้แก่ ใบรับรองสัญชาติออสเตรเลียที่ออกโดยรัฐบาล ใบขับขี่ของรัฐที่ออกโดยชื่อของผู้ยื่นคำขอ หนังสือเดินทางออสเตรเลียที่ยังไม่หมดอายุหรือถ้าหมดอายุต้องไม่เกิน 2 ปีที่หมดอายุ สูติบัตรที่ออกโดยรัฐบาลรัฐหรือดินแดนของออสเตรเลีย บัตรประจำตัวทหารต่างประเทศ เป็นต้น

เอกสารที่ออกโดยหน่วยงานที่น่าเชื่อถือ ได้แก่ สมุดบัญชีเงินฝากหรือใบแจ้งยอดที่ออกโดยธนาคารซึ่งใบแจ้งยอดบัตรหรือสมุดบัญชีเงินฝากต้องครอบคลุมธุรกรรมทางการเงินอย่างน้อย 6 เดือนและอยู่ในชื่อของบุคคลที่ยื่นคำขอ ลายเซ็นของบุคคลที่ยื่นคำขอต้องอยู่บนบัตรและต้องมีที่อยู่ปัจจุบันในใบแจ้งยอดหรือสมุดบัญชีเงินฝาก โดยถ้าเป็นธนาคารต่างประเทศจะไม่รับพิจารณา บัตรประกันสุขภาพ บัตรประจำตัวนักเรียนที่ออกโดยสถาบันการศึกษาระดับอุดมศึกษาของออสเตรเลียหรือโรงเรียนมัธยมออสเตรเลียหรือองค์กรฝึกอบรมที่จดทะเบียน เป็นต้น

(ข) การใช้บริการตรวจสอบออนไลน์ของทางรัฐบาล

3. กรณีที่ผู้ให้บริการโทรคมนาคมจะต้องทำการตรวจสอบและใช้บริการตรวจสอบออนไลน์ของทางรัฐบาล ตามข้อ 2 (ข) ว่าบุคคลที่ยื่นคำขอเป็นผู้ถือสิทธิ์ในการใช้งานจริงๆ หากบุคคลที่ยื่นคำขอต่อผู้ให้บริการโทรคมนาคมมีหมายเลขโทรศัพท์ที่ระบุในเอกสารราชการที่ไม่ซ้ำกันอย่างน้อยสองฉบับโดยข้อมูลที่ให้ไว้เกี่ยวกับเอกสารราชการทั้ง 2 ฉบับจะถูกตรวจสอบในบริการตรวจสอบออนไลน์ของรัฐบาล
4. ผู้ให้บริการโทรคมนาคมต้องไม่ดำเนินการย้ายหมายเลขโทรศัพท์ เว้นแต่จะมีการใช้กระบวนการยืนยันตัวตนเพิ่มเติมขั้นตอนใดขั้นตอนหนึ่งใน 1 หรือ 2
5. ผู้ให้บริการโทรคมนาคมต้องไม่เรียกเก็บค่าธรรมเนียมจากลูกค้าหรือตัวแทนที่ได้รับอนุญาตของลูกค้าสำหรับข้อความ SMS ที่ใช้เพื่อดำเนินการยืนยันตัวตน

นอกจากนี้ ผู้ให้บริการโทรคมนาคมต้องเผยแพร่ข้อมูลบนเว็บไซต์ของตนเพื่อแนะนำลูกค้าว่าเพื่อปกป้องลูกค้าจากการย้ายหมายเลขโทรศัพท์ที่ไม่ได้รับอนุญาตโดยจะมีการใช้กระบวนการยืนยันตัวตนเพื่อยืนยันตัวตนของบุคคลที่ส่งคำขอย้ายก่อนที่จะมีการย้ายหมายเลขโทรศัพท์และในกรณีที่ลูกค้าสงสัยว่าหมายเลขโทรศัพท์ถูกย้ายโดยผิดกฎหมายลูกค้าสามารถรายงานไปยังหน่วยงานที่เกี่ยวข้องของภาครัฐหรือแจ้งตำรวจสหพันธรัฐออสเตรเลียหรือตำรวจรัฐหรือเขตแดนที่เกี่ยวข้องได้

จะเห็นได้ว่า มาตราฐานอุตสาหกรรมดังกล่าวจะเน้นการป้องกันจากการโอนย้ายหมายเลขโทรศัพท์มือถือเป็นส่วนใหญ่ โดยถ้าผู้ให้บริการโทรคมนาคมดังกล่าวไม่ปฏิบัติตาม ACMA สามารถออกคำเตือนอย่างเป็นทางการหากบุคคลนั้นฝ่าฝืนมาตรฐานอุตสาหกรรม[102] และจะมีบทลงโทษทางการเงินสำหรับการฝ่าฝืนซึ่งถือเป็นบทลงโทษทางแพ่งตามมาตรา 128 The Telecommunication Act 1997[103] เนื่องจากประเทศออสเตรเลียใช้ระบบกฎหมายแบบจารีตประเพณี (Common Law) ดังนั้น การกำหนดตัวเงินค่าปรับจะขึ้นอยู่กับการพิจารณาของศาลเป็นส่วนใหญ่ซึ่งศาลจะทำการพิจารณาองค์ประกอบต่างๆของการฝ่าฝืนนั้น เช่น ลักษณะของการฝ่าฝืน ความเสียหายที่เกิดขึ้นจากการฝ่าฝืนของผู้ให้บริการโทรคมนาคม[104]

---

[102] The Telecommunication Act 1997, section 129

[103] The Telecommunication Act 1997, section 128 (3)

[104] The Telecommunication Act 1997, section 570 (1) , (2)

4.3.1.2 Reducing Scams Call Industry Code

เมื่อวันที่ 2 ธันวาคม 2020 ทาง ACMA ได้จดทะเบียนรหัส C661:2020 Reducing Scam Calls Code (รหัส 2020) พัฒนาขึ้นโดย The WC92: Reducing Scam Calls Working Committee ซึ่งเป็นหน่วยงานที่ตั้งขึ้นเพื่อปฏิบัติงานเกี่ยวกับการหลอกลวงผู้บริโภคและเพื่อให้แน่ใจว่า industry code ดังกล่าวอยู่ภายใต้ขอบเขตของส่วนที่ 6 ของ the Telecommunications Act 1997 ตามมาตรา 109 ที่ได้กล่าวว่ากิจกรรมโทรคมนาคมจะครอบคลุมถึงเรื่องใดบ้างและหมวดต่างๆของอุตสาหกรรมที่จะครอบคลุม[105] และ มาตรา 110 ที่กล่าวไว้ว่า ส่วนต่างๆของอุตสาหกรรมโทรคมนาคมตามมาตรา 109 ต้องได้รับการตรวจสอบตามมาตรานี้[106] ตามลำดับ โดยในคณะทำงาน WC92 ประกอบไปด้วยตัวแทนของผู้ให้บริการโทรคมนาคมในประเทศออสเตรเลีย ได้แก่ AMTA, Optus, Pivotel, Sinch, Symbio, Telstra, TPG Telecom, Twilio, Verizon and Vocus โดยการจัดทำ Industry Code นี้มีวัตถุประสงค์เพื่อให้เป็นไปตามแผนปฏิบัติการ The Combating Scams Action Plan ที่แนะนำให้มีการพัฒนาภาระผูกพันที่บังคับใช้กับกลุ่มกิจการโทรคมนาคม และในปัจจุบันได้ถูกแทนที่ด้วย C661:2022 Reducing Scam Calls and Scam SMs Industry Code ซึ่งเป็นฉบับแก้ไขล่าสุด

Reducing Scams Call Industry Code เป็นหลักเกณฑ์ในการบังคับใช้ภาระผูกพันที่กำหนดให้บริษัทโทรคมนาคมต้องตรวจจับ ติดตาม และปิดกั้นการใช้งานเบอร์โทรศัพท์ที่มีการโทรหลอกลวง โดย Reducing Scams Call Industry Code ได้ถูกพัฒนาและปรับปรุงจากคำแนะนำโดยตรงมาจากแผนปฏิบัติการ Combating Scams Action Plan ของ ACMA ที่ได้กล่าวมาข้างต้น ซึ่งวัตถุประสงค์หลักของหลักเกณฑ์นี้คือ ต้องการที่จะลดการปริมาณเบอร์โทรศัพท์และลดจำนวนการโทรหลอกลวงที่โทรเข้ามาหลอกประชาชน โดยผู้ให้บริการโทรคมนาคมจะต้องตรวจสอบและตรวจจับการรับส่งข้อมูลการโทรหลอกลวงบนเครือข่ายของตน โดยเฉพาะอย่างยิ่งเน้นการแบ่งปันข้อมูลของเบอร์โทรศัพท์ที่ทำการหลอกลวงกับผู้ให้บริการโทรคมนาคมรายอื่นและหน่วยงานภาครัฐที่

[105] The Telecommunication Act 1997, section 109

[106] The Telecommunication Act 1997, section 110

เกี่ยวข้องดังนั้นการแชร์ข้อมูลของเบอร์โทรศัพท์ระหว่างกันดังกล่าวจะไม่มีผลต่อ Privacy Act 1988 ตามมาตรา 116A ของ the Telecommunications Act 1997[107] รวมไปถึงต้องทำการตรวจสอบ ติดตาม และปิดกั้นการใช้งานเบอร์โทรศัพท์ที่ทำการหลอกลวง แจ้งการโทรหลอกลวงต่อเจ้าหน้าที่และให้คำแนะนำและข้อมูลแก่ลูกค้า อีกทั้ง Communications Alliance (CA) และสมาชิกมุ่งมั่นที่จะหากลยุทธ์ในการบรรเทาแก๊งคอลเซ็นเตอร์ตามบริบทของสภาพแวดล้อมของออสเตรเลียรวมไปถึงรูปแบบการหลอกลวงต่างๆซึ่งเป็นส่วนหนึ่งของรูปแบบการปรับปรุงอย่างต่อเนื่องจะเห็นได้ว่าวัตถุประสงค์ของการออกหลักเกณฑ์ในการบังคับใช้นี้จะมีความคล้ายคลึงกับแผนปฏิบัติการที่ 2 ของ Combating Scams Action Plan ที่ได้กล่าวไปข้างต้น แสดงให้เห็นว่าได้มีการพัฒนามาจากแผนปฏิบัติการดังกล่าวนั่นเอง

ACMA ได้ขอความร่วมมือกับบริษัทโทรคมนาคมและกลุ่มสื่อสารมวลชนเพื่อพัฒนาหลักเกณฑ์ใหม่และทำให้ประสบความสำเร็จในการริเริ่มโครงการนำร่องเพื่อลดผลกระทบต่อที่เกิดจากแก๊งคอลเซ็นเตอร์ของชาวออสเตรเลียซึ่งที่ผ่านมาบริษัทผู้ให้บริการโทรคมนาคมรายใหญ่รายงานว่าได้ทำการปิดกั้นการใช้งานหมายเลขโทรศัพท์ที่มีการโทรหลอกลวงกว่า 30 ล้านครั้งในช่วง 12 เดือนที่ผ่านมา เนื่องจากพวกเขาพยายามทดลองใช้การยืนยันระบุตัวตนก่อนการโอนย้ายหมายเลขและใช้แผนปฏิบัติการลดการโทรหลอกลวง

ในปี2020 หลังจากที่มีการประกาศใช้หลักเกณฑ์ใหม่นี้ จากรายงาน Targeting Scams report ในปี 2020 ที่จัดทำโดย ACCC จำนวนรายงานที่ส่งไปยัง Scamwatch เกี่ยวกับการขโมยข้อมูลประจำตัวในปี 2020 เพิ่มขึ้น 84% 20,939 รายงาน) จากรายงาน 11,373 ฉบับในปี 2019 แต่อย่างไรก็ตาม ความสูญเสียจากการหลอกลวงลดลงจาก 4.3 ล้านดอลลาร์ในปี 2019 เหลือ 3.1 ล้านดอลลาร์ในปี 2020[108] ซึ่งการเปลี่ยนแปลงของตัวเลขของความสูญเสียส่วนหนึ่งเกิดจากกฎใหม่ที่ ACMA นำมาใช้ในเดือนเมษายน 2020 ที่กำหนดให้ผู้ให้บริการขนส่งเคลื่อนที่ทุกรายใช้การยืนยันตัวตนเพิ่มเติมก่อนที่จะย้ายหมายเลขโทรศัพท์มือถือจากผู้ให้บริการรายหนึ่งไปยังอีกรายหนึ่งและผลกระทบต่อความ

---

[107] The Telecommunication Act 1997, section 116A

[108] Australian Competition and Consumer Commission, Targeting Scam Report of the ACCC on scams activity 2020, June 2021

สูญเสียที่เกี่ยวข้องกับการโจรกรรมข้อมูลระบุตัวตนที่รายงานไปยัง ACCC ในปี 2019 การสูญเสีย 1.1 ล้านดอลลาร์เกิดจากการหลอกลวงทางโทรศัพท์ที่รายงานไปยัง Scamwatch ในปี 2020 ความสูญเสียที่เกี่ยวข้องกับการหลอกลวงการโอนสายโทรศัพท์ลดลงเหลือเพียง 540,000 ดอลลาร์อีกด้วย[109] นอกจากนี้ยังส่งผลต่อตัวเลขของการหลอกลวง phishing ที่ถึงแม้จะเป็นประเภทการหลอกลวงที่มีอัตราและจำนวนรายงานสูงสุดแต่กลับมีมูลค่าความเสียหายเมื่อเทียบกับจำนวนรายงานต่ำที่สุด ดังรูปภาพด้านล่าง

[109] Australian Competition and Consumer Commission, Targeting Scam Report of the ACCC on scams activity 2020, June 2021

รูปภาพที่ 10[110] Breakdown of scam categories by reports and reported losses.

Reports by numbers

Scam type	Number of reports 2020	Reported losses 2020	Number of reports with loss
Phishing	44,079	$1,689,406	696 (1.6%)
Threats to life, arrest or other	32,215	$11,833,508	558 (1.7%)
Identity theft	20,939	$3,072,287	673 (3.2%)
Online shopping scams	15,306	$7,384,733	8,349 (54.5%)
False billing	13,120	$18,464,903	1,799 (13.7%)
Hacking	8,691	$1,419,353	425 (4.9%)
Remote access scams	8,473	$8,441,632	667 (7.9%)
Classified scams	7,928	$5,529,413	2,497 (31.5%)
Investment scams	7,295	$65,820,313	2,464 (33.8%)
Unexpected prize & lottery scams	4,543	$1,706,253	298 (6.6%)
Ransomware & malware	3,885	$74,076	42 (1.1%)
Dating & romance scams	3,708	$38,916,120	1,289 (34.8%)
Jobs & employment scams	2,933	$1,268,582	290 (9.9%)
Rebate scams	1,827	$701,250	91 (5.0%)
Inheritance scams	1,676	$1,434,544	59 (3.5%)
Overpayment scams	1,658	$701,729	358 (21.6%)
Mobile premium services	1,523	$141,549	148 (9.7%)
Health & medical products	1,459	$3,915,689	382 (26.2%)
Fake charity scams	1,425	$133,214	139 (9.8%)
Nigerian scams	577	$896,115	92 (15.9%)
Betting & sports investment scams	448	$985,926	150 (33.5%)
Pyramid schemes	406	$286,107	85 (20.9%)
Psychic & clairvoyant	230	$230,273	90 (39.1%)
Travel prize scams	151	$11,754	17 (11.3%)
Scratchie scams	143	$243,348	14 (9.8%)
Other scams	31,449	$382,014	1,213 (3.9%)
Total	216,087	$175,684,091	22885 (10.6%)

จะสามารถวิเคราะห์จากรูปภาพที่9ได้ว่า จำนวน Phishing ที่ถูกรายงานเข้ามาทั้งหมดมีจำนวน 44,079 รายงานซึ่งมีจำนวนมากที่สุด โดยเป็นรายงานที่รายงานมาพร้อมกับความเสียหายจำนวน 696 รายการ คิดเป็นร้อยละ 1.6 เท่านั้น

ในปี 2022 ได้มีการปรับปรุงแก้ไขฉบับใหม่ขึ้นคือ ฉบับปรังปรุงใหม่ 2022 และได้ถูกนำมาแทนที่ฉบับ C661:2020 Reducing Scam Calls Code (รหัส 2020) โดยในฉบับ C661:2022 Reducing Scam Calls and Scam SMs Industry Code ได้มีวัตถุประสงค์การเพิ่มเติมดังประเด็นต่อไปนี้

[110] Australian Competition and Consumer Commission, Targeting Scam Report of the ACCC on scams activity 2020, June 2021

(ก) ประเด็นการหลอกลวงทาง SMS เช่น ภาระหน้าที่มุ่งลด Scam SMS

(ข) ปรับปรุงข้อผูกมัดซึ่งเน้นที่การลด Scam Calls

(ค) ภาระหน้าที่ในการแจ้ง ACMA ในขั้นตอนต่างๆ ในกระบวนการสืบสวนและติดตาม (สำหรับทั้ง Scam Calls และ Scam SM) เพื่อให้มีมุมมองแบบองค์รวมว่าในการรับส่งข้อมูลมิจฉาชีพอยู่ที่ใด

(ง) เพิ่มภาระหน้าที่ในการยกเลิกบริการที่มีการใช้หมายเลขโทรศัพท์ของออสเตรเลียสำหรับการหลอกลวงแบบการโทรกลับ (Wangiri Scam)

(จ) มีการจัดทำแม่แบบสำหรับการรายงานเบอร์โทรหลอกลวงและการหลอกลวงทาง SMS ที่จะต้องจัดเตรียมให้กับ ACMA

(ฉ) มีการแก้ไขบทบรรณาธิการเพื่อปรับปรุงความชัดเจนในคำจำกัดความและส่วนต่างๆ ของหลักการนี้ให้มีความชัดเจนมากยิ่งขึ้น

แม้ว่าการจัดทำ Industry Code ดังกล่าวจะทำการสร้างภาระประกอบกับมีต้นทุนที่ทำให้ผู้ให้บริการโทรคมนาคมเนื่องจากมีค่าใช้จ่ายที่เกี่ยวข้องกับการจัดตั้งและการบำรุงรักษาระบบสนับสนุนและข้อตกลงที่จำเป็นในการดำเนินการตามบทบัญญัติใหม่ใน Industry Code นอกจากนี้ยังมีค่าใช้จ่ายที่ดำเนินอยู่อย่างต่อเนื่องเพื่อจัดการกับวิธีการที่มิจฉาชีพพยายามหลอกลวงผู้บริโภคแต่เนื่องจากบทบัญญัติของกฎหมายและอำนาจบังคับใช้ทำให้ผู้ให้บริการโทรคมนาคมต้องปฏิบัติตามอย่างหลีกเลี่ยงไม่ได้ ดังนั้นผู้วิจัยจึงมีความเห็นว่าประเทศไทยอาจจะต้องมีการนำมาปรับใช้ในเท่าที่จำเป็นเพื่อเป็นการไม่ก่อให้เกิดภาระแก่ผู้ให้บริการโทรคมนาคมมากจนเกินไปซึ่งจะขัดกับหลักความได้สัดส่วนของหลักนิติธรรม

ในส่วนของบทลงโทษ เมื่อผู้ให้บริการโทรคมนาคมได้มีการละเมิดหลักปฏิบัติในอุตสาหกรรม ทาง ACMA สามารถออกคำเตือนอย่างเป็นทางการหากมีการฝ่าฝืน Industry Code ดังกล่าวที่ได้ลงทะเบียนไว้ภายใต้ส่วนนี้[111] และมีอำนาจสั่งให้ผู้ให้บริการโทรคมนาคมปฏิบัติตามหลักเกณฑ์ของ industry code นอกจากนี้ยังมีบทลงโทษทาง

[111] The Telecommunication Act 1997, section 122

การเงินสำหรับการฝ่าฝืนซึ่งถือเป็นบทลงโทษทางแพ่ง[112] โดยการกำหนดตัวเงินค่าปรับจะขึ้นอยู่กับการพิจารณาของศาลเป็นส่วนใหญ่ซึ่งศาลจะทำการพิจารณาองค์ประกอบต่างๆ ของการฝ่าฝืนนั้น เช่น ลักษณะของการฝ่าฝืน ความเสียหายที่เกิดขึ้นจากการฝ่าฝืนของผู้ให้บริการโทรคมนาคมเช่นเดียวกับการฝ่าฝืนมาตรฐานอุตสาหกรรมตามหัวข้อ 4.3.1.1 ข้างต้น

4.3.2 ประเทศสหราชอาณาจักร

เนื่องจาก Ofcom เป็นหน่วยงานในการกำกับดูแลหมายเลขโทรศัพท์ของประเทศสหราชอาณาจักรโดยเฉพาะอย่างยิ่งการดูแลหมายเลขโทรศัพท์ที่ถูกนำมาใช้อย่างผิดกฎหมาย ไม่ว่าจะเป็น การออกเบอร์ที่ไม่เป็นไปตามข้อกำหนดหรือการนำหมายเลขโทรศัพท์ที่มีการเปิดใช้งานแล้วแต่ไม่มีการใช้งานมาใช้ในทางที่ไม่ชอบ ดังนั้นทาง Ofcom จึงได้ทำการออกข้อกำหนด The National Telephone Numbering Plan เป็นแผนการกำหนดหมายเลขโทรศัพท์ที่จะสามารถทำการออกหมายเลขรวมไปถึงและการกำหนดข้อจำกัดต่างๆเกี่ยวกับวิธีการนำหมายเลขโทรศัพท์ไปใช้[113] ถ้าหมายเลขโทรศัพท์ที่ผู้ให้บริการออกหมายเลขไปโดยมีความแตกต่างไปจากข้อกำหนดนี้จะถือว่าเป็นหมายเลขที่ผิดกฎหมาย ในส่วนของแผนปฏิบัติการ จากการศึกษาของผู้วิจัยพบว่า Ofcom อาศัยอำนาจของ The Communications Act 2003 ซึ่งมีหน้าที่ในการเผยแพร่นโยบายต่างๆ และบังคับให้เป็นไปตามมาตรฐานรวมถึงสามารถแก้ไขนโยบายต่างๆได้หากเห็นว่าเหมาะสมเพื่อให้สอดคล้องกับสถานการณ์ปัจจุบันอยู่เสมอ[114] ประกอบหลักแนวทางการกำกับดูแลหน่วยงานที่ทาง Ofcom จะยึดหลักการไม่เข้าไปแทรกแซงในเรื่องที่ไม่จำเป็นแต่ใช้หลักการยุติธรรมสนับสนุนการตัดสินใจในการใช้อำนาจในการกำกับดูแลนั้น โดยมีการทำงานร่วมกับหน่วยงานอื่นที่เกี่ยวข้องในการควบคุมกำกับดูแลด้วยกัน ด้วยแนวคิดการกำกับดูแลดังกล่าวทำให้กฎหมายที่นำมาบังคับใช้ในแผนปฏิบัติการส่วนใหญ่จะเน้นไปในบทลงโทษผู้ที่กระทำความผิดซึ่งรวมถึงบุคคลหรือบริษัทที่สร้างความรำคาญให้กับประชาชนและมิจฉาชีพที่ใช้

---

[112] The Telecommunication Act 1997, section 121

[113] The Communications Act 2003, Section 56

[114] The Communications Act 2003, Section 8

หมายเลขโทรศัพท์เป็นเครื่องมือในการหลอกลวงซึ่งแตกต่างจากประเทศออสเตรเลียที่มีการออกมาตรฐานอุตสาหกรรมเพื่อใช้บังคับกับผู้ให้บริการโทรคมนาคมในการพิสูจน์และยืนยันตัวตนของผู้ใช้บริการ

ในส่วนของประเทศสหราชอาณาจักร จะเน้นการทำข้อตกลงระหว่างการย้ายเครือข่าย ผู้ให้บริการโทรคมนาคมต้องจัดทำสัญญา Record Of Consent ขึ้นซึ่งสัญญาดังกล่าวต้องทำกับผู้ใช้บริการที่ทำการร้องขอการย้ายเครือข่าย โดยผู้ให้บริการโทรคมนาคมแต่ละรายที่จะต้องจัดทำและเก็บบันทึกสัญญาดังกล่าวกับผู้ใช้บริการแต่ละรายซึ่งภายในสัญญามีรายการที่ต้องทำการจัดเก็บเป็นระยะเวลาไม่น้อยกว่าสิบสองเดือน[115] และมีเงื่อนไขว่าผู้ให้บริการต้องทำการจัดเก็บสัญญาแม้ว่าสัญญาดังกล่าวจะถูกยกเลิกหรือยุติภายในระยะเวลาสิบสองเดือน[116] โดยรายละเอียดสัญญาต้องประกอบด้วยดังนี้

(ก) บันทึกความยินยอมโดยตรงที่ผู้ใช้บริการร้องขอในการย้ายเครือข่าย โดยแสดงผู้ให้บริการโทรคมนาคมรายเก่าและรายใหม่

(ข) ชื่อและที่อยู่ของผู้ใช้บริการที่ทำการร้องขอการโอนย้ายและที่อยู่

(ค) เวลา วันที่ และวิธีการที่ได้รับความยินยอมในส่วนของข้อ (ก) ข้างต้น

(ง) สถานที่ให้ความยินยอมในส่วนของข้อ (ก) ข้างต้นและชื่อพนักงานที่เกี่ยวข้องตามความเหมาะสม

(จ) ที่อยู่

นอกจากนี้ ผู้ให้บริการโทรคมนาคมต้องทำการส่งจดหมายแจ้งการโอนย้ายให้กับผู้ใช้บริการที่ทำการร้องขอ โดยรายละเอียดจดหมายจะต้องระบุเงื่อนไขที่ชัดเจนและเข้าใจได้ง่าย มีรายละเอียดดังต่อไปนี้

(ก) วันที่ของจดหมาย

(ข) ชื่อของผู้ใช้บริการที่ร้องขอการโอนย้ายเครือข่าย

(ค) ประเภทของบริการด้านการสื่อสารที่เกี่ยวข้องทั้งหมดที่จะถูกโอนย้าย

(ง) วันที่ที่มีผลการย้ายเครือข่าย

---

115 The General Conditions of Entitlement, C7.7

116 The General Conditions of Entitlement, C7.8

(จ) สิทธิของผู้ใช้บริการในการบอกเลิกสัญญาตามที่กำหนดไว้รวมไปถึงวิธีการใช้สิทธิในการบอกเลิกและวันที่ที่ต้องใช้สิทธิในการบอกเลิก

(ฉ) รายละเอียดการติดต่อที่เกี่ยวข้อง

โดยประเด็นสำคัญคือ ผู้ให้บริการโทรคมนาคมรายเดิมต้องส่งจดหมายแจ้งให้ผู้ใช้บริการในการเปลี่ยนแปลงตามกระบวนการที่ตกลงร่วมกัน ซึ่งภายในจดหมายจะต้องระบุเงื่อนไขที่ชัดเจนและทำให้ผู้ใช้บริการสามารถเข้าใจได้ง่าย

จากที่กล่าวไปข้างต้นว่าการกำกับดูแลของทาง Ofcom จะยึดหลักการไม่เข้าไปแทรกแซงแต่ใช้หลักการสนับสนุนการตัดสินใจในการใช้อำนาจในการกำกับดูแลของผู้ให้บริการโทรคมนาคมแทน โดย Ofcom ได้กำหนดนโยบายในการใช้อำนาจที่ได้รับจากกฎหมาย โดยนโยบายดังกล่าวคือ “A statement of Ofcom’s general policy on the exercise of its enforcement powers” ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 1 มีนาคม 2017 เป็นต้นมา ดังนั้นการใช้บทลงโทษต่างๆจึงเน้นไปที่ผู้ที่ใช้บริการเครือข่ายหรือใช้บริการสื่อสารทางอิเล็กทรอนิกส์ในทางที่ผิดซึ่งพฤติกรรมดังกล่าวจะมีลักษณะที่ก่อให้เกิดหรือมีแนวโน้มที่จะทำให้บุคคลอื่นโดยเฉพาะผู้บริโภคได้รับอันตราย ดังนั้น Ofcom สามารถดำเนินการเพื่อระงับและลงโทษบุคคลเหล่านั้นโดยสามารถกำหนดบทลงโทษได้สูงถึง 2 ล้านปอนด์ ซึ่งอำนาจในการลงโทษดังกล่าวนั้นอยู่ภายใต้ของกฎหมาย The Communications Act 2003[117] นอกจากนี้ Ofcom ได้จัดทำบันทึกความเข้าใจกับผู้ให้บริการโทรคมนาคมรายใหญ่สิ่งนี้กำหนดกรอบการทำงานสำหรับความร่วมมือโดยสมัครใจเกี่ยวกับมาตรการทางเทคนิคระหว่างองค์กรที่เข้าร่วม รวมถึงวิธีที่จะทำงานร่วมกันเพื่อบรรลุเป้าหมายร่วมกันในการลดผลกระทบของการก่อกวนที่ผิดกฎหมายต่อผู้บริโภค

เงื่อนไขบังคับที่ผู้ให้บริการโทรคมนาคมต้องปฏิบัติตามหากต้องการให้บริการในสหราชอาณาจักร[118] ที่ในปัจจุบันยังคงมีการปรับปรุงแก้ไขและรวบรวมฉบับล่าสุดยังไม่แล้วเสร็จดี โดยในส่วนที่เกี่ยวเนื่องกับการเกิดอาชญากรรมได้คือส่วนของ การย้ายหมายเลขโดยมีเงื่อนไขที่กำหนดกฎให้ผู้ให้บริการโทรคมนาคมต้องปฏิบัติตามเมื่อผู้ใช้บริการยื่นคำขอการ

[117] The Communications Act 2003, Section 128, 129, 130

[118] The General Conditions of Entitlement

โอนย้ายหมายเลขซึ่ง ณ ปัจจุบัน อยู่ในระหว่างการออกกฎเกณฑ์ใหม่ที่จะมีผลบังคับใช้ปี 2023 โดยการปรับปรุงกฎเกณฑ์ใหม่จะเน้นการปกป้องลูกค้าที่เป็นบุคคลธรรมดาและธุรกิจขนาดเล็ก(SME)ในประเทศที่อยู่ระหว่างกระบวนการเปลี่ยนผู้ให้บริการโทรศัพท์บ้านและ/หรือบริการบรอดแบนด์ ไม่ว่าจะเป็นเมื่อย้ายจากผู้ให้บริการโทรคมนาคมรายหนึ่งไปยังอีกราย หรืออยู่กับผู้ให้บริการโทรคมนาคมรายเดิมเมื่อย้ายตำแหน่ง หรือเปลี่ยนบริการด้วยรายเดียวกัน โดยในปี2023 ผู้ให้บริการสื่อสารจะมีการใช้ “One Touch Switch Process”[119] ซึ่งทำเกิดความรวดเร็วในขั้นตอนการย้ายหมายเลขโทรศัพท์และนำมาแทนที่ขั้นตอนการแจ้งการโอนที่มีอยู่ในปัจจุบัน ในส่วนของโทรศัพท์มือถือ จะใช้กระบวนการ Auto-Switch ซึ่งจะมีการบังคับใช้ในปี 2023 โดยกระบวนการใหม่ทั้ง2 กระบวนการจะมีการแก้ไขเพิ่มเติมใน The General Conditions of Entitlement ซึ่งถือเป็นแนวทางปฏิบัติหลักสำหรับผู้ให้บริการโทรคมนาคมและจะมีผลบังคับใช้วันที่ 3 เมษายน 2023 โดยที่ในปัจจุบันประกาศดังกล่าวอยู่ในระหว่างการแก้ไขและไม่มีผลบังคับใช้ทางกฎหมาย

[119] Ofcom, Quick, easy and reliable switching: Statement on changes to the General Conditions, 3 February 2022

บทที่ 5
บทวิเคราะห์และเปรียบเทียบ

5.1 บทวิเคราะห์และเปรียบเทียบแนวทางการป้องกันแก๊งคอลเซ็นเตอร์โดยการกำกับดูแลของอุตสาหกรรมโทรคมนาคมของประเทศออสเตรเลียและประเทศสหราชอาณาจักรเปรียบเทียบกับประเทศไทย

จากการศึกษาและค้นคว้าของผู้วิจัยเกี่ยวกับแนวทางการป้องกันแก๊งคอลเซ็นเตอร์โดยการกำกับดูแลของอุตสาหกรรมโทรคมนาคมและบทกฎหมายที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ของประเทศออสเตรเลียและประเทศ สหราชอาณาจักรเปรียบเทียบกับประเทศไทย ผู้วิจัยจะขอทำการวิเคราะห์และแยกประเด็นเกี่ยวกับแนวทางการป้องกันที่เป็นสาระสำคัญดังต่อไปนี้

(1) การมีส่วนร่วมขององค์กรภาครัฐและเอกชนรวมไปถึงการวางแผนปฏิบัติการในการป้องกันแก๊งคอลเซ็นเตอร์อย่างเป็นรูปธรรมที่สามารถติดตามผลและวัดผลได้

การมีส่วนร่วมขององค์กรภาครัฐและภาคเอกชนในการหาทางออกหรือหาแนวทางในการป้องกันแก๊งคอลเซ็นเตอร์ถือเป็นปัจจัยสำคัญอย่างหนึ่งเนื่องจากทางภาครัฐไม่สามารถที่จะจัดการปัญหาดังกล่าวได้ถ้าขาดการร่วมมือของภาคเอกชนไม่ว่าจะเป็นผู้ให้บริการโทรคมนาคมหรือบริษัทอื่นๆที่มีส่วนได้ส่วนเสียกับเรื่องดังกล่าว ในประเทศออสเตรเลียการร่วมมือกันของทั้ง2ภาคส่วนถือว่าประสบความสำเร็จเนื่องจากได้มีการคิดริเริ่ม The Scam Technology Project ซึ่งเป็นโครงการที่ร่วมกันจัดให้มีขึ้นเพื่อลดความเสียหายและเป็นการป้องกันมิจฉาชีพในการหลอกลวงตั้งแต่ต้นทางบวกกับแก๊งคอลเซ็นเตอร์ได้สร้างความรำคาญให้กับประชาชนชาวออสเตรเลียอย่างมาก ดังนั้นจึงเป็นหน้าที่ของภาครัฐในการหาวิธีการที่จะยับยั้งและบรรเทาความรำคาญนั้นให้กับประชาชนโดยไม่มากก็น้อย โดยที่โครงการดังกล่าวได้ทำให้เกิดการวางแผนปฏิบัติการที่เป็นรูปธรรมเรียกว่า The Combating Scams Action Plan ซึ่งเป็นจุดเริ่มต้นในการออกกฎเกณฑ์ที่บังคับใช้กับผู้ให้บริการโทรคมนาคมในการป้องกันและตรวจสอบความผิดปกติของหมายเลขโทรศัพท์ได้ตั้งแต่ต้นทางส่งผลให้ตัวเลขของการสูญเสียทางด้านการเงินในการหลอกลวงลดน้อยลงอย่างมีนัยสำคัญ ในส่วนของประเทศอังกฤษ ทางภาครัฐได้มีการจัดทำแผนปฏิบัติการที่เรียกว่า Nuisance calls and messages Update to ICO - Ofcom joint action plan ซึ่งแผนปฏิบัติการดังกล่าวเกิดขึ้นครั้ง

แรกเมื่อปี 2013 ทำให้เห็นว่าภาครัฐได้ตระหนักถึงการก่อให้เกิดความเสียหายและก่อความรำคาญให้กับประชาชนเป็นอย่างมาก แม้ว่าในช่วงแรกของการวางแผนปฏิบัติการภาครัฐจะยังไม่มีการขอความร่วมมือกับภาคเอกชนก็ตาม ซึ่งภายหลังของแผนที่ได้วางเป้าหมายหลักไว้คือ การทำงานร่วมกับบริษัทโทรคมนาคมเพื่อปรับปรุงและหาวิธีในการป้องกันการโทรศัพท์ที่ทำการรบกวนประชาชนไม่ว่าวัตถุประสงค์นั้นจะเพื่อทำการตลาดขายผลิตภัณฑ์หรือเพื่อหลอกลวงประชาชนก็ตาม ในส่วนของประเทศไทยสำนักงานตำรวจแห่งชาติได้มีการเรียกผู้มีเกี่ยวข้องในเรื่องต่างๆ ไม่ว่าจะเป็น ธนาคารแห่งประเทศไทยและตัวแทนธนาคารต่างๆ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ตัวแทนจากบริษัทผู้ให้บริการโทรคมนาคม และหน่วยงานอื่นๆ รวมไปถึงหน่วยงานหลัก คือสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) ที่มีหน้าที่ความรับผิดชอบโดยตรงเกี่ยวกับอุตสาหกรรมโทรคมนาคมและมีอำนาจในการบังคับใช้กฎเกณฑ์ต่างๆ เข้ามาร่วมกันหารือแนวทางแก้ไขปัญหาแก๊งคอลเซ็นเตอร์อยู่หลายครั้ง ซึ่งส่วนใหญ่จะทำเป็นลักษณะของข้อตกลงร่วมกัน (MOU) และประเทศไทยจะเน้นการที่ภาครัฐขอความร่วมมือกับภาคเอกชนเสียมากกว่า

จะเห็นได้ว่า ในประเทศไทยการที่ให้ภาคส่วนที่เกี่ยวข้องได้เข้ามาหารือร่วมกันโดยมีลักษณะเป็น การทำข้อตกลงร่วมกัน (MOU) นั้นและมีลักษณะเป็นการขอความร่วมมือซึ่งอาจจะไม่สามารถใช้บังคับได้อย่างเต็มที่เนื่องจากการทำข้อตกลงร่วมกัน (MOU) มีลักษณะที่ไม่มีผลบังคับตามกฎหมายประกอบกับประเทศไทยไม่ได้มีการวางแผนปฏิบัติการอย่างเป็นรูปธรรมเหมือนประเทศออสเตรเลียและประเทศสหราชอาณาจักรจึงไม่สามารถติดตามและวัดผลเพื่อที่จะนำมาปรับปรุงข้อกำหนดหรือวางแผนบังคับใช้ในการป้องกันได้อย่างมีประสิทธิภาพ

(2) การจัดตั้งหน่วยงานรับเรื่องร้องเรียนแบบ One Stop Service

จากการศึกษาของผู้วิจัยพบว่า ในประเทศออสเตรเลียภาครัฐได้เล็งเห็นถึงความสำคัญของระบบเทคโนโลยีเพื่อเฝ้าระวังการหลอกลวงดังนั้นจึงได้มีการจัดทำเว็บไซต์ Scamwatch โดยภายในเว็บไซต์ Scamwatch จะบอกรายละเอียดของการหลอกลวงแต่ละประเภทเพื่อส่งเสริมการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับ

การหลอกลวงของแก๊งมิจฉาชีพรวมถึงด้านอื่นๆของการคุ้มครองผู้บริโภคและมีช่องทางและขั้นตอนการร้องเรียนต่างๆ ซึ่งประชาชนสามารถทำการสอบถามหรือทำการรายงานได้ตลอด 24 ชั่วโมง และยังมีตัวเลขสรุปรายงานทั้งจำนวนครั้งที่มีการรายงานเข้ามาโดยเป็นจำนวนตัวเลขของความเสียหายที่มีการอัพเดตแบบทันที (real time) ซึ่งทำให้ประชาชนได้เข้าถึงการรับรู้ของการถูกหลอกลวงได้ทันท่วงที นอกจากนี้ Scamwatch มีหน้าที่รายงานตัวเลขของประชาชนที่ถูกหลอกลวงเป็นประจำทุกปีเพื่อที่จะนำตัวเลขนั้นไปหารือและนำไปสู่การปรับปรุงแผนปฏิบัติการป้องกันหรือบทกฎหมายต่างๆให้ทันกับกลุ่มมิจฉาชีพ ในส่วนของประเทศสหราชอาณาจักร ได้มีการจัดทำเว็บไซต์ที่ใช้รายงานการหลอกลวงรูปแบบต่างๆเช่นเดียวกัน คือ Action Fraud และภายในเว็บไซต์มีลักษณะที่คล้ายคลึงกับ Scamwatch โดยประชาชนสามารถศึกษารูปแบบการหลอกลวงรวมไปถึงการแจ้งรายงานได้ทันที ในส่วนของประเทศไทยได้มีการเปิดเว็บไซต์ https://www.thaipoliceonline.com/ ให้ประชาชนได้เข้าไปรายงานซึ่งเว็บไซต์ดังกล่าวอยู่ภายใต้การดูแลของสำนักงานตำรวจแห่งชาติที่จะทำการรับเรื่องการแจ้งความออนไลน์คดีอาชญากรรมทางเทคโนโลยีไว้

จะเห็นได้ว่า ในประเทศออสเตรเลียและประเทศสหราชอาณาจักรถ้าเทียบกับประเทศไทยแล้ว มีวิธีการรับเรื่องร้องเรียนที่คล้ายกันแต่แตกต่างตรงที่ในประเทศออสเตรเลียและประเทศสหราชอาณาจักร ประชาชนสามารถรายงานเหตุการณ์อาชญากรรมได้ตั้งแต่การพบความผิดปกติหรือสงสัยว่าตนจะถูกหลอกลวงไปจนถึงหลังจากที่โดนมิจฉาชีพหลอกลวงแล้ว แต่ในประเทศไทยการแจ้งความดังกล่าวจะต้องเป็นกรณีที่ประชาชนถูกหลอกลวงไปแล้วเท่านั้น นอกจากนี้การรายงานของประชาชนที่รายงานไปในเว็บไซต์ของ Scamwatch และ Action Fraud จะถูกบันทึกสถิติแล้วนำสถิตินั้นมาวิเคราะห์หาแนวทางป้องกันให้กับอุตสาหกรรมโทรคมนาคมที่เหมาะสมเพิ่มเติมจากแผนปฏิบัติการหรือกฎหมายที่มีอยู่ในปัจจุบัน แต่ในส่วนของการแจ้งความของประเทศไทยเป็นการแจ้งความเพื่อรอทางเจ้าหน้าที่ตำรวจไปจับกุมเท่านั้นโดยที่ไม่ได้นำตัวเลขของการแจ้งความมาปรับปรุงหรือหาแนวทางในการป้องกันที่เหมาะสมแต่อย่างใด

(3) การแบ่งปันข้อมูลระหว่างหน่วยงาน

นอกจากเรื่องระบบเทคโนโลยีเพื่อเฝ้าระวังการหลอกลวงที่ภาครัฐได้เล็งเห็นถึงความสำคัญแล้ว ในส่วนของประเทศออสเตรเลีย ทางภาครัฐได้เล็งเห็นความสำคัญของการเชื่อมโยงฐานข้อมูลหมายเลขโทรศัพท์ที่กระทำความผิดระหว่างภาครัฐกับฐานข้อมูลของภาคเอกชนเพื่อร่วมกันแก้ไขปัญหาอย่างบูรณาการและทันท่วงทีโดยหลังจากที่มีการบังคับใช้ Reducing Scams Call Industry Code ตามที่ได้กล่าวไปในบทที่ 4 ข้างต้น ผู้ให้บริการโทรคมนาคมรายต่างๆในออสเตรเลียสามารถแชร์ข้อมูลหมายเลขโทรศัพท์ที่ทำการหลอกลวงประชาชนระหว่างกันได้โดยไม่ผิดกฎหมายเรื่องการแชร์ข้อมูลส่วนบุคคลเนื่องจากมีข้อยกเว้นอยู่ในมาตรา 116A ของ Telecommunication Act 1997 และสามารถเชื่อมฐานข้อมูลกับหน่วยงานภาครัฐได้อย่างทันท่วงทีทำให้หลังจากมีการบังคับใช้ Industry Code ดังกล่าวหนึ่งในบริษัทของผู้ให้บริการโทรคมนาคมคือบริษัท Telcos ได้ออกมาเปิดเผยว่าสามารถทำการปิดกั้นการใช้งานหมายเลขโทรศัพท์ที่ทำการหลอกลวงได้ถึง 55 ล้านครั้งที่ดำเนินการผ่านหมายเลขโทรศัพท์ในประเทศออสเตรเลียซึ่งถือว่าเป็นตัวเลขที่สูงมาก ในประเทศสหราชอาณาจักร มีการแบ่งปันข้อมูลระหว่างผู้ให้บริการโทรคมนาคมด้วยกันรวมไปถึงประเทศพันธมิตรของสหราชอาณาจักรและหน่วยงานภาครัฐเพื่อให้การตรวจสอบข้อมูลเป็นไปอย่างรวดเร็วและมีประสิทธิภาพในการจับกุม ในประเทศไทยยังไม่มีแนวคิดในการแบ่งปันข้อมูลเบอร์โทรศัพท์ที่ทำการหลอกลวงระหว่างผู้ให้บริการโทรคมนาคมด้วยกันเองและยังไม่มีระบบเชื่อมต่อไปยังฐานข้อมูลของภาครัฐ มีเพียงแต่การทำงานแยกเป็นหน่วยงานอิสระ เช่น เมื่อประชาชนต้องการที่จะแจ้งเบาะแสหมายเลขโทรศัพท์ของแก๊งคอลเซ็นเตอร์หรือต้องการให้มีการปิดกั้นการใช้งานหมายเลขโทรศัพท์ดังกล่าว ประชาชนจะต้องโทรเข้าเบอร์แจ้งเหตุที่แต่ละค่ายมือถือจัดเตรียมไว้หลังจากนั้นค่ายมือถือดังกล่าวต้องทำการตรวจสอบข้อมูล หากพบว่าเป็นแก๊งคอลเซ็นเตอร์ค่ายมือถือเหล่านั้นจะทำการปิดกั้นการใช้งานหมายเลขโทรศัพท์และส่งข้อมูลให้กับเจ้าหน้าที่ตำรวจต่อไป

ดังนั้นจึงจะเห็นได้ว่ากระบวนการตรวจสอบ ติดตามและปิดกั้นการใช้งานหมายเลขโทรศัพท์ของประเทศไทยยังต้องทำเป็นขั้นตอนและใช้ระยะเวลาซึ่งไม่สามารถตอบโจทย์ให้ไปกับอาชญากรรมทางเทคโนโลยีที่เกิดขึ้นในปัจจุบันได้

5.2 บทวิเคราะห์และเปรียบเทียบการบังคับใช้กฎหมายเพื่อป้องกันแก๊งคอลเซ็นเตอร์ของประเทศออสเตรเลียและประเทศสหราชอาณาจักรเปรียบเทียบกับประเทศไทย

จากการที่ผู้วิจัยได้ทำการศึกษากฎหมายที่เกี่ยวข้องกับการป้องกันหมายเลขโทรศัพท์ที่นำมาใช้แบบผิดกฎหมายว่าแต่ละประเทศมีการบังคับใช้กฎหมายเพื่อป้องกันการนำหมายเลขโทรศัพท์ไปใช้ในทางที่ผิดกฎหมายอย่างไรพบว่าการบังคับใช้กฎหมายของประเทศไทยเมื่อนำมาเปรียบเทียบกับประเทศออสเตรเลียและประเทศ สหราชอาณาจักรมีลักษณะคล้ายกันในบางส่วนและข้อแตกต่างที่เป็นสาระสำคัญอยู่บ้าง ซึ่งสามารถสรุปสาระสำคัญได้ดังต่อไปนี้

(1) การให้อำนาจองค์กรอิสระในการกำกับดูแลกิจการโทรคมนาคม

โดยส่วนที่มีความคล้ายกันคือแต่ละประเทศมีกฎหมายให้อำนาจหน่วยงานกำกับดูแลไว้เพื่อให้องค์กรนั้นทำหน้าที่เป็นหน่วยงานที่มีหน้าที่กำกับดูแลที่เป็นอิสระต่อผู้ให้บริการโทรคมนาคมเนื่องจากกระแสผลักดันที่ทำให้เกิดหน่วยงานกำกับดูแลตามข้อกำหนดที่ 5 ในเอกสารอ้างอิงขององค์การการค้าโลก (WTO Reference Paper) ซึ่งระบุให้หน่วยงานกำกับดูแลต้องแยกออกจากผู้ให้บริการโทรคมนาคมพื้นฐานและไม่ต้องมีความรับผิดต่อผู้ให้บริการโทรคมนาคมรายใดรายหนึ่งเป็นพิเศษรวมถึงการออกกฎเกณฑ์ที่ใช้บังคับกับผู้ให้บริการโทรคมนาคมเหล่านั้น นอกจากนี้การบังคับใช้กฎหมายเพื่อป้องกันการถูกหลอกจากมิจฉาชีพของประเทศไทยมีลักษณะค่อนข้างที่จะคล้ายคลึงกับประเทศออสเตรเลียมากกว่าประเทศสหราชอาณาจักรเนื่องจากประเทศไทยและประเทศออสเตรเลียมีบทกฎหมายได้ให้อำนาจหน่วยงานไว้เพื่อออกเป็นกฎเกณฑ์ใช้บังคับกับผู้ให้บริการโทรคมนาคมจะต้องปฏิบัติตามกฎหรือคำสั่งในเรื่องต่างๆ ถ้าหากไม่ปฏิบัติตามจะมีบทลงโทษ ซึ่งบทลงโทษดังกล่าวจะมีลักษณะเพื่อเป็นการยับยั้งและป้องกันเนื่องจากต้องการให้ผู้ให้บริการโทรคมนาคมปฏิบัติตามกฎเกณฑ์อย่างเคร่งครัด แต่ในทางกลับกัน การกำกับดูแลของหน่วยงานที่มีอำนาจในการออกกฎเกณฑ์และบังคับใช้กับผู้ให้บริการเครือข่ายของประเทศสหราชอาณาจักรจะเน้นการ

ไม่เข้าไปแทรกแซงเว้นเสียแต่ว่าเรื่องที่ต้องแทรกแซงเป็นเรื่องที่จำเป็นจริงๆ กล่าวคือ เน้นการขอความร่วมมือและความสมัครใจ เช่น การใช้อำนาจของ Ofcom กับผู้ให้บริการโทรคมนาคมโดยผู้ให้บริการโทรคมนาคมจะต้องดำเนินการตามขั้นตอนที่เหมาะสมในการตรวจสอบและระบุหมายเลขโทรศัพท์ที่ทำการหลอกลวง แต่ขั้นตอนดังกล่าวให้ขึ้นอยู่กับผู้ให้บริการโทรคมนาคมแต่ละรายในการกำหนด เป็นต้น จึงทำให้บทลงโทษในแผนปฏิบัติการของประเทศสหราชอาณาจักรจะเน้นไปที่ตัวผู้ที่กระทำการนำหมายเลขโทรศัพท์มาใช้ในการหลอกลวงหรือก่อกวนโดยกำหนดบทลงโทษได้สูงถึง 2 ล้านปอนด์ซึ่งการลงโทษลักษณะดังกล่าวเป็นการลงโทษที่มุ่งที่จะตอบแทนหรือทดแทนการกระทำความผิดในอดีตโดยมองถึงการกระทำและเป็นการป้องกันไม่ให้มีการกระทำความผิดเกิดขึ้นซ้ำอีกในอนาคต ตามแนวความคิดของทฤษฎีการลงโทษเพื่อเป็นการตอบแทนแก้แค้น

(2) การพิสูจน์และยืนยันตัวตน

เนื่องจากแก๊งคอลเซ็นเตอร์มักใช้หมายเลขโทรศัพท์เป็นเครื่องมือในการก่ออาชญากรรมการดังนั้นการพิสูจน์และยืนยันตัวตนก่อนการเปิดใช้หมายเลขโทรศัพท์หรือการพิสูจน์ยืนยันตัวตนก่อนที่จะมีการย้ายผู้ให้บริการโทรคมนาคมถือเป็นสิ่งสำคัญอย่างยิ่งเนื่องจากจะทำให้รู้ว่าเจ้าของหมายเลขโทรศัพท์ที่แท้จริงมีตัวตนจริงหรือไม่ ดังนั้นการออกกฎเกณฑ์บังคับใช้ดังกล่าวจึงตกอยู่กับหน่วยงานกำกับดูแล โดยประเทศไทยได้ออกประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติในเรื่องการพิสูจน์ยืนยันตัวตนก่อนเปิดใช้หมายเลขโทรศัพท์รวมไปถึงการย้ายหมายเลขโทรศัพท์ด้วยเพื่อเป็นแนวทางการปฏิบัติให้กับผู้ให้บริการโทรคมนาคมจะต้องปฏิบัติตามและหากไม่ปฏิบัติตามก็จะมีโทษทางปกครองที่ได้ทำการกล่าวไว้ในบทที่3 ในขณะเดียวกันประเทศออสเตรเลียก็มีการออกกฎเกณฑ์ที่ใช้บังคับให้ผู้ให้บริการโทรคมนาคมต้องปฏิบัติในการยืนยันตัวตนของลูกค้าก่อนที่จะทำการเปิดหมายเลขโทรศัพท์เช่นเดียวกันซึ่งถ้าไม่ปฏิบัติตามก็จะมีบทลงโทษทางแพ่งที่จะต้องขึ้นอยู่กับศาลวินิจฉัยว่าการไม่ปฏิบัติตามกฎนั้นมีผลกระทบร้ายแรงหรือไม่อย่างไร เนื่องจากประเทศออสเตรเลียเป็นประเทศที่ใช้ระบบกฎหมายจารีตประเพณี

(Common law) และในประเทศ สหราชอาณาจักร การออกหมายเลขโทรศัพท์ใหม่ผู้ให้บริการโทรคมนาคมจะต้องดำเนินการตามให้เป็นไปตามข้อกำหนด The National Telephone Numbering Plan ซึ่งเป็นการบอกว่าหมายเลขโทรศัพท์ที่จะทำการออกต้องประกอบด้วยองค์ประกอบอะไรบ้างและในส่วนของการย้ายหมายเลขโทรศัพท์บ้านจากผู้ให้บริการโทรคมนาคมรายหนึ่งไปอีกรายหนึ่งหรือการย้ายตำแหน่ง ทาง Ofcom ได้ยืนยันการให้ผู้ให้บริการโทรคมนาคมพัฒนาและดำเนินการกระบวนการ One Touch Switch Process เพื่อแทนที่ขั้นตอนการแจ้งการโอนย้ายที่มีอยู่ในปัจจุบันและต้องการลดขั้นตอนโดยมุ่งเน้นการอำนวยความสะดวกให้กับผู้ใช้บริการซึ่งจะมีผลบังคับใช้ในปี 2023 ในส่วนของโทรศัพท์มือถือจะมีการใช้ Auto-Switch Process และมีผลบังคับใช้ในปี 2023 เช่นเดียวกัน

จากการที่ทางผู้วิจัยได้ทำการวิเคราะห์หลักการพิสูจน์และยืนยันตัวตนของประเทศไทยเปรียบเทียบกับประเทศออสเตรเลียและประเทศสหราชอาณาจักรแล้ว พบประเด็นที่เกิดขึ้นดังนี้

1. หลักเกณฑ์ดังกล่าวตามประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่ไม่ได้มีวัตถุประสงค์ในการจัดทำเพื่อป้องกันการโทรหลอกลวงโดยตรงเหมือนหลักเกณฑ์ของออสเตรเลีย แต่หลักเกณฑ์ของประเทศไทยมีไว้เพื่อคุ้มครองผลประโยชน์ของผู้ใช้บริการเมื่อผู้ใช้บริการต้องการเปลี่ยนผู้ให้บริการหรือประเภทบริการเพื่อเป็นการส่งเสริมการให้บริการโทรคมนาคมและเกิดการแข่งขันอย่างเสรีและเป็นธรรมเหมือนกับประเทศสหราชอาณาจักรกล่าวคือผู้ให้บริการไม่สามารถทำการขัดขวางผู้ใช้บริการในการดำเนินการย้ายเครือข่ายได้ แม้ว่าประกาศดังกล่าวผู้ให้บริการรายใหม่จะต้องทำการยืนยันตัวตนก็ตาม ในขณะที่ประเทศออสเตรเลียมีวัตถุประสงค์ในการยืนยันตัวตนของลูกค้าอย่างชัดเจน คือ ป้องกันการโอนย้ายหมายเลขโทรศัพท์โดยไม่ได้รับอนุญาตประกอบและเน้นการลดปริมาณการหลอกลวงและการฉ้อโกงใน

การโอนย้ายอุปกรณ์เคลื่อนที่ ดังนั้นด้วยเหตุผลดังกล่าวอาจจะทำให้เกิดการละเลยการปฏิบัติหน้าที่ของผู้ให้บริการโทรคมนาคมในไทยได้เนื่องจากเห็นว่าเป็นเรื่องไม่สำคัญ เช่น ประเทศไทยสามารถส่งซิมการ์ดให้กับลูกค้าเพื่อทำการยืนยันตัวตนด้วยตนเองได้แต่ทางผู้ให้บริการโทรคมนาคมต้องกำหนดวิธีการยืนยันตัวตนดังกล่าวประกอบไปด้วย โดนวิธีการนั้นต้องผ่านการอนุมัติจาก กสทช. ซึ่งทางผู้วิจัยมองว่าอาจจะมีความเสี่ยงที่เกิดขึ้นจากการให้ลูกค้าทำการยืนยันตัวตนด้วยตนเอง เป็นต้น

2. นอกจากนี้ในประเทศไทย ประชาชน 1 คนสามารถมีหมายเลขโทรศัพท์ได้มากกว่า 1 หมายเลขแต่ไม่เกิน 5 หมายเลขโทรศัพท์ต่อหนึ่งเครือข่ายซึ่งแตกต่างจากประเทศออสเตรเลียว่า ถ้าพบประชาชนมีหมายเลขโทรศัพท์ในฐานข้อมูลที่ให้ไว้กับทางราชการต่างๆมากกว่าหนึ่งหมายเลข กรณีนี้ผู้ให้บริการโทรคมนาคมจะต้องทำการตรวจสอบและ<u>ใช้บริการตรวจสอบออนไลน์ของทางรัฐบาลเพื่อยืนยัน</u>ว่าบุคคลที่ยื่นคำขอเป็นผู้ถือสิทธิ์ในการใช้งานจริงๆ และหมายเลขโทรศัพท์ที่ระบุในเอกสารราชการที่ไม่ซ้ำกันอย่างน้อยสองฉบับนั้นจะถูกตรวจสอบในบริการตรวจสอบออนไลน์ของรัฐบาลเป็นการสะท้อนให้เห็นว่าทางภาครัฐของออสเตรเลียมีระบบการจัดเก็บหมายเลขโทรศัพท์ที่ทำการเชื่อมโยงระหว่างภาครัฐและผู้ให้บริการโทรคมนาคมซึ่งถือเป็นหน่วยงานภาคเอกชนและมีการเพิ่มระบบเทคโนโลยีเพื่อเฝ้าระวังการหลอกลวงที่สามารถทำได้ตามช่องทางต่างๆ ไม่ว่าจะเป็น ข้อความ หรือ โทรศัพท์ รวมไปถึงแอปพลิเคชัน โดยเฉพาะการปรับปรุงขั้นตอนการร้องเรียนให้รวดเร็วและสะดวกยิ่งขึ้นและทำให้ผู้บริโภคเข้าถึงความช่วยเหลือต่าง ๆ ประกอบกับจุดอ่อนของประเทศไทยคือระบบการทำงานแยกส่วนซึ่งทำให้ล่าช้ากว่าที่ควรจะเป็นและเป็นการเปิดช่องให้กลุ่มมิจฉาชีพมีเวลาในการหลบเลี่ยงการถูกจับกุม

(3) การตรวจจับ ติดตาม และปิดกั้นการใช้งานหมายเลขโทรศัพท์ รวมไปถึงการแชร์ข้อมูลระหว่างกัน

เนื่องจากทางภาครัฐของประเทศออสเตรเลียและประเทศสหราชอาณาจักรได้เล็งเห็นถึงปัญหาที่อาจจะเกิดขึ้นจึงทำการสนับสนุนให้เกิดการเชื่อมโยงกับฐานข้อมูลระหว่างภาครัฐและภาคเอกชน ในประเทศออสเตรเลียการเล็งเห็นปัญหาดังกล่าวทำให้เกิดการบังคับใช้ Reducing Scams Call Industry Code โดยเน้นการให้ผู้ให้บริการโทรคมนาคมจะต้องตรวจสอบและตรวจจับการรับส่งข้อมูลการโทรหลอกลวงบนเครือข่ายของตน โดยเฉพาะอย่างยิ่งเน้นการแบ่งปันข้อมูลของหมายเลขโทรศัพท์ที่ทำการหลอกลวงกับผู้ให้บริการโทรคมนาคมรายอื่นและหน่วยงานภาครัฐที่เกี่ยวข้องรวมไปถึงต้องทำการตรวจสอบ ติดตามและปิดกั้นการใช้งานหมายเลขโทรศัพท์ที่ทำการหลอกลวงให้ได้อย่างทันท่วงที ซึ่งหลังจากการประกาศใช้ดังกล่าว ทางผู้ให้บริการโทรคมนาคมก็สามารถทำการปิดกั้นการใช้งานหมายเลขโทรศัพท์ที่มีความเสี่ยงเป็นมิจฉาชีพได้เป็นจำนวนมาก ในประเทศ สหราชอาณาจักร ทางภาครัฐมีการทำงานร่วมกับผู้ให้บริการโทรคมนาคมโดยจัดตั้งเป็นคณะทำงาน ซึ่งเป็นหนึ่งในแผนปฏิบัติการเพื่อป้องกันการโทรหลอกลวงที่รบกวนประชาชนโดยมีการแบ่งปันข้อมูลระหว่างกันรวมไปถึงพันธมิตรระหว่างประเทศของสหราชอาณาจักรด้วย ในส่วนของประเทศไทยยังไม่ได้ออกกฎเกณฑ์เกี่ยวกับเรื่องดังกล่าวอย่างชัดเจน การตรวจจับ ติดตามและปิดกั้นการใช้งานหมายเลขโทรศัพท์ยังเป็นหน้าที่หลักของผู้บริโภคที่จะต้องเตือนสติตัวเองอยู่เสมอว่าหมายเลขที่ทำการโทรเข้ามาเป็นหมายเลขจริงหรือหมายเลขปลอมแม้ว่าในปัจจุบันจะมีแอปพลิเคชัน Whocalls ที่ช่วยกรองว่าหมายเลขโทรศัพท์ว่าเป็นหมายเลขของมิจฉาชีพหรือไม่แต่การจะค้นหาเบอร์ดังกล่าวก็ยังเป็นหน้าที่ของผู้บริโภคและถ้าจะทำการปิดกั้นการใช้งานหมายเลขนั้นก็ต้องอัพเกรดและเสียค่าใช้จ่ายในแอปพลิเคชันนั้นด้วยตนเอง แต่ก็ยังมีอีกทางหนึ่งที่ผู้บริโภคไม่ต้องเสียค่าใช้จ่ายในการปิดกั้นการใช้งานหมายเลขนั่นคือการโทรไปหาผู้ให้บริการโทรคมนาคมที่ตนใช้บริการอยู่และทำการแจ้งว่าจะทำการปิดกั้นการใช้งานหมายเลขซึ่งผู้ให้บริการโทรคมนาคมดังกล่าวก็ต้องทำการตรวจสอบรายละเอียดของหมายเลขนั้นก่อนที่จะปิดกั้นการใช้งานได้ ทำให้เห็นว่าระบบในประเทศไทยยังไม่ดีเท่าที่ควรเนื่องจากมีขั้นตอนการตรวจสอบ การแจ้ง และการปฏิบัติการอยู่มาก

ทำให้กว่าจะจับมิจฉาชีพได้ก็หนีไปเสียแล้ว รวมไปถึงระบบฐานข้อมูลยังไม่มีการรวมเป็นฐานข้อมูลเดียวซึ่งทำให้ยากต่อการตรวจสอบมากเนื่องจากต่างค่ายต่างก็มีเบอร์แจ้งเหตุที่แตกต่างกันออกไปดังรูปภาพที่11

รูปภาพที่ 11[120] เปิดช่องทางการแจ้ง ครบทุกค่ายมือถือ ใช้บล็อกเบอร์แก๊งคอลเซ็นเตอร์ ตร. จับมือผู้ให้บริการเครือข่ายโทรศัพท์มือถือ เปิดสายด่วนแจ้งเบอร์แก๊งคอลเซ็นเตอร์ ปิดกั้นการใช้งาน และดำเนินคดีตามกฎหมาย

[120] เดลินิวส์ ออนไลน์, เปิดช่องทางการแจ้ง ครบทุกค่ายมือถือ ใช้บล็อกเบอร์แก๊งคอลเซ็นเตอร์ ตร. จับมือผู้ให้บริการเครือข่ายโทรศัพท์มือถือ เปิดสายด่วนแจ้งเบอร์แก๊งคอลเซ็นเตอร์ ปิดกั้นการใช้งาน และดำเนินคดีตามกฎหมาย, [ออนไลน์], 2565, แหล่งที่มา https://www.dailynews.co.th/news/985369/ [11 ธันวาคม 2565]

บทที่ 6
บทสรุปและข้อเสนอแนะ

6.1 บทสรุป

เนื่องจากสภาพสังคมของประเทศไทยในปัจจุบันได้มีการอาศัยเทคโนโลยีในการดำรงชีวิตประจำวันมากขึ้นโดยเฉพาะอย่างยิ่งการติดต่อสื่อสารที่มีการพัฒนาและเจริญก้าวหน้าไปอย่างรวดเร็วโดยมีรูปแบบการติดต่อสื่อสารผ่านช่องทางที่หลากหลายจนทำให้เกิดช่องว่างในการหลอกลวงต่างๆมากมาย ซึ่งเป็นปัญหาที่ประเทศไทยประสบในช่วงที่ผ่านมาประกอบกับสถานการณ์โรคระบาดโควิด19เป็นช่วงเวลาที่ประชาชนมีความอ่อนไหวทำให้เหล่ามิจฉาชีพได้ใช้โอกาสนี้ทำการหลอกลวงเหยื่อ ไม่ว่าจะเป็นการลงทุนเพื่อให้ผลตอบแทนที่สูงหรือการหลวงลวงแต่ละรูปแบบที่แตกต่างกันไป การกลับมาระบาดของแก๊งคอลเซ็นเตอร์ในประเทศไทยในครั้งนี้ได้ก่อให้เกิดความเสียหายเป็นวงกว้างและได้สร้างความสูญเสียทางด้านการเงินอย่างมหาศาลอีกครั้ง อีกทั้งไม่เพียงแต่ประเทศไทยที่เจอปัญหากับแก๊งคอลเซ็นเตอร์ดังกล่าว ต่างประเทศก็ประสบปัญหาดังกล่าวเช่นเดียวกัน

จากการค้นคว้ากฎหมายที่เกี่ยวข้องเกี่ยวกับเรื่องแก๊งคอลเซ็นเตอร์ ผู้วิจัยพบว่าในประเทศไทยได้มีการบังคับใช้กฎหมายที่ใช้ในการปราบปรามโดยการกำหนดความผิดทางอาญาและการใช้นโยบายทางอาญาของรัฐแต่ยังไม่รวมถึงมาตรการในการป้องกันอาชญากรรมของภาคส่วนอุตสาหกรรมโทรคมนาคมประกอบกับบริบทต่างๆที่ทำให้การบังคับกฎหมายดังกล่าวยังไม่มีประสิทธิภาพเท่าที่ควรจึงทำให้การบังคับใช้กฎหมายทางอาญาในปัจจุบันไม่สามารถจับกุมและกวาดล้างได้อย่างสมบูรณ์เนื่องจากมิจฉาชีพเหล่านี้มักมีที่อยู่ไม่เป็นหลักแหล่งและรูปแบบการหลอกลวงมีวิธีที่ซับซ้อนมากขึ้นทำให้ยากต่อการสืบสาวต้นตอซึ่งการบังคับใช้บทกฎหมายที่ใช้ในการปราบปรามทางผู้วิจัยมองว่าเป็นการแก้ปัญหาทางปลายเหตุ เนื่องจากบทกฎหมายที่เกี่ยวข้องมักเป็นบทกฎหมายทางอาญา กล่าวคือ การที่จะสามารถลงโทษผู้กระทำความผิดดังกล่าวได้จะต้องเกิดเหตุการณ์ขึ้นแล้วเท่านั้นประกอบกับการลงโทษผู้กระทำผิดจะต้องอาศัยองค์ประกอบของการเกิดเหตุต่างๆเนื่องจากเป็นการลงโทษทางอาญา จะเห็นได้ว่าการที่จะนำตัวผู้กระทำความผิดมาลงโทษแทบจะไม่ได้มีผลอะไรที่ทำให้แก๊งคอลเซ็นเตอร์ลดน้อยลง ดังนั้นประเทศไทยจึงควรหันมาให้ความสำคัญกับการป้องกันและกำกับดูแลก่อนที่จะเกิดเหตุเสียมากกว่าเพราะการหาแนวทางในการ

ป้องกันตั้งแต่ต้นจะสามารถช่วยลดความเสียหายได้ไม่มากก็น้อยและเป็นการสร้างความตื่นตัวให้กับประชาชน (Public Awareness Raising) ในการระมัดระวังแก๊งคอลเซ็นเตอร์ในปัจจุบัน

ปัญหาการจับกุมและการบังคับใช้กฎหมายในการปราบปรามดังกล่าวยังคงเป็นปัญหาหลักของต่างประเทศเช่นเดียวกับประเทศไทย จากการศึกษาของผู้วิจัยพบว่าในต่างประเทศมักจะเน้นการใช้แผนปฏิบัติการเชิงรุกซึ่งภายในแผนปฏิบัติการส่งผลให้มีการบังคับใช้มาตรการทางกฎหมายที่ใช้ในการป้องกันแก๊งคอลเซ็นเตอร์เพื่อที่จะช่วยบรรเทาความเสียหายให้กับประชาชนมากกว่าการเน้นการปราบปรามและวิธีที่จะช่วยการป้องกันได้ดีคือการให้ภาคส่วนอุตสาหกรรมโทรคมนาคมเป็นตัวดักจับความผิดปกติของหมายเลขโทรศัพท์เนื่องจากแก๊งคอลเซ็นเตอร์ส่วนใหญ่มักใช้หมายเลขโทรศัพท์ที่ผิดกฎหมายหรือใช้หมายเลขโทรศัพท์ที่มีการเปิดใช้งานไว้แต่ไม่มีคนใช้งานและอาศัยการใช้เทคโนโลยีในการแปลงหมายเลขและแอบอ้างเป็นหน่วยงานหรือบุคคลที่น่าเชื่อถือหรือใช้หมายเลขโทรศัพท์ผิดกฎหมายที่โทรมาจากต่างประเทศ ดังนั้นถ้าในส่วนของต้นทางคือกิจการโทรคมนาคมสามารถทำการตรวจสอบหรือตรวจพบตั้งแต่แรกจะทำให้ประชาชนเกิดความสูญเสียลดน้อยลง โดยจากการที่ต่างประเทศหันมาสนใจการป้องกันมากกว่าปราบปรามพบว่าสถิติการสูญเสียของประชาชนลดลงอย่างมีนัยสำคัญ ดังเช่น ประเทศสหราชอาณาจักรที่มีการจัดทำและแก้ไขแผนปฏิบัติการทุกปีโดยมีการร่วมมือของภาครัฐและภาคเอกชนในส่วนของอุตสาหกรรมโทรคมนาคมได้ร่วมมือกันในการตรวจสอบหมายเลขโทรศัพท์ประกอบกับมีการแบ่งปันข้อมูลหมายเลขโทรศัพท์ระหว่างหน่วยงานภาครัฐและผู้ให้บริการโทรคมนาคม ในส่วนของประเทศออสเตรเลียที่เน้นกระบวนการป้องกันแก๊งคอลเซ็นเตอร์โดยทางภาครัฐได้เล็งเห็นถึงความสำคัญของปัญหาดังกล่าวจึงได้จัดทำแผนปฏิบัติการอย่างเป็นรูปธรรมเพื่อนำแผนปฏิบัติการนั้นมาใช้วัดผลและปรับปรุง โดยภายใต้แผนปฏิบัติการก่อให้เกิดการออกกฎหมายกำหนดให้ผู้ให้บริการโทรคมนาคมปฏิบัติตามกฎเกณฑ์ที่กฎหมายได้กำหนดเพื่อตรวจสอบและยืนยันตัวตนของเจ้าของหมายเลขโทรศัพท์เหล่านั้นก่อนการเปิดใช้หมายเลขโทรศัพท์หรือการย้ายหมายเลขโทรศัพท์ประกอบกับการกำหนดแนวทางให้หน่วยงานผู้ให้บริการโทรคมนาคมสามารถทำการแบ่งปันข้อมูลหมายเลขโทรศัพท์ที่กระทำผิดรวมไปถึงการเชื่อมต่อกับระบบฐานข้อมูลของภาครัฐซึ่งทำให้กระบวนการตรวจสอบหมายเลขโทรศัพท์ว่าเป็นหมายเลขที่ใช้ในการหลอกลวงหรือไม่ มีความรวดเร็วและส่งผลให้ผู้ให้บริการโทรคมนาคมทำการตรวจจับหมายเลขโทรศัพท์ที่ทำการหลอกลวงได้อย่างทันท่วงทีมากขึ้น ในขณะที่ประเทศไทยไม่ได้มีการออกกฎหมายมาเพื่อใช้บังคับกับผู้ให้บริการโทรคมนาคมในการ

ร่วมกันตรวจสอบหมายเลขโทรศัพท์รวมไปถึงไม่ได้มีการแบ่งปันข้อมูลหมายเลขโทรศัพท์ระหว่างกัน เนื่องจากลักษณะการทำงานของผู้ให้บริการโทรคมนาคมของประเทศไทยเป็นการทำงานแบบอิสระ ทำให้กระบวนการตรวจสอบและตรวจจับหมายเลขยังมีขั้นตอนซึ่งต้องใช้เวลาในการจัดการกับปัญหาดังกล่าว นอกจากนี้ทั้งประเทศสหราชอาณาจักรและประเทศออสเตรเลียต่างก็ได้จัดทำเว็บไซต์ที่มีลักษณะเป็น One Stop Service โดยทำการส่งเสริมและสร้างความตระหนักรู้ให้ประชาชนสามารถเข้ามาศึกษารูปแบบการหลอกลวงประเภทต่างๆ รวมไปถึงสามารถรายงานการหลอกลวงซึ่งเว็บไซต์ดังกล่าวจะทำการประสานงานไปยังภาคส่วนที่เกี่ยวข้องเอง ดังนั้นการออกมาตรการในการบังคับใช้กับผู้ให้บริการโทรคมนาคมเพื่อการป้องกันหมายเลขโทรศัพท์ที่มีความผิดปกติแม้ว่าจะไม่ได้ช่วยลดปริมาณการโทรเข้ามาหลอกลวงประชาชนแต่ช่วยให้ลดความสูญเสียทางด้านการเงินได้อย่างมากเนื่องจากประชาชนได้ตระหนักถึงการหลอกลวงและมีความรู้ในการตัดสินใจว่าหมายเลขโทรศัพท์ดังกล่าวที่โทรเข้ามาเป็นการหลอกลวงหรือไม่

การพิสูจน์และตรวจสอบยืนยันตัวตนของผู้ใช้บริการหมายเลขโทรศัพท์ในประเทศไทยมีการบังคับใช้อยู่ในปัจจุบันโดยอยู่ภายใต้ ประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่ซึ่งอาศัยอำนาจจากมาตรา 27 (7) และ (24) และมาตรา 81 แห่งพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์และกิจการ โทรคมนาคม พ.ศ. 2553 ประกอบกับมาตรา 12 วรรคสี่ แห่งพระราชบัญญัติการประกอบกิจการ โทรคมนาคม พ.ศ. 2544 โดยกรณีที่ผู้ใช้บริการต้องการย้ายเครือข่ายแต่หมายเลขโทรศัพท์เดิมต้องทำการพิสูจน์และตรวจสอบยืนยันตัวตนก่อนที่จะสามารถเปิดใช้หมายเลขโทรศัพท์ดังกล่าวภายใต้การกำกับดูแลของผู้ให้บริการรายใหม่ได้และผู้ให้บริการโทรคมนาคมรายใหม่ต้องจัดให้มีการยืนยันตัวตนทุกครั้ง ซึ่งจุดประสงค์หลักของประกาศดังกล่าวคือรักษาสิทธิของผู้ใช้บริการในการครอบครองและใช้งานหมายเลขโทรศัพท์โดยที่ผู้ให้บริการโทรคมนาคมรายใหม่ไม่สามารถทำการขัดขวางการย้ายค่ายได้ ดังนั้นจะเห็นได้ว่าภายใต้ประกาศเน้นการคุ้มครองสิทธิในการโอนย้ายหมายเลขโทรศัพท์ของผู้ใช้บริการเป็นส่วนใหญ่ โดยที่ไม่ได้มีจุดประสงค์หลักเพื่อคุ้มครองหรือป้องกันการใช้หมายเลขโทรศัพท์ในทางที่ผิดกฎหมายแม้ว่าประกาศฉบับนี้จะมีการให้ผู้ให้บริการโทรคมนาคมรายใหม่ทำการพิสูจน์และยืนยันตัวตนก่อนก็ตามซึ่งทำให้หลักเกณฑ์ในประกาศดังกล่าวที่มีการบังคับใช้ยังไม่เหมาะสมเท่าที่ควร เนื่องจากไม่ได้มีการออกแบบมาเพื่อวัตถุประสงค์ในการป้องกันการหลอกลวงหรือการใช้หมายเลข

โทรศัพท์ในทางที่ผิดซึ่งทำให้ผู้วิจัยมองว่า สามารถเกิดช่องโหว่ในขั้นตอนการยืนยันตัวตนได้ ยกตัวอย่างเช่น กรณีการให้ลูกค้ายื่นคำขอผ่านทางออนไลน์และจัดส่งซิมการ์ดให้ วิธีการดังกล่าวอาจจะมีช่องโหว่เกิดขึ้นในกรณีที่ซิมการ์ดที่ถูกจัดส่งนั้นสูญหายระหว่างทางและอาจทำให้เกิดการสวมสิทธิของหมายเลขโทรศัพท์นั้นได้ เป็นต้น

แม้ว่าประเทศไทยจะมีสำนักงาน กสทช. ที่มีอำนาจทางกฎหมายในการออกประกาศในเรื่องต่างๆเพื่อใช้บังคับกับผู้ให้บริการโทรคมนาคมที่ต้องปฏิบัติตามไม่ว่าจะเป็นเรื่องการพิสูจน์และยืนยันตัวตนหรือเรื่องอื่นๆก็ตาม รวมไปถึงการออกประกาศในการจัดให้มีการตรวจสอบยืนยันตัวตนแต่วัตถุประสงค์หลักของประกาศดังกล่าวคือการรักษาสิทธิของผู้ใช้บริการโดยที่ผู้ให้บริการไม่สามารถขัดขวางได้ซึ่งทำให้ขั้นตอนและวิธีการในการพิสูจน์และยืนยันตัวตนอาจจะยังคงมีช่องโหว่อยู่บ้าง เนื่องจากประกาศฉบับไม่ได้เน้นการป้องกันกรณีที่ผู้บริโภคจะถูกหลอกลวงจากการสวมสิทธิการย้ายหมายเลขโทรศัพท์ ด้วยเหตุนี้ผู้วิจัยจึงเห็นว่าในเมื่อสำนักงาน กสทช. ได้รับอำนาจจากกฎหมายในการออกประกาศแล้ว สำนักงาน กสทช.ควรออกประกาศเกี่ยวกับวิธีการยืนยันตัวตนเพื่อป้องกันการหลอกลวงทางโทรศัพท์โดยเฉพาะแยกเป็นอีกหนึ่งฉบับ เพื่อจะได้นำมาปรับขั้นตอนและวิธีการพิสูจน์ยืนยันตัวตนให้เหมาะสมกับการป้องกันการหลอกลวงทางโทรศัพท์ดังตัวอย่างของประเทศออสเตรเลียที่ได้กำหนดกฎเกณฑ์ในการพิสูจน์และยืนยันตัวตนเพื่อป้องกันการโอนย้ายหมายเลขโทรศัพท์โดยไม่ได้รับอนุญาตและลดอันตรายต่อผู้ใช้บริการที่อาจเกิดจากการย้ายหมายเลขโทรศัพท์โดยไม่ได้รับอนุญาต ทำให้กระบวนการและวิธีการในการพิสูจน์และยืนยันตัวตนมีความชัดเจนและสอดคล้องกับวัตถุประสงค์ นอกจากนี้ควรผลักดันให้สำนักงาน กสทช. กำหนดให้มีการแบ่งปันข้อมูลหมายเลขโทรศัพท์ที่กระทำความผิดระหว่างหน่วยงานภาครัฐที่เกี่ยวข้องและผู้ให้บริการโทรคมนาคมเหมือนประเทศออสเตรเลียและประเทศสหราชอาณาจักร โดยการส่งเสริมการนำเทคโนโลยีมาใช้ในการเชื่อมต่อฐานข้อมูลระหว่างหน่วยงานภาครัฐกับผู้ให้บริการโทรคมนาคมในการตรวจสอบหมายเลขโทรศัพท์เพื่อที่จะได้ทำการตรวจจับหรือปิดกั้นการใช้งานหมายเลขได้อย่างทันท่วงทีและส่งเสริมการร่วมกันทำงานแบบบูรณาการโดยรวมเป็นฐานข้อมูลส่วนกลางไม่แยกส่วนเนื่องจากในปัจจุบันผู้ให้บริการโทรคมนาคมแต่ละเครือข่ายยังคงทำงานแยกเป็นอิสระรวมไปถึงขั้นตอนในการตรวจสอบหมายเลขที่ต้องผ่านกระบวนการและใช้เวลาค่อนข้างมาก ทำให้บางครั้งการปิดกั้นการใช้งานหมายเลขโทรศัพท์เหล่านั้นอาจไม่ทันการ ประกอบกับเพื่อลดความเป็นอิสระของหน่วยงานทั้งภาครัฐและภาคเอกชนให้น้อยลง

6.2 ข้อเสนอแนะ

จากการศึกษาและวิเคราะห์เปรียบเทียบแนวทางการป้องกันแก๊งคอลเซ็นเตอร์ภายใต้กฎหมายที่ให้อำนาจไว้ของประเทศไทยและต่างประเทศแล้ว ทางผู้วิจัยขอเสนอประเด็น ดังต่อไปนี้

1. แนวทางการป้องกันแก๊งคอลเซ็นเตอร์โดยอาศัยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคม

ปัจจุบันประเทศไทยยังไม่มีแนวทางการป้องกันแก๊งคอลเซ็นเตอร์โดยอาศัยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคมที่ชัดเจน ดังนั้นควรหาแนวทางป้องกันในรูปต่างๆ คือ การวางแผนปฏิบัติการที่เป็นรูปธรรม โดยการเร่งผลักดันให้ สำนักงาน กสทช. ซึ่งเป็นหน่วยงานหลักในการรับผิดชอบผู้ให้บริการโทรคมนาคมใช้อำนาจทางกฎหมายที่มีในการจัดทำแผนปฏิบัติการที่เป็นรูปธรรมที่เน้นการมีส่วนร่วมของหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน รวมไปถึงการออกกฎเกณฑ์บังคับใช้กับผู้ให้บริการโทรคมนาคมต่างๆเพื่อนำแผนปฏิบัติการดังกล่าวมาใช้ในการวิเคราะห์ ติดตามผลและปรับปรุงกฎเกณฑ์ให้มีประสิทธิภาพเพิ่มมากขึ้นและเพื่อทำให้การประชุมเกี่ยวกับแก๊งคอลเซ็นเตอร์ไม่เป็นเพียงแค่การทำข้อตกลง (MOU) อีกต่อไป

2. การพิสูจน์และยืนยันตัวตน

ขั้นตอนการพิสูจน์ยืนยันตัวตนก่อนการเปิดใช้หมายเลขโทรศัพท์หรือการย้ายหมายเลขโทรศัพท์ ประเทศไทยควรเลือกประเทศออสเตรเลียเป็นต้นแบบ เนื่องจากมีการกำหนดให้พิสูจน์และยืนยันตัวตนก่อนการเปิดใช้หมายเลขโทรศัพท์หรือการย้ายหมายเลขโทรศัพท์ที่เป็นไปในทางทิศเดียวกัน แต่มีบางประเด็นที่ประเทศไทยยังขาดคือหลักเกณฑ์ที่ไม่เหมาะสมกล่าวคือประเทศไทยยังไม่มีประกาศบังคับใช้ในเรื่องการพิสูจน์การยืนยันตัวตนเพื่อป้องกันหมายเลขโทรศัพท์ที่ทำการหลอกลวงอย่างชัดเจน ทำให้วิธีในการพิสูจน์หรือยืนยันตัวตนที่มีอยู่ในปัจจุบันอาจมีขั้นตอนที่ไม่เหมาะสมและไม่ตอบโจทย์วัตถุประสงค์ในการป้องกันดังกล่าวได้ ประกอบกับความเป็นอิสระของหน่วยงานต่างๆรวมไปถึงความซ้ำซ้อนในหน้าที่ของหน่วยงานภาครัฐ ดังนั้นผู้วิจัยจึงเห็นว่า ในเมื่อกฎหมายได้ให้อำนาจหน่วยงานในการกำกับดูแลแล้วทำไมเราไม่พัฒนากฎเกณฑ์ต่างๆให้เหมาะสมมาก

ยิ่งขึ้นเหมือนประเทศออสเตรเลียโดยการออกประกาศเกี่ยวกับวิธีการพิสูจน์และยืนยันตัวตนเพื่อป้องกันการหลอกลวงทางโทรศัพท์โดยเฉพาะแยกเป็นอีกหนึ่งฉบับเพื่อจะได้นำมาปรับปรุงขั้นตอนและวิธีการพิสูจน์ยืนยันตัวตนให้เหมาะสมกับการป้องกันการหลอกลวงทางโทรศัพท์มากยิ่งขึ้น

3. **ระบบ One Stop Service**

ผลักดันให้ภาครัฐมีการวางระบบที่สามารถทำงานร่วมกันระหว่างรัฐและเอกชนเพื่อผู้บริโภคได้อย่างมีประสิทธิภาพโดยจัดทำระบบที่มีลักษณะเป็น One Stop Service ดังเช่นระบบ Scamwatch ของประเทศออสเตรเลียและระบบ Action Fraud ของประเทศสหราชอาณาจักรซึ่งภายในเว็บไซต์จะมีรวบรวมข้อมูลด้านการหลอกลวงรูปแบบต่างๆไม่จำเป็นแค่ว่าต้องเป็นแก๊งคอลเซ็นเตอร์เท่านั้นซึ่งหมายถึง ประชาชนสามารถเข้ามาศึกษาวิธีการหลอกลวงรูปแบบต่างๆ รวมไปถึงการรายงานและแจ้งความผิดปกติภายในเว็บไซต์ได้ทันทีและระบบจะทำการส่งเรื่องไปยังหน่วยงานที่เกี่ยวข้องเอง นอกจากนี้ประชาชนยังสามารถรายงานการหลอกลวงได้ทั้งก่อนเกิดเหตุคือตั้งแต่ที่มีการสงสัยว่าอาจจะถูกหลอกและหลังเกิดเหตุที่เกิดขึ้นแล้ว เนื่องจากระบบแจ้งเหตุที่ใช้ในประเทศไทยในปัจจุบันเป็นเพียงการแจ้งความหลังจากเกิดเหตุการณ์ขึ้นแล้วเท่านั้น

4. **การตรวจจับ ติดตาม ปิดกั้นการใช้งาน รวมถึงการแบ่งปันข้อมูลหมายเลขโทรศัพท์ที่มีการโทรหลอกลวง**

ผลักดันให้ภาครัฐส่งเสริมการนำเทคโนโลยีมาใช้ในการเชื่อมต่อฐานข้อมูลหมายเลขโทรศัพท์ที่กระทำความผิดระหว่างภาครัฐกับผู้ให้บริการโทรคมนาคมเหมือนประเทศออสเตรเลียและประเทศสหราชอาณาจักร โดยสามารถแบ่งปันข้อมูลหมายเลขโทรศัพท์ที่กระทำความผิดระหว่างหน่วยงานที่เกี่ยวข้องในการตรวจสอบหมายเลขโทรศัพท์เพื่อที่จะได้ทำการตรวจจับหรือปิดกั้นการใช้งานหมายเลขได้อย่างทันท่วงทีและส่งเสริมการร่วมกันทำงานระหว่างภาครัฐและเอกชนแบบบูรณาการโดยรวมเป็นฐานข้อมูลส่วนกลางไม่แยกส่วนเพื่อการตรวจสอบ ตรวจจับ ติดตาม และปิดกั้นการใช้งานเบอร์โทรศัพท์ที่มีการโทรหลอกลวง

บรรณานุกรม

7HDร้อนออนไลน์. ผบ.ตร. นัดถกหน่วยงานภาครัฐและเอกชน ร่วมมือออกมาตรการจัดการแก๊งคอลเซ็นเตอร์.[ออนไลน์]. 2565. แหล่งที่มา: https://news.ch7.com/detail/569172 [9 พฤศจิกายน 2565]

ข่าวช่อง 8. ด่าทอ ให้ร้าย ผ่านโซเชียล อันดับ 1 อาชญากรรมไซเบอร์ปี 64. [ออนไลน์]. 2565. แหล่งที่มา:https://www.thaich8.com/news_detail/104021 [11 พฤษภาคม 2565]

ข่าวเศรษฐกิจ. กสทช.ฟัน ‘ค่ายมือถือ’ วันละล้านไร้น้ำยาปราบคอลเซ็นเตอร์. [ออนไลน์]. 2565. แหล่งที่มา: https://www.bangkokbiznews.com/business/1014117 [27 พฤศจิกายน 2565]

ข่าวอาชญากรรม. ขยายผลจับ "นายทุนจีน" ปลอมบัตร ปชช.ไทย ล่าสุดพบ เอี่ยว "แก๊งคอลเซ็นเตอร์". [ออนไลน์].2565. แหล่งที่มา:https://www.komchadluek.net/news/crime/535195 [30 พฤศจิกายน 2565]

จิตสุภา ฤทธิผลิน. ทิศทางและนโยบายการกำกับดูแลกิจการกระจายเสียง และกิจการโทรทัศน์ในยุคของการหลอมรวมสื่อ : กรณีศึกษาเปรียบเทียบยุทธศาสตร์ ของ FCC และ OFCOM, วิทยานิพนธ์ของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ, 2560.

ชนัญสรา อรนพ ณ อยุธยา และ พิมลพรรณ ไชยนันท์. โครงการพัฒนาและส่งเสริมแนวทางการกำกับดูแลกันเองขององค์กรวิชาชีพ ด้านกิจการกระจายเสียงและกิจการโทรทัศน์, วิทยานิพนธ์ของศูนย์ศึกษานโยบายสื่อ คณะนิเทศศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2559.

โชคสุข กรกิตติชัย. สหราชอาณาจักรบริเตนใหญ่และไอร์แลนด์เหนือ กับการป้องกันและปราบปรามการทุจริต. เอกสารวิชาการอิเล็กทรอนิกส์ สำนักวิชาการ สำนักงานเลขาธิการสภาผู้แทนราษฎร (สิงหาคม 2565):13.

ณัฐฐ์วัฒน์ สุทธิโยธิน. กฎหมายอาญาและอาชญาวิทยาชั้นสูง ทฤษฎีการลงโทษ หน่วยที่6 สาขาวิชานิติศาสตร์.กรุงเทพมหานคร : มหาวิทยาลัยสุโขทัยธรรมาธิราช.

เดลินิวส์ ออนไลน์. เปิดช่องทางการแจ้ง ครบทุกค่ายมือถือ ใช้บล็อกเบอร์แก๊งคอลเซ็นเตอร์ ตร. จับมือผู้ให้บริการเครือข่ายโทรศัพท์มือถือ เปิดสายด่วนแจ้งเบอร์แก๊งคอลเซ็นเตอร์ ปิดกั้นการใช้งาน และดำเนินคดีตามกฎหมาย. [ออนไลน์]. 2565. แหล่งที่มา: https://www.dailynews.co.th/news/985369/ [11 ธันวาคม 2565]

ทัน LINE ไทยคู่ฟ้า. ครม. ไฟเขียว ร่าง MOU ไทย – กัมพูชา ผนึกกำลังปราบแก๊ง Call Center และ Hybrid Scam ข้ามแดน. [ออนไลน์]. 2565.แหล่งที่มา: https://www.thaigov.go.th/news/contents/details/56680 [11 ตุลาคม 2565]

ทีมพัฒนาและวิเคราะห์ข้อมูล ฝ่ายนโยบายระบบการชำระเงิน. Financial Fraud : กลโกงทางการเงินใกล้ตัวกว่าที่คิด. [ออนไลน์]. 2565. แหล่งที่มา: https://www.bot.or.th/Thai/PaymentSystems/Publication/payment_insight/Documents/Bi-monthly_report_Vol14-2022_April.pdf [30 ตุลาคม 2565]

ไทยรัฐออนไลน์. รพ.สระบุรีโดนมัลแวร์เรียกค่าไถ่ ระบบคอมฯ พัง ต้องซักประวัติใหม่ทำล่าช้า. [ออนไลน์]. 2563. แหล่งที่มา: https://www.thairath.co.th/news/local/central/1926639 [22 [10 มีนาคม 2565]

ไทยรัฐออนไลน์. หวัง PDPA ลดแก๊งคอลเซ็นเตอร์. [ออนไลน์]. 2565. แหล่งที่มา https://www.thairath.co.th/business/economics/2429726 [22 ตุลาคม 2565]

บรรณศักดิ์ ยุวมิตร. Phishing คืออะไร ป้องกันอย่างไร. [ออนไลน์]. 2563. แหล่งที่มา: https://www.cyfence.com/article/what-is-phishing/ [10 มีนาคม 2565]

บรรณศักดิ์ ยุวมิตร. Phishing คืออะไร. [ออนไลน์]. 2564. แหล่งที่มา: https://www.cyfence.com/article/what-is-phishing/ [1 มิถุนายน 2565]

ปฐมพงศ์ ศรีแสงจันทร์. คณะทำงานพหุภาคีแก้ไขปัญหาคอลเซ็นเตอร์เสนอบอร์ด กสทช. ขีดเส้นตายให้โอเปอเรเตอร์ทุกรายสร้างระบบให้ประชาชนเลือกสมัครบริการปฏิเสธไม่รับสายที่โทรมาจากต่างประเทศ เพื่อลดความเดือดร้อนจากปัญหาดังกล่าวโดยเร็วที่สุด. [ออนไลน์]. 2565. แหล่งที่มา: https://www.nbtc.go.th/News/Press-Center/55326.aspx?lang=th-th [25 พฤศจิกายน 2565]

ประชาชาติธุรกิจออนไลน์. แก๊งคอลเซ็นเตอร์โทรไม่หยุด เอกชนเสียหาย ประกาศดำเนินคดีขั้นสุด. [ออนไลน์].2565. แหล่งที่มา: https://www.prachachat.net/general/news-917443 [30 ตุลาคม 2565]

ปราโมทย์ เสริมศีลธรรม. หลักเกณฑ์ในการกำหนดโทษทางอาญา ภายใต้โครงการสนับสนุนสารสนเทศเพื่อการทำงานของสมาชิกรัฐสภา. กรุงเทพมหานคร: สถาบันพระปกเกล้า, 2564.

ผู้จัดการออนไลน์. ค่ายมือถือหวั่น กสทช.ถูกปรับวันละล้าน เข้มงวดร้านลูกตู้ลงทะเบียนซิม 1 คน 1 ค่ายไม่เกิน 5 เบอร์. [ออนไลน์]. 2565. แหล่งที่มา: https://mgronline.com/onlinesection/detail/9650000078487 [15 พฤศจิกายน 2565]

ผู้จัดการออนไลน์**.** กสทช.กำชับค่ายมือถือตัดไฟแต่ต้นลม บล็อกเบอร์แก๊งคอลเซ็นเตอร์ไม่ให้โทร.เข้าไทย. [ออนไลน์]. 2565**.** แหล่งที่มา**:** https://mgronline.com/cyberbiz/detail/9650000005777 [10 พฤษภาคม 2565]

ผู้จัดการออนไลน์. เปิดขั้นตอนแจ้งความออนไลน์ thaipoliceonline.com รับเฉพาะคดีอาชญากรรมทางเทคโนโลยี. [ออนไลน์]. 2565. แหล่งที่มา: https://mgronline.com/onlinesection/detail/9650000021035 [22 ตุลาคม 2565]

พิมพ์ธัญญา ฆ้องเสนาะ. บัญชีม้า. [ออนไลน์]. 2565. แหล่งที่มา: https://library.parliament.go.th/th/radioscript/rr2565-may6 [19 ตุลาคม 2565]

พิมพ์ผกา ทรายข้าว. Cybercrime หรือ Computer Crime. [ออนไลน์]. 2564. แหล่งที่มา: https://www.nsm.or.th/other-service/671-online-science/knowledge-inventory/sci-vocabulary/sci-vocabulary-information-technology-museum/4267-cybercrime.html [3 มีนาคม 2565]

พิมพ์พชา ปิยะเกศิน และ พัชรี พิชณุษากร และ อโนชา หงส์บุรินทร์ และ ทิพย์สุรางค์ วาทิตต์พันธุ์ และ อภิญญา บัณฑิตวุฒิสกุล. ความรู้ทั่วไปเกี่ยวกับการกำกับดูแลกิจการโทรคมนาคมและการออกใบอนุญาตประกอบกิจการโทรคมนาคม, พิมพ์ครั้งที่ 1. กรุงเทพมหานคร : แอ๊ปป้า พริ้นติ้ง กรุ๊ป จำกัด, 2552.

พี่กวาง. เตือนภัย! "Wangiri Fraud" มิจฉาชีพแนวใหม่ Missed Call ให้เราเสียเงิน!. [ออนไลน์]. 2561. แหล่งที่มา: https://www.dek-d.com/teentrends/49294/ [11 พฤศจิกายน 2565]

รังสรรค์ โรจน์ชีวิน และ มนตรี จิตร์วิวัฒน์ และ ดิลก เสริมวิริยะกุล และ สมชาติ เลิศลิขิตวรกุล และ ชัชวาล วิบุลสันติ และ หฤทัย ประพุทธนิติสาร. กฎหมายคุ้มครองผู้บริโภค และการดำเนินคดีคุ้มครองผู้บริโภค ประเทศออสเตรเลีย ศึกษาเกี่ยวกับกรณี การกระทำในทางการค้าทำให้ผู้บริโภคเกิดความเข้าใจผิด หรือหลอกลวงผู้บริโภคทางการค้า การเอาเปรียบผู้บริโภคที่มีความด้อยหรือความเสียเปรียบในทางการค้า หลักประกันผู้บริโภค การเยียวยา และอำนาจการบังคับใช้ของ ACCC การพิจารณาคดีผู้บริโภคโดยช่องทางพิเศษ การนำอิเล็กทรอนิกส์และเทคโนโลยีมาใช้ในการดำเนินกระบวนพิจารณาคดีของศาล, การฝึกอบรมหลักสูตร “กฎหมายเกี่ยวกับวิธีพิจารณาความแพ่งชั้นสูง” ณ มหาวิทยาลัยนิวเซาท์เวลส์ ประเทศออสเตรเลีย. สำนักการต่างประเทศ

วสันต์ ลิ่วลมไพศาล. Spear Phishing ภัยธุรกิจสร้างความเสียหายได้มากกว่าที่คิด. [ออนไลน์]. 2564. แหล่งที่มา: https://www.mfec.co.th/th/cto-brief/spear-phishing-%E0%B8%A0%E0%B8%B1%E0%B8%A2%E0%B8%98%E0%B8%B8%E0%B8%A3%E0%B8%81%E0%B8%B4%E0%B8%88%E0%B8%AA%E0%B8%A3%E0%B9%89%E0%B8%B2%E0%B8%87%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B9%80%E0%B8%AA/ [1 มิถุนายน 2565]

ศูนย์ไซเบอร์กองทัพอากาศ. Phishing" ภัยออนไลน์ที่ไม่ควรมองข้าม !!!. [ออนไลน์]. 2565. แหล่งที่มา: https://cyber.rtaf.mi.th/publish/page.aspx?id=912 [3 มิถุนายน 2565]

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักข่าวกรองแห่งชาติ. ออสเตรเลียเริ่มปิดกั้นข้อความหลอกลวงที่อ้างว่ามาจากหน่วยงานของรัฐบาล. [ออนไลน์]. 2564. แหล่งที่มา: https://www.nia.go.th/cyber/cyberpage/588/ [13 พฤศจิกายน 2565]

สถานเอกอัครราชทูต ณ กรุงพนมเปญ. ประกาศเตือน การเดินทางไปทำงานในกัมพูชาโดยผิดกฎหมาย. [ออนไลน์]. 2564. แหล่งที่มา: https://phnompenh.thaiembassy.org/th/content/ประกาศเตือน-การเดินทางไปทำงานในกัมพูชาโดยผิดกฎหมาย [1 ตุลาคม 2565]

สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (องค์การมหาชน). ผู้เชี่ยวชาญ มั่นใจ ชีวิตวิถีใหม่ อยู่ภายใต้ภัยคุกคามทางไซเบอร์ แนะทุกหน่วยงานต้องออกแบบระบบที่ทำงานได้แม้ถูกโจมตี. [ออนไลน์]. 2563. แหล่งที่มา: https://www.tijthailand.org/th/highlight/detail/cybercrime-covid-19 [15 พฤษภาคม 2565]

สยามรัฐออนไลน์. สกัดแก๊งคอลเซ็นเตอร์ "กสทช." จ่อปรับ 1 ล้านบาท ค่ายมือถือไม่จัดการลงทะเบียนซิมการ์ด. [ออนไลน์]. 2565. แหล่งที่มา: https://siamrath.co.th/n/363170 [3 พฤศจิกายน 2565]

สัญญพงศ์ ลิ่มประเสริฐ และ สุธีราภรณ์ แสงจันทร์ศรี และ อนิสา มานะทน. การลงโทษผู้กระทำผิดทางอาญา. รายงานประชุมวิชาการระดับชาติ มหาวิทยาลัยรังสิต ประจำปี 2562, หน้า 1489. ณ คณะนิติศาสตร์ มหาวิทยาลัยรังสิต ปทุมธานี ประเทศไทย, 26 เมษายน 2562

สุพิศาล ภักดีนฤบาล. 4 Dimensions การบริหารงานสืบสวน : กองบังคับการปราบปราม. ครั้งที่พิมพ์ 2. นนทบุรี : กรีนแอปเปิ้ล กราฟฟิคปริ้นติ้ง จำกัด, 2556.

สุภาพิชญ์ ถิระวัฒน์. กองบัญชาการตำรวจไซเบอร์. [ออนไลน์]. 2564. แหล่งที่มา: https://library.parliament.go.th/th/radioscript-rr2564-nov1 [17 ตุลาคม 2565]

โสภิดา วีรกุลเทวัญ. แนวทางการจัดการกับปัญหาการส่งข้อความสั้นหรือโทรศัพท์ที่ไม่พึง ประสงค์ (spam) และหลอกลวง (scam) ต่อผู้บริโภคในต่างประเทศ , หน้า 2

อัจฉรียา ชูตินันทน์. อาชญาวิทยาและทัณฑวิทยา. กรุงเทพมหานคร : สำนักพิมพ์วิญญูชน, 2561.

อาริยา สุขโต วิทยากรชำนาญการพิเศษ กลุ่มงานบริการวิชาการ 2 สำนักวิชาการ. ภัยอาชญากรรมแก๊งคอลเซ็นเตอร์. [ออนไลน์]. 2565. แหล่งที่มา https://library.parliament.go.th/th/radioscript/rr2565-jul7 [13 ตุลาคม 2565]

Andrew Penn. Tackling the changing face of our customer. [Online]. 2019. Source: https://www.linkedin.com/pulse/tackling-changing-face-our-customer-andrew-penn/ [2022, November 13]

BBC News. บัตรเครดิต-เดบิต: แบงก์ชาติ- ส.ธนาคารไทย พบเหตุถูกตัดเงินผิดปกติ เกิดจากธุรกรรมกับร้านค้าออนไลน์. [ออนไลน์]. 2564. แหล่งที่มา: https://www.bbc.com/thai/thailand-58950301 [10 มีนาคม 2565]

Knowledge Center. วิธีย้ายค่ายมาเป็นครอบครัว AIS. [ออนไลน์]. แหล่งที่มา: https://aiscallcenter.ais.co.th/ikm/acc/index.php?kmid=KM1020179 [29 ตุลาคม 2565]

Mobileocta_Admin. Gogolook ปั้น Whoscall แพลตฟอร์มต่อต้านการฉ้อโกงแห่งแรกในประเทศไทย ปกป้องคนไทยไม่ให้ตกเป็นเหยื่อการใช้โทรศัพท์และข้อความหลอกลวง. [ออนไลน์]. 2565. แหล่งที่มา: https://www.mobileocta.com/gogolook-creates-whoscall-the-first-anti-fraud-platform-in-thailand/ [25 พฤศจิกายน 2565]

Nation Online. เปิดคู่มือ “รับมือแก๊งคอลเซ็นเตอร์” พร้อม "เปิดโปงขบวนการข้ามชาติ". [ออนไลน์]. 2565. แหล่งที่มา: https://www.nationtv.tv/news/378864640 [13 ตุลาคม 2565]

Nithin Gangadharan. What is Wangiri Fraud and how does it impact telecom operators?. [Online]. 2019. Source: https://www.subex.com/blog/What-is-wangiri-fraud-how-does-it-impact-for-telecom-operators/ [2022, November 13]

Ofcom. Tackling nuisance calls and messages. [Online]. 2021. Source: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/tackling-nuisance-calls-messages [2022, December 21]

Stop Scams UK. WORKING TOGETHER TO STOP SCAMS AT SOURCE. [Online]. 2022. Source: https://stopscamsuk.org.uk/about-stop-scams-uk [2022, December 10]

Telecommunications Services: Reference Paper. Negotiating group on basic telecommunications, [Online]. 1996. Source: https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm [2022, November 25]

The Chapt. Phishing คืออะไร? รู้ทันการโจรกรรมบนโลกไซเบอร์ ปี 2022. [ออนไลน์]. 2565. แหล่งที่มา: https://thechapt.com/phishing/ [10 มีนาคม 2565]

Workpoint TODAY. สำรวจเบอร์อันตราย ห้ามรับสาย ห้ามโทรกลับ ก่อนสูญเงิน. [ออนไลน์]. 2562. แหล่งที่มา: https://workpointtoday.com/%E0%B8%AB%E0%B9%89%E0%B8%B2%E0%B8%A1%E0%B8%A3%E0%B8%B1%E0%B8%9A%E0%B8%AA%E0%B8%B2%E0%B8%A2-%E0%B8%AB%E0%B9%89%E0%B8%B2%E0%B8%A1%E0%B9%82%E0%B8%97%E0%B8%A3%E0%B8%81%E0%B8%A5%E0%B8%B1%E0%B8%9A/ [11 พฤศจิกายน 2565]

กฎหมายไทยที่ใช้ในการศึกษา

- รัฐธรรมนูญแห่งราชอาญาจักรไทย พ.ศ.2560
- พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544
- พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- พระราชบัญญัติให้ใช้ประมวลกฎหมายอาญา พ.ศ. 2499
- พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการ วิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม (ฉบับที่ 3) พ.ศ. 2562
- พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553
- ประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม แห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่
- ประกาศสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่อง กำหนดหลักเกณฑ์การบังคับทางปกครองในกิจการโทรคมนาคม
- หลักเกณฑ์การโอนย้ายผู้ให้บริการโทรศัพท์เคลื่อนที่ของผู้ใช้บริการโทรศัพท์เคลื่อนที่ ตามประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคม

แห่งชาติ เรื่อง หลักเกณฑ์บริการคงสิทธิเลขหมายโทรศัพท์เคลื่อนที่ (MNP Porting Process Manual) ฉบับตามมติ กสทช. ครั้งที่ 15/2564

กฎหมายต่างประเทศ

- The Telecommunication Act 1997
- Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020
- Telecommunications (Industry Standard for Mobile Number Pre-Porting Additional Identity Verification) Direction 2019
- Reducing Scams Call Industry Code
- The Communications Act 2003
- The General Conditions of Entitlement
- The National Telephone Numbering Plan

อื่นๆ

- รายงานข้อมูลการกำกับดูแลกิจการโทรคมนาคม ไตรมาส 1 ปี 2565
- Australian Competition and Consumer Commission, Targeting Scams report 2020
- Australian Competition and Consumer Commission, Targeting Scam Report of the ACCC on scams activity 2020
- Australian Communication and Media Authority, Combating scams Action plan summary, November 2019
- Ofcom, Quick, easy and reliable switching: Statement on changes to the General Conditions, 3 February 2022
- The Information Commissioner’s Office (ICO) and Ofcom Nuisance calls and messages, Update to ICO-Ofcom joint action plan 2019