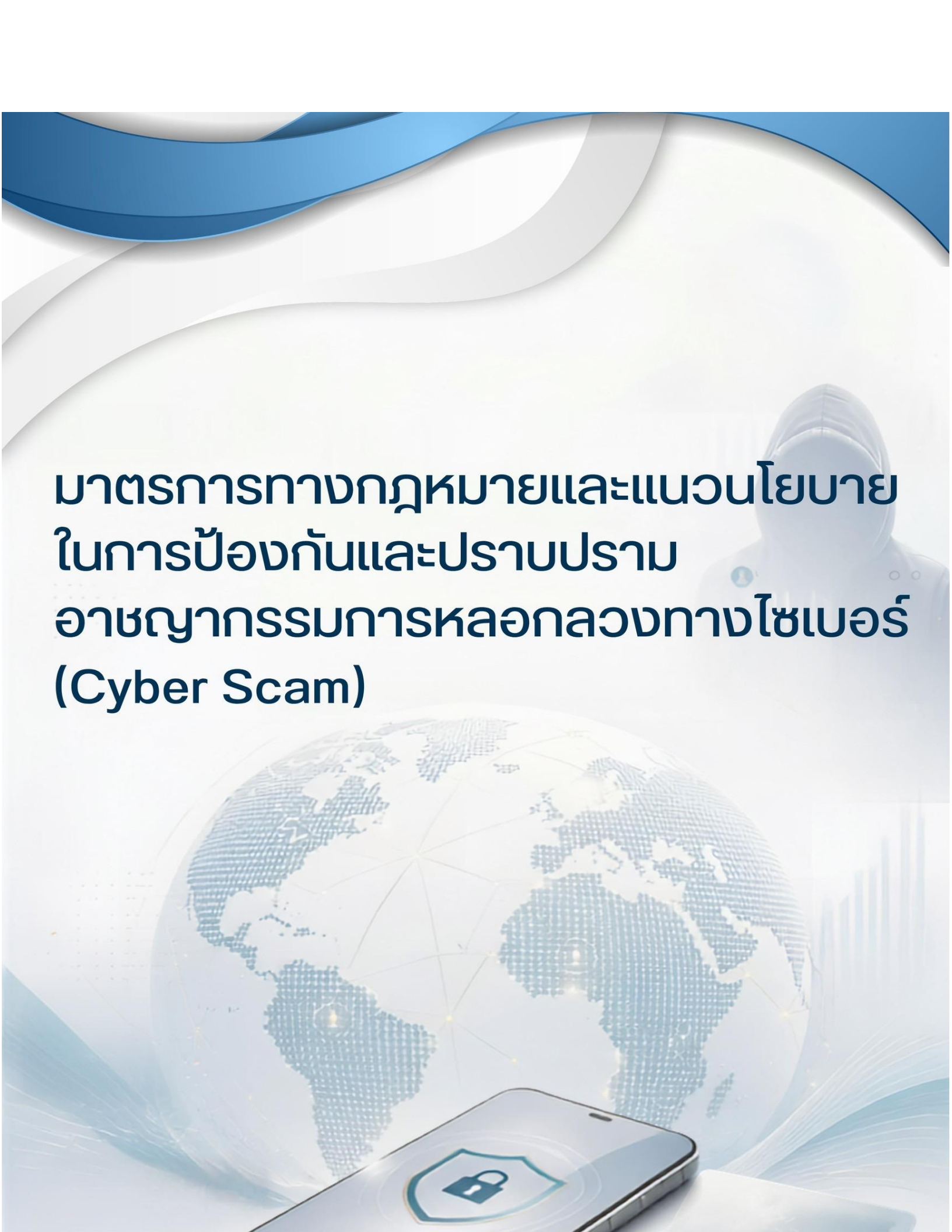




มาตรการทางกฎหมายและแนวนโยบาย ในการป้องกันและปราบปราม อาชญากรรมการหลอกลวงทางไซเบอร์ (Cyber Scam)

คำนำ

ปัจจุบันเทคโนโลยีดิจิทัลและเครือข่ายอินเทอร์เน็ตมีบทบาทสำคัญต่อการดำเนินชีวิตของประชาชนในทุกมิติ ไม่ว่าจะเป็นด้านการสื่อสาร การทำธุรกรรมทางการเงิน หรือการประกอบธุรกิจ ความก้าวหน้าดังกล่าวแม้จะอำนวยความสะดวกและประสิทธิภาพในการดำเนินกิจกรรมต่าง ๆ แต่ในขณะเดียวกันก็เปิดช่องให้เกิดอาชญากรรมที่อาศัยเทคโนโลยีเป็นเครื่องมือในการกระทำความผิด โดยเฉพาะอย่างยิ่งอาชญากรรมการหลอกลวงทางไซเบอร์ (Cyber Scam) ซึ่งสร้างความเสียหายต่อทรัพย์สินของประชาชนและระบบเศรษฐกิจโดยรวมเป็นมูลค่ามหาศาล

อาชญากรรมการหลอกลวงทางไซเบอร์มีลักษณะเป็นอาชญากรรมข้ามชาติที่อาศัยเทคโนโลยีดิจิทัล ระบบการเงิน และแพลตฟอร์มออนไลน์เป็นเครื่องมือในการกระทำความผิด ส่งผลให้การบังคับใช้กฎหมายในรูปแบบดั้งเดิมมีข้อจำกัด ทั้งในเรื่องเขตอำนาจศาล การพิสูจน์และติดตามทรัพย์สิน การติดตามเส้นทางการเงิน ตลอดจนการดำเนินคดีต่อผู้กระทำความผิดที่อยู่ในต่างประเทศ ด้วยเหตุนี้ ฝ่ายค้านคว่ำและเปรียบเทียบกฎหมาย กองกฎหมายต่างประเทศ จึงเห็นสมควรศึกษาค้นคว้าเรื่อง “มาตรการทางกฎหมายและแนวนโยบายในการป้องกันและปราบปรามอาชญากรรมการหลอกลวงทางไซเบอร์ (Cyber Scam)” โดยมีวัตถุประสงค์เพื่อศึกษามาตรการที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมดังกล่าว ทั้งในส่วนของมาตรการเชิงป้องกัน มาตรการเชิงลงโทษ กลไกการกำกับดูแลแพลตฟอร์มดิจิทัล มาตรการทางการเงินและการติดตามทรัพย์สิน รวมถึงบทบาทของหน่วยงานรัฐและความร่วมมือระหว่างประเทศในบริบทของไทย ตลอดจนศึกษาเปรียบเทียบมาตรการของต่างประเทศ ได้แก่ แคนาดา เยอรมนี ออสเตรเลีย จีน เกาหลีใต้ และสิงคโปร์ เพื่อนำมาวิเคราะห์และเสนอแนะแนวทางที่เหมาะสมอันจะเป็นประโยชน์ต่อการพัฒนากฎหมายและนโยบายของประเทศไทยต่อไป

งานค้นคว้านี้ประกอบด้วยเนื้อหา ๕ บท ได้แก่ บทที่ ๑ บทนำว่าด้วยความหมายและประเภทของอาชญากรรมการหลอกลวงทางไซเบอร์ (Cyber Scam) บทที่ ๒ ความตกลงระหว่างประเทศเกี่ยวกับการหลอกลวงทางไซเบอร์ บทที่ ๓ มาตรการที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมการหลอกลวงทางไซเบอร์ของต่างประเทศ บทที่ ๔ มาตรการที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมการหลอกลวงทางไซเบอร์ของประเทศไทย และบทที่ ๕ บทสรุป ในการนี้ ผู้จัดทำหวังเป็นอย่างยิ่งว่างานค้นคว้านี้จะเป็นประโยชน์ต่อผู้ที่สนใจศึกษาและหน่วยงานที่เกี่ยวข้องในการพัฒนามาตรการทางกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมการหลอกลวงทางไซเบอร์ต่อไป

ฝ่ายค้านคว่ำและเปรียบเทียบกฎหมาย

กองกฎหมายต่างประเทศ

กันยายน ๒๕๖๙

สารบัญ

	หน้า
บทที่ ๑ บทนำ	๑
บทที่ ๒ ความตกลงระหว่างประเทศเกี่ยวกับการหลอกลวงทางไซเบอร์	๕
บทที่ ๓ มาตรการที่เกี่ยวข้องกับการป้องกันและปราบปราม อาชญากรรมการหลอกลวงทางไซเบอร์ของต่างประเทศ	๘
๓.๑ แคนาดา	๘
๓.๒ เยอรมนี	๑๙
๓.๓ ออสเตรเลีย	๓๓
๓.๔ จีน	๔๓
๓.๕ สาธารณรัฐเกาหลี (เกาหลีใต้)	๕๗
๓.๖ สิงคโปร์	๗๒
บทที่ ๔ มาตรการที่เกี่ยวข้องกับการป้องกันและปราบปราม อาชญากรรมการหลอกลวงทางไซเบอร์ของประเทศไทย	๘๘
บทที่ ๕ บทสรุป	๑๐๐

บทที่ ๑ บทนำ*

๑. ความหมายของอาชญากรรมการหลอกลวงทางไซเบอร์ (Cyber Scam)

อาชญากรรมไซเบอร์ (Cyber Crime)^๑ หมายถึง การกระทำความผิดใด ๆ โดยใช้ระบบคอมพิวเตอร์หรืออินเทอร์เน็ตซึ่งครอบคลุมการกระทำที่ผิดกฎหมายหลายประเภท เช่น การแฮ็ก การขโมยข้อมูลส่วนบุคคล สื่อกลั่นแกล้งทางไซเบอร์ และการกระจายมัลแวร์ อาชญากรรมทางคอมพิวเตอร์อาจมุ่งเป้าไปที่บุคคล องค์กร สถาบัน และนิติบุคคลอื่น ๆ ซึ่งผลที่ตามมาอาจรวมถึงการสูญเสียทางการเงิน เสียชื่อเสียง และความบอบช้ำทางจิตใจ

อาชญากรรมไซเบอร์ (Cyber Crime) เป็นคำกว้างที่รวมถึงการฉ้อโกงทางไซเบอร์ (Cyber Fraud) และการหลอกลวงทางไซเบอร์ (Cyber Scam) ไว้ด้วย โดยการฉ้อโกงทางไซเบอร์ (Cyber Fraud)^๒ หมายถึงการกระทำความผิดเป็นการฉ้อโกงหรือหลอกลวงบุคคลหรือองค์กรโดยใช้คอมพิวเตอร์ จากบทนิยามดังกล่าวจะเห็นได้ว่า “Cyber Fraud” มีความหมายกว้าง โดยจะรวมถึง “Cyber Scam” เข้าไปด้วย อย่างไรก็ตาม คำทั้งสองคำมักมีการใช้ปนกัน อาจเพราะมีจุดร่วมกันที่สำคัญ^๓ คือ (๑) มีแรงจูงใจทางการเงินเป็นแกนกลาง กล่าวคือผู้กระทำความผิดมุ่งแสวงหาผลประโยชน์ทางการเงินหรือทรัพย์สินโดยมิชอบ (๒) มีองค์ประกอบของ “การหลอกลวง” (deception) เป็นกลไกหลักในการกระทำความผิด ต่างจากอาชญากรรมประเภทเจาะระบบที่อาศัยช่องโหว่ทางเทคนิคเป็นหลัก และ (๓) ในทางปฏิบัติ นักวิชาการจำนวนไม่น้อยยังคงใช้คำทั้งสองแทนกันในงานเขียน ซึ่งสะท้อนให้เห็นว่าเส้นแบ่งระหว่าง ๒ คำนี้ในทางปฏิบัติยังไม่ชัดเจนนัก

อย่างไรก็ดี ปัจจุบันขอบเขตความหมายของ Cyber Scam ขยายไปกว้างมาก โดยจากรายงานของ UNODC^๔ ได้ขยายขอบเขตความหมายให้ครอบคลุมถึงปรากฏการณ์ “ศูนย์หลอกลวง” (scam centres) ซึ่งเป็นการรวมตัวกันของกลุ่มอาชญากรรมข้ามชาติที่ดำเนินการหลอกลวงในเชิงอุตสาหกรรม โดยอาศัยแรงงานที่ถูกค้ำมนุษย์มาบังคับใช้แรงงานในการกระทำความผิด ศูนย์หลอกลวงเหล่านี้มักตั้งอยู่ในพื้นที่ปิดล้อมในประเทศเมียนมา กัมพูชา และฟิลิปปินส์ และมีการดำเนินการในระดับ

* จัดทำโดยนางสาวฉันทพิมพ์ บรรจงจิตร ผู้อำนวยการฝ่ายค้นคว้าและเปรียบเทียบกฎหมายกองกฎหมายต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

^๑ Difference between Cyber Crime and Cyber Fraud, สืบค้นเมื่อวันที่ ๑๕ กรกฎาคม ๒๕๖๙, จาก <https://cybersapiens.com.au/difference-between-cyber-crime-and-cyber-fraud/>

^๒ อ้างแล้ว

^๓ Harding, N., Cooper, E., Sales, T., McDonald, A., & Kingston, S. (2025), “The Liminality of Fraud: Reimagining Fraud Theory to Inform Financial Crime Prevention. The British Journal of Criminology”, Vol. 65, No. 3, P. 618–638 สืบค้นเมื่อวันที่ ๒๐ กรกฎาคม ๒๕๖๙, จาก <https://doi.org/10.1093/bjc/azae069>

^๔ United Nations Office on Drugs and Crime, “Crushing scam farms”, สืบค้นเมื่อวันที่ ๑๕ มิถุนายน ๒๕๖๙, จาก <https://www.unodc.org/unodc/frontpage/2024/July/crushing-scam-farms-southeast-asias-criminal-service-providers.html>

อุตสาหกรรม ซึ่งสะท้อนให้เห็นว่า Cyber Scam ในปัจจุบันมีความหมายกว้าง โดยมีได้เป็นเพียงการกระทำความผิดของปัจเจกบุคคล แต่ได้พัฒนาไปสู่รูปแบบอาชญากรรมที่จัดตั้งเป็นองค์กรและเชื่อมโยงกับอาชญากรรมประเภทอื่น เช่น การค้ำมนุษย์และการฟอกเงิน^๕

๒. วิธีการหลอกลวงทางไซเบอร์^๖

การหลอกลวงทางไซเบอร์มีหลายรูปแบบและหลายช่องทาง แต่ล้วนเกี่ยวข้องกับ การหลอกลวงโดยมีเจตนาที่จะทำให้เข้าใจผิด ผู้กระทำความผิดมักใช้ความต้องการและแรงจูงใจพื้นฐานของมนุษย์ เช่น โอกาสที่จะนำไปสู่ความมั่นคงทางการเงิน หรือมิตรภาพ ซึ่งกระตุ้นการตอบสนองทางอารมณ์ เทคนิคการโน้มน้าวใจที่ผู้กระทำความผิดใช้มักมีการออกแบบมาเพื่อกระตุ้นปฏิกิริยาทางอารมณ์อย่างรวดเร็ว ซึ่งทำให้เกิดการตัดสินใจที่หุนหันพลันแล่นหรือขาดความรอบคอบ และทำให้เหยื่อไม่ทันได้คิดถึงความเสี่ยงหรือความน่าเชื่อถือของกลโกง ทั้งนี้ ผู้สูงอายุอาจมีความเสี่ยงต่อการถูกหลอกลวงทางไซเบอร์มากกว่า แต่ก็มีได้หมายความว่าบุคคลวัยอื่น ๆ จะถูกหลอกลวงน้อยกว่า

ในการหลอกลวง ผู้กระทำความผิดจะใช้กลยุทธ์ทางวิศวกรรมเพื่อหลอกลวงเหยื่อให้เปิดเผยรายละเอียดความปลอดภัยในการทำธุรกรรมธนาคารออนไลน์ ผ่านทางโทรศัพท์ ข้อความ และอีเมลหลอกลวง คนส่วนใหญ่มักอยากช่วยเหลือและให้ความร่วมมือ ผู้กระทำความผิดจึงใช้ประโยชน์จากจุดนี้และจะใช้ทักษะในการหลอกล่อเหยื่อให้เปิดเผยข้อมูลส่วนบุคคล ซึ่งมักทำได้โดยการแอบอ้างเป็นองค์กรที่ถูกต้องตามกฎหมาย เช่น ธนาคาร กรมสรรพากร หรือหน่วยงานราชการ

นอกจากนี้ ผู้กระทำความผิดจำนวนมากมักจะ “ซ่อนตัว” โดยอาศัยข้อเท็จจริงที่ว่าตนเองอาจไม่สามารถระบุตัวตนได้ง่ายจากบัญชีโซเชียลมีเดีย ซึ่งเป็นเหตุผลว่าทำไมวิธีการเหล่านี้จึงมักจะมีการนำมาใช้เพื่อเข้าถึงเป้าหมาย

คณะกรรมการการค้าแห่งสหรัฐอเมริกา (FTC) ได้มีการระบุสัญญาณเตือนภัยทั่วไปที่บ่งชี้ถึงการหลอกลวงไว้ ดังนี้^๗

- มิฉฉาชีพอ้างแอบอ้างเป็นองค์กรที่น่าเชื่อถือ เช่น หน่วยงานราชการหรือธนาคาร
- อาจบอกว่ามีเหตุฉุกเฉินหรือมีปัญหาเกี่ยวกับบัญชีของเหยื่อ
- กดดันให้เหยื่อต้องดำเนินการทันที
- แจ้งให้เหยื่อชำระเงินด้วยวิธีใดวิธีหนึ่งโดยเฉพาะ เช่น ด้วยสกุลเงินดิจิทัลหรือ

แอปพลิเคชันการชำระเงินเฉพาะ

^๕ AML Right Source, “Scam States: The Cybercrime-Corruption Complex in Southeast Asia and the Collapse of Anti-Money Laundering Enforcement”, สืบค้นเมื่อวันที่ ๑๕ มิถุนายน ๒๕๖๙, จ ๑ ก <https://www.amlrightsource.com/resources/scam-states-the-cybercrime-corruption-complex-in-southeast-asia-and-the-collapse-of-anti-money-laundering-enforcement>

^๖ “Cyber Fraud and Scamming Guidance and Advice” สืบค้นเมื่อวันที่ ๒๔ กรกฎาคม ๒๕๖๙, จาก <https://proceduresonline.com/trixcms2/media/1377/cyber-fraud-and-scamming-ecopy-2.pdf>

^๗ “Fraud vs. Scams: What’s the Difference?”, สืบค้นเมื่อวันที่ ๑๕ กรกฎาคม ๒๕๖๙, จาก <https://bpi.com/fraud-vs-scams-whats-the-difference/>

๓. ประเภทของการหลอกลวงทางไซเบอร์^๔

การหลอกลวงทางไซเบอร์มีหลายหลายรูปแบบ โดยรูปแบบที่พบได้บ่อยสามารถจำแนกได้ดังนี้

(๑) การหลอกลวงแบบฟิชชิ่ง (Phishing Scam) เป็นรูปแบบการหลอกลวงที่ผู้กระทำความผิดส่งข้อความหรืออีเมลที่ปลอมแปลงให้ดูเหมือนมาจากองค์กรหรือบุคคลที่น่าเชื่อถือเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลส่วนบุคคล เช่น รหัสผ่านในการเข้าสู่ระบบหรือหมายเลขบัตรเครดิต โดยอาจใช้ลิงก์หรือไฟล์แนบที่เป็นอันตรายเพื่อติดตั้งมัลแวร์ในอุปกรณ์ของเหยื่อ หรือเพื่อนำเหยื่อไปยังเว็บไซต์ปลอมที่จำลองขึ้นให้คล้ายกับเว็บไซต์จริง

(๒) การหลอกลวงการลงทุน (Investment Scam) เป็นการหลอกลวงโดยใช้ข้อเสนอผลตอบแทนสูงในระยะเวลาอันรวดเร็วเป็นเครื่องมือชักจูงเหยื่อให้ลงทุนในสินทรัพย์หรือโครงการที่ไม่มีอยู่จริง โดยมักเป็นข้อเสนอที่มีลักษณะจำกัดเวลาเพื่อกดดันให้เหยื่อตัดสินใจอย่างรวดเร็ว ปัจจุบันการหลอกลวงในลักษณะนี้มักเกี่ยวข้องกับสินทรัพย์ดิจิทัลหรือสกุลเงินคริปโทเคอร์เรนซี ซึ่งเป็นช่องทางที่ติดตามเส้นทางการเงินได้ยาก

(๓) การหลอกลวงเชิงโรแมนซ์ (Romance Scam) เป็นการที่ผู้กระทำความผิดสร้างโปรไฟล์ปลอมบนแพลตฟอร์มหาคู่หรือสื่อสังคมออนไลน์ เพื่อสร้างความสัมพันธ์เชิงชู้สาวกับเหยื่อก่อนจะชักชวนให้ย้ายการสนทนาไปยังช่องทางส่วนตัวเพื่อหลีกเลี่ยงระบบป้องกันของแพลตฟอร์ม และเมื่อสร้างความไว้วางใจได้แล้วจึงเริ่มเรียกร้องเงิน ของขวัญ หรือข้อมูลส่วนบุคคลจากเหยื่อ รูปแบบที่พัฒนาขึ้นในปัจจุบันคือการหลอกลวงแบบผสมผสานระหว่างความสัมพันธ์เชิงชู้สาวกับการชักชวนลงทุน หรือที่เรียกว่า “Pig Butchering Scam”

(๔) การหลอกลวงผ่านศูนย์บริการลูกค้าปลอม (Call Center Scam) เป็นการที่ผู้กระทำความผิดแอบอ้างเป็นเจ้าหน้าที่ของหน่วยงานรัฐ สถาบันการเงิน หรือบริษัทเอกชนที่มีความน่าเชื่อถือ ติดต่อเหยื่อทางโทรศัพท์เพื่อแจ้งข้อมูลอันเป็นเท็จ เช่น การพัวพันกับคดีอาญาหรือการกระทำความผิดเกี่ยวกับบัญชีธนาคาร เพื่อสร้างความตื่นตระหนกและชักจูงให้เหยื่อโอนเงินหรือเปิดเผยข้อมูลทางการเงิน

(๕) การหลอกลวงทางพาณิชย์อิเล็กทรอนิกส์ (Online Shopping Scam) เป็นการสร้างเว็บไซต์หรือร้านค้าออนไลน์ปลอมที่เลียนแบบแพลตฟอร์มซื้อขายที่ถูกกฎหมายโดยมักโฆษณาสินค้าที่หายากหรือมีส่วนลดสูงผิดปกติ และใช้เทคนิคการปรับแต่งให้ติดอันดับการค้นหาประกอบกับการสร้างความเร่งด่วนเพื่อกระตุ้นให้เหยื่อตัดสินใจซื้อ ซึ่งส่งผลให้เหยื่อสูญเสียเงินโดยไม่ได้รับสินค้าตามที่สั่งซื้อ

^๔ Australian Government, Australian Signals Directorate, “Types of scams” สืบค้นเมื่อวันที่ ๑๕ มิถุนายน ๒๕๖๙, จาก <https://www.cyber.gov.au/learn-basics/watch-out-threats/types-scams> และ Keeper Security, “The Types of Online Scams” สืบค้นเมื่อวันที่ ๑๗ มิถุนายน ๒๕๖๙, จาก <https://www.keepersecurity.com/blog/2023/11/28/the-types-of-online-scams/>

(๖) การหลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล (Cryptocurrency Scam) เป็นการหลอกลวงผ่านเว็บไซต์ซื้อขายสินทรัพย์ดิจิทัลปลอมหรือกระเป๋าสตางค์ดิจิทัลปลอม โดยผู้กระทำความผิดมักใช้บัญชีปลอมของบุคคลที่มีชื่อเสียงหรือบริษัทเพื่อล่อลวงเหยื่อ และเมื่อเหยื่อกรอกข้อมูลรับรองตัวตนแล้ว ผู้กระทำความผิดจะสามารถขโมยสินทรัพย์ดิจิทัลของเหยื่อได้

(๗) การหลอกลวงทางธุรกิจผ่านอีเมล (Business Email Compromise (BEC)) เป็นการหลอกลวงที่มุ่งเป้าไปที่องค์กรธุรกิจโดยผู้กระทำความผิดมักแอบอ้างเป็นผู้บริหารระดับสูงหรือลูกค้าทางธุรกิจเพื่อขอให้มีการโอนเงินผ่านช่องทางที่เป็นการฉ้อโกง อาชญากรรมประเภทนี้สร้างความเสียหายต่อภาคธุรกิจเป็นมูลค่าสูง เนื่องจากมักเกี่ยวข้องกับการโอนเงินจำนวนมากในคราวเดียว

นอกจากการจำแนกประเภทตามลักษณะวิธีการหลอกลวงข้างต้นแล้ว จากรายงานของ UNODC^๔ แสดงให้เห็นถึงพัฒนาการเชิงโครงสร้างขององค์กรอาชญากรรมที่อยู่เบื้องหลัง Cyber Scam ในภูมิภาคเอเชียตะวันออกเฉียงใต้ว่าได้พัฒนาไปสู่รูปแบบ “ผู้ให้บริการอาชญากรรม” (criminal service providers) ที่มีการแบ่งหน้าที่กันอย่างเป็นระบบ บางกลุ่มเชี่ยวชาญด้านการจัดหาแรงงาน บางกลุ่มเชี่ยวชาญด้านการดำเนินการหลอกลวง และบางกลุ่มเชี่ยวชาญด้านการฟอกเงิน ซึ่งโครงสร้างที่แบ่งเป็นส่วน ๆ เช่นนี้ เอื้อให้การดำเนินกิจกรรมเป็นไปได้อย่างต่อเนื่อง แม้จะถูกหน่วยงานบังคับใช้กฎหมายกดดัน ซึ่งสะท้อนให้เห็นว่าการจัดประเภทของ Cyber Scam ในปัจจุบัน จำเป็นต้องพิจารณาทั้งในมิติของรูปแบบวิธีการหลอกลวงที่มีต่อเหยื่อโดยตรง และมีมิติเชิงโครงสร้างขององค์กรอาชญากรรมที่อยู่เบื้องหลังการกระทำความผิดควบคู่กันไป อันจะเป็นประโยชน์ต่อการกำหนดมาตรการทางกฎหมายและนโยบายในการป้องกันและปราบปรามที่เหมาะสมต่อไป

^๔ UNODC, October 2024, “Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape”

บทที่ ๒

ความตกลงระหว่างประเทศเกี่ยวกับการหลอกลวงทางไซเบอร์*

๑. ความเป็นมา

เมื่อปี ค.ศ. ๒๐๑๗ รัสเซียยื่นข้อเสนอต่อสหประชาชาติว่า สมควรให้มีอนุสัญญาระหว่างประเทศเกี่ยวกับการต่อต้านการใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อวัตถุประสงค์ทางอาญา^๑ ซึ่งสหประชาชาติได้แต่งตั้งคณะกรรมการเฉพาะกิจเพื่อจัดทำอนุสัญญาระหว่างประเทศฉบับสมบูรณ์เพื่อต่อต้านการใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อวัตถุประสงค์ทางอาญา (Ad Hoc Committee to Elaborate a Comprehensive International Convention to Combat the Use Information Communication Technologies for Criminal Purposes) เพื่อจัดทำอนุสัญญาระหว่างประเทศฉบับสมบูรณ์ว่าด้วยการต่อต้านการใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อวัตถุประสงค์ทางอาญา จนกระทั่งมีมติอนุมัติร่างอนุสัญญาในเดือนสิงหาคม ๒๕๖๗^๒ และเสนอให้ที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติพิจารณา

ที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติได้ลงมติรับรองอนุสัญญาสหประชาชาติต่อต้านอาชญากรรมไซเบอร์ (United Nations Convention Against Cybercrime) เมื่อวันที่ ๒๔ ธันวาคม ๒๐๒๔ โดยมติที่ ๗๙/๒๔๓ และเปิดให้ลงนามเมื่อวันที่ ๒๕ ตุลาคม ๒๕๖๘ ในพิธีลงนามที่จัดขึ้น ณ กรุงฮานอย ประเทศเวียดนาม และที่สำนักงานใหญ่สหประชาชาติใน นครนิวยอร์กจนถึงวันที่ ๓๑ ธันวาคม ๒๕๖๙^๓ ปัจจุบันมีประเทศที่ลงนามอนุสัญญา ๗๘ ประเทศ และมีรัฐภาคี ๓ ประเทศที่ให้สัตยาบันต่ออนุสัญญาโดยสมบูรณ์ (ข้อมูล ณ วันที่ ๒๙ มิถุนายน ๒๕๖๙)^๔ ซึ่งประเทศไทยได้เข้าร่วมพิธีลงนามอนุสัญญาดังกล่าว^๕

* จัดทำโดยนางสาวนพรัตน์ พิริยานสรณ์ นักกฎหมายกฤษฎีกาชำนาญการพิเศษ ฝ่ายค้นคว้าและเปรียบเทียบกฎหมาย กองกฎหมายต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

^๑ Kevin Poireault, “UN Adopts Controversial Cybercrime Treaty”, สืบค้นเมื่อวันที่ ๒๙ มิถุนายน ๒๕๖๙, จาก UN Adopts Controversial Cybercrime Treaty - Infosecurity Magazine

^๒ United Nations, “Ad Hoc Committee to Elaborate a Comprehensive International Convention to Combat the Use Information Communication Technologies for Criminal Purposes”, สืบค้นเมื่อวันที่ ๒๙ มิถุนายน ๒๕๖๙, จาก Ad Hoc Committee - Home

^๓ United Nations, “United Nations Convention against Cybercrime”, สืบค้นเมื่อวันที่ ๒๙ มิถุนายน ๒๕๖๙, จาก United Nations Convention against Cybercrime

^๔ สืบค้นเมื่อวันที่ ๒๙ มิถุนายน ๒๕๖๙, จาก UNTC

^๕ กระทรวงการต่างประเทศ, “ไทยร่วมลงนามอนุสัญญาสหประชาชาติต่อต้านอาชญากรรมไซเบอร์”, สืบค้นเมื่อวันที่ ๓๐ มิถุนายน ๒๕๖๙, จาก ไทยร่วมลงนามอนุสัญญาสหประชาชาติต่อต้านอาชญากรรมไซเบอร์ - กระทรวงการต่างประเทศ

๒. สารสำคัญ

อนุสัญญาสหประชาชาติต่อต้านอาชญากรรมไซเบอร์ (United Nations Convention Against Cybercrime)^๖ เป็นสนธิสัญญาระหว่างประเทศในกรอบของสหประชาชาติฉบับแรก โดยมีวัตถุประสงค์ตามที่กำหนดไว้ใน Article 1 คือ (๑) ส่งเสริมและเสริมสร้างมาตรการในการป้องกันและปราบปรามอาชญากรรมไซเบอร์อย่างมีประสิทธิภาพและประสิทธิผลยิ่งขึ้น (๒) ส่งเสริม สนับสนุน และเสริมสร้างความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมไซเบอร์ และ (๓) ส่งเสริม สนับสนุน และช่วยเหลือด้านความช่วยเหลือทางเทคนิคและการเสริมสร้างศักยภาพในการป้องกันและปราบปรามอาชญากรรมไซเบอร์ โดยเฉพาะอย่างยิ่งเพื่อประโยชน์ของประเทศกำลังพัฒนา^๗

อนุสัญญาฯ ประกอบด้วย อาร์รัมบท บทที่ ๑ บทบัญญัติทั่วไป บทที่ ๒ การกำหนดความผิดทางอาญา บทที่ ๓ เขตอำนาจ บทที่ ๔ มาตรการเชิงกระบวนการและการบังคับใช้กฎหมาย บทที่ ๕ ความร่วมมือระหว่างประเทศ บทที่ ๖ มาตรการป้องกัน บทที่ ๗ ความช่วยเหลือทางวิชาการและการแลกเปลี่ยนข้อมูล บทที่ ๘ กลไกการอนุวัติการ และบทที่ ๙ บทบัญญัติสุดท้าย สรุปใจความสำคัญของอนุสัญญาฯ นี้ได้ ๓ ส่วน ดังนี้

(๑) การกำหนดความผิดทางอาญา เป็นการกำหนดให้รัฐภาคีต้องตรากฎหมายภายในเพื่อกำหนดให้การกระทำความผิดต่อไปนี้เป็นความผิดทางอาญา คือ (ก) การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยมิชอบ (ข) การดักจับข้อมูลโดยมิชอบ (ค) การแทรกแซงข้อมูลอิเล็กทรอนิกส์/ระบบเทคโนโลยีสารสนเทศและการสื่อสาร (ง) การใช้งานอุปกรณ์โดยมิชอบ (จ) การปลอมแปลงที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร (ฉ) การโจรกรรมหรือฉ้อโกงที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร (ช) การกระทำความผิดที่ข้องกับสื่อที่แสดงการล่วงละเมิดทางเพศต่อเด็กทางออนไลน์หรือการแสวงหาประโยชน์ทางเพศจากเด็ก (ซ) การล่อลวงหรือการเตรียมการเพื่อความมุ่งประสงค์ในการกระทำความผิดทางเพศต่อเด็ก (ฌ) การเผยแพร่ภาพส่วนตัวโดยไม่ได้รับความยินยอม และ (ญ) การฟอกทรัพย์สินที่ได้มาจากการกระทำความผิด

^๖ United Nations, United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes สืบค้นเมื่อวันที่ ๓๐ มิถุนายน ๒๕๖๙, จาก UN Cybercrime Convention - Full Text

^๗ **Article 1: Statement of purpose**

The purposes of this Convention are to:

(a) Promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively;

(b) Promote, facilitate and strengthen international cooperation in preventing and combating cybercrime; and

(c) Promote, facilitate and support technical assistance and capacity-building to prevent and combat cybercrime, in particular for the benefit of developing countries.

(๒) ความร่วมมือระหว่างประเทศ กำหนดหลักการทั่วไป การคุ้มครองข้อมูลส่วนบุคคล การส่งผู้ร้ายข้ามแดน การโอนตัวบุคคลผู้ต้องคำพิพากษา การโอนการดำเนินคดีอาญา หลักการและกระบวนการทั่วไปเกี่ยวกับความช่วยเหลือซึ่งกันและกันทางกฎหมาย เครือข่าย ๒๔/๗ (หมายถึงหน่วยงานติดต่อประสานงานที่สามารถติดต่อได้ตลอด ๒๔ ชั่วโมง/วัน ๗ วัน/สัปดาห์) ความร่วมมือในการบังคับใช้กฎหมาย การสืบสวนสอบสวนร่วม ความร่วมมือพิเศษ กลไกในการติดตามทรัพย์สินกลับคืนผ่านความร่วมมือระหว่างประเทศในการริบทรัพย์สิน การส่งคืนและจัดการทรัพย์สินที่ได้มาจากการกระทำความผิดหรือทรัพย์สินที่ถูกริบ ตลอดจนความร่วมมือระหว่างประเทศเพื่อความมุ่งประสงค์ต่าง ๆ ซึ่งได้แก่ (ก) การเก็บรักษาข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บไว้ (ข) การเปิดเผยข้อมูลจราจรที่เก็บรักษาไว้ (ค) การเข้าถึงข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บไว้ (ง) การเก็บรวบรวมข้อมูลจราจรตามเวลาจริง (จ) การดักจับข้อมูลเนื้อหา และ (ฉ) การริบทรัพย์สิน

(๓) ความช่วยเหลือทางเทคนิคและการแลกเปลี่ยนข้อมูล กำหนดให้รัฐภาคีต้องพิจารณาดำเนินการให้แก่กันและกันตามขีดความสามารถของตน โดยเฉพาะอย่างยิ่งเพื่อประโยชน์ของรัฐภาคีกำลังพัฒนา ทั้งการให้ความช่วยเหลือทางวิชาการและการเสริมสร้างขีดความสามารถ รวมถึงการฝึกอบรมและการให้ความช่วยเหลือในรูปแบบอื่น ๆ การแลกเปลี่ยนประสบการณ์ที่เกี่ยวข้องและความรู้เฉพาะทางร่วมกัน ตลอดจนการแลกเปลี่ยนข้อมูลระหว่างกัน

บทที่ ๓
มาตรการที่เกี่ยวข้องกับการป้องกันและปราบปราม
อาชญากรรมการหลอกลวงทางไซเบอร์ของต่างประเทศ

แคนาดา*

๑. บทนำ

ด้วยการพัฒนาเทคโนโลยีอย่างก้าวกระโดดในปัจจุบัน ส่งผลให้เกิดการวิวัฒนาการของเทคโนโลยีที่ถูกสร้างขึ้นเพื่อตอบสนองต่อความต้องการของมนุษย์อย่างรอบด้านซึ่งเข้ามามีบทบาทที่สำคัญและมีความจำเป็นต่อการดำรงชีวิตมนุษย์อย่างหลีกเลี่ยงไม่ได้ นำไปสู่ยุคของเทคโนโลยีดิจิทัล ส่งผลให้เกิดการยกระดับคุณภาพชีวิต เพิ่มประสิทธิภาพและเป็นประโยชน์ในการทำงานของบุคคล สร้างโอกาสรูปแบบใหม่ในด้านต่าง ๆ ที่หลากหลาย ตลอดจนอำนวยความสะดวกในชีวิตประจำวัน อย่างไรก็ตาม เทคโนโลยีอาจนำมาซึ่งภัยที่ไม่อาจคาดคิด เพราะมีฉาชีพหรือผู้ที่ไม่หวังดีอาจอาศัยประโยชน์จากเทคโนโลยีเป็นช่องทางในการกระทำความผิด เพื่อแสวงหาผลประโยชน์อันมิชอบด้วยกฎหมาย และด้วยการพัฒนาของเทคโนโลยีที่ดำเนินไปอย่างรวดเร็วและไม่หยุดยั้งในปัจจุบัน เทคโนโลยีอาจได้รับการพัฒนาในรูปแบบใหม่ ๆ เพื่อให้ได้มาซึ่งข้อมูลหรือแสวงหาประโยชน์อันมิชอบ นำไปสู่อาชญากรรมทางไซเบอร์ที่มีลักษณะเป็นการใช้อิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิด ซึ่งส่วนใหญ่นั้นจะกระทำผ่านเครือข่ายคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ที่มีการเชื่อมต่อเครือข่ายระหว่างกัน หรือกระทำผ่านช่องทางออนไลน์ต่าง ๆ เช่น โซเชียลมีเดีย เว็บไซต์ เป็นต้น ก่อให้เกิดความเสียหายแก่บุคคลและภาคธุรกิจ ตลอดจนความมั่นคงของประเทศ จึงเป็นความท้าทายในยุคเทคโนโลยีดิจิทัลที่ภาครัฐทั่วโลกต่างต้องรับมือในการแก้ไขปัญหาดังกล่าว

แคนาดาต้องเผชิญกับการก่ออาชญากรรมทางออนไลน์ในรูปแบบที่หลากหลาย ทั้งในรูปแบบการหลอกลวงผ่านการใช้เทคโนโลยีหรือ cyber scam เช่น การฉ้อโกงเพื่อหลอกลวงการลงทุน การหลอกลวงแบบ pig-butchering การลงทุนแบบฟิชซิง (Investment fraud phishing) การขโมยข้อมูลประจำตัว การกรรโชกทรัพย์ และรวมถึงกรณีที่เป็นอาชญากรรมทางไซเบอร์ในรูปแบบต่าง ๆ เช่น การโจมตีด้วย Ransomware และอื่น ๆ ทำให้ประชากรและภาคธุรกิจของแคนาดาได้รับความเสียหายอย่างยิ่ง ภาครัฐจึงได้จัดตั้งหน่วยงานกำกับดูแลเพื่อสอดส่องการกระทำความผิดและรับเรื่องราวจากประชาชน ตลอดจนการให้ความรู้ในด้านต่าง ๆ เพื่อให้ประชาชนได้ตระหนักถึงภัยดังกล่าวล่วงหน้าและรู้เท่าทันต่อกลโกงของมีฉาชีพ บทความฉบับนี้จึงได้นำเสนอถึงมาตรการทางกฎหมายของแคนาดาที่บังคับใช้เพื่อลงโทษผู้กระทำความผิดและตัวอย่างคดีที่น่าสนใจ

* จัดทำโดยนางสาวอรอร ฤกษ์ณะทรัพย์ บุคลากรจัดทำฐานข้อมูลกฎหมาย ฝ่ายค้นคว้าและเปรียบเทียบกฎหมาย กองกฎหมายต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

๒. สถานการณ์ภายในแคนาดา

อาชญากรรมทางไซเบอร์ที่เกิดขึ้นภายในแคนาดานั้น ตามข้อมูลของ Statistics Canada ปี ค.ศ. ๒๐๒๕ รายงานว่า อาชญากรรมที่ได้รับการรายงานจากเจ้าหน้าที่ตำรวจนั้นเพิ่มเป็น ๒๒๕.๑ เหตุการณ์ต่อประชากรจำนวน ๑๐๐,๐๐๐ คน ในปี ค.ศ. ๒๐๒๔ คิดเป็นอัตรา ๙๑.๙ เป็น ๒ เท่าในปี ค.ศ. ๒๐๑๘ ภาคธุรกิจของแคนาดาต้องสูญเสียค่าใช้จ่ายถึง ๑.๒ พันล้านดอลลาร์ฯ เพื่อเยียวยาความเสียหาย ในปี ค.ศ. ๒๐๒๓ ซึ่งเป็นจำนวนเงินที่เพิ่มขึ้นเป็น ๒ เท่าเมื่อเทียบกับปี ค.ศ. ๒๐๒๑ โดยครอบคลุมถึง เหตุการณ์ต่าง ๆ ที่ล้นกระทำโดยมิจฉาชีพ เช่น การใช้กลวิธีแบบ Ransomware กลวิธีแบบ Phishing การรั่วไหลของข้อมูล การขโมยข้อมูลส่วนบุคคล และภัยคุกคามจากต่างประเทศ

๒.๑ รูปแบบการหลอกลวงแบบ Cyber Scam ในปี ค.ศ. ๒๐๒๔ การฉ้อโกงเป็นความผิดที่มีการรายงานมากที่สุด โดยเกิดเหตุการณ์ทั้งสิ้น ๔๖,๓๐๑ ครั้ง ซึ่งคำนวณได้เป็นเกือบครึ่งหนึ่งของอาชญากรรมทางไซเบอร์ทั้งหมดที่ถูกรายงานโดยเจ้าหน้าที่ตำรวจ ความผิดเกี่ยวกับการฉ้อโกงนี้หมายรวมถึงการฉ้อโกง การขโมยข้อมูลส่วนบุคคล การฉ้อโกงข้อมูลส่วนบุคคล และการกรรโชกทรัพย์ โดยคิดเป็นร้อยละ ๖๒ นอกจากนี้ การฉ้อโกงการลงทุน (Investment fraud) การหลอกลวงด้วยความรัก (Romance scams) และการมุ่งเป้าหมายไปที่ผู้สูงอายุนั้นก็เป็นอีกรูปแบบหนึ่งของการฉ้อโกงที่เกิดขึ้นในแคนาดาด้วย

การใช้กลวิธีแบบ spear phishing และ Business Email Compromise หรือ BEC ได้สร้างความเสียหายรวมเป็นมูลค่าถึง ๖๗.๓ ล้านดอลลาร์แคนาดาในปี ค.ศ. ๒๐๒๔ ซึ่งเป็นความเสียหายจากอาชญากรรมไซเบอร์ที่ใหญ่เป็นอันดับ ๒ รองจากการฉ้อโกงการลงทุน โดยการหลอกลวงแบบ BEC นั้นมักอ้างว่าตนเป็นหน่วยงานของรัฐหรือองค์กรต่าง ๆ เช่น Canada Revenue Agency Canada Post และ Amazon อีกทั้งการหลอกลวงแบบ pig-butcher และการลงทุนแบบฟิชซิง (Investment fraud phishing)

ในปัจจุบันได้ใช้กลยุทธ์ทางสังคมรูปแบบแบบเดียวกันกับอาชญากรรมไซเบอร์ประเภท BEC ปัจจุบันมิจฉาชีพใช้ Large Language Models (LLMs) ในการสร้างข้อความฟิชซิงที่ปรับให้เหมาะสมกับกลุ่มเป้าหมายรายบุคคลในจำนวนมาก และสร้าง Deepfake ที่ทำให้เกิดการโจมตีทางวิศวกรรมสังคม (social engineering) ที่เกิดขึ้นภายในแคนาดาให้ตรวจจับได้ยากขึ้น ส่งผลทำให้จำนวนเหตุการณ์ที่เกี่ยวข้องกับความเสียหายที่เกิดจากการใช้ AI ที่ถูกรายงานต่อสาธารณะเพิ่มขึ้นจาก ๓๖ กรณีในปี ค.ศ. ๒๐๒๒ เป็นจำนวน ๑๐๗ กรณีในปี ค.ศ. ๒๐๒๓ และคาดว่าจะเพิ่มเป็น ๑๓๘ กรณีในปี ค.ศ. ๒๐๒๔

อีกทั้งมิจฉาชีพได้ใช้กลวิธีการขโมยข้อมูลประจำตัว (Identity Theft) ในภาคธุรกิจของแคนาดา สัดส่วนของธุรกิจที่รายงานว่าได้รับผลกระทบเพิ่มขึ้นจากร้อยละ ๒๐ เป็นร้อยละ ๓๑ ในระหว่างปี ค.ศ. ๒๐๒๑ - ๒๐๒๓ ชาวแคนาดาอายุ ๑๕ ปีขึ้นไปประมาณร้อยละ ๗.๘ หรือประมาณ ๒.๕ ล้านคน ก็ตกเป็นเหยื่อของการฉ้อโกง อย่างไรก็ตาม มีเพียงร้อยละ ๑๑ ของเหยื่อเหล่านั้นที่ได้แจ้งเหตุให้ตำรวจทราบ โดยผู้ที่ใช้อินเทอร์เน็ตมีโอกาสตกเป็นเหยื่อการฉ้อโกงมากกว่าผู้ที่ไม่เคยใช้อินเทอร์เน็ตเกือบ ๓ เท่า โดยผู้สูงอายุภายในแคนาดาได้รับความเสียหายจากการหลอกลวงทางเทคโนโลยีและการปลอมแปลงตัวตน (Tech-impersonation phishing) ในสัดส่วนที่สูงกว่ากลุ่มอื่นเป็นอย่างมากจากการที่มิจฉาชีพแอบอ้างว่าเป็นเจ้าหน้าที่จากกรมสรรพากร

๒.๒ รูปแบบอาชญากรรมทางไซเบอร์แบบอื่น ๆ การใช้กลวิธีแบบ Ransomware เพิ่มขึ้นเฉลี่ยถึงร้อยละ ๒๖ ต่อปีในระหว่างปี ค.ศ. ๒๐๒๑ ถึง ค.ศ. ๒๐๒๔ ค่าไถ่ที่องค์กรภายในแคนาดา ต้องจ่ายเพิ่มขึ้นนั้นเฉลี่ยถึง ๑.๑๓ ล้านดอลลาร์แคนาดาในปี ค.ศ. ๒๐๒๓ ซึ่งเพิ่มขึ้นเป็นร้อยละ ๑๕๐ ภายในสองปี สำหรับสถิติในระดับโลกนั้น การจ่ายค่าไถ่ได้ทำสถิติสูงสุดที่ ๑ พันล้านดอลลาร์สหรัฐฯ ในปี ค.ศ. ๒๐๒๓ แคนาดาต้องเผชิญความท้าทายกับ Ransomware ในเหตุการณ์ต่าง ๆ ดังต่อไปนี้

เดือนธันวาคม ค.ศ. ๒๐๒๒ เหตุเกิด ณ โรงพยาบาล SickKids ถูกโจมตีด้วย Ransomware ซึ่งรบกวนระบบการดูแลผู้ป่วยที่ The Hospital for Sick Children ในเขตเมือง Toronto ต่อมาในเดือน ตุลาคม ค.ศ. ๒๐๒๓ โรงพยาบาล ๕ แห่งในแถบเมือง Southern Ontario ถูกโจมตีด้วย Ransomware แบบประสานงานที่เกิดขึ้นอย่างพร้อมเพรียงกัน ส่งผลทำให้ต้องส่งต่อผู้ป่วยไปยังโรงพยาบาลอื่น และ ส่งผลให้เกิดความล่าช้าในการทำการหัตถการให้แก่ผู้ป่วย

ต่อมาคือ เหตุการณ์ MOVEit supply-chain ในเดือนมิถุนายน ค.ศ. ๒๐๒๓ กลุ่ม ClOp Ransomware ได้ใช้ประโยชน์จากช่องโหว่แบบ Zero-day ภายในซอฟต์แวร์ MOVEit Transfer ทำให้ เกิดการบุกรุกองค์กรประมาณ ๒,๗๕๐ แห่งและส่งผลกระทบต่อผู้คนจำนวน ๙๔ ล้านคนทั่วโลก สำหรับ ในแคนาดานั้น เกิดการรั่วไหลข้อมูลของเจ้าหน้าที่รัฐของรัฐ Nova Scotia จำนวน ๑๐๐,๐๐๐ คน ต่อมา ในช่วงปี ค.ศ. ๒๐๒๔-๒๐๒๕ ได้มีการแจ้งเตือน CCCS pre-ransomware ระบุว่า Canadian Centre for Cyber Security ได้ออกการแจ้งเตือน Pre-ransomware notifications จำนวน ๓๓๖ ครั้งแก่องค์กร ในแคนาดา มากกว่า ๓๐๐ แห่งในช่วงปี ค.ศ. ๒๐๒๔-๒๐๒๕ ซึ่งช่วยประหยัดความเสียหายทางเศรษฐกิจ ได้สูงถึง ๑๘ ล้านดอลลาร์แคนาดา^๑

รัฐบาลแคนาดาได้เตือนภัยแก่ประชาชนเพื่อให้เกิดการตระหนักรู้เท่าทันถึงสัญญาณของ กลโกงที่มีฉฉฉฉนั้นสามารถใช้ปัญญาประดิษฐ์เพื่อสร้างข้อความ รูปภาพ และเว็บไซต์ที่เสมือนจริงได้ ซึ่ง มักจะเลียนแบบหน่วยงานของรัฐหรือเจ้าหน้าที่รัฐเพื่อให้เข้าถึงข้อมูลส่วนบุคคลและข้อมูลทางการเงิน หากมีลักษณะที่มีการเรียกร้องให้ชำระเงินอย่างทันที การใช้ภาษาที่มีลักษณะข่มขู่ การส่งลิงค์และขอให้ ผู้รับคลิกลิงค์ดังกล่าว การขอให้ชำระเงินเพื่อปล่อยหรือกู้คืนเงินทุน (Recover funds) การขอข้อมูลส่วนบุคคลหรือข้อมูลทางการเงิน การขอให้ชำระเงินด้วยสกุลเงินดิจิทัลหรือบิตคอยน์ของขบวนการ ทั้งนี้ ประชาชน โปรดใช้เวลาทบทวนก่อนการดำเนินการดังกล่าว หากไม่แน่ใจติดต่อแผนกหรือหน่วยงานของรัฐโดยตรง

มีฉฉฉฉมักใช้กลโกงที่เกี่ยวข้องกับการให้บริการของรัฐ โดยสร้างว่ามาจากแผนกงาน ของรัฐหรือหน่วยงานของรัฐ เช่น หน่วยงานที่ให้บริการของแคนาดา (Service Canada) กรมสรรพากร สำนักงานตรวจคนเข้าเมือง หน่วยงานเกี่ยวกับการบริการเกี่ยวกับชายแดน ศูนย์ต่อต้านการฉ้อโกงแห่ง แคนาดา (Canadian Anti-Fraud Centre) หากพบเห็นมีฉฉฉฉอ้างว่าตนมาจากหน่วยงานดังกล่าว รัฐบาลได้ขอให้ประชาชนนั้นรายงานการพบเห็นไปถึงเว็บไซต์ของหน่วยงานเหล่านี้^๒

^๑ James Ganvilla, “Cybercrime Statistics Canada [2026]”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๙, จาก Cybercrime Statistics Canada [2026]

^๒ Royal Canadian Mounted Police, “Cybercrime and the Criminal Code”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๙, จาก Scams and fraud - Government of Canada - Canada.ca.

สถิติการรายงานของอาชญากรรมทางไซเบอร์ที่เกิดขึ้นในแคนาดา สรุปได้ตามตารางดังต่อไปนี้

ปี	อัตราการรายงานของ เจ้าหน้าที่ตำรวจ (ต่อประชากร ๑๐๐,๐๐๐ คน)	ความสูญเสียที่ รายงานโดย CAFC	ร้อยละของธุรกิจ ที่ได้รับผลกระทบ
2018	91.9	-	
2019	-	-	21%
2021	-	\$383M	18%
2022	-	\$530M	-
2023 (peak)	~246 (est.)	\$567M	16%
2024	225.1	\$638M	-

ตารางแสดงอัตราการเกิดอาชญากรรมทางไซเบอร์ภายในแคนาดา

ที่มาของภาพ : *Cybercrime Statistics Canada [2026]*

ภูมิภาค	อัตราการรายงานของ เจ้าหน้าที่ตำรวจ (ต่อประชากร ๑๐๐,๐๐๐ คน ในปี ค.ศ.๒๐๒๔)	หมายเหตุ
British Columbia	423.0	Highest provincial rate
National average	225.1	Statistics Canada UCR 2024
Large cities	237.7	Rate in Canada's largest CMAs
Smaller towns	186.8	Rate in smaller urban areas
Nunavut	114.2	Lowest territorial rate
Alberta (self-reported fraud, 5-yr)	22% victimization rate	2019 GSS, most recent available
Atlantic provinces (self-reported fraud, 5-yr)	13–14% victimization rate	2019 GSS, most recent available

ตารางแสดงอัตราการเกิดอาชญากรรมทางไซเบอร์ตามจังหวัดและขนาดของเมือง

ที่มาของภาพ : *Cybercrime Statistics Canada [2026]*

๓. มาตรการทางกฎหมายเพื่อบังคับใช้กับการแก้ไขปัญหาอาชญากรรมทางไซเบอร์

ภายใต้กฎหมายของแคนาดาได้กำหนดให้คำว่า “อาชญากรรมทางไซเบอร์ (Cyber-crime)” นั้นครอบคลุมถึงกิจกรรม ๒ ประเภท ดังนี้

(๑) การกระทำความผิดที่ใช้ระบบไซเบอร์ (Cyber-dependent offences) คืออาชญากรรมที่สามารถกระทำได้โดยผ่านเทคโนโลยีดิจิทัลเท่านั้น

(๒) การกระทำความผิดผ่านระบบไซเบอร์ (Cyber-enabled offences) คืออาชญากรรมที่กระทำในรูปแบบแบบดั้งเดิมที่มีการขยายลักษณะการกระทำเพิ่มประสิทธิภาพขึ้นหรือเพิ่มประสิทธิภาพด้วยเทคโนโลยี เช่น การฉ้อโกงและการขโมยข้อมูลส่วนบุคคล^๓

ทั้งนี้ อาจพิจารณาได้อีกแง่หนึ่งว่า การแบ่งประเภทอาชญากรรมทางไซเบอร์ในแคนาดานั้นแบ่งได้ ๒ ประเภท คือ การใช้เทคโนโลยีเป็นเป้าหมาย (Technology-as-target) ที่ผู้กระทำความผิดอาจใช้คอมพิวเตอร์หรือซอฟต์แวร์ที่เป็นอันตรายเพื่อขโมยข้อมูลส่วนบุคคลหรือก่อการทางออนไลน์ และการใช้เทคโนโลยีเป็นเครื่องมือ (Technology-as-instrument) ที่ผู้กระทำความผิดอาจใช้อินเทอร์เน็ตหรือเทคโนโลยีอื่น ๆ เพื่อก่ออาชญากรรม เช่น การขโมยข้อมูลส่วนบุคคลหรือการฉ้อโกง

๓.๑ ประมวลกฎหมายอาญาของแคนาดา (The criminal code of Canada) ได้บัญญัติความรับผิดทางอาญาของอาชญากรรมทางไซเบอร์ไว้ในมาตราต่าง ๆ ที่กำหนดลักษณะการกระทำและความรับผิดไว้ ดังนี้^๔

อนุมาตรา ๔๓๐(๑.๑) การทำลายข้อมูลคอมพิวเตอร์ (Mischief in relation to computer data) เป็นความผิดที่บัญญัติไว้สำหรับการกระทำความผิดโดยเจตนาที่ผู้กระทำนั้นได้ลบทำลาย หรือเปลี่ยนแปลงข้อมูลใด ๆ ในคอมพิวเตอร์ ขัดขวางหรือแทรกแซงการใช้ข้อมูลคอมพิวเตอร์โดยชอบด้วยกฎหมาย หรือป้องกันหรือกีดกันไม่ให้บุคคลอื่นเข้าถึงข้อมูลคอมพิวเตอร์โดยชอบด้วยกฎหมาย

กรณีตัวอย่าง

- Adam แอบดูเพื่อนขณะกำลังกรอกชื่อผู้ใช้งานหรือ Username และรหัสผ่านหรือ password และเข้าใช้งานบัญชีของเพื่อนโดยไม่ได้รับอนุญาต และลบข้อความออกจากบัญชีดังกล่าว

- ขณะเล่นเกมออนไลน์ Sarah พบว่าเพื่อนของเธอทำคะแนนได้สูงกว่า ด้วยความหงุดหงิด Sarah จึงใช้เครื่องมือ Distributed Denial-of-Service (DDoS) หรือที่เรียกว่า “booter” เพื่อทำให้เพื่อนของเธอนั้นหลุดออกจากระบบและไม่สามารถใช้งานการเชื่อมต่อได้

มาตรา ๓๔๒.๑ การใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาต (Unauthorized use of a computer) เป็นความผิดที่บัญญัติไว้สำหรับการกระทำความผิดบุคคลใดบุคคลหนึ่งกระทำโดยทุจริตได้เข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ใช้อุปกรณ์ดักจับ (ยกตัวอย่างเช่น การดักฟังหรือบันทึก) หรือการทำงานใด ๆ ของระบบคอมพิวเตอร์ การใช้ระบบคอมพิวเตอร์โดยมีเจตนาที่จะกระทำความผิดและการจัดการรหัสผ่านให้ผู้อื่น โดยรหัสผ่านนั้นทำให้บุคคลดังกล่าวสามารถก่ออาชญากรรมได้

^๓ James Ganvilla, “Cybercrime Statistics Canada [2026]”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๙, จาก Cybercrime Statistics Canada [2026]

^๔ Royal Canadian Mounted Police, “Cybercrime and the Criminal Code”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๙, จาก Cybercrime and the Criminal Code | Royal Canadian Mounted Police

กรณีตัวอย่าง

- Jason เป็นโปรแกรมเมอร์ที่มีความรู้ความสามารถด้านคอมพิวเตอร์ ได้แฮ็กเข้าไปในบริษัทโทรศัพท์เพื่อลดค่าบริการรายเดือน

- Sophie เข้าถึงรายชื่อของรหัสผ่านที่ถูกขโมยบน Dark web และขายข้อมูลเหล่านั้นบางส่วนให้กับเพื่อน โดยรู้ดีว่ารหัสผ่านเหล่านั้นจะถูกนำไปใช้เพื่อเข้าสู่บัญชีธนาคารของเหยื่อได้

- Edward แอบเข้าไปในห้องทำงานของผู้จัดการและติดตั้งอุปกรณ์เข้ากับคอมพิวเตอร์ของผู้จัดการ ซึ่งอุปกรณ์นั้นจะบันทึกทุกสิ่งที่ผู้จัดการพิมพ์ลงในคอมพิวเตอร์

มาตรา ๓๔๒.๒ การครอบครองอุปกรณ์ที่ใช้ในการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต หรือเพื่อก่อให้เกิดความเสียหาย (Possession of a device used to obtain unauthorized use of computer system or to commit mischief)

กรณีตัวอย่าง ในเวลาว่าง Andrew จะดัดแปลงโปรแกรมโทรศัพท์มือถือเพื่อให้สามารถแฮ็กอุปกรณ์อื่น ๆ ได้ง่ายขึ้น จากนั้นเขาก็ขายโทรศัพท์เหล่านั้นให้กับเพื่อน ๆ ที่เชี่ยวชาญด้านเทคโนโลยี

มาตรา ๑๘๔ การดักฟังการสื่อสาร (Interception of communications)
บทบัญญัติที่กำหนดความรับผิดให้กับบุคคลที่จงใจดักฟังการสื่อสารแบบส่วนตัวโดยใช้อุปกรณ์แม่เหล็กไฟฟ้า อุปกรณ์เสียง อุปกรณ์กลไก หรืออุปกรณ์อื่นใด

กรณีตัวอย่าง Leah ตั้งค่าโทรศัพท์ให้มีการบันทึกเสียงและวางไว้ในห้องกับเพื่อน ๆ โดยที่พวกเขาไม่รู้ และเธอก็ได้ฟังบทสนทนาส่วนตัวของพวกเขาเกี่ยวกับตัวเธอ

อนุมาตรา ๓๔๖(๑) การกรรโชกทรัพย์ (Extortion)

กรณีตัวอย่าง Stephanie ได้รับภาพส่วนตัวจากคนที่เธอคุยด้วยทางออนไลน์ โดยบอกกับคนนั้นว่า ถ้าไม่โอนเงินให้ ภาพนั้นจะถูกนำไปเผยแพร่ให้กับครอบครัวและเพื่อน ๆ

อนุมาตรา ๔๐๒.๒ การขโมยข้อมูลประจำตัว (Identity Theft)

กรณีตัวอย่าง Kevin นำหมายเลขประกันสังคม (social insurance number) ของแฟนสาวไปใช้ และใช้ข้อมูลนั้นในการกรอกใบสมัครกู้เงินทางออนไลน์ จากนั้น เขาได้รับเงินกู้ดังกล่าวโดยใช้หมายเลขประกันสังคมและวันเดือนปีเกิดของแฟนสาว

มาตรา ๔๐๓ การฉ้อโกงโดยใช้ข้อมูลประจำตัว (Identity fraud)

กรณีตัวอย่าง พ่อของ Amanda เป็นเจ้าของธุรกิจขนาดเล็ก Amanda แอบอ้างเป็นพ่อของตน และใช้บัญชีอีเมลปลอมในการส่งอีเมลถึงลูกค้าเพื่อขอให้ลูกค้าดำเนินการชำระเงินไปยังบัญชีธนาคารของเธอ

๓.๒ กฎหมาย Canada's anti-spam legislation (CASL) มีผลบังคับใช้ในปี ค.ศ. ๒๐๑๔ มีวัตถุประสงค์เพื่อคุ้มครองผู้บริโภคและภาคธุรกิจจากการใช้เทคโนโลยีดิจิทัลในทางที่ผิด รวมถึง spam และภัยคุกคามทางอิเล็กทรอนิกส์อื่น ๆ นอกจากนี้ ยังช่วยให้ธุรกิจต่าง ๆ สามารถแข่งขันได้ภายใน

ตลาดดิจิทัลในระดับโลก ส่งเสริมให้เกิดการเรียนรู้กฎหมาย ตลอดจนวิธีการป้องกันตนเองจาก spam และการรายงานในกรณีที่มีความจำเป็น^๕

กฎหมาย CASL กำหนดบทบัญญัติเกี่ยวกับฐานความผิด กลไกการบังคับใช้ และบทลงโทษที่มีความรุนแรง รวมถึงความรับผิดชอบของนายจ้าง กรรมการบริษัท และเจ้าหน้าที่ของบริษัท โดยมีวัตถุประสงค์เพื่อห้ามการส่งข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ Commercial electronic messages (“CEMs”) ที่ไม่ได้รับการร้องขอหรือมีลักษณะเป็นการหลอกลวง ตลอดจนการติดตั้งและการใช้โปรแกรมคอมพิวเตอร์ที่ใช้เพื่อวัตถุประสงค์ทางการค้าภายในระบบคอมพิวเตอร์ของบุคคลอื่นโดยไม่ได้รับอนุญาต รวมทั้งการฉ้อโกงทางออนไลน์ในรูปแบบอื่น ๆ เช่น การขโมยข้อมูลประจำตัว (Identity theft) และการหลอกลวงแบบฟิชซิง (phishing)^๖ สำหรับบทลงโทษนั้นอยู่ในรูปแบบค่าปรับเป็นตัวเงิน (Administrative monetary penalties: AMPs) การกำหนดค่าปรับจะพิจารณาจากปัจจัยหลายประการ ได้แก่ ลักษณะของการกระทำ ประวัติการทำความผิดว่าเคยฝ่าฝืนกฎหมาย CASL ในอดีตหรือไม่ บริษัทได้รับประโยชน์ทางการเงินจากการทำความผิดหรือไม่ และความสามารถของบริษัทในการชำระค่าปรับ ซึ่งค่าปรับนั้นอาจสูงถึง ๑ ล้านดอลลาร์สำหรับบุคคลธรรมดา และ ๑๐ ล้านดอลลาร์สำหรับธุรกิจ^๗

กฎหมายฉบับนี้ ห้ามการส่งข้อความอิเล็กทรอนิกส์เชิงพาณิชย์ (Commercial electronic messages: CEMs) ไปยังที่อยู่อีเมลใด ๆ เว้นแต่ผู้ส่งจะได้รับความยินยอมเช่นนั้นและข้อความนั้นต้องเป็นไปตามข้อกำหนดที่ระบุไว้ในกฎหมาย ซึ่งข้อความอิเล็กทรอนิกส์ที่ใช้ในเชิงพาณิชย์ หรือ CEMs คือ ข้อความทางอิเล็กทรอนิกส์ที่ก่อให้เกิดการกระตุ้นการมีส่วนร่วมในกิจกรรมเชิงพาณิชย์ หมายรวมถึงกรณีดังต่อไปนี้

- (ก) ข้อเสนอในการซื้อ ขาย แลกเปลี่ยน หรือเช่าสินค้าหรือบริการ
 - (ข) ข้อเสนอในการให้โอกาสทางธุรกิจ การลงทุน หรือการพนัน
 - (ค) การโฆษณาหรือส่งเสริมกิจกรรมในข้อ (ก) และ (ข) และ
 - (ง) การส่งเสริมให้บุคคลกระทำหรือจะทำกิจกรรมใด ๆ ตามที่กำหนดไว้ในข้อ (ก) ถึง (ค)
- ข้อความอิเล็กทรอนิกส์นั้น หมายรวมถึงข้อความที่ส่งผ่านด้วยวิธีการสื่อสารผ่านทางไกล

ใด ๆ เช่น ข้อความตัวอักษร เสียง คำพูด หรือภาพ^๘

^๕ Government of Canada, “Canada's anti-spam legislation”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๙, จาก Canada's anti-spam legislation

^๖ BORDEN LADNER GERVAIS LLP, “Preparing for CASL’s Private Right of Action”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๙, หน้า ๑, จาก Publication_4930.pdf

^๗ Government of Canada, “Understanding Canada’s anti-spam legislation”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๙, จาก Understanding Canada’s anti-spam legislation

^๘ Mark Blumberg and Yi-Mei Ting, “Canada’s Anti-Spam Legislation (CASL) for Canadian Registered Charities and Non-profit Organizations”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๙, จาก Canadas_Anti-Spam_Legislation_(CASL).pdf

สาระสำคัญของกฎหมายฉบับนี้ได้กำหนดถึงแนวทางสำหรับวิธีการที่ธุรกิจต่างๆ สามารถส่ง CEMs ไว้อย่างเข้มงวด ไม่ว่าจะเป็นการส่งผ่านทางอีเมล ข้อความ หรือการสื่อสารทางอิเล็กทรอนิกส์อื่น ๆ โดยองค์กรต่าง ๆ ต้องปฏิบัติตามข้อกำหนดดังนี้

๑. การได้รับความยินยอม (consent) ก่อนการส่งอีเมลทางการตลาดใด ๆ ธุรกิจต้องได้รับความยินยอมโดยชัดแจ้ง (Express consent) หรือความยินยอมโดยปริยาย (Implied consent) จากผู้รับ ซึ่งความยินยอมโดยชัดแจ้งนั้นเป็นกรณีที่บุคคลได้ตกลงอย่างชัดเจนที่จะรับข้อความนั้น ๆ เช่น การทำเครื่องหมายในช่องการสมัครรับข้อมูลบนเว็บไซต์ และความยินยอมโดยปริยาย เช่น ความสัมพันธ์ทางธุรกิจที่มีอยู่เดิม

๒. การระบุตัวตนอย่างชัดเจน (Clear Identification) CEMs ต้องระบุตัวตนผู้ส่งอย่างชัดเจน รวมถึงชื่อธุรกิจและข้อมูลการติดต่อ เพื่อให้ผู้รับทราบถึงข้อมูลผู้ติดต่อ

๓. การยกเลิกการสมัครการรับข้อมูล (Unsubscribe Mechanism) อีเมลทางการตลาดทุกฉบับต้องมีวิธีการที่ชัดเจนและใช้งานง่ายในการที่ผู้รับสามารถยกเลิกการสมัครรับข้อมูล หากมีการขอให้ยกเลิกการสมัครรับข้อมูลแล้ว จะต้องดำเนินการภายใน ๑๐ วัน และห้ามขอการยืนยันเพิ่มเติมใด ๆ อีก^๙

CASL ได้เสริมสร้างแนวทางปฏิบัติที่ดีในการทำงานด้านการตลาดผ่านช่องทางอีเมลและต่อสู้กับ spam และภัยคุกคามทางไซเบอร์ที่เกี่ยวข้อง ภัยคุกคามเหล่านี้รวมถึงการขโมยข้อมูลส่วนบุคคล การหลอกลวงผ่านทางอีเมล และการแพร่กระจายของซอฟต์แวร์ที่เป็นอันตราย เช่น Virus Worm และ Malware เดิมแคนาดานั้นเคยเป็นที่ตั้งขององค์กรที่เกี่ยวกับการส่ง spam เป็นลำดับที่ ๗ จาก ๑๐๐ อันดับแรกของโลก ภายหลังการบังคับใช้กฎหมายฉบับนี้ ในปี ค.ศ. ๒๐๑๔ และจนถึงปัจจุบัน ก็ทำให้ไม่มีองค์กรของแคนาดาอยู่ในรายชื่อตามอันดับดังกล่าวอีกต่อไป^{๑๐} หน่วยงานที่รับผิดชอบต่อการบังคับใช้กฎหมายดังกล่าว ได้แก่ Canadian Radio-television and Telecommunications Commission หรือ CRTC มีอำนาจกำหนดค่าปรับสำหรับการฝ่าฝืนบทบัญญัติมาตรา ๖ ถึงมาตรา ๙ ของกฎหมาย CASL

สำนักงาน Competition Bureau มีอำนาจดำเนินการเพื่อขอให้พิจารณาการกำหนดค่าปรับหรือดำเนินมาตรการการลงโทษทางอาญาตามกฎหมาย Competition Act และ Office of the Privacy Commissioner of Canada มุ่งเน้นการบังคับใช้กฎหมายในกรณีการกระทำความผิด ๒ ลักษณะ คือ (๑) การรวบรวมข้อมูลส่วนบุคคลโดยการเข้าถึงระบบคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์อย่างผิดกฎหมาย (กระทำได้ผ่านทาง Spyware จากการรวบรวมข้อมูลที่ปราศจากความยินยอมและสามารถเปลี่ยนแปลงวิธีการทำงานของคอมพิวเตอร์นั้น ๆ) และ (๒) การเก็บรวบรวมที่อยู่อีเมล^{๑๑}

^๙ Jan Gellago, “What is Canada’s Anti-Spam Legislation (CASL)?”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๔, จาก What is Canada’s Anti-Spam Legislation (CASL)? - GetTerms

^{๑๐} Government of Canada, “Canada’s anti-spam legislation”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๔, จาก Canada’s anti-spam legislation

^{๑๑} Government of Canada, “Understanding Canada’s anti-spam legislation”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๔, จาก Understanding Canada’s anti-spam legislation

๓.๓ กฎหมาย BILL C-8 An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts วัตถุประสงค์ของกฎหมายฉบับนี้มุ่งเน้นการสนับสนุนความมั่นคงของระบบโทรคมนาคมของประเทศ และยกระดับความมั่นคงปลอดภัยทางไซเบอร์ในภาคส่วนต่าง ๆ ได้แก่ ภาคการเงิน โทรคมนาคม พลังงาน และการขนส่ง

กฎหมายฉบับนี้ได้แก้ไขเพิ่มเติมกฎหมาย Telecommunications Act เพื่อแสดงถึงนโยบายและมอบอำนาจให้แก่รัฐบาลในการสั่งการเพื่อดำเนินการรับมือภัยคุกคามต่อระบบโทรคมนาคม นอกจากนี้ ได้นำเสนอร่างกฎหมาย Critical Cyber Systems Protection Act ซึ่งกำหนดกรอบการกำกับดูแลให้แก่ผู้ประกอบการที่ในภาคการเงิน โทรคมนาคม พลังงาน และการขนส่ง โดยต้องดำเนินการคุ้มครองระบบไซเบอร์ของตน ทั้งนี้ การแก้ไขเพิ่มเติม Telecommunications Act จะมีผลบังคับใช้ทันทีเมื่อได้รับพระบรมราชานุญาต ส่วนกฎหมาย Critical Cyber Systems Protection Act จะดำเนินการอย่างค่อยเป็นค่อยไปโดยบทบัญญัติบางประการจะทยอยมีผลบังคับใช้ตามลำดับขั้นตอน

การนำกฎหมายฉบับนี้มาบังคับใช้นั้น นับว่าเป็นเรื่องสำคัญอย่างยิ่งสำหรับชาวแคนาดา เนื่องจากช่วยปกป้องโครงสร้างพื้นฐานที่สำคัญจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างต่อเนื่องและมีความซับซ้อนเพิ่มมากขึ้น กฎหมายฉบับนี้กำหนดให้องค์กรต้องดำเนินมาตรการรักษาความปลอดภัยให้มีความเข้มงวดมากยิ่งขึ้น ต้องรายงานเหตุการณ์สำคัญที่เกิดขึ้น และมีความรับผิดชอบต่อการทำงานของตน โดยจะช่วยคุ้มครองด้านความปลอดภัย ความเป็นส่วนตัว และเสถียรภาพทางเศรษฐกิจของชาวแคนาดา โดยรับประกันว่าการบริการที่จำเป็นต่าง ๆ นั้นจะยังคงมั่นคงปลอดภัย และสามารถดำเนินงานต่อไปท่ามกลางความเสี่ยงทางดิจิทัลที่เกิดความเปลี่ยนแปลงอยู่ตลอดเวลา^{๑๒}

๔. ตัวอย่างคดีที่น่าสนใจ

ในปี ค.ศ.๒๐๑๕ บริษัท CompuFinder ส่งอีเมลโฆษณาบริการด้านการศึกษาและการฝึกอบรมโดยไม่ได้รับอนุญาตจำนวน ๓ แคมเปญ จึงก่อให้เกิดการร้องเรียนมายังศูนย์ Spam Reporting Centre และนำไปสู่การสืบสวน จึงมีการออกหนังสือแจ้งเตือนพร้อมกำหนดโทษปรับทางปกครอง (Administrative Monetary Penalty: AMP) เป็นจำนวน ๑.๑ ล้านดอลลาร์

CompuFinder ได้ยื่นคำร้องต่อ Canadian Radio-television and Telecommunications Commission CRTC เพื่อขอให้ทบทวนหนังสือแจ้งเตือนดังกล่าว โดยบริษัทมีข้อต่อสู้ว่าอีเมลของตนนั้นได้รับการยกเว้นแบบ business-to-business exemption หรือการส่งโดยอาศัยความยินยอมโดยปริยาย รวมถึงอีเมลนั้นมีกลไกการยกเลิกการรับข้อมูล (Unsubscribe mechanism) ที่ถูกต้องครบถ้วน นอกจากนี้ บริษัทยังทำทนายความขอด้วยรัฐธรรมนูญของกฎหมาย CASL อีกด้วย

CRTC มีคำวินิจฉัย ๒ ฉบับ ฉบับแรกระบุว่ากฎหมาย CASL นั้นชอบด้วยรัฐธรรมนูญและไม่ขัดต่อ Canadian Charter of Rights and Freedoms และในฉบับที่สองระบุว่า CompuFinder

^{๑๒} Government of Canada, “Government of Canada Strengthens Cyber Security and Critical Infrastructure with Royal Assent of Bill C-8”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๔, จาก Government of Canada Strengthens Cyber Security and Critical Infrastructure with Royal Assent of Bill C-8 - Canada.ca

ได้ฝ่าฝืนกฎหมาย CASL ด้วยการส่ง CEMs โดยไม่ได้รับความยินยอม และไม่มีกลไกการยกเลิกการรับข้อมูลที่เป็นไปตามข้อกำหนด เนื่องจากอีเมลแต่ละฉบับมีกลไกการยกเลิกการรับข้อมูลชุดที่ ๒ ที่ไม่สามารถใช้งานได้ อย่างไรก็ตาม CRTC พิจารณาแล้วเห็นว่าโทษปรับ ๑.๑ ล้านดอลลาร์ที่ระบุในหนังสือแจ้งเตือนนั้นสูงเกินสมควร จึงกำหนดโทษปรับใหม่เป็นจำนวน ๒๐๐,๐๐๐ ดอลลาร์แทน

CompuFinder ได้ยื่นอุทธรณ์ต่อคำวินิจฉัยของ CRTC ต่อศาลอุทธรณ์กลาง (Federal Court of Appeal) แต่ศาลอุทธรณ์ดังกล่าวโดยวินิจฉัยว่า CASL นั้นชอบด้วยรัฐธรรมนูญ เพราะอยู่ในอำนาจนิติบัญญัติของรัฐสภาเกี่ยวกับการค้าและพาณิชย์ที่ส่งผลกระทบต่อประเทศแคนาดาทั้งหมด นอกจากนี้ กฎหมายนี้ไม่ได้ละเมิดต่อ Charter of Rights and Freedoms เนื่องจากการจำกัดเสรีภาพในการแสดงออกเชิงพาณิชย์ที่ได้รับความคุ้มครองตามรัฐธรรมนูญอย่างสมเหตุสมผล และไม่ได้ละเมิดสิทธิอื่น ๆ ที่ได้รับการคุ้มครองตามกฎหมายเช่นว่านี้ และศาลพิจารณาว่า CRTC ไม่ได้บังคับใช้ข้อยกเว้น business-to-business exemption ผิดไป เพราะองค์กรผู้ส่งต้องมีความสัมพันธ์ทางธุรกิจกับองค์กรผู้รับอย่างแท้จริง ไม่ใช่แค่เพียงกับพนักงานบางคนเท่านั้น ความสัมพันธ์ระหว่างองค์กรผู้ส่งและองค์กรผู้รับ CEM นั้นต้องมีความเข้มข้นมากกว่าความสัมพันธ์ทางธุรกิจเดิมที่มีอยู่ เพื่อใช้สร้างความยินยอมโดยปริยายของบุคคล เพราะข้อยกเว้นนี้อุญาตให้ส่ง CEM ไปยังพนักงานทั้งหมดขององค์กรผู้รับได้ แต่ความสัมพันธ์ตามสัญญาที่มีธุรกรรมเพียงเล็กน้อยและส่งผลกระทบต่อพนักงานเพียงไม่กี่คนนั้น ก็ไม่ถือว่าเป็นความสัมพันธ์ตามนัยของข้อยกเว้นดังกล่าว

CASL ระบุว่า บุคคลจะถือว่าให้ความยินยอมโดยปริยาย เพื่อรับ CEMs ที่ส่งไปยังที่อยู่อีเมลของตน หากเข้าเงื่อนไขดังนี้ (ก) บุคคลนั้นได้เผยแพร่หรือให้มีการเผยแพร่ที่อยู่อีเมลของตนอย่างชัดเจน (ข) การเผยแพร่ไม่ได้ระบุว่าบุคคลไม่ต้องการรับ CEMs ที่ไม่ได้ร้องขอในอีเมลดังกล่าว และ (ค) CEMs ต้องเกี่ยวข้องกับธุรกิจ บทบาท หน้าที่ หรือภาระงานของบุคคลนั้นในทางธุรกิจหรือหน้าที่ โดยศาลได้วินิจฉัยหลัก Conspicuous publication rule ว่า องค์กรไม่ได้อนุญาตให้ตั้งที่อยู่อีเมลจากเว็บไซต์ของบุคคลที่สามหรือจากเว็บไซต์ที่มีการประกาศห้ามส่งอีเมลที่ไม่ได้ร้องขอ ดังนั้น องค์กรมีภาระการพิสูจน์ให้ครบทั้ง ๓ เงื่อนไข รวมถึงต้องพิสูจน์ว่าผู้รับ CEMs นั้นได้เผยแพร่ที่อยู่อีเมลของตนอย่างชัดเจนหรือทำให้มีการเผยแพร่ และต้องระบุอย่างชัดเจนว่า ผู้รับ CEMs มีธุรกิจ บทบาท หน้าที่ หรือภาระงานอย่างไร และต้องอธิบายว่าเพราะเหตุใด CEMs มีความเกี่ยวข้องต่อผู้รับนั้น ๆ ทั้งนี้ ตำแหน่งงานของผู้รับ CEMs เพียงอย่างเดียวนั้นไม่เพียงพอที่จะยืนยันถึงบทบาทหน้าที่หรือความเกี่ยวข้องของ CEMs ได้

กฎหมายกำหนดว่า CEMs แต่ละฉบับนั้นต้องมีกลไกการยกเลิกการรับข้อมูล (unsubscribe mechanism) ที่ทำให้ผู้รับ CEMs สามารถแสดงความประสงค์ที่จะไม่รับ CEMs อีกต่อไป โดยต้องไม่มีค่าใช้จ่ายใด ๆ กฎระเบียบ Electronic Commerce Protection Regulations กำหนดว่า กลไกดังกล่าวต้องสามารถดำเนินการได้อย่างง่ายและต้องสามารถเข้าถึงได้โดยไม่ยากหรือไม่ล่าช้า และต้องง่าย รวดเร็ว และสะดวกสำหรับผู้บริโภคในการใช้งาน ซึ่งศาลพิจารณาว่า การกำหนดกลไกการยกเลิกการรับ ๒ แบบใน CEMs เดียวกันนั้น โดยแบบหนึ่งสามารถใช้งานได้จริง แต่อีกแบบที่ใช้งานไม่ได้

ก่อให้เกิดความสับสนและไม่เป็นไปตามบทบัญญัติ ในกฎหมาย CASL ที่กำหนดให้กลไกดังกล่าวต้องชัดเจน เด่นชัด และสามารถดำเนินการได้อย่างง่าย^{๑๓}

๕. บทสรุป

ท่ามกลางสภาพการพัฒนาเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็วและต่อเนื่องนำมาซึ่งภัยคุกคามทางเทคโนโลยีในรูปแบบต่าง ๆ โดยเฉพาะอย่างยิ่งในกรณีของ cyber scam ที่มีลักษณะเป็นการใช้เทคโนโลยีในการหลอกลวงผู้ใช้งานเพื่อให้ได้ไปซึ่งประโยชน์ทางทรัพย์สิน แคนาดาต้องเผชิญกับการก่ออาชญากรรมทางออนไลน์ในรูปแบบที่หลากหลาย ด้วยเหตุนี้ ภาครัฐจึงได้กำหนดมาตรการทางกฎหมายต่าง ๆ ได้แก่ บทบัญญัติความผิดในลักษณะต่าง ๆ ภายในประมวลกฎหมายอาญาของแคนาดา กฎหมาย Canada's anti-spam legislation (CASL) และกฎหมาย BILL C-8 An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts เพื่อแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ไม่ว่าจะเป็น Cyber Scam และอาชญากรรมทางไซเบอร์ในรูปแบบอื่น ๆ เพื่อจัดการกับปัญหาที่มีฉ้อฉลได้อาศัยประโยชน์จากเทคโนโลยีเพื่อหลอกลวงผู้ใช้งานอันส่งผลกระทบต่อผลประโยชน์ด้านลบและความเสียหายที่เกิดจากมิจฉาชีพทั้งต่อประชากรและภาคธุรกิจ ตลอดจนความมั่นคงของรัฐ การบังคับใช้กฎหมายเหล่านี้ทำให้แคนาดาสามารถแก้ไขปัญหาดังกล่าวได้ อันเป็นการสร้างความปลอดภัยให้แก่ประชากรและภาคธุรกิจในการรับมือกับมิจฉาชีพทั้งจากในประเทศและต่างประเทศ เพื่อยกระดับคุณภาพชีวิตของชาวแคนาดาตลอดจนการรักษาเสถียรภาพของความมั่นคงของรัฐ

^{๑๓} Government of Canada, “Federal Court of Appeal Rules CASL Constitutionally Valid and Provides Interpretive Guidance”, สืบค้นเมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๙, จาก Federal Court of Appeal Rules CASL Constitutionally Valid and Provides Interpretive Guidance | BLG.

เยอรมนี*

๑. บทนำ

ความก้าวหน้าทางเทคโนโลยีสารสนเทศมีบทบาทสำคัญในการยกระดับคุณภาพชีวิตของบุคคลในสังคม โดยช่วยอำนวยความสะดวกในการติดต่อสื่อสาร การทำธุรกรรม และการประกอบกิจกรรมทางเศรษฐกิจให้เป็นไปอย่างรวดเร็วและมีประสิทธิภาพยิ่งขึ้น อย่างไรก็ตาม เทคโนโลยีอาจถูกนำไปใช้เพื่อเป็นช่องทางในการแสวงหาประโยชน์โดยมิชอบ โดยเฉพาะการหลอกลวงทางไซเบอร์ ซึ่งผู้กระทำความผิดมักอาศัยข้อบกพร่องทางเทคนิคและความเปราะบางของพฤติกรรมมนุษย์ เช่น ความเชื่อถือนและไว้วางใจ ความเร่งรีบ หรือการขาดความระมัดระวังในการใช้งานระบบดิจิทัลเพื่อหลอกลวงผู้เสียหาย ซึ่งการกระทำ ความผิดดังกล่าวมีรูปแบบการกระทำและพฤติการณ์แวดล้อมที่แตกต่างจากความผิดทั่วไป กล่าวคือ ผู้กระทำความผิดสามารถปกปิดตัวตนที่แท้จริงได้โดยไม่จำเป็นต้องเผชิญหน้ากับผู้เสียหาย และกระทำการจากระยะไกลแต่ก่อความเสียหายในวงกว้างได้ภายในระยะเวลาอันสั้น อีกทั้งในบางกรณียังมียอดประกอบข้ามพรมแดน ส่งผลให้การสืบสวนสอบสวนและการติดตามตัวผู้กระทำความผิดมาดำเนินคดีเป็นไปได้ยาก

ความรุนแรงของปัญหาการใช้เทคโนโลยีเป็นเครื่องมือในการกระทำความผิดในประเทศเยอรมนีปรากฏให้เห็นอย่างชัดเจนจากข้อมูลสถิติการดำเนินคดีของสำนักงานสอบสวนอาชญากรรมแห่งสหพันธ์ (Bundeskriminalamt: BKA)^๑ ซึ่งระบุว่า ในปี ๒๕๖๘ มีคดีอาชญากรรมไซเบอร์ที่เกี่ยวข้องกับเยอรมนี ๓๓๓,๙๒๒ คดี แบ่งเป็นคดีที่เกิดในประเทศ ๑๒๖,๐๓๔ คดี คิดเป็นร้อยละ ๒.๓ ของคดีอาญาที่เกิดขึ้นในประเทศทั้งหมด และคดีจากต่างประเทศ ๒๐๗,๘๘๘ คดี คิดเป็นร้อยละ ๓๑.๔ ของคดีอาญาจากต่างประเทศทั้งหมด นอกจากนี้ ยังมีการตรวจพบรูปแบบภัยคุกคามทางไซเบอร์ที่สำคัญอีกหลายประการ เช่น การโจมตีด้วยแรนซัมแวร์^๒ ๑,๐๔๑ กรณี การโจมตีแบบ DDoS^๓ ๓๖,๗๐๖ กรณี และการตรวจพบอีเมลฟิชซิง^๔ ๓๘๒,๔๗๐ รายการ สถิติเหล่านี้สะท้อนให้เห็นว่า การหลอกลวงทางไซเบอร์มิใช่เพียงปัญหาทางเทคนิค หากแต่เป็นภัยคุกคามทางเศรษฐกิจและความปลอดภัยของประชาชน อีกทั้งยังสร้างข้อจำกัดต่อการบังคับใช้กฎหมายในการป้องกันและปราบปราม เนื่องจากพฤติการณ์บางส่วนอาจเกิดขึ้นนอกเขตอำนาจรัฐ แต่ผลเสียหายกลับเกิดขึ้นภายในประเทศ

* จัดทำโดยนายณัฐพล สกุลเมฆา นักกฎหมายกฤษฎีกาชำนาญการพิเศษ ฝ่ายค้นคว้าและเปรียบเทียบกฎหมาย กองกฎหมายต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

^๑ Bundeskriminalamt (BKA), “Bundeslagebild Cybercrime 2025”, สืบค้นเมื่อวันที่ ๕ มิถุนายน ๒๕๖๙, จาก https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2025.pdf?__blob=publicationFile&v=3

^๒ แรนซัมแวร์ (Ransomware) หมายถึง โปรแกรมหรือชุดคำสั่งคอมพิวเตอร์ ซึ่งผู้กระทำความผิดใช้เพื่อขัดขวาง จำกัด หรือระงับการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลของผู้เสียหาย โดยมักใช้วิธีเข้ารหัสข้อมูลหรือปิดกั้นระบบแล้วเรียกร้องให้ผู้เสียหายชำระเงินหรือทรัพย์สินดิจิทัลเป็นค่าไถ่เพื่อแลกกับการคืนสิทธิในการเข้าถึงระบบหรือข้อมูลดังกล่าว

^๓ การโจมตีแบบ DDoS (Distributed Denial of Service) หมายถึง การโจมตีระบบคอมพิวเตอร์ เครือข่ายเว็บไซต์ หรือบริการออนไลน์ โดยอาศัยคอมพิวเตอร์หรืออุปกรณ์จำนวนมากส่งคำร้องขอหรือปริมาณข้อมูลเข้าสู่ระบบเป้าหมายพร้อมกันเป็นปริมาณสูงผิดปกติจนเป็นเหตุให้ระบบเป้าหมายไม่สามารถให้บริการแก่ผู้ใช้งานทั่วไปได้ตามปกติ

^๔ อีเมลฟิชซิง (Phishing Email) หมายถึง อีเมลที่มีลักษณะหลอกลวงหรือแอบอ้างว่าเป็นบุคคลหน่วยงาน หรือผู้ให้บริการที่น่าเชื่อถือ เพื่อชักจูงให้ผู้รับเปิดเผยข้อมูลสำคัญ เช่น รหัสผ่าน ข้อมูลบัญชีธนาคารหรือข้อมูลบัตรเครดิตหรือให้กดลิงก์หรือเปิดไฟล์แนบอันอาจนำไปสู่การติดตั้งมัลแวร์หรือการเข้าถึงระบบโดยมิชอบ

ในการดำเนินคดีเพื่อนำผู้กระทำความผิดมาลงโทษทางอาญา ประเทศเยอรมนีจึงต้องเผชิญกับความท้าทายหลายประการ ไม่ว่าจะเป็นการปรับใช้บทบัญญัติในกฎหมายอาญาที่มีอยู่เดิมให้ครอบคลุมรูปแบบการหลอกลวงทางอินเทอร์เน็ตสมัยใหม่ การสืบสวนสอบสวนที่ต้องดำเนินการด้วยความรวดเร็วเพื่อให้ทันต่อพยานหลักฐานดิจิทัลซึ่งอาจถูกลบ แก้ไขหรือไม่สามารถตรวจสอบย้อนหลังได้ เมื่อพ้นระยะเวลาการเก็บข้อมูลของผู้ให้บริการ ตลอดจนการติดตามเครือข่ายผู้กระทำความผิดที่อาจกระจายตัวอยู่นอกอาณาเขตของรัฐมาดำเนินคดีในประเทศ และโดยที่การหลอกลวงทางไซเบอร์จำนวนมากมิได้เกิดจากผู้กระทำความผิดรายเดียว แต่มีลักษณะเป็นขบวนการมืออาชีพที่แบ่งหน้าที่กันทำงานอย่างเป็นระบบ เช่น กรณีการหลอกลวงทุนออนไลน์หรือร้านค้าออนไลน์ปลอม อาจมีบุคคลฝ่ายหนึ่งรับผิดชอบจัดทำเว็บไซต์หรือแพลตฟอร์มปลอมให้ดูน่าเชื่อถือเพื่อให้อีกฝ่ายหนึ่งใช้ในการทำโฆษณาหรือส่งข้อความติดต่อผู้เสียหาย และผู้กระทำความผิดอีกกลุ่มจะคอยทำหน้าที่พูดคุยโน้มน้าวหรือแอบอ้างเป็นพนักงานบริษัทเพื่อสร้างความไว้วางใจจนกระทั่งผู้เสียหายยินยอมชำระเงินผ่านบัญชีที่รับโอนเงินซึ่งมีคนกลางจัดหาไว้แล้ว โดยจะมีการโอนเงินผ่านผู้พอกเงินหลายทอดเพื่อปกปิดแหล่งที่มาของทรัพย์สินที่ได้จากการกระทำความผิด ในหลายกรณีเจ้าหน้าที่จึงติดตามดำเนินคดีได้เพียงบุคคลชั้นปลาย เช่น ผู้รับโอนเงินหรือผู้พอกเงิน ขณะที่ผู้บงการอยู่เบื้องหลังติดตามตัวมาลงโทษได้ยาก การรับมือกับความผิดประเภทนี้จึงไม่อาจจำกัดอยู่เพียงการกำหนดฐานความผิดให้ครอบคลุมพฤติกรรมทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็วเท่านั้น แต่จำเป็นต้องอาศัยมาตรการสืบสวนสอบสวนที่ทันต่อพยานหลักฐานดิจิทัลความร่วมมือระหว่างประเทศ และกลไกทางกฎหมายที่สามารถติดตาม ตัดวงจร และริบคืนผลประโยชน์ที่ได้จากการกระทำความผิดเพื่อนำมาชดเชยให้กับผู้เสียหายได้อย่างมีประสิทธิภาพ

บทความนี้จึงมุ่งนำเสนอแนวทางการรับมือกับการหลอกลวงทางไซเบอร์ในระบบกฎหมายเยอรมัน โดยพิจารณาความหมายและลักษณะของการหลอกลวงทางไซเบอร์ ฐานความผิดทางอาญาที่เกี่ยวข้อง มาตรการสืบสวนสอบสวน และข้อจำกัดในการบังคับใช้กฎหมายต่อความผิดที่มีลักษณะข้ามพรมแดน ซึ่งการศึกษาประสบการณ์ของประเทศเยอรมนีจะช่วยให้เข้าใจลักษณะของอาชญากรรมทางอินเทอร์เน็ตสมัยใหม่ ตลอดจนแนวทางการออกแบบกฎหมายและนโยบายเพื่อป้องกันและปราบปรามการหลอกลวงทางไซเบอร์ อันจะเป็นประโยชน์ต่อการพิจารณากำหนดนโยบายทางกฎหมายของประเทศไทยให้เหมาะสมกับระดับความร้ายแรงของภัยคุกคามจากการอาศัยความก้าวหน้าทางเทคโนโลยีเป็นเครื่องมือในการกระทำความผิดที่เกิดขึ้น

๒. ความหมายและลักษณะของการหลอกลวงทางไซเบอร์ (Cyber Scam) ในระบบกฎหมายเยอรมัน

ในระบบกฎหมายเยอรมัน อาชญากรรมไซเบอร์อาจจำแนกได้เป็น ๒ ประเภท ได้แก่ อาชญากรรมไซเบอร์ในความหมายอย่างแคบ (Cybercrime im engeren Sinne)^๕ และอาชญากรรม

^๕ อาชญากรรมไซเบอร์ในความหมายอย่างแคบ (Cybercrime im engeren Sinne) หมายถึง บรรดาความผิดที่มุ่งกระทำต่อข้อมูล ระบบคอมพิวเตอร์ หรือเครือข่ายโดยตรง โดยคุณธรรมทางกฎหมาย (Rechtsgüter) ที่รัฐประสงค์จะให้ความคุ้มครอง ได้แก่ ความลับ (Vertraulichkeit) ความถูกต้องสมบูรณ์ (Integrität) และความพร้อมใช้งาน (Verfügbarkeit) ของข้อมูล ระบบคอมพิวเตอร์ และเครือข่าย ตัวอย่างฐานความผิดในประมวลกฎหมายอาญาเยอรมัน ได้แก่ ความผิดฐานล้วงข้อมูลตามมาตรา ๒๐๒a StGB ความผิดฐานดักจับข้อมูลตามมาตรา ๒๐๒b StGB ความผิดฐานเตรียมการล้วงหรือดักจับข้อมูลตามมาตรา ๒๐๒c StGB ความผิดฐานรับหรือจำหน่ายข้อมูลที่ได้มาโดยมิชอบตามมาตรา ๒๐๒d StGB ความผิดฐานเปลี่ยนแปลงข้อมูล ตามมาตรา ๓๐๓a StGB และความผิดฐานก่อวินาศกรรมคอมพิวเตอร์ตามมาตรา ๓๐๓b StGB

ไซเบอร์ในความหมายอย่างกว้าง (Cybercrime im weiteren Sinne)^๖ โดยอาชญากรรมไซเบอร์ในความหมายอย่างแคบมุ่งคุ้มครองความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งานของข้อมูลระบบคอมพิวเตอร์ และเครือข่าย ในฐานะวัตถุแห่งการกระทำความผิดโดยตรง ในขณะที่อาชญากรรมไซเบอร์ในความหมายอย่างกว้างครอบคลุมกรณีที่ผู้กระทำความผิดใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือหรือช่องทางในการกระทำความผิดตามกฎหมายอาญาทั่วไป เมื่อพิจารณาตามหลักการจำแนกดังกล่าว การหลอกลวงทางไซเบอร์หรือ Cyber Scam จึงอยู่ในขอบเขตของอาชญากรรมไซเบอร์ในความหมายอย่างกว้าง เนื่องจากผู้กระทำความผิดมิได้มุ่งโจมตีระบบเทคโนโลยีสารสนเทศโดยตรง แต่เป็นกรณีที่ผู้กระทำความผิดใช้เทคโนโลยีเป็นเครื่องมือในการหลอกลวงให้ผู้เสียหายกระทำการอย่างหนึ่งอย่างใด เช่น การโอนเงิน การเปิดเผยข้อมูลส่วนบุคคล ข้อมูลบัญชี รหัสผ่าน ข้อมูลการชำระเงิน หรือข้อมูลที่ใช้ในการทำธุรกรรม เพื่อให้ผู้กระทำความผิดได้ไปซึ่งทรัพย์สินหรือประโยชน์ทางเศรษฐกิจโดยมิชอบ^๗ ด้วยเหตุนี้ คำว่า “Cyber Scam” จึงมิใช่ชื่อฐานความผิดเฉพาะในประมวลกฎหมายอาญาเยอรมัน (Strafgesetzbuch: StGB) แต่เป็นถ้อยคำที่ใช้เรียกพฤติการณ์การกระทำความผิด

เนื่องจากประมวลกฎหมายอาญาเยอรมันมิได้บัญญัติฐานความผิดเฉพาะสำหรับกรณีการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการหลอกลวงผู้เสียหายไว้ การดำเนินคดีเกี่ยวกับการหลอกลวงทางไซเบอร์จึงต้องอาศัยการปรับใช้บทบัญญัติในประมวลกฎหมายอาญาที่มีอยู่กับข้อเท็จจริงในแต่ละกรณีเป็นสำคัญ กล่าวคือ หากผู้กระทำความผิดใช้กลอุบายหลอกลวงให้ผู้เสียหายกระทำการเกี่ยวกับทรัพย์สิน เช่น โอนเงินหรือส่งมอบทรัพย์สิน การกระทำความผิดดังกล่าวอาจเข้าองค์ประกอบความผิดฐานฉ้อโกงตามมาตรา ๒๖๓ StGB แต่หากเป็นกรณีที่ผู้กระทำความผิดใช้ข้อมูลหรือระบบคอมพิวเตอร์โดยมิชอบเพื่อก่อให้เกิดผลเสียหายในทางทรัพย์สิน ย่อมต้องพิจารณาในกรอบความผิดฐานฉ้อโกงโดยใช้คอมพิวเตอร์ตามมาตรา ๒๖๓a StGB^๘ การจำแนกระหว่างอาชญากรรมไซเบอร์ในความหมายอย่างแคบและอย่าง

^๖ อาชญากรรมไซเบอร์ในความหมายอย่างกว้าง (Cybercrime im weiteren Sinne) หมายถึง กรณีที่ผู้กระทำความผิดใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือหรือช่องทางในการกระทำความผิดตามกฎหมายอาญาทั่วไป เช่น ความผิดฐานฉ้อโกงตามมาตรา ๒๖๓ StGB ความผิดฐานฉ้อโกงโดยใช้คอมพิวเตอร์ตามมาตรา ๒๖๓a StGB ความผิดฐานปลอมแปลงข้อมูลที่มีความสำคัญในทางพยานหลักฐานตามมาตรา ๒๖๔ StGB และความผิดฐานฟอกเงิน (Geldwäsche) ตามมาตรา ๒๖๑ StGB ในกรณีที่มีการรับ โอน หรือปกปิดทรัพย์สินที่ได้จากการหลอกลวงทางไซเบอร์

^๗ Bundeskriminalamt (BKA), Bundeslagebild Cybercrime 2011, สืบค้นเมื่อวันที่ ๕ มิถุนายน ๒๕๖๔ จาก https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2011.pdf?__blob=publicationFile&v=6

^๘ มาตรา ๒๖๓ StGB เป็นบทบัญญัติที่กำหนดความผิดฐานฉ้อโกง โดยใช้กับกรณีที่ผู้กระทำความผิดมีเจตนาให้ตนเองหรือบุคคลที่สามได้ประโยชน์ทางทรัพย์สินโดยมิชอบ ด้วยการหลอกลวงให้บุคคลอื่นสำคัญผิดในข้อเท็จจริงซึ่งอาจกระทำโดยการแสดงข้อความอันเป็นเท็จหรือปกปิดข้อความจริงที่มีหน้าที่ต้องแจ้งอันเป็นเหตุให้ผู้เสียหายกระทำการเกี่ยวกับทรัพย์สินและเกิดความเสียหาย (Vermögensverfügung) ส่วนมาตรา ๒๖๓a StGB เป็นความผิดฐานฉ้อโกงโดยใช้คอมพิวเตอร์ ที่บัญญัติขึ้นเพื่ออุดช่องว่างของความผิดฐานฉ้อโกงในกรณีที่ขาดองค์ประกอบ การหลอกลวงมนุษย์โดยตรง แต่ผู้กระทำความผิดใช้ข้อมูลที่ไม่ถูกต้อง ไม่ครบถ้วน หรือใช้ข้อมูลโดยไม่ได้รับอนุญาต เพื่อให้เกิดผลเสียหายในทางทรัพย์สิน ดังนั้น มาตรา ๒๖๓ StGB จึงมุ่งคุ้มครองทรัพย์สินของบุคคลจากการถูกหลอกลวงให้ตัดสินใจดำเนินการเกี่ยวกับทรัพย์สินในทางที่ก่อให้เกิดความเสียหาย ขณะที่มาตรา ๒๖๓a StGB รองรับการกระทำความผิด

กว้างจึงมีนัยสำคัญ เพราะข้อเท็จจริงเดียวกันอาจประกอบด้วยการหลอกลวงผู้เสียหาย การได้มาซึ่งข้อมูลโดยมิชอบ และการใช้ข้อมูลหรือระบบคอมพิวเตอร์เพื่อก่อให้เกิดความเสียหายทางทรัพย์สิน เช่น การฟิชซิง (Phishing) ที่เริ่มจากการหลอกให้ผู้เสียหายเปิดเผยรหัสผ่าน แล้วนำข้อมูลดังกล่าวไปใช้ทำธุรกรรมโดยมิชอบ หรือการแอบอ้างเป็นฝ่ายสนับสนุนทางเทคนิคเพื่อหลอกให้ผู้เสียหายติดตั้งโปรแกรมควบคุมระยะไกล แล้วใช้การเข้าถึงดังกล่าวขโมยข้อมูลหรือส่งโอนเงิน แม้พฤติการณ์ในแต่ละขั้นตอนล้วนแล้วแต่เป็นการกระทำที่มุ่งผลสำเร็จเพื่อให้ได้รับประโยชน์ในทางทรัพย์สินจากผู้เสียหายรายเดียวกัน แต่การวินิจฉัยความรับผิดในทางอาญาจำเป็นต้องพิจารณาด้วยการกระทำในแต่ละช่วงนั้นเข้าองค์ประกอบความผิดฐานใด และมีความสัมพันธ์กันในลักษณะกรรมเดียวผิดกฎหมายหลายบท (Tateinheit) หรือการกระทำหลายกรรมต่างวาระ (Tatmehrheit)^๙

กลวิธีที่ผู้กระทำความผิดใช้ในการหลอกลวงผู้เสียหายทางไซเบอร์ในเยอรมนีมีความหลากหลาย ตั้งแต่วิธีการพื้นฐานไปจนถึงการกระทำที่มีการวางแผนอย่างเป็นระบบและใช้เทคนิคเฉพาะทาง โดยมีปรับเปลี่ยนไปตามช่องทางดิจิทัลและพฤติกรรมของผู้ใช้งาน เช่น การหลอกลวงโดยแอบอ้างเป็นฝ่ายสนับสนุนทางเทคนิค (Technical Support Scam) ซึ่งผู้กระทำความผิดแอบอ้างเป็นเจ้าหน้าที่ของบริษัทเทคโนโลยี อ้างว่าคอมพิวเตอร์ของผู้เสียหายมีปัญหาด้านความปลอดภัยและชักจูงให้ผู้เสียหายอนุญาตให้เข้าถึงเครื่องคอมพิวเตอร์จากระยะไกลหรือดำเนินการชำระเงินตามคำสั่ง^{๑๐} การหลอกลวงด้วย

ฉ้อโกงที่เกิดขึ้นผ่านระบบคอมพิวเตอร์หรือกระบวนการประมวลผลข้อมูลโดยไม่จำเป็นต้องมีบุคคลใดถูกหลอกให้สำคัญผิดโดยตรง

^๙ ในกรณีที่พฤติการณ์เดียวกันเกี่ยวข้องกับความผิดหลายฐาน ต้องพิจารณาตามหลักว่าด้วยความสัมพันธ์ระหว่างความผิดหลายฐาน (Konkurrenzverhältnis) กล่าวคือ หากการหลอกลวง การได้มาซึ่งข้อมูล และการใช้ข้อมูลหรือระบบคอมพิวเตอร์เกิดขึ้นต่อเนื่องใกล้ชิดกันภายใต้กระบวนการและเจตนาเดียวกัน รวมทั้งมีความเป็นเอกภาพของพฤติการณ์โดยรวม เช่น ผู้กระทำความผิดแอบอ้างเป็นฝ่ายสนับสนุนทางเทคนิค หลอกให้ผู้เสียหายเปิดโปรแกรมควบคุมระยะไกล และในคราวเดียวกันใช้การเข้าถึงดังกล่าวส่งโอนเงินหรือชักจูงให้ผู้เสียหายยืนยันธุรกรรม จนอาจพิจารณาได้ว่าตามวิสัยและพฤติการณ์ทั่วไปแล้วถือเป็นการกระทำเดียวกันในทางธรรมชาติ (natürliche Handlungseinheit) ก็จะเข้าลักษณะกรรมเดียวผิดกฎหมายหลายบท (Tateinheit หรือ Idealkonkurrenz) ตามมาตรา ๕๒ StGB อย่างไรก็ตามก็ดี หากการได้มาซึ่งข้อมูลและการนำข้อมูลไปใช้เกิดขึ้นต่างช่วงเวลา ต่างขั้นตอนหรืออาศัยการตัดสินใจใหม่ของผู้กระทำความผิด เช่น หลอกให้ผู้เสียหายเปิดเผยรหัสผ่านในครั้งหนึ่ง ภายหลังจึงนำรหัสผ่านดังกล่าวไปเข้าสู่ระบบและโอนเงินอีกครั้ง ย่อมมีแนวโน้มเป็นการกระทำหลายกรรมต่างวาระ (Tatmehrheit หรือ Realkonkurrenz) ตามมาตรา ๕๓ StGB ทั้งนี้ การวินิจฉัยต้องพิจารณาจากความต่อเนื่องของเวลา สถานที่ วิธีการกระทำ เจตนา และความสัมพันธ์ของการกระทำในแต่ละขั้นตอนเป็นรายกรณี

^{๑๐} ตัวอย่างคดี Technical Support Scam ศาลแขวงมิวนิกมีคำพิพากษาในคดีที่ผู้เสียหายซึ่งเป็นผู้รับบำนาญถูกบุคคลไม่ทราบชื่อโทรศัพท์มาแอบอ้างว่าเป็นเจ้าหน้าที่ของบริษัทผู้ให้บริการ Microsoft และอ้างว่าคอมพิวเตอร์ของผู้เสียหายติดไวรัสหรือมีปัญหาด้านความปลอดภัย พร้อมเสนอให้ช่วยแก้ไขผ่านการเข้าถึงคอมพิวเตอร์จากระยะไกล ผู้เสียหายจึงอนุญาตให้บุคคลดังกล่าวควบคุมคอมพิวเตอร์ของตน และเข้าใจว่าตนตกลงซื้อบริการป้องกันภัยทางอินเทอร์เน็ตในราคา ๒๕ ยูโร อย่างไรก็ตาม ในระหว่างการทำธุรกรรมออนไลน์ ผู้กระทำความผิดได้กรอกข้อมูลบัญชีของบุคคลที่สามลงในแบบฟอร์มออนไลน์แบบกึ่งอัตโนมัติ และให้ผู้เสียหายยืนยันรายการด้วยรหัส TAN ต่อมา ผู้เสียหายพบว่าเงินจำนวน ๔,๐๐๐ ยูโร ถูกโอนไปยังบัญชีของบุคคลดังกล่าวแทนที่จะเป็นเงิน ๒๕ ยูโร ตามที่เข้าใจ ผู้เสียหายปฏิเสธการคืนเงินโดยอ้างว่าตนเองก็ตกเป็นเหยื่อของกลโกง Microsoft Support Scam เช่นกัน โดยได้ให้ข้อมูลบัญชีแก่

การสร้างความสัมพันธ์ส่วนตัวหรืออาศัยความไว้วางใจเพื่อให้ผู้เสียหายโอนเงิน (Romance Scam หรือ Love Scam)^{๑๑} การหลอกลวงผ่านเว็บไซต์หรือแพลตฟอร์มดิจิทัลโดยเสนอผลตอบแทนเกินจริง (Boiler Room Scam หรือ Cybertrading)^{๑๒} ตลอดจนการหลอกละการทำงานออนไลน์โดยอ้างว่าจะได้รับค่าตอบแทน

ผู้กระทำความผิดเพราะเชื่อว่าจะได้รับเงินชดเชยความเสียหายจากการที่ตนเคยถูกหลอกละให้ชำระเงินและล่วงข้อมูล ศาลวินิจฉัยว่า ผู้เสียหายมีสิทธิเรียกเงินคืนจากผู้รับเงินตามหลักกฎหมายได้ เนื่องจากไม่มีนิติสัมพันธ์หรือมูลทางกฎหมายระหว่างผู้เสียหายกับผู้รับเงินที่ทำให้ผู้รับเงินมีสิทธิเก็บเงินจำนวนดังกล่าวไว้ได้ แม้ผู้รับเงินจะอ้างว่าตนได้รับเงินตามข้อตกลงกับกลุ่มผู้กระทำความผิดก็ตาม ข้อตกลงดังกล่าวมิใช่มูลทางกฎหมายที่ใช้อย่างต่อเนื่องกับผู้เสียหายได้ (AG München, Urteil vom 16.01.2019, Az. 122 C 19127/18)

^{๑๑} ตัวอย่างคดี Love Scam ศาลสูงสุดแห่งรัฐบาวเรียพิจารณาคดีที่จำเลยยินยอมให้ใช้บัญชีธนาคารของตนเป็นบัญชีรับโอนเงินจากผู้เสียหายหลายราย โดยเงินดังกล่าวมีที่มาจากกลโกงแบบ Love Scam ซึ่งผู้กระทำความผิดแอบอ้างตัวตน ประวัติชีวิต ความสัมพันธ์แห่งความไว้วางใจ และความจำเป็นเร่งด่วนในการใช้เงิน อันเป็นเท็จ เพื่อจูงใจให้ผู้เสียหายโอนเงินให้ โดยมักให้โอนผ่านบัญชีของบุคคลที่สาม ภายหลังได้รับเงินแล้วผู้กระทำความผิดจะตัดการติดต่อและหลบหนีไปโดยไม่สามารถติดตามตัวได้ ประเด็นสำคัญของคดีอยู่ที่ว่าแม้ผู้เสียหายจะเป็นฝ่ายโอนเงินโดยสมัครใจ และตระหนักว่าการโอนเงินย่อมทำให้ทรัพย์สินของตนลดลง แต่ศาลเห็นว่าข้อเท็จจริงดังกล่าวไม่ทำให้ความผิดฐานฉ้อโกงหมดไป เนื่องจากการโอนเงินดังกล่าวเกิดจากการหลอกลวงเกี่ยวกับตัวตน ความสัมพันธ์ ความจำเป็นในการใช้เงิน และวัตถุประสงค์ของการให้ทรัพย์สิน ศาลจึงวินิจฉัยว่าพฤติการณ์ Love Scam เข้าองค์ประกอบความผิดฐานฉ้อโกงตามมาตรา ๒๖๓ StGB นอกจากนี้ ศาลยังเห็นว่าเงินฝากในบัญชีธนาคารอาจเป็นวัตถุแห่งความผิดฐานพอกเงินได้ และเมื่อจำเลยยินยอมให้ใช้บัญชีของตนเป็นทางผ่านของเงินจากบุคคลที่ตนไม่รู้จัก ทั้งที่พฤติการณ์โดยรวมชี้ให้เห็นอย่างชัดเจนถึงความเป็นไปได้ว่าเงินดังกล่าวมีที่มาจากการฉ้อโกง การกระทำของจำเลยจึงเป็นการพอกเงินโดยประมาทเลินเล่ออย่างร้ายแรงตามมาตรา ๒๖๑ StGB (BayObLG, Beschluss vom 04.04.2024, Az. 203 StRR 104/24)

^{๑๒} ตัวอย่างคดี Cybertrading ศาลมลรัฐบัมแบร์ก (Landgericht Bamberg) มีคำพิพากษาในคดีหลอกลวงลงทุนออนไลน์ขนาดใหญ่คดีหนึ่งของเยอรมนี โดยจำเลยหลักถูกพิพากษาว่ามีความผิดฐานฉ้อโกงเป็นอาชีพและเป็นขบวนการ (gewerbs- und bandenmäßiger Betrug) จากการดำเนินเครือข่ายหลอกลวงลงทุนผ่านแพลตฟอร์มซื้อขายปลอม เช่น Trade Capital, Nobel Trade, Forbslab, Huludox และ Fibonetix ผู้กระทำความผิดใช้โฆษณาปลอมและแอบอ้างบุคคลมีชื่อเสียง เช่น Thomas Gottschalk (พิธีกรชื่อดัง) เพื่อสร้างความน่าเชื่อถือและชักจูงให้นักลงทุนโอนเงิน โดยทำให้แพลตฟอร์มดังกล่าวดูเหมือนเป็นการลงทุนที่ถูกต้องและน่าเชื่อถือ ทั้งที่แท้จริงมีการดำเนินงานผ่านคอลเซ็นเตอร์ในต่างประเทศ เช่น บัลแกเรียและเซอร์เบีย และมีได้มีการลงทุนจริงตามที่กล่าวอ้าง สำนักงานอัยการสูงสุดเมืองบัมแบร์กประเมินว่า เฉพาะความเสียหายของนักลงทุนชาวเยอรมันในคดีนี้มีมูลค่าประมาณ ๑๐ ล้านยูโร ศาลลงโทษจำคุกผู้บงการ ๔ ปี ๖ เดือน และลงโทษหัวหน้าคอลเซ็นเตอร์จำคุก ๒ ปี โดยให้รอการลงโทษ ภายหลังจากมีส่วนร่วมในกระบวนการเยียวยาความเสียหายระหว่างผู้กระทำความผิดกับผู้เสียหาย (Täter-Opfer-Ausgleich) นอกจากนี้ ศาลยังมีคำสั่งริบทรัพย์สินที่ถูกยึดไว้ก่อนหน้านี้เป็นมูลค่าหลายล้านยูโร รวมถึงรถยนต์หรูยี่ห้อ Lamborghini และ Rolls-Royce โดยรายได้จากการจำหน่ายทรัพย์สินดังกล่าวจะนำไปชดเชยความเสียหายแก่ผู้เสียหายต่อไป คดีนี้จึงเป็นตัวอย่างสำคัญของการหลอกลวงไซเบอร์ในรูปแบบ Cybertrading หรือการหลอกลวงลงทุนออนไลน์ ซึ่งอยู่ในกลุ่มอาชญากรรมไซเบอร์ในความหมายอย่างกว้าง เนื่องจากผู้กระทำความผิดมิได้โจมตีระบบคอมพิวเตอร์โดยตรง แต่ใช้เว็บไซต์ แพลตฟอร์มดิจิทัล โฆษณาออนไลน์ และคอลเซ็นเตอร์เป็นเครื่องมือในการหลอกลวงให้ผู้เสียหายตัดสินใจโอนเงินลงทุน (LG Bamberg, Urteil vom 05.08.2025, Cybertrading-Prozess)

ก่อนชักจูงให้ผู้เสียหายโอนเงินเข้าระบบหรือบัญชีเสมือนเพื่อถอนเงิน^{๑๓} นอกจากนี้ ยังปรากฏการหลอกลวงในรูปแบบอื่นเช่น การหลอกให้ชำระเงินล่วงหน้า (Vorschussbetrug) การแอบอ้างเป็นญาติที่ประสบเหตุฉุกเฉิน (Enkeltrick) การแอบอ้างเป็นผู้บริหารบริษัทเพื่อสั่งให้โอนเงิน (CEO Fraud) และการประกาศรับสมัครงานปลอมเพื่อให้ได้ข้อมูลส่วนบุคคลหรือข้อมูลสำคัญของผู้สมัคร (Job Scam)^{๑๔} ทั้งนี้ ลักษณะร่วมของการกระทำเหล่านี้ คือ การใช้เทคโนโลยีเป็นเครื่องมือสร้างความน่าเชื่อถือ หลอกให้ผู้เสียหายตัดสินใจผิดพลาดหรือเปิดเผยข้อมูลสำคัญอันนำไปสู่ความเสียหายทางทรัพย์สินหรือการละเมิดข้อมูลส่วนบุคคล

จากรูปแบบการหลอกลวงทางไซเบอร์ที่ปรากฏในเยอรมนี จะเห็นได้ว่า ความผิดประเภทนี้มีลักษณะซับซ้อนกว่าการฉ้อโกงโดยใช้ข้อความหลอกลวงทั่วไป เนื่องจากการผสมผสานระหว่างกลอุบายในการหลอกลวง การใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือ และการอาศัยช่องทางดิจิทัลเพื่อปกปิดตัวตนหรือขยายขอบเขตความเสียหาย การวินิจฉัยความรับผิดชอบทางอาญาจึงต้องพิจารณาทั้งพฤติการณ์การหลอกลวง วิธีการได้มาหรือการใช้ข้อมูลโดยมิชอบ และผลเสียหายทางทรัพย์สินที่เกิดขึ้นอย่างใดก็ดี การปรับใช้กฎหมายอาญากับการหลอกลวงทางไซเบอร์ในระบบกฎหมายเยอรมันที่ไม่มีกฎหมายเฉพาะในการป้องปรามการกระทำความผิดในลักษณะดังกล่าวจำเป็นต้องพิจารณาโดยคำนึงถึงหลักไม่มีกฎหมายไม่มีโทษ (Gesetzlichkeit der Strafe) ตามที่บัญญัติไว้ในมาตรา ๑๐๓ วรรคสอง ของรัฐธรรมนูญแห่งสหพันธ์สาธารณรัฐเยอรมนี ซึ่งกำหนดให้บุคคลจะถูกลงโทษได้ต่อเมื่อการกระทำนั้น

^{๑๓} ตัวอย่างรูปแบบการหลอกลวงออนไลน์ดังกล่าวปรากฏตามรายงานข่าวของ NDR กรณีชายจากเมือง Strassburg ในรัฐเมคเคิลบวร์ก-พอร์พอมเมิร์น ซึ่งถูกหลอกผ่านแอปพลิเคชัน TikTok ให้ทำงานเสริมโดยดูภาพยนตร์และส่งภาพหน้าจอเพื่อรับค่าตอบแทน ผู้กระทำความผิดแอบอ้างเป็นบริษัทภาพยนตร์ “Universal” โดยในระยะแรกมีการจ่ายเงินจำนวนเล็กน้อยให้แก่ผู้เสียหายเพื่อสร้างความน่าเชื่อถือ ก่อนชักจูงให้ผู้เสียหายโอนเงินเข้าสู่บัญชีเสมือนในระบบออนไลน์ (virtuelles Konto) โดยอ้างว่าเป็นเงินโบนัสในการถอนเงิน จนผู้เสียหายสูญเสียเงินเกือบ ๑๐,๐๐๐ ยูโร (NDR, Die schwere Jagd nach Online-Betrügern, สืบค้นเมื่อวันที่ ๕ มิถุนายน ๒๕๖๔, จาก <https://www.ndr.de/nachrichten/mecklenburg-vorpommern/die-schwere-jagd-nach-online-betruegern,onlinebetrug-102.html>)

^{๑๔} ตัวอย่างพฤติการณ์ของการหลอกลวงผ่านประกาศรับสมัครงานปลอม (Job Scam) ปรากฏจากรายงานของศูนย์คุ้มครองผู้บริโภคแห่งรัฐเฮสเซน (Verbraucherzentrale Hessen) เรื่อง Job-Scamming: Geldwäschekonto statt Job ซึ่งระบุกรณีของ Anna B. จากเมือง Offenbach ที่ได้รับข้อเสนองานซึ่งอ้างว่าสามารถทำงานจากที่บ้าน มีเวลาทำงานยืดหยุ่น และมีรายได้ดี โดยลักษณะงานคือการทดสอบและประเมินระบบการเปิดบัญชีธนาคารออนไลน์ ผู้เสียหายจึงถูกชักจูงให้ทดลองเปิดบัญชีกระแสรายวันผ่านระบบออนไลน์ของธนาคารที่อ้างว่าเป็นธนาคารพันธมิตร ดำเนินกระบวนการยืนยันตัวตนทางวิดีโอ (Video-Ident-Verfahren) อัปโหลดภาพถ่ายตนเองพร้อมบัตรประจำตัวประชาชน และกรอกข้อมูลติดต่อที่ผู้กระทำความผิดจัดเตรียมไว้ผ่าน WhatsApp ทั้งยังถูกขอไม่ให้แจ้งธนาคารว่าการเปิดบัญชีดังกล่าวเป็นเพียงการทดสอบ เพราะต้องการให้การทดสอบดูสมจริง อย่างไรก็ดี บัญชีที่อ้างว่าเป็นบัญชีทดสอบมิได้ถูกลบในภายหลังตามที่กล่าวอ้างแต่ถูกนำไปใช้ในการรับหรือโอนเงิน การฟอกเงิน การฉ้อโกง หรือการขบถเงินเบิกเกินบัญชีในนามของผู้เสียหายกรณีนี้จึงแสดงให้เห็นว่า Job Scam อาจมีได้มุ่งให้ผู้เสียหายโอนเงินโดยตรง แต่เป็นการหลอกให้ผู้เสียหายเปิดเผยข้อมูลส่วนบุคคลและยืนยันตัวตนเพื่อเปิดบัญชี ซึ่งผู้กระทำความผิดนำไปใช้เป็นเครื่องมือในการกระทำความผิดอื่นต่อไปได้ (Verbraucherzentrale Hessen, Job-Scamming: Geldwäschekonto statt Job), สืบค้นเมื่อวันที่ ๕ มิถุนายน ๒๕๖๔, จาก <https://www.verbraucherzentrale-hessen.de/pressemitteilungen/jobscamming-geldwaeschekonto-statt-job-104988>)

มีกฎหมายบัญญัติไว้อย่างชัดเจนและแน่นอนว่าเป็นความผิด อีกทั้งยังต้องอยู่ภายใต้หลักห้ามใช้กฎหมายอาญาโดยเทียบเคียงในทางที่เป็นโทษแก่ผู้ถูกกล่าวหา (Analogieverbot) แม้ข้อเท็จจริงที่เกิดขึ้นจะแสดงให้เห็นถึงช่องว่างของกฎหมายก็ตาม เพราะการกำหนดความผิดและโทษเป็นอำนาจหน้าที่ของฝ่ายนิติบัญญัติในการตรากฎหมายขึ้นใช้บังคับ เพื่อให้บุคคลสามารถทราบล่วงหน้าได้ว่าการกระทำใดเป็นความผิดและมีโทษทางอาญา ฝ่ายตุลาการจึงไม่อาจอาศัยการตีความเพื่อสร้างฐานความผิดขึ้นใหม่หรือขยายขอบเขตความรับผิดชอบทางอาญาให้ครอบคลุมกรณีที่กฎหมายมิได้บัญญัติไว้โดยชัดแจ้งได้ นอกจากนี้มาตรการสืบสวนสอบสวนที่กระทบสิทธิของบุคคล เช่น การเข้าถึงข้อมูล การติดตามพยานหลักฐานดิจิทัลหรือการขอข้อมูลจากผู้ให้บริการ ก็ต้องมีฐานอำนาจตามกฎหมายวิธีพิจารณาความอาญาและสอดคล้องกับหลักนิติรัฐตามมาตรา ๒๐ วรรคสาม ของรัฐธรรมนูญฯ ด้วยเช่นกัน กรณีจึงเห็นได้ว่า การรับมือกับการหลอกลวงทางไซเบอร์ในระบบกฎหมายเยอรมันต้องดำเนินไปโดยรักษาดุลยภาพระหว่างประสิทธิภาพในการบังคับใช้กฎหมายกับหลักประกันสิทธิและเสรีภาพของบุคคลในกระบวนการยุติธรรมทางอาญา

๓. มาตรการทางกฎหมายที่ใช้บังคับกับการหลอกลวงทางไซเบอร์ในระบบกฎหมายเยอรมัน

โดยที่ระบบกฎหมายเยอรมันมิได้มีกฎหมายเฉพาะเพื่อจัดการกับการหลอกลวงทางไซเบอร์ (Cyber Scam) อย่างครอบคลุมตั้งแต่กระบวนการควบคุม ปราบปราม การนำผู้กระทำความผิดมาลงโทษ ตลอดจนการติดตามและริบทรัพย์เพื่อชดเชยคืนแก่ผู้เสียหาย การรับมือกับการกระทำความผิดจึงต้องอาศัยการปรับใช้กฎหมายที่มีอยู่ตามลักษณะของพฤติกรรมและผลเสียหายที่เกิดขึ้น โดยในทางอาญา การกำหนดความรับผิดและโทษของผู้กระทำความผิดเป็นไปตามประมวลกฎหมายอาญา (Strafgesetzbuch: StGB) ซึ่งจะต้องพิจารณาว่าการกระทำที่เป็นมูลเหตุให้เกิดความเสียหายนั้นเข้าองค์ประกอบความผิดฐานใด ส่วนการเยียวยาผู้เสียหายในทางแพ่งจะเป็นไปตามประมวลกฎหมายแพ่ง (Bürgerliches Gesetzbuch: BGB) โดยเฉพาะหลักกฎหมายว่าด้วยธุรกรรมการชำระเงินที่ไม่ได้รับอนุญาต ลาภมิควรได้ และความรับผิดชอบทางละเมิด ขณะที่การรวบรวมพยานหลักฐานดิจิทัล การติดตามตัวผู้กระทำความผิด และการติดตามทรัพย์สินที่ได้จากการกระทำความผิดต้องอาศัยมาตรการตามกฎหมายวิธีพิจารณาความอาญา (Strafprozessordnung: StPO) นอกจากนี้ ยังมีกฎหมายอื่นที่มีบทบาทเสริมในการกำกับดูแลระบบการเงินและระบบดิจิทัลให้มีความปลอดภัยและมีประสิทธิภาพยิ่งขึ้น เช่น กฎหมายกำกับบริการชำระเงิน^{๑๕}

^{๑๕} กฎหมายกำกับบริการชำระเงินของเยอรมนี (Zahlungsdiensteaufsichtsgesetz: ZAG) เป็นกฎหมายที่กำหนดกรอบการกำกับดูแลผู้ให้บริการชำระเงินและบริการเงินอิเล็กทรอนิกส์ โดยมีสาระสำคัญเกี่ยวกับการอนุญาตประกอบธุรกิจ การกำกับดูแลผู้ให้บริการ หน้าที่ด้านความมั่นคงปลอดภัย และการคุ้มครองผู้ใช้บริการชำระเงินในบริบทของการหลอกลวงทางไซเบอร์ บทบัญญัติที่มีความสำคัญ ได้แก่ มาตรา ๕๕ ZAG ซึ่งกำหนดให้ผู้ให้บริการชำระเงินต้องใช้การยืนยันตัวตนลูกค้าอย่างเข้มงวด (starke Kundenauthentifizierung) เมื่อผู้จ่ายเข้าถึงบัญชีชำระเงินออนไลน์ เริ่มทำธุรกรรมอิเล็กทรอนิกส์ หรือดำเนินการผ่านช่องทางระยะไกลที่มีความเสี่ยงต่อการฉ้อโกงหรือการใช้ในทางมิชอบ กฎหมายฉบับนี้จึงมีบทบาทในเชิงป้องกันและลดความเสี่ยงจากการใช้ข้อมูลชำระเงินโดยมิชอบ แม้มิใช่กฎหมายที่กำหนดฐานความผิด Cyber Scam โดยตรง

กฎหมายป้องกันและปราบปรามการฟอกเงิน^{๑๖} กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์^{๑๗} อย่างไรก็ตาม วัตถุประสงค์นี้จะมุ่งพิจารณามาตรการทางกฎหมายในสามส่วนหลัก ได้แก่ มาตรการทางอาญา มาตรการทางแพ่ง และมาตรการสืบสวนสอบสวน

๓.๑ มาตรการทางอาญา^{๑๘}

ความผิดฐานฉ้อโกงตามมาตรา ๒๖๓ StGB เป็นฐานความผิดหลักที่ใช้กับการหลอกลวงทางไซเบอร์ในกรณีที่ผู้กระทำความผิดใช้กลอุบายหลอกลวงให้ผู้เสียหายเกิดความสำคัญผิด และอาศัยความสำคัญผิดนั้นเป็นเหตุให้ผู้เสียหายกระทำการเกี่ยวกับทรัพย์สิน เช่น โอนเงิน ชำระค่าสินค้าหรือบริการ ส่งมอบทรัพย์สิน หรือเข้าร่วมลงทุนออนไลน์ปลอม ทั้งนี้ การที่ผู้เสียหายเป็นผู้โอนเงินหรือส่งมอบทรัพย์สินด้วยตนเองไม่ทำให้ความผิดฐานฉ้อโกงหมดไป หากการตัดสินใจนั้นเกิดจากข้อเท็จจริงอันเป็นเท็จที่ผู้กระทำความผิดสร้างขึ้น เช่น การแอบอ้างตัวตน การแสดงสถานะทางธุรกิจที่ไม่มีอยู่จริง การเสนอผลตอบแทนเกินจริง หรือการสร้างควมไว้วางใจเพื่อจูงใจให้ผู้เสียหายโอนเงิน อย่างไรก็ตาม หากความเสียหายทางทรัพย์สินมิได้เกิดจากการหลอกลวงมนุษย์โดยตรงในขั้นตอนสุดท้าย แต่เกิดจากการใช้ข้อมูลหรือกระบวนการประมวลผลของระบบคอมพิวเตอร์โดยมิชอบ เช่น การนำรหัสผ่านที่ได้จากการฟิชซิงไปเข้าสู่ระบบธนาคารออนไลน์และสั่งโอนเงินเองในภายหลัง ต้องพิจารณาความผิดฐานฉ้อโกงโดยใช้คอมพิวเตอร์ตามมาตรา ๒๖๓a StGB อันเป็นบทบัญญัติที่อุดช่องว่างในกรณีที่ระบบคอมพิวเตอร์ถูกใช้เป็นกลไกก่อให้เกิดผลเสียหายทางทรัพย์สินโดยไม่จำเป็นต้องมีบุคคลใดถูกหลอกให้ สำคัญผิดในขณะทำธุรกรรมนั้น

นอกจากความผิดที่มุ่งคุ้มครองทรัพย์สินโดยตรงแล้ว การหลอกลวงทางไซเบอร์จำนวนมากยังเริ่มจากการได้มาซึ่งข้อมูลสำคัญของผู้เสียหาย เช่น รหัสผ่าน ข้อมูลบัญชี ข้อมูลบัตรชำระเงินหรือข้อมูลยืนยันตัวตน การกระทำในขั้นตอนเตรียมการดังกล่าวจึงต้องพิจารณาตามบทบัญญัติที่กำหนดฐาน

^{๑๖} กฎหมายป้องกันและปราบปรามการฟอกเงินของเยอรมนี (Geldwäschegesetz: GwG) เป็นกฎหมายที่มุ่งป้องกันมิให้ระบบการเงินถูกใช้เพื่อฟอกเงินหรือสนับสนุนการกระทำความผิด โดยกำหนดหน้าที่แก่ผู้มีหน้าที่ตามกฎหมาย เช่น สถาบันการเงิน ผู้ให้บริการทางการเงิน และผู้ประกอบการวิชาชีพบางประเภท ในการตรวจสอบลูกค้า เก็บรักษาข้อมูล จัดให้มีมาตรการภายใน และรายงานธุรกรรมที่มีเหตุอันควรสงสัย บทบัญญัติที่สำคัญ ได้แก่ มาตรา ๑๐ GwG ว่าด้วยหน้าที่ตรวจสอบลูกค้า (Sorgfaltspflichten) และมาตรา ๔๓ GwG ว่าด้วยการรายงานข้อเท็จจริงที่น่าสงสัยต่อหน่วยงานที่เกี่ยวข้อง ในบริบทของการหลอกลวงทางไซเบอร์ กฎหมายฉบับนี้มีบทบาทในขั้นตอนหลังการหลอกลวง โดยเฉพาะกรณีการใช้บัญชีบุคคลที่สาม บัญชีม้า การโอนเงินหลายทอดหรือการนำเงินที่ได้จากการฉ้อโกงเข้าสู่ระบบการเงิน

^{๑๗} กฎหมายว่าด้วยสำนักงานกลางเพื่อความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยสารสนเทศของหน่วยงานหรือกิจการที่เกี่ยวข้อง (BSI-Gesetz: BSIg) เป็นกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ของเยอรมนี ซึ่งกำหนดบทบาทของสำนักงานกลางเพื่อความมั่นคงปลอดภัยสารสนเทศ (Bundesamt für Sicherheit in der Informationstechnik: BSI) รวมทั้งหน้าที่ของหน่วยงานหรือกิจการที่มีความสำคัญในการจัดให้มีมาตรการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ การป้องกัน ตรวจสอบ และรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ตลอดจนหน้าที่เกี่ยวกับการรายงานเหตุการณ์สำคัญ กฎหมายฉบับนี้มีได้มุ่งโทษการหลอกลวงทางไซเบอร์เป็นการเฉพาะ แต่มีบทบาทเชิงป้องกันและกำกับดูแลโครงสร้างพื้นฐานและบริการดิจิทัลที่อาจถูกใช้เป็นช่องทางหรือเป้าหมายของการกระทำความผิดทางไซเบอร์

^{๑๘} Ceffinato, Einführung in das Internetstrafrecht, JuS 2019, 337; Beukelmann, Cyber-Attacken – Erscheinungsformen, Strafbarkeit und Prävention, NJW-Spezial 2017, 376.

ความผิดเกี่ยวกับข้อมูลตามมาตรา ๒๐๒a ถึงมาตรา ๒๐๒d StGB ได้แก่ การล้วงข้อมูล การดักจับข้อมูล การเตรียมการล้วงหรือดักจับข้อมูล และการรับหรือจำหน่ายข้อมูลที่ได้มาโดยมิชอบ ซึ่งเป็นกลุ่มฐานความผิดที่กำหนดขึ้นเพื่อคุ้มครองความลับและความปลอดภัยของข้อมูลโดยตรง ในกรณีนี้ผู้กระทำความผิดใช้ข้อมูลอิเล็กทรอนิกส์หรือเอกสารดิจิทัลปลอมเพื่อสร้างความน่าเชื่อถือ เช่น เว็บไซต์ปลอม เอกสารรับรองการลงทุนปลอม หลักฐานการโอนเงินปลอม หรือข้อมูลที่ทำให้ผู้เสียหายเข้าใจว่าธุรกรรมมีอยู่จริง อาจต้องพิจารณาความผิดฐานปลอมแปลงข้อมูลที่มีความสำคัญในทางพยานหลักฐานตามมาตรา ๒๖๙ StGB ประกอบด้วย ทั้งนี้ การใช้ข้อความหลอกลวงผ่านอีเมลหรือเว็บไซต์มิได้เข้าองค์ประกอบมาตรา ๒๖๙ StGB โดยอัตโนมัติ แต่ต้องพิจารณาว่าข้อมูลนั้นมีคุณสมบัติเป็นข้อมูลที่ใช้พิสูจน์ข้อเท็จจริงในทางกฎหมายได้หรือไม่

เมื่อทรัพย์สินถูกโอนจากผู้เสียหายแล้ว การดำเนินคดีทางอาญายังต้องพิจารณาการเคลื่อนย้าย ช้อนเงิน หรือเปลี่ยนสภาพทรัพย์สินที่ได้จากการกระทำความผิด โดยเฉพาะกรณีการใช้บัญชีบุคคลที่สาม บัญชีม้า บัญชีที่เปิดโดยใช้ข้อมูลของผู้เสียหายหรือคนกลางรับโอนเงินรวมถึงการโอนเงินหลายทอดไปยังต่างประเทศ ซึ่งอาจเกี่ยวข้องกับความผิดฐานฟอกเงินตามมาตรา ๒๖๑ StGB แม้บุคคลที่รับหรือโอนเงินต่อไปจะเป็นผู้หลอกลวงผู้เสียหายโดยตรง แต่หากรู้หรือควรรู้ตามพฤติการณ์ว่าเงินหรือทรัพย์สินนั้นมีที่มาจากกระทำความผิด ก็อาจมีความรับผิดชอบฟอกเงินได้ นอกจากนี้มาตรการริบทรัพย์สินหรือริบผลประโยชน์ที่ได้จากการกระทำความผิดตามมาตรา ๗๓ StGB ยังมีความสำคัญต่อการตัดวงจรผลประโยชน์ของเครือข่ายผู้กระทำความผิด และอาจสนับสนุนการนำทรัพย์สินกลับมาใช้เพื่อเยียวยาผู้เสียหายในทางปฏิบัติ

๓.๒ มาตรการทางแพ่งและการเยียวยาผู้เสียหาย^{๑๙}

การเยียวยาผู้เสียหายจากการหลอกลวงทางไซเบอร์ที่ดำเนินการผ่านธุรกรรมธนาคารออนไลน์หรือบริการชำระเงิน มีการบัญญัติไว้ในประมวลกฎหมายแพ่ง (Bürgerliches Gesetzbuch: BGB) มาตรา ๖๗๕j มาตรา ๖๗๕n และมาตรา ๖๗๕v ซึ่งวางหลักเกี่ยวกับความรับผิดชอบของผู้ให้บริการในกรณีที่มีการทำธุรกรรมชำระเงินโดยไม่ได้รับอนุญาต (nicht autorisierter Zahlungsvorgang) กล่าวคือ ธุรกรรมชำระเงินจะมีผลเป็นธุรกรรมที่ได้รับอนุญาตได้ต่อเมื่อผู้จ่ายให้ความยินยอมตามมาตรา ๖๗๕j BGB โดยในกรณีที่พิสูจน์ได้ว่าเป็นธุรกรรมที่ไม่ได้รับอนุญาต ผู้ให้บริการชำระเงินของผู้จ่าย เช่น ธนาคาร มีหน้าที่คืนเงินหรือทำให้บัญชีกลับคืนสู่สถานะเสมือนไม่มีธุรกรรมนั้นเกิดขึ้นตามมาตรา ๖๗๕n BGB เว้นแต่เป็นกรณีที่ความเสียหายเกิดจากการที่ผู้จ่ายจงใจหรือประมาทเลินเล่ออย่างร้ายแรงในการรักษาข้อมูลหรือเครื่องมือชำระเงิน ซึ่งกรณีดังกล่าวผู้จ่ายต้องรับผิดชอบในความเสียหายที่เกิดขึ้นเอง โดยไม่อาจเรียกร้องจากผู้ให้บริการได้ตามมาตรา ๖๗๕v BGB^{๒๐}

^{๑๙} Kirchner, Die Verteilung von Haftungsrisiken bei Zahlungsvorgängen unter Einsatz von Debitkarte, BKR 2023, 703.

^{๒๐} ตัวอย่างแนวคำพิพากษาเกี่ยวกับความรับผิดชอบของผู้ให้บริการชำระเงินในกรณีธุรกรรมชำระเงินที่ไม่ได้รับอนุญาต ปรากฏจากคำพิพากษาศาลสูงมลรัฐโคเบลนซ์ (Oberlandesgericht Koblenz) วันที่ ๑๗ เมษายน ๒๕๖๙ คดีหมายเลข 8 U 682/24 ซึ่งพิพากษาให้ธนาคาร Sparkasse คืนเงินแก่ลูกค้าจำนวน ๕๖,๐๙๙.๙๑ ยูโร จากกรณีที่ผู้กระทำความผิดทำรายการโอนเงินแบบทันทีหลายรายการไปยังบัญชีต่างประเทศโดยอาศัยกลโกงฟิชซิง

หลักการดังกล่าวมีความสำคัญในคดีพิขิงหรือการใช้ข้อมูลธนาคารออนไลน์โดยมิชอบ ซึ่งมีประเด็นต้องพิจารณาข้อเท็จจริงให้ได้ข้อยุติในเบื้องต้นก่อนว่าผู้เสียหายได้อนุญาตให้ดำเนินการธุรกรรมที่ก่อให้เกิดความเสียหายหรือไม่ หากผู้กระทำความผิดนำข้อมูลของผู้เสียหายไปใช้สั่งโอนเงินเองโดยที่ผู้เสียหายมิได้ให้ความยินยอมต่อธุรกรรมนั้น ย่อมอาจเป็นธุรกรรมการชำระเงินที่ไม่ได้รับอนุญาตซึ่งก่อให้เกิดสิทธิเรียกร้องต่อผู้ให้บริการชำระเงินตามมาตรา ๖๗๕๐ BGB ได้ ในทางกลับกัน หากผู้เสียหายเป็นผู้สั่งโอนเงินเองโดยรู้ว่าเป็นการโอนเงิน แม้จะกระทำไปเพราะถูกหลอกเกี่ยวกับตัวตน เหตุผล หรือวัตถุประสงค์ของการโอนเงิน เช่น Romance Scam การหลอกให้ชำระเงินล่วงหน้า (Vorschussbetrug) หรือ Technical Support Scam กรณีดังกล่าวอาจไม่อยู่ในขอบเขตของธุรกรรมการชำระเงินที่ไม่ได้รับอนุญาตเสมอไป จึงต้องพิจารณาสิทธิเรียกร้องในความเสียหายที่เกิดขึ้นโดยอาศัยฐานตามกฎหมายอื่นต่อไป

นอกจากสิทธิเรียกร้องต่อผู้ให้บริการชำระเงินแล้ว ผู้เสียหายอาจอาศัยหลักกลาภมิควรได้ตามมาตรา ๘๑๒ BGB เพื่อเรียกคืนเงินจากผู้รับเงินที่ได้รับทรัพย์สินไปโดยไม่มีมูลทางกฎหมาย เช่น ผู้รับโอนเงินปลายทางที่ไม่มีนิติสัมพันธ์กับผู้เสียหาย^{๒๑} หรือผู้ถือบัญชีที่ยินยอมให้บุคคลอื่นใช้บัญชีของตนเป็นช่องทางรับและโอนเงินจากการหลอกลวงทางอินเทอร์เน็ต^{๒๒} หรืออาจเรียกค่าเสียหายทางละเมิดตาม

ข้อเท็จจริงปรากฏว่า ลูกค้าได้รับโทรศัพท์จากบุคคลที่แอบอ้างว่าเป็นเจ้าหน้าที่ฝ่ายเทคนิคของธนาคาร แจ้งว่าจำเป็นต้องเปลี่ยนระบบยืนยันธุรกรรมจาก ChipTAN เป็น pushTAN โดยผู้โทรมีข้อมูลเกี่ยวกับบัญชีของลูกค้าหลายประการ และหมายเลขโทรศัพท์ที่ปรากฏก็เป็นหมายเลขของธนาคาร ต่อมาลูกค้าได้กดลิงก์เปิดใช้งาน (Aktivierungslink) ที่เกี่ยวข้องกับกระบวนการเปลี่ยนระบบดังกล่าว ซึ่งธนาคารอ้างว่าเป็นพฤติกรรมที่แสดงถึงความประมาทเลินเล่ออย่างร้ายแรงของลูกค้า อย่างไรก็ตาม ศาลเห็นว่า การกดลิงก์ดังกล่าวโดยลำพังยังไม่เพียงพอที่จะถือว่าลูกค้ากระทำการโดยขาดความระมัดระวังอย่างร้ายแรง เนื่องจากพฤติกรรมโดยรวมทำให้ลูกค้าอาจเข้าใจได้ว่าเป็นขั้นตอนปกติในการเปิดใช้งานระบบยืนยันธุรกรรมของธนาคาร ศาลจึงวินิจฉัยว่า รายการโอนเงินดังกล่าวมิได้รับอนุญาตจากลูกค้าและก่อก่อสิทธิเรียกร้องให้ธนาคารคืนเงินตามมาตรา ๖๗๕๐ BGB ส่วนข้ออ้างว่าลูกค้าประมาทเลินเล่ออย่างร้ายแรงนั้น ธนาคารมีภาระพิสูจน์แต่ไม่สามารถพิสูจน์ได้ อีกทั้งผู้เชี่ยวชาญยังเห็นว่าในทางเทคนิคมีความเป็นไปได้ที่รหัสเปิดใช้งานสำคัญจะปรากฏบนอุปกรณ์ของผู้กระทำความผิดโดยตรงโดยที่ลูกค้ามิได้ส่งมอบรหัสดังกล่าวให้แก่ผู้กระทำความผิด คำพิพากษานี้จึงสะท้อนว่า ในคดีพิขิง การที่ผู้เสียหายกดลิงก์หรือดำเนินการบางอย่างผ่านระบบออนไลน์มิได้ทำให้ผู้เสียหายต้องรับผิดชอบโดยอัตโนมัติ แต่ต้องพิจารณาพฤติการณ์ของกลโกง ภาระพิสูจน์ของธนาคาร และความสามารถของผู้ใช้บริการทั่วไปในการสังเกตเห็นความผิดปกตินั้นเป็นรายกรณี (OLG Koblenz, Urteil vom 17.04.2026, Az. 8 U 682/24)

^{๒๑} โปรดดูตัวอย่างแนวคำพิพากษาในเชิงอรรถที่ ๑๐

^{๒๒} ตัวอย่างแนวคำวินิจฉัยเกี่ยวกับความรับผิดชอบฐานกลาภมิควรได้ของผู้ถือบัญชีที่ยอมให้บุคคลอื่นใช้บัญชีของตนเป็นช่องทางรับเงินจากการหลอกลวงทางอินเทอร์เน็ต ปรากฏจากคำวินิจฉัยศาลสูงมลรัฐเดรสเดน (Oberlandesgericht Dresden) วันที่ ๒๐ กรกฎาคม ๒๕๖๔ คดีหมายเลข 8 U 840/21 ข้อเท็จจริงในคดีดังกล่าวปรากฏว่า จำเลยเปิดบัญชีธุรกิจและส่งมอบข้อมูล Online Banking ให้แก่บุคคลที่ไม่รู้จักผ่านการติดต่อทางอินเทอร์เน็ต โดยได้รับค้ำประกันว่าจะได้รับค่าตอบแทนเดือนละ ๖๐๐ ยูโร ต่อมา โจทก์ประสงค์จะซื้อทองคำจำนวน ๖ กิโลกรัมและได้ค้นหาข้อมูลผ่านอินเทอร์เน็ตจนเข้าสู่เว็บไซต์ซื้อขายทองคำปลอม ซึ่งแจ้งให้โจทก์ชำระเงินล่วงหน้าเข้าบัญชีธนาคารที่ระบุไว้ โจทก์จึงโอนเงินจำนวน ๓๑๐,๕๓๐.๘๐ ยูโร เข้าบัญชีที่จำเลยเปิดไว้ในชื่อตนเอง และภายหลังเงินดังกล่าวถูกโอนต่อไปยังบัญชีอื่นโดยบุคคลที่ไม่ปรากฏตัว เมื่อโจทก์ไม่ได้รับทองคำและไม่สามารถเรียกเงินโอนกลับคืนได้ จึงฟ้องจำเลยเรียกเงินบางส่วนจำนวน ๖๐,๐๐๐ ยูโร ศาลเห็นว่า การโอนเงินเข้าบัญชีของจำเลยทำให้จำเลยได้รับประโยชน์ในทางทรัพย์สินตามมาตรา ๘๑๒ วรรคหนึ่ง ประโยคหนึ่ง BGB (Leistungskondiktion) เพราะจำเลยเป็นเจ้าของบัญชี

มาตรา ๘๒๓ วรรคสอง BGB ในกรณีที่การกระทำของผู้กระทำความผิดเป็นการฝ่าฝืนกฎหมายที่มีวัตถุประสงค์คุ้มครองบุคคลอื่น^{๒๓} เช่น ความผิดฐานฉ้อโกงตามมาตรา ๒๖๓ StGB อย่างไรก็ตาม การเยียวยาทางแพ่งในทางปฏิบัติยังมีข้อจำกัดจากการระบุตัวผู้กระทำความผิด การติดตามบัญชีปลายทาง และการบังคับคดีกับทรัพย์สินที่ถูกโอนต่อไปหลายทอดหรือถูกโอนไปยังต่างประเทศ

๓.๓ มาตรการสืบสวนสอบสวน

การสืบสวนสอบสวนคดีหลอกลวงทางไซเบอร์ในระบบกฎหมายเยอรมันต้องดำเนินการตามกฎหมายวิธีพิจารณาความอาญา (Strafprozessordnung: StPO) โดยมีปัญหาและอุปสรรคที่สำคัญในขั้นตอนการแสวงหา รวบรวม และรักษาพยานหลักฐานดิจิทัลให้ทันต่อสภาพของข้อมูลที่อาจถูกลบแก้ไข หรือไม่สามารถตรวจสอบย้อนหลังได้เมื่อพ้นระยะเวลาการเก็บรักษาของผู้ให้บริการ^{๒๔} มาตรการ

และมีสิทธิเรียกร้องต่อธนาคารจากยอดเงินที่เข้าบัญชี แม้ภายหลังเงินจะถูกบุคคลอื่นโอนต่อไปก็ตาม นอกจากนี้ จำเลยไม่อาจอ้างว่าลาภหมดสิ้นไปแล้วตามมาตรา ๘๑๘ วรรคสาม BGB ได้ (Entreichungseinwand) เนื่องจากต้องรับผิดชอบโดยเคร่งครัดตามมาตรา ๘๑๙ วรรคหนึ่ง ประกอบมาตรา ๘๑๘ วรรคสี่ BGB โดยศาลเห็นว่า จำเลยยอมให้บุคคลที่ไม่รู้จักใช้บัญชีเป็นปกติโดยไม่ควบคุมหรือตรวจสอบทั้งที่มีพฤติการณ์น่าสงสัยหลายประการ เช่น การได้รับคำตอบแทนสูงเพียงเพื่อให้ใช้บัญชี การใช้บัญชีของบุคคลอื่นเพื่อธุรกิจออนไลน์ และการส่งมอบบัญชีหรือข้อมูลบัญชีหลายบัญชี พฤติการณ์ดังกล่าวทำให้จำเลยไม่อาจอ้างความไม่รู้หรือยกข้อต่อสู้เรื่องหมดสิ้นลาภเพื่อหลีกเลี่ยงความรับผิดได้ (OLG Dresden, Beschluss vom 20.07.2021, Az. 8 U 840/21)

^{๒๓} ตัวอย่างแนวคำพิพากษาเกี่ยวกับความรับผิดทางแพ่งของบุคคลที่ยอมให้ใช้บัญชีธนาคารของตนเป็นช่องทางรับเงินจากการฉ้อโกงทางอินเทอร์เน็ต ปรากฏจากคำพิพากษาศาลยุติธรรมสหพันธ์เยอรมนี (Bundesgerichtshof: BGH) วันที่ ๑๙ ธันวาคม ๒๕๕๕ คดีหมายเลข VIII ZR 302/11 ข้อเท็จจริงในคดีนี้ปรากฏว่า ผู้เสียหายสั่งซื้อกล้องดิจิทัลจากร้านค้าออนไลน์ปลอมและโอนเงินค่าสินค้าเข้าบัญชีของจำเลย ซึ่งจำเลยได้เปิดเผยข้อมูลการเข้าถึงบัญชีกระแสรายวันออนไลน์ของตนแก่บุคคลที่ไม่รู้จักผ่านอินเทอร์เน็ต และยอมให้บุคคลดังกล่าวใช้บัญชีอย่างต่อเนื่องโดยได้รับคำตอบแทน ภายในระยะเวลาไม่นานมีเงินผ่านบัญชีของจำเลยประมาณ ๕๑,๐๐๐ ยูโร จำเลยถูกลงโทษฐานฟอกเงินโดยประมาทเลินเล่ออย่างร้ายแรงตามมาตรา ๒๖๑ StGB โดยมีความผิดมูลฐานเป็นการฉ้อโกงเป็นอาชญากรรมตามมาตรา ๒๖๓ StGB ทั้งนี้ BGH วินิจฉัยว่า ผู้เสียหายมีสิทธิเรียกค่าเสียหายจากจำเลยตามมาตรา ๘๒๓ วรรคสอง BGB ประกอบมาตรา ๒๖๑ StGB เนื่องจากความผิดฐานฟอกเงินมีวัตถุประสงค์คุ้มครองทรัพย์สินของผู้เสียหายจากความผิดมูลฐานด้วย จึงเป็นกฎหมายที่มีวัตถุประสงค์คุ้มครองบุคคลอื่น (Schutzgesetz) ในความหมายของมาตรา ๘๒๓ วรรคสอง BGB (BGH, Urteil vom 19.12.2012, Az. VIII ZR 302/11)

^{๒๔} ประเด็นเรื่องระยะเวลาการเก็บรักษาข้อมูลของผู้ให้บริการเป็นปัญหาสำคัญในการสืบสวนสอบสวนคดีอาญาทางอินเทอร์เน็ตในเยอรมนี เนื่องจาก IP address มักเป็นร่องรอยทางเทคนิคสำคัญในการระบุตัวผู้ใช้งาน แต่ IP address จำนวนมากถูกกำหนดให้แก่ผู้ใช้งานแบบชั่วคราว และผู้ให้บริการบางรายเก็บข้อมูลไว้เพียงไม่กี่วัน ทำให้ไม่สามารถระบุตัวย้อนหลังได้เมื่อข้อมูลถูกลบไปแล้ว ในปี ๒๕๖๙ รัฐบาลเยอรมนีจึงมีข้อเสนอให้ผู้ให้บริการเก็บรักษา IP address พร้อมข้อมูลทางเทคนิคประกอบ เช่น port number เวลาเริ่มต้นหรือสิ้นสุดการใช้งาน เป็นเวลา ๓ เดือน เพื่อให้หน่วยงานบังคับใช้กฎหมายสามารถระบุตัวผู้ใช้งานได้ในกรณีข้อสงสัยเบื้องต้นเกี่ยวกับความผิดอาญาที่มีความร้ายแรง อย่างไรก็ตาม ข้อเสนอดังกล่าวยังเป็นที่ถกเถียงเนื่องจากฝ่ายคัดค้านเห็นว่าเป็นการเก็บข้อมูลของผู้ใช้อินเทอร์เน็ตทั่วไปไว้ล่วงหน้าโดยไม่มีเหตุเฉพาะราย และอาจมีลักษณะใกล้เคียงกับการเก็บข้อมูลจราจรทางการสื่อสารไว้ล่วงหน้า (Vorratsdatenspeicherung) ซึ่งกระทบต่อสิทธิขั้นพื้นฐาน, Deutschlandfunk, Kampf gegen Cyberkriminalität: Der Streit um die IP-Adressen-Speicherung, สืบค้นเมื่อวันที่ ๕ มิถุนายน ๒๕๖๙, จาก <https://www.deutschlandfunk.de/ip-adresse-speicherung-digitale-gewalt-stra-verfolgung-100.html>

พื้นฐานที่อาจนำมาใช้ ได้แก่ การยึดหรืออายัดพยานหลักฐานตามมาตรา ๙๔ ถึงมาตรา ๙๘ StPO การตรวจค้นสถานที่หรือระบบที่เกี่ยวข้องตามมาตรา ๑๐๒ และมาตรา ๑๐๓ StPO รวมทั้งการเรียกหรือขอข้อมูลจากผู้ให้บริการที่เกี่ยวข้อง ทั้งนี้ การใช้มาตรการดังกล่าวต้องมีฐานอำนาจตามกฎหมายและอยู่ภายใต้หลักความได้สัดส่วน เนื่องจากการเข้าถึงข้อมูลดิจิทัลมักกระทบต่อสิทธิในความเป็นส่วนตัวและการคุ้มครองข้อมูลของบุคคล^{๒๕}

ในกรณีที่การหลอกลวงทางไซเบอร์มีลักษณะเป็นเครือข่ายหรือมีการใช้ช่องทางสื่อสารทางอิเล็กทรอนิกส์อย่างเป็นระบบ เจ้าหน้าที่อาจต้องอาศัยมาตรการสืบสวนสอบสวนที่มีลักษณะเข้มข้นขึ้น เช่น การดักจับหรือเฝ้าระวังการสื่อสารทางโทรคมนาคมตามมาตรา ๑๐๐a StPO การเก็บหรือขอข้อมูลจราจรทางการสื่อสารตามมาตรา ๑๐๐g StPO หรือในกรณีความผิดร้ายแรงบางประเภท การค้นระบบเทคโนโลยีสารสนเทศโดยลับตามมาตรา ๑๐๐b StPO อย่างไรก็ตาม มาตรการเหล่านี้มิได้ใช้ได้โดยทั่วไปกับทุกกรณีของการหลอกลวงทางไซเบอร์ แต่ต้องพิจารณาตามฐานความผิด ความร้ายแรงของคดี เงื่อนไขเฉพาะที่กฎหมายกำหนด และการอนุญาตจากศาลหรือองค์กรที่มีอำนาจตามที่กฎหมายบัญญัติ การบังคับใช้กฎหมายจึงต้องรักษาดุลยภาพระหว่างประสิทธิภาพในการติดตามผู้กระทำความผิดกับหลักประกันสิทธิของบุคคลในกระบวนการยุติธรรมทางอาญา

นอกจากการติดตามตัวผู้กระทำความผิดแล้ว การสืบสวนสอบสวนคดีหลอกลวงทางไซเบอร์ยังต้องมุ่งติดตามเส้นทางทรัพย์สินที่ได้จากการกระทำความผิดควบคู่กันไป โดยเฉพาะกรณีที่มีการโอนเงินผ่านบัญชีบุคคลที่สาม บัญชีม้า ผู้รับโอนหลายทอด หรือการโอนเงินไปต่างประเทศ กฎหมายวิธีพิจารณาความอาญาเยอรมันจึงมีมาตรการยึดอายัด หรือรักษาทรัพย์สินไว้เพื่อรองรับการริบทรัพย์สิน หรือการคืนทรัพย์สินแก่ผู้เสียหายตามมาตรา ๑๑๑b ถึงมาตรา ๑๑๑q StPO อย่างไรก็ตาม ข้อจำกัดสำคัญของการสืบสวนสอบสวนคดีประเภทนี้อยู่ที่ความรวดเร็วในการเคลื่อนย้ายข้อมูลและทรัพย์สิน การใช้โครงสร้างพื้นฐานข้ามพรมแดน และการที่ผู้เกี่ยวข้องแต่ละรายอาจทำหน้าที่เพียงบางช่วงของกระบวนการ เช่น ผู้เปิดบัญชี ผู้รับโอน คนกลาง หรือผู้ฟอกเงิน ทำให้การดำเนินคดีต้องอาศัยทั้งมาตรการทางเทคนิคความร่วมมือกับผู้ให้บริการ และความร่วมมือระหว่างประเทศประกอบกัน^{๒๖}

^{๒๕} ในทางวิชาการเยอรมันมีข้อสังเกตว่า ปัญหาสำคัญของกฎหมายวิธีพิจารณาความอาญาในบริบทการดำเนินคดีเกี่ยวกับความผิดทางอินเทอร์เน็ต นั้น มีสาเหตุสืบเนื่องจากมาตรการสืบสวนสอบสวนทางเทคนิคที่ทันสมัยได้รับการบัญญัติรองรับไว้โดยตรงในประมวลกฎหมายวิธีพิจารณาความอาญา แม้แต่กรณีการยึดอีเมลซึ่งมิใช่มาตรการสืบสวนสอบสวนที่มีลักษณะใหม่หรือซับซ้อนเป็นพิเศษ ก็ยังไม่มีบทบัญญัติเฉพาะรองรับโดยตรง ดังนั้น ในกรณีที่เจ้าหน้าที่ประสงค์จะใช้มาตรการสืบสวนสอบสวนทางเทคนิค จึงต้องพิจารณาว่า เมื่อคำนึงถึงลักษณะของสิทธิที่ถูกกระทบและระดับความรุนแรงของการกระทบสิทธิแล้ว มาตรการดังกล่าวสามารถปรับเข้ากับฐานอำนาจที่มีอยู่ใน StPO ได้หรือไม่ ทั้งนี้ การตีความดังกล่าวต้องอยู่ภายใต้หลักนิติรัฐ หลักความได้สัดส่วน และหลักประกันสิทธิของบุคคลในกระบวนการยุติธรรมทางอาญา, Ceffinato, Einführung in das Internetstrafrecht, JuS 2019, 337

^{๒๖} รายงานสถานการณ์อาชญากรรมไซเบอร์ของสหพันธ์ (Bundeslagebild Cybercrime) ระบุว่า การระบุตัวและดำเนินคดีกับผู้กระทำความผิดเป็นแนวทางสำคัญในการรับมือกับอาชญากรรมไซเบอร์อย่างยั่งยืน อย่างไรก็ตาม เนื่องจากผู้กระทำความผิดทางไซเบอร์จำนวนมากพำนักอยู่ในต่างประเทศ และในบางกรณีอาจได้รับการยินยอมหรือรู้เห็นเป็นใจให้ดำเนินการหรือได้รับการคุ้มครองจากบางประเทศ ทำให้การนำตัวผู้กระทำความผิดเข้าสู่กระบวนการยุติธรรมเป็นไปได้ยาก มาตรการของเจ้าหน้าที่ตำรวจจึงมุ่งลดทอนหรือทำลายโครงสร้างพื้นฐานของผู้กระทำความผิดควบคู่กันไปด้วย แนวทางดังกล่าวปรากฏในรายงานสถานการณ์อาชญากรรมไซเบอร์ปี ๒๕๖๖ ที่สามารถติดตาม

สำหรับหน่วยงานที่มีภารกิจรับผิดชอบการปราบปรามการหลอกลวงทางไซเบอร์ในเยอรมนี นั้น อยู่ภายใต้การบูรณาการการบังคับใช้กฎหมายหลายระดับ โดยในระดับมลรัฐ หน่วยงานตำรวจอาชญากรรมของแต่ละมลรัฐ (Landeskriminalämter) มีบทบาทสำคัญในการสืบสวนสอบสวนและดำเนินการกับคดีไซเบอร์ที่เกิดขึ้นในพื้นที่รับผิดชอบ ส่วนในระดับสหพันธ์ สำนักงานตำรวจอาชญากรรมแห่งสหพันธ์ (Bundeskriminalamt: BKA) มีบทบาทเป็นหน่วยงานกลางในการประสานงานสนับสนุน และรวบรวมข้อมูลเกี่ยวกับอาชญากรรมไซเบอร์ รวมทั้งจัดทำรายงานสถานการณ์อาชญากรรมไซเบอร์ของสหพันธ์ (Bundeslagebild Cybercrime) เป็นประจำทุกปี ทั้งนี้ เนื่องจากการหลอกลวงทางไซเบอร์มักมีลักษณะข้ามพรมแดน การดำเนินคดีจึงไม่อาจอาศัยกลไกภายในประเทศเพียงอย่างเดียว แต่ต้องอาศัยความร่วมมือกับหน่วยงานระหว่างประเทศ โดยเฉพาะหน่วยงานกลางแห่งสหภาพยุโรป เพื่อความร่วมมือด้านการบังคับใช้กฎหมาย (European Union Agency for Law Enforcement Cooperation: Europol) ผ่านศูนย์อาชญากรรมไซเบอร์ยุโรป (European Cybercrime Centre: EC3) ซึ่งสนับสนุนการปฏิบัติการของประเทศสมาชิกการวิเคราะห์ข้อมูล และการแลกเปลี่ยนข้อมูลข่าวกรอง ตลอดจนองค์การตำรวจสากล (International Criminal Police Organization – INTERPOL: ICPO–INTERPOL) Interpol ซึ่งทำหน้าที่ส่งเสริมความร่วมมือระหว่างตำรวจของประเทศสมาชิก การแลกเปลี่ยนข้อมูล และการสนับสนุนทางเทคนิคและการปฏิบัติการในคดีอาชญากรรมข้ามพรมแดน

๔. บทสรุป

ระบบกฎหมายเยอรมันไม่ได้มีกฎหมายที่กำหนดกลไกสำหรับการป้องกันและปราบปรามการหลอกลวงทางไซเบอร์ (Cyber Scam) ไว้โดยตรงในกฎหมายฉบับเดียวที่มีบทบัญญัติในลักษณะเบ็ดเสร็จหรือครบวงจร ซึ่งแตกต่างจากแนวทางของบางประเทศที่เลือกตรากฎหมายเฉพาะเพื่อจัดการกับการหลอกลวงทางเทคโนโลยีหรือธุรกรรมดิจิทัล การดำเนินการดังกล่าวสะท้อนให้เห็นถึงนโยบายกฎหมายที่มุ่งอาศัยการปรับใช้บทบัญญัติที่มีอยู่ในกฎหมายหลายสาขาให้สอดคล้องกับลักษณะของการกระทำและผลเสียหายที่เกิดขึ้นโดยไม่จำเป็นต้องจัดตั้งฐานความผิดหรือกลไกขึ้นใหม่แยกต่างหาก ซึ่งทำให้ระบบกฎหมายมีความยืดหยุ่น สามารถนำบทบัญญัติที่มีอยู่ไปปรับใช้กับรูปแบบการกระทำความผิดที่เปลี่ยนแปลงตามเทคโนโลยีได้ โดยยังคงรักษาโครงสร้างและหลักประกันพื้นฐานของกฎหมายไว้ กล่าวคือ ในทางอาญาอาจพิจารณาตามความผิดฐานฉ้อโกง ฉ้อโกงโดยใช้คอมพิวเตอร์ ความผิดเกี่ยวกับข้อมูล การปลอมแปลงข้อมูลอิเล็กทรอนิกส์ และฟอกเงิน ส่วนในทางแพ่ง ผู้เสียหายอาจได้รับการเยียวยาผ่านหลักธุรกรรมการ

แหล่งเงินจำนวนมากออกจากระบบเศรษฐกิจใต้ดิน(Underground Economy) ยึดระบบเทคโนโลยีสารสนเทศและข้อมูลที่เป็นประโยชน์ต่อการสืบสวนสอบสวนเพิ่มเติม ปิดระบบ Crypto-Mixerและตลาดผิดกฎหมายหลายแห่ง จำกัดกิจกรรมของโทรจันสำคัญบางส่วน และหยุดยั้งกิจกรรมเรียกค่าไถ่ของกลุ่มแรนซัมแวร์บางกลุ่ม อันแสดงให้เห็นว่าแนวทางที่มุ่งจัดการกับโครงสร้างพื้นฐานของผู้กระทำความผิด (Infrastrukturansatz) และความร่วมมือระหว่างประเทศมีความสำคัญอย่างยิ่งต่อการดำเนินคดีอาชญากรรมไซเบอร์ โดยเฉพาะการเข้าควบคุมหรือทำลายโครงสร้างพื้นฐานของผู้กระทำความผิดเพื่อนำไปสู่การสืบสวนสอบสวนตัวบุคคลต่อไป, Bundeskriminalamt, Bundeslagebild Cybercrime 2023), สืบค้นเมื่อวันที่ ๕ มิถุนายน ๒๕๖๕, จาก https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2023/CC_2023.html

ชำระเงินที่ไม่ได้รับอนุญาต ลาภมิควรได้ และละเมิด ขณะที่การสืบสวนสอบสวนต้องอาศัยมาตรการตามประมวลกฎหมายวิธีพิจารณาความอาญาเพื่อรวบรวมพยานหลักฐานดิจิทัล ระบุตัวผู้กระทำความผิด และติดตามทรัพย์สิน โดยต้องคำนึงถึงฐานอำนาจตามกฎหมาย หลักความได้สัดส่วน และความร่วมมือระหว่างหน่วยงานทั้งในและต่างประเทศ แนวทางของเยอรมนีจึงเป็นการบูรณาการกฎหมายและกลไกที่มีอยู่เพื่อรับมือกับพฤติกรรมการณ์การกระทำความผิดที่เปลี่ยนแปลงไปตามเทคโนโลยี

ออสเตรเลีย*

๑. บทนำ

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารมีการพัฒนาอย่างรวดเร็วและต่อเนื่อง ส่งผลให้การเข้าถึงข้อมูลข่าวสารและการติดต่อสื่อสารเป็นไปได้อย่างสะดวกมากยิ่งขึ้น เทคโนโลยีดังกล่าวได้เข้ามามีบทบาทสำคัญในชีวิตประจำวันของประชาชน โดยช่วยให้สามารถเข้าถึงสื่อออนไลน์และบริการต่าง ๆ ผ่านอุปกรณ์อิเล็กทรอนิกส์ได้อย่างไร้ข้อจำกัด ทั้งยังเอื้อให้เกิดการติดต่อสื่อสารระหว่างบุคคลได้หลากหลายรูปแบบ มนุษย์ใช้โซเชียลมีเดียเพื่อการสนทนา ค้นหาข้อมูลทำธุรกรรม และซื้อขายสินค้า ซึ่งสามารถดำเนินการได้ตลอดเวลาที่ทั่วทุกหนทุกแห่งผ่านระบบอินเทอร์เน็ตนี้ ส่งผลให้หน่วยงานและองค์กรต่าง ๆ ต้องปรับเปลี่ยนแนวทางการดำเนินงานให้เข้ากับการเกิดขึ้นของโซเชียลมีเดีย อย่างไรก็ตาม เมื่อโซเชียลมีเดียหรือเทคโนโลยีสารสนเทศเข้ามามีอิทธิพลต่อการดำรงชีวิตก็ย่อมมีผู้ที่ไม่หวังดีที่เข้ามาหลอกลวง ขโมย และโจรกรรมข้อมูลต่าง ๆ ทางไซเบอร์เพื่อนำไปใช้ในทางที่ผิดกฎหมายจนนำมาซึ่งอาชญากรรมทางไซเบอร์ โดยลักษณะของอาชญากรรมทางไซเบอร์นั้นส่วนหนึ่งเกิดจากความไม่ระมัดระวังของผู้ใช้งานเอง เช่น การเปิดเผยรหัสผ่านแก่บุคคลที่ไม่น่าเชื่อถือ การติดต่อสื่อสารผ่านแพลตฟอร์มโซเชียลมีเดีย การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต พฤติกรรมที่อยากรู้อยากเห็น การเปิดเผยช่องโหว่ที่อาจทำให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลส่วนบุคคล และความไม่ตื่นตัวถึงความเสี่ยงทางไซเบอร์ เป็นต้น^๑

ในปี ค.ศ. ๒๐๒๕ ที่ผ่านมา ประชาชนในออสเตรเลียต้องสูญเสียเงินไปเกือบ ๓๓๕ ล้านดอลลาร์ หรือประมาณ ๗,๓๐๐ ล้านบาท จากกลโกงต่าง ๆ โดยการหลอกลวงด้านการลงทุนเป็นสาเหตุของการสูญเสียที่มากที่สุด ซึ่งหน่วยงาน Scamwatch ของคณะกรรมการการแข่งขันและคุ้มครองผู้บริโภคแห่งออสเตรเลีย (The Australian Competition and Consumer Commission: ACCC) ได้เผยแพร่ตัวเลขประจำเดือนธันวาคมซึ่งสะท้อนผลกระทบจากการหลอกลวงตลอดทั้งปี ค.ศ. ๒๐๒๕ และถึงแม้ว่าจำนวนข้อร้องเรียนจะลดลงจาก ๒๔๙,๔๔๘ รายการในปี ค.ศ. ๒๐๒๔ เหลือ ๒๐๐,๗๐๐ รายการในปี ค.ศ. ๒๐๒๕ แต่ความเสียหายที่มีการรายงานกลับเพิ่มขึ้นจาก ๓๑๘.๗ ล้านดอลลาร์เป็น ๓๓๔.๘ ล้านดอลลาร์ หรือเพิ่มขึ้น ๑๖.๑ ล้านดอลลาร์ โดยมีรายงานว่าอีเมลเป็นรูปแบบการติดต่อที่ได้รับความนิยมมากที่สุดในหมู่มีจมาชีพ โดยมีรายงานการหลอกลวงทางอีเมลมากกว่า ๘๔,๘๐๐ ครั้ง รองลงมาเป็นการหลอกลวงที่มาจากช่องทางออนไลน์อื่น ๆ รวมถึงโซเชียลมีเดีย โทรศัพท์มือถือ หรือพื้นที่ออนไลน์ประมาณ ๔๓,๐๐๐ ครั้ง โดยรายงานความเสียหายรวมทั้งสิ้น ๑๕๘.๕ ล้านดอลลาร์ และการหลอกลวงทางโทรศัพท์เป็นจำนวนเกือบ ๓๘,๐๐๐ ครั้ง^๒

* จัดทำโดยนางสาวภรภัทร ปัญญานิช บุคลากรจัดทำฐานข้อมูลกฎหมาย ฝ่ายค้นคว้าและเปรียบเทียบกฎหมาย กองกฎหมายต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

^๑ ศรัณย์รัฐ เนาวอุไรรัตน์, “การหลอกลวงทางไซเบอร์: กรณีแก๊งคอลเซ็นเตอร์,” (วิทยานิพนธ์ปริญญารัฐศาสตรมหาบัณฑิต สาขาวิชาการบริหารงานยุติธรรมและสังคม คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา, ๒๕๖๓)

^๒ Atitaya Teepawat. “สแกมเมอร์หลอกชาวออสเตรเลียสูญเงินถึง ๓๓๐ ล้านดอลลาร์ในปีได้อย่างไร”, สืบค้นเมื่อวันที่ ๑ มิถุนายน ๒๕๖๙, จาก<https://www.sbs.com.au/language/thai/th/article/how-over-330-million-was-taken-from-australians-in-a-year-and-the-tactics-behind-it/m9wc9a9co>



เว็บไซต์ Scamwatch ให้ข้อมูลล่าสุดเกี่ยวกับการหลอกลวงที่เกิดขึ้นในออสเตรเลียในปัจจุบัน
ข้อมูลจาก www.scamwatch.gov.au

รัฐสภาของออสเตรเลียจึงได้ผ่านกรอบกฎหมายการจัดการและป้องกันอาชญากรรมทางเทคโนโลยีหรือการหลอกลวงทางไซเบอร์ (Scams Prevention Framework: SPF) ขึ้นเพื่อรับมือกับการหลอกลวงในรูปแบบต่าง ๆ และคุ้มครองผู้บริโภคจากความเสียหายที่เกิดขึ้น โดยกรอบกฎหมาย SPF เป็นส่วนหนึ่งของกฎหมายคุ้มครองผู้บริโภค (Competition and Consumer Act 2010: Cth)

๒. สารสำคัญ

๒.๑ ประเด็นสำคัญของกรอบกฎหมาย SPF

(๑) หลักการสำคัญ ๖ ประการ ได้แก่ การกำกับดูแล การป้องกัน การตรวจจับ การรายงาน การขัดขวาง และการรับมือกับการหลอกลวง

(๒) ภาคส่วน ๓ ภาคส่วนที่สำคัญตามกรอบกฎหมาย SPF ได้แก่ ธนาคาร เครือข่ายโทรคมนาคม และแพลตฟอร์มดิจิทัล

(๓) หน่วยงานกำกับดูแลที่เกี่ยวข้อง ได้แก่

- คณะกรรมการการแข่งขันและคุ้มครองผู้บริโภค (Australian Competition and Consumer Commission: ACCC) ทำหน้าที่ในการกำกับดูแลแพลตฟอร์มดิจิทัล
- คณะกรรมการด้านหลักทรัพย์และการลงทุน (Australian Securities and Investments Commission: ASIC) ทำหน้าที่ในการกำกับดูแลธนาคาร และ
- หน่วยงานกิจการแพร่ภาพและกระจายเสียง (Australian Communications and Media Authority: ACMA) ทำหน้าที่ในการกำกับดูแลผู้ให้บริการเครือข่ายโทรคมนาคม

กรอบกฎหมาย SPF เป็นส่วนหนึ่งของกฎหมายคุ้มครองผู้บริโภค (Competition and Consumer Act) โดยมีกรอบกฎหมาย SPF และประมวลกฎหมายเฉพาะเป็นกฎหมายลำดับรอง โดยกฎหมายมิได้กำหนดมาตรการเกี่ยวกับการชดเชยเยียวยาแก่ผู้เสียหายจากการหลอกลวงทางไซเบอร์ แต่ใช้ช่องทางในการเยียวยาอื่น ๆ ได้ เช่น การระงับข้อพิพาทภายในองค์กรและการระงับข้อพิพาทภายนอก ซึ่งดำเนินการโดยหน่วยงานรับเรื่องร้องเรียนทางการเงินของออสเตรเลีย (Australian Financial Complaints Authority: AFCA) รวมถึงยังสามารถดำเนินคดีต่อศาลได้

สำหรับบทลงโทษทางแพ่งแบ่งเป็น ๒ ระดับ ได้แก่ ระดับที่ ๑ สำหรับการฝ่าฝืนหลักการด้านการป้องกัน การตรวจจับ การขัดขวาง หรือการรับมือต่อการหลอกลวง และระดับที่ ๒ สำหรับการฝ่าฝืนหลักการด้านการรายงาน การกักกักดูแล หรือข้อกำหนดเฉพาะของแต่ละภาคส่วน

ทั้งนี้ กฎหมายมีผลใช้บังคับเมื่อวันที่ ๒๑ กุมภาพันธ์ ค.ศ. ๒๐๒๕ ภายหลังจากได้รับพระบรมราชานุญาต (royal assent) อย่างไรก็ตาม หน่วยงานที่อยู่ภายใต้การกำกับจะยังไม่ต้องปฏิบัติตามกรอบกฎหมาย SPF จนกว่าภาคส่วนของตนจะได้รับแจ้งให้ปฏิบัติตามอย่างเป็นทางการ และอาจมีการกำหนดด้านระยะเวลาในการเปลี่ยนผ่านก่อนการบังคับใช้กฎหมายอย่างเต็มรูปแบบขึ้นอยู่กับข้อกำหนดของเฉพาะของแต่ละภาคส่วน และในขั้นตอนต่อไป รัฐบาลจะจัดทำกฎเกณฑ์และแนวปฏิบัติภายใต้กรอบกฎหมาย SPF สำหรับ ๓ ภาคส่วนดังกล่าวที่อยู่ในขอบเขตการบังคับใช้ โดยต้องเปิดรับฟังความคิดเห็นจากภาคอุตสาหกรรมที่เกี่ยวข้องก่อนดำเนินการ

๒.๒ การเตรียมความพร้อมของภาคส่วนต่าง ๆ เพื่อปฏิบัติตามกรอบกฎหมาย SPF

ภาคธุรกิจ ใน ๓ ภาคส่วนแรก ได้แก่ ธนาคาร เครือข่ายโทรคมนาคม และแพลตฟอร์มดิจิทัล รวมถึงภาคส่วนที่อาจถูกกำหนดเพิ่มเติมในอนาคต เช่น กองทุนบำนาญ ประกันภัย ตลาดซื้อขายสินค้าออนไลน์ และสินทรัพย์ดิจิทัล ควรเตรียมความพร้อมสำหรับการบังคับใช้กรอบกฎหมาย SPF โดยดำเนินการในประเด็นสำคัญ ดังต่อไปนี้

(๑) เข้าร่วมการรับฟังความคิดเห็นเกี่ยวกับการกำหนดภาคส่วนที่อยู่ภายใต้การกำกับ และการจัดทำข้อกำหนดภายใต้กรอบกฎหมาย SPF ซึ่งกำหนดหน้าที่ที่ต้องปฏิบัติตาม รวมถึงมาตรการควบคุมและระบบกำกับดูแลที่แต่ละหน่วยงานต้องจัดให้มี

(๒) จัดทำหรือพัฒนามาตรการป้องกันอาชญากรรมทางเทคโนโลยีหรือการหลอกลวงเพิ่มเติม เพื่อใช้ในการป้องกัน ตรวจจับ ขัดขวาง และรายงานการหลอกลวง รวมถึงพัฒนาระบบรวบรวมข้อมูลและข่าวกรองเกี่ยวกับการหลอกลวง

(๓) ปรับปรุงนโยบายความเป็นส่วนตัวและเอกสารแจ้งการเก็บรวบรวมข้อมูลส่วนบุคคล โดยเพิ่มวัตถุประสงค์เกี่ยวกับการป้องกัน ตรวจจับ และรับมือกับการหลอกลวง เพื่อให้สามารถนำไปใช้ได้ทันทีเมื่อมีการประกาศใช้ข้อกำหนดภายใต้กรอบกฎหมาย SPF

(๔) ทบทวนหรือปรับปรุงโครงสร้างการกำกับดูแล การกำหนดหน้าที่ความรับผิดชอบ มาตรการกำกับการปฏิบัติตามกฎหมาย และกระบวนการระงับข้อพิพาทภายในองค์กร เพื่อให้สามารถป้องกัน ตรวจจับ ขัดขวาง และรายงานการหลอกลวงได้อย่างมีประสิทธิภาพ รวมถึงรองรับการรับเรื่องร้องเรียนที่เกี่ยวข้องกับการหลอกลวง

(๕) ทบทวนและวิเคราะห์ข้อร้องเรียนที่เคยเกิดขึ้นและเกี่ยวข้องกับการดำเนินงานขององค์กรของตน ถ้าหากมี

๒.๓ สารสำคัญของกรอบกฎหมาย SPF

กรอบกฎหมาย SPF กำหนดให้ “การหลอกลวง” (Scam) หมายถึง การพยายามติดต่อหรือเข้าถึงผู้ให้บริการที่อยู่ภายใต้การคุ้มครองของกฎหมาย ไม่ว่าจะทางตรงหรือทางอ้อม และไม่ว่าการกระทำนั้นจะสำเร็จหรือไม่ก็ตาม โดยหากสามารถพิจารณาได้อย่างสมเหตุสมผลว่า (ก) การกระทำนั้นมีลักษณะเป็นการหลอกลวงหรือการใช้ข้อมูลอันเป็นเท็จ และ (ข) หากสำเร็จจะก่อให้เกิดความเสียหายแก่

ผู้เสียหาย เช่น การได้มาซึ่งข้อมูลส่วนบุคคล หรือการได้รับผลประโยชน์ทางการเงินหรือประโยชน์อื่นใดจากผู้เสียหายหรือบุคคลที่เกี่ยวข้อง ก็จะต้องเป็นการหลอกลวงตามกฎหมาย โดยการกำหนดนิยามดังกล่าวมีวัตถุประสงค์เพื่อให้ครอบคลุมรูปแบบการหลอกลวงที่หลากหลายของมิจฉาชีพที่อาจมีการเปลี่ยนแปลงและพัฒนาตามไปตามกาลเวลา

“ผู้ใช้บริการที่อยู่ภายใต้การคุ้มครองของกฎหมาย” (SPF Consumer) หมายถึง บุคคลธรรมดาและผู้ประกอบการธุรกิจขนาดเล็ก โดยกรอบกฎหมาย SPF มีผลบังคับใช้นอกอาณาเขต (extra-territorial reach) ต่อบุคคลธรรมดาที่มีถิ่นที่อยู่ตามปกติในออสเตรเลีย และต่อนิติบุคคลที่ให้บริการนอกออสเตรเลียซึ่งเป็นผู้มีถิ่นที่อยู่ในออสเตรเลียหรือมีสถานประกอบการถาวรเพื่อวัตถุประสงค์ด้านภาษีเงิน

ในระยะแรก กฎหมายจะบังคับใช้กับ ๓ ภาคส่วนหลัก ได้แก่ ธนาคาร เครือข่ายโทรคมนาคม และแพลตฟอร์มดิจิทัล ซึ่งครอบคลุมสื่อสังคมออนไลน์ การโฆษณาผ่านระบบค้นหา และบริการส่งข้อความโดยตรง ขณะที่ภาคส่วนอื่น ได้แก่ กองทุนบำนาญ ประกันภัย ตลาดซื้อขายสินค้าออนไลน์ และธุรกิจสินทรัพย์ดิจิทัลนั้น เป็นภาคส่วนที่อาจถูกกำหนดให้อยู่ภายใต้การบังคับใช้ของกฎหมายในอนาคต

กรอบกฎหมาย SPF ยึดหลักการสำคัญ ๖ ประการที่หน่วยงานที่ถูกกำกับดูแลต้องปฏิบัติตาม ดังต่อไปนี้

๑) การกำกับดูแล (Govern) หน่วยงานต้องจัดให้มีระบบการกำกับดูแล การติดตาม และการประเมินผลการดำเนินงานด้านการป้องกันการหลอกลวงที่ชัดเจนและมีเอกสารหลักฐานเป็นลายลักษณ์อักษร

๒) การป้องกัน (Prevent) หน่วยงานต้องดำเนินการที่เหมาะสมเพื่อป้องกันการหลอกลวง โดยไม่จำกัดเฉพาะการดำเนินการตามข้อมูลข่าวกรองเกี่ยวกับการหลอกลวงที่ได้รับมาเท่านั้น

๓) การตรวจจับ (Detect) หน่วยงานต้องดำเนินการที่เหมาะสมเพื่อตรวจจับการหลอกลวงโดยทันทีในขณะที่เกิดเหตุการณ์ดังกล่าวขึ้นหรือไม่นานหลังจากเกิดเหตุการณ์นั้น

๔) การรายงาน (Report) หน่วยงานต้องรายงานข้อมูลข่าวกรองเกี่ยวกับการหลอกลวงที่สามารถนำไปใช้ดำเนินงานได้ต่อคณะกรรมการการแข่งขันและคุ้มครองผู้บริโภค (Australian Competition and Consumer Commission: ACCC)

๕) การขัดขวาง (Disrupt) หน่วยงานต้องดำเนินการที่เหมาะสม อย่างทันทั่วถึง และได้สัดส่วนกับความเสียหาย เพื่อยับยั้งหรือขัดขวางการหลอกลวง รวมถึงป้องกันความเสียหายที่อาจเกิดขึ้นจากการหลอกลวงดังกล่าว

๖) การรับมือ (Respond) หน่วยงานต้องจัดให้มีกลไกสำหรับการแจ้งเหตุหรือรายงานการหลอกลวงที่ประชาชนสามารถเข้าถึงได้ง่าย รวมถึงมีกระบวนการภายในในการจัดการ ข้อร้องเรียน และระงับข้อพิพาทที่เกี่ยวข้องกับการหลอกลวง

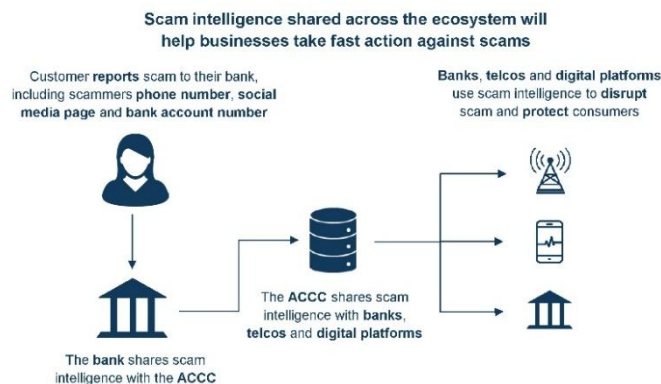
ในการพิจารณาว่าหน่วยงานได้ดำเนินการตามมาตรการที่เหมาะสมหรือไม่จะพิจารณาจากหลายปัจจัยประกอบกัน เช่น การปฏิบัติตามข้อกำหนดที่กำหนดไว้ในแนวปฏิบัติภายใต้กรอบกฎหมาย SPF ขนาดขององค์กร ลักษณะการให้บริการ กลุ่มผู้ใช้บริการ และระดับความเสี่ยงต่อการถูกหลอกลวงของหน่วยงานนั้น ๆ

นอกจากนี้ กฎหมายยังกำหนดความคุ้มครองตามกฎหมาย (Safe Harbour) สำหรับหน่วยงานที่อยู่ภายใต้การกำกับดูแล โดยหากหน่วยงานดำเนินมาตรการเพื่อขัดขวางหรือยับยั้งการหลอกลวง หน่วยงานดังกล่าวจะได้รับความคุ้มครองจากความรับผิดในคดีแพ่งเป็นระยะเวลาไม่เกิน ๒๘ วัน นับจากวันที่ได้รับข่าวกรองซึ่งหน่วยงานสามารถนำไปใช้ดำเนินการมาตรการป้องกันได้ ทั้งนี้ หน่วยงานจะต้องดำเนินการโดยสุจริต ปฏิบัติตามข้อกำหนดของกรอบกฎหมาย SPF และใช้มาตรการที่มีความเหมาะสม ได้สัดส่วนกับความเสี่ยง และสามารถยกเลิกหรือแก้ไขผลกระทบที่เกิดขึ้นได้ในภายหลัง

๒.๔ บทบาทของหน่วยงานกำกับดูแลภายใต้กรอบกฎหมาย SPF

คณะกรรมการการแข่งขันและคุ้มครองผู้บริโภค (ACCC) จะทำหน้าที่เป็นหน่วยงานหลักในการกำกับดูแล ในขณะที่แต่ละภาคส่วนจะมีหน่วยงานกำกับดูแลเฉพาะของตน ได้แก่ (๑) คณะกรรมการด้านหลักทรัพย์และการลงทุน (ASIC) สำหรับธนาคาร (๒) หน่วยงานกิจการแพร่ภาพและกระจายเสียง (ACMA) สำหรับผู้ให้บริการโทรคมนาคม และ (๓) คณะกรรมการการแข่งขันและคุ้มครองผู้บริโภค (ACCC) สำหรับแพลตฟอร์มดิจิทัล และหากมีการกำหนดภาคส่วนใหม่เพิ่มเติมในอนาคต คณะกรรมการการแข่งขันและคุ้มครองผู้บริโภค (ACCC) จะทำหน้าที่เป็นหน่วยงานกำกับดูแลชั่วคราวจนกว่าจะมีการแต่งตั้งหน่วยงานกำกับดูแลเฉพาะสำหรับภาคส่วนนั้น นอกจากนี้ หน่วยงานกำกับดูแลในแต่ละภาคส่วนจะต้องจัดทำแนวทางความร่วมมือระหว่างกันเพื่อบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการกำกับดูแล เช่น ความไม่ชัดเจนเกี่ยวกับบทบาทและหน้าที่รับผิดชอบ การตีความหรือการบังคับใช้กฎหมายที่ไม่สอดคล้องกัน ตลอดจนการดำเนินการกำกับดูแลหรือการบังคับใช้กฎหมายที่ซ้ำซ้อนกัน

หน่วยงานกำกับดูแลสามารถแลกเปลี่ยนข้อมูลเพื่อสนับสนุนการบริหารหรือการบังคับใช้ SPF ได้ (โดยไม่ต้องแจ้งบุคคลที่ได้รับผลกระทบ) ทั้งนี้ หน่วยงานกำกับดูแลมีอำนาจแลกเปลี่ยนข้อมูลระหว่างกันเพื่อสนับสนุนการบริหารและการบังคับใช้กรอบกฎหมาย SPF โดยไม่จำเป็นต้องแจ้งให้บุคคลที่เกี่ยวข้องทราบล่วงหน้า นอกจากนี้ กระบวนการคล่องตัวให้หน่วยงานที่ถูกกำกับดูแลสามารถแบ่งปันข้อมูลกับคณะกรรมการการแข่งขันและคุ้มครองผู้บริโภค (ACCC) ได้ ซึ่ง ACCC สามารถแบ่งปันต่อกับหน่วยงานที่ถูกกำกับดูแลอื่น ๆ ได้เช่นกัน



แผนภาพการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

ข้อมูลจาก <https://www.corrs.com.au/insights/the-new-scams-prevention-framework-key-considerations-for-regulated-entities>

๒.๕ บทลงโทษทางแพ่ง

บทลงโทษทางแพ่งตามกรอบกฎหมาย SPF ถูกกำหนดเป็น ๒ ระดับ โดยพิจารณาจากลักษณะและความร้ายแรงของการฝ่าฝืน เนื่องจากการฝ่าฝืนหลักการบางประการอาจก่อให้เกิดความเสียหายต่อผู้บริโภคโดยตรงและในระดับที่สูงกว่า ในขณะที่การฝ่าฝืนบางประการเกี่ยวข้องกับระบบการดำเนินงาน กระบวนการภายในองค์กร หรือการกำกับดูแลเป็นหลัก จึงมีการกำหนดระดับบทลงโทษที่แตกต่างกันให้เหมาะสมกับผลกระทบที่อาจเกิดขึ้นจากการกระทำนั้น

การฝ่าฝืน	บทลงโทษ
ระดับที่ ๑ การฝ่าฝืนหลักการด้านการป้องกัน การตรวจจับ การขัดขวาง หรือการ รับมือกับการหลอกลวง	สำหรับนิติบุคคล ศาลสามารถกำหนดโทษปรับทางแพ่งในอัตรา สูงสุด ดังต่อไปนี้ • ๕๒.๗ ล้านดอลล่าร์ออสเตรเลีย หรือ • ๓ เท่าของมูลค่ารวมของประโยชน์ที่ได้รับจากการฝ่าฝืน หรือ • ในกรณีที่ศาลไม่สามารถกำหนดมูลค่าของประโยชน์ประโยชน์ที่ได้รับจากการฝ่าฝืนดังกล่าวได้ ให้ปรับเป็นจำนวนร้อยละ ๓๐ ของรายได้รวมที่ปรับปรุงแล้ว (adjusted turnover) ของนิติบุคคลในช่วงเวลาที่มีการฝ่าฝืน สำหรับบุคคลธรรมดา ศาลสามารถกำหนดโทษปรับทางแพ่งในอัตรา สูงสุด ๒,๖๓๖,๗๐๐ ดอลล่าร์ออสเตรเลีย
ระดับที่ ๒ สำหรับการฝ่าฝืนหลักการกำกับ ดูแล การรายงาน รวมถึงข้อกำหนด ตามกรอบกฎหมาย SPF	สำหรับนิติบุคคล ศาลสามารถกำหนดโทษปรับทางแพ่งในอัตรา สูงสุด ดังต่อไปนี้ • ๑๐.๕ ล้านดอลล่าร์ออสเตรเลีย หรือ • ๓ เท่าของมูลค่ารวมของประโยชน์ที่ได้รับจากการฝ่าฝืน หรือ • ในกรณีที่ศาลไม่สามารถกำหนดมูลค่าของประโยชน์ประโยชน์ที่ได้รับจากการฝ่าฝืนดังกล่าวได้ ให้ปรับเป็นจำนวนร้อยละ ๑๐ ของรายได้รวมที่ปรับปรุงแล้ว (adjusted turnover) ของนิติบุคคลในช่วงเวลาที่มีการฝ่าฝืน สำหรับบุคคลธรรมดา ศาลสามารถกำหนดโทษปรับทางแพ่งในอัตรา สูงสุด ๕๒๘,๐๐๐ ดอลล่าร์ออสเตรเลีย

หน่วยงานกำกับดูแลสามารถขอให้ศาลมีคำสั่งหรือกำหนดมาตรการทางกฎหมายหลายประการสำหรับการฝ่าฝืนครั้งเดียวของหน่วยงานที่ถูกกำกับดูแล แต่ไม่สามารถกำหนดโทษปรับทางแพ่งหลายบทซ้ำซ้อนกันสำหรับการฝ่าฝืนเดียวกัน ทั้งนี้ มาตรการเยียวยาอื่น ๆ ที่อาจนำมาใช้ ได้แก่ คำสั่งห้ามกระทำการหรือคำสั่งคุ้มครองชั่วคราว (injunctions) ข้อตกลงที่มีผลผูกพันตามกฎหมาย (enforceable undertakings) และการดำเนินคดีเรียกค่าเสียหายตามกฎหมาย

๒.๖ การเยียวยาผู้เสียหาย

กรอบกฎหมาย SPF ไม่ได้กำหนดให้หน่วยงานที่อยู่ภายใต้การกำกับต้องชดเชยความเสียหายแก่ผู้เสียหายจากการหลอกลวงโดยบังคับ แต่กำหนดให้หน่วยงานที่ถูกกำกับดูแลต้องจัดให้มีกลไกการเยียวยาให้ผู้บริโภค โดยครอบคลุมถึงกระบวนการระงับข้อพิพาทภายในองค์กร (Internal Dispute Resolution: IDR) และกระบวนการระงับข้อพิพาทภายนอกองค์กร (External Dispute Resolution: EDR) รวมถึงผู้เสียหายยังสามารถใช้สิทธิฟ้องร้องต่อศาลได้

เจตนารมณ์ของกฎหมายคือ การดำเนินการรับเรื่องร้องเรียนภายในองค์กรโดยยึดหลัก “No Wrong Door” กล่าวคือ ผู้เสียหายสามารถยื่นเรื่องร้องเรียนต่อหน่วยงานใดก็ได้ที่เกี่ยวข้องกับการหลอกลวงดังกล่าว และหน่วยงานนั้นจะต้องร่วมมือกับหน่วยงานอื่นที่เกี่ยวข้องเพื่อแก้ไขข้อร้องเรียนด้วยความสุจริต และหากหน่วยงานไม่สามารถแก้ไขข้อร้องเรียนได้ ผู้เสียหายสามารถส่งเรื่องเข้าสู่กระบวนการระงับข้อพิพาทภายนอกองค์กรผ่านหน่วยงานรับเรื่องร้องเรียนทางการเงินของออสเตรเลีย (Australian Financial Complaints Authority: AFCA) ได้

หน่วยงานที่อยู่ภายใต้การกำกับดูแลจะต้องจัดทำหนังสือรับรองการปฏิบัติตามกฎหมาย (Statement of Compliance) ให้แก่ผู้ใช้บริการในระหว่างกระบวนการระงับข้อพิพาทภายในองค์กร โดยเอกสารดังกล่าวสามารถนำไปใช้เป็นพยานหลักฐานในกระบวนการระงับข้อพิพาทภายนอกและการดำเนินคดีในศาลได้ อย่างไรก็ตาม หากมีการให้ข้อมูลเท็จหรือข้อมูลที่เข้าใจผิด ประเด็นดังกล่าวอาจถูกส่งต่อให้คณะกรรมการการแข่งขันและคุ้มครองผู้บริโภค (ACCC) ดำเนินการสืบสวน หากหน่วยงานระบุในหนังสือรับรองว่าตนไม่ได้ปฏิบัติตามข้อกำหนดตามกรอบกฎหมาย SPF หน่วยงานนั้นอาจต้องชดเชยค่าเสียหายแก่ผู้บริโภคสำหรับความสูญเสียที่เกิดจากการหลอกลวง หรือต้องแสดงเหตุผลประกอบหากจะไม่ชดเชยค่าเสียหายดังกล่าวให้

๒.๗ ประเด็นที่กรอบกฎหมาย SPF ไม่ได้ครอบคลุม

๒.๗.๑ การแบ่งสัดส่วนความรับผิดชอบระหว่างหน่วยงานที่เกี่ยวข้อง

กรอบกฎหมาย SPF กำหนดหลักเกณฑ์เกี่ยวกับ “ผู้ร่วมกระทำความผิด” (concurrent wrongdoer) ซึ่งกำหนดให้ศาลแบ่งสัดส่วนความรับผิดชอบระหว่างหน่วยงานที่มีส่วนเกี่ยวข้องกับความเสียหายจากการหลอกลวงแต่ละรายอย่างเป็นธรรม อย่างไรก็ตาม กรอบกฎหมาย SPF ไม่ได้กำหนดวิธีการแบ่งสัดส่วนความรับผิดชอบในชั้นการระงับข้อพิพาทภายในองค์กร (Internal Dispute Resolution: IDR) และการระงับข้อพิพาทภายนอกองค์กร (External Dispute Resolution: EDR) ทั้งนี้ ระหว่างการพิจารณาร่างกฎหมายในวุฒิสภาได้มีการเพิ่มเติมบทบัญญัติเพื่อยืนยันว่า แนวทางการแบ่งสัดส่วนความรับผิดชอบที่ใช้ในกระบวนการระงับข้อพิพาทภายในองค์กร ไม่จำเป็นต้องสอดคล้องกับหลักความรับผิดชอบตามสัดส่วน (proportionate liability) ที่ศาลใช้ในการพิจารณาคดีเรียกค่าเสียหายแต่อย่างใด

๒.๗.๒ การฟ้องคดีแบบกลุ่ม

ปัจจุบันยังไม่มีมติความชัดเจนว่ามาตรา 137H แห่งกฎหมายคุ้มครองผู้บริโภค (Competition and Consumer Act) ที่กำหนดให้ผลการวินิจฉัยและการรับสารภาพในกระบวนการพิจารณาคดีใด ๆ ภายใต้กฎหมายคุ้มครองผู้บริโภคของออสเตรเลียถือเป็นพยานหลักฐานเบื้องต้นในกระบวนการพิจารณาประเภทอื่นภายใต้กฎหมายดังกล่าวจะมีผลบังคับใช้กับกรอบกฎหมาย SPF หรือไม่ แต่อย่างไรก็ตาม มีความเป็นไปได้

ที่จะเกิดความเสียหายจากการฟ้องคดีแบบกลุ่มในลักษณะคดีต่อเนื่อง (follow-on class action) กล่าวคือ ผู้เสียหายอาจอาศัยผลการบังคับใช้กฎหมายของหน่วยงานกำกับดูแลมาเป็นฐานในการดำเนินคดีเรียกร้องสิทธิของตนเองต่อไป หรืออาจมีการฟ้องคดีแบบกลุ่มโดยไม่ต้องอาศัยการดำเนินการของหน่วยงานกำกับดูแล หากการหลอกลวงดังกล่าวส่งผลกระทบต่อผู้เสียหายเป็นวงกว้างมากเพียงพอที่จะจูงใจให้สำนักงานกฎหมายหรือผู้สนับสนุนเงินทุนในการดำเนินคดีเข้ามาดำเนินการฟ้องคดีแทนกลุ่มผู้เสียหาย

๒.๘ ความเชื่อมโยงกับกฎหมายป้องกันการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินในการก่อการร้าย

ปัจจุบัน กรอบกฎหมาย SPF ยังไม่ได้กำหนดความสัมพันธ์หรือแนวทางการบังคับใช้ร่วมกับพระราชบัญญัติป้องกันการฟอกเงินและต่อต้านการสนับสนุนทางการเงินในการก่อการร้าย ค.ศ. ๒๐๐๖ (Anti-Money Laundering and Counter-Terrorism Financing Act 2006: Cth) ไว้โดยชัดเจน โดยเฉพาะในประเด็นเกี่ยวกับการส่งเสริมความร่วมมือในการป้องกันการหลอกลวงระหว่างหน่วยงานต่าง ๆ และการลดภาระการปฏิบัติตามกฎหมายที่อาจซ้ำซ้อน เช่น การรายงานข้อมูลชุดเดียวกันต่อหลายหน่วยงาน

อย่างไรก็ตาม เมื่อไม่นานมานี้ได้มีการแก้ไขกฎหมายป้องกันและปราบปรามการฟอกเงิน (Anti-Money Laundering) และการต่อต้านการสนับสนุนทางการเงินในการก่อการร้าย (Counter-Terrorist Financing) หรือกฎหมาย AML/CTF ที่จะอนุญาตให้ธนาคารแลกเปลี่ยนข้อมูลระหว่างกันได้ แต่กฎเกณฑ์ดังกล่าวยังไม่ได้ประกาศให้มีผลใช้บังคับ อีกทั้งยังไม่ครอบคลุมถึงการแลกเปลี่ยนข้อมูลเกี่ยวกับการหลอกลวงระหว่างธนาคารกับผู้ให้บริการเครือข่ายโทรคมนาคมหรือแพลตฟอร์มเทคโนโลยีดิจิทัล

ดังนั้น トラบเท่าที่หน่วยงานวิเคราะห์และรายงานธุรกรรมทางการเงินของออสเตรเลีย (Australian Transaction Reports and Analysis Centre: AUSTRAC) ยังไม่ได้ออกแนวทางเพิ่มเติม ธนาคารต่าง ๆ ต้องพิจารณาด้วยตนเองว่าข้อมูลใดสามารถเปิดเผยหรือแลกเปลี่ยนกับหน่วยงานอื่นได้ และการเปิดเผยข้อมูลดังกล่าวจะส่งผลกระทบหรือเป็นอุปสรรคต่อการสืบสวนหรือการดำเนินการภายใต้กฎหมาย AML/CTF ฉบับใหม่หรือไม่ อย่างไร

๒.๙ ความเชื่อมโยงกับกฎหมายว่าด้วยความเป็นส่วนตัว

การที่กรอบกฎหมาย SPF กำหนดให้การได้มาซึ่งข้อมูลส่วนบุคคลโดยมิชอบเป็นส่วนหนึ่งของนิยามคำว่า “การหลอกลวง” ทำให้มีความทับซ้อนกับกฎหมายว่าด้วยความเป็นส่วนตัว (Privacy Act 1988) และกฎหมายอื่น ๆ ของรัฐที่มีเนื้อหาในลักษณะเดียวกัน ซึ่งกฎหมายดังกล่าวกำหนดหน้าที่เกี่ยวกับการจัดการข้อมูลส่วนบุคคล อย่างไรก็ตาม กรอบกฎหมาย SPF ยังไม่ได้กำหนดแนวทางที่ชัดเจนเกี่ยวกับความสัมพันธ์ระหว่างกฎหมายทั้งสองฉบับ

คำชี้แจงประกอบร่างกฎหมายฉบับปรับปรุง (Revised Explanatory Memorandum) ในส่วนความสอดคล้องกับหลักสิทธิมนุษยชนได้กล่าวถึงประเด็นดังกล่าวและเห็นว่า การดำเนินการตามกรอบกฎหมาย SPF ไม่น่าจะก่อให้เกิดปัญหาด้านความเป็นส่วนตัว เนื่องจากหน่วยงานที่มีหน้าที่รับและเปิดเผยข้อมูลส่วนบุคคลภายใต้กรอบกฎหมาย SPF โดยทั่วไปจะอยู่ภายใต้ข้อกำหนดของกฎหมายความเป็นส่วนตัวอยู่แล้ว อย่างไรก็ตาม เพื่อให้การดำเนินงานยังคงสอดคล้องกับกฎหมายด้านความเป็นส่วนตัว ภาครัฐจึงควรทบทวนและปรับปรุงนโยบายความเป็นส่วนตัว รวมถึงเอกสารแจ้งการเก็บรวบรวมข้อมูล

ส่วนบุคคลของตนและการเปิดเผยข้อมูลส่วนบุคคลของลูกค้าแก่บุคคลที่สาม เพื่อป้องกันการขัดขวางและการรับมือกับการหลอกลวง

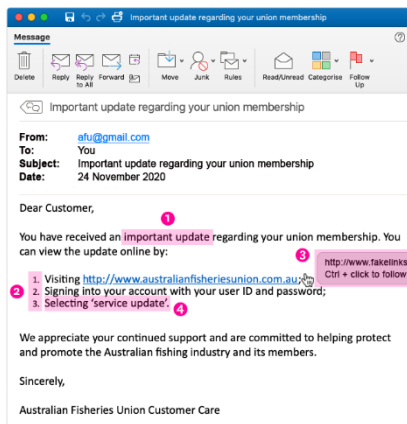
๒.๑๐ ระเบียบแนวปฏิบัติเฉพาะสำหรับแต่ละภาคส่วนภายใต้กรอบกฎหมาย SPF

กฎหมาย SPF ปัจจุบันกำหนดเพียงกรอบการดำเนินงานในภาพรวมเท่านั้น โดยรายละเอียดเกี่ยวกับการปฏิบัติและหน้าที่เฉพาะของหน่วยงานที่อยู่ภายใต้การกำกับจะถูกกำหนดเพิ่มเติมในกฎหมายลำดับรอง ซึ่งประกอบด้วยกฎเกณฑ์ภายใต้กรอบกฎหมาย SPF และระเบียบแนวปฏิบัติเฉพาะสำหรับแต่ละภาคส่วน

สำหรับ ๓ ภาคส่วนแรก ได้แก่ ธนาคาร เครือข่ายโทรคมนาคม และแพลตฟอร์มดิจิทัล รัฐบาลออสเตรเลียมีแผนจัดทำระเบียบแนวปฏิบัติเฉพาะภาคส่วนผ่านกระบวนการรับฟังความคิดเห็นจากภาคธุรกิจและผู้บริโภคภายในปี ค.ศ. ๒๐๒๕ ซึ่งมีสาระสำคัญดังต่อไปนี้

- ธนาคาร ต้องนำเทคโนโลยีมาใช้เพื่อเพิ่มความมั่นใจให้แก่ลูกค้าว่าเงินจะถูกโอนไปยังผู้รับที่ลูกค้าตั้งใจจะโอนเงินไป
- แพลตฟอร์มดิจิทัล ต้องตรวจสอบว่าผู้ลงโฆษณาผลิตภัณฑ์ทางการเงินทุกรายได้รับใบอนุญาตให้บริการทางการเงินของออสเตรเลีย (Australian Financial Services Licence) โดยถูกต้อง
- โทรคมนาคม ต้องจัดให้มีระบบกรองและปิดกั้นข้อความ SMS ที่มีลิงก์ฟิชซิง (phishing)^๓ ซึ่งเคยถูกระบุว่าใช้ในการหลอกลวง

ตัวอย่างการหลอกลวงทางอีเมลที่มีลิงก์ฟิชซิง



ข้อมูลจาก <https://ovic.vic.gov.au/privacy/resources-for-organisations/phishing-attacks-and-how-to-protect-against-them/>

^๓ ฟิชซิง (phishing) เป็นหนึ่งในการหลอกลวงทางโลกออนไลน์ที่พบได้บ่อยที่สุด ฟิชซิงมีหลายรูปแบบ การหลอกลวงประเภทนี้มักจะเกี่ยวข้องกับการใช้กลยุทธ์หลอกล่อผู้ใช้งาน และการแอบอ้างเป็นเว็บไซต์ที่น่าเชื่อถือ เช่น เว็บไซต์ธนาคาร หรือบัญชีโซเชียลมีเดีย ซึ่งมักจะแตกต่างจากของจริง มีการเปลี่ยนชื่อในลิงก์เพียงเล็กน้อยทำให้เราไม่สังเกต บ่อยครั้งที่แฮกเกอร์ส่งอีเมลเพื่อขอให้คุณล็อกอินเข้าสู่ระบบธนาคาร หรือหน้าบัญชีอื่น ๆ เพื่อตรวจสอบหรือยืนยันข้อมูลของคุณ พร้อมกับลิงก์ไปยังเพจปลอม, สืบค้นเมื่อวันที่ ๑๖ มีนาคม ๒๕๖๙, จาก https://www.bitdefender.co.th/post/phishing/?srsltid=AfmBOoodx-8ZZWpNDZ2LJOltOrUXjwYvTclNykJD_Uk8ilM7w6-IJzhG

๒.๑๑ ระยะเวลาเปลี่ยนผ่าน

กรอบกฎหมาย SPF มีผลใช้บังคับเมื่อวันที่ ๒๑ กุมภาพันธ์ ค.ศ. ๒๐๒๕ หลังจากได้รับพระบรมราชานุญาต (royal assent) อย่างไรก็ตาม หน่วยงานที่อยู่ภายใต้การกำกับดูแลยังไม่มีหน้าที่ต้องปฏิบัติตามกรอบกฎหมายดังกล่าวจนกว่าจะได้รับการกำหนดระยะเวลาเปลี่ยนผ่านจากรัฐมนตรี (เช่น การเลื่อนการมีผลบังคับใช้จนกว่าจะมีระเบียบแนวปฏิบัติเฉพาะสำหรับแต่ละภาคส่วน) ซึ่งหมายความว่าหน่วยงานที่อยู่ภายใต้การกำกับดูแลต้องเตรียมความพร้อมและปฏิบัติตามกรอบกฎหมาย SPF ภายในระยะเวลาจำกัดโดยมีเวลาไม่มากนักในการปรับปรุงระบบงาน นโยบาย และกระบวนการภายในองค์กรให้สอดคล้องกับข้อกำหนดใหม่ ตัวอย่างเช่น หน่วยงานต้องพัฒนาระบบและกระบวนการรายงานการหลอกลวงไว้ล่วงหน้า เพื่อให้สามารถรายงานต่อคณะกรรมการการแข่งขันและคุ้มครองผู้บริโภค (ACCC) ได้ภายใน ๒๔ ชั่วโมงนับแต่ทราบเรื่อง

นอกจากนี้ หน่วยงานที่อยู่ภายใต้การกำกับดูแลยังต้องได้รับการรับรองการปฏิบัติตามกรอบกฎหมาย SPF จากเจ้าหน้าที่ระดับสูงขององค์กร (Senior Officer) ภายในระยะเวลา ๑๒ เดือน นับจากวันที่หน่วยงานนั้นเข้าสู่การกำกับดูแล และหลังจากนั้นจะต้องได้รับการรับรองดังกล่าวเป็นประจำทุกปีภายใน ๗ วันนับจากวันครบรอบของระยะเวลาดังกล่าว^๔

๓. บทสรุป

ที่ผ่านมาออสเตรเลียประสบปัญหาการหลอกลวงทางไซเบอร์และอาชญากรรมทางเทคโนโลยีที่สร้างความเสียหายแก่ประชาชนและภาคธุรกิจเป็นจำนวนมาก ส่งผลให้รัฐบาลออสเตรเลียต้องพัฒนากรอบกฎหมายการจัดการและป้องกันอาชญากรรมทางเทคโนโลยีหรือการหลอกลวงทางไซเบอร์ (Scams Prevention Framework: SPF) ขึ้น เพื่อกำหนดหน้าที่และความรับผิดชอบของภาคส่วนต่าง ๆ ที่มีบทบาทสำคัญในการให้บริการทางดิจิทัล ได้แก่ ธนาคาร ผู้ให้บริการเครือข่ายโทรคมนาคม และแพลตฟอร์มดิจิทัล ให้มีมาตรการในการป้องกัน ตรวจสอบ ชัดขวาง รายงาน และรับมือกับการหลอกลวงอย่างเป็นระบบ ภายใต้การกำกับดูแลของหน่วยงานของรัฐ อันจะช่วยยกระดับมาตรฐานการป้องกันการหลอกลวงทางไซเบอร์ สร้างกลไกความรับผิดชอบร่วมกันระหว่างภาครัฐและภาคเอกชน เพิ่มประสิทธิภาพในการคุ้มครองผู้บริโภค ลดความเสียหายจากอาชญากรรมทางเทคโนโลยี และเสริมสร้างความเชื่อมั่นของประชาชนต่อระบบเศรษฐกิจและบริการดิจิทัลในระยะยาว

^๔ Eugenia Kolivos, Lucinda Hill, Caroline Marshall, Rebecca LeBherz, Ciara Lavender. “The new Scams Prevention Framework: key considerations for regulated entities”, สืบค้นเมื่อวันที่ ๑๗ มีนาคม ๒๕๖๙, จาก <https://www.corrs.com.au/insights/the-new-scams-prevention-framework-key-considerations-for-regulated-entities>

จีน*

๑. สภาพปัญหาสู่สถานการณ์ปัจจุบัน^๑

ปัญหาการฉ้อโกงทางโทรคมนาคมและออนไลน์เริ่มปรากฏให้เห็นในสาธารณรัฐประชาชนจีนนับตั้งแต่ทศวรรษ ๑๙๙๐ ก่อนจะขยายตัวเป็นวงกว้างและส่งผลกระทบต่อความปลอดภัยในทรัพย์สินของประชาชน ผู้นำระดับสูงของจีนตระหนักถึงความสำคัญเร่งด่วนของปัญหานี้ โดยกำหนดให้ยึดหลักการ “ประชาชนเป็นศูนย์กลาง” พร้อมวางยุทธศาสตร์ที่เน้นการกำกับดูแลจากต้นทางและการบริหารจัดการแบบบูรณาการ (comprehensive governance) กล่าวคือ การปฏิบัติการร่วมกัน การป้องกัน และการกำกับดูแลที่ประชาชนมีส่วนร่วมเพื่อยับยั้งแนวโน้มการเกิดอาชญากรรมดังกล่าว นโยบายของรัฐบาลจีนจึงดำเนินไปบนแนวทางดังกล่าวควบคู่ไปกับการสร้างสรรค์นวัตกรรมใหม่โดยอาศัยการวิเคราะห์ปัญหา (problem orientation) และการคิดเชิงระบบ (systemic thinking) ความพยายามอย่างจริงจังในระดับที่ไม่เคยปรากฏมาก่อนนี้นำไปสู่ความสำเร็จเชิงประวัติศาสตร์อย่างเป็นรูปธรรม กล่าวคือ ในปี ค.ศ. ๒๐๒๑ สถิติการคลี่คลายคดีฉ้อโกงทางโทรคมนาคมและออนไลน์เพิ่มสูงขึ้นกว่า ๕ เท่าเมื่อเทียบกับช่วงห้าปีก่อนหน้า อีกทั้งอัตราการเกิดคดีดังกล่าวในจีนได้ลดลงอย่างต่อเนื่องเมื่อเปรียบเทียบกับช่วงเวลาเดียวกันของปีก่อนหน้า โดยตัวเลขคดีลดลงติดต่อกันถึง ๑๗ เดือน (year on year for 17 consecutive months) ตั้งแต่เดือนมิถุนายน ค.ศ. ๒๐๒๑ เป็นต้นมา ซึ่งสะท้อนให้เห็นถึงประสิทธิภาพของมาตรการควบคุมและปราบปรามที่บังคับใช้ และท่ามกลางสถานการณ์ปัจจุบันที่อาชญากรรมทางเทคโนโลยีได้ทวีความรุนแรงไปทั่วทุกภูมิภาคจนกลายเป็นภัยคุกคามระดับโลก ประเทศจีนได้พัฒนาแนวทางแก้ไขปัญหาในแบบฉบับของตนเองหรือที่เรียกว่า “Chinese solution” ซึ่งมีพื้นฐานจากประสบการณ์การแก้ไขปัญหาก็ประสบความสำเร็จภายในประเทศ เพื่อนำมาเป็นต้นแบบในการรับมือกับปัญหาระดับโลกนี้ โดยมีหลักการสำคัญ ได้แก่ การยึดประชาชนเป็นศูนย์กลาง การเสริมสร้างความเข้มแข็งอย่างรอบด้านผ่านการพัฒนางานวิจัยเฉพาะด้าน การจัดตั้งทีมเฉพาะกิจ การดำเนินการแก้ไขคดีเฉพาะ การพัฒนาบุคลากรผู้เชี่ยวชาญ ตลอดจนการบูรณาการภายในและการประสานความร่วมมือกับภายนอก

ในการตอบสนองต่อสถานการณ์ข้างต้น จีนได้ดำเนินมาตรการสำคัญหลายประการดังต่อไปนี้

๑. การสร้างงานวิจัยเฉพาะด้านเพื่อพัฒนาระบบกฎหมายอย่างต่อเนื่อง

อาชญากรรมทางโทรคมนาคมและการฉ้อโกงออนไลน์ถือเป็นปัญหาด้านการบริหารจัดการสังคมที่มีความซับซ้อน (social governance problem) การวิจัยเฉพาะด้านที่มีความหลากหลาย

* จัดทำโดยนางสาวนัฐกานต์ ขำยัง นักกฎหมายกฤษฎีกาชำนาญการพิเศษ ฝ่ายวิเคราะห์และคดีปกครองกองกฎหมายปกครอง สำนักงานคณะกรรมการกฤษฎีกา

^๑ Embassy of the People’s Republic of China in the Democratic Socialist Republic of Sri Lanka, “Successful Anti-Fraud Practice in China”, 2024-10-14, สืบค้นเมื่อ ๑๗ มีนาคม ๒๕๖๙, จาก https://lk.china-embassy.gov.cn/eng/zytz/202410/t20241014_11507299.htm

และครอบคลุมการดำเนินการในทุกระดับจึงเป็นมาตรการพื้นฐานที่จำเป็นต่อการวางแผนและเป็นปัจจัยสำคัญแห่งความสำเร็จ สรุปได้ดังนี้

๑.๑ การจัดทำเอกสารเชิงนโยบาย โดยอาศัยการวิจัยเฉพาะด้าน รัฐบาลจีนได้จัดทำและประกาศเอกสารเชิงนโยบายที่เป็นบรรทัดฐานหลายฉบับ^๒ เช่น ความเห็นเกี่ยวกับการสร้างความเข้มแข็งในการปราบปรามและควบคุมอาชญากรรมทางโทรคมนาคมและการฉ้อโกงออนไลน์ ประกาศว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางโทรคมนาคมและการฉ้อโกงออนไลน์ ข้อกำหนดเรื่องการเสริมสร้างการบริหารจัดการการเงินและการหักบัญชีและการป้องกันกิจกรรมผิดกฎหมายและอาชญากรรมรูปแบบใหม่ทางโทรคมนาคมและออนไลน์ แผนการดำเนินงานเพื่อส่งเสริมการสร้างกลไกระยะยาวในการป้องกันและควบคุมอาชญากรรมทางโทรคมนาคมและการฉ้อโกงออนไลน์โดยใช้ฐานข้อมูลขนาดใหญ่และบทบัญญัติบางประการว่าด้วยการคืนเงินที่ถูกอายัดในคดีที่เกี่ยวข้องกับการละเมิดกฎหมายและอาชญากรรมรูปแบบใหม่ทางเครือข่ายโทรคมนาคม

๑.๒ การจัดทำความเห็นเชิงกฎหมาย เพื่อปราบปรามอาชญากรรมทางโทรคมนาคมและการฉ้อโกงออนไลน์ ศาลประชาชนสูงสุด (the Supreme People's Court) สำนักงานอัยการสูงสุด (the Supreme People's Procuratorate) และกระทรวงความมั่นคงสาธารณะ (the Ministry of Public Security) ได้ร่วมกันออกความเห็น (ฉบับที่ ๑) และ (ฉบับที่ ๒) ในประเด็นต่าง ๆ ที่เกี่ยวข้องกับการใช้กฎหมายในการดำเนินคดีอาญาเกี่ยวกับการฉ้อโกงทางโทรคมนาคมและออนไลน์ นอกจากนี้ได้มีการประกาศใช้บังคับกฎหมายว่าด้วยการปราบปรามอาชญากรรมทางโทรคมนาคมและการฉ้อโกงออนไลน์ (Law on Combating Telecom and Online Fraud) อย่างเป็นทางการในเดือนกันยายน ค.ศ. ๒๐๒๒ เพื่อเป็นหลักประกันทางกฎหมายที่เข้มแข็งต่อการดำเนินการในเรื่องนี้

๑.๓ การวิจัยรูปแบบอาชญากรรมและมาตรการจัดการ รัฐบาลจีนได้จัดให้มีระบบการวิจัยที่หลากหลายครอบคลุมมิติที่สำคัญ เช่น ความมั่นคงสาธารณะ (public security) การสื่อสารการเงิน อินเทอร์เน็ต โดยมีสถาบันการศึกษา สถาบันวิจัย และสมาคมต่าง ๆ เข้ามามีส่วนร่วมเพื่อเฝ้าติดตามการเปลี่ยนแปลงของวิธีการก่ออาชญากรรมและกำหนดมาตรการปราบปรามที่เหมาะสม การเฝ้าติดตามการเปลี่ยนแปลงของกลุ่มอาชญากรและการเสริมสร้างการวิจัยเกี่ยวกับมาตรการแก้ไขปรับปรุงที่เหมาะสม รวมทั้งการเฝ้าติดตามการเปลี่ยนแปลงของกลุ่มผู้ถูกฉ้อโกงและเสริมสร้างการวิจัยเกี่ยวกับมาตรการเตือนภัย การเผยแพร่ประชาสัมพันธ์ และมาตรการป้องกัน โดยในปี ค.ศ. ๒๐๒๑ รัฐบาลจีนได้จัดตั้งศูนย์วิจัยแห่งชาติว่าด้วยอาชญากรรมรูปแบบใหม่ (the National Center for Study of New

^๒ the Opinions on Strengthening the Work of Cracking down on and Controlling Crimes of Telecom and Online Fraud, the Announcement on Preventing and Cracking down on Crimes of Telecom and Online Fraud, the Notice on Matters concerning Strengthening the Administration of Payment and Settlement and Preventing New-Type Illegal and Criminal Telecom and Online Activities, the Work Plan for Advancing the Construction of a Long-term Mechanism for Preventing and Controlling Crimes of Telecom and Online Fraud Using Big Data and the Several Provisions on the Return of Frozen Funds Involved in Cases of New-Type Violations of Laws and Crimes Related to Telecommunications Networks

Types of Crimes) และศูนย์ย่อยอีก ๑๑ แห่ง เพื่อเสริมสร้างการวิจัยอย่างต่อเนื่องเกี่ยวกับอาชญากรรมรูปแบบใหม่ ปัญหาใหม่ แนวโน้มใหม่ และสถานการณ์ใหม่ ที่อาจจะเกิดขึ้น เพื่อคงไว้ซึ่งความได้เปรียบเชิงรุกในการปราบปรามอาชญากรรม

๒. การสร้างทีมเฉพาะกิจเพื่อยกระดับขีดความสามารถและมาตรฐานอย่างต่อเนื่อง

อาชญากรรมทางโทรคมนาคมและการฉ้อโกงออนไลน์เป็นอาชญากรรมข้ามชาติที่มีลักษณะเฉพาะและเป็นขบวนการ รัฐบาลจีนจึงต้องปราบปรามอาชญากรรมเฉพาะทางดังกล่าวด้วยมาตรการพิเศษ โดยมีการจัดตั้งหน่วยงานเฉพาะกิจ เพิ่มอัตรากำลังเจ้าหน้าที่เฉพาะทาง และเสริมสร้างการฝึกอบรมเฉพาะด้าน เพื่อให้เกิดการยกระดับขีดความสามารถและมาตรฐานในการปราบปรามอาชญากรรมทางโทรคมนาคมและการฉ้อโกงออนไลน์อย่างก้าวกระโดด สรุปได้ดังนี้

๒.๑ การจัดตั้งศูนย์ต่อต้านการฉ้อโกง ๔ ระดับ (Four-tiered anti-fraud centers)

จีนได้จัดตั้งศูนย์ต่อต้านการฉ้อโกงแห่งชาติและศูนย์ย่อยอีก ๘ แห่ง โดยบูรณาการบุคลากรผู้เชี่ยวชาญ (professional talents) วิธีการเชิงวิชาชีพ (professional means) เครื่องมืออุปกรณ์เฉพาะทาง (professional equipment) และศักยภาพเชิงวิชาชีพ (professional capabilities) พร้อมทั้งส่งเสริมให้มณฑล เมือง และเขตต่าง ๆ จัดตั้งศูนย์ต่อต้านการฉ้อโกงที่สอดคล้องกัน

๒.๒ การเพิ่มอัตรากำลังเจ้าหน้าที่ต่อต้านการฉ้อโกงเฉพาะทาง ตามหลักการจัดสรรกำลังเจ้าหน้าที่ตำรวจตามระดับความเร่งด่วน จีนได้เพิ่มกำลังทีมต่อต้านการฉ้อโกงเฉพาะทางอย่างต่อเนื่อง โดยพิจารณาจากอัตราการเกิดคดีฉ้อโกงทางโทรคมนาคมและออนไลน์ในแต่ละพื้นที่ อีกทั้งหน่วยงานกำกับดูแลด้านการเงิน การสื่อสาร และอินเทอร์เน็ต ก็ได้จัดให้มีเจ้าหน้าที่เฉพาะทางเพื่อรับผิดชอบงานต่อต้านการฉ้อโกง ซึ่งทีมเหล่านี้มีการขยายตัวอย่างต่อเนื่องเช่นกัน

๒.๓ การจัดตั้งทีมผู้เชี่ยวชาญต่อต้านการฉ้อโกง รัฐบาลจีนได้จัดตั้งคลังสมองแห่งชาติ (a national think tank) และทีมผู้เชี่ยวชาญในการปราบปรามอาชญากรรมทางโทรคมนาคมและการฉ้อโกงออนไลน์ โดยคัดเลือกผู้เชี่ยวชาญจากหลากหลายสาขาอาชีพ ตำรวจจีนได้เชิญผู้เชี่ยวชาญด้านการสืบสวนคดีอาญา ผู้เชี่ยวชาญด้านการต่อต้านการฉ้อโกง และบุคลากรที่มีความสามารถในระดับต่าง ๆ เพื่อช่วยสนับสนุนทางวิชาการที่เข้มแข็งสำหรับงานต่อต้านการฉ้อโกง

๒.๔ การฝึกอบรมเฉพาะทางด้านการต่อต้านการฉ้อโกง สำนักงานอัยการ ศาล และหน่วยงานด้านความมั่นคงสาธารณะ รวมถึงหน่วยงานที่มีอำนาจกำกับดูแลด้านการเงิน การสื่อสาร และอินเทอร์เน็ต ได้จัดการฝึกอบรมเฉพาะทางเกี่ยวกับการปราบปรามอาชญากรรมทางโทรคมนาคมและการฉ้อโกงออนไลน์มากกว่า ๑๐,๐๐๐ ครั้ง และในปี ค.ศ. ๒๐๒๑ มหาวิทยาลัยตำรวจสืบสวนคดีอาญาแห่งประเทศจีนได้ริเริ่มเปิดสาขาการสืบสวนคดีฉ้อโกงทางโทรคมนาคมและออนไลน์ในหลักสูตรวิชาวิทยาการสืบสวนคดีอาญา และได้เปิดรับนักศึกษา รุ่นแรกในเดือนกันยายนปีเดียวกัน ซึ่งถือเป็นการบุกเบิกแนวทางใหม่ให้แก่สถาบันการศึกษาด้านความมั่นคงสาธารณะในการผลิตบุคลากรเฉพาะทางด้านการต่อต้านการฉ้อโกง

๓. คติพิเศษในการปราบปรามและการยับยั้งอาชญากรรม

การปราบปรามเป็นมาตรการป้องกันที่ทรงประสิทธิภาพมากที่สุด ด้วยเหตุนี้ ตำรวจจีนจึงดำเนินการปราบปรามอาชญากรรมด้านการฉ้อโกงทางโทรคมนาคมและออนไลน์อย่างเข้มข้น

มาโดยตลอด อีกทั้งกระทรวงความมั่นคงสาธารณะได้ดำเนินการและเปิดตัวปฏิบัติการ “the Cloud Sword Operation Fraud” ของหน่วยงานความมั่นคงสาธารณะแห่งชาติ เพื่อปราบปรามอาชญากรรมดังกล่าวอย่างจริงจัง โดยมีการจัดระเบียบและระดมหน่วยงานความมั่นคงสาธารณะทั่วประเทศจีนให้เข้มงวดในการปราบปรามอาชญากรรมดังกล่าว ซึ่งปฏิบัติการนี้บรรลุผลสำเร็จอย่างเป็นรูปธรรมและสามารถยับยั้งการก่ออาชญากรรมได้อย่างมีประสิทธิภาพ สรุปได้ดังนี้

๓.๑ การปราบปรามการฉ้อโกงข้ามชาติ จีนได้ดำเนินการปราบปรามการฉ้อโกงข้ามชาติอย่างเข้มงวดโดยการสร้างความร่วมมือด้านการบังคับใช้กฎหมายและกระบวนการยุติธรรมกับต่างประเทศ โดยยึดหลักการเคารพอธิปไตยของแต่ละประเทศ ซึ่งตำรวจจีนได้รับเชิญให้เข้าร่วมปฏิบัติการต่าง ๆ ในต่างประเทศเป็นจำนวนมาก และด้วยการสนับสนุนอย่างเต็มที่จากหน่วยงานบังคับใช้กฎหมายและกระบวนการยุติธรรมของประเทศเจ้าภาพ ตำรวจจีนจึงสามารถควบคุมตัวผู้ต้องสงสัยชาวจีนที่เกี่ยวข้องกับการฉ้อโกงได้หลายราย ผ่านกระบวนการส่งผู้ร้ายข้ามแดนและมาตรการทางกฎหมายอื่น

๓.๒ การปราบปรามแก๊งนำและหัวหน้าขบวนการ จีนได้ดำเนินปฏิบัติการที่เรียกว่า “The Nail Pulling operation” เพื่อจับกุมและลงโทษแกนนำและหัวหน้ากลุ่มฉ้อโกงทางโทรคมนาคมและออนไลน์ โดยกระทรวงความมั่นคงสาธารณะได้ออกหมายจับผู้ต้องสงสัยที่ก่อให้เกิดอันตรายร้ายแรงในระดับ “Class-A Wanted Orders” ซึ่งปัจจุบันมีแกนนำและหัวหน้ากลุ่มฉ้อโกงถูกจับกุมแล้วประมาณ ๑๐๐ ราย

๓.๓ การปราบปรามคดีร้ายแรง มีการจัดตั้งกลไกการสืบสวนคดีใหญ่ที่มีมูลค่าความเสียหายสูง โดยกระทรวงความมั่นคงสาธารณะจะเข้าดำเนินการสืบสวนคดีสำคัญเหล่านี้โดยตรงสำหรับคดีที่เกิดขึ้นบ่อย เช่น การคืนเงินจากการซื้อขายที่เป็นการฉ้อโกง (rebates for false purchases) การกู้ยืมออนไลน์ การซื้อขายออนไลน์ การลงทุนออนไลน์ ได้มีการจัดตั้งศูนย์บัญชาการเฉพาะกิจเพื่อปราบปรามโดยตรง ส่วนกรณีที่มีการใช้บัตรโทรศัพท์และบัตรธนาคารจำนวนมากในการฉ้อโกง ได้มีการดำเนินการ “ปฏิบัติการตัดบัตร” (the card cutting campaign) โดยมีวัตถุประสงค์เพื่อเพิ่มภาระต้นทุนแก่ผู้ก่ออาชญากรรม ทำให้การก่ออาชญากรรมกระทำได้ยากขึ้น และสำหรับกรณีที่มีการจัดตั้งและรับสมัครบุคคลเพื่อไปทำการฉ้อโกงในต่างประเทศ ได้มีการดำเนินการ “ปฏิบัติการตัดเส้นทาง” (the flow cutting campaign) เพื่อปราบปรามผู้จัดตั้งเบื้องหลัง ตลอดจนควบคุมและจำกัดพื้นที่การเคลื่อนไหวของกลุ่มฉ้อโกงอย่างต่อเนื่อง

๓.๔ การปราบปรามอาชญากรรมตลาดมืด (Black market crimes) เพื่อตอบสนองต่อสถานการณ์ที่เปลี่ยนแปลง ตำรวจจีนได้พัฒนาวิธีการปราบปรามรูปแบบใหม่สำหรับอาชญากรรมตลาดมืดที่เกี่ยวข้องกับการฉ้อโกงทางโทรคมนาคมและออนไลน์ เช่น การสร้างหรือซื้อปริมาณการเข้าชมที่ไม่เป็นจริงเพื่อใช้ในการโปรโมตหรือสร้างภาพลักษณ์ปลอม (traffic attraction for promotion) การพัฒนาเทคโนโลยี การโอนเงินเพื่อฟอกเงิน การเช่าเซิร์ฟเวอร์ และการขายต่อชื่อโดเมน โดยได้มีการจัดตั้งศูนย์บัญชาการรบเชิงภูมิภาคทั่วประเทศ (nationwide regional battles) โดยหน่วยงานด้านความมั่นคงสาธารณะ การสื่อสาร การเงิน และอินเทอร์เน็ต ได้บูรณาการทรัพยากรที่มีอยู่ทั่วประเทศในการกำหนดเบาะแสอาชญากรรมอย่างมีประสิทธิภาพ และดำเนินการปราบปรามแบบรวมศูนย์เพื่อเพิ่มประสิทธิภาพสูงสุดของการปราบปรามในวงกว้าง

๔. การสร้างความเชี่ยวชาญเพื่อเพิ่มประสิทธิภาพการทำงานอย่างต่อเนื่อง

อาชญากรรมด้านการฉ้อโกงทางโทรคมนาคมและออนไลน์เป็นอาชญากรรมเฉพาะทางที่มีเทคโนโลยีขั้นสูง ซึ่งกลุ่มผู้กระทำผิดได้ปรับปรุงและพัฒนาวิธีการโดยใช้นวัตกรรมใหม่และรูปแบบธุรกิจใหม่ เช่น บล็อกเชน สกุลเงินดิจิทัล (virtual currencies) ปัญญาประดิษฐ์ (AI) GOIP^๓ อีกทั้งยังใช้เครือข่ายการสื่อสารและการโอนเงินเพื่อการฟอกเงิน ดังนั้น ในการปราบปรามและป้องกันอาชญากรรมดังกล่าว รัฐบาลจีนจึงให้ความสำคัญอย่างยิ่งต่อการวิจัยและการประยุกต์ใช้ความเชี่ยวชาญด้านการต่อต้านการฉ้อโกง สรุปได้ดังนี้

๔.๑ การป้องกันทางเทคนิค หน่วยงานด้านความมั่นคงสาธารณะ การเงิน การสื่อสาร และอินเทอร์เน็ตของจีนได้ปรับปรุงกลไกการป้องกันและควบคุมความเสี่ยง และพัฒนาระบบการเตือนภัยล่วงหน้า การระบุตัวตน ตลอดจนมาตรการป้องกันและการจัดการเพื่อดำเนินงานทางเทคนิคที่เกี่ยวข้องกับการโทรศัพท์หลอกลวง การส่งข้อความ (SMS) ชื่อโดเมน เว็บไซต์ และบัญชีเครือข่าย

๔.๒ การแจ้งเตือนและการเตือนภัย ยึดหลัก “การปราบปรามและการป้องกันควบคู่กัน โดยให้ความสำคัญเป็นลำดับแรกกับการป้องกัน” มีการใช้ฐานข้อมูลขนาดใหญ่ การประมวลผลบนระบบคลาวด์ และเทคโนโลยีอื่น เพื่อให้การระบุตัวผู้เสียหายเป็นไปอย่างทันท่วงทีและส่งการแจ้งเตือนที่แม่นยำ นอกจากนี้ รัฐบาลจีนได้เปิดสายด่วน 96110 และแพลตฟอร์ม SMS 12381 ซึ่งจะช่วยเพิ่มประสิทธิภาพของการแจ้งเตือนและการเตือนภัย และสามารถป้องกันประชาชนจำนวนมากจากการถูกฉ้อโกงได้

๔.๓ การพัฒนาห้องปฏิบัติการเฉพาะทาง ตำรวจจีนได้ผลักดันการสร้างระบบความมั่นคงสาธารณะอัจฉริยะ เพื่อใช้ประโยชน์ในการสนับสนุนด้านวิทยาศาสตร์อาชญากรรมและเทคโนโลยีและพัฒนาขีดความสามารถในการวิเคราะห์และการเก็บรวบรวมพยานหลักฐานที่เกี่ยวข้องกับกระแสด การเคลื่อนย้ายของเงินทุน ข้อมูล และเครือข่ายอย่างครอบคลุม อันจะเป็นการสนับสนุนทางเทคนิคที่แข็งแกร่งในการปราบปรามอาชญากรรมฉ้อโกงทางโทรคมนาคมและออนไลน์

๕. การประสานความร่วมมือภายในเพื่อเริ่มต้นจัดทำรูปแบบการทำงานต่อต้านการฉ้อโกงในระดับสังคม

รัฐบาลจีนได้จัดตั้งรูปแบบการทำงานต่อต้านการฉ้อโกงในระดับสังคม โดยมีจุดเด่นคือ “รัฐบาลเป็นผู้นำ กำหนดหน่วยงานผู้รับผิดชอบหลัก ภาคอุตสาหกรรมหรือผู้ประกอบการมีบทบาทและความรับผิดชอบในการกำกับดูแลการดำเนินงานของตนเอง มีการทำงานร่วมกันของหน่วยงานที่เกี่ยวข้อง และการมีส่วนร่วมจากทุกภาคส่วนของสังคม” สรุปได้ดังนี้

๕.๑ กลไกการทำงานร่วมกันเพื่อต่อต้านการฉ้อโกง ซึ่งจัดตั้งโดยรัฐบาลและคณะรัฐมนตรี (The State Council of China) ได้อนุมัติการจัดตั้งระบบการประชุมร่วมระหว่างกระทรวง โดยมีกระทรวงความมั่นคงสาธารณะเป็นผู้รับผิดชอบหลัก และมีหน่วยงานและองค์กรต่าง ๆ รวม ๒๕ แห่ง

^๓ GSM over Internet Protocol เป็นอุปกรณ์ที่ทำหน้าที่เป็นสะพานเชื่อมระหว่างเครือข่ายโทรศัพท์มือถือ (GSM) กับระบบโทรศัพท์ผ่านอินเทอร์เน็ต (VoIP) โดยอาศัยอินเทอร์เน็ตโพรโทคอล (IP) ในการส่งข้อมูล และสามารถควบคุมจากระยะไกล ทำให้สามารถโทรออกหรือส่งข้อความผ่านอินเทอร์เน็ตได้แม้ผู้ใช้งานจะอยู่ห่างจากตัวเครื่อง

เข้าร่วมเพื่อปราบปรามการละเมิดกฎหมายและอาชญากรรมรูปแบบใหม่ที่เกี่ยวข้องกับเครือข่ายโทรคมนาคม นอกจากนี้ รัฐบาลระดับมณฑล เมือง และอำเภอยังได้จัดให้มีกลไกการประชุมร่วมกัน เพื่อพัฒนากลไกการทำงานต่อต้านการฉ้อโกงให้มีความทันสมัยและสอดคล้องกับนวัตกรรมใหม่ด้วย

๕.๒ กลไกการทำงานต่อต้านการฉ้อโกงโดยใช้กำลังตำรวจทั้งระบบ ได้รับการจัดตั้งโดยหน่วยงานความมั่นคงสาธารณะ โดยมีแนวทางการดำเนินการ ๓ ประการ ได้แก่ ความร่วมมือที่เชื่อมโยงอย่างมีประสิทธิภาพในทุกระดับ ความร่วมมือในระดับภูมิภาคที่มีการประสานงานทั่วประเทศ และความร่วมมือที่มีการประสานงานใกล้ชิดระหว่างตำรวจประเภทต่าง ๆ

๕.๓ การดำเนินงานต่อต้านการฉ้อโกงโดยอุตสาหกรรมสารสนเทศและการสื่อสาร กระทรวงอุตสาหกรรมและเทคโนโลยีสารสนเทศของจีน (The Ministry of Industry and Information Technology of China: MIIT) ได้จัดให้มีทีมงานเฉพาะด้านต่อต้านการฉ้อโกงในระดับกระทรวง มณฑล และองค์กรธุรกิจ เพื่อสืบสวนและจัดการกับบัตรโทรศัพท์และบัญชีอินเทอร์เน็ตที่เกี่ยวข้องกับการฉ้อโกง อีกทั้งยังได้จัดทำบัญชีความรับผิดชอบด้านการต่อต้านการฉ้อโกงของผู้ประกอบการโทรคมนาคมและอินเทอร์เน็ต พร้อมทั้งกำชับให้ผู้ประกอบการดำเนินมาตรการต่าง ๆ เช่น การประเมินและความรับผิดชอบ การแจ้งเตือนและการสัมภาษณ์ การกำกับดูแลและการจัดการ

๕.๔ การกำกับดูแลที่เข้มงวดในอุตสาหกรรมการเงิน ธนาคารประชาชนจีนและคณะกรรมการกำกับดูแลการธนาคารและการประกันภัยของจีน กำหนดให้อุตสาหกรรมการเงินจัดระบบการป้องกันและควบคุมการฉ้อโกงสำหรับระบบการชำระเงิน และระบบการจัดการบัญชี ตรวจสอบระบบบัญชีโดยต้องใช้ข้อเท็จจริง และปรับปรุงกลไกการติดตามความเสี่ยงด้านการฉ้อโกง ตลอดจนให้การสนับสนุนหน่วยงานความมั่นคงสาธารณะในการปราบปรามธุรกรรมทางบัญชี ทั้งนี้ การฉ้อโกงถือเป็นข้อห้ามเด็ดขาด (red line) ด้านการกำกับดูแล และต้องนำสถานการณ์ที่เกี่ยวข้องกับการฉ้อโกงของสถาบันการเงินและสถาบันการชำระเงินมาประเมินในด้านการกำกับดูแล

๕.๕ การประชาสัมพันธ์และการป้องกันการฉ้อโกงได้รับการดำเนินการในระดับสังคมโดยรวม หน่วยงานด้านประชาสัมพันธ์ของคณะกรรมการกลางพรรคคอมมิวนิสต์จีน กระทรวงการต่างประเทศ กระทรวงศึกษาธิการ กระทรวงอุตสาหกรรมและเทคโนโลยีสารสนเทศ ธนาคารประชาชนจีน และหน่วยงานอื่น ได้ปฏิบัติหน้าที่อย่างเข้มแข็ง และจัดให้มีการประชาสัมพันธ์ การปราบปรามการฉ้อโกงทางโทรคมนาคมและออนไลน์ในชุมชน พื้นที่ชนบท ครอบครัว โรงเรียน และองค์กรธุรกิจ รวมทั้งจัดกิจกรรมประชาสัมพันธ์ แจกจ่ายเอกสารประชาสัมพันธ์ และส่งข้อความเพื่อสาธารณประโยชน์ นอกจากนี้ ศูนย์ต่อต้านการฉ้อโกงแห่งชาติยังได้เผยแพร่วิดีโอเพื่อเพิ่มพูนความรู้ความสามารถของประชาชนในการป้องกันการฉ้อโกง และสร้างบรรยากาศต่อต้านการฉ้อโกงที่เข้มแข็งในระดับสังคมโดยรวม

๖. การส่งเสริมความร่วมมือภายนอกในการบังคับใช้กฎหมายและความร่วมมือทางตุลาการระหว่างประเทศ

ในยุคโลกาภิวัตน์ย่อมไม่มีประเทศใดสามารถแยกตัวออกจากสังคมโลกได้ และในท่ามกลางสถานการณ์ที่ร้ายแรงและซับซ้อนของการฉ้อโกงทางโทรคมนาคมและเครือข่ายข้ามชาติ ความมุ่งมั่นของประเทศต่าง ๆ ในการปราบปราม ควบคุม และแสวงหาความร่วมมือ จึงเป็นเรื่องจำเป็นและ

สำคัญอย่างยิ่ง โดยความร่วมมือด้านการบังคับใช้กฎหมายระหว่างตำรวจจีนและตำรวจฟิลิปปินส์เกิดขึ้นครั้งแรกในปี ค.ศ. ๒๐๑๐ ทำให้สามารถปราบปรามกลุ่มอาชญากรรมการฉ้อโกงทางโทรคมนาคมและออนไลน์ข้ามชาติขนาดใหญ่ได้สำเร็จ รัฐบาลจีนจึงได้มุ่งมั่นปฏิบัติตามพันธกรณีระหว่างประเทศ ส่งเสริมความร่วมมือด้านการบังคับใช้กฎหมาย โดยยึดถือภูมิปัญญาและแนวทางแก้ไขที่เป็นแบบฉบับของตนเอง (Chinese wisdom, Chinese solutions) ตลอดจนสร้างความร่วมมือระหว่างประเทศในการปราบปรามอาชญากรรมการฉ้อโกงทางโทรคมนาคมและออนไลน์ สรุปได้ดังนี้

๖.๑ ในภูมิภาคเอเชียแปซิฟิกและแอฟริกา จีนได้ดำเนินการความร่วมมือด้านการบังคับใช้กฎหมายกับกัมพูชา ฟิลิปปินส์ สหรัฐอาหรับเอมิเรตส์ เคนยา ฯลฯ เพื่อปราบปรามอาชญากรรมการฉ้อโกงทางโทรคมนาคมและออนไลน์ได้อย่างมีประสิทธิภาพ

๖.๒ ในยุโรป การดำเนินการของตำรวจจีนและตำรวจสเปนในปฏิบัติการ “Great Wall” ในปี ค.ศ. ๒๐๑๖ สามารถปราบปรามกลุ่มอาชญากรรมการฉ้อโกงทางโทรคมนาคมและออนไลน์ประสบความสำเร็จอย่างมาก ถือเป็นแบบอย่างของความร่วมมือด้านการบังคับใช้กฎหมายระหว่างประเทศ และในปี ค.ศ. ๒๐๑๘ เจ้าหน้าที่กระทรวงความมั่นคงสาธารณะของจีนได้เยือน Europol เพื่อแลกเปลี่ยนประสบการณ์เกี่ยวกับปฏิบัติการ “Great Wall” และหารือความร่วมมือด้านการบังคับใช้กฎหมายระหว่างจีนและกลุ่มประเทศยุโรปโดยอ้างอิงจากปฏิบัติการดังกล่าว

๖.๓ ในระดับพหุภาคี ตำรวจจีนได้เข้าร่วมปฏิบัติการต่อต้านการฉ้อโกง “the anti-fraud Operation First Light” ร่วมกับตำรวจจาก ๗๖ ประเทศสมาชิก ภายใต้กรอบขององค์การตำรวจสากล (INTERPOL) ระหว่างเดือนมีนาคมถึงมิถุนายน ค.ศ. ๒๐๒๒ ซึ่งสามารถปราบปรามแหล่งกบดานของผู้ฉ้อโกงได้หลายแห่งในหลายประเทศ จับกุมผู้ต้องสงสัย และสกัดกั้นเงินผิดกฎหมายได้เป็นจำนวนมากถึง ๕๐ ล้านดอลลาร์สหรัฐ

การปราบปรามอาชญากรรมการฉ้อโกงทางโทรคมนาคมและออนไลน์ในประเทศจีนมีแนวโน้มที่ดีขึ้นอย่างต่อเนื่องและถือว่าบรรลุผลสำเร็จ ซึ่งย่อมเป็นเครื่องพิสูจน์ได้ว่า แนวทางแก้ไขปัญหามาแบบฉบับของจีนเป็นแนวทางที่ถูกต้องในการแก้ไขปัญหาการฉ้อโกงทางโทรคมนาคมและออนไลน์ข้ามชาติ ความสำเร็จนี้มิได้อาศัยการปราบปรามทางกายภาพเท่านั้น หากแต่เกิดจากการวางโครงสร้างที่เชื่อมโยงกันระหว่าง “นโยบาย บุคลากร เทคโนโลยี ความร่วมมือ” และที่สำคัญที่สุดคือ การกลั่นกรองประสบการณ์ทั้งหมดเพื่อนำไปสู่การตรากฎหมายเฉพาะทาง ซึ่งสาระสำคัญของกฎหมายดังกล่าวจะได้กล่าวถึงในหัวข้อถัดไป

๒. กฎหมายว่าด้วยการปราบปรามการฉ้อโกงทางโทรคมนาคมและออนไลน์^๔

๒.๑ กฎหมายว่าด้วยการปราบปรามการฉ้อโกงทางโทรคมนาคมและออนไลน์ “Anti-Telecom and Online Fraud Law of the People’s Republic of China” เป็นกฎหมายที่ตราขึ้น

^๔ อ้างอิงฉบับแปลภาษาอังกฤษจาก “Law on Countering Telecommunications Network Fraud By China Law Translate on 2022/09/02”, ซึ่งใช้แหล่งข้อมูลจาก Ministry of Justice of the People’s Republic of China, “Anti-Telecom and Online Fraud Law of the People’s Republic of China”, สืบค้นเมื่อวันที่ ๓๐ เมษายน ๒๕๖๕, จาก <https://www.chinalawtranslate.com/en/anti-telecom-fraud-law/>

โดยมีวัตถุประสงค์เพื่อป้องกัน ควบคุม ลงโทษการฉ้อโกงทางโทรคมนาคมและออนไลน์ และปราบปรามอาชญากรรมดังกล่าว โดยสภาประชาชนแห่งชาติ (the National People's Congress) ได้ริเริ่มการตรากฎหมายฉบับนี้ในเดือนเมษายน ค.ศ. ๒๐๒๑ ผ่านการรับรองเป็นกฎหมายในเดือนกันยายน ค.ศ. ๒๐๒๒ และมีผลบังคับใช้ในวันที่ ๑ ธันวาคม ค.ศ. ๒๐๒๒ ถือเป็นกฎหมายเฉพาะฉบับแรกที่สร้างระบบและมีเนื้อหาครบถ้วนสมบูรณ์ในการกำกับดูแลการปราบปรามการฉ้อโกงทางโทรคมนาคมและออนไลน์ที่มีลักษณะเฉพาะแบบจีน มีหลักการสำคัญสรุปได้ดังนี้^๕

๑. กำหนดบทนิยามคำว่า “การฉ้อโกงทางโทรคมนาคมและออนไลน์” กำหนดหลักเกณฑ์เกี่ยวกับเขตอำนาจศาล ตลอดจนวางหลักการทำงาน ได้แก่ การกำกับดูแลที่ต้นทาง การกำกับดูแลแบบบูรณาการ การดำเนินการร่วมกัน การป้องกันโดยมวลชน และการป้องกันและควบคุมที่แม่นยำ พร้อมทั้งจัดให้มีมาตรการเชิงสถาบันที่มีประสิทธิภาพ (established a series of effective institutional measures)

๒. การปรับปรุงระบบการกำกับดูแล โดยคณะรัฐมนตรีได้กำหนดให้มีกลไกการประชุมร่วมต่อต้านการฉ้อโกง (the State Council's anti-fraud joint meeting mechanism) กำหนดให้หน่วยงานความมั่นคงสาธารณะเป็นผู้รับผิดชอบหลัก รวมทั้งปรับปรุงระบบการกำกับดูแลเป็นความรับผิดชอบเชิงพื้นที่ของรัฐบาลท้องถิ่น ความสำเร็จด้านความรับผิดชอบด้านการกำกับดูแลของหน่วยงานอุตสาหกรรมที่เกี่ยวข้อง และความรับผิดชอบในการกำหนดโทษของหน่วยงานอัยการ ศาล และองค์กรด้านความมั่นคงสาธารณะซึ่งถือเป็นแกนหลักสำคัญ

๓. ความรับผิดชอบของสถานประกอบการ โดยกำหนดหน้าที่ในการป้องกันและควบคุมความเสี่ยงการฉ้อโกงของกิจการโทรคมนาคม การเงิน และอินเทอร์เน็ต การประเมินความเสี่ยงของธุรกิจใหม่ และกำหนดให้หน่วยงานอุตสาหกรรมมีอำนาจลงโทษทางปกครอง เช่น การระงับกิจการ การเพิกถอนใบอนุญาต และการปรับ โดยผู้ซึ่งก่อให้เกิดความเสียหายแก่บุคคลอื่นต้องรับผิดชอบทางแพ่งด้วย

๔. การบังคับใช้ระบบชื่อจริง (real name system) โดยกำหนดให้มีระบบการลงทะเบียนข้อมูลจริงสำหรับบัตรโทรศัพท์และบริการอินเทอร์เน็ต รวมทั้งมีระบบการตรวจสอบที่น่าเชื่อถือ (due diligence system) ในบริการทางการเงิน หากบัตรโทรศัพท์ บัญชีธนาคาร หรือบัญชีอินเทอร์เน็ตมีความผิดปกติ ต้องมีการตรวจสอบยืนยันข้อมูลใหม่ และหากไม่ผ่านการตรวจสอบจะไม่สามารถใช้งานต่อไปได้

๕. การกำกับดูแลตลาดมืด (the black market) มุ่งเน้นการตรวจสอบและกำกับดูแลการใช้งานโทรศัพท์ที่มีการเปลี่ยนหมายเลข การโทรหลอกลวง (false calling) ตลอดจนอุปกรณ์แอปพลิเคชัน และชื่อโดเมนที่เกี่ยวข้องกับการฉ้อโกง และในกรณีที่ผู้ผลิต ผู้ซื้อขาย ผู้จัดหา หรือผู้ใช้อุปกรณ์หรือซอฟต์แวร์ กระทำการโดยมิชอบด้วยกฎหมาย หรือผู้ให้การสนับสนุนต่อกิจกรรมฉ้อโกงทางโทรคมนาคม หน่วยงานด้านความมั่นคงสาธารณะมีอำนาจในการยึดรายได้ที่ผิดกฎหมาย ดำเนินการปรับและควบคุมตัวได้

^๕ Ministry of Public Security of the People's Republic of China, “Legal System Construction Improved to Punish Illegal and Criminal Activities Related to Telecom and Online Fraud According to Law”, 2023-3-16, สืบค้นเมื่อวันที่ ๓๐ เมษายน ๒๕๖๕, จาก <https://www.mps.gov.cn/n2255079/n6865805/n7355748/n7355818/c8924716/content.html>

๖. การเพิ่มความเข้มงวดในการลงโทษ โดยบัญญัติให้ผู้ที่เกี่ยวข้องในการกระทำ ความผิดอาชญากรรมฉ้อโกงทางโทรคมนาคมและออนไลน์ รวมทั้งความผิดที่เกี่ยวข้อง ต้องถูกบันทึกไว้ในประวัติด้านเครดิต (credit history) และถูกดำเนินมาตรการทางวินัย (disciplinary measures) ที่เหมาะสม สำหรับผู้ที่มีการกระทำไม่ถึงขั้นเป็นความผิดอาญา อาจถูกควบคุมตัวทางปกครองและปรับ (administratively detained and fined) และผู้ที่ก่อให้เกิดความเสียหายแก่ผู้อื่นต้องรับผิดชอบแพ่งด้วย นอกจากนี้ กฎหมายยังบัญญัติไว้ด้วยว่า ในขณะที่มีการบังคับใช้มาตรการกำกับดูแลที่เกี่ยวข้องตามกฎหมายจะต้องจัดให้มีช่องทางการเยียวยาและอุทธรณ์ที่สะดวก โดยยึดหลักการว่า “ผู้ใดเป็นผู้มีคำ ตัดสิน ผู้นั้นต้องรับผิดชอบ” (whoever makes a decision shall be responsible) เพื่อให้สามารถรับ และแก้ไขข้อร้องเรียนของประชาชนได้อย่างทันที่ และเพื่อให้กิจกรรมการผลิตและการประกอบธุรกิจ ดำเนินไปได้ตามปกติ รวมทั้งอำนวยความสะดวกต่อการดำรงชีวิตของประชาชน

สำหรับสาระในส่วนของการป้องกันมิให้มีการฉ้อโกงเกิดขึ้นตั้งแต่ต้น ซึ่งกฎหมายว่าด้วยการปราบปรามการฉ้อโกงทางโทรคมนาคมและออนไลน์ให้ความสำคัญอย่างยิ่ง นั้น มีรายละเอียดเพิ่มเติม ดังนี้^๖

๑. ความรับผิดชอบของผู้ให้บริการ (Responsibilities of Service Providers)

กำหนดหน้าที่แก่ธุรกิจหลักในภาคโทรคมนาคม การเงิน และอินเทอร์เน็ต ได้แก่ บริษัทโทรคมนาคม ธนาคารและผู้ให้บริการชำระเงินอื่น ๆ ตลอดจนผู้ให้บริการอินเทอร์เน็ต เพื่อควบคุมและป้องกันความ เสี่ยงจากการฉ้อโกงในภาคโทรคมนาคม

กรณีบริษัทโทรคมนาคมต้องดำเนินการบังคับใช้ข้อกำหนดการลงทะเบียนด้วยชื่อจริง สำหรับผู้ใช้บริการโทรศัพท์ทุกรายอย่างครอบคลุม และต้องบังคับใช้ข้อจำกัดจำนวนบัตรซิมสูงสุดที่ อนุญาตต่อผู้ใช้หนึ่งรายตามข้อบังคับที่แยกต่างหาก (มาตรา ๙ และมาตรา ๑๐) เมื่อบริษัทตรวจพบ ซิมการ์ดที่มีลักษณะผิดปกติหรือเกี่ยวข้องกับการฉ้อโกง บริษัทอาจกำหนดให้มีการตรวจสอบยืนยันตัวตน ของผู้ใช้ใหม่ และหากการตรวจสอบไม่สำเร็จ บริษัทมีสิทธิจำกัดหรือระงับการใช้งานซิมการ์ดนั้นได้ (มาตรา ๑๑) นอกจากนี้ บริษัทโทรคมนาคมต้องแสดงหมายเลขโทรศัพท์ที่แท้จริงของผู้โทร (รวมถึงรหัส ประเทศและรหัสพื้นที่) บนหน้าจอแสดงหมายเลขของผู้รับอย่างถูกต้อง และต้องดำเนินการปิดกั้นและ ติดตามการโทรที่มีการปลอมแปลงหมายเลข (spoofed calls) (มาตรา ๑๓)

กรณีบริษัทด้านการเงิน สถาบันการธนาคารและผู้ให้บริการชำระเงินที่มีใช้ธนาคาร มีหน้าที่รับผิดชอบในการตรวจสอบสถานะและยืนยันข้อมูลลูกค้าอย่างรอบคอบ (due diligence) ระบุตัว ผู้ถือผลประโยชน์ที่แท้จริง และดำเนินมาตรการบริหารความเสี่ยงที่เหมาะสม (มาตรา ๑๕) ต้องจัดให้มี ระบบเพื่อตรวจสอบบัญชีที่ผิดปกติและธุรกรรมที่น่าสงสัย และดำเนินมาตรการป้องกันที่เหมาะสมเมื่อ พบว่ามีบัญชีหรือธุรกรรมดังกล่าว (มาตรา ๑๘ วรรคสาม) ในการตรวจสอบดังกล่าว ธนาคารและผู้ให้ บริการชำระเงินอื่นได้รับอนุญาตตามกฎหมาย สามารถเก็บข้อมูลที่อยู่ IP ของลูกค้า รหัสประจำอุปกรณ์ เครือข่าย (ที่อยู่ MAC) ข้อมูลเครื่องรับชำระเงิน ณ จุดขาย (point-of-sale terminal) และข้อมูลอื่นที่

^๖ Changhao Wei & Taige Hu, “Legislation Summary: China’s New Law to Fight Telecom and Internet Fraud”, Posted on September 7, 2022, สืบค้นเมื่อวันที่ ๓๐ เมษายน ๒๕๖๔, จาก <https://npcobserver.com/2022/09/07/legislation-summary-chinas-new-law-to-fight-telecom-and-internet-fraud/>

จำเป็นเกี่ยวกับธุรกรรมหรือสถานที่ตั้งของอุปกรณ์ได้ (มาตรา ๑๘ วรรคสี่) อย่างไรก็ตาม หากล้มเหลวได้รับความยินยอมจากลูกค้า ห้ามมิให้นำข้อมูลดังกล่าวไปใช้เพื่อวัตถุประสงค์อื่นใดนอกจากการป้องกันและปราบปรามการฉ้อโกง

กรณีบริษัทอินเทอร์เน็ต กฎหมายเน้นย้ำถึงข้อกำหนดที่ให้บริการโทรคมนาคมและผู้ให้บริการอินเทอร์เน็ต (ISPs) ต้องตรวจสอบและยืนยันตัวตนของผู้ใช้ก่อนที่จะให้บริการในด้านต่าง ๆ ได้แก่ การเข้าถึงอินเทอร์เน็ต บริการพร็อกซี การจดทะเบียนโดเมน การบริการที่ให้เช่าพื้นที่บนเซิร์ฟเวอร์ เพื่อเก็บข้อมูลเว็บไซต์ (web hosting) การบริการคลาวด์ การเผยแพร่เนื้อหาและซอฟต์แวร์ การสื่อสารแบบข้อความโต้ตอบทันที การชำระเงินออนไลน์ เกม การถ่ายทอดสด และการโฆษณา (มาตรา ๒๑) เมื่อผู้ให้บริการตรวจพบบัญชีที่มีลักษณะผิดปกติหรือเกี่ยวข้องกับการฉ้อโกง ผู้ให้บริการต้องดำเนินการตรวจสอบยืนยันตัวตนของผู้ใช้อีกครั้ง (มาตรา ๒๒ วรรคหนึ่ง) และเมื่อได้รับการร้องขอจากเจ้าหน้าที่ผู้ให้บริการต้องดำเนินการตรวจสอบยืนยันตัวตนสำหรับบัญชีอินเทอร์เน็ตที่เชื่อมโยงกับซิมการ์ดที่เกี่ยวข้องกับคดีฉ้อโกง หรือซิมการ์ดที่มีลักษณะผิดปกติและเกี่ยวข้องกับการฉ้อโกง (มาตรา ๒๒ วรรคสอง) นอกจากนี้ กฎหมายยังได้กำหนดให้บริการโทรคมนาคมและผู้ให้บริการอินเทอร์เน็ตมีหน้าที่ในการใช้ความระมัดระวังอย่างสมเหตุสมผล “duty of reasonable care” ในการกำกับดูแล ตรวจสอบ และดำเนินการแก้ไขการใช้บริการที่ถูกนำไปใช้เพื่อการฉ้อโกง (มาตรา ๒๕ วรรคสอง)

ทั้งนี้ ผู้ให้บริการที่กล่าวถึงข้างต้นยังมีหน้าที่ในการเสริมสร้างความตระหนักรู้ของลูกค้าเกี่ยวกับการฉ้อโกงทางโทรคมนาคมและออนไลน์ รวมถึงการแจ้งเตือนให้ลูกค้าระมัดระวังการฉ้อโกงในระหว่างการทำธุรกรรมทางธุรกิจ และการแจ้งเตือนอย่างทันทั่วถึงเกี่ยวกับกลยุทธ์ใหม่ที่ผู้ฉ้อโกงใช้ในแต่ละภาคส่วนบริการที่เกี่ยวข้องด้วย (มาตรา ๓๐)

๒. การบังคับใช้กฎหมาย (Law Enforcement Obligations & Powers) หน่วยงานของรัฐทุกระดับมีหน้าที่ในการเสริมสร้างความตระหนักรู้ของประชาชนเกี่ยวกับการฉ้อโกงทางโทรคมนาคมและออนไลน์ รวมทั้งเสริมสร้างความสามารถในการระบุพฤติกรรมฉ้อโกง (มาตรา ๘ วรรคหนึ่ง) หน่วยงานการศึกษาและกิจการพลเรือนต้องจัดให้มีการรณรงค์ด้านการศึกษาเพื่อมุ่งเป้าไปยังผู้สูงอายุ ซึ่งส่วนใหญ่มีแนวโน้มตกเป็นเหยื่อของการฉ้อโกง เยาวชนซึ่งมีความเสี่ยงที่จะถูกชักชวนโดยผู้ฉ้อโกงและกลุ่มเปราะบางอื่น ๆ (มาตรา ๘ วรรคสอง) นอกจากนี้ กฎหมายกำหนดให้เจ้าหน้าที่ตำรวจต้องเปิดการสอบสวนอย่างเป็นทางการทุกครั้งที่ได้รับแจ้งหรือพบกิจกรรมการฉ้อโกงทางโทรคมนาคมและออนไลน์ (มาตรา ๒๗ วรรคสอง) ในการสอบสวนคดีดังกล่าว ตำรวจต้องตรวจสอบแหล่งที่มาของข้อมูลส่วนบุคคลที่ถูกนำมาใช้ด้วย (มาตรา ๒๙ วรรคสอง) และตำรวจต้องร่วมมือกับหน่วยงานกำกับดูแลด้านการเงิน โทรคมนาคม และไซเบอร์ รวมทั้งผู้ให้บริการ เพื่อจัดให้มีระบบการเตือนล่วงหน้าและการยับยั้ง “a system of early warning and dissuasion” เพื่อระบุผู้ที่อาจตกเป็นเหยื่อและยับยั้งมิให้มีการดำเนินธุรกรรมที่เป็นการฉ้อโกงต่อไป (มาตรา ๓๔) การใช้มาตรการควบคุมความเสี่ยงชั่วคราวต่อภูมิภาคที่มีระดับกิจกรรมการฉ้อโกงทางโทรคมนาคมและทางออนไลน์สูง โดยตำรวจและหน่วยงานกำกับดูแลด้านการเงิน และโทรคมนาคมอาจใช้มาตรการดังกล่าวได้โดยได้รับความเห็นชอบจาก the State Council’s inter-ministerial conference on cybercrime (มาตรา ๓๕) อีกทั้งกฎหมายยังได้ให้อำนาจแก่สำนักงานอัยการ

ในการยื่นฟ้องคดีเพื่อประโยชน์สาธารณะต่อการกระทำที่เป็นการละเมิดหรือเป็นภัยต่อประโยชน์แห่งชาติ หรือประโยชน์สาธารณะในการปฏิบัติงานด้านการต่อต้านการฉ้อโกง (มาตรา ๔๗)

๓. เทคโนโลยีและกิจกรรมที่เอื้อต่อการฉ้อโกง (Fraud-Enabling Technologies & Activities) กฎหมายฉบับนี้ให้ความสำคัญและเข้มงวดต่อเทคโนโลยีและความผิดที่เป็น “ต้นทางของการฉ้อโกง” (upstream offenses) ซึ่งหากปราศจากสิ่งเหล่านี้ การฉ้อโกงทางโทรคมนาคมและออนไลน์ย่อมไม่สามารถแพร่หลายได้ กฎหมายจึงกำหนดห้ามบุคคลหรือองค์กรใดผลิต จำหน่าย ซื้อมา จัดหา หรือใช้อุปกรณ์หรือซอฟต์แวร์เพื่อกระทำการฉ้อโกงทางโทรคมนาคมและออนไลน์ เช่น กล่องซิม (SIM boxes) เทคโนโลยีปลอมแปลงหมายเลขผู้โทร (caller ID spoofing) ระบบสลับบัญชีอัตโนมัติ และแพลตฟอร์มที่สามารถส่งหรือรับรหัสยืนยันทาง SMS จำนวนมาก (มาตรา ๑๔) นอกจากนี้ กฎหมายยังกำหนดห้ามการกระทำใด ๆ ที่เป็นการสนับสนุนหรือช่วยเหลือการฉ้อโกงทางโทรคมนาคมและออนไลน์ รวมถึงการจำหน่ายหรือจัดหาข้อมูลส่วนบุคคล และการช่วยเหลือผู้ฉ้อโกงในการฟอกเงิน (รวมถึงผ่านสกุลเงินดิจิทัล) (มาตรา ๒๕) และโดยที่ผู้ฉ้อโกงมักจะพึ่งพาการใช้ซิมการ์ด บัญชีธนาคารหรือบัญชีการชำระเงินอื่น ๆ รวมถึงบัญชีอินเทอร์เน็ตที่เชื่อมโยงกับบุคคลที่สาม กฎหมายจึงได้กำหนดห้ามกิจกรรมหลายประเภทที่เกี่ยวข้องกับซิมการ์ดและบัญชีดังกล่าว ไม่ว่าจะเป็นถูกใช้เพื่อการฉ้อโกงหรือไม่ เช่น การซื้อขายโดยมิชอบ การช่วยเหลือในการยืนยันตัวตนด้วยชื่อจริง (assisting with real-name verification) การเปิดบัญชีหรือบัญชีโดยการแอบอ้างบุคคลอื่น (มาตรา ๓๑ วรรคหนึ่ง) การฝ่าฝืนข้อห้ามทั้งหมดดังกล่าวจะส่งผลให้ถูกริบผลประโยชน์ที่ได้มาโดยมิชอบ ถูกปรับ และหากการฝ่าฝืนมีความร้ายแรงจะถูกกักขังทางปกครองไม่เกิน ๑๕ วัน (concurrent administrative detention of up to 15 days) (มาตรา ๔๒ และมาตรา ๔๔) ส่วนผู้ที่ฝ่าฝืนกฎเกณฑ์การลงทะเบียนด้วยชื่อจริง รวมทั้งผู้ที่ถูกตัดสินว่ามีความผิดฐานฉ้อโกงทางโทรคมนาคมและออนไลน์หรือความผิดที่เกี่ยวข้อง จะมีบทลงโทษเพิ่มเติม ได้แก่ การจำกัดการใช้บัตรหรือบัญชี และการห้ามทำธุรกรรมทางไกลหรือการทำธุรกิจใหม่ (มาตรา ๓๑ วรรคสอง)

๔. ภูมิภาคหรือพื้นที่ที่เป็นแหล่งรวมการฉ้อโกงทางโทรคมนาคมและออนไลน์ในต่างประเทศ (Overseas Fraud Hotspots) กฎหมายฉบับนี้ได้กำหนดบทบัญญัติเพื่อควบคุมการดำเนินการฉ้อโกงจากต่างประเทศที่มุ่งโจมตีประชาชนภายในประเทศ ภายใต้บทบัญญัติในมาตราต่าง ๆ ที่เกี่ยวข้องกับเขตอำนาจนอกดินแดน (extraterritoriality provision) เจ้าหน้าที่มีอำนาจในการดำเนินคดีต่อองค์กรหรือบุคคลในต่างประเทศที่กระทำการฉ้อโกงทางโทรคมนาคมและออนไลน์ต่อผู้เสียหายในจีนแผ่นดินใหญ่ หรือผู้ที่ให้การสนับสนุนแก่ผู้กระทำการดังกล่าว (มาตรา ๓ วรรคสอง) และเพื่อสกัดกั้นการเดินทางออกนอกประเทศของผู้ที่มีแนวโน้มจะกระทำการฉ้อโกง หน่วยงานตรวจคนเข้าเมืองอาจกำหนดห้ามการออกนอกประเทศสำหรับบุคคลที่เดินทางไปยังภูมิภาคเสี่ยงในต่างประเทศ และมีเหตุอันควรสงสัยอย่างยิ่งว่าจะเข้าไปมีส่วนเกี่ยวข้องกับการฉ้อโกงทางโทรคมนาคมและออนไลน์เมื่ออยู่ต่างประเทศ (มาตรา ๓๖ วรรคหนึ่ง) นอกจากนี้ เจ้าหน้าที่ตำรวจอาจสั่งห้ามมิให้บุคคลที่ถูกพิพากษาว่ามีความผิดฐานฉ้อโกงทางโทรคมนาคมและออนไลน์เดินทางออกนอกประเทศเป็นระยะเวลาหกเดือนถึงสามปีภายหลังจากที่ได้พ้นโทษแล้ว (มาตรา ๓๖ วรรคสอง) อนึ่ง กระทรวงความมั่นคงสาธารณะและกระทรวงการต่างประเทศมีหน้าที่ในการเสริมสร้างความร่วมมือกับหน่วยงานบังคับใช้กฎหมายของ

ต่างประเทศและองค์กรระหว่างประเทศในด้านการแลกเปลี่ยนข้อมูล การสืบสวน การจับกุมผู้ต้องสงสัย และการติดตามทรัพย์สินที่ถูกลักขโมย (มาตรา ๓๗)

๒.๒ การแก้ไขเพิ่มเติมประมวลกฎหมายอาญาเพื่อใช้ในการปราบปรามตลาดมืดทางออนไลน์^๗ นอกเหนือจากการตรากฎหมายเฉพาะเพื่อปราบปรามการฉ้อโกงทางโทรคมนาคมและออนไลน์แล้ว ก่อนหน้านั้น รัฐบาลจีนได้แก้ไขเพิ่มเติมประมวลกฎหมายอาญาเพื่อให้เท่าทันต่อสถานการณ์ปัจจุบันที่การพัฒนาของเทคโนโลยีสารสนเทศทางเครือข่ายเป็นไปอย่างรวดเร็ว โดยเฉพาะประเด็นเรื่องขอบเขตของตลาดมืดออนไลน์ที่ผิดกฎหมายซึ่งครอบคลุมถึงการกระทำในรูปแบบต่าง ๆ เช่น การลงทะเบียนบัญชีเครือข่ายโดยมิชอบ การจำหน่ายข้อมูลผู้ใช้ การสร้างเว็บไซต์ปลอม (phishing website) และการดำเนินการโจมตีทางเครือข่าย ซึ่งการกระทำเหล่านี้ขยายตัวอย่างมากและก่อให้เกิดระบบนิเวศอุตสาหกรรมซึ่งสนับสนุนการฉ้อโกงทางโทรคมนาคมและออนไลน์ที่เชื่อมโยงกันทั้งต้นทางและปลายทาง ตลอดจนความผิดทางไซเบอร์อื่น ๆ ส่งผลให้ต้นทุนในการก่ออาชญากรรมลดลง แต่วิธีการก่ออาชญากรรมกลับมีความหลากหลายมากยิ่งขึ้น ทำให้การปราบปรามเป็นไปด้วยความยากลำบาก และก่อให้เกิดความเสียหายร้ายแรงอย่างยิ่ง ดังนั้น เพื่อให้การปราบปรามตลาดมืดออนไลน์เป็นไปอย่างมีประสิทธิภาพ และจำกัดขอบเขตการแพร่ขยายของการฉ้อโกงทางโทรคมนาคมและออนไลน์ จึงได้มีการแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ ๙) ซึ่งประกาศใช้ในเดือนสิงหาคม ค.ศ. ๒๐๑๕ โดยได้บัญญัติความผิดฐาน “การช่วยเหลือกิจกรรมอาชญากรรมที่เกี่ยวข้องกับเครือข่ายสารสนเทศ” (the crime of assisting with information network-related criminal activities) และบัญญัติให้ผู้ใดซึ่งรู้อยู่แล้วว่าบุคคลอื่นกำลังกระทำความผิดโดยใช้เครือข่ายสารสนเทศ และได้ให้การสนับสนุนหรือช่วยเหลือในการกระทำความผิดนั้น หากมีลักษณะร้ายแรง ต้องรับผิดทางอาญา ต่อมา ในเดือนตุลาคม ค.ศ. ๒๐๑๙ ศาลประชาชนสูงสุดและสำนักงานอัยการสูงสุดได้ร่วมกันออกคำอธิบายเกี่ยวกับการตีความบางประการในการใช้กฎหมายว่าด้วยการดำเนินคดีอาญาที่เกี่ยวข้องกับความผิดฐานใช้เครือข่ายสารสนเทศโดยมิชอบ หรือให้การช่วยเหลือกิจกรรมอาชญากรรมที่เกี่ยวข้องกับเครือข่ายสารสนเทศ เพื่อกำหนดมาตรฐานการลงโทษสำหรับความผิดดังกล่าวและการบังคับใช้กฎหมายที่เกี่ยวข้องซึ่งได้กลายเป็นฐานอำนาจทางกฎหมายที่สำคัญสำหรับเจ้าหน้าที่ตำรวจจีนในการปราบปรามและควบคุมตลาดมืดออนไลน์และอาชญากรรมที่เกี่ยวข้องกับการฉ้อโกงทางโทรคมนาคมและออนไลน์ นอกจากนี้ ในเดือนตุลาคม ค.ศ. ๒๐๒๐ กระทรวงความมั่นคงสาธารณะของจีนได้เปิดตัว “ปฏิบัติการตัดบัตร” (card cutting campaign) อีกทั้งเจ้าหน้าที่ตำรวจทั่วประเทศได้ปราบปรามผู้กระทำความผิดจำนวนมากที่มีการซื้อขาย ให้เช่า และให้ยืมบัตรโทรศัพท์ บัตรธนาคาร และบัญชีอินเทอร์เน็ตโดยมิชอบ โดยอาศัยมาตรฐานของความผิดดังกล่าวตามกฎหมาย ซึ่งอัยการและผู้พิพากษาได้ดำเนินการฟ้องร้องและพิจารณาคดีต่อกลุ่มผู้กระทำความผิดโดยใช้มาตรฐานของความผิดดังกล่าวเช่นกัน การดำเนินการเหล่านี้มีส่วนอย่างมากในการส่งเสริมการปราบปราม

^๗ Ministry of Public Security of the People's Republic of China, “Legal System Construction Improved to Punish Illegal and Criminal Activities Related to Telecom and Online Fraud According to Law”, 2023-3-16, สืบค้นเมื่อวันที่ ๓๐ เมษายน ๒๕๖๙, จาก <https://www.mps.gov.cn/n2255079/n6865805/n7355748/n7355818/c8924716/content.html>

และควบคุมการฉ้อโกงทางโทรคมนาคมและออนไลน์ตั้งแต่ต้นทางทำให้จำนวนคดีฉ้อโกงทางโทรคมนาคมและออนไลน์ลดลงอย่างต่อเนื่อง

๒.๓ แนวทางการใช้บังคับกฎหมาย^๔ ศาลประชาชนสูงสุด สำนักงานอัยการสูงสุด และกระทรวงความมั่นคงสาธารณะ ได้ร่วมกันจัดทำแนวทางการใช้บังคับกฎหมาย (Legal guiding opinions) รวมสองฉบับในเดือนธันวาคม ค.ศ. ๒๐๑๖ และเดือนมิถุนายน ค.ศ. ๒๐๒๑ ตามลำดับ เพื่อใช้เป็นแนวปฏิบัติในการกำหนดมาตรฐานการใช้กฎหมายในการดำเนินคดีที่เกี่ยวข้องกับการฉ้อโกงทางโทรคมนาคมและออนไลน์ และเพื่อแก้ไขปัญหาสำคัญที่ปรากฏโดยทั่วไปในทางปฏิบัติของกระบวนการยุติธรรม โดยเอกสารแนวทางทั้งสองฉบับได้เน้นย้ำถึงการลงโทษการกระทำที่ผิดกฎหมายและอาชญากรรมที่เกี่ยวข้องกับการฉ้อโกงทางโทรคมนาคมและออนไลน์อย่างเคร่งครัด ครอบคลุม และถูกต้องตามกฎหมาย สรุปสาระสำคัญได้ดังนี้

๑. กำหนดมาตรฐานขั้นต่ำในการลงโทษทางอาญา และการรอลงอาญาอย่างเข้มงวด โดยกำหนดว่า การฉ้อโกงทางโทรคมนาคมและออนไลน์ที่เกี่ยวข้องกับทรัพย์สินสาธารณะหรือเอกชน หากมีมูลค่าไม่น้อยกว่า ๓๐,๐๐๐ หยวน ให้ถือเป็นความผิดอาญา สำหรับจำเลยที่กระทำความผิดเกี่ยวกับการฉ้อโกงทางโทรคมนาคมและออนไลน์ การใช้โทษรอลงอาญาจะถูกควบคุมอย่างเข้มงวด และเงื่อนไขในการใช้โทษรอลงอาญาจะต้องถูกกำหนดและบังคับใช้อย่างเคร่งครัด

๒. กำหนดสถานการณ์ที่ต้องลงโทษหนักขึ้น ได้แก่ กรณีที่การฉ้อโกงทำให้ผู้เสียหายฆ่าตัวตายหรือเสียชีวิต การฉ้อโกงโดยแอบอ้างเป็นเจ้าของที่ตุลาการหรือหน่วยงานของรัฐ การฉ้อโกงในต่างประเทศ การฉ้อโกงทรัพย์สินจากผู้พิการ ผู้สูงอายุ ผู้เยาว์ และนักเรียน และการสั่งการหรือการควบคุมแก๊งฉ้อโกงทางโทรคมนาคมและออนไลน์ (directing a telecom and online fraud gang)

๓. กำหนดให้มีการปราบปรามความผิดที่เกี่ยวข้อง โดยกำหนดโทษสำหรับความผิดต้นทางและปลายทางที่เกี่ยวข้องกับการฉ้อโกงทางโทรคมนาคมและออนไลน์ เช่น การละเมิดข้อมูลส่วนบุคคลของประชาชน การช่วยเหลือกิจกรรมอาชญากรรมที่เกี่ยวข้องกับเครือข่ายสารสนเทศ การปกปิดหรือซ่อนเร้นทรัพย์สินที่ได้มาจากการกระทำความผิด

๔. มุ่งเน้นการแก้ไขปัญหาการฉ้อโกงทางโทรคมนาคมและออนไลน์ข้ามพรมแดน โดยกำหนดว่า หากบุคคลใดเดินทางไปต่างประเทศเพื่อเข้าร่วมแก๊งฉ้อโกงทางโทรคมนาคมและออนไลน์ และพักอยู่ในแหล่งกบดานในต่างประเทศ (the overseas hideout) รวมกันเกินกว่าสามสิบวันภายในหนึ่งปี หรือเดินทางออกนอกประเทศไปยังแหล่งกบดานฉ้อโกงหลายครั้ง (repeatedly leaves) บุคคลนั้นจะต้องรับผิดชอบทางอาญาในความผิดฐานฉ้อโกงหรือพยายามฉ้อโกง

๕. มุ่งเน้นการแก้ไขปัญหาการใช้กฎหมายที่เกี่ยวข้องกับความผิดเกี่ยวกับบัตรโทรศัพท์และบัตรธนาคาร โดยกำหนดว่า การซื้อขายหรือให้เช่าบัตรธนาคารเกินกว่าห้าใบ หรือการซื้อขายหรือให้เช่าบัตรโทรศัพท์ บัตรข้อมูล หรือบัตรหรือซิมการ์ดที่ใช้เชื่อมต่ออุปกรณ์อินเทอร์เน็ต (Internet of things

^๔ Ministry of Public Security of the People's Republic of China, "Legal System Construction Improved to Punish Illegal and Criminal Activities Related to Telecom and Online Fraud According to Law", 2023-3-16, สืบค้นเมื่อวันที่ ๓๐ เมษายน ๒๕๖๕, จาก <https://www.mps.gov.cn/n2255079/n6865805/n7355748/n7355818/c8924716/content.html>

cards) ของบุคคลอื่นเกินกว่ายี่สิบใบ ถือเป็นความผิดฐานช่วยเหลือกิจกรรมอาชญากรรมที่เกี่ยวข้องกับเครือข่ายสารสนเทศ

๖. เอกสารแนวทางทั้งสองฉบับยึดถือนโยบายโทษทางอาญาที่ผสมผสานความผ่อนปรนกับความเข้มงวด (combining leniency with rigidity) โดยกำหนดให้ผู้จัดตั้ง ผู้วางแผน ผู้สั่งการ และสมาชิกแกนหลักของแก๊งค์ช่องทางโทรคมนาคมและออนไลน์ ต้องได้รับโทษหนักตามกฎหมายสำหรับผู้สมรู้ร่วมคิด (the accomplices) ผู้กระทำความผิดครั้งแรก ผู้กระทำความผิดเป็นครั้งคราว (occasional offenders) ผู้เยาว์ และนักเรียน จะได้รับโทษเบาหรือได้รับการลดหย่อนโทษตามกฎหมาย

บทสรุป

การขยายตัวของกลุ่มแก๊งค์และกลุ่มแฮกเกอร์และการปราบปรามในประเทศจีนสะท้อนให้เห็นถึงความท้าทายและเทคโนโลยีที่ซับซ้อนในยุคดิจิทัล ซึ่งกลไกการบริหารจัดการไม่อาจพึ่งพาเพียงมาตรการใดมาตรการหนึ่ง แต่ต้องอาศัยการบูรณาการระหว่างการบังคับใช้กฎหมายที่มีประสิทธิภาพ ความร่วมมือระหว่างประเทศ และการสร้างความตระหนักรู้ให้แก่ประชาชน โดยเฉพาะอย่างยิ่งกลุ่มเปราะบาง การปรับปรุงบทบัญญัติของกฎหมายหรือการมีกฎหมายเฉพาะเพื่อให้ทันต่ออาชญากรรมทางโทรคมนาคมและออนไลน์ที่เปลี่ยนแปลงไปอย่างรวดเร็วเป็นสิ่งจำเป็น เพื่อสร้างความเชื่อมั่นว่าผู้กระทำความผิดจะถูกลงโทษดำเนินคดีอย่างจริงจัง อย่างไรก็ตาม การแก้ไขปัญหาไม่อาจอาศัยเพียงการปราบปราม แต่ต้องสร้างระบบนิเวศดิจิทัลที่ปลอดภัยและยั่งยืนผ่านความร่วมมือจากทุกภาคส่วนทั้งภายในและระหว่างประเทศ เพื่อลดความสูญเสียจากภัยคุกคามดังกล่าวที่สร้างความเสียหายอย่างมหาศาล และบางกรณีรุนแรงถึงขั้นนำไปสู่การสูญเสียชีวิต สังคมโลกจึงควรตระหนักถึงความสำคัญของปัญหาเหล่านี้และร่วมมือกันอย่างจริงจัง เพื่อให้การใช้ประโยชน์จากเทคโนโลยีเป็นไปอย่างมั่นคงปลอดภัยและลดผลกระทบเชิงลบที่มีต่อสังคม

สาธารณรัฐเกาหลี (เกาหลีใต้)*

๑. บทนำ

สาธารณรัฐเกาหลี (เกาหลีใต้) ได้ชื่อว่าเป็นประเทศที่สร้างสภาพแวดล้อมของโลกไซเบอร์ (cyberspace) ที่ก้าวหน้ามากที่สุดแห่งหนึ่งของโลก ทั้งในเรื่องเทคโนโลยีสารสนเทศและการสื่อสาร (information and communications technology (ICT)) และโครงสร้างพื้นฐานที่เกี่ยวข้องกับเทคโนโลยีดังกล่าว ในปัจจุบันนี้ cyberspace มีความสำคัญต่อชีวิตประจำวัน การดำเนินกิจกรรมทางเศรษฐกิจ การประกอบธุรกิจ การดำเนินงานของภาครัฐ และการให้บริการพื้นฐาน แต่โดยที่การเชื่อมต่อระหว่างอุปกรณ์ด้านสารสนเทศและการสื่อสารมีความหลากหลาย และ cyberspace มีความซับซ้อนเพิ่มมากขึ้นและทำให้ยากต่อการจัดการเพื่อให้เกิดความปลอดภัย อีกทั้ง cyberspace มีลักษณะเป็นเทคโนโลยีไร้พรมแดนทำให้เกิดความสับสนเสี่ยงที่จะใช้เพื่อเป็นภัยคุกคามต่อโลกไซเบอร์ได้ ในอดีตที่ผ่านมา กลุ่มผู้ก่อการร้ายได้นำเทคโนโลยีไซเบอร์เป็นเครื่องมือในการมุ่งประสงค์จะก่ออาชญากรรมไซเบอร์ขยายในวงกว้างเนื่องจากได้รับการสนับสนุนจากผู้มีบทบาทในระดับรัฐและวิธีการโจมตีก็มีความหลากหลายมากขึ้นทั้งในรูปแบบของการขโมยข้อมูลและทรัพย์สินเงินทองรวมถึงการสร้างควมวุ่นวายให้สังคมเกิดความไม่สงบสุขโดยมุ่งเป้าไปยังวัตถุประสงค์ทางการเมืองและทำลายโครงสร้างพื้นฐานของประเทศ การก่ออาชญากรรมไซเบอร์มีแนวโน้มที่จะรุนแรงขึ้นเป็นสงครามไซเบอร์ (cyber war) ซึ่งอาจสร้างความเสียหายได้รุนแรงเทียบเท่ากับการโจมตีด้วยอาวุธยุทโธปกรณ์ในรูปแบบที่มีมาแต่ดั้งเดิม

ข้อพิพาททางการเมือง เศรษฐกิจ และการทหารระหว่างประเทศ เป็นปัจจัยที่นำไปสู่ความขัดแย้งในโลกไซเบอร์ และรัฐบาลของประเทศต่าง ๆ ได้สนับสนุนงบประมาณเพื่อพัฒนาเทคโนโลยีไซเบอร์ให้มีความทันสมัยโดยอาศัยปัญญาประดิษฐ์และการวิเคราะห์ข้อมูลขนาดใหญ่ หรือ big data รวมทั้งการเสริมสร้างขีดความสามารถในการจัดเก็บข้อมูลความล้าสมัยด้านไซเบอร์ การก่อกวนเครือข่ายอินเทอร์เน็ต และการคุกคามสิ่งอำนวยความสะดวกที่สำคัญ อีกทั้งอาชญากรรมไซเบอร์ยังคงสร้างความเสียหายต่อภาคธุรกิจและประชาชนอย่างต่อเนื่องอันเนื่องมาจากความก้าวหน้าทางเทคโนโลยีและความซับซ้อนที่เพิ่มขึ้นของการโจมตีทางไซเบอร์ เช่น การโจรกรรมข้อมูลส่วนบุคคล การเข้ามามีส่วนเกี่ยวข้องของกลุ่มผู้มีอำนาจในระดับรัฐและกลุ่มก่อการร้ายยังเป็นปัจจัยสำคัญที่ก่อความเสียหายจากอาชญากรรมไซเบอร์ให้รุนแรงและร้ายแรงยิ่งขึ้นอันนำไปสู่ความเสียหายต่อความมั่นคงของประเทศ ด้วยเหตุนี้ทำให้เกาหลีใต้กำหนดนโยบายและมาตรการทางกฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมการหลอกลวงทางไซเบอร์เพื่อปกป้องผลประโยชน์ของประเทศชาติและทรัพย์สินของประชาชนของตนอย่างจริงจังและต่อเนื่อง^๑

* จัดทำโดยนางสาววารีรัตน์ รัตนวิบูลย์สม นักกฎหมายกฤษฎีกาชำนาญการพิเศษ ฝ่ายกฎหมายกระบวนการยุติธรรมทางแพ่ง กองกฎหมายกระบวนการยุติธรรม

^๑ CHEONG WA DAE, “National Cybersecurity Strategy”, National Security Office: April 2019, pp. 6-8.

๒. แนวนโยบายของรัฐในการป้องกันและปราบปรามไซเบอร์

รัฐบาลเกาหลีใต้ได้จัดทำยุทธศาสตร์ความมั่นคงทางไซเบอร์แห่งชาติ (National Cybersecurity Strategy)^๒ โดยมีวิสัยทัศน์เพื่อสร้าง cyberspace ให้เป็นพื้นที่เสรีและปลอดภัย สร้างความมั่นคงทางเศรษฐกิจ และสนับสนุนให้เกิดสันติภาพระหว่างประเทศ เพื่อนำไปสู่เป้าหมายดังต่อไปนี้

๑. สร้างความเชื่อมั่นในการดำเนินงานของรัฐ (Ensure stable operations of the state): เสริมสร้างความมั่นคงและความพร้อมในด้านโครงสร้างพื้นฐานที่จำเป็นของประเทศเพื่อการดำเนินงานที่ต่อเนื่องแม้อยู่ในสถานการณ์ที่ต้องเผชิญกับการคุกคามทางไซเบอร์

๒. การตอบสนองต่อการโจมตีทางไซเบอร์ (Respond to cyber attacks) เพิ่มขีดความสามารถด้านความมั่นคงเพื่อยับยั้งภัยคุกคามทางไซเบอร์ ตรวจจับและสกัดกั้นการคุกคามทางไซเบอร์ได้อย่างรวดเร็วและตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างทันท่วงที

๓. เสริมสร้างความเข้มแข็งด้านความมั่นคงทางไซเบอร์ (Build a strong cybersecurity foundation) ส่งเสริมให้เทคโนโลยีไซเบอร์ ทรัพยากรมนุษย์ และอุตสาหกรรม มีความสามารถในการแข่งขัน

ยุทธศาสตร์ความมั่นคงทางไซเบอร์แห่งชาติประกอบด้วยหลักการพื้นฐานที่สำคัญได้แก่

๑. สร้างความสมดุลระหว่างสิทธิส่วนบุคคลและความมั่นคงทางไซเบอร์ (Balance individual rights with cybersecurity) การสร้างความสมดุลให้เกิดขึ้นระหว่างการปกป้องโลกไซเบอร์ และการคุ้มครองสิทธิขั้นพื้นฐานของบุคคล

๒. ดำเนินกิจกรรมด้านความมั่นคงบนพื้นฐานของหลักนิติธรรม (Conduct security activities based on the rule of law) ดำเนินนโยบายและกิจกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ของรัฐบาลอย่างโปร่งใส และสอดคล้องกับหลักกฎหมายภายในประเทศและระหว่างประเทศ

๓. สร้างระบบการมีส่วนร่วมและความร่วมมือ (Build an system of participation and cooperation) ส่งเสริมให้ปัจเจกชน ภาคธุรกิจ และรัฐบาล ร่วมมือดำเนินกิจกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ และมุ่งเน้นความร่วมมืออย่างใกล้ชิดกับประชาคมระหว่างประเทศ

ภารกิจตามที่กำหนดไว้ในยุทธศาสตร์แบ่งออกได้เป็น ๖ ภารกิจ ประกอบด้วย

๑. การเพิ่มความปลอดภัยของโครงสร้างพื้นฐานที่สำคัญระดับชาติ (Increase the Safety of the National Core Infrastructure)

รัฐบาลเกาหลีใต้มุ่งยกระดับเครือข่ายข้อมูลและการติดต่อสื่อสารระดับชาติ โดยมุ่งเน้นความมั่นคงปลอดภัยจากการคุกคามทางไซเบอร์ตลอดทั้งกระบวนการตั้งแต่การติดตั้ง การดำเนินงาน และการทำลาย เพิ่มความยืดหยุ่นและพัฒนาระบบการสำรองข้อมูลให้เกิดความต่อเนื่อง ใช้เทคโนโลยีเข้าสู่รหัสขั้นสูงเพื่อป้องกันข้อมูลรั่วไหล ตลอดจนเตรียมความพร้อมรับมือกับเทคโนโลยียุคใหม่ด้วยการพัฒนาเครือข่ายข้อมูลและสร้างระบบการยืนยันตัวตนที่ปลอดภัยในยุคดิจิทัลปัจจุบัน

^๒ CHEONG WA DAE, “National Cybersecurity Strategy”, National Security Office: April 2019, pp. 12-26.

๒. การยกระดับขีดความสามารถในการตอบโต้การโจมตีทางไซเบอร์ (Enhance Cyber Attack Response Capabilities)

การยกระดับขีดความสามารถในการตอบโต้การโจมตีทางไซเบอร์ของเกาหลีใต้ ประกอบด้วย การดำเนินการทั้งในมิติเชิงรับและเชิงรุก กล่าวคือ นโยบายเชิงรับของรัฐบาล รัฐบาลมีการจัดเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ครั้งใหญ่โดยมีการประเมินและพัฒนาระบบการแบ่งปันข้อมูล การสืบสวนสอบสวน และการมีปฏิริยาตอบโต้ของหน่วยงานที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ดังกล่าวพร้อมทั้งได้เพิ่มขีดความสามารถในการตอบสนองต่อวิกฤตการณ์ทางไซเบอร์ที่เกิดขึ้นให้ครอบคลุมทั่วประเทศ ในส่วนของนโยบายเชิงรุกนั้น รัฐบาลได้จัดการป้องกันเพื่อตอบโต้ภัยคุกคามที่กระทบต่อความมั่นคงของประเทศอย่างจริงจังและเพิ่มขีดความสามารถในการวิเคราะห์สาเหตุของการโจมตีและสืบหาตัวผู้กระทำผิด อีกทั้งการกำหนดให้มีมาตรการตอบโต้เชิงรุกโดยการพัฒนายุทธศาสตร์และกำลังพลทางทหารเพื่อคุ้มกันความมั่นคงของประเทศ ผักผ่อนทักษะความเชี่ยวชาญเฉพาะด้าน และเสริมสร้างขีดความสามารถในการสืบสวนสอบสวนและจับกุมตัวผู้กระทำความผิดและการดำเนินคดีอย่างมีประสิทธิภาพ

๓. การกำหนดหลักธรรมาภิบาลบนพื้นฐานของความไว้วางใจและความร่วมมือ (Establish Governance Based on Trust and Cooperation)

โดยอาศัยการประสานความร่วมมือระหว่างภาครัฐ เอกชน และทหาร เพื่อสร้างระบบการบริหารจัดการโดยมีสำนักงานสภาความมั่นคงแห่งชาติ (National Security Office) เป็นหน่วยงานกำกับดูแลความร่วมมือดังกล่าว รวมทั้งพัฒนาและนำนโยบายความมั่นคงทางไซเบอร์ไปปรับใช้ร่วมกันเป็นแผนระดับชาติ นอกจากนี้ มีการสร้างระบบแบ่งปันข้อมูลทั่วประเทศเพื่อมุ่งเน้นการส่งผ่านข้อมูลร่วมกันทุกภาคส่วนเพื่อป้องกันการเผยแพร่ข้อมูลเท็จเกี่ยวกับการคุกคามทางไซเบอร์ รวมถึงการเสริมสร้างมาตรการทางกฎหมายเพื่อรองรับการดำเนินการด้านความมั่นคงทางไซเบอร์ซึ่งอาจอยู่ในรูปแบบของการปรับปรุงกฎหมายและร่วมมือกับสถาบันหรือหน่วยงานที่เกี่ยวข้องเพื่อรับมือกับภัยคุกคามหรือความท้าทายที่อาจเกิดขึ้นใหม่ เช่น การอุดช่องโหว่จากการใช้เทคโนโลยี AI

๔. การวางรากฐานรองรับการเติบโตของอุตสาหกรรมความมั่นคงทางไซเบอร์ (Build Foundations for Cybersecurity Industry Growth)

ขยายการลงทุนด้านความมั่นคงทางไซเบอร์ทั้งในด้านการปฏิรูปกฎหมาย เพิ่มงบประมาณของรัฐเพื่อใช้ในกรณีที่มีเหตุฉุกเฉิน ใช้มาตรการทางภาษีจูงใจภาคเอกชนให้ลงทุนด้านความมั่นคงและการวิจัยและพัฒนา (R&D) เสริมสร้างขีดความสามารถในการแข่งขันของบุคลากรและเทคโนโลยี ส่งเสริมสภาพแวดล้อมเพื่อการเติบโตของบริษัทด้านความมั่นคงทางไซเบอร์ และกำหนดหลักเกณฑ์การแข่งขันที่เป็นธรรมในตลาดด้านความมั่นคงทางไซเบอร์

๕. การปลูกฝังวัฒนธรรมความมั่นคงทางไซเบอร์ (Foster a Cybersecurity Culture)

การสร้างตระหนักรู้และแนวปฏิบัติเกี่ยวกับความมั่นคงทางไซเบอร์โดยมุ่งเน้นการพัฒนาและการประยุกต์ใช้กฎระเบียบในชีวิตประจำวันได้จริง การจัดหลักสูตรการเรียนการสอนเกี่ยวกับจริยธรรมในการใช้ไซเบอร์ในกลุ่มนักเรียน นักศึกษา เจ้าหน้าที่ของรัฐ ทหาร และพนักงานบริษัท

การสร้างจิตสำนึกให้กับภาคธุรกิจให้รับผิดชอบในการรักษาความปลอดภัยของผลิตภัณฑ์และบริการ ตลอดจนการสร้างความสัมพันธ์ระหว่างสิทธิขั้นพื้นฐานและความมั่นคงทางไซเบอร์เพื่อสร้างความเชื่อมั่นว่าภาครัฐจะไม่เข้าแทรกแซงหรือละเมิดสิทธิของประชาชนโดยผิดกฎหมาย

๖. การเป็นผู้นำความร่วมมือระหว่างประเทศด้านความมั่นคงทางไซเบอร์ (Lead International Cooperation in Cybersecurity)

การเสริมสร้างระบบความร่วมมือระหว่างประเทศทั้งในรูปแบบทวิภาคีและพหุภาคี รวมถึงการกระชับความสัมพันธ์ร่วมกับองค์การระหว่างประเทศและการเข้าเป็นภาคีความตกลงระหว่างประเทศโดยมีกรอบความร่วมมือครอบคลุมทั้งด้านความมั่นคง การบังคับใช้กฎหมาย การร่วมมือกับภาคเอกชน เพื่อรับมือกับภัยคุกคาม สงคราม การก่อการร้าย และอาชญากรรม พร้อมทั้งมีการแบ่งปันข้อมูลระหว่างกันผ่านกลไกความร่วมมือระหว่างประเทศ การสร้างความเป็นผู้นำความร่วมมือระหว่างประเทศยังช่วยเพิ่มการมีส่วนร่วมในการจัดทำกฎระเบียบระหว่างประเทศร่วมกันด้านความมั่นคงทางไซเบอร์และนำไปสู่การเผยแพร่หลักเกณฑ์และแนวปฏิบัติที่ดีที่สุด (best practices) ในอนาคต รวมทั้งยังเพิ่มการมีส่วนร่วมในการสร้างความเชื่อมั่นสำหรับการป้องกันภัยคุกคามอันเนื่องมาจากความเข้าใจผิดในโลกไซเบอร์และพัฒนาขีดความสามารถด้านความมั่นคงทางไซเบอร์ให้แก่กลุ่มประเทศกำลังพัฒนาด้วยการแบ่งปันเทคโนโลยีและระบบความมั่นคงทางไซเบอร์

แผนการดำเนินงานตามยุทธศาสตร์

รัฐบาลเกาหลีใต้ได้ระบุในแผนการดำเนินงานตามยุทธศาสตร์ว่าจะปฏิบัติหน้าที่ตามความรับผิดชอบและแสดงภาวะความเป็นผู้นำเพื่อให้บรรลุผลสำเร็จตามวิสัยทัศน์และเป้าหมายของ “ยุทธศาสตร์ความมั่นคงทางไซเบอร์แห่งชาติ (National Cybersecurity Strategy)” โดยจะร่วมมือกับภาคประชาชนและภาคธุรกิจตลอดจนประชาคมระหว่างประเทศ ทั้งนี้ รัฐบาลจะออกแผนงานที่สำคัญเพิ่มเติม ๒ แผนงาน ได้แก่ ๑. แผนพื้นฐานความมั่นคงทางไซเบอร์แห่งชาติ (National Cybersecurity Basic Plan) และ ๒. แผนการดำเนินงานด้านความมั่นคงทางไซเบอร์แห่งชาติ (National Cybersecurity Implementation Plan) เพื่อให้แผนยุทธศาสตร์มีผลเป็นรูปธรรม ทุกกระทรวงและทุกหน่วยงานมีหน้าที่ดำเนินการตามเป้าหมายที่กำหนดไว้ในยุทธศาสตร์ ปฏิบัติตามหลักการพื้นฐาน และปฏิบัติการเชิงยุทธศาสตร์ในการสนับสนุนให้มีกฎหมาย สถาบัน และนโยบาย ที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ นอกจากนี้ National Security Office มีหน้าที่ติดตามตรวจสอบการดำเนินงานตามยุทธศาสตร์และการตรวจสอบด้านการใช้จ่ายงบประมาณของบุคลากรและองค์กรต่าง ๆ เพื่อสร้างความน่าเชื่อถือและความโปร่งใสให้สาธารณชนได้รับทราบอย่างต่อเนื่อง

๓. มาตรการทางกฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมการหลอกลวงทางไซเบอร์

กฎหมายและกฎระเบียบเป็นสิ่งจำเป็นต่อการจัดทำมาตรการตอบโต้การคุกคามทางไซเบอร์ในอนาคตให้เกิดประสิทธิภาพ เกาหลีใต้เป็นหนึ่งในประเทศที่ตรากฎหมายหลายฉบับที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ เช่น Special Act on the Prevention of telecommunications-Based Financial Fraud and Refund of Fraudulently Obtained Assets, National Information Framework Act, Act on the Promotion of Information and Communications, Act on the Protection of Information and Communications Infrastructure หรือ Electronic Government

Act เป็นต้น กฎหมายหลายฉบับได้มีการปรับปรุงแก้ไขเพิ่มเติมในเวลาต่อมาเพื่อให้เหมาะสมกับสถานการณ์ปัจจุบันซึ่งเป็นสิ่งสะท้อนนโยบายและการกำกับดูแลระดับประเทศที่มีต่อความมั่นคงทางไซเบอร์อย่างมีประสิทธิภาพ สรุปได้ดังนี้^๓

๑. Special Act on the Prevention of Telecommunications-Based Financial Fraud and Refund of Fraudulently Obtained Assets^๔

วัตถุประสงค์^๕

กฎหมายพิเศษว่าด้วยการป้องกันการฉ้อโกงทางการเงินผ่านทางโทรคมนาคมและการคืนทรัพย์สินที่ได้มาโดยมิชอบจากการฉ้อโกงมีวัตถุประสงค์เพื่อกำหนดมาตรการของรัฐในการป้องกันความสูญเสียและกำหนดความรับผิดชอบของสถาบันการเงินในการป้องกันความสูญเสีย เพื่อบ่งหมายที่จะป้องกันการฉ้อโกงทางการเงินผ่านทางโทรคมนาคม อีกทั้งยังได้กำหนดขั้นตอนการระงับสิทธิเรียกร้อง (extinguishment of claims) ต่อบัญชีที่ถูกฉ้อโกง ขั้นตอนการเรียกร้องค่าชดเชยความเสียหาย เพื่อชดเชยความสูญเสียให้แก่ผู้เสียหายจากการฉ้อโกงทางการเงินผ่านโทรคมนาคมและช่วยเยียวยาให้ผู้เสียหายสามารถฟื้นฟูความสูญเสียทางทรัพย์สินได้อย่างรวดเร็ว

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

๑.๑ บทนิยามคำว่า “การฉ้อโกงทางการเงินผ่านทางโทรคมนาคม (telecommunications-based financial fraud)” หมายความว่า การกระทำใดที่มุ่งหมายเพื่อให้ตนเองหรือบุคคลที่สามได้รับประโยชน์ในรูปของเงินหรือผลประโยชน์ทางเศรษฐกิจ โดยการฉ้อโกงหรือกรรโชกทรัพย์สินจากบุคคลอื่นผ่านระบบโทรคมนาคม และคำว่า “ธุรกรรมทางการเงินอิเล็กทรอนิกส์ (electronic financial transaction)” หมายความว่า ธุรกรรมที่สถาบันการเงินให้บริการแก่ผู้ใช้บริการผ่านผลิตภัณฑ์ทางการเงินหรือผ่านอุปกรณ์อิเล็กทรอนิกส์โดยไม่มีการพบปะหรือสื่อสารโดยตรงกับพนักงานบริษัท

๑.๒ การตอบโต้การฉ้อโกงผ่านระบบโทรคมนาคม (มาตรา ๒-๒) Financial Services Commission (FSC) มีหน้าที่ในการจัดเตรียมมาตรการป้องกันและลดการสูญเสียความเสียหายที่เกิดจากการฉ้อโกงผ่านทางโทรคมนาคม เช่น รวบรวมและเผยแพร่ข้อมูลการฉ้อโกงทางการเงินผ่านทางโทรคมนาคม ตลอดจนเมื่อมีเหตุจำเป็นเพื่อป้องกันการฉ้อโกงทางการเงินผ่านทางโทรคมนาคม FSC อาจ

^๓ Santiago Paz et al., “Executive Summary”, National Cybersecurity Law, Governance, and Infrastructure: IN THE REPUBLIC OF KOREA: 2024, pp. VIII-IX.

^๔ Act No. 19418, May 16, 2023

^๕ Article 1 (Purpose)

The purpose of this Act is to prescribe Government measures to prevent loss and financial companies' responsibilities for the prevention of loss in an attempt to prevent telecommunications-based financial fraud, and to stipulate procedures for extinguishment of claims for accounts exploited for fraud, procedures for the compensation of loss, etc. in order to compensate loss to victims of telecommunications-based financial fraud so as to contribute to the prevention of telecommunications-based financial fraud and rapid recovery of property loss of victims.

ให้คำแนะนำ ร้องขอ หรือออกคำสั่งให้สถาบันการเงินปรับปรุงแผนการดำเนินงานโดยพิจารณาจากจำนวนเงินชดเชยความสูญเสียที่จ่ายไปในแต่ละปีและจำนวนครั้งของบัญชีที่ถูกใช้ในการฉ้อโกง

๑.๓ การจำกัดธุรกรรมทางการเงินอิเล็กทรอนิกส์ (มาตรา ๑๓-๒) กำหนดให้ Financial Supervisory Service (FSS) มีอำนาจกำหนดให้เจ้าของบัญชี (บัญชีม้า) เป็น “บุคคลซึ่งถูกจำกัดการทำธุรกรรมทางการเงินอิเล็กทรอนิกส์ (person subject to restriction of electronic financial transactions)” หากบุคคลดังกล่าวมีลักษณะเข้าหลักเกณฑ์ดังต่อไปนี้

(๑) โอนหรือให้ยืมช่องทางเข้าถึงบัญชี เช่น ให้ยืมบัตร ATM หรือรหัสผ่าน โดยยังไม่พ้นกำหนด ๓ ปี (สำหรับโทษปรับ) หรือ ๕ ปี (สำหรับโทษจำคุกหรือรอลงอาญา)

(๒) ให้ข้อมูลบัญชีเพื่อใช้ในการฉ้อโกง

(๓) กระทำความผิดฐานฉ้อโกงโดยตรงและยังไม่พ้นกำหนด ๓ ปี (สำหรับโทษปรับ) หรือ ๕ ปี (สำหรับโทษจำคุกหรือรอลงอาญา)

๑.๔ การระงับการใช้หมายเลขโทรศัพท์ (มาตรา ๑๓-๓) กรณีที่มีการตรวจสอบพบหมายเลขโทรศัพท์ถูกใช้ในการฉ้อโกงทางการเงิน หน่วยงานที่เกี่ยวข้องอาจยื่นคำร้องขอให้รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์และเทคโนโลยีสารสนเทศและการสื่อสาร (Minister of Science and ICT) (เรียกว่า รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์และ ICT) ระงับการให้บริการโทรคมนาคมสำหรับหมายเลขโทรศัพท์นั้นได้

๒. Act on Promotion of Information and Communications Network Utilization and Information Protection^๖

วัตถุประสงค์^๗

กฎหมายว่าด้วยการส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลและการสื่อสาร และการคุ้มครองข้อมูล (หรือเรียกว่า กฎหมายเครือข่ายสารสนเทศและการสื่อสาร) มีวัตถุประสงค์เพื่อพัฒนาคุณภาพชีวิตของประชาชนและส่งเสริมสวัสดิการแห่งรัฐด้วยการสนับสนุนการใช้ประโยชน์จากเครือข่ายข้อมูลและการสื่อสาร การคุ้มครองประชาชนผู้ใช้บริการเครือข่าย และปรับปรุงสภาพแวดล้อมที่เอื้อให้ประชาชนสามารถใช้ประโยชน์จากเครือข่ายข้อมูลและการสื่อสารได้อย่างเหมาะสมและปลอดภัยยิ่งขึ้น

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

๑.๑ บทนิยามคำว่า “เหตุภัยคุกคามต่อความปลอดภัยคอมพิวเตอร์ (computer security incident)” (มาตรา ๒) หมายความว่า เหตุการณ์ที่เกิดขึ้นเนื่องมาจากการโจมตีเครือข่าย

^๖ Act No. 20069, Jan. 23, 2024.

^๗ Article 1 (Purpose)

The purpose of this Act is to contribute to improving citizens' lives and enhancing public welfare by facilitating utilization of information and communications networks, protecting people using information and communications services, and developing an environment in which people can utilize information and communications networks in a healthier and safer way. <Amended on Feb. 4, 2020>

ข้อมูลสารสนเทศและการสื่อสารหรือระบบข้อมูลที่เกี่ยวข้องกับเครือข่ายดังกล่าว เช่น การขโมยข้อมูลหรือการติดตั้งโปรแกรมที่ข้ามขั้นตอนการป้องกันตามปกติที่ต้องดำเนินการ

๑.๒ ความรับผิดชอบของผู้ให้บริการและผู้ให้บริการข้อมูลสารสนเทศและการสื่อสาร (มาตรา ๓) ผู้ให้บริการข้อมูลสารสนเทศทุกคนมีหน้าที่คุ้มครองสิทธิและผลประโยชน์ของผู้ใช้บริการ และมีความช่วยเหลือในการสร้างสรรค์สังคมสารสนเทศที่เหมาะสม โดยรัฐบาลอาจสนับสนุนองค์กรที่ประกอบด้วยผู้ให้บริการและผู้ให้บริการข้อมูลสารสนเทศและการสื่อสารเพื่อคุ้มครองข้อมูลและปกป้องเยาวชนในเครือข่ายสารสนเทศและการสื่อสารดังกล่าว

๑.๓ การกำหนดนโยบายส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลสารสนเทศและการสื่อสาร และการคุ้มครองข้อมูลสารสนเทศ (มาตรา ๔) รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์และ ICT หรือคณะกรรมการการสื่อสารแห่งชาติ (Korea Communications Commission) มีหน้าที่กำหนดนโยบายเพื่อวางรากฐานรองรับสังคมสารสนเทศโดยผ่านการส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลสารสนเทศ บริหารจัดการและดำเนินการดำเนินงานเครือข่ายดังกล่าวอย่างมีประสิทธิภาพ และคุ้มครองผู้ใช้บริการ โดยนโยบายที่รัฐมนตรีกำหนดนั้นต้องมีรายละเอียดเกี่ยวกับการพัฒนาและการเผยแพร่เทคโนโลยีที่เกี่ยวข้องกับเครือข่ายข้อมูลสารสนเทศและการสื่อสาร การกำหนดมาตรฐานของเครือข่ายข้อมูลสารสนเทศและการสื่อสาร การส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลสารสนเทศและการสื่อสาร การสนับสนุนการแบ่งปันข้อมูลผ่านเครือข่ายข้อมูลสารสนเทศและการสื่อสาร การส่งเสริมใช้งานอินเทอร์เน็ต การคุ้มครองเยาวชนในเครือข่ายข้อมูลสารสนเทศและการสื่อสาร การพัฒนาและการเผยแพร่เทคโนโลยีที่ตรวจจับเสียง ภาพ ภาพนิ่ง หรือสิ่งอื่นใดอันเป็นเท็จที่สร้างขึ้นโดยเทคโนโลยีปัญญาประดิษฐ์หรือ AI การยกระดับความปลอดภัยและความน่าเชื่อถือของเครือข่ายข้อมูลสารสนเทศและการสื่อสาร รวมทั้งเรื่องอื่นที่จำเป็นสำหรับการส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลสารสนเทศและการสื่อสารและการคุ้มครองข้อมูลสารสนเทศ โดยนโยบายส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลสารสนเทศและการสื่อสารต้องสอดคล้องกับแผนแม่บทข้อมูลสารสนเทศแห่งชาติตามมาตรา ๖ แห่ง Framework Act on National Information

๑.๔ การพัฒนาเทคโนโลยี (มาตรา ๖) รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์และ ICT อาจมอบหมายให้สถาบันวิจัยที่เกี่ยวข้องตามที่กฎหมายกำหนด ดำเนินโครงการศึกษาวิจัยและพัฒนาความร่วมมือทางเทคนิค การถ่ายทอดเทคโนโลยี การให้คำแนะนำทางเทคนิค เพื่อส่งเสริมการพัฒนาเทคโนโลยีและอุปกรณ์ที่เกี่ยวข้องกับเครือข่ายข้อมูลสารสนเทศและการสื่อสาร โดยรัฐบาลอาจเป็นผู้สนับสนุนงบประมาณแก่สถาบันวิจัยเพื่อดำเนินโครงการศึกษาวิจัยดังกล่าวนี้

๑.๕ มาตรการป้องกันและรักษาความมั่นคงของเครือข่ายข้อมูลสารสนเทศและการสื่อสาร (มาตรา ๔๕ ถึงมาตรา ๔๗) (๑) กำหนดให้ผู้ให้บริการมีหน้าที่กำหนดมาตรการป้องกันเพื่อสร้างเสถียรภาพของข้อมูลโดยมีแนวทางปฏิบัติที่ครอบคลุมทั้งมาตรการด้านกายภาพ ด้านเทคนิค และด้านการบริหาร เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และป้องกันการรั่วไหลหรือดัดแปลงแก้ไขข้อมูลนั้น (๒) กำหนดให้ผู้ให้บริการแต่งตั้ง “เจ้าหน้าที่ด้านความมั่นคงของข้อมูลสารสนเทศระดับสูง (Chief Information Security Officers)” เพื่อบอกหมายให้กำหนดแผนการป้องกัน ตรวจสอบและปรับปรุงข้อกำหนดและแนวปฏิบัติในการป้องกันข้อมูล ระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับการป้องกันข้อมูล ตลอดจนการดูแลความมั่นคงและปลอดภัยของระบบข้อมูล (๓) กำหนดมาตรการการ

คุ้มครองศูนย์ข้อมูล (Data Centers) เพื่อให้การดำเนินงานของสิ่งอำนวยความสะดวกด้านข้อมูลสารสนเทศและการสื่อสารมีเสถียรภาพ และ (๔) กำหนดให้มีการรับรองระบบการจัดการความมั่นคงด้านข้อมูลสารสนเทศ (Certification of Information Security Management Systems) ซึ่งรัฐมนตรีว่าการกระทรวงวิทยาศาสตร์และ ICT อาจให้การรับรองระบบดังกล่าวแก่ผู้ซึ่งปฏิบัติตามมาตรฐานที่กำหนดไว้ครบถ้วน ทั้งนี้ เพื่อสร้างความเชื่อมั่นในเสถียรภาพของเครือข่าย

๑.๖ การห้ามการกระทำผิดทางไซเบอร์ (มาตรา ๔๘ ถึงมาตรา ๔๙-๒) กฎหมายกำหนดห้ามบุคคลใดกระทำการรุกรานหรือบุกรุกเข้ามาในเครือข่ายข้อมูลสารสนเทศและการสื่อสารโดยไม่มีสิทธิหรือกระทำเกินกว่าสิทธิที่ได้รับ รวมทั้งกำหนดห้ามการทำลาย แก้ไข ดัดแปลง หรือปลอมแปลงข้อมูล หรือแพร่กระจายโปรแกรมในลักษณะที่เป็นการขัดขวางการทำงานของระบบ ข้อมูล หรือโปรแกรม นอกจากนี้ กฎหมายได้มุ่งหมายที่จะคุ้มครองความลับโดยกำหนดห้ามบุคคลใดล่วงละเมิด นำไปใช้โดยมิชอบ หรือเปิดเผยข้อมูลของบุคคลอื่นที่จัดเก็บอยู่ในเครือข่ายข้อมูลสารสนเทศและการสื่อสาร รวมทั้งห้ามเก็บรวบรวมข้อมูลของบุคคลอื่นโดยวิธีการหลอกลวงหรือล่อลวงให้บุคคลอื่นให้ข้อมูลผ่านเครือข่าย

๑.๗ การตอบโต้ การรายงาน และการวิเคราะห์ (มาตรา ๔๘-๒ ถึงมาตรา ๔๘-๔) กำหนดให้รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์และ ICT จัดทำมาตรการตอบโต้ต่ออุบัติการณ์ที่เกิดขึ้นเกี่ยวกับความมั่นคงปลอดภัยของคอมพิวเตอร์ เช่น การเตือนภัยหรือจัดทำมาตรการฉุกเฉิน และกำหนดให้ผู้ให้บริการมีหน้าที่รายงานอุบัติการณ์ทางไซเบอร์ที่เกิดขึ้นต่อรัฐมนตรีว่าการกระทรวงวิทยาศาสตร์และ ICT หรือหน่วยงานด้านอินเทอร์เน็ตและความมั่นคงแห่งเกาหลี (Korea Internet and Security Agency) และกำหนดให้มีการวิเคราะห์สาเหตุของการเกิดอุบัติการณ์เพื่อที่จะหยุดยั้งความเสียหายและมีมาตรการที่จำเป็นในการเยียวยาความเสียหายและป้องกันมิให้อุบัติการณ์เกิดขึ้นซ้ำอีก

๑.๘ บทกำหนดโทษ (Penalty Provisions) (มาตรา ๗๐ ถึงมาตรา ๗๖) กำหนดโทษอาญาและโทษปรับทางปกครองไว้สำหรับกรณีกระทำความผิดเกี่ยวกับเครือข่ายข้อมูลสารสนเทศและการสื่อสาร เช่น กำหนดโทษจำคุกไม่เกิน ๗ ปี หรือปรับไม่เกิน ๗๐ ล้านบาท สำหรับความผิดฐานปล่อยโปรแกรมที่มุ่งร้ายต่อเครือข่าย หรือกำหนดโทษปรับทางปกครองไม่เกิน ๓๐ ล้านบาท สำหรับความผิดทางเทคนิค เช่น ไม่แต่งตั้ง Chief Information Security Officers เป็นต้น

๓. Act on the Protection of Information and Communications Infrastructure^๔

วัตถุประสงค์^๕

กฎหมายว่าด้วยการคุ้มครองโครงสร้างพื้นฐานข้อมูลสารสนเทศและการสื่อสารมีวัตถุประสงค์เพื่อให้โครงสร้างพื้นฐานด้านข้อมูลสารสนเทศและการสื่อสารสามารถดำเนินงานได้อย่างมีเสถียรภาพโดยกำหนดรูปแบบและดำเนินมาตรการต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองโครงสร้างพื้นฐานดังกล่าว

^๔ Act No. 20068, Jan. 23, 2024

^๕ Article 1 (Purpose)

The purpose of this Act is to operate critical information and communications infrastructure in a stable manner by formulating and implementing measures concerning the protection of such infrastructure, in case of an electronic intrusion, thereby contributing to the safety of the State and the stability in people's lives.

รวมทั้งเตรียมความพร้อมในการตอบโต้กรณีเกิดการบุกรุกทางอิเล็กทรอนิกส์เพื่อปกป้องชีวิตของมวลมนุษยชาติและความมั่นคงของประเทศ

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

๑.๑ บทนิยามคำว่า “การบุกรุกทางอิเล็กทรอนิกส์ (electronic intrusion)”

หมายความว่า การกระทำใดที่เป็นการโจมตีโครงสร้างพื้นฐานข้อมูลสารสนเทศและการสื่อสารโดยการเจาะระบบข้อมูล (hacking) ไวรัสคอมพิวเตอร์ (computer viruses) การระเบิดมัลแวร์หรืออีเมล (logic or email bombs) การปฏิเสธการให้บริการ (denial of service) คลื่นแม่เหล็กไฟฟ้ากำลังสูง (high power electromagnetic waves) เป็นต้น และ คำว่า “อุบัติการณ์ความมั่นคงปลอดภัยทางไซเบอร์ (intrusion incident)” หมายความว่า อุบัติการณ์ใด ๆ ที่เกิดขึ้นโดยการบุกรุกทางอิเล็กทรอนิกส์^{๑๐}

๑.๒ มาตรการป้องกันและวิเคราะห์ช่องโหว่ของโครงสร้างพื้นฐานด้านข้อมูลสารสนเทศและการสื่อสาร (มาตรา ๕ ถึงมาตรา ๙)

(๑) กำหนดให้ผู้บริหารองค์กรซึ่งดูแลจัดการโครงสร้างพื้นฐานด้านข้อมูลสารสนเทศและการสื่อสาร (ผู้จัดการองค์กร) มีหน้าที่กำหนดและดำเนินมาตรการความปลอดภัยทั้งด้านกายภาพและด้านเทคนิค เช่น การป้องกันอุบัติการณ์ การสำรองข้อมูล และการกู้คืนระบบ รวมทั้งมีหน้าที่แต่งตั้ง Chief Information Security Officers เพื่อรับผิดชอบการคุ้มครองโครงสร้างพื้นฐานเช่นว่านี้โดยตรง

(๒) กำหนดให้มีการวิเคราะห์และประเมินช่องโหว่ของโครงสร้างพื้นฐานอย่างสม่ำเสมอ เพื่อหาวิธีการที่จะป้องกันภัยคุกคามรูปแบบใหม่ ๆ ที่อาจเกิดขึ้นในอนาคต

^{๑๐} Article 2 (Definitions)

The terms used in this Act are defined as follows:

1. The term "information and communications infrastructure" means electronic control and management system related to the operations for the national security, administration, national defense, public security, finance, communications, transportation, energy, etc. and information and communications network under Article 2 (1) 1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection;

2. The term "electronic intrusion" means any act of attacking information and communications infrastructure by any of the following:

(a) Means of hacking, computer virus, logic or email bombs, denial of service, high-power electromagnetic waves, etc.;

(b) Means of installing a program, technical device, etc. that enables to circumvent normal protection and authentication processes for access to the information and communications infrastructure in the information and communications infrastructure;

3. The term "cyber security incident" means a situation took place by any act of electronic intrusions.

๑.๓ ข้อห้ามและการกระทำความผิดทางไซเบอร์ (มาตรา ๑๐ ถึงมาตรา ๑๖)

(๑) กำหนดแนวทางและมาตรการคุ้มครองโดยให้หัวหน้าหน่วยงานส่วนกลางที่เกี่ยวข้องจัดทำแนวทางปฏิบัติเพื่อคุ้มครองโครงสร้างพื้นฐานที่อยู่ภายใต้การกำกับดูแล และมีคำสั่งให้ดำเนินมาตรการคุ้มครองเพิ่มเติมได้

(๒) กำหนดข้อห้ามการบุกรุกโครงสร้างพื้นฐานที่สำคัญ เช่น การเข้าถึงระบบโดยไม่มีสิทธิ การทำลายข้อมูลหรือใช้โปรแกรมที่เป็นอันตราย หรือการระดมส่งสัญญาณโจมตีการทำงานของโครงสร้างพื้นฐาน

(๓) กำหนดหน้าที่ในการแจ้งเตือนและมาตรการเยียวยา โดยเมื่อองค์กรบริหารจัดการพบว่าเกิดเหตุหรืออุบัติการณ์เกี่ยวกับการโจมตีโครงสร้างพื้นฐานเกิดขึ้น ย่อมมีหน้าที่แจ้งให้หน่วยงานที่เกี่ยวข้อง หน่วยงานสอบสวน หรือ KISA ทราบข้อเท็จจริงที่เกิดขึ้นนั้น และต้องกำหนดมาตรการเยียวยาที่จำเป็นและคุ้มครองโครงสร้างพื้นฐานด้านข้อมูลสารสนเทศและการสื่อสารที่เกี่ยวข้องดังกล่าว

๑.๔ กลไกการรับมือและการแบ่งปันข้อมูล (มาตรา ๑๕ และมาตรา ๑๖) กำหนดให้มีการจัดตั้ง “ศูนย์บัญชาการรับมือกับอุบัติการณ์ความมั่นคงทางไซเบอร์ (Countermeasure Headquarters)” ขึ้นเป็นการชั่วคราวเพื่อกำหนดระยะเวลาดำเนินการรองรับเหตุฉุกเฉิน สนับสนุนทางเทคนิค และเยียวยาความเสียหายที่เกิดขึ้น และให้มีการจัดตั้ง “ศูนย์วิเคราะห์และแบ่งปันข้อมูล (Information Sharing and Analysis Center)” แยกตามกลุ่มอุตสาหกรรมเพื่อกำหนดหน้าที่ให้ข้อมูลเกี่ยวกับสาเหตุและแนวทางแก้ไข และการบริหารจัดการระบบวิเคราะห์และแจ้งเตือนภัยแบบทันที

๑.๕ บทลงโทษ (มาตรา ๒๔ ถึงมาตรา ๓๐)

(๑) โทษอาญา: บุคคลซึ่งบุกรุกหรือรบกวนการดำเนินงานของโครงสร้างพื้นฐานด้านข้อมูลสารสนเทศและการสื่อสารต้องระวางโทษจำคุกไม่เกิน ๑๐ ปี หรือปรับไม่เกิน ๑๐๐ ล้านบาท

(๒) โทษปรับทางปกครอง: กรณีบุคคลซึ่งไม่ปฏิบัติตามคำสั่งกู้คืนระบบหรือไม่วิเคราะห์ช่องโหว่ตามที่กฎหมายกำหนด ระวางโทษปรับตั้งแต่ ๕ ล้านบาท ถึง ๕๐ ล้านบาท แล้วแต่กรณี

๔. Framework Act on National Informatization^{๑๑}

วัตถุประสงค์^{๑๒}

กฎหมายว่าด้วยโครงสร้างพื้นฐานการสร้างสังคมสารสนเทศแห่งชาติมีวัตถุประสงค์เพื่อขับเคลื่อนไปสู่สังคมที่อยู่บนพื้นฐานของความรู้และข้อมูลสารสนเทศอย่างยั่งยืน ยกระดับคุณภาพชีวิตของประชาชนโดยการกำหนดทิศทางพื้นฐานและนโยบายที่จำเป็นเพื่อทำให้เป็นสังคมสารสนเทศระดับชาติ

^{๑๑} Act No. 14572, Mar. 14, 2017

^{๑๒} Article 1 (Purpose)

The purpose of this Act is to contribute to the realization of a sustainable knowledge and information based society, and to improve the quality of life for the nation by prescribing matters necessary for the establishment and promotion of the basic direction of national informatization and policies relevant thereto.

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

๑.๑ บทนิยามคำว่า “การสร้างสังคมสารสนเทศแห่งชาติ (National Informatization)” หมายความว่า การส่งเสริมการนำเทคโนโลยีสารสนเทศมาใช้โดยหน่วยงานระดับชาติ หน่วยงานท้องถิ่น หรือสถาบันหรือองค์กรใดที่สนับสนุนการดำเนินกิจกรรมผ่านกระบวนการสารสนเทศนี้ คำว่า “การคุ้มครองข้อมูลสารสนเทศ (protection of information)” หมายความว่า การจัดทำมาตรการการบริหารจัดการและเทคนิคที่จะป้องกันความเสียหาย การดัดแปลง หรือการรั่วไหลใด ๆ ของข้อมูลนี้อาจเกิดขึ้นมาจากกระบวนการจัดเก็บ รวบรวม ดำเนินการ จัดเก็บข้อมูลซ้ำ เรียกคืน ส่ง หรือรับ ข้อมูลสารสนเทศนั้น และคำว่า “เครือข่ายด้านข้อมูลสารสนเทศและการสื่อสาร (information and communications network)” หมายความว่า เครือข่ายข้อมูลการสื่อสารสารสนเทศซึ่งรวมถึงอุปกรณ์สื่อสารสนเทศ ซอฟต์แวร์ ฐานข้อมูล ที่ใช้ในการเชื่อมต่อกับเครือข่ายดังกล่าว

๑.๒ การกำหนดนโยบายและการขับเคลื่อนข้อมูลสารสนเทศระดับชาติ (มาตรา ๖ ถึงมาตรา ๑๔)

(๑) กำหนดให้รัฐจัดทำแผนแม่บทระดับชาติทุกห้าปีเพื่อส่งเสริมการคุ้มครองข้อมูลสารสนเทศ เครือข่ายด้านข้อมูลสารสนเทศและการสื่อสาร และจริยธรรมในการสื่อสารข้อมูลสารสนเทศ

(๒) กำหนดให้แต่ละหน่วยงานแต่งตั้งเจ้าหน้าที่รัฐผู้รับผิดชอบด้านข้อมูลสารสนเทศเพื่อกำกับดูแลการกำหนดและดำเนินนโยบายและความร่วมมือด้านข้อมูลสารสนเทศระดับประเทศ

(๓) กำหนดให้มีสำนักงานสังคมสารสนเทศแห่งชาติ (National Information Society Agency: NIA) เพื่อสนับสนุนการพัฒนานโยบายในการส่งเสริมข้อมูลสารสนเทศระดับชาติและการสร้างสรรค์วัฒนธรรมด้านสารสนเทศระดับชาติ

๑.๓ การส่งเสริมการเป็นสังคมสารสนเทศแห่งชาติ (มาตรา ๑๕ ถึงมาตรา ๒๘)

รัฐมีหน้าที่ส่งเสริมการใช้บริการเครือข่ายด้านข้อมูลสารสนเทศและการสื่อสาร เช่น อินเทอร์เน็ต การทำธุรกรรมทางอิเล็กทรอนิกส์ ส่งเสริมการกำหนดมาตรฐานเพื่อเพิ่มประสิทธิภาพข้อมูลสารสนเทศระดับชาติ กำหนดนโยบายการเชื่อมโยงเครือข่ายสารสนเทศของหน่วยงานของรัฐเพื่อให้การใช้ข้อมูลร่วมกันเกิดประสิทธิภาพ ส่งเสริมการจัดตั้งและดำเนินการของ “ศูนย์ข้อมูล” (Data Center) เพื่อความมั่นคงและเสถียรภาพของโครงสร้างพื้นฐานทางไซเบอร์

๑.๔ การป้องกันผลกระทบเชิงลบของข้อมูลสารสนเทศแห่งชาติ (มาตรา ๒๙ ถึงมาตรา ๔๒)

รัฐมีหน้าที่จัดทำแผนระดับชาติเพื่อป้องกันปัญหาการติดอินเทอร์เน็ตโดยจัดตั้งศูนย์ให้คำปรึกษาและบำบัดผู้ติดอินเทอร์เน็ต และอาจออนุมัติ “Green Internet Certification” แก่ผู้ให้บริการซึ่งมีมาตรการป้องกันการติดอินเทอร์เน็ต รับรองการเข้าถึงและใช้งานอินเทอร์เน็ตของผู้สูงอายุและผู้ทุพพลภาพ กำหนดนโยบายเพื่อรับประกันความปลอดภัยในการเผยแพร่ข้อมูลตลอดทั้งกระบวนการกำหนดมาตรฐานและความน่าเชื่อถือของระบบการคุ้มครองข้อมูลสารสนเทศ กำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล และกำหนดมาตรฐานทางจริยธรรมไซเบอร์ที่เหมาะสม

๑.๕ การยกระดับโครงสร้างพื้นฐานข้อมูลสารสนเทศและการสื่อสาร (มาตรา ๔๓ ถึง มาตรา ๔๗)

รัฐอาจจัดตั้งเครือข่ายความเร็วสูงเพื่อให้องค์การที่ไม่แสวงหากำไรสามารถนำไปใช้งานได้ในราคาประหยัด ขยายความร่วมมือด้านการให้บริการเครือข่ายดิจิทัล และสนับสนุนหน่วยงานของรัฐให้ใช้โครงสร้างพื้นฐานข้อมูลสารสนเทศและการสื่อสารที่ทันสมัย

๕. *Electronic Government Act*^{๑๓}

วัตถุประสงค์^{๑๔}

กฎหมายว่าด้วยรัฐบาลอิเล็กทรอนิกส์มีวัตถุประสงค์เพื่อส่งเสริมการพัฒนารัฐบาลอิเล็กทรอนิกส์อย่างมีประสิทธิภาพ เพิ่มประสิทธิผล ความโปร่งใส และความเป็นประชาธิปไตยในการบริหารราชการแผ่นดิน รวมถึงการพัฒนาคุณภาพชีวิตของประชาชนโดยกำหนดหลักการพื้นฐาน กระบวนการ วิธีการดำเนินงาน และเรื่องอื่นที่เกี่ยวข้องกับการบริหารราชการแผ่นดินด้วยวิธีการทางอิเล็กทรอนิกส์

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

๑.๑ หลักการของรัฐบาลอิเล็กทรอนิกส์ (มาตรา ๔) หน่วยงานของรัฐต้องคำนึงถึงการสร้างความเชื่อมั่นในการรักษาความปลอดภัยและความน่าเชื่อถือของระบบสารสนเทศ (information systems) และการคุ้มครองข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัว

๑.๒ แผนแม่บทรัฐบาลอิเล็กทรอนิกส์ (มาตรา ๕) หน่วยงานกลางมีหน้าที่จัดทำแผนแม่บทรัฐบาลอิเล็กทรอนิกส์ทุกห้าปี โดยรวบรวมแผนงานของหน่วยงานต่าง ๆ เพื่อใช้เป็นกรอบในการพัฒนา การดำเนินงาน และการขับเคลื่อนรัฐบาลอิเล็กทรอนิกส์ของประเทศ

๑.๓ มาตรการรักษาความปลอดภัยสำหรับการบริการสาธารณะ (มาตรา ๒๔) รัฐมนตรีว่าการกระทรวงมหาดไทย (Minister of the Interior and Safety) มีหน้าที่กำหนดมาตรการรักษาความปลอดภัยที่เกี่ยวข้องกับการบริการสาธารณะทางอิเล็กทรอนิกส์โดยต้องหารือร่วมกับ Director of the National Intelligence Service ก่อน

๑.๔ การกระทำที่ต้องห้าม (มาตรา ๓๕) กฎหมายกำหนดห้ามบุคคลกระทำการในลักษณะที่เป็นการปลอมแปลง ดัดแปลง ทำลาย ลบข้อมูลของหน่วยงานภาครัฐ หรือใช้ระบบสารสนเทศเพื่อการแบ่งปันข้อมูลโดยไม่มีเหตุอันสมควร ตลอดจนเปิดเผยหรือเผยแพร่โปรแกรมที่ทำให้สามารถดัดแปลงหรือลบข้อมูลของหน่วยงานภาครัฐได้

๑.๕ การจัดทำมาตรการรักษาความปลอดภัยสำหรับเครือข่ายข้อมูลสารสนเทศและการสื่อสาร (มาตรา ๕๖) หน่วยงานของรัฐต้องจัดทำมาตรการเพื่อรักษาความปลอดภัยและความ

^{๑๓} Act No. 14914, Oct. 24, 2017

^{๑๔} Article 1 (Purpose)

The purpose of this Act is to facilitate the efficient realization of electronic government, enhance productivity, transparency and democracy in the public administration, and improve the quality of life of citizens by providing for fundamental principles, procedures, methods of promotion, and other relevant matters for the electronic processing of administrative affairs.

นำเชื่อถือของเครือข่ายข้อมูลสารสนเทศและการสื่อสาร รวมถึงข้อมูลเกี่ยวกับการบริหารราชการ เพื่อป้องกันการปลอมแปลง การรั่วไหล หรือการทำลายเอกสารอิเล็กทรอนิกส์

๑.๖ การป้องกันและการตอบสนองต่อความล้มเหลวของระบบ (มาตรา ๕๖-๒)

หัวหน้าหน่วยงานของรัฐมีหน้าที่จัดทำมาตรการป้องกันและตอบสนองต่อความล้มเหลวของระบบเพื่อให้การทำงานและการจัดการระบบข้อมูลมีเสถียรภาพ

๑.๗ การกำกับดูแลระบบสารสนเทศ (มาตรา ๕๗)

หัวหน้าหน่วยงานของรัฐมีหน้าที่กำหนดให้มีการตรวจสอบและติดตามการดำเนินงานของระบบสารสนเทศเพื่อแก้ไขและประกันความปลอดภัยของระบบดังกล่าว

๑.๘ บทกำหนดโทษ (มาตรา ๗๖)

กำหนดโทษจำคุกและโทษปรับสำหรับผู้ซึ่งละเมิดการรักษาความปลอดภัยทางไซเบอร์ เช่น การทำลายข้อมูลทางปกครอง ระวังโทษจำคุกไม่เกิน ๑๐ ปี หรือกรณีที่มีการเข้าถึงข้อมูลสารสนเทศโดยมิชอบ ระวังโทษจำคุกไม่เกิน ๕ ปีหรือปรับไม่เกิน ๕๐ ล้านบาท เป็นต้น

๖. *Electronic Financial Transactions Act*^{๑๕}

วัตถุประสงค์^{๑๖}

กฎหมายว่าด้วยธุรกรรมทางการเงินอิเล็กทรอนิกส์มีวัตถุประสงค์เพื่อสร้างความเชื่อมั่นในความปลอดภัยและความน่าเชื่อถือของธุรกรรมทางการเงินอิเล็กทรอนิกส์โดยการกำหนดความสัมพันธ์ในแง่ของกฎหมายให้มีความชัดเจน ตลอดจนอำนวยความสะดวกทางการเงินแก่ประชาชนและส่งเสริมการพัฒนาทางเศรษฐกิจของประเทศด้วยการวางรากฐานการพัฒนาระบบธุรกรรมทางการเงินอิเล็กทรอนิกส์ได้อย่างเหมาะสม

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

๑.๑ บทนิยามคำว่า “โครงสร้างพื้นฐานทางการเงินทางอิเล็กทรอนิกส์ (Electronic

Financial Infrastructure)” หมายความว่า ระบบการประมวลผลข้อมูลที่ใช้ในธุรกรรมทางการเงินอิเล็กทรอนิกส์และเครือข่ายข้อมูลสารสนเทศและการสื่อสาร และคำว่า “การละเมิดทางอิเล็กทรอนิกส์ (electronic infringement)” หมายความว่า การโจมตีโครงสร้างพื้นฐานทางการเงินอิเล็กทรอนิกส์ด้วยวิธีการต่าง ๆ เช่น การเจาะระบบข้อมูล (hacking) ไวรัสคอมพิวเตอร์ (computer viruses) การระเบิดมัลแวร์หรืออีเมล (logic bomb, email bomb) การปฏิเสธการให้บริการ (denial of service) คลื่นแม่เหล็กไฟฟ้ากำลังสูง (high power electromagnetic wave) เป็นต้น

๑.๒ หน้าที่ในการประกันความปลอดภัย (มาตรา ๒๑)

สถาบันการเงินและผู้ประกอบธุรกิจมีหน้าที่ปฏิบัติตามมาตรฐานที่ Financial Services Commission (FSC) กำหนด ทั้งในด้าน

^{๑๕} Act No. 21205, Dec. 17, 2026

^{๑๖} Article 1 (Purpose)

The purpose of this Act is to ensure the safety and reliability of electronic financial transactions by clarifying their legal relations and to promote financial conveniences for people and contribute to national economic development by creating a foundation for the sound development of the electronic financial industry.

ทรัพยากรมนุษย์ สิ่งอำนวยความสะดวก อุปกรณ์อิเล็กทรอนิกส์ และค่าใช้จ่ายในการทำธุรกรรมทางอิเล็กทรอนิกส์ต่าง ๆ ให้มีความปลอดภัยและน่าเชื่อถือ รวมถึงต้องมีการจัดทำแผนงานด้านเทคโนโลยีสารสนเทศเป็นประจำทุกปีและเสนอต่อ FSC

๑.๓ การแต่งตั้งเจ้าหน้าที่ด้านความปลอดภัยสารสนเทศ และการวิเคราะห์และประเมินช่องโหว่ (มาตรา ๒๑-๒ และมาตรา ๒๑-๓) กำหนดให้สถาบันการเงินหรือผู้ประกอบการธุรกิจแต่งตั้งเจ้าหน้าที่ด้านความปลอดภัยสารสนเทศ (chief information security officer) เพื่อรับผิดชอบการจัดการด้านความปลอดภัยแก่ธุรกิจทางการเงินอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศ ตลอดจนกำหนดให้สถาบันการเงินและผู้ประกอบการธุรกิจการเงินอิเล็กทรอนิกส์มีหน้าที่วิเคราะห์และประเมินเหตุที่มีความเกี่ยวข้องกับโครงสร้างพื้นฐานทางการเงินอิเล็กทรอนิกส์และรายงานต่อ FSC

๑.๔ การห้ามละเมิดทางอิเล็กทรอนิกส์ การแจ้งและตอบโต้เหตุละเมิด (มาตรา ๒๑-๔ ถึงมาตรา ๒๑-๖) กฎหมายกำหนดห้ามการเข้าถึงโครงสร้างพื้นฐานทางการเงินอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต ห้ามการติดตั้งโปรแกรม เช่น ไวรัสคอมพิวเตอร์ หรือมัลแวร์ โดยมีวัตถุประสงค์เพื่อทำลายข้อมูลหรือขัดขวางการทำงานของโครงสร้างพื้นฐานดังกล่าว และในกรณีมีเหตุละเมิดอันทำให้ระบบไม่สามารถทำงานต่อไปได้ สถาบันการเงินและผู้ประกอบการธุรกิจทางการเงินอิเล็กทรอนิกส์ย่อมมีหน้าที่แจ้งให้ FSC ทราบทันที และ FSC ต้องรวบรวมข้อเท็จจริงของเหตุการณ์ที่เกิดขึ้นและออกประกาศเตือนเกี่ยวกับเหตุละเมิดดังกล่าว พร้อมทั้งกำหนดมาตรการฉุกเฉินเพื่อตอบโต้ต่อเหตุการณ์ที่เกิดขึ้น

๑.๕ บทกำหนดโทษ (มาตรา ๔๙)

(๑) กำหนดโทษจำคุกไม่เกิน ๑๐ ปี หรือปรับไม่เกิน ๑๐๐ ล้านบาท สำหรับผู้ซึ่งทำลายข้อมูล ติดตั้งโปรแกรม หรือโจมตีโครงสร้างพื้นฐานทางการเงินอิเล็กทรอนิกส์

(๒) กำหนดโทษจำคุกไม่เกิน ๗ ปี หรือปรับไม่เกิน ๕๐ ล้านบาท สำหรับบุคคลซึ่งปลอมแปลงวิธีการเข้าถึง (means of access) หรือบุกรุกระบบเพื่อให้ได้มาซึ่งการเข้าถึงการใช้งานธุรกรรม

๗. National Intelligence Service Korea Act^{๑๗}

วัตถุประสงค์^{๑๘}

กฎหมายว่าด้วยสำนักงานข่าวกรองแห่งสาธารณรัฐเกาหลีมีวัตถุประสงค์เพื่อกำหนดเรื่องที่เกี่ยวข้องกับการจัดระเบียบองค์กรและกำหนดขอบเขตหน้าที่ของสำนักงานข่าวกรองแห่งชาติ ตลอดจนการปฏิบัติการกิจด้านความมั่นคงแห่งชาติให้เป็นไปอย่างมีประสิทธิภาพ

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

๑.๑ หน้าที่ของ National Intelligence Service (NIS) เกี่ยวกับไซเบอร์ (มาตรา ๔)
กำหนดให้ NIS มีหน้าที่ในการรวบรวม จัดเตรียม และเผยแพร่ข่าวกรองเกี่ยวกับความมั่นคงทางไซเบอร์ (Intelligence on cybersecurity) เช่น ข้อมูลเกี่ยวกับผู้เจาะระบบข้อมูลขององค์กรทั้งในระดับประเทศ

^{๑๗} Act No. 18519, Oct. 19, 2021

^{๑๘} Article 1 (Purpose)

The purpose of this Act is to provide for matters necessary for the organization and the scope of duties of the National Intelligence Service and for its efficient performance of national security service.

และระหว่างประเทศ รวมถึงการจัดทำมาตรการป้องกันและตอบโต้การโจมตีและการคุกคามทางไซเบอร์ที่มุ่งเป้าไปยังหน่วยงานส่วนกลางและส่วนท้องถิ่น

๑.๒ อำนาจในการสืบสวนสอบสวน (มาตรา ๕) กำหนดให้พนักงานของ NIS มีอำนาจในการสืบสวนสอบสวนและเข้าถึงเอกสาร การเก็บตัวอย่าง การร้องขอข้อมูลเพิ่มเติมได้

๑.๓ บทกำหนดโทษ (มาตรา ๒๑ ถึงมาตรา ๒๓) กำหนดโทษกรณีฝ่าฝืนกฎหมาย ประกอบด้วยโทษจำคุกและพักใช้ใบอนุญาตแล้วแต่ฐานความผิดเป็นรายกรณี

๔. บทสรุป

กล่าวโดยสรุป เกาหลีใต้เป็นหนึ่งในประเทศที่มีการกำหนดนโยบายและมาตรการทางกฎหมายที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ไว้อย่างชัดเจน ทั้งในแง่ของการป้องกันและปราบปรามอาชญากรรมการหลอกลวงทางไซเบอร์ (cyber scam) และการสร้างเสถียรภาพและความน่าเชื่อถือในด้านความมั่นคงทางไซเบอร์ อันแสดงให้เห็นถึงความตระหนักของรัฐบาลที่ให้ความสำคัญกับการมุ่งหมายที่จะปกป้องผลประโยชน์ของประเทศชาติและคุ้มครองทรัพย์สินของประชาชน อีกทั้งนโยบายและกฎหมายต่าง ๆ ที่รัฐบาลได้ตราออกมานั้นมีการปรับปรุงให้ทันสมัยและทันต่อเหตุการณ์หรืออุบัติการณ์ที่เกิดขึ้นอยู่อย่างสม่ำเสมอ เกาหลีใต้จึงเป็นตัวอย่างที่ดีที่ประเทศไทยจะได้ศึกษาพัฒนาการและเรียนรู้ข้อดีและข้อเสียเกี่ยวกับนโยบายและมาตรการทางกฎหมายเพื่อเทียบเคียงนำมาปรับใช้ให้เข้ากับบริบทในประเทศไทยต่อไปได้ในอนาคต

สิงคโปร์*

๑. บทนำ

ในยุคปัจจุบันที่โลกเชื่อมโยงถึงกันอย่างไร้พรมแดนด้วยเทคโนโลยีอินเทอร์เน็ตซึ่งเอื้อให้บุคคลจากหลากหลายภูมิภาคสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และดำเนินกิจกรรมทางเศรษฐกิจร่วมกันได้อย่างสะดวกรวดเร็วและมีประสิทธิภาพนั้น ขณะเดียวกันก็ได้ก่อให้เกิดความเสี่ยงและภัยคุกคามรูปแบบใหม่ที่พัฒนาไปอย่างรวดเร็วตามวิวัฒนาการของเทคโนโลยีด้วยเช่นกัน โดยเฉพาะอย่างยิ่งอาชญากรรมที่เกิดขึ้นผ่านระบบเครือข่ายอินเทอร์เน็ตอันมีลักษณะซับซ้อนและยากต่อการควบคุมมากกว่าอาชญากรรมในโลกกายภาพ

หนึ่งในอาชญากรรมดังกล่าว ได้แก่ การหลอกลวงทางไซเบอร์ (Cyber Scam) ซึ่งเป็นการนำเทคโนโลยีและความรู้ด้านสารสนเทศมาใช้เป็นเครื่องมือในการกระทำความผิดโดยทุจริต ส่งผลให้เกิดความเสียหายต่อทรัพย์สินของประชาชนผู้สุจริต โดยเฉพาะอย่างยิ่งผู้ที่ขาดความรู้เท่าทันต่อรูปแบบของการหลอกลวงที่มีการพัฒนาอย่างต่อเนื่องและรวดเร็ว ปรากฏการณ์ดังกล่าวส่งผลให้ Cyber Scam กลายเป็นประเด็นปัญหาระดับนานาชาติที่หลายประเทศให้ความสำคัญในการกำหนดมาตรการเชิงนโยบายและกฎหมายเพื่อป้องกันและปราบปรามอย่างจริงจัง

สิงคโปร์เป็นหนึ่งในประเทศที่เผชิญกับปัญหาอาชญากรรม Cyber Scam อย่างมีนัยสำคัญ โดยรัฐบาลสิงคโปร์ ตลอดจนหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้อง ได้ดำเนินการศึกษาวิเคราะห์ และพัฒนาแนวทางในการรับมือกับปัญหาดังกล่าวอย่างเป็นระบบ ทั้งในมิติของการกำหนดนโยบายสาธารณะ การตรากฎหมายที่เกี่ยวข้อง และการดำเนินมาตรการเชิงปฏิบัติอื่นควบคู่กันไป

หัวข้อนี้จึงมุ่งศึกษาสถานการณ์ของอาชญากรรม Cyber Scam ในประเทศสิงคโปร์ โดยพิจารณาทั้งในด้านสถิติและลักษณะรูปแบบของการกระทำความผิด แนวนโยบายของรัฐในการป้องกันและปราบปราม ตลอดจนกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การสังเคราะห์ข้อสรุปเกี่ยวกับความเหมาะสมและประสิทธิภาพของมาตรการดังกล่าวต่อไป

๒. สถานการณ์คดี Cyber Scam ในสิงคโปร์

สำนักงานตำรวจสิงคโปร์ (Singapore Police Force : SPF) ได้จัดทำรายงานสรุปประจำปีเกี่ยวกับการหลอกลวงและอาชญากรรมทางไซเบอร์ (Annual Scam and Cybercrime Brief) เผยแพร่ทางเว็บไซต์ SPF ทุกปี โดยเอกสารดังกล่าวมีสาระสำคัญเป็นการรายงานสถานการณ์โดยรวมของ Scam และ Cybercrime ในแต่ละปี (จำนวนคดี, มูลค่าความเสียหาย, จำนวนเงินที่ได้รับคืน, ประเภทของ Scam และ Cybercrime, ช่องทางการติดต่อ, ประวัติของเหยื่อ, ความพยายามของ SPR กับหน่วยงานภาครัฐเพื่อต่อสู้กับ Scam และ Cybercrime ตลอดจนการรณรงค์ให้ภาคประชาชนมีส่วนร่วมเกี่ยวกับเรื่องนี้

* จัดทำโดยนางสาวนพรัตน์ พิริยานสรณ์ นักกฎหมายกฤษฎีกาชำนาญการพิเศษ ฝ่ายค้นคว้าและเปรียบเทียบกฎหมาย กองกฎหมายต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

ข้อความหรือเอกสารนี้มีส่วนที่สร้างขึ้นโดยเทคโนโลยีปัญญาประดิษฐ์ (AI) และผู้จัดทำได้ตรวจสอบความถูกต้องแล้ว

สถิติจำนวนคดี มูลค่าความเสียหาย และจำนวนเงินที่สามารถติดตามคืนได้ (ค.ศ. ๒๐๒๒-๒๐๒๕)

ปี ค.ศ./ จำนวน	ลักษณะความผิด		ความเสียหาย (ล้านดอลลาร์ สิงคโปร์)	เงินที่ได้รับคืน (ล้านดอลลาร์ สิงคโปร์)
	Scam	Cybercrime		
๒๐๒๒ ^๑	๓๑,๗๒๘ คดี	๑,๙๔๑ คดี	๖๖๐.๗	๑๔๖.๖
๒๐๒๓ ^๒	๔๖,๕๖๓ คดี	๓,๘๑๓ คดี	๖๕๑.๘	๑๐๐.๗
๒๐๒๔ ^๓	๕๑,๕๐๑ คดี	๔,๓๐๙ คดี	๑,๑๑๒.๔	๑๘๒.๘
๒๐๒๕ ^๔	๓๗,๓๐๘ คดี	๔,๖๖๖ คดี	๙๑๓.๑	๑๔๐.๕

ประเภท/ลักษณะของคดีการหลอกลวง (Scam) ที่เกิดขึ้น

จากการรวบรวมและวิเคราะห์ข้อมูลโดย SPF พบว่า ในช่วงปี ค.ศ. ๒๐๒๒-๒๐๒๕ ประเภทหรือ “ลักษณะสำคัญของคดีการหลอกลวง (scam)” ที่เกิดขึ้นเป็นประจำในประเทศสิงคโปร์ สามารถจัดจำแนกได้เป็น ๕ ประเภทหลัก^๕ ดังต่อไปนี้

^๑ PUBLIC AFFAIRS DEPARTMENT SINGAPORE POLICE FORCE, “Annual Scams and Cybercrime Brief 2022”, สืบค้นเมื่อ ๑ มิถุนายน ๒๕๖๙, จาก <https://www.police.gov.sg/-/media/SPF/Media-Room/Statistics/Annual-Scams-and-Cybercrime-Brief-2022/Police-News-Release---Annual-Scams-and-Cybercrime-Brief-2022.pdf>

^๒ PUBLIC AFFAIRS DEPARTMENT SINGAPORE POLICE FORCE, “Annual Scams and Cybercrime Brief 2023”, สืบค้นเมื่อวันที่ ๑ มิถุนายน ๒๕๖๙, จาก <https://www.police.gov.sg/-/media/SPF/Media-Room/Statistics/Annual-Scams-and-Cybercrime-Brief-2023/Annual-Scams-and-Cybercrime-Brief-2023.pdf>

^๓ PUBLIC AFFAIRS DEPARTMENT SINGAPORE POLICE FORCE, “Annual Scams and Cybercrime Brief 2024”, สืบค้นเมื่อวันที่ ๑ มิถุนายน ๒๕๖๙, จาก <https://www.police.gov.sg/-/media/SPF/Media-Room/Statistics/Annual-Scams-and-Cybercrime-Brief-2024/Annual-Scams-and-Cybercrime-Brief-2024.pdf>

^๔ PUBLIC AFFAIRS DEPARTMENT SINGAPORE POLICE FORCE, “Annual Scam and Cybercrime Brief 2025”, สืบค้นเมื่อวันที่ ๑ มิถุนายน ๒๕๖๙, จาก <https://www.police.gov.sg/-/media/SPF/Media-Room/Statistics/Annual-Scams-and-Cybercrime-Brief-2025/Annual-Scam-and-Cybercrime-Brief-2025.pdf>

^๕ สรุปจากเอกสารตามที่ระบุไว้ในเชิงอรรถที่ ๑ - ๔

(๑) การหลอกลวงให้ทำงาน (Job scam) เป็นกรณีที่เหยื่อได้รับข้อเสนอให้เข้าทำงานผ่านช่องทางออนไลน์ ซึ่งสามารถปฏิบัติงานได้จากที่พักอาศัย เพื่อแลกเปลี่ยนกับค่าคอมมิชชั่น โดยมีลักษณะของงาน เช่น การสั่งซื้อสินค้าล่วงหน้า การกดถูกใจ (Like) บนสื่อสังคมออนไลน์ การรีวิวโรงแรม ร้านอาหาร หรือสายการบิน การตอบแบบสำรวจ การเพิ่มมูลค่าของสกุลเงินดิจิทัล การเพิ่มคะแนนของรายการสินค้าสำหรับร้านค้าออนไลน์ การให้คะแนนแอปพลิเคชันมือถือเพื่อปรับปรุงอันดับใน App Store ตลอดจนการโอนเงินไปยังบัญชีธนาคารที่มีฉ้อโกงกำหนด เพื่อแลกกับค่าคอมมิชชั่นในจำนวนเล็กน้อย และในระยะต่อมามีฉ้อโกงจะชักจูงให้เหยื่อโอนเงินในจำนวนที่เพิ่มสูงขึ้น โดยอ้างว่าจะได้รับผลตอบแทนที่สูงขึ้นตามลำดับ ซึ่งเหยื่อจะทราบว่าถูกหลอกลวงเมื่อไม่ได้รับค่าคอมมิชชั่น ไม่สามารถถอนเงินจากบัญชีธนาคารได้ หรือไม่สามารถติดต่อมีฉ้อโกงได้อีกต่อไป โดยส่วนใหญ่เหยื่อจะได้รับข้อเสนอผ่านข้อความจากหมายเลขโทรศัพท์ที่ไม่รู้จักผ่านแอปพลิเคชันสื่อสาร หรือพบโฆษณาออนไลน์ที่มีข้อเสนอของงาน โดยมีการเสนอเงื่อนไขว่าผู้ทำงานจะได้รับเงินเดือนในอัตราสูงและสามารถปฏิบัติงานในลักษณะทางไกล และมักมีการระบุหมายเลข WhatsApp, Telegram หรือแนบลิงก์เว็บไซต์ต่าง ๆ เพื่อให้เหยื่อที่สนใจติดต่อเพิ่มเติมเพื่อลงทะเบียนทำงานหรือจัดทำบัญชีของตน ในบางกรณีมีฉ้อโกงจะสร้างความสัมพันธ์กับเหยื่อผ่านช่องทางออนไลน์และขอความช่วยเหลือในงาน part-time หรือเสนอให้เข้าร่วมโอกาสในการหารายได้ โดยเหยื่อจะได้รับเว็บไซต์ e-commerce และถูกกำหนดให้แคปหน้าจอผลิตภัณฑ์ที่ระบุ รวมทั้งให้ชำระเงินล่วงหน้าไปยังบัญชีธุรกิจปลอมเพื่อรับค่าคอมมิชชั่นพร้อมเงินคืนตามที่มีการอ้าง กระบวนการดังกล่าวจะดำเนินการซ้ำหลายครั้ง โดยเริ่มจากสินค้าที่มีราคาต่ำก่อนที่จะเพิ่มไปสู่สินค้าที่มีราคาสูงขึ้น โดยในระยะแรกเหยื่อจะได้รับค่าคอมมิชชั่นและเงินคืน แต่ในที่สุดมีฉ้อโกงจะอ้างว่าพบปัญหาและยุติการจ่ายค่าคอมมิชชั่นให้กับเหยื่อก่อนที่จะไม่สามารถติดต่อได้อีกต่อไป

(๒) การหลอกลวงแบบ Phishing^๗ (Phishing scam) โดยทั่วไปเป็นการกระทำที่เกี่ยวข้องกับการติดต่อผ่านอีเมล ข้อความ การโทรศัพท์ หรือโฆษณา โดยมีฉ้อโกงแอบอ้างเป็นเจ้าหน้าที่ของรัฐ สถาบันการเงิน หรือองค์กรธุรกิจ เพื่อชักจูงให้เหยื่อเปิดเผยข้อมูลส่วนบุคคลที่มีความสำคัญ เช่น ชื่อผู้ใช้ รหัสผ่าน ข้อมูลบัญชีธนาคาร และ/หรือข้อมูลบัตรเครดิตหรือบัตรเครดิต ผ่านการคลิกลิงก์ที่เป็นอันตรายหรือผ่านการติดต่อทางโทรศัพท์ เมื่อมีฉ้อโกงได้รับข้อมูลดังกล่าวแล้ว จะนำไปใช้ในการทำธุรกรรมที่ไม่ได้รับอนุญาตในบัญชีธนาคารหรือบัตรเครดิต/เครดิตของเหยื่อ ซึ่ง Phishing scam ที่เกิดขึ้นบ่อยมีรูปแบบดังต่อไปนี้

^๖ รีวิว หมายถึง ข้อมูลเกี่ยวกับประสบการณ์ของผู้บริโภคที่มีต่อสินค้าหรือบริการที่ได้รับจากผู้ประกอบการซึ่งเผยแพร่ต่อสาธารณะโดยผู้บริโภค (ถือว่าผู้บริโภคเป็นผู้เขียนรีวิว), สืบค้นเมื่อวันที่ ๑ มิถุนายน ๒๕๖๙ จาก COLLECTION, MODERATION AND PUBLICATION OF ONLINE CUSTOMER REVIEWS

^๗ Phishing คือ การหลอกลวงทางอินเทอร์เน็ตเพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิตโดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชซิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้นจะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง, สืบค้นเมื่อวันที่ ๑ มิถุนายน ๒๕๖๙ จาก <4D6963726F736667420576F7264202D20A4D9E8C1D7CDC0D1C2A4D8C1A4D2C1B7D2A7A4CDC1BED4C7E0B5CDC3EC205F322E646F6378>

(ก) การแอบอ้างเป็นผู้ซื้อที่สนใจผ่านแพลตฟอร์มตลาดออนไลน์ มิฉะพิจจะแอบอ้างเป็นผู้ซื้อที่มีศักยภาพและติดต่อเหี่ยวโดยแสดงความสนใจในสินค้าที่ลงขายในแพลตฟอร์มตลาดออนไลน์ โดยเหี่ยวจะได้รับลิงก์ URL หรือรหัส QR ที่เป็นอันตรายผ่านทางอีเมลหรือข้อความในแอปพลิเคชัน โดยอ้างว่าจะใช้ในการรับชำระเงินสำหรับสินค้าหรือชำระค่าบริการจัดส่งเพื่ออำนวยความสะดวกในการจัดส่งสินค้า เมื่อเหี่ยวคลิกลิงก์ดังกล่าวจะถูกนำไปยังเว็บไซต์ธนาคารหรือบริษัทจัดส่งปลอม ซึ่งเหี่ยวจะถูกหลอกให้เปิดเผยข้อมูลบัญชีธนาคาร รายละเอียดบัตรเดบิต บัตรเครดิต และรหัสยืนยันแบบใช้ครั้งเดียว (One Time Password : OTP)

(ข) การแอบอ้างเป็นเจ้าหน้าที่รัฐผ่านโทรศัพท์ เหี่ยวจะได้รับการติดต่อผ่านการโทรศัพท์หรือข้อความในแอปพลิเคชันที่ไม่ได้ร้องขอ โดยมีฉะพิจอ้างว่าเป็นเจ้าหน้าที่ของรัฐ เช่น SPF หรือกระทรวงแรงงาน (MoM) และแจ้งว่าบัญชีธนาคารของเหี่ยวมีปัญหาและต้องทำการตรวจสอบเพิ่มเติม จากนั้นเหี่ยวจะถูกชักจูงให้เปิดเผยข้อมูลบัญชีธนาคาร รายละเอียดบัตรเดบิต บัตรเครดิต รหัส OTP และ/หรือข้อมูลส่วนบุคคล ทั้งนี้ ในปี ค.ศ. ๒๐๒๕ SPF ได้พบลักษณะใหม่ของการโอนเงินของเหี่ยวในคดีประเภทดังกล่าวอีก ๒ ลักษณะ ได้แก่ ๑) การโอนเงินจากบัญชีธนาคารของเหี่ยวไปยังบัญชีของผู้ให้บริการชำระเงิน เช่น YouTrip ซึ่งอยู่ภายใต้การควบคุมของมิฉะพิจผ่านระบบ PayNow และ ๒) การโอนเงินในรูปแบบคริปโทเคอร์เรนซี โดยให้เหี่ยวจัดตั้งบัญชีคริปโทเคอร์เรนซีใหม่ เติมเงินเข้าสู่บัญชีดังกล่าวผ่านการโอนเงินสกุลปกติจากบัญชีธนาคารของเหี่ยว ก่อนที่จะซื้อคริปโทเคอร์เรนซี และโอนสินทรัพย์ดิจิทัลไปยังบัญชีคริปโทเคอร์เรนซีที่มิฉะพิจควบคุม

(ค) การแอบอ้างเป็นธนาคารผ่าน SMS ปลอม เหี่ยวจะได้รับข้อความจากหมายเลขโทรศัพท์ต่างประเทศและในประเทศ หรือจากรหัสสั้น (short code) ที่แอบอ้างเป็นธนาคาร โดยมีข้อความแจ้งเตือนว่าเกี่ยวข้องกับธุรกรรมที่ไม่ได้รับอนุญาตในบัญชีธนาคารหรือบัตรเครดิต และแนะนำให้เหี่ยวคลิกลิงก์เพื่อยืนยันหรือระงับธุรกรรม เมื่อเหี่ยวคลิกลิงก์ดังกล่าวจะถูกนำไปยังเว็บไซต์ธนาคารปลอม และถูกหลอกให้เปิดเผยข้อมูลบัญชี รายละเอียดบัตรเดบิต บัตรเครดิต หรือรหัส OTP ซึ่งเปิดโอกาสให้มิฉะพิจสามารถทำธุรกรรมโดยไม่ได้รับอนุญาตจากเหี่ยว โดยเหี่ยวจะทราบว่าตนเองถูกหลอกลงเมื่อพบว่ามีการทำธุรกรรมที่ไม่ได้รับอนุญาตจากบัญชีของตน

(ง) การทำธุรกรรมบัตรเครดิตโดยไม่ได้รับอนุญาต เป็นกรณีที่เหี่ยวได้เปิดเผยรายละเอียดบัตรและรหัสยืนยันผ่าน OTP หรือ digital token ให้แก่มิฉะพิจโดยไม่รู้ตัว เพื่อใช้ในการทำธุรกรรมซื้อสินค้าที่มีลักษณะเสมือนถูกต้องตามกฎหมาย

^๔ มาตรา ๓ แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. ๒๕๖๑ บัญญัตินิยามคำว่า “คริปโทเคอร์เรนซี” ไว้ว่า “หมายความว่า หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะใช้เป็นสื่อกลางในการแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้า บริการ หรือสิทธิอื่นใด หรือแลกเปลี่ยนระหว่างสินทรัพย์ดิจิทัล และให้หมายความรวมถึงหน่วยข้อมูลอิเล็กทรอนิกส์อื่นใดตามที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด

^{๑๐} คือ แพลตฟอร์มซื้อและขายสินค้าออนไลน์สัญชาติสิงคโปร์, สืบค้นเมื่อวันที่ ๑ มิถุนายน ๒๕๖๙, จาก ทำความรู้จัก Carousell "ยูนีคอร์น" ล่าสตของอาเซียน

เหยื่อได้โอนเงินจำนวนมากไปยังมิฉาซีฟเพื่อการลงทุนแล้ว เหยื่อจะประสบปัญหาในการถอนเงินหรือไม่สามารถถอนผลตอบแทนได้ และจึงทราบว่าตนตกเป็นเหยื่อของการหลอกลวง นอกจากนี้ เหยื่ออาจถูกชักจูงให้เข้าร่วมเป็นสมาชิกในกลุ่มแชทหรือช่องทางต่าง ๆ ผ่านแพลตฟอร์มการสื่อสาร เช่น WhatsApp หรือ Telegram โดยอ้างว่าเป็นโอกาสในการลงทุนภายในกลุ่มดังกล่าว ซึ่งเหยื่อจะได้รับข้อมูลหรือคำกล่าวอ้างจากสมาชิกอื่นเกี่ยวกับผลกำไรจากการลงทุนจนเกิดความหลงเชื่อ และทำการติดต่อมิฉาซีฟ เปิดเผยข้อมูลส่วนบุคคล เพื่อจัดตั้งบัญชีและโอนเงินเพื่อการลงทุน ต่อมามิฉาซีฟจะเรียกเก็บค่าธรรมเนียมต่าง ๆ ที่เกี่ยวข้องกับการลงทุน และเหยื่อจะทราบว่าถูกหลอกลวงเมื่อไม่สามารถถอนผลกำไรได้ แม้ว่าได้ชำระค่าธรรมเนียมดังกล่าวแล้วก็ตาม

๓. แนวนโยบายของรัฐในการป้องกันและปราบปราม Cyber Scam

(๑) ระดับภายในประเทศ

รัฐบาลสิงคโปร์ได้ดำเนินมาตรการเชิงรุกเพื่อรับมือกับความเสี่ยงจาก Cyber Scam ตลอดจนเพื่อสร้างสภาพแวดล้อมทางออนไลน์ที่มีความปลอดภัยและน่าเชื่อถือ ซึ่งมีส่วนช่วยในการเสริมสร้างความเชื่อมั่นให้แก่ประชาชนในการใช้ประโยชน์จากโอกาสที่เกิดขึ้นจากการพัฒนาเทคโนโลยีดิจิทัล โดยมีมาตรการสำคัญ ดังนี้

(ก) การจำกัดผลกระทบจากการหลอกลวง (Containing the impact of scams)

รัฐได้เสริมสร้างขีดความสามารถในการกู้คืนเงินที่สูญเสียไป และจำกัดความเสียหายที่อาจเกิดขึ้นจากการหลอกลวงให้มีประสิทธิภาพยิ่งขึ้น ดังต่อไปนี้

๑) SPF ได้จัดตั้งหน่วย Anti-Scam Command (ASCom) โดยมีวัตถุประสงค์เพื่อเสริมสร้างความเป็นเอกภาพและประสิทธิภาพในการดำเนินงานของหน่วยงานต่าง ๆ ภายใน SPF ที่เกี่ยวข้องกับการป้องกันและปราบปรามการหลอกลวง ผ่านการบูรณาการภารกิจด้านการสืบสวน การตอบสนองต่อเหตุการณ์ การแทรกแซง การบังคับใช้กฎหมาย และการวิเคราะห์ข้อมูลเข้าไว้ภายใต้โครงสร้างเดียวกัน ประกอบด้วยศูนย์ป้องกันการหลอกลวง (Anti-Scam Centre) หน่วยสืบสวนการหลอกลวงจำนวน ๓ หน่วย (Anti-Scam Investigation Branches) และกำกับดูแลหน่วยปฏิบัติการ Scam Strike Teams ซึ่งประจำอยู่ในกองกำลังตำรวจพื้นที่ทั้ง ๗ แห่งของประเทศ โดยหน่วย ASCom ได้สร้างความร่วมมือกับองค์กรหลายแห่งในการป้องกันและปราบปราม scam ซึ่งรวมถึงธนาคารทั้งในประเทศและต่างประเทศ กลุ่มรักษาความปลอดภัยของบัตร สถาบันการเงินที่มีโซ่นาการ (เช่น Grab และ Singtel DASH) บริษัทเทคโนโลยีทางการเงิน (FinTech) และผู้ให้บริการด้านคริปโทเคอร์เรนซี (เช่น Wise, Xfers Pte Ltd และ Coinhako) ตลอดจนผู้ให้บริการโอนเงินในสิงคโปร์ โดยมีวัตถุประสงค์เพื่อจัดตั้งช่องทางการสื่อสารโดยตรงและเสริมสร้างความสัมพันธ์ในการปฏิบัติงานร่วมกัน โดยมุ่งให้สามารถระงับบัญชีได้อย่างรวดเร็ว กู้คืนทรัพย์สิน และลดความเสียหายของเหยื่อ^{๑๑} ซึ่งในช่วงครึ่งแรกของปี ค.ศ.

^{๑๑} PUBLIC AFFAIRS DEPARTMENT SINGAPORE POLICE FORCE, “Opening Of Anti-Scam Command Office”, สืบค้นเมื่อวันที่ ๒ มิถุนายน ๒๕๖๙, จาก SPF | Opening Of Anti-Scam Command Office

๒๐๒๓ หน่วย ACom สามารถระงับบัญชีธนาคารได้มากกว่า ๙,๐๐๐ บัญชี และสามารถกู้คืนเงินได้ประมาณ ๕๐.๘ ล้านดอลลาร์สิงคโปร์^{๑๒}

๒) รัฐบาลร่วมมือกับธนาคารและ CPF Board^{๑๓} ในการจัดให้มีเครื่องมือสำหรับช่วยเหลือเหยื่อเพื่อลดความเสียหายกรณีที่บัญชีถูกเข้าถึงโดยมิชอบ ตัวอย่างเช่น ตั้งแต่เดือนตุลาคม ค.ศ. ๒๐๒๒ ธนาคารได้ให้บริการระบบฉุกเฉินแบบบริการตนเอง (self-service “kill-switch”^{๑๔}) เพื่อให้ผู้ใช้สามารถระงับบัญชีธนาคารที่ถูกละเมิดได้ และตั้งแต่เดือนพฤศจิกายน ค.ศ. ๒๐๒๓ ได้มีการนำฟิเจอร์ “Money Lock”^{๑๕} ซึ่งเป็นกลไกด้านความปลอดภัยมาใช้เพื่อให้ลูกค้าสามารถกักเงินจำนวนหนึ่งไว้โดยไม่สามารถโอนหรือใช้ผ่านระบบดิจิทัลได้ ขณะเดียวกัน CPF Board ได้กำหนดวงเงินเริ่มต้นในการถอนเงินผ่านระบบออนไลน์ไว้ที่ ๒,๐๐๐ ดอลลาร์สิงคโปร์ต่อวัน และไม่สามารถปรับเพิ่มได้โดยปราศจากการยืนยันตัวตนที่มีความมั่นคงสูง ทั้งนี้ สมาชิกยังสามารถเลือกปรับลดวงเงินดังกล่าวลงเป็นศูนย์เพื่อระงับการถอนเงินออนไลน์ทั้งหมดได้

(ข) การป้องกันการหลอกลวง (Preventing scams)

รัฐบาลดำเนินมาตรการเชิงป้องกันเพื่อขัดขวางมิให้มีฉ้อโกงเข้าถึงเหยื่อ ตลอดจนเพิ่มความเข้มงวดในการบังคับใช้กฎหมายเพื่อยับยั้งการกระทำความผิด

๑) IMDA^{๑๖} ยกระดับมาตรการป้องกันการโทรหลอกลวงและข้อความ SMS หลอกลวงอย่างต่อเนื่อง อาทิ การบล็อกสายโทรศัพท์จากหมายเลขที่ทราบว่าจะเกี่ยวข้องกับการหลอกลวง และหมายเลขภายในประเทศที่ถูกปลอมแปลง การบล็อกการโทรศัพท์แบบอัตโนมัติ (robocalls) โดยการใช้การ

^{๑๒} Ministry of Digital Development and Information, “Measures to protect Singaporeans against online scams”, สืบค้นเมื่อวันที่ ๒ มิถุนายน ๒๕๖๙, จาก Measures to protect Singaporeans against online scams | Ministry of Digital Development and Information

^{๑๓} คณะกรรมการกองทุนสำรองเลี้ยงชีพส่วนกลางของสิงคโปร์ (Central Provident Fund Board : CPF), สืบค้นเมื่อวันที่ ๒ มิถุนายน ๒๕๖๙ จาก บทความเรื่อง “ระบบการประกันสังคมของประเทศสิงคโปร์” – สำนักงานแรงงานในประเทศสิงคโปร์

^{๑๔} Kill-Switch คือ การระงับการใช้บริการ mobile banking ด้วยตนเอง, สืบค้นเมื่อวันที่ ๒ มิถุนายน ๒๕๖๙ จาก หัวเรื่องที่ต้องการนำเสนอ

^{๑๕} แนวคิดเกี่ยวกับ “Money Lock” ได้รับการกำกับและผลักดันโดย Monetary Authority of Singapore (MAS) ร่วมกับ Association of Banks in Singapore (ABS) เป็นมาตรการที่เปิดโอกาสให้ผู้ให้บริการธนาคารสามารถกักเงินบางส่วนออกจากการทำธุรกรรมผ่านระบบดิจิทัล โดยลูกค้าธนาคารเป็นผู้กำหนดจำนวนเงินที่ต้องการ “ล็อก” ซึ่งเงินดังกล่าวยังคงปรากฏในบัญชีและได้รับดอกเบี้ยตามปกติ อย่างไรก็ตาม เงินที่ถูกกำหนดดังกล่าวจะไม่สามารถโอนออกผ่านทางธนาคารบนมือถือหรือระบบออนไลน์ได้ แม้ในกรณีที่มิฉ้อโกงสามารถเข้าควบคุมอุปกรณ์ของผู้ใช้บริการได้ก็ตาม โดยการปลดล็อกเงินจำเป็นต้องดำเนินการผ่านการยืนยันตัวตนด้วยตนเอง ณ สาขาของธนาคารหรือเครื่องเอทีเอ็ม, สืบค้นเมื่อวันที่ ๒ มิถุนายน ๒๕๖๙, จาก Fraud Solutions WP_web.pdf

^{๑๖} Infocomm Media Development Authority (IMDA) เป็นหน่วยงานหลักที่มีบทบาทสำคัญในการขับเคลื่อนการเปลี่ยนผ่านสู่ดิจิทัลของประเทศสิงคโปร์ โดยมุ่งพัฒนาโครงสร้างพื้นฐานด้านดิจิทัล และส่งเสริมนวัตกรรมทางดิจิทัล เพื่อสนับสนุนการพัฒนากำลังแรงงานดิจิทัลที่มีศักยภาพ ตลอดจนสร้างสังคมดิจิทัลที่มีความปลอดภัย ครอบคลุม และสามารถปรับตัวได้อย่างยั่งยืนในบริบทของสภาพแวดล้อมดิจิทัลที่มีการเปลี่ยนแปลงอย่างรวดเร็วในปัจจุบัน, สืบค้นเมื่อวันที่ ๒ มิถุนายน ๒๕๖๙, จาก Who We Are | IMDA

ตรวจจับรูปแบบ และการบล็อกข้อความ SMS ที่มีเนื้อหาอันเป็นอันตรายหรือมีลิงก์ที่ไม่ปลอดภัย โดยมาตรการดังกล่าวสามารถช่วยป้องกันสายโทรศัพท์ที่อาจเป็นการหลอกลวงได้มากกว่า ๓๑๐ ล้านสาย ในปี ค.ศ. ๒๐๒๓ และจำนวนสายโทรจากต่างประเทศที่พยายามปลอมหมายเลขภายในประเทศลดลงอย่างมีนัยสำคัญจาก ๗๐๖ ล้านสายในปี ค.ศ. ๒๐๒๒ เหลือเพียง ๑๘ ล้านสายในปี ค.ศ. ๒๐๒๓

๒) ตั้งแต่เดือนมกราคม ค.ศ. ๒๐๒๓ ได้มีการกำหนดให้ต้องจดทะเบียนชื่อผู้ส่ง SMS แบบอักษร (alphanumeric sender ID) ทั้งหมดในระบบทะเบียน Singapore SMS Sender ID Registry (SSIR) เพื่อป้องกันการปลอมแปลงชื่อผู้ส่งที่ถูกต้อง และกำหนดให้ข้อความจากผู้ส่งที่ไม่ได้ลงทะเบียนถูกระบุว่าเป็น “Likely-SCAM” ส่งผลให้จำนวนคดี SMS หลอกลวงลดลงร้อยละ ๗๐ ภายในระยะเวลา ๓ เดือนหลังการบังคับใช้มาตรการดังกล่าว

๓) ตั้งแต่ปี ค.ศ. ๒๐๒๒ รัฐบาลกำหนดให้มีการยืนยันตัวตนด้วยใบหน้า (facial verification) ผ่านระบบ Singpass สำหรับธุรกรรมที่มีความเสี่ยงสูง และตั้งแต่เดือนมิถุนายน ค.ศ. ๒๐๒๓ ได้ขยายมาตรการดังกล่าวไปยังบริการ CPF ที่มีความเสี่ยงสูง ส่งผลให้ไม่พบรายงานกรณีการหลอกลวงผ่านมัลแวร์ที่เกี่ยวข้องกับการถอนเงิน CPF โดยมีขบอีกต่อไป

๔) ได้มีการแก้ไขกฎหมายเพื่อกำหนดบทลงโทษที่เข้มงวดขึ้นสำหรับบุคคลที่ยินยอมให้มิฉาซีพีใช้บัญชี Singpass หรือบัญชีธนาคารของตนโดยมิชอบ รวมถึงกรณีการขายบัญชีธนาคารหรือเปิดเผยข้อมูลการเข้าถึง Singpass เพื่ออำนวยความสะดวกในการกระทำความผิด

๕) ตรากฎหมาย Online Criminal Harms Act ซึ่งกำหนดหน้าที่เชิงป้องกันล่วงหน้า (ex-ante requirements) ให้แพลตฟอร์มออนไลน์ต้องดำเนินการเพื่อคุ้มครองผู้ใช้บริการ และให้อำนาจแก่หน่วยงานของรัฐในการสั่งระงับบัญชีหรือเนื้อหาที่เป็นการฉ้อโกงได้โดยรวดเร็ว เพื่อป้องกันมิให้ผู้ร้ายอื่นตกเป็นเหยื่อ (ซึ่งจะกล่าวถึงโดยละเอียดในหัวข้อต่อไป)

(ค) การส่งเสริมสภาพแวดล้อมออนไลน์ที่ปลอดภัยและน่าเชื่อถือ (Fostering a safe and trusted online environment)

รัฐบาลร่วมมือกับภาคเอกชนเพื่อให้บริษัทต่าง ๆ ยกระดับมาตรการด้านความปลอดภัย เพื่อให้ผู้ใช้สามารถทำธุรกรรมและมีปฏิสัมพันธ์ทางออนไลน์ได้อย่างปลอดภัย ดังต่อไปนี้

๑) ร่วมมือกับธนาคารหลักในการพัฒนาแนวทางตรวจจับการฉ้อโกงและภัยคุกคามจากมัลแวร์ เพื่อป้องกันการเข้าถึงบัญชีโดยไม่ได้รับอนุญาต โดยธนาคารหลายแห่งได้ปรับปรุงแอปพลิเคชันของตนเพื่อป้องกันการเข้าถึงจากอุปกรณ์ที่อาจติดมัลแวร์

๒) เสริมสร้างความร่วมมือกับผู้ประกอบการภาคเอกชน เช่น Google เพื่อออกแบบฟีเจอร์ด้านความปลอดภัยสำหรับอุปกรณ์ของผู้ใช้ในสิงคโปร์ โดยมุ่งให้ระบบและอุปกรณ์มีความปลอดภัยตั้งแต่ขั้นตอนการออกแบบ (secure-by-design) เพื่อลดความเสี่ยงจากการหลอกลวงผ่านมัลแวร์

๓) ดำเนินการตามกรอบ Shared Responsibility Framework (SRF) เพื่อกำหนดให้ธนาคารและผู้ให้บริการโทรคมนาคมมีความรับผิดชอบต่อมาตรการคุ้มครองลูกค้าจากการโจมตีแบบฟิชซิง และเพื่อให้เหยื่อสามารถใช้สิทธิเรียกร้องได้อย่างรวดเร็วในกรณีที่หน่วยงานดังกล่าวไม่ปฏิบัติตามที่ตามมาตรการป้องกันการหลอกลวง

๔) รัฐบาลจัดทำโครงการให้ความรู้แก่ประชาชนเพื่อเสริมสร้างศักยภาพในการป้องกันตนเองจากการหลอกลวง อาทิ บุคคลทั่วไปสามารถใช้หลักการ “ACT” ในการป้องกันการหลอกลวง โดยการติดตั้งแอปพลิเคชัน ScamShield การใช้ฟีเจอร์ด้านความปลอดภัย การตรวจสอบสัญญาณเตือนของการหลอกลวง และการแจ้งเหตุแก่หน่วยงานที่เกี่ยวข้องหรือเจ้าของแพลตฟอร์มเมื่อพบการหลอกลวง หรือประชาชนยังสามารใช้เครื่องมือให้ความรู้สำหรับผู้บริโภค เช่น ระบบการให้คะแนนความปลอดภัยของธุรกรรมในตลาดออนไลน์ (Transaction Safety Ratings: TSR) และ Internet Hygiene Portal (IHP) เพื่อประกอบการตัดสินใจในการทำธุรกรรมออนไลน์อย่างมีข้อมูลและรอบคอบ^{๑๗}

(๒) ระดับระหว่างประเทศ

เพื่อพัฒนาแนวทางที่มีความเป็นระบบและสอดคล้องกันในระดับโลกในการจัดการกับภัยคุกคามดังกล่าว รัฐบาลสิงคโปร์โดย IMDA ได้ดำเนินการสร้างความร่วมมือกับหน่วยงานกำกับดูแลในต่างประเทศ เพื่อส่งเสริมการแลกเปลี่ยนองค์ความรู้และความเข้าใจเกี่ยวกับมาตรการและแนวทางในการป้องกันและปราบปราม Cyber Scam โดย IMDA ได้ลงนามบันทึกความเข้าใจ (Memorandum of Understanding: MoU) กับหน่วยงานกำกับดูแลในต่างประเทศหลายแห่ง เพื่อเสริมสร้างความร่วมมือข้ามพรมแดนในการรับมือกับการสื่อสารที่เกี่ยวข้องกับการหลอกลวงและข้อความไม่พึงประสงค์ ซึ่งเป็นส่วนหนึ่งของแนวทางเชิงยุทธศาสตร์ในระดับระหว่างประเทศของ IMDA ในการทำงานร่วมกับหน่วยงานกำกับดูแลต่างประเทศ เพื่อเพิ่มประสิทธิภาพในการป้องกันและปราบปรามการหลอกลวงที่เกิดขึ้นผ่านช่องทางสื่อสาร อาทิ ข้อความสั้น (SMS) และการติดต่อทางโทรศัพท์ โดยมีความร่วมมือระหว่างประเทศที่สำคัญ ได้แก่ การดำเนินงานร่วมกับ United States Federal Communications Commission, New Zealand Department of Internal Affairs, Australian Communications and Media Authority และ Malaysian Communications and Multimedia Commission)^{๑๘}

๔. กฎหมายที่ใช้บังคับเกี่ยวกับ Cyber Scam

(๑) The Computer Misuse Act 1993^{๑๙} (กฎหมาย CMA) มีบทบาที่สำคัญในฐานะกฎหมายที่มุ่งควบคุมการใช้ระบบคอมพิวเตอร์โดยมิชอบ โดยเฉพาะพฤติกรรมที่เกี่ยวข้องกับการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การแก้ไขหรือแทรกแซงข้อมูล และการใช้บริการคอมพิวเตอร์เพื่อวัตถุประสงค์ที่มิชอบ กฎหมายฉบับนี้จึงมีความเกี่ยวข้องกับการกระทำความผิดเกี่ยวกับ cyber scam โดยตรง ในส่วนที่การหลอกลวงผ่านระบบดิจิทัลต้องอาศัยการเข้าถึงหรือควบคุมระบบคอมพิวเตอร์ของผู้อื่น เช่น การเข้าถึงบัญชี การดักข้อมูล หรือการใช้ข้อมูลรับรอง (credentials) โดยมิชอบ

Part 1 เป็นบทเบื้องต้นที่กำหนดหน้าที่ทั้งในการกำหนดคำจำกัดความและวางหลักเกณฑ์สำหรับการตีความองค์ประกอบความผิดตามกฎหมายฉบับนี้ โดย section 2 กำหนดนิยามสำคัญ

^{๑๗} โปรดดูเชิงอรรถที่ ๑๒

^{๑๘} Infocomm Media Development Authority, “Anti-Scam Measures”, สืบค้นเมื่อวันที่ ๒ มิถุนายน ๒๕๖๙, จาก Anti-Scam Measures | IMDA

^{๑๙} สืบค้นเมื่อวันที่ ๒ มิถุนายน ๒๕๖๙, จาก https://sso.agc.gov.sg/Act/CMA1993?ViewType=Pdf&_id=20260121200812

หลายประการ อาทิ “computer”, “computer service”, “damage”, “data”, “intercept” และ “program or computer program” ตลอดจนคำว่า “scam offence” ซึ่งหมายถึงความผิดที่ระบุไว้ใน Second Schedule ทำกฎหมาย นอกจากนี้ Part 1 ยังมีความสำคัญในเชิงโครงสร้าง เพราะบัญญัติหลักเกณฑ์ว่าการกระทำใดถือเป็นการได้มาซึ่งการเข้าถึง (secure access) โปรแกรมหรือข้อมูล การเข้าถึงโดยไม่ได้รับอนุญาต และการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต อันเป็นฐานคิดที่ใช้ประกอบการตีความความผิดใน Part 2 ทั้งระบบ

Part 2 (sections 3–12) เป็นบทบัญญัติว่าด้วยความผิดตามกฎหมาย CMA ซึ่งแบ่งได้เป็น ๕ กลุ่ม ดังนี้

(ก) ความผิดเกี่ยวกับการเข้าถึงและใช้ระบบคอมพิวเตอร์โดยมิชอบ (section 3, section 4 และ section 6) โดย section 3 เป็นความผิดฐานเข้าถึงโปรแกรมหรือข้อมูลในคอมพิวเตอร์โดยไม่มีอำนาจ ส่วน section 4 เป็นความผิดฐานเข้าถึงโปรแกรมหรือข้อมูลด้วยเจตนาจะกระทำความผิดอีกฐานหนึ่งที่กฎหมายกำหนด ทั้งนี้ จุดสำคัญของ section 4 คือ ตัวบทถือว่าไม่เป็นสาระว่าการเข้าถึงนั้นเป็นการเข้าถึงโดยมีอำนาจหรือไม่ หากผู้กระทำความผิดจะใช้การเข้าถึงนั้นเป็นเครื่องมือไปสู่ความผิดเกี่ยวกับทรัพย์สิน ฉ้อโกง ความไม่ซื่อสัตย์ หรือความผิดที่ก่อให้เกิดอันตรายแก่ร่างกาย สำหรับ section 6 เป็นความผิดเกี่ยวกับการใช้หรือการดักจับ (intercept^{๒๐}) บริการคอมพิวเตอร์โดยมิชอบ ซึ่งครอบคลุมทั้งการเข้าถึงคอมพิวเตอร์เพื่อให้ได้มาซึ่ง computer service โดยไม่มีอำนาจ การดักจับการทำงานของคอมพิวเตอร์โดยไม่ได้รับอนุญาต และการใช้คอมพิวเตอร์หรืออุปกรณ์อื่นเพื่อกระทำการดังกล่าว ในเชิงนโยบายกฎหมาย กลุ่มบทบัญญัติเหล่านี้มีนัยสำคัญต่อการรับมือ cyber scam เพราะพฤติกรรมอย่าง phishing, credential harvesting หรือการดักจับข้อมูลเพื่อนำไปหลอกลวงทางออนไลน์มักเริ่มต้นจากการเข้าถึงหรือใช้บริการคอมพิวเตอร์โดยมิชอบก่อนจะลุกลามไปสู่การฉ้อโกงต่อทรัพย์สินหรือข้อมูลของผู้เสียหาย

(ข) ความผิดเกี่ยวกับการแก้ไข ทำลาย หรือรบกวนระบบและข้อมูลคอมพิวเตอร์ (section 5 และ section 7) โดย section 5 ว่าด้วยการกระทำที่ผู้กระทำรู้ว่าจะก่อให้เกิดการแก้ไขข้อมูลหรือเนื้อหาในคอมพิวเตอร์โดยไม่มีอำนาจ ไม่ว่าการแก้ไขนั้นจะเป็นการเปลี่ยนแปลงถาวรหรือชั่วคราว ส่วน section 7 ว่าด้วยการแทรกแซง ขัดขวาง หรือรบกวนการใช้คอมพิวเตอร์โดยชอบด้วยกฎหมาย รวมทั้งการขัดขวางการเข้าถึงหรือทำให้ประโยชน์ใช้สอยหรือประสิทธิภาพของโปรแกรมหรือข้อมูลที่เก็บอยู่ในคอมพิวเตอร์ลดลง บทบัญญัติกลุ่มนี้สะท้อนว่ากฎหมายมิได้มุ่งคุ้มครองเพียง “การเข้าถึงข้อมูล” เท่านั้น แต่ยังคุ้มครอง “ความพร้อมใช้” และ “ความสมบูรณ์” ของระบบและข้อมูล ซึ่งเป็นคุณค่าแกนกลางของความมั่นคงปลอดภัยไซเบอร์ในทางกฎหมายอาญา

^{๒๐} Interpretation

2.—(1) In this Act, unless the context otherwise requires —
etc. etc.

“intercept”, in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;
etc. etc.

(ค) ความผิดเชิงป้องกันเกี่ยวกับรหัส ข้อมูลที่ระบุตัวตน (identity) ข้อมูลที่ใช้ยืนยันตัวตน (credential) และเครื่องมือที่ใช้ก่ออาชญากรรมคอมพิวเตอร์ (section 8, section 8A, section 8B, section 9 และ section 10) โดย section 8 ว่าด้วยการเปิดเผยรหัสผ่าน รหัสการเข้าถึง หรือวิธีการเข้าถึงข้อมูลหรือระบบโดยไม่มีอำนาจเพื่อประโยชน์โดยมิชอบ เพื่อการอันมิชอบด้วยกฎหมาย หรือโดยรู้ว่าจะก่อให้เกิดความเสียหายโดยมิชอบแก่ผู้อื่น ขณะที่ section 8A และ section 8B เป็นบทเฉพาะที่เกี่ยวข้องกับ national digital identity service และข้อมูลที่ใช้ยืนยันตัวตน (credential) ของบุคคลอื่น ส่วน section 9 เป็นความผิดเกี่ยวกับการจัดหา ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลที่ได้มาโดยฝ่าฝืนบทบัญญัติบางมาตราในกฎหมายนี้ และ section 10 ว่าด้วยการได้มา ครอบครอง หรือจัดการสิ่งของสำหรับใช้ในการกระทำความผิดบางประเภท ซึ่งได้แก่ อุปกรณ์ใด ๆ รวมทั้งโปรแกรมคอมพิวเตอร์ ซึ่งได้รับการออกแบบหรือดัดแปลงโดยมีวัตถุประสงค์หลัก หรือสามารถใช้ได้ เพื่อประโยชน์ในการกระทำความผิดตาม section 3, 4, 5, 6 และ 7 รหัสผ่าน รหัสการเข้าถึง หรือข้อมูลในลักษณะคล้ายคลึงกันซึ่งทำให้สามารถเข้าถึงคอมพิวเตอร์ได้ บทบัญญัติกลุ่มนี้มีลักษณะเป็นบทบัญญัติความผิดในลักษณะเชิงป้องกัน (preventive offences) ที่มุ่งตัดวงจรของอาชญากรรมตั้งแต่ขั้นเตรียมการอย่างเด่นชัด โดยเฉพาะในบริบท cyber scam ซึ่งการซื้อขายบัญชี มอบข้อมูลรับรองตัวตน (credential) ให้ผู้อื่น หรือส่งต่อข้อมูลส่วนบุคคลที่ได้มาโดยมิชอบ มักเป็นกลไกสำคัญในการอำพรางตัวผู้กระทำและขยายผลการหลอกลวง

(ง) ความผิดที่มีลักษณะเป็นเหตุฉกรรจ์เมื่อเกี่ยวข้องกับคอมพิวเตอร์ที่ได้รับ **ความคุ้มครอง (protected computers)** (section 11) ซึ่งเป็นเหตุเพิ่มโทษสำหรับการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ที่ได้รับความคุ้มครองเป็นพิเศษ แนวคิดของบทบัญญัตินี้อยู่บนฐานที่ว่าความเสียหายต่อระบบคอมพิวเตอร์บางประเภทมีผลกระทบต่อสาธารณะหรือความมั่นคงสูงกว่าปกติ จึงสมควรได้รับการคุ้มครองที่เข้มข้นกว่า

(จ) ความผิดฐานสนับสนุน พยายาม หรือกระทำการเตรียมการเพื่อนำไปสู่ความผิดตามกฎหมายนี้ (section 12) ซึ่งบัญญัติให้การสนับสนุน การพยายาม หรือการกระทำอันเป็นขั้นเตรียมการ หรือเพื่อส่งเสริมการกระทำความผิดตามกฎหมายนี้ เป็นความผิดได้เช่นกัน จึงทำให้โครงสร้างของกฎหมายฉบับนี้ครอบคลุมตั้งแต่การเตรียมการ การเข้าถึง การใช้ การดัดแปลง การเปิดเผยข้อมูลหรือเครื่องมือ ตลอดจนผลกระทบที่ร้ายแรงต่อ protected computers อย่างเป็นลำดับครบวงจร

(๒) The Online Criminal Harms Act 2023^{๒๑} (กฎหมาย OCHA) เป็นกฎหมายที่ตราขึ้นเพื่อให้รัฐมีเครื่องมือแทรกแซงกิจกรรมออนไลน์ที่เกี่ยวข้องเนื่องกับการก่ออาชญากรรมได้อย่างรวดเร็วและมีประสิทธิภาพ โดยเฉพาะการหลอกลวงทางไซเบอร์และกิจกรรมไซเบอร์ที่เป็นอันตราย กฎหมายฉบับนี้จึงมิได้มุ่งเพียงการระงับเนื้อหาที่ผิดกฎหมายเท่านั้น แต่ยังครอบคลุมมาตรการเชิงป้องกันการกำกับผู้ให้บริการแพลตฟอร์มออนไลน์ และกลไกบังคับใช้ต่อผู้ไม่ปฏิบัติตามคำสั่งของรัฐด้วย

^{๒๑} สืบค้นเมื่อวันที่ ๒ มิถุนายน ๒๕๖๙, จาก https://sso.agc.gov.sg/Act/OCHA2023?ViewType=Pdf&_id=20260814195031

บุคคลและกิจกรรมที่อยู่ภายใต้บังคับแห่งกฎหมาย OCHA นี้เป็นไปตามที่บัญญัติไว้ใน Section 2 ซึ่งแยกอธิบายได้เป็น ๒ กลุ่ม ได้แก่ (๑) บุคคล และ (๒) การกระทำ อย่างไรก็ตาม Section 2 ยังมีนิยามสำคัญอื่นอีกหลายประการ เช่น “online activity” “online location”, “online material”, “Singapore person”, “specified offence”, “Part 2 direction” และ “Part 6 order” ซึ่งเป็นฐานแนวคิดของกลไกบังคับใช้ตามกฎหมายฉบับนี้ด้วย

กระบวนการดำเนินการตาม OCHA จะเกิดขึ้นเมื่อเจ้าหน้าที่ที่ได้รับการแต่งตั้งเฉพาะ (designated officer) มีเหตุอันควรสงสัยว่ามีความผิดที่กำหนดไว้ (specified offence) เกิดขึ้นแล้ว และมีกิจกรรมออนไลน์ที่เป็นไปเพื่อส่งเสริมการกระทำความผิดนั้น หรือมีเหตุสงสัยหรือเหตุให้เชื่อได้ว่า กิจกรรมออนไลน์ใดเป็นการเตรียมการหรือเป็นไปเพื่อส่งเสริมการกระทำความผิดเกี่ยวกับ scam หรือ ความผิดเกี่ยวกับกิจกรรมไซเบอร์ที่เป็นอันตราย (malicious cyber activity offence) ดังนั้น กฎหมายฉบับนี้จึงเชื่อมโยงกับความผิด Cyber scam โดยตรง เพราะให้อำนาจรัฐเข้าแทรกแซงได้ตั้งแต่วะเตรียมการหรือระยะที่กิจกรรมออนไลน์ยังทำหน้าที่ “เอื้อ” ต่อการหลอกลวงหรือกิจกรรมไซเบอร์ที่เป็นอันตราย

ภายใต้ Part 2 เจ้าหน้าที่อาจออกคำสั่งได้ ๕ ประเภท ได้แก่ (๑) คำสั่งให้ระงับการสื่อสาร (stop communication direction) เพื่อให้ผู้ควบคุมเนื้อหาที่เกี่ยวข้องหรือเจ้าของสถานที่ออนไลน์ที่เกี่ยวข้องลบเนื้อหา หยุดเก็บ โพสต์ จัดหา หรือส่งต่อเนื้อหาที่คล้ายกัน หรือปิดกั้นการเข้าถึงสถานที่ออนไลน์นั้น (๒) คำสั่งให้ปิดการเข้าถึง (disabling direction) เพื่อให้ผู้ให้บริการออนไลน์ปิดการเข้าถึงของบุคคลในสิงคโปร์ต่อเนื้อหาหรือสถานที่ออนไลน์ที่เกี่ยวข้องบนบริการของตน (๓) คำสั่งปิดกั้นการเข้าถึง (access blocking direction) เพื่อให้ผู้ให้บริการอินเทอร์เน็ตปิดกั้นการเข้าถึงของบุคคลในสิงคโปร์ไปยังสื่อหรือสถานที่ออนไลน์ที่เกี่ยวข้อง (๔) คำสั่งจำกัดบัญชี (account restriction direction) เพื่อไม่อนุญาตหรือจำกัดการปฏิสัมพันธ์ระหว่างบัญชีที่เกี่ยวข้องกับบุคคลในสิงคโปร์ ซึ่งอาจรวมถึงการยุติระงับ หรือจำกัดบางฟังก์ชันของบริการออนไลน์ และ (๕) คำสั่งให้ลบแอป (app removal direction) เพื่อให้ผู้ให้บริการจำหน่ายแอประงับการเผยแพร่และยับยั้งการดาวน์โหลดแอปที่เกี่ยวข้องโดยบุคคลในสิงคโปร์

นอกจากมาตรการเฉพาะรายดังกล่าวแล้ว กฎหมาย OCHA ยังมี Part 4 ซึ่งให้อำนาจแก่ competent authority กำหนดบริการออนไลน์บางประเภทให้เป็นบริการออนไลน์ที่กำหนด (designated online service) ได้ หากเห็นว่าบริการนั้นถูกใช้หรือมีแนวโน้มจะถูกใช้ในการอำนวยความสะดวกหรือก่อความผิดในกลุ่มความผิดที่เกี่ยวข้อง และบุคคลในสิงคโปร์สามารถเข้าถึงบริการนั้นได้ เมื่อมีการกำหนดเช่นนั้นแล้ว competent authority อาจออกแนวปฏิบัติ (code of practice), หนังสือแจ้งให้ใช้แนวปฏิบัติ (code application notice), หนังสือแจ้งให้แก้ไขข้อบกพร่อง (rectification notice) และคำสั่งให้ดำเนินการมาตรการ (implementation directive) เพื่อบังคับให้ผู้ให้บริการจัดให้มีระบบกระบวนการ หรือมาตรการที่เหมาะสมในการลดความเสี่ยงจากความผิดที่เกี่ยวข้องได้

ในมิติของ Cyber scam มาตรการตาม Part 4 และ Third Schedule มีความสำคัญอย่างยิ่ง เพราะไม่ได้มุ่งเพียงการลบหรือบล็อกเนื้อหาที่เป็นปัญหา แต่ยังกำหนดวัตถุประสงค์ของระบบหรือมาตรการที่ผู้ให้บริการพึงมี เช่น การลดการสัมผัสของผู้ใช้ในสิงคโปร์ต่อ scam หรือกิจกรรมไซเบอร์ที่

เป็นอันตราย การตรวจสอบความแท้จริงของบัญชี การป้องกันบัญชีปลอมและการปลอมตัว การรับข้อมูลจากผู้ที่เกี่ยวข้อง scam ที่สงสัย การแลกเปลี่ยนข้อมูลกับ competent authority การตรวจจับและยับยั้งเชิงรุก การเก็บรักษาข้อมูลเพื่อสนับสนุนการสืบสวน และการมีกลไกคุ้มครองการชำระเงินออนไลน์

หากผู้รับคำสั่งหรือผู้ให้บริการไม่ปฏิบัติตามข้อกำหนดดังกล่าว กฎหมายยังให้อำนาจ competent authority ออก Part 6 orders against non-compliance ได้อีก ๓ ประเภท ได้แก่ คำสั่งปิดกั้นการเข้าถึง (access blocking order), คำสั่งให้ลบแอป (app removal order) และคำสั่งจำกัดการให้บริการ (service restriction order) เพื่อจำกัดหรือปิดกั้นการให้บริการของผู้ให้บริการที่ไม่ปฏิบัติตามคำสั่งเดิม อันเป็นกลไกบังคับใช้ต่อเนื่องเพื่อให้การแทรกแซงของรัฐมีประสิทธิภาพในทางปฏิบัติ

ในกรณีที่ผู้ได้รับคำสั่งประสงค์จะได้แย้งคำสั่งดังกล่าว OCHA กำหนดกลไกทบทวนและอุทธรณ์ไว้ โดยมีได้ใช้ถ้อยคำอย่างกว้างว่าอุทธรณ์ต่อ “ศาล” เสมอไป กล่าวคือ ผู้ได้รับ “Part 2 direction” ต้องยื่นคำขอให้พิจารณาใหม่ (reconsideration) ต่อเจ้าหน้าที่ที่ได้รับการแต่งตั้ง (designated officer) ก่อน และหากยังไม่พอใจจึงอุทธรณ์ต่อคณะพิจารณาทบทวนคำสั่ง (Reviewing Tribunal) ได้ ส่วนผู้ได้รับ Part 6 order ต้องร้องขอให้มีการพิจารณาใหม่ต่อ competent authority ก่อนแล้วจึงอุทธรณ์ต่อคณะพิจารณาทบทวนคำสั่งได้ ขณะที่กรณีคำสั่งหรือข้อกำหนดตาม Part 4 ผู้มีสิทธิอุทธรณ์จะยื่นอุทธรณ์ต่อรัฐมนตรี และรัฐมนตรีอาจอาศัยความเห็นของคณะกรรมการที่ปรึกษาการอุทธรณ์ (Appeals Advisory Committee) มาประกอบการพิจารณา

นอกจากนี้ OCHA ยังให้อำนาจเรียกข้อมูลที่จำเป็นต่อการบริหารกฎหมายและการสืบสวนเกี่ยวกับกิจกรรมออนไลน์ (online activity) ที่เกี่ยวเนื่องกับความผิดที่กำหนด scam หรือความผิดเกี่ยวกับกิจกรรมไซเบอร์ที่เป็นอันตรายได้ และมีบทกำหนดโทษสำหรับการไม่ปฏิบัติตาม Part 2 directions, หนังสือแจ้งให้แก้ไขข้อบกพร่อง, คำสั่งให้ดำเนินมาตรการ, Part 6 orders และหนังสือแจ้งเรียกข้อมูล รวมทั้งกำหนดเรื่องข้อต่อสู้ ความผิดที่จับได้และประกันตัว และเขตอำนาจศาลสำหรับการกระทำนอกราชอาณาจักรไว้ด้วย

กล่าวโดยสรุป OCHA เป็นกฎหมายที่ออกแบบมาเพื่อรับมือกับอาชญากรรมออนไลน์และ Cyber scam อย่างเป็นระบบ ตั้งแต่มาตรการเชิงปฏิบัติการต่อเนื่องหา บัญชี สถานะออนไลน์ และแอป มาตรการกำกับแพลตฟอร์มในระดับโครงสร้าง ไปจนถึงกลไกบังคับใช้ต่อผู้ไม่ปฏิบัติตามและอำนาจเรียกข้อมูลเพื่อสนับสนุนการสืบสวนและป้องกันความเสียหายล่วงหน้า^{๒๒}

(๓) The Protection from Scams Act 2025^{๒๓} (กฎหมาย PSA) เป็นกฎหมายที่มุ่งป้องกันความเสียหายจากการหลอกลวงทางไซเบอร์โดยการแทรกแซงทางการเงินโดยตรงต่อเหยื่อ

^{๒๒} เนื้อหาส่วนนี้ได้ปรับปรุงเพิ่มเติมจากบทความ “รัฐบัญญัติว่าด้วยอันตรายที่เป็นความผิดอาญาทางออนไลน์ของสิงคโปร์ (The Online Criminal Harms Act 2023 :OCHA)” ซึ่งตีพิมพ์ใน “กฤษฎีกาสาร” ปีที่ ๒๐ ฉบับที่ ๑ (ต.ค. - พ.ย. ๒๕๖๗) หน้า ๑๕-๑๙, สืบค้นเมื่อวันที่ ๓ มิถุนายน ๒๕๖๙, จาก MDUyMDU1MDNhMDdIMDVjMDUwMDNlMDdiMDQyMDY3MDNkMDdIMDRiMDU1MDc4MDRmMDZjMDU0

^{๒๓} สืบค้นเมื่อวันที่ ๒ มิถุนายน ๒๕๖๙, จาก https://sso.agc.gov.sg/Act/PSA2025?ViewType=Pdf&_id=20251030155907

กฎหมายฉบับนี้ให้อำนาจเจ้าหน้าที่ออกคำสั่งจำกัดธุรกรรมทางธนาคารและการใช้สินเชื่อของบุคคลที่มีความเสี่ยงจะตกเป็นเหยื่อของการหลอกลวง เพื่อหยุดยั้งความเสียหายก่อนที่จะเกิดขึ้น

กฎหมาย PSA มี ๔ หมวด ได้แก่ หมวด ๑ บทบัญญัติเบื้องต้น หมวด ๒ คำสั่งจำกัด (Restriction order : RO) หมวด ๓ การอุทธรณ์ และหมวด ๔ บทเบ็ดเตล็ด โดยหลักการและแนวทางปฏิบัติสำคัญจะอยู่ในหมวด ๒ และหมวด ๓

ในเบื้องต้น ต้องทำความเข้าใจเกี่ยวกับบทนิยามในกฎหมายฉบับนี้ซึ่งบัญญัติไว้ใน Section 2 ก่อน ซึ่งได้แก่

“ธนาคาร” หมายความว่า ธนาคารในสิงคโปร์ตามที่กำหนดใน Section 2 (1) แห่งรัฐบัญญัติการธนาคาร ค.ศ. ๑๙๗๐

“บัญชีธนาคาร” หมายความว่า บัญชีที่ตกเป็นเหยื่อของการหลอกลวง โดย (ก) มีเงินในบัญชีซึ่งเป็นชื่อของเหยื่อของการหลอกลวง หรือ (ข) มีเงินอยู่ในบัญชีซึ่งชื่อของบุคคลตั้งแต่สองคนขึ้นไป โดยหนึ่งในนั้นเป็นเหยื่อ

“อุปกรณ์การสื่อสาร” หมายความว่า เครื่องจักรหรืออุปกรณ์ที่ใช้ในการส่งหรือรับข้อมูลหรือการสื่อสารในรูปแบบต่าง ๆ ตามที่กฎหมายกำหนด

“วงเงินสินเชื่อ” หมายความว่า เงินกู้หรือสิ่งอำนวยความสะดวกทางการเงินที่ธนาคารให้แก่ลูกค้า

“การสื่อสารทางไกล” หมายความว่า การสื่อสารผ่านอินเทอร์เน็ต โทรศัพท์ หรือเทคโนโลยีอิเล็กทรอนิกส์อื่น

“เหยื่อการหลอกลวง” หมายความว่า บุคคลธรรมดาซึ่งถูกกระทำความผิดฐานหลอกลวงหรือมีเจตนาจะถูกกระทำความผิดดังกล่าว

“ความผิดฐานหลอกลวง” หมายความว่า ความผิดใด ๆ ตามที่กำหนดไว้ในบัญชีท้ายกฎหมาย

“ผู้หลอกลวง” หมายความว่า บุคคลใด ๆ ที่เจ้าหน้าที่เชื่อตามสมควรว่าได้กระทำหรือมีส่วนเกี่ยวข้องกับการหลอกลวง

ดังที่กล่าวไว้ข้างต้นว่า สาระสำคัญของกฎหมายฉบับนี้อยู่ในหมวด ๒ ว่าด้วยคำสั่งจำกัด (Restriction order : RO) และหมวด ๓ ว่าด้วยอุทธรณ์ กระบวนการทางกฎหมายทั้งหมดจะเริ่มต้นขึ้นเมื่อเจ้าหน้าที่ได้รับแจ้งข้อมูลและปรากฏว่ามีเหตุผลอันสมควรเชื่อได้ว่าเหยื่อผู้ถูกหลอกลวงจะ (ก) สั่งให้ธนาคารโอนเงินจากบัญชีธนาคารไปยังผู้หลอกลวง (ข) ถอนเงินจากบัญชีธนาคารโดยตั้งใจจะมอบให้แก่ผู้หลอกลวง หรือ (ค) สมัครง้อใช้วงเงินสินเชื่อโดยมีเจตนาให้ผลประโยชน์แก่ผู้หลอกลวง

ในกรณีดังกล่าว เจ้าหน้าที่อาจออกคำสั่งจำกัด (RO) ไปยังธนาคาร เพื่อ “สั่งห้าม” มิให้ธนาคารอนุญาตให้มีการโอนหรือถอนเงินจากบัญชีของเหยื่อ และมีให้มีการให้หรือใช้วงเงินสินเชื่อในระหว่างที่คำสั่งดังกล่าวมีผลใช้บังคับ อันเป็นมาตรการเชิงป้องกันเพื่อหยุดยั้งความเสียหายก่อนที่จะเกิดขึ้นจริง ทั้งนี้ คำสั่ง RO จำกัดเฉพาะธุรกรรมทางการเงินและสินเชื่อของบุคคลที่เป็นเหยื่อเท่านั้น ไม่รวมถึงบุคคลที่สาม เว้นแต่บุคคลดังกล่าวมีลักษณะเป็นเหยื่อเช่นเดียวกัน และสำหรับระยะเวลาที่คำสั่ง RO มีผลใช้บังคับ เป็นระยะเวลา ๓๐ วันหรือน้อยกว่านั้น และอาจขยายได้ครั้งละไม่เกิน ๓๐ วัน และไม่เกิน ๕ ครั้ง โดยเจ้าหน้าที่อาจยกเลิกหรือแก้ไขคำสั่ง RO ได้ โดยการยกเลิกไม่กระทบต่อการดำเนินการที่

ได้กระทำไปก่อนหน้านี้ และในกรณีที่ธนาคารไม่ปฏิบัติตามคำสั่ง RO โดยไม่มีเหตุผลอันสมควร ย่อมมีความผิดและต้องระวางโทษปรับไม่เกิน ๓,๐๐๐ ดอลลาร์สิงคโปร์

คำสั่ง RO อาจถูกอุทธรณ์ได้ โดยเหยื่อหรือผู้มีส่วนเกี่ยวข้องต้องยื่นคำร้องในแบบที่กำหนด และการอุทธรณ์ดังกล่าวจะได้รับการพิจารณาโดยเจ้าหน้าที่ที่ได้รับการแต่งตั้งให้ทำหน้าที่พิจารณาอุทธรณ์ตามกฎหมาย มิใช่ศาลโดยตรง

กล่าวโดยสรุป กฎหมายฉบับนี้มีลักษณะเป็นมาตรการเชิงป้องกันที่มุ่งคุ้มครอง “เหยื่อการหลอกลวง” โดยตรง ผ่านการจำกัดการเคลื่อนไหวของเงินและสินเชื่อ ซึ่งเป็นหัวใจของการกระทำผิดในลักษณะ Cyber scam^{๒๔}

๕. บทสรุป

สถานการณ์ปัญหา Cyber scam ในสิงคโปร์ระหว่างช่วงปี ค.ศ. ๒๐๒๒-๒๐๒๕ สะท้อนให้เห็นถึงแนวโน้มการเพิ่มขึ้นของอาชญากรรมในลักษณะการหลอกลวงผ่านช่องทางดิจิทัลอย่างรวดเร็ว และต่อเนื่อง อันเป็นผลมาจากการพัฒนาของเทคโนโลยีสารสนเทศและพฤติกรรมของผู้ใช้อินเทอร์เน็ตที่เปลี่ยนแปลงไป ส่งผลให้รัฐจำเป็นต้องปรับเปลี่ยนแนวทางการบังคับใช้กฎหมายจากรูปแบบเชิงปราบปรามภายหลังเกิดเหตุ ไปสู่การออกแบบมาตรการเชิงป้องกันและเชิงแทรกแซงที่สามารถตอบสนองต่อสถานการณ์ได้อย่างทันท่วงที

ภายใต้บริบทดังกล่าว รัฐสิงคโปร์ได้พัฒนาแนวนโยบายในการจัดการกับปัญหา Cyber scam ในลักษณะบูรณาการ โดยมุ่งเน้นการดำเนินมาตรการในหลายระดับควบคู่กัน กล่าวคือ การปราบปรามผู้กระทำความผิด การควบคุมสภาพแวดล้อมดิจิทัล และการคุ้มครองเหยื่ออย่างมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งการนำมาตรการเชิงป้องกันมาใช้เพื่อลดความเสี่ยงของการเกิดความเสียหาย

ในเชิงกฎหมาย แนวทางดังกล่าวสะท้อนผ่านการบังคับใช้กฎหมายสำคัญ ๓ ฉบับ ได้แก่ กฎหมาย CMA ซึ่งทำหน้าที่เป็นกฎหมายอาญาหลักในการกำหนดฐานความผิดเกี่ยวกับการกระทำทางไซเบอร์ กฎหมาย OCHA ซึ่งมุ่งควบคุมแพลตฟอร์มและกิจกรรมออนไลน์ที่เกี่ยวข้องกับการกระทำความผิด และกฎหมาย PSA ซึ่งให้อำนาจรัฐในการแทรกแซงธุรกรรมทางการเงินของบุคคลที่มีความเสี่ยงจะตกเป็นเหยื่อของการหลอกลวง โดยเฉพาะผ่านคำสั่งจำกัดต่อธนาคาร ซึ่งกฎหมายทั้ง ๓ ฉบับดังกล่าวทำหน้าที่เสริมกันอย่างเป็นระบบ กล่าวคือ กฎหมาย CMA มุ่งจัดการผู้กระทำความผิด กฎหมาย OCHA มุ่งควบคุมเครื่องมือและช่องทางของอาชญากรรมในโลกออนไลน์ และกฎหมาย PSA มุ่งคุ้มครองเหยื่อโดยการหยุดยั้งการเคลื่อนไหวของเงินก่อนที่จะเกิดความเสียหาย ดังนั้น แนวทางของสิงคโปร์จึงเป็นรูปแบบของการจัดการ Cyber scam ที่ครอบคลุมทั้งต้นน้ำ กลางน้ำ และปลายน้ำของกระบวนการก่ออาชญากรรม

^{๒๔} เนื้อหาในส่วนนี้ได้ปรับปรุงเพิ่มเติมจากบทความ “รัฐบัญญัติว่าด้วยความคุ้มครองจากการหลอกลวงทางการเงินของสิงคโปร์ (The Protection from Scam Act 2025)” ซึ่งตีพิมพ์ใน “กฤษฎีกาสาร” ปีที่ ๒๐ ฉบับที่ ๕ (ม.ย. – ก.ค. ๒๕๖๘) หน้า ๒๔-๒๘, สืบค้นเมื่อวันที่ ๓ มิถุนายน ๒๕๖๘, จาก <https://www.ocs.go.th/fb694c>

กล่าวโดยสรุป ระบบกฎหมายของสิงคโปร์ในการรับมือกับปัญหา Cyber scam มีลักษณะเป็นการบูรณาการมาตรการเชิงป้องกันและเชิงบังคับใช้กฎหมายอย่างมีประสิทธิภาพ โดยให้ความสำคัญกับการลดความเสียหายล่วงหน้าเป็นสำคัญ อันเป็นแนวโน้มสำคัญของการพัฒนากฎหมายในยุคดิจิทัล และอาจเป็นต้นแบบที่มีประโยชน์ต่อการพัฒนากฎหมายในประเทศอื่นต่อไป

บทที่ ๔
มาตรการที่เกี่ยวข้องกับการป้องกันและปราบปราม
อาชญากรรมการหลอกลวงทางไซเบอร์ของประเทศไทย*

๔.๑ สภาพปัญหา

โดยที่ในช่วงระยะเวลาที่ผ่านมา ประชาชนไทยจำนวนมากประสบปัญหาถูกมิจฉาชีพหลอกลวงทางออนไลน์จนก่อให้เกิดการสูญเสียทรัพย์สินเงินทองไปเป็นจำนวนมาก การหลอกลวงของมิจฉาชีพได้เกิดขึ้นอย่างต่อเนื่องผ่านรูปแบบต่าง ๆ ไม่ว่าจะเป็นการหลอกลวงโดยแก๊งคอลเซ็นเตอร์ซึ่งเป็นกลุ่มมิจฉาชีพที่ทำการหลอกลวงเหยื่อผ่านทางโทรศัพท์ โดยมักแอบอ้างเป็นเจ้าหน้าที่จากหน่วยงานต่าง ๆ เช่น หน่วยงานรัฐ ธนาคาร บริษัทขนส่ง และพุดจาให้เกิดความน่าเชื่อถือเพื่อหลอกลวงให้เหยื่อหลงเชื่อ หรืออาจพุดข่มขู่ให้เกิดความหวาดกลัวเพื่อให้โอนเงินไป หรืออาจใช้วิธีการส่งลิงก์มาให้กด หรือหลอกให้ติดตั้งแอปพลิเคชันบางอย่างเพื่อดูดเงิน หรือให้กรอกข้อมูลส่วนตัว เพื่อขโมยเงินออกไปจากบัญชีของผู้นั้น นอกจากการหลอกลวงโดยแก๊งคอลเซ็นเตอร์แล้ว ยังมีการหลอกลวงผ่านทางเครือข่ายสื่อสังคมออนไลน์หรือเว็บไซต์ในรูปแบบต่าง ๆ อีกมากมาย เช่น หลอกขายสินค้าออนไลน์ซึ่งมิจฉาชีพมักจะโฆษณาสินค้าเกินจริงหรือจัดหน้าร้านให้ดูน่าเชื่อถือ แต่เมื่อเหยื่อโอนเงินซื้อสินค้าไปแล้วกลับหนีหายหรือส่งสินค้าให้แต่ไม่ตรงปก หลอกให้ลงทุนโดยหลอกว่าจะได้ผลตอบแทนที่สูงเกินจริงในระยะเวลาอันสั้น ส่งข้อความหรือลิงก์ปลอมเพื่อหลอกลวงให้เหยื่อกรอกข้อมูลส่วนตัวเพื่อดูดเงินออกจากบัญชี หลอกให้รักแล้วออกอุบายให้โอนเงิน หรือแอบอ้างเป็นคนรู้จักโดยอาจปลอมโปรไฟล์โซเชียลมีเดียเพื่อหามาขอยืมเงินเร่งด่วน หรือหลอกให้สมัครงานหรือทำงานพิเศษแต่ต้องโอนเงินค่าต่าง ๆ ให้ก่อน^๑ และเมื่อมิจฉาชีพได้รับเงินจากเหยื่อแล้วก็มักจะรีบโอนเงินที่ได้มานั้นต่อไปยังบัญชีอื่น ๆ อีกหลายทอดอย่างรวดเร็วเพื่อปิดบังการกระทำความผิดและเพื่อทำให้การติดตามเส้นทางการเงินทำได้ยากขึ้น

เมื่อการหลอกลวงของมิจฉาชีพทวีความรุนแรงมากขึ้นเรื่อย ๆ ประชาชนจำนวนมากได้หลงเชื่อกลโกงจนได้รับความเสียหายเป็นวงกว้าง ส่งผลให้ประชาชนเกิดความไม่ปลอดภัยต่อชีวิตและทรัพย์สินของตนเอง และเป็นอันตรายต่อระบบเศรษฐกิจของประเทศ รัฐจึงตราพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ ขึ้น เพื่อเป็นเครื่องมือทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้เกิดประสิทธิภาพและให้หมดไปโดยเร็ว ตลอดจนเพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในทางเศรษฐกิจของประเทศ

* จัดทำโดยนางสาวพิมสิริ วิเศษโพนารนนท์ และนายสรวิชัย ล้ออัศจรรย์ นักกฎหมายกฤษฎีกาชำนาญการพิเศษ ฝ่ายค้นคว้าและเรียบเรียงกฎหมาย กองกฎหมายต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

^๑ ข้อมูลจากกรมประชาสัมพันธ์, สืบค้นเมื่อวันที่ ๑๕ มิถุนายน ๒๕๖๙, จาก <https://www.prd.go.th/th/content/category/detail/id/33/iid/459323> และ <https://www.prd.go.th/th/content/category/detail/id/39/iid/462580>

ต่อมากลุ่มมิจาซีพีได้ปรับปรุงแบบการยกย้ายถ่ายเทเงินที่ได้มาจากการหลอกลวงเหยื่อให้ซับซ้อนยิ่งขึ้น โดยนำเงินที่ได้จากการกระทำความผิดอาชญากรรมทางเทคโนโลยีไปซื้อขายสินทรัพย์ดิจิทัล เพื่อให้ยากต่อการติดตามหาตัวผู้กระทำความผิด รวมทั้งยากต่อการตรวจสอบการทำธุรกรรมและการระงับการทำธุรกรรม นอกจากนี้ ยังมีการใช้บริการโทรคมนาคมเพื่อกระทำความผิดอาชญากรรมทางเทคโนโลยี และการนำข้อมูลของบุคคลหรือผู้ถึงแก่กรรมมาใช้ในการกระทำความผิดดังกล่าว รัฐจึงตราพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ๒) พ.ศ. ๒๕๖๘ เพื่อกำหนดมาตรการเพิ่มเติมสำหรับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้ครอบคลุมและมีประสิทธิภาพมากยิ่งขึ้น รวมทั้งมีการจัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และกำหนดให้มีกระบวนการการคืนเงินแก่ผู้เสียหายให้เป็นไปโดยเร็ว รวมทั้งสร้างการมีส่วนร่วมรับผิดชอบต่อความเสียหายที่เกิดจากการกระทำความผิดอาชญากรรมทางเทคโนโลยีเพื่อเยียวยาผู้เสียหาย ตลอดจนการกำหนดโทษในส่วนที่เกี่ยวข้องด้วย

อย่างไรก็ดี เมื่อพิจารณาจำนวนสถิติคดีการหลอกลวงทางออนไลน์ตั้งแต่วันที่ ๑ มกราคม ๒๕๖๘ ถึงวันที่ ๑๗ มิถุนายน ๒๕๖๙ ปรากฏคดีออนไลน์จำนวน ๕๔๐,๖๕๗ เรื่อง คิดเป็นมูลค่าความเสียหายรวม ๓๔,๐๗๘,๑๓๘,๗๔๑ บาท หากเฉลี่ยคดีออนไลน์ที่ปรากฏในแต่ละวันจะมีทั้งสิ้น ๑,๐๑๑ เรื่องต่อวัน โดยคดีออนไลน์ที่พบมากที่สุดคือใน ๗ อันดับแรก ได้แก่ การหลอกลวงด้านสินค้าและบริการ คิดเป็นร้อยละ ๕๙ การหลอกลวงเสนอผลประโยชน์อื่น คิดเป็นร้อยละ ๑๖ การหลอกลวงด้านการจ้างงาน คิดเป็นร้อยละ ๙ การหลอกลวงโดยการแอบอ้างบุคคลอื่น คิดเป็นร้อยละ ๘ การหลอกลวงด้านการเงินและการลงทุน คิดเป็นร้อยละ ๕ ประเภทคดีฉ้อโกงทางเทคโนโลยี คิดเป็นร้อยละ ๓ และการโจมตีทางเทคนิคเชิงรุก คิดเป็นร้อยละ ๐^๒

สำหรับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของประเทศไทยนั้น เป็นไปดังที่ได้กล่าวถึงข้างต้นว่า รัฐได้ตราพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ ขึ้นใช้บังคับ โดยมีวัตถุประสงค์เพื่อป้องกัน ปราบปราม และจัดการปัญหาอาชญากรรมทางเทคโนโลยีที่มีแนวโน้มที่จะทวีความรุนแรงเพิ่มมากขึ้นในประเทศไทยให้หมดไปโดยเร็ว^๓ การกำหนดมาตรการเชิงป้องกัน มาตรการเชิงลงโทษ และมาตรการในการติดตามทรัพย์สินของผู้ถูกหลอกลวงจากอาชญากรรมทางเทคโนโลยีให้ได้กลับคืนมาโดยเร็ว

^๒ ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.), “เตือนภัยไซเบอร์”, สืบค้นเมื่อวันที่ ๑๗ มิถุนายน ๒๕๖๙, จาก <https://www.thaipoliceonline.go.th>

^๓ เหตุผลในการประกาศใช้พระราชกำหนดฉบับนี้ คือ โดยที่ปัจจุบันมีการใช้วิธีการทางเทคโนโลยีหลอกลวงประชาชนทั่วไปผ่านอุปกรณ์เทคโนโลยีต่าง ๆ จนทำให้ประชาชนสูญเสียทรัพย์สินเป็นจำนวนมาก และผู้หลอกลวงได้โอนทรัพย์สินที่ได้จากการกระทำความผิดดังกล่าวผ่านบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลอื่นต่อไปเป็นทอด ๆ อย่างรวดเร็ว เพื่อปกปิดหรืออำพรางการกระทำความผิด ซึ่งแต่ละวันประชาชนผู้สุจริตถูกหลอกลวงจำนวนมากและมีมูลค่าความเสียหายสูงมาก และการหลอกลวงดังกล่าวซึ่งเป็นการกระทำความผิดได้เพิ่มมากขึ้น ส่งผลกระทบต่อประชาชนในวงกว้างและเป็นอันตรายร้ายแรงต่อระบบเศรษฐกิจของประเทศ เป็นกรณีฉุกเฉินที่มีความจำเป็นรีบด่วนอันมิอาจหวั่นไหวได้ เพื่อประโยชน์ในอันที่จะต้องมีการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีดังกล่าว เพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในทางเศรษฐกิจของประเทศ จึงจำเป็นต้องตราพระราชกำหนดนี้

๔.๒ มาตรการเชิงป้องกัน^๔

(๑) การแลกเปลี่ยนข้อมูล (มาตรา ๔^๕) กำหนดกลไกการเปิดเผยและแลกเปลี่ยนข้อมูลระหว่างสถาบันการเงิน ผู้ประกอบธุรกิจ และผู้ให้บริการที่เกี่ยวข้อง ผ่านระบบหรือกระบวนการที่หน่วยงานกำกับดูแลเห็นชอบร่วมกัน เพื่อให้หน่วยงานของรัฐสามารถนำข้อมูลดังกล่าวไปใช้ในการป้องกัน ปราบปราม และระงับอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพ

(๒) การกำหนดมาตรฐานเพื่อป้องกันอาชญากรรมทางเทคโนโลยี (มาตรา ๔/๑^๖) เป็นการวางฐานทางกฎหมายสำหรับการกำหนดมาตรการป้องกันอาชญากรรมทางเทคโนโลยีแก่ผู้ให้บริการที่เกี่ยวข้อง โดยกำหนดให้หน่วยงานกำกับดูแลและผู้ให้บริการที่เกี่ยวข้องมีหน้าที่ดำเนินมาตรการป้องกันอาชญากรรมทางเทคโนโลยีตามมาตรฐานหรือหลักเกณฑ์ที่กำหนด เพื่อลดโอกาสที่บริการด้านการสื่อสารหรือช่องทางดิจิทัลจะถูกนำไปใช้เป็นเครื่องมือในการกระทำความผิด และเพิ่มประสิทธิภาพในการป้องกันและตรวจจับการกระทำที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี

^๔ ข้อความหรือเอกสารในหัวข้อนี้มีส่วนที่สร้างขึ้นโดยเทคโนโลยีปัญญาประดิษฐ์ (AI) ในการเรียบเรียงถ้อยคำ และผู้จัดทำได้ตรวจสอบความถูกต้องแล้ว

^๕ มาตรา ๔ เพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ในกรณีที่มีเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงินและผู้ประกอบธุรกิจมีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้ายที่เกี่ยวข้อง และเลขที่กระเป๋าสินทรัพย์ดิจิทัลในระหว่างสถาบันการเงินและผู้ประกอบธุรกิจนั้นผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน ธนาคารแห่งประเทศไทย และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ เห็นชอบร่วมกัน

เพื่อดำเนินการตามวัตถุประสงค์ตามวรรคหนึ่ง ให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องมีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลการให้บริการที่เกี่ยวข้องระหว่างกันผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เห็นชอบร่วมกัน

เมื่อมีการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามวรรคหนึ่งหรือวรรคสองแล้ว ให้ผู้เปิดเผยหรือแลกเปลี่ยนข้อมูลแจ้งให้สำนักงานตำรวจแห่งชาติหรือกรมสอบสวนคดีพิเศษ แล้วแต่กรณี และสำนักงานป้องกันและปราบปรามการฟอกเงิน ทราบโดยทันที และเมื่อได้รับแจ้งแล้ว ให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ หรือสำนักงานป้องกันและปราบปรามการฟอกเงิน แล้วแต่กรณี มีอำนาจนำข้อมูลดังกล่าวไปใช้ประโยชน์เพื่อป้องกันปราบปราม หรือระงับอาชญากรรมทางเทคโนโลยีได้

^๖ มาตรา ๔/๑ เพื่อประโยชน์แห่งมาตรา ๘/๑๐ ให้ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ และคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กำหนดมาตรฐานหรือมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยี

ให้ผู้ให้บริการเครือข่ายโทรศัพท์และผู้ให้บริการโทรคมนาคมอื่นมีหน้าที่ตรวจสอบเพื่อคัดกรองเนื้อหาการบริการสารสั้น (SMS) ที่อาจเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีตามมาตรฐานหรือมาตรการที่สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติกำหนดตามวรรคหนึ่ง

(๓) การระงับการทำธุรกรรมต้องสงสัย (มาตรา ๖^๗ และมาตรา ๗^๘) กำหนดกลไกการระงับการทำธุรกรรมที่เกี่ยวข้องหรืออาจเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี โดยให้สถาบันการเงินและผู้ประกอบธุรกิจมีหน้าที่ระงับธุรกรรมเป็นการชั่วคราวและส่งต่อข้อมูลผ่านระบบแลกเปลี่ยนข้อมูล เพื่อให้ผู้รับโอนทุกทอดดำเนินการระงับธุรกรรมในทำนองเดียวกัน อันเป็นการตัดเส้นทางการเงินของผู้กระทำความผิดและรักษาทรัพย์สินไว้ระหว่างการตรวจสอบข้อเท็จจริง โดยกลไกดังกล่าวอาจเริ่มต้นจากการตรวจพบเหตุอันควรสงสัยของสถาบันการเงินหรือผู้ประกอบธุรกิจ การได้รับข้อมูล

^๗ มาตรา ๖ ในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจพบเหตุอันควรสงสัยเองหรือได้รับข้อมูลจากระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา ๔ ว่าบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ใดถูกใช้หรืออาจถูกใช้ทำธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีหรือการกระทำความผิดมูลฐานหรือความผิดฐานฟอกเงินตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ให้สถาบันการเงินหรือผู้ประกอบธุรกิจมีหน้าที่ระงับการทำธุรกรรมและแจ้งสถาบันการเงินหรือผู้ประกอบธุรกิจที่รับโอนถัดไป พร้อมทั้งนำข้อมูลเข้าสู่ระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา ๔ เพื่อให้สถาบันการเงินและผู้ประกอบธุรกิจผู้รับโอนทุกทอดทราบและระงับการทำธุรกรรมดังกล่าวไว้ทันทีเป็นการชั่วคราวไม่เกินเจ็ดวันนับแต่วันที่พบเหตุอันควรสงสัยหรือได้รับแจ้ง แล้วแต่กรณี เพื่อตรวจสอบความถูกต้องแท้จริง และแจ้งให้เจ้าพนักงานผู้มีอำนาจดำเนินคดีอาญาหรือเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินดำเนินการตรวจสอบ

ในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจได้รับแจ้งเหตุตามวรรคหนึ่งจากเจ้าพนักงานผู้มีอำนาจดำเนินคดีอาญาหรือเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน ให้สถาบันการเงินหรือผู้ประกอบธุรกิจมีหน้าที่ระงับการทำธุรกรรม พร้อมทั้งนำข้อมูลเข้าสู่ระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา ๔ เพื่อให้สถาบันการเงินและผู้ประกอบธุรกิจผู้รับโอนทุกทอดทราบและระงับการทำธุรกรรมดังกล่าวไว้ทันที แล้วแจ้งให้ผู้ที่เกี่ยวข้องทราบ

เมื่อเจ้าพนักงานผู้มีอำนาจดำเนินคดีอาญาหรือเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินตรวจสอบแล้ว ปรากฏพยานหลักฐานอันควรเชื่อได้ว่าบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์นั้นถูกใช้ในการกระทำความผิด ให้ดำเนินการตามกฎหมายภายในเจ็ดวันนับแต่วันที่ได้รับแจ้งการระงับการทำธุรกรรมตามวรรคหนึ่งหรือแจ้งสถาบันการเงินหรือผู้ประกอบธุรกิจตามวรรคสอง หากไม่ปรากฏพยานหลักฐานที่เชื่อได้ว่าบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์นั้นถูกใช้ในการกระทำความผิด ให้แจ้งผลการตรวจสอบให้สถาบันการเงินหรือผู้ประกอบธุรกิจทราบเพื่อยกเลิกการระงับการทำธุรกรรมต่อไป

เมื่อพ้นกำหนดเวลาตามวรรคสามแล้ว หากเจ้าพนักงานผู้มีอำนาจดำเนินคดีอาญาหรือเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินไม่แจ้งผลการดำเนินการ ให้สถาบันการเงินหรือผู้ประกอบธุรกิจยกเลิกการระงับการทำธุรกรรมนั้น

^๘ มาตรา ๗ ในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจได้รับแจ้งจากผู้เสียหายซึ่งเป็นผู้ถือบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ว่า ได้มีการทำธุรกรรมโดยบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวและเข้าข่ายเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงินหรือผู้ประกอบธุรกิจดังกล่าวมีหน้าที่ระงับการทำธุรกรรมนั้นไว้ชั่วคราว พร้อมทั้งนำข้อมูลเข้าสู่ระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา ๔ เพื่อให้สถาบันการเงินและผู้ประกอบธุรกิจผู้รับโอนทุกทอดทราบและระงับการทำธุรกรรมดังกล่าวไว้ทันที และแจ้งให้ผู้เสียหายไปร้องทุกข์ต่อพนักงานสอบสวนภายในเจ็ดสิบสองชั่วโมง เมื่อมีการร้องทุกข์แล้ว ให้พนักงานสอบสวนแจ้งให้สถาบันการเงินหรือผู้ประกอบธุรกิจที่ได้รับการทำธุรกรรมไว้ทราบ และให้พนักงานสอบสวนพิจารณาดำเนินการเกี่ยวกับบัญชีเงินฝากและบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวภายในเจ็ดวันนับแต่วันที่ได้รับความร้องทุกข์ หากไม่มีคำสั่งให้ระงับการทำธุรกรรมไว้ต่อไปภายในเวลาดังกล่าว ให้สถาบันการเงินหรือผู้ประกอบธุรกิจยกเลิกการระงับการทำธุรกรรมนั้น

จากระบบแลกเปลี่ยนข้อมูล การได้รับแจ้งจากหน่วยงานของรัฐ หรือการแจ้งเหตุโดยผู้เสียหาย ซึ่งกฎหมายกำหนดกรอบเวลาสำหรับการตรวจสอบและการดำเนินการของหน่วยงานที่เกี่ยวข้อง เพื่อคุ้มครองทั้งประสิทธิภาพในการปราบปรามอาชญากรรมและสิทธิของผู้เกี่ยวข้อง

๔.๓ มาตรการเชิงลงโทษ^๙

พระราชกำหนดฯ มิได้มุ่งลงโทษเฉพาะผู้กระทำการหลอกลวงโดยตรงเท่านั้น แต่กำหนดความผิดครอบคลุมบุคคลและองค์กรที่มีส่วนสนับสนุน เอื้ออำนวย หรือสร้างเงื่อนไขให้เกิดอาชญากรรมทางเทคโนโลยีได้ โดยแบ่งออกเป็น ๔ กลุ่มความผิด ได้แก่

(๑) ความผิดเกี่ยวกับการไม่ปฏิบัติตามหน้าที่ตามกฎหมาย เป็นการกำหนดลักษณะความผิดและโทษเพื่อบังคับให้สถาบันการเงิน ผู้ประกอบธุรกิจ และบุคคลที่เกี่ยวข้องปฏิบัติตามมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีอย่างเคร่งครัด ได้แก่ มาตรา ๘/๑๑^{๑๐} และมาตรา ๘/๑๒^{๑๑}

(๒) ความผิดเกี่ยวกับบัญชีม้าและช่องทางการเงิน กฎหมายกำหนดความผิดสำหรับบุคคลที่เปิดบัญชีหรือยินยอมให้ใช้บัญชีของตน รวมทั้งบุคคลที่ทำหน้าที่จัดหา ซื้อขาย หรือโฆษณาบัญชีดังกล่าว เพื่อตัดเครื่องมือสำคัญที่ผู้กระทำความผิดใช้รับและเคลื่อนย้ายทรัพย์สินที่ได้จากการหลอกลวง ซึ่งได้แก่ มาตรา ๙^{๑๒} และมาตรา ๑๐^{๑๓}

^๙ ข้อความหรือเอกสารในหัวข้อนี้มีส่วนที่สร้างขึ้นโดยเทคโนโลยีปัญญาประดิษฐ์ (AI) ในการเรียบเรียงถ้อยคำ และผู้จัดทำได้ตรวจสอบความถูกต้องแล้ว

^{๑๐} มาตรา ๘/๑๑ สถาบันการเงินหรือผู้ประกอบธุรกิจใดไม่ปฏิบัติตามมาตรา ๔/๒ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

ในกรณีที่การกระทำความผิดตามวรรคหนึ่งเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

^{๑๑} มาตรา ๘/๑๒ ผู้ใดไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ตามมาตรา ๗/๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

^{๑๒} มาตรา ๙ ผู้ใดเปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของตน โดยมีได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้องหรือยินยอมให้บุคคลอื่นใช้หรือยืมใช้เลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ของตน ทั้งนี้ โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินสามแสนบาท หรือทั้งจำทั้งปรับ

^{๑๓} มาตรา ๑๐ ผู้ใดเป็นธุระจัดหา โฆษณา หรือโฆษณาโดยประการใด ๆ เพื่อให้มีการซื้อ ขาย ให้เช่า หรือให้ยืม บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ เพื่อใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ

(๓) ความผิดเกี่ยวกับซิมม้าและการใช้บริการโทรคมนาคมโดยมิชอบ กฎหมายขยายมาตรการลงโทษไปยังช่องทางการสื่อสารที่มักถูกใช้ในการหลอกลวงประชาชน ได้แก่ เลขหมายโทรศัพท์เคลื่อนที่ ซึ่งได้แก่ มาตรา ๔ มาตรา ๑๑^{๑๔} และมาตรา ๑๑/๑^{๑๕}

(๔) ความผิดเกี่ยวกับข้อมูลส่วนบุคคลที่นำไปใช้ก่ออาชญากรรม กฎหมายกำหนดความผิดเกี่ยวกับการใช้ การเก็บรวบรวม การครอบครอง หรือการเปิดเผยข้อมูลส่วนบุคคลที่สามารถระบุตัวบุคคลได้ หากมีวัตถุประสงค์เพื่อนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดอาญาอื่น ซึ่งได้แก่ มาตรา ๑๑/๒^{๑๖}

๔.๔ มาตรการในการติดตามทรัพย์สิน

พระราชกำหนดฯ กำหนดมาตรการเรื่องนี้ซึ่งแบ่งเป็น ๒ ขั้นตอนสำคัญ ได้แก่ ขั้นตอนที่ ๑ การระงับธุรกรรมและการตรวจสอบข้อมูลธุรกรรมต้องสงสัย และขั้นตอนที่ ๒ การคืนเงินหรือสินทรัพย์ดิจิทัลแก่ผู้เสียหาย

ขั้นตอนที่ ๑ การระงับธุรกรรมและการตรวจสอบข้อมูลธุรกรรมต้องสงสัย (ซึ่งได้กล่าวโดยสังเขปไปแล้วในหัวข้อ ๔.๒ มาตรการเชิงป้องกัน) เป็นมาตรการเร่งด่วนเพื่อรักษาทรัพย์สินและตัดเส้นทางการเงินที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีก่อนที่ทรัพย์สินดังกล่าวจะถูกโอนต่อ

^{๑๔} มาตรา ๑๑ ผู้ใดเป็นธุระจัดหา โฆษณา หรือโฆษณาโดยประการใด ๆ เพื่อให้มีการซื้อหรือขายเลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ ต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ

^{๑๕} มาตรา ๑๑/๑ ในกรณีที่ผู้ซื้อเลขหมายโทรศัพท์ลงทะเบียนเพื่อใช้บริการ หรือผู้ขายเลขหมายโทรศัพท์ที่มีหน้าที่เกี่ยวกับการลงทะเบียนให้แก่ผู้ใช้บริการ ลงทะเบียนไม่ถูกต้องครบถ้วนตามที่คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติกำหนด โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

^{๑๖} มาตรา ๑๑/๒ ผู้ใดใช้ข้อมูลเกี่ยวกับบุคคลหรือผู้ถึงแก่กรรมซึ่งทำให้สามารถระบุตัวบุคคลหรือผู้ถึงแก่กรรมนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เพื่อกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ผู้ใดเก็บรวบรวม ครอบครอง หรือเปิดเผยข้อมูลเกี่ยวกับบุคคลหรือผู้ถึงแก่กรรมซึ่งทำให้สามารถระบุตัวบุคคลหรือผู้ถึงแก่กรรมนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เพื่อนำไปใช้หรือให้บุคคลอื่นใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษตามที่บัญญัติในวรรคหนึ่ง

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสองได้กระทำโดยซื้อ เสนอซื้อ ขาย เสนอขาย แลกเปลี่ยน เสนอแลกเปลี่ยน หรือแสวงหาประโยชน์ที่มีควรได้โดยชอบด้วยกฎหมาย ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ไปยังบุคคลอื่น โดยเมื่อผู้เสียหายแจ้งเหตุแก่สถาบันการเงิน ผู้ประกอบธุรกิจ^{๑๗} ศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.)^{๑๘} หรือพนักงานสอบสวน แล้วแต่กรณี หน่วยงานหรือบุคคลดังกล่าวมีหน้าที่ดำเนินการระงับธุรกรรมตามที่กฎหมายกำหนด พร้อมทั้งนำข้อมูลเข้าสู่ระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล เพื่อให้ผู้รับโอนและผู้เกี่ยวข้องสามารถดำเนินมาตรการระงับธุรกรรมได้อย่างต่อเนื่อง ทั้งนี้ กฎหมายยังเปิดให้ผู้เสียหายแจ้งเหตุหรือร้องทุกข์โดยวิธีการทางอิเล็กทรอนิกส์ และให้อำนาจ ศปอท. ในการรับแจ้งเหตุ ระงับธุรกรรม รวบรวมข้อมูล และประกาศรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี เพื่อให้หน่วยงานที่

^{๑๗} มาตรา ๓ ในพระราชกำหนดนี้

“อาชญากรรมทางเทคโนโลยี” หมายความว่า การกระทำหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือริดเอาทรัพย์สินบุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง กรรโชก หรือริดเอาทรัพย์สิน โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ

“สถาบันการเงิน” หมายความว่า ธนาคารพาณิชย์และสถาบันการเงินของรัฐที่มีกฎหมายเฉพาะจัดตั้งขึ้น ทั้งนี้ ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“ผู้ประกอบธุรกิจ” หมายความว่า ผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงินและผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลตามกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล

“กระเป๋าสินทรัพย์ดิจิทัล” หมายความว่า ระบบที่ใช้ในการจัดเก็บสินทรัพย์ดิจิทัล (wallet)

“บัญชีเงินอิเล็กทรอนิกส์” หมายความว่า บัญชีสินทรัพย์ดิจิทัล

^{๑๘} มาตรา ๘/๕ ให้จัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เรียกโดยย่อว่า “ศปอท.” ในสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีหน้าที่และอำนาจดังต่อไปนี้

(๑) รับแจ้งเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยีจากผู้เสียหาย และให้ถือว่าการแจ้งเหตุดังกล่าวเป็นการร้องทุกข์โดยวิธีการทางอิเล็กทรอนิกส์ตามมาตรา ๘ วรรคสอง

(๒) ระงับการทำธุรกรรมที่เป็นบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ที่ปรากฏพยานหลักฐานอันควรเชื่อได้ว่าเกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยีโดยทันที หรือเพิกถอนการระงับการทำธุรกรรมดังกล่าวในกรณีพิสูจน์ได้ว่ามิได้เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี

(๓) สั่งให้สถาบันการเงินหรือผู้ประกอบธุรกิจนำส่งข้อมูลเกี่ยวกับบัญชีและธุรกรรมที่ต้องสงสัย

(๔) รวบรวมจำนวนบัญชีเงินฝากที่บุคคลใดถือไว้ เพื่อประโยชน์ในการตรวจสอบว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยี แต่ทั้งนี้ ไม่รวมถึงจำนวนเงินฝากทั้งหมดหรือของแต่ละบัญชี

(๕) เปิดเผยหรือแลกเปลี่ยนข้อมูลที่เกี่ยวข้องเพื่อประโยชน์ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีกับหน่วยงานของรัฐและหน่วยงานเอกชนที่เกี่ยวข้อง

(๖) ประกาศรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี และเพิกถอนรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลดังกล่าว ทั้งนี้ ตามหลักเกณฑ์ที่ ศปอท. ประกาศกำหนด

(๗) แจ้งข้อมูลหมายเลขโทรศัพท์ บริการสารสั้น (SMS) หรือชื่อผู้ส่งสารสั้น หรือข้อมูลการใช้บริการโทรคมนาคมอื่น ให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติทราบ เพื่อดำเนินการตามมาตรา ๕ วรรคสอง

(๘) รวบรวมข้อมูลเกี่ยวกับอาชญากรรมทางเทคโนโลยีเพื่อปฏิบัติการตามพระราชกำหนดนี้

(๙) จัดทำรายงานผลการดำเนินการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเสนอคณะกรรมการตามมาตรา ๑๓ เดือนละหนึ่งครั้ง

เกี่ยวข้องสามารถตรวจสอบเส้นทางการเงิน พิสูจน์ความเชื่อมโยงของบัญชีหรือสินทรัพย์ดิจิทัลกับการกระทำความผิด และดำเนินมาตรการทางกฎหมายเกี่ยวกับทรัพย์สินที่เกี่ยวข้องต่อไป(มาตรา ๖^๙ มาตรา ๗^{๑๐} มาตรา ๘^{๑๑} มาตรา ๘/๓^{๑๒} และมาตรา ๘/๕^{๑๓})

ขั้นตอนที่ ๒ การคืนเงินหรือสินทรัพย์ดิจิทัลแก่ผู้เสียหาย

เดิมการคืนเงินให้แก่ผู้เสียหายต้องดำเนินการตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒ แต่กระบวนการดังกล่าวมีหลายขั้นตอนและมีความล่าช้า ทำให้ผู้เสียหายจากอาชญากรรมทางเทคโนโลยีไม่ได้รับการแก้ไขเยียวยาอย่างที่เหมาะสม และทำให้มีเงินคงค้างในระบบการเงินเป็นจำนวนมาก จึงได้มีการตราพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ๒) พ.ศ. ๒๕๖๘ เพื่อแก้ไขกระบวนการการคืนเงินให้แก่ผู้เสียหายให้เป็นไปอย่างรวดเร็วมากขึ้น โดยเพิ่มบทบัญญัติเกี่ยวกับการคืนเงินให้แก่ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี โดยกำหนดให้คณะกรรมการธุรกรรมเป็นผู้มีอำนาจสั่งคืนเงินให้แก่ผู้เสียหาย และให้แจ้งธนาคารหรือสถาบันการเงินคืนเงินให้แก่ผู้เสียหายโดยตรง โดยไม่ต้องรอให้ศาลสั่งเช่นเดิมอีกต่อไป เพื่อให้ประชาชนที่ตกเป็นผู้เสียหายจากอาชญากรรมทางเทคโนโลยีได้รับการเยียวยาโดยได้รับเงินคืนรวดเร็วยิ่งขึ้น และยังเป็นการนำเงินที่คงค้างจากการระงับการทำธุรกรรมที่รอการตรวจสอบกลับคืนสู่ระบบเศรษฐกิจ

สำหรับหลักเกณฑ์ ขั้นตอน และวิธีการเกี่ยวกับการคืนเงินให้แก่ผู้เสียหายนั้น กำหนดไว้ในกฎกระทรวงการคืนเงินให้แก่ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๙ ซึ่งมีสาระสำคัญเกี่ยวกับการรายงานและตรวจสอบข้อมูลธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี การประกาศข้อมูลบัญชีหรือบัญชีเงินอิเล็กทรอนิกส์ที่เกี่ยวข้อง การแจ้งผู้เสียหายและผู้มีส่วนได้เสีย การยื่นคำร้องขอรับเงินหรือสินทรัพย์ดิจิทัลคืน การยื่นคำคัดค้าน ตลอดจนกระบวนการพิจารณาและมีคำสั่งคืนเงินหรือสินทรัพย์ดิจิทัลแก่ผู้เสียหาย โดยมีเป้าหมายเพื่อให้การติดตามทรัพย์สิน การพิสูจน์สิทธิ และการเยียวยา

^๙ โปรดดูเชิงอรรถที่ ๗

^{๑๐} โปรดดูเชิงอรรถที่ ๘

^{๑๑} มาตรา ๘ การแจ้งข้อมูลหรือหลักฐานตามมาตรา ๖ และมาตรา ๗ จะกระทำทางโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ก็ได้ ในกรณีที่กระทำทางโทรศัพท์ ให้ผู้ได้รับแจ้งบันทึกไว้เป็นลายลักษณ์อักษร ลงลายมือชื่อผู้รับแจ้ง และวันเวลาที่ได้รับไว้เป็นหลักฐาน พร้อมทั้งส่งสำเนาให้ผู้แจ้งเก็บไว้เป็นหลักฐานด้วย

การร้องทุกข์ในความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีจะกระทำต่อพนักงานสอบสวน ณ สถานีตำรวจแห่งใดในราชอาณาจักรหรือตอกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีก็ได้ และจะร้องทุกข์โดยวิธีการทางอิเล็กทรอนิกส์ก็ได้ โดยให้ถือว่าเป็นการร้องทุกข์โดยชอบด้วยประมวลกฎหมายวิธีพิจารณาความอาญา และในการสอบสวนหรือดำเนินการเกี่ยวกับการกระทำความผิดดังกล่าว ให้พนักงานสอบสวนที่รับคำร้องทุกข์ไม่ว่าประจำอยู่ที่ใดหรือพนักงานสอบสวนที่ผู้บัญชาการตำรวจแห่งชาติกำหนด เป็นพนักงานสอบสวนผู้รับผิดชอบมีอำนาจสอบสวนและดำเนินการเกี่ยวกับการกระทำความผิดดังกล่าวได้ไม่ว่าความผิดนั้นจะเกิดขึ้น ณ ที่ใดในราชอาณาจักร

^{๑๒} มาตรา ๘/๓ ให้ตามมาตรา ๘/๑ และมาตรา ๘/๒ มาใช้บังคับแก่กรณีที่สำนักงานป้องกันและปราบปรามการฟอกเงินพบเหตุอันควรสงสัยเองหรือได้รับข้อมูลจากระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา ๔ ด้วยโดยอนุโลม

^{๑๓} โปรดดูเชิงอรรถที่ ๑๘

ผู้เสียหายจากอาชญากรรมทางเทคโนโลยีเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และตรวจสอบได้ ทั้งนี้ กฎกระทรวงยังเปิดโอกาสให้ผู้เสียหายและผู้ที่เกี่ยวข้องสามารถใช้สิทธิยื่นคำร้องหรือคำคัดค้านพร้อม พยานหลักฐานตามกระบวนการที่กำหนดไว้ เพื่อให้การคืนเงินหรือสินทรัพย์ดิจิทัลเป็นไปอย่างเป็นธรรม แก่ทุกฝ่าย

๔.๕ บทบาทของภาครัฐและความร่วมมือด้านการติดตามทรัพย์สิน

บทบาทของภาครัฐในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ปรากฏ ทั้งในระดับนโยบายของรัฐบาล นำไปสู่การขับเคลื่อนการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยีโดยฝ่ายบริหาร ผ่านทางมติคณะรัฐมนตรี การแต่งตั้งคณะกรรมการอำนวยการป้องกัน และปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีและอาชญากรรมข้ามชาติ เพื่อให้เกิด การบูรณาการการทำงานร่วมกันอย่างมีประสิทธิภาพ ตลอดจนการสร้างความร่วมมือระหว่างหน่วยงาน ที่เกี่ยวข้องโดยการจัดทำบันทึกความเข้าใจเพื่อร่วมมือกันในการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี มีสาระสำคัญดังนี้

(๑) บทบาทของภาครัฐ

การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเป็นเรื่องที่รัฐบาลกำหนดให้เป็น นโยบายสำคัญ ปรากฏจากคำแถลงนโยบายของคณะรัฐมนตรี ซึ่งนายกรัฐมนตรี (นายอนุทิน ชาญวีรกูล) แถลงไว้ต่อรัฐสภา เมื่อวันที่ ๙ เมษายน ๒๕๖๔ ข้อ ๑๐ นโยบายเรื่องการสร้างความมั่นคง ปลอดภัยในชีวิตและทรัพย์สินของประชาชน เพื่อให้ประชาชนปลอดภัยจากอาชญากรรมในรูปแบบต่าง ๆ ซึ่งรวมถึงการฉ้อโกง การหลอกลวงทางไซเบอร์ หรือการฟอกเงิน และยังมีการทบทวนนโยบายการตรวจ ลงตรา (Free Visa) และกฎหมายที่เกี่ยวข้องให้สอดคล้องกับข้อตกลงระหว่างประเทศ เพื่อตัดช่องทาง การเงินของเครือข่ายสแกมเมอร์อาชญากรข้ามชาติทุกรูปแบบ รวมถึงการฟอกเงินและทุนเทาด้วย นอกจากนี้ ในข้อ ๙.๑ ของคำแถลงนโยบายของคณะรัฐมนตรีดังกล่าวยังมีนโยบายเกี่ยวกับการป้องกัน ฝึกระวัง และจัดเตรียมมาตรการรองรับผลกระทบจากภัยคุกคามที่เกิดขึ้นทั้งในและนอกราชอาณาจักร ซึ่งรวมถึงปัญหาสแกมเมอร์ด้วย^{๒๔}

(๒) การขับเคลื่อนมาตรการโดยฝ่ายบริหาร

๑) มติคณะรัฐมนตรี

ในปี พ.ศ. ๒๕๖๘ คณะรัฐมนตรีได้มีการขับเคลื่อนการป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีเพื่อให้เกิดผลเป็นรูปธรรม โดยเมื่อวันที่ ๒๑ ตุลาคม ๒๕๖๘ คณะรัฐมนตรีได้มีมติเห็นชอบให้การป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยี เป็น “วาระแห่งชาติ” เพื่อเป็นการยกระดับการป้องกันและปราบปรามการกระทำความผิดอาชญากรรม ทางเทคโนโลยีและการจัดการกับเงินที่ได้จากการกระทำผิดดังกล่าวให้มีประสิทธิภาพ และประสิทธิผล มากยิ่งขึ้น และเพื่อให้ส่วนราชการ หน่วยงานของรัฐ เอกชน และประชาชนในทุกภาคส่วน ได้ตระหนักและ

^{๒๔} สำนักเลขาธิการคณะรัฐมนตรี, “คำแถลงนโยบายของคณะรัฐมนตรี นายอนุทิน ชาญวีรกูล นายกรัฐมนตรี แถลงต่อรัฐสภา (วันที่ ๙ เมษายน พ.ศ. ๒๕๖๔)”, สืบค้นเมื่อวันที่ ๑๗ มิถุนายน ๒๕๖๔, จาก https://www.soc.go.th/wp-content/uploads/2026/04/Policy_69_th.pdf

ให้ความสำคัญกับการเข้ามามีส่วนร่วมแก้ไขปัญหาดังกล่าวอย่างจริงจังและต่อเนื่อง ให้เกิดผลเป็นรูปธรรม โดยเร็ว ต่อมาคณะรัฐมนตรีได้มีมติเมื่อวันที่ ๔ พฤศจิกายน ๒๕๖๘ เรื่อง การแก้ไขปัญหาการกระทำความผิดอาชญากรรมทางเทคโนโลยี เห็นชอบให้ปัญหาการกระทำความผิดอาชญากรรมทางเทคโนโลยี หรือการหลอกลวงทางออนไลน์ (Scammer) ขบวนการฟอกเงิน ขบวนการค้ามนุษย์ ยาเสพติด และบ่อนการพนัน ถือเป็นภัยร้ายแรงต่อความมั่นคงของรัฐและเศรษฐกิจของประเทศในภาพรวม จึงกำชับให้ทุกส่วนราชการและหน่วยงานของรัฐที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงมหาดไทย กระทรวงยุติธรรม สำนักงานตำรวจแห่งชาติ ธนาคารแห่งประเทศไทย และหน่วยงานความมั่นคงต่าง ๆ ให้ความร่วมมือในการดำเนินการในส่วนที่เกี่ยวข้องอย่างรวดเร็ว จริงจัง และเต็มศักยภาพ เพื่อให้การแก้ไขปัญหการกระทำความผิดในเรื่องนี้เป็นไปอย่างมีประสิทธิภาพและบรรลุผลเป็นรูปธรรมโดยเร็ว

๒) การบูรณาการการทำงานโดยการแต่งตั้งคณะกรรมการอำนวยการป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีและอาชญากรรมข้ามชาติ

โดยที่เพื่อให้การป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยี เป็นไปอย่างต่อเนื่อง และสอดคล้องกับนโยบายของรัฐบาลในการสร้างความมั่นคงปลอดภัยในชีวิตและทรัพย์สินของประชาชน นายกรัฐมนตรีจึงแต่งตั้งคณะกรรมการอำนวยการป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีและอาชญากรรมข้ามชาติขึ้น ตามคำสั่งสำนักนายกรัฐมนตรี ที่ ๑๓๖/๒๕๖๙ เรื่อง แต่งตั้งคณะกรรมการอำนวยการป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีและอาชญากรรมข้ามชาติ ลงวันที่ ๑๑ พฤษภาคม พ.ศ. ๒๕๖๙^{๒๕} โดยมีนายกรัฐมนตรีเป็นประธานกรรมการ องค์ประกอบของคณะกรรมการรวมทั้งสิ้น ๓๔ คน ซึ่งมาจากหลายภาคส่วน มีหน้าที่และอำนาจในการกำหนดนโยบาย มาตรการ และแนวทางปฏิบัติในการป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีและอาชญากรรมข้ามชาติ และกำกับดูแลและบูรณาการการทำงานของหน่วยงานที่เกี่ยวข้องเพื่อเพิ่มขีดความสามารถในการดำเนินงานตามหน้าที่และอำนาจตามกฎหมาย รวมทั้งดำเนินการติดตามและประเมินผลการปฏิบัติการป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีและอาชญากรรมข้ามชาติเพื่อรายงานให้นายกรัฐมนตรีหรือคณะรัฐมนตรีทราบอย่างต่อเนื่องด้วย

๓) ความร่วมมือของหน่วยงานที่เกี่ยวข้อง

โดยที่อาชญากรรมทางเทคโนโลยีเป็นปัญหาระดับชาติ และการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีจะต้องดำเนินโดยหน่วยงานที่เกี่ยวข้องหลายหน่วยงาน ทั้งภาครัฐและภาคเอกชน จึงจำเป็นที่ทุกหน่วยงานจะต้องประสานความร่วมมือระหว่างกันเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี จึงมีการจัดทำบันทึกความเข้าใจว่าด้วยความร่วมมือในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เมื่อวันที่ ๖ พฤศจิกายน ๒๕๖๘ ณ ตึกสันติไมตรี ทำเนียบ

^{๒๕} คำสั่งสำนักนายกรัฐมนตรี ที่ ๑๓๖/๒๕๖๙ เรื่อง แต่งตั้งคณะกรรมการอำนวยการป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีและอาชญากรรมข้ามชาติ ลงวันที่ ๑๑ พฤษภาคม พ.ศ. ๒๕๖๙ ออกโดยอาศัยอำนาจตามความในมาตรา ๑๑ (๖) และ (๙) แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔

รัฐบาล โดยจัดทำขึ้นระหว่างหน่วยงานที่เกี่ยวข้อง รวม ๑๕ หน่วยงาน ได้แก่ กระทรวงการคลัง กระทรวงการต่างประเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงมหาดไทย กระทรวงยุติธรรม กระทรวงพาณิชย์ สำนักงานตำรวจแห่งชาติ สำนักงานป้องกันและปราบปรามการฟอกเงิน (สำนักงาน ปปง.) สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ (สำนักงาน ป.ป.ท.) กรมสอบสวนคดีพิเศษ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ สมาคมธนาคารไทย และสมาคมสถาบันการเงินของรัฐ สำหรับวัตถุประสงค์ของบันทึกความเข้าใจฉบับนี้มีขึ้นเพื่อยกระดับการปราบปรามอาชญากรรมทางเทคโนโลยีและเพื่อป้องกันมิให้ระบบการเงินของประเทศไทยถูกใช้เป็นแหล่งฟอกเงิน สร้างความเชื่อมั่นแก่ประชาชนและนานาชาติในการปราบปรามผู้กระทำความผิดอย่างจริงจัง รวมทั้งบูรณาการความร่วมมือและสร้างเครือข่ายด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เสริมสร้างสนับสนุนการสื่อสาร ประชาสัมพันธ์ ตลอดจนสร้างการรับรู้ให้แก่ประชาชน จึงจำเป็นที่ทุกหน่วยงานทั้งภาครัฐและภาคเอกชน ต้องประสานความร่วมมือในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อให้การบังคับใช้กฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินเป็นไปอย่างมีประสิทธิภาพ โดยมีสาระสำคัญแบ่งออกเป็นด้านการป้องกันและการปราบปรามอาชญากรรมทางเทคโนโลยี สรุปได้ดังนี้

(ก) ด้านการป้องกันอาชญากรรมทางเทคโนโลยี

หน่วยงานที่เกี่ยวข้องทั้ง ๑๕ หน่วยงานจะร่วมมือกันดำเนินการ ดังนี้ ๑) พัฒนามาตรการและสร้างกลไกในการแลกเปลี่ยนข้อมูลที่เป็นประโยชน์ต่อการป้องกันการเกิดอาชญากรรมทางเทคโนโลยีและการฟอกเงินให้ทันทั่วถึง เช่น การฉ้อโกงรูปแบบใหม่ ข้อมูลธุรกรรมทางการเงิน ข้อมูลบัญชี หรือพฤติกรรมที่มีความเสี่ยงสูงที่อาจเป็นสัญญาณของอาชญากรรมทางเทคโนโลยีและการฟอกเงิน ในขณะเดียวกันทุกหน่วยงานต้องร่วมมือกันสร้างเครือข่ายและประชาสัมพันธ์ข้อมูลข่าวสารที่ถูกต้องเพื่อให้ความรู้แก่ประชาชนมิให้ตกเป็นเหยื่อจากการกระทำความผิด ๒) ร่วมกันแลกเปลี่ยนองค์ความรู้และข้อมูลเชิงวิชาการระหว่างกัน รวมทั้งร่วมผลักดันข้อเสนอเชิงนโยบายด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีและการฟอกเงินเพื่อให้เกิดผลในทางปฏิบัติอย่างสูงสุด ๓) ร่วมกันยกระดับมาตรฐานในการพิสูจน์ทราบตัวตนที่เข้มงวด เพื่อมิให้มีการใช้ธุรกรรมทางการเงินในการกระทำความผิด เช่น การเปิดบัญชีม้า และการยกระดับมาตรฐานความปลอดภัยไซเบอร์ เพื่อมิให้เกิดอาชญากรรมทางเทคโนโลยี ๔) ยกระดับมาตรฐานหรือมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยี พร้อมทั้งติดตามตรวจสอบอย่างเป็นรูปธรรม

(ข) ด้านการปราบปรามอาชญากรรมทางเทคโนโลยี

ในการร่วมมือกันปราบปรามอาชญากรรมทางเทคโนโลยีให้เกิดประสิทธิภาพ หน่วยงานที่เกี่ยวข้องได้ร่วมกันจัดทำบันทึกความร่วมมือฯ โดยการกำหนดให้ ๑) หน่วยงานบังคับใช้กฎหมายต้องกำหนดมาตรการและบังคับใช้กฎหมายอย่างเคร่งครัดกับผู้กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี และส่งข้อมูลหรือพยานหลักฐานให้สำนักงาน ปปง. เพื่อดำเนินการกับทรัพย์สินและคุ้มครองสิทธิให้แก่ผู้เสียหายโดยเร็ว โดยทุกหน่วยงานจะร่วมกันสนับสนุนข้อมูลที่เป็นประโยชน์ นอกจากนี้จะมีการประชุมเชิงปฏิบัติการระหว่างหน่วยงานที่เกี่ยวข้องอย่างน้อยเดือนละ ๒ ครั้ง และรายงานผลการ

ปฏิบัติงานให้คณะกรรมการอำนวยการป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีเพื่อทราบ ๒) ทุกหน่วยงานจะร่วมการบูรณาการ แลกเปลี่ยน และเชื่อมโยงข้อมูลหรือพยานหลักฐาน เพื่อดำเนินคดีอาญาที่เกี่ยวกับอาชญากรรมทางเทคโนโลยี และดำเนินการกับทรัพย์สินตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ๓) ทุกหน่วยงานจะตรวจสอบเจ้าหน้าที่ของรัฐที่เข้าไปเกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี หากพบว่ามีเจ้าหน้าที่ของรัฐเกี่ยวข้องกับความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ให้ดำเนินการทางวินัยและทางอาญาอย่างเด็ดขาด รวมทั้งให้ส่งเรื่องไปยังสำนักงาน ป.ป.ท. เพื่อดำเนินการตามกฎหมายต่อไป

บทที่ ๕ บทสรุป*

การหลอกลวงทางไซเบอร์หรือ Cyber Scam เป็นอาชญากรรมร้ายแรงที่เป็นปัญหาใหญ่ในหลายประเทศที่เติบโตพร้อมกับความก้าวหน้าของเทคโนโลยีสมัยใหม่ที่มีความซับซ้อน รูปแบบของการหลอกลวงทางไซเบอร์มีระบบการติดต่อสื่อสารที่รวดเร็ว ฉับไว และหลายครั้งเป็นระบบที่ยากต่อการตรวจสอบ มีรูปแบบของการหลอกลวงมีวิธีการที่แยบยล หลากหลาย เช่น การหลอกลวงโดยการสร้างศูนย์บริการลูกค้าปลอม การหลอกลวงแบบฟิชซิง การหลอกลวงแบบสินทรัพย์ดิจิทัล การหลอกลวงให้ลงทุน การหลอกลวงมีรูปแบบต่าง ๆ และแปลกใหม่อยู่เสมอ ตัวผู้กระทำความผิดก็ไม่ได้ดำเนินการเพียงคนเดียว แต่กลับร่วมมือกันกระทำความผิดในลักษณะเป็นกลุ่ม เป็นเครือข่าย ขยายวงกว้างไปถึงการรวมตัวกันเป็นองค์กรที่อยู่ในประเทศเดียวกันและข้ามประเทศ และการหลอกลวงไม่ได้เน้นเหยื่อที่อ่อนแอ เช่น เด็ก ผู้หญิง หรือคนสูงอายุเท่านั้น แต่ขยายไปถึงประชาชนกลุ่มอื่น ๆ ด้วย เช่น นักธุรกิจ นักลงทุน ประชาชนทั่วไปที่หลงเชื่อตกเป็นเหยื่อต้องสูญเสียเงินและ/หรือทรัพย์สินเป็นจำนวนมาก อีกทั้งผู้กระทำความผิดยังหลอกลวงขอข้อมูลส่วนบุคคล เช่น วันเดือนปีเกิด เลขบัตรเครดิต หมายเลขบัญชีธนาคาร เพื่อนำไปแสวงหาประโยชน์โดยทุจริตในรูปแบบอื่น ๆ กระบวนการของอาชญากรรมเหล่านี้ประกอบด้วยผู้กระทำความผิดที่มีความรู้ความเชี่ยวชาญเกี่ยวกับเทคโนโลยีใหม่ ๆ เป็นอย่างดี รวมทั้งมีความรวดเร็วในการเรียนรู้เกี่ยวกับการเปลี่ยนแปลงระบบทางอินเทอร์เน็ตรูปแบบใหม่ ๆ มีการปรับปรุงพัฒนารูปแบบ วิธีการ การเข้าถึงผู้เสียหายได้อย่างง่ายดาย ผู้กระทำความผิดแบ่งหน้าที่กันทำทั้งเรื่องการจัดหาคนมาช่วยกระทำความผิด การยักยอกถ่ายเทเงินหรือทรัพย์สินอื่นนอกจากการตรวจสอบของเจ้าหน้าที่ตำรวจ การจัดหาวิธีการใหม่ ๆ ในการกระทำความผิด ทำให้ยากในการตรวจสอบการกระทำความผิดรวมทั้งการติดตามเอาคืนซึ่งทรัพย์สินของผู้เสียหาย นอกจากนี้ ในการกระทำความผิดส่วนหนึ่งผู้กระทำความผิดยังใช้กลวิธีในการหลอกลวงผู้เสียหายด้วยการกดดันทางจิตวิทยาให้ผู้เสียหายหลงเชื่อและทำตามที่ผู้กระทำความผิดเสนอ รูปแบบการก่ออาชญากรรมเหล่านี้ทำให้เกิดความเสียหายในแต่ละประเทศขยายวงกว้างจากความเสียหายในระดับครอบครัว ชุมชน เมือง จนถึงระดับประเทศ ซึ่งเป็นภัยคุกคามทางเศรษฐกิจ ความมั่นคง และความปลอดภัยในทรัพย์สินของประชาชน ดังนั้น ประเทศต่าง ๆ และสหประชาชาติจึงได้กำหนดมาตรการต่าง ๆ ทั้งทางด้านการบริหารและกฎหมายเพื่อแก้ไขปัญหาควบคุม รวมทั้งป้องกันไม่ให้เกิดอาชญากรรมเหล่านี้ ดังนี้

ในระดับความตกลงระหว่างประเทศ ปัจจุบันมีความตกลงระหว่างประเทศเกี่ยวกับการต่อต้านอาชญากรรมไซเบอร์ คือ อนุสัญญาสหประชาชาติต่อต้านอาชญากรรมไซเบอร์ (United Nations Convention Against Cybercrime) เป็นสนธิสัญญาระหว่างประเทศในกรอบสหประชาชาติฉบับแรก มีวัตถุประสงค์ในการส่งเสริมและเสริมสร้างมาตรการในการป้องกันและปราบปราม

* จัดทำโดยนางสาวปัทมา เผ่าสังข์ทอง นักกฎหมายกฤษฎีกาชำนาญการพิเศษ ฝ่ายค้นคว้าและเปรียบเทียบกฎหมาย กองกฎหมายต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

อาชญากรรมไซเบอร์ให้มีประสิทธิภาพและประสิทธิผลยิ่งขึ้น ส่งเสริม สนับสนุน และเสริมสร้างความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมไซเบอร์ และส่งเสริม สนับสนุน และช่วยเหลือด้านความช่วยเหลือทางเทคนิคและการเสริมสร้างศักยภาพในการป้องกันและปราบปรามอาชญากรรมไซเบอร์ โดยเฉพาะอย่างยิ่งเพื่อประโยชน์ของประเทศกำลังพัฒนา โดยอนุสัญญากำหนดเนื้อหาสาระที่สำคัญ ๓ ส่วน คือ (๑) การกำหนดความผิดทางอาญา (๒) ความร่วมมือระหว่างประเทศ และ (๓) ความช่วยเหลือทางเทคนิคและการแลกเปลี่ยนข้อมูล ซึ่งประเทศไทยได้เข้าร่วมพิธีลงนามอนุสัญญาดังกล่าวแล้วด้วย

สำหรับมาตรการที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมการหลอกลวงทางไซเบอร์ของต่างประเทศ สรุปได้ดังนี้

ประเทศแคนาดา

มีการจัดตั้งหน่วยงานภาครัฐในการกำกับดูแลและมีการกำหนดมาตรการทางกฎหมายต่าง ๆ เช่น การกำหนดความผิดไว้ในประมวลกฎหมายอาญา กฎหมาย Canada's anti-spam legislation (CASL) ที่มีวัตถุประสงค์ในการคุ้มครองผู้บริโภคและภาคธุรกิจจากการใช้เทคโนโลยีดิจิทัลในทางที่ผิด รวมถึง spam และภัยคุกคามทางอิเล็กทรอนิกส์อื่น ๆ และกฎหมาย BILL C-8 An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts ที่มุ่งเน้นการสนับสนุนความมั่นคงของระบบโทรคมนาคมของประเทศ และยกระดับความมั่นคงปลอดภัยทางไซเบอร์ในภาคส่วนต่าง ๆ เพื่อแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ทั้งเรื่องของ Cyber Scam และอาชญากรรมทางไซเบอร์ในรูปแบบอื่น ๆ ด้วย

ประเทศเยอรมนี

ในระบบกฎหมายเยอรมันไม่มีกฎหมายที่กำหนดกลไกสำหรับการป้องกันและปราบปรามการหลอกลวงทางไซเบอร์ไว้โดยตรงในกฎหมายฉบับเดียว ระบบกฎหมายเยอรมันได้กำหนดมาตรการทางกฎหมายที่ใช้บังคับกับการกระทำความผิดในเรื่องของการหลอกลวงทางไซเบอร์โดยอาศัยการปรับใช้กฎหมายที่มีอยู่ตามลักษณะของพฤติกรรมและผลเสียหายที่เกิดขึ้น ระบบกฎหมายเยอรมันมีการกำหนดมาตรการทางกฎหมายแบ่งได้เป็นสามส่วนหลัก ได้แก่ มาตรการทางอาญา มาตรการทางแพ่ง และมาตรการสืบสวนสอบสวน โดยในส่วนของการกระทำความผิดทางอาญา เช่น ความผิดฐานฉ้อโกง การปลอมแปลงข้อมูลทางอิเล็กทรอนิกส์ การกำหนดความรับผิดและโทษของผู้กระทำความผิดในทางอาญาจะเป็นไปตามประมวลกฎหมายอาญา ซึ่งต้องพิจารณาว่าการกระทำที่เป็นมูลเหตุให้เกิดความเสียหายนั้นเข้าองค์ประกอบความผิดฐานใด ส่วนการเยียวยาผู้เสียหายในทางแพ่งจะเป็นไปตามบทบัญญัติในประมวลกฎหมายแพ่ง โดยเฉพาะหลักกฎหมายว่าด้วยธุรกรรมการชำระเงินที่ไม่ได้รับอนุญาตตามกฎหมายได้ และความรับผิดทางละเมิด นอกจากนี้ ในเรื่องของการรวบรวมพยานหลักฐานดิจิทัล การติดตามตัวผู้กระทำความผิด และการติดตามทรัพย์สินที่ได้จากการกระทำความผิดจะเป็นไปตามมาตรการตามกฎหมายวิธีพิจารณาความอาญา นอกจากกฎหมายหลักดังกล่าวข้างต้น ระบบกฎหมายเยอรมันยังมีกฎหมายอื่นที่มีบทบาทเสริมในการกำกับดูแลระบบการเงินและระบบดิจิทัลให้มีความปลอดภัยและมีประสิทธิภาพยิ่งขึ้น เช่น กฎหมายกำกับบริการชำระเงิน กฎหมายป้องกันและปราบปรามการฟอกเงิน กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์

ประเทศออสเตรเลีย

รัฐบาลออสเตรเลียพัฒนากฎหมายการจัดการและป้องกันอาชญากรรมทางเทคโนโลยีหรือการหลอกลวงทางไซเบอร์ (Scams Prevention Framework: SPF) ขึ้น กฎหมาย SPF ถือเป็นส่วนหนึ่งของกฎหมายคุ้มครองผู้บริโภค ซึ่งมีหลักการสำคัญ ๖ ประการ คือ การกำกับดูแล การป้องกัน การตรวจจับ การรายงาน การขัดขวาง และการรับมือกับการหลอกลวง รวมทั้งกำหนดการทำงานในลักษณะของคณะกรรมการในการช่วยดูแลและแก้ไขปัญหาดังกล่าวนี้นี้ ผู้ที่กระทำความผิดตามกฎหมายนี้ต้องได้รับบทลงโทษทางแพ่ง นอกจากนี้ กฎหมายฉบับนี้ยังกำหนดให้หน่วยงานที่ถูกกำกับดูแลต้องจัดให้มีกลไกการเยียวยาให้ผู้บริโภค โดยครอบคลุมถึงกระบวนการระงับข้อพิพาทภายในองค์กร และกระบวนการระงับข้อพิพาทภายนอก รวมถึงผู้เสียหายยังสามารถใช้สิทธิฟ้องร้องต่อศาลได้ด้วย เพื่อเป็นการคุ้มครองและเยียวยาผู้ได้รับความเสียหายในคราวเดียวกัน

ประเทศจีน

จีนเป็นประเทศที่มีความเจริญก้าวหน้าทางเทคโนโลยีเป็นอย่างมาก แต่ในอีกด้านหนึ่งของการพัฒนาเทคโนโลยีอย่างรวดเร็ว ก็มีการเกิดขึ้นของอาชญากรรมทางเทคโนโลยีและทวีความรุนแรงไปทั่วทุกภูมิภาคจนกลายเป็นภัยคุกคามระดับโลก เพื่อแก้ไขปัญหาดังกล่าวนี้นี้ จีนจึงได้พัฒนาแนวทางแก้ไขปัญหาคือที่เรียกว่า “Chinese solution” ซึ่งมีพื้นฐานจากประสบการณ์การแก้ไขปัญหาที่ประสบความสำเร็จภายในประเทศ เพื่อนำมาเป็นต้นแบบในการรับมือกับปัญหาระดับโลกนี้ โดยมีหลักการสำคัญ ได้แก่ การยึดประชาชนเป็นศูนย์กลาง การเสริมสร้างความเข้มแข็งอย่างรอบด้านผ่านการพัฒนางานวิจัยเฉพาะด้าน การจัดตั้งทีมเฉพาะกิจ การดำเนินการแก้ไขคดีเฉพาะ การพัฒนาบุคลากรผู้เชี่ยวชาญ ตลอดจนมีการบูรณาการภายในประเทศและการประสานความร่วมมือกับต่างประเทศในการบังคับใช้กฎหมายให้มีประสิทธิภาพ ซึ่งจีนมีการบังคับใช้กฎหมายว่าด้วยการปราบปรามการฉ้อโกงทางโทรคมนาคมและออนไลน์เพื่อกำกับดูแลการปราบปรามการฉ้อโกงทางโทรคมนาคมและออนไลน์ที่มีลักษณะเฉพาะแบบจีน นอกจากนี้ จีนยังได้แก้ไขเพิ่มเติมประมวลกฎหมายอาญาเพื่อใช้ในการปราบปรามตลาดมืดทางออนไลน์เพื่อให้เท่าทันต่อสถานการณ์ปัจจุบันที่มีการเปลี่ยนแปลงรูปแบบของกลวิธีในการก่ออาชญากรรมทางเทคโนโลยีอย่างรวดเร็ว ซึ่งความพยายามปราบปรามอย่างจริงจังเช่นนี้ช่วยทำให้สถิติคดีด้านอาชญากรรมทางเทคโนโลยีลดลงได้มาก

ประเทศเกาหลีใต้

เกาหลีใต้ต้องเผชิญกับปัญหาการก่ออาชญากรรมไซเบอร์ที่รุนแรงที่มาจากข้อพิพาททางการเมือง เศรษฐกิจ และการทหารระหว่างประเทศ ด้วยปัจจัยดังกล่าว เกาหลีใต้จึงได้กำหนดแนวนโยบายของรัฐในการจัดทำยุทธศาสตร์ความมั่นคงทางไซเบอร์แห่งชาติ (National Cybersecurity Strategy) และมาตรการทางกฎหมายในเรื่องต่าง ๆ รวมทั้งปรับปรุงแก้ไขเพิ่มเติมกฎหมายหลายฉบับ ซึ่งปัจจุบันมีการบังคับใช้กฎหมายที่สำคัญหลายฉบับเพื่อแก้ไขปัญหาดังกล่าวนี้นี้ เช่น กฎหมายพิเศษว่าด้วยการป้องกันการฉ้อโกงทางการเงินผ่านทางโทรคมนาคมและการคืนทรัพย์สินที่ได้มาโดยมิชอบจากการฉ้อโกง กฎหมายว่าด้วยการส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลและการสื่อสาร และการคุ้มครองข้อมูลหรือกฎหมายว่าด้วยการคุ้มครองโครงสร้างพื้นฐานข้อมูลสารสนเทศและการสื่อสาร ซึ่งมีเนื้อหาสาระกำหนดบทนิยามของการกระทำความผิด การกระทำความผิดในลักษณะต่าง ๆ รวมทั้งมีบทกำหนดโทษไว้

อย่างชัดเจนเพื่อให้เหมาะสมกับสถานการณ์ปัจจุบัน และเป็นการป้องกันและปราบปรามอาชญากรรมทาง
หลอกลวงทางไซเบอร์เพื่อปกป้องผลประโยชน์ของประเทศชาติและทรัพย์สินของประชาชนอย่างจริงจัง
และต่อเนื่องอย่างเป็นรูปธรรม

ประเทศสิงคโปร์

สิงคโปร์ต้องเผชิญกับปัญหาอาชญากรรมทางไซเบอร์ที่กลายเป็นประเด็นปัญหาระดับ
นานาชาติ ปัญหาอาชญากรรมทางไซเบอร์ที่เกิดขึ้นในสิงคโปร์มีหลายประเภท เช่น การหลอกลวง
ให้ทำงาน หรือการหลอกลวงให้ลงทุน ซึ่งก่อให้เกิดความเสียหายจำนวนมาก รัฐบาลสิงคโปร์ได้ดำเนิน
มาตรการเชิงรุกเพื่อรับมือกับความเสียหายจาก Cyber Scam โดยมีแนวนโยบายทั้งในระดับประเทศที่เป็น
ความร่วมมือระหว่างรัฐบาลกับเอกชน เช่น ธนาคาร และระดับระหว่างประเทศที่เป็นความร่วมมือกับ
หน่วยงานกำกับดูแลในต่างประเทศ เพื่อส่งเสริมการแลกเปลี่ยนองค์ความรู้และความเข้าใจเกี่ยวกับ
มาตรการและแนวทางในการป้องกันและปราบปราม นอกจากนี้ ยังมีการบังคับใช้กฎหมายเพื่อ
ปราบปรามการกระทำความผิดดังกล่าวนี้ด้วย คือ The Computer Misuse Act 1993 ที่เน้นการควบคุม
การใช้ระบบคอมพิวเตอร์โดยมิชอบ ซึ่งมีความเกี่ยวข้องกับการกระทำความผิดเกี่ยวกับ cyber scam
โดยตรง หรือ The Online Criminal Harms Act 2023 เป็นกฎหมายที่ตราขึ้นเพื่อให้รัฐมีเครื่องมือ
แทรกแซงกิจกรรมออนไลน์ที่เกี่ยวข้องกับการก่ออาชญากรรมได้อย่างรวดเร็วและมีประสิทธิภาพ
ซึ่งออกแบบมาเพื่อรับมือกับอาชญากรรมออนไลน์และ Cyber scam ได้อย่างเป็นระบบ และ The
Protection from Scams Act 2025 เป็นกฎหมายที่มุ่งป้องกันความเสียหายจากการหลอกลวงทาง
ไซเบอร์โดยการแทรกแซงทางการเงินโดยตรงต่อเหยื่อ ด้วยการให้อำนาจเจ้าหน้าที่ออกคำสั่งจำกัด
ธุรกรรมทางธนาคารและการใช้สินเชื่อของบุคคลที่มีความเสี่ยงจะตกเป็นเหยื่อของการหลอกลวง
เพื่อหยุดยั้งความเสียหายก่อนที่จะเกิดขึ้น จึงเห็นได้ว่า การกำหนดมาตรการเชิงนโยบายและกฎหมาย
เพื่อป้องกันและปราบปรามอย่างจริงจัง มีส่วนสำคัญในการป้องกันและแก้ไขปัญหาแบบองค์รวมของ
สิงคโปร์ที่เกิดขึ้น และช่วยลดจำนวนอัตราความเสียหายพร้อมกับช่วยยับยั้งการเกิดขึ้นของอาชญากรรม
ทางไซเบอร์ได้เป็นอย่างดี

ประเทศไทย

ไทยประสบปัญหาของการก่ออาชญากรรมทางไซเบอร์ในหลากหลายรูปแบบและทำให้
ประชาชนได้รับความเสียหายทางการเงินเป็นจำนวนมาก และส่งผลกระทบต่อความมั่นคงของเศรษฐกิจ
ของประเทศเช่นเดียวกับประเทศอื่น ๆ รัฐจึงได้จัดทำมาตรการในการป้องกันและปราบปรามอาชญากรรม
ทางเทคโนโลยีของประเทศไทยทั้งมาตรการทางบริหาร มาตรการเชิงป้องกันและมาตรการเชิงลงโทษ
รวมทั้งมาตรการทางกฎหมาย โดยมีกลไกการกำกับดูแลแพลตฟอร์มดิจิทัล ตลอดจนมีมาตรการในการ
ติดตามทรัพย์สินของผู้ถูกหลอกลวงทางไซเบอร์ให้ได้กลับคืนมาโดยเร็ว โดยมีการตราพระราชกำหนด
มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ ขึ้น เพื่อเป็นเครื่องมือในการ
ป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้หมดไปโดยเร็วและเกิดประสิทธิภาพ ตลอดจนเพื่อ
รักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะและความมั่นคงในทางเศรษฐกิจของประเทศ
และต่อมาได้มีการแก้ไขเพิ่มเติมกฎหมายฉบับดังกล่าวโดยมีการตราพระราชกำหนดมาตรการป้องกันและ
ปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ๒) พ.ศ. ๒๕๖๘ ขึ้นเพื่อให้มีมาตรการเพิ่มเติมสำหรับการ

ป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้ครอบคลุมและมีประสิทธิภาพมากยิ่งขึ้น รวมทั้งมีการจัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และกำหนดให้มีกระบวนการการคืนเงินแก่ผู้เสียหายให้เป็นไปโดยเร็ว รวมทั้งสร้างการมีส่วนร่วมรับผิดชอบต่อความเสียหายที่เกิดจากการกระทำความผิดอาชญากรรมทางเทคโนโลยีเพื่อเยียวยาผู้เสียหาย ตลอดจนการกำหนดโทษในส่วนที่เกี่ยวข้องด้วย

เพื่อให้การปราบปรามอาชญากรรมทางไซเบอร์มีความเด็ดขาดและจริงจัง ในปี พ.ศ. ๒๕๖๘ รัฐบาลได้เห็นชอบให้การป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีเป็น “วาระแห่งชาติ” เพื่อเป็นการยกระดับการป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีและการจัดการกับเงินที่ได้จากการกระทำความผิดดังกล่าวให้มีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น ส่งผลให้ปัญหาการกระทำความผิดอาชญากรรมทางเทคโนโลยีหรือการหลอกลวงทางออนไลน์ (Scammer) ขบวนการฟอกเงิน ขบวนการค้ายาเสพติด และบ่อนการพนัน ถือเป็นภัยร้ายแรงต่อความมั่นคงของรัฐและเศรษฐกิจของประเทศ ที่หน่วยงานที่เกี่ยวข้องทุกภาคส่วนจะร่วมมือกันแก้ไขปัญหาการกระทำความผิดในเรื่องนี้ให้หมดสิ้นไปจากประเทศไทยและผู้ที่ได้รับความเสียหายได้รับความช่วยเหลืออย่างเหมาะสมต่อไป

จากการศึกษาแนวทางการแก้ไขปัญหาอาชญากรรมทางไซเบอร์จากประเทศต่าง ๆ ข้างต้นแล้ว เห็นได้ว่านอกจากการบังคับใช้กฎหมายภายในประเทศเพื่อการปราบปรามยังยั้งการกระทำความผิดในทุกรูปแบบอย่างทันทั่วทั้งที่แล้ว การป้องกัน แก้ไข และปราบปรามอาชญากรรมทางไซเบอร์จะประสบความสำเร็จได้ต้องพึ่งพาแนวนโยบายที่ชัดเจนของประเทศในการปราบปรามอาชญากรรมดังกล่าวนี้ พร้อมกับต้องอาศัยความร่วมมือจากทุกภาคส่วน ภาครัฐ ภาคเอกชน ภาคธนาคาร และภาคประชาชน ตลอดจนได้รับความร่วมมือจากประเทศต่าง ๆ อย่างจริงจังและต่อเนื่อง การศึกษาแนวทางการแก้ไขปัญหาอาชญากรรมทางไซเบอร์จากประเทศต่าง ๆ ถือเป็นข้อมูลส่วนหนึ่งที่มีประโยชน์ในการนำมาปรับใช้กับการแก้ไขปัญหาอาชญากรรมทางไซเบอร์ในบริบทที่เหมาะสมกับประเทศไทยต่อไป

จัดทำโดย

ที่ปรึกษา

๑. นายณพดล เกริกฤกษ์	เลขาธิการคณะกรรมการกฤษฎีกา
๒. นางสาวนุชนาถ เกษมพิบูลย์ไชย	รองเลขาธิการคณะกรรมการกฤษฎีกา
๓. นายจิตรพรต พัฒนสิน	กรรมการร่างกฎหมายประจำ
๔. นางกาญจนารักษ์ อินทปนต์ เลิศลอย	ผู้อำนวยการกองกฎหมายต่างประเทศ

ฝ่ายค้นคว้าและเปรียบเทียบกฎหมาย กองกฎหมายต่างประเทศ

๑. นางสาวฉันทพิมพ์ บรรจงจิตร	ผู้อำนวยการฝ่ายฯ
๒. นางสาวนพรัตน์ พิริยานสรณ์	นักกฎหมายกฤษฎีกาชำนาญการพิเศษ
๓. นางสาวพิมพ์สิริ วิเศษโอฬารนนท์	นักกฎหมายกฤษฎีกาชำนาญการพิเศษ
๔. นางสาวปัทมา เผ่าสังข์ทอง	นักกฎหมายกฤษฎีกาชำนาญการพิเศษ
๕. นายสรวิทย์ ล้ออัศจรรย์	นักกฎหมายกฤษฎีกาชำนาญการพิเศษ
๖. นายณัฐพล สกุลเมฆา	นักกฎหมายกฤษฎีกาชำนาญการพิเศษ
๗. นางสาวนันทกานต์ ขำยัง	นักกฎหมายกฤษฎีกาชำนาญการพิเศษ
๘. นางสาววาริรัตน์ รัตนวิบูลย์สม	นักกฎหมายกฤษฎีกาชำนาญการพิเศษ
๙. นางสาวกรภัทร ปัญญาวนิช	เจ้าหน้าที่โครงการจัดจ้างบุคลากร สำหรับจัดทำฐานข้อมูลกฎหมายฯ
๑๐. นางสาวอรอร กฤษณะทรัพย์	เจ้าหน้าที่โครงการจัดจ้างบุคลากร สำหรับจัดทำฐานข้อมูลกฎหมายฯ