

มาตรการทางกฎหมายและแนวนโยบายในการป้องกันและปราบปรามอาชญากรรมการหลอกลวงทางไซเบอร์ (Cyber Scam)

นางสาววาริรัตน์ รัตนวิบูลย์สม^๑

๑. บทนำ

สาธารณรัฐเกาหลี (เกาหลีใต้) ได้ขึ้นชื่อว่าเป็นประเทศที่สร้างสภาพแวดล้อมของโลกไซเบอร์ (cyberspace) ที่ก้าวหน้ามากที่สุดแห่งหนึ่งของโลกทั้งในเรื่องเทคโนโลยีสารสนเทศและการสื่อสาร (information and communications technology (ICT)) และโครงสร้างพื้นฐานที่เกี่ยวข้องกับเทคโนโลยีดังกล่าว ในปัจจุบันนี้ cyberspace มีความสำคัญต่อชีวิตประจำวัน การดำเนินกิจกรรมทางเศรษฐกิจ การประกอบธุรกิจ การดำเนินงานของภาครัฐ และการให้บริการพื้นฐาน แต่โดยที่การเชื่อมต่อระหว่างอุปกรณ์ด้านสารสนเทศและการสื่อสารมีความหลากหลาย และ cyberspace มีความซับซ้อน เพิ่มมากขึ้นและทำให้ยากต่อการจัดการเพื่อให้เกิดความปลอดภัย อีกทั้ง cyberspace มีลักษณะเป็นเทคโนโลยีไร้พรมแดนทำให้เกิดความสับสนเสี่ยงที่จะใช้เพื่อเป็นภัยคุกคามต่อโลกไซเบอร์ได้ ในอดีตที่ผ่านมา กลุ่มผู้ก่อการร้ายได้นำเทคโนโลยีไซเบอร์เป็นเครื่องมือในการมุ่งประสงค์จะก่ออาชญากรรมไซเบอร์ขยายในวงกว้างเนื่องจากได้รับการสนับสนุนจากผู้มีบทบาทในระดับรัฐ และวิธีการโจมตีที่มีความหลากหลายมากขึ้นทั้งในรูปแบบของการขโมยข้อมูลและทรัพย์สินเงินทอง รวมถึงการสร้างควมวุ่นวายให้สังคมเกิดความไม่สงบสุขโดยมุ่งเป้าไปยังวัตถุประสงค์ทางการเมือง และทำลายโครงสร้างพื้นฐานของประเทศ การก่ออาชญากรรมไซเบอร์มีแนวโน้มที่จะรุนแรงขึ้นเป็นสงครามไซเบอร์ (cyber war) ซึ่งอาจสร้างความเสียหายได้รุนแรงเทียบเท่ากับการโจมตีด้วยอาวุธยุทโธปกรณ์ในรูปแบบที่มีมาแต่ดั้งเดิม

ข้อพิพาททางการเมือง เศรษฐกิจ และการทหารระหว่างประเทศ เป็นปัจจัยที่นำไปสู่ความขัดแย้งในโลกไซเบอร์ และรัฐบาลของประเทศต่าง ๆ ได้สนับสนุนงบประมาณเพื่อพัฒนาเทคโนโลยีไซเบอร์ให้มีความทันสมัยโดยอาศัยปัญญาประดิษฐ์และการวิเคราะห์ข้อมูลขนาดใหญ่ หรือ big data รวมทั้งการเสริมสร้างขีดความสามารถในการจัดเก็บข้อมูลความล้าสมัยด้านไซเบอร์ การก่อวินาศกรรมเครือข่ายอินเทอร์เน็ต และการคุกคามสิ่งอำนวยความสะดวกที่สำคัญ อีกทั้งอาชญากรรมไซเบอร์ยังคงสร้างความเสียหายต่อภาคธุรกิจและประชาชนอยู่อย่างต่อเนื่องอันเนื่องมาจากความก้าวหน้าทางเทคโนโลยีและความซับซ้อนที่เพิ่มขึ้นของการโจมตีทางไซเบอร์ เช่น การโจรกรรมข้อมูลส่วนบุคคล การเข้ามามีส่วนเกี่ยวข้องของกลุ่มผู้มีอำนาจในระดับรัฐและกลุ่มผู้ก่อการร้ายยังเป็นปัจจัยสำคัญที่ก่อความเสียหายจากอาชญากรรมไซเบอร์ให้รุนแรงและร้ายแรงยิ่งขึ้นอันนำไปสู่ความเสียหายต่อความมั่นคงของประเทศ ด้วยเหตุนี้ทำให้เกาหลีใต้กำหนดนโยบายและมาตรการทางกฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมการหลอกลวงทางไซเบอร์เพื่อปกป้องผลประโยชน์ของประเทศชาติและทรัพย์สินของประชาชนของตนอย่างจริงจังและต่อเนื่อง^๒

^๑ นักกฎหมายกฤษฎีกาชำนาญการพิเศษ ฝ่ายกฎหมายกระบวนการยุติธรรมทางแพ่ง กองกฎหมายกระบวนการยุติธรรม

^๒ CHEONG WA DAE, “National Cybersecurity Strategy”, National Security Office: April 2019, pp. 6-8.

๒. แนวนโยบายของรัฐในการป้องกันและปราบปรามไซเบอร์

รัฐบาลเกาหลีใต้ได้จัดทำยุทธศาสตร์ความมั่นคงทางไซเบอร์แห่งชาติ (National Cybersecurity Strategy)^๓ โดยมีวิสัยทัศน์เพื่อสร้าง cyberspace ให้เป็นพื้นที่เสรีและปลอดภัย สร้างความมั่นคงทางเศรษฐกิจ และสนับสนุนให้เกิดสันติภาพระหว่างประเทศ เพื่อนำไปสู่เป้าหมายดังต่อไปนี้

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

๒. การตอบสนองต่อการโจมตีทางไซเบอร์ (Respond to cyber attacks) เพิ่มขีดความสามารถด้านความมั่นคงเพื่อยับยั้งภัยคุกคามทางไซเบอร์ ตรวจสอบและสกัดกั้นการคุกคามทางไซเบอร์ได้อย่างรวดเร็วและตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างทันท่วงที

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

ยุทธศาสตร์ความมั่นคงทางไซเบอร์แห่งชาติประกอบด้วยหลักการพื้นฐานที่สำคัญได้แก่

๑. สร้างความสมดุลระหว่างสิทธิส่วนบุคคลและความมั่นคงทางไซเบอร์ (Balance individual rights with cybersecurity) การสร้างความสมดุลให้เกิดขึ้นระหว่างการปกป้องโลกไซเบอร์และการคุ้มครองสิทธิขั้นพื้นฐานของบุคคล

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 เพิ่มความยืดหยุ่นและพัฒนาระบบการสำรองข้อมูลให้เกิดความต่อเนื่องใช้เทคโนโลยีเข้าสู่รหัสขั้นสูงเพื่อป้องกันข้อมูลรั่วไหล ตลอดจนเตรียมความพร้อมรับมือกับเทคโนโลยียุคใหม่ด้วยการพัฒนาเครือข่ายข้อมูลและสร้างระบบการยืนยันตัวตนที่ปลอดภัยในยุคดิจิทัลปัจจุบัน

^๓ เฟิ่งอ่า ๑๒-๒๖.

๒. การยกระดับขีดความสามารถในการตอบโต้การโจมตีทางไซเบอร์ (Enhance Cyber Attack Response Capabilities)

การยกระดับขีดความสามารถในการตอบโต้การโจมตีทางไซเบอร์ของเกาหลีใต้ ประกอบด้วย การดำเนินการทั้งในมิติเชิงรับและเชิงรุก กล่าวคือ นโยบายเชิงรับของรัฐบาล รัฐบาล มีการจัดเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ครั้งใหญ่โดยมีการประเมินและพัฒนาระบบ การแบ่งปันข้อมูล การสืบสวนสอบสวน และการมีปฏิกิริยาตอบโต้ของหน่วยงานที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ดังกล่าวพร้อมทั้งได้เพิ่มขีดความสามารถในการตอบสนองต่อวิกฤตการณ์ทางไซเบอร์ที่เกิดขึ้นให้ครอบคลุมทั่วประเทศ ในส่วนของนโยบายเชิงรุกนั้น รัฐบาลได้จัดการป้องกันปราม เพื่อตอบโต้ภัยคุกคามที่กระทบต่อความมั่นคงของประเทศอย่างจริงจังและเพิ่มขีดความสามารถ ในการวิเคราะห์สาเหตุของการโจมตีและสืบหาตัวผู้กระทำผิด อีกทั้งการกำหนดให้มีมาตรการตอบโต้เชิงรุกโดยการพัฒนายุทธศาสตร์และกำลังพลทางทหารเพื่อคุ้มกันความมั่นคงของประเทศ ผักผ่อน ทักษะความเชี่ยวชาญเฉพาะด้าน และเสริมสร้างขีดความสามารถในการสืบสวนสอบสวนและจับกุมตัว ผู้กระทำความผิดและการดำเนินคดีอย่างมีประสิทธิภาพ

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

โดยอาศัยการประสานความร่วมมือระหว่างภาครัฐ เอกชน และทหาร เพื่อสร้างระบบ การบริหารจัดการโดยมีสำนักงานสภาความมั่นคงแห่งชาติ (National Security Office) เป็นหน่วยงาน กำกับดูแลความร่วมมือดังกล่าว รวมทั้งพัฒนาและนำนโยบายความมั่นคงทางไซเบอร์ไปปรับใช้ ร่วมกันเป็นแผนระดับชาติ นอกจากนี้ มีการสร้างระบบแบ่งปันข้อมูลทั่วประเทศเพื่อมุ่งเน้นการส่งผ่าน ข้อมูลร่วมกันทุกภาคส่วนเพื่อป้องกันการเผยแพร่ข้อมูลเท็จเกี่ยวกับการคุกคามทางไซเบอร์ รวมถึงการ เสริมสร้างมาตรการทางกฎหมายเพื่อรองรับการดำเนินการด้านความมั่นคงทางไซเบอร์ซึ่งอาจอยู่ใน รูปแบบของการปรับปรุงกฎหมายและร่วมมือกับสถาบันหรือหน่วยงานที่เกี่ยวข้องเพื่อรับมือกับภัย คุกคามหรือความท้าทายที่อาจเกิดขึ้นใหม่ เช่น การอุดช่องโหว่จากการใช้เทคโนโลยี AI

๔. การวางรากฐานรองรับการเติบโตของอุตสาหกรรมความมั่นคงทางไซเบอร์ (Build Foundations for Cybersecurity Industry Growth)

ขยายการลงทุนด้านความมั่นคงทางไซเบอร์ทั้งในด้านการปฏิรูปกฎหมาย เพิ่มงบประมาณของรัฐเพื่อใช้ในกรณีที่มีเหตุฉุกเฉิน ใช้มาตรการทางภาษีจูงใจภาคเอกชนให้ลงทุน ด้านความมั่นคงและการวิจัยและพัฒนา (R&D) เสริมสร้างขีดความสามารถในการแข่งขันของบุคลากร และเทคโนโลยี ส่งเสริมสภาพแวดล้อมเพื่อการเติบโตของบริษัทด้านความมั่นคงทางไซเบอร์ และ กำหนดหลักเกณฑ์การแข่งขันที่เป็นธรรมในตลาดด้านความมั่นคงทางไซเบอร์

๕. การปลูกฝังวัฒนธรรมความมั่นคงทางไซเบอร์ (Foster a Cybersecurity Culture)

การสร้างตระหนักรู้และแนวปฏิบัติเกี่ยวกับความมั่นคงทางไซเบอร์ โดยมุ่งเน้นการพัฒนาและการประยุกต์ใช้กฎระเบียบในชีวิตประจำวันได้จริง การจัดหลักสูตรการเรียน การสอนเกี่ยวกับจริยธรรมในการใช้ไซเบอร์ในกลุ่มนักเรียน นักศึกษา เจ้าหน้าที่ของรัฐ ทหาร และ พนักงานบริษัท การสร้างจิตสำนึกให้กับภาคธุรกิจให้รับผิดชอบในการรักษาความปลอดภัยของ ผลิตภัณฑ์และบริการ ตลอดจนการสร้างสมดุลระหว่างสิทธิขั้นพื้นฐานและความมั่นคงทางไซเบอร์ เพื่อสร้างความเชื่อมั่นว่าภาครัฐจะไม่เข้าแทรกแซงหรือละเมิดสิทธิของประชาชนโดยผิดกฎหมาย

๖. การเป็นผู้นำความร่วมมือระหว่างประเทศด้านความมั่นคงทางไซเบอร์ (Lead International Cooperation in Cybersecurity)

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

แผนการดำเนินงานตามยุทธศาสตร์

รัฐบาลเกาหลีใต้ได้รับระบุในแผนการดำเนินงานตามยุทธศาสตร์ว่าจะปฏิบัติหน้าที่ตามความรับผิดชอบและแสดงภาวะความเป็นผู้นำเพื่อให้บรรลุผลสำเร็จตามวิสัยทัศน์และเป้าหมายของ “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 และปฏิบัติภารกิจเชิงยุทธศาสตร์ในการสนับสนุนให้มีกฎหมาย 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 กฎหมายหลายฉบับได้มีการปรับปรุงแก้ไขเพิ่มเติมในเวลาต่อมาเพื่อให้

เหมาะสมกับสถานการณ์ปัจจุบันซึ่งเป็นสิ่งสะท้อนนโยบายและการกำกับดูแลระดับประเทศที่มีต่อความมั่นคงทางไซเบอร์อย่างมีประสิทธิภาพ สรุปได้ดังนี้^๔

๑. Special Act on the Prevention of Telecommunications-Based Financial Fraud and Refund of Fraudulently Obtained Assets^๕

วัตถุประสงค์^๖

กฎหมายพิเศษว่าด้วยการป้องกันการฉ้อโกงทางการเงินผ่านทางโทรคมนาคม และการคืนทรัพย์สินที่ได้มาโดยมิชอบจากการฉ้อโกงมีวัตถุประสงค์เพื่อกำหนดมาตรการของรัฐในการป้องกันความสูญเสียและกำหนดความรับผิดชอบของสถาบันการเงินในการป้องกันความสูญเสีย เพื่อมุ่งหมายที่จะป้องกันการฉ้อโกงทางการเงินผ่านทางโทรคมนาคม อีกทั้งยังได้กำหนดขั้นตอนการระงับสิทธิเรียกร้อง (extinguishment of claims) ต่อบัญชีที่ถูกฉ้อโกง ขั้นตอนการเรียกร้องค่าชดเชยความเสียหาย เพื่อชดเชยความสูญเสียให้แก่ผู้เสียหายจากการฉ้อโกงทางการเงินผ่านโทรคมนาคมและช่วยเยียวยาให้ผู้เสียหายสามารถฟื้นฟูความสูญเสียทางทรัพย์สินได้อย่างรวดเร็ว

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

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

๑.๒ การตอบโต้การฉ้อโกงผ่านระบบโทรคมนาคม (มาตรา ๒-๒) Financial Services Commission (FSC) มีหน้าที่ในการจัดเตรียมมาตรการป้องกันและลดการสูญเสียความเสียหายที่เกิดจากการฉ้อโกงผ่านทางโทรคมนาคม เช่น รวบรวมและเผยแพร่ข้อมูลการฉ้อโกงทางการเงินผ่านทางโทรคมนาคม ตลอดจนเมื่อมีเหตุจำเป็นเพื่อป้องกันการฉ้อโกงทางการเงินผ่านทางโทรคมนาคม FSC อาจให้คำแนะนำ ร้องขอ หรือออกคำสั่งให้สถาบันการเงินปรับปรุงแผนการดำเนินงานโดยพิจารณาจากจำนวนเงินชดเชยความสูญเสียที่จ่ายไปในแต่ละปีและจำนวนครั้งของบัญชีที่ถูกใช้ในการฉ้อโกง

^๔ Santiago Paz et al., “Executive Summary”, National Cybersecurity Law, Governance, and Infrastructure: IN THE REPUBLIC OF KOREA: 2024, pp. VIII-IX.

^๕ Act No. 19418, May 16, 2023

^๖ 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.

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^๗

วัตถุประสงค์^๘

กฎหมายว่าด้วยการส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลและการสื่อสาร และการคุ้มครองข้อมูล (หรือเรียกว่า กฎหมายเครือข่ายสารสนเทศและการสื่อสาร) มีวัตถุประสงค์เพื่อพัฒนาคุณภาพชีวิตของประชาชนและส่งเสริมสวัสดิการแห่งรัฐด้วยการสนับสนุนการใช้ประโยชน์จากเครือข่ายข้อมูลและการสื่อสาร การคุ้มครองประชาชนผู้ใช้บริการเครือข่าย และปรับปรุงสภาพแวดล้อมที่เอื้อให้ประชาชนสามารถใช้ประโยชน์จากเครือข่ายข้อมูลและการสื่อสารได้อย่างเหมาะสมและปลอดภัยยิ่งขึ้น

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

๑.๑ บทนิยามคำว่า “เหตุภัยคุกคามต่อความปลอดภัยคอมพิวเตอร์ (computer security incident)” (มาตรา ๒) หมายความว่า เหตุการณ์ที่เกิดขึ้นเนื่องมาจากการโจมตีเครือข่ายข้อมูลสารสนเทศและการสื่อสารหรือระบบข้อมูลที่เกี่ยวข้องกับเครือข่ายดังกล่าว เช่น การขโมยข้อมูล หรือการติดตั้งโปรแกรมที่ข้ามขั้นตอนการป้องกันตามปกติที่ต้องดำเนินการ

๑.๒ ความรับผิดชอบของผู้ให้บริการและผู้ให้บริการข้อมูลสารสนเทศและการสื่อสาร (มาตรา ๓) ผู้ให้บริการข้อมูลสารสนเทศทุกคนมีหน้าที่คุ้มครองสิทธิและผลประโยชน์ของผู้ใช้บริการ และมีหน้าที่ให้ความช่วยเหลือในการสร้างสรรค์สังคมสารสนเทศที่เหมาะสม โดยรัฐบาล

^๗ Act No. 20069, Jan. 23, 2024.

^๘ 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>

อาจสนับสนุนองค์กรที่ประกอบด้วยผู้ให้บริการและผู้ให้บริการข้อมูลสารสนเทศและการสื่อสาร เพื่อคุ้มครองข้อมูลและปกป้องเยาวชนในเครือข่ายสารสนเทศและการสื่อสารดังกล่าว

๑.๓ การกำหนดนโยบายส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลสารสนเทศและการสื่อสาร และการคุ้มครองข้อมูลสารสนเทศ (มาตรา ๔) รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์และ ICT หรือคณะกรรมการการสื่อสารแห่งเกาหลี (Korea Communications Commission) มีหน้าที่กำหนดนโยบายเพื่อวางรากฐานรองรับสังคมข้อมูลสารสนเทศโดยผ่านการส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลสารสนเทศ บริหารจัดการและการดำเนินงานเครือข่ายดังกล่าวอย่างมีประสิทธิภาพ และคุ้มครองผู้ใช้บริการ โดยนโยบายที่รัฐมนตรีกำหนดนั้นต้องมีรายละเอียดเกี่ยวกับการพัฒนาและการเผยแพร่เทคโนโลยีที่เกี่ยวข้องกับเครือข่ายข้อมูลสารสนเทศและการสื่อสาร การกำหนดมาตรฐานของเครือข่ายข้อมูลสารสนเทศและการสื่อสาร การส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลสารสนเทศและการสื่อสาร การสนับสนุนการแบ่งปันข้อมูลผ่านเครือข่ายข้อมูลสารสนเทศและการสื่อสาร การส่งเสริมการใช้งานอินเทอร์เน็ต การคุ้มครองเยาวชนในเครือข่ายข้อมูลสารสนเทศและการสื่อสาร การพัฒนาและการเผยแพร่เทคโนโลยีที่ตรวจจับเสียง ภาพ ภาพนิ่ง หรือสิ่งอื่นใดอันเป็นเท็จที่สร้างขึ้นโดยเทคโนโลยีปัญญาประดิษฐ์หรือ AI การยกระดับความปลอดภัยและความน่าเชื่อถือของเครือข่ายข้อมูลสารสนเทศและการสื่อสาร รวมทั้งเรื่องอื่นที่จำเป็นสำหรับการส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลสารสนเทศและการสื่อสาร และการคุ้มครองข้อมูลสารสนเทศ โดยนโยบายส่งเสริมการใช้ประโยชน์จากเครือข่ายข้อมูลสารสนเทศและการสื่อสารต้องสอดคล้องกับแผนแม่บทข้อมูลสารสนเทศแห่งชาติตามมาตรา ๖ แห่ง Framework Act on National Information

๑.๔ การพัฒนาเทคโนโลยี (มาตรา ๖) รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์และ ICT อาจมอบหมายให้สถาบันวิจัยที่เกี่ยวข้องตามที่กฎหมายกำหนด ดำเนินโครงการศึกษาวิจัยและพัฒนา ความร่วมมือทางเทคนิค 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) กำหนดมาตรการการคุ้มครองศูนย์ข้อมูล (Data Centers) เพื่อให้การดำเนินงานของสิ่งอำนวยความสะดวกด้านข้อมูลสารสนเทศและการสื่อสารมีประสิทธิภาพ 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 หรือแพร่กระจายโปรแกรมในลักษณะที่เป็นการขัดขวางการทำงานของระบบข้อมูล 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^๙

วัตถุประสงค์^{๑๐}

กฎหมายว่าด้วยการคุ้มครองโครงสร้างพื้นฐานข้อมูลสารสนเทศและการสื่อสารมีวัตถุประสงค์เพื่อให้โครงสร้างพื้นฐานด้านข้อมูลสารสนเทศและการสื่อสารสามารถดำเนินงานได้อย่างมีประสิทธิภาพโดยกำหนดรูปแบบและดำเนินมาตรการต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองโครงสร้างพื้นฐานดังกล่าวรวมทั้งเตรียมความพร้อมในการตอบโต้กรณีเกิดการบุกรุกทางอิเล็กทรอนิกส์เพื่อปกป้องชีวิตของมวลมนุษยชาติและความมั่นคงของประเทศ

^๙ Act No. 20068, Jan. 23, 2024

^{๑๐} 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.

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^{๑๑}

๑.๒ มาตรการป้องกันและวิเคราะห์ช่องโหว่ของโครงสร้างพื้นฐานด้านข้อมูลสารสนเทศและการสื่อสาร (มาตรา ๕ ถึงมาตรา ๙)

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

(๒) กำหนดให้มีการวิเคราะห์และประเมินช่องโหว่ของโครงสร้างพื้นฐานอย่างสม่ำเสมอเพื่อหาวิธีการที่จะป้องกันภัยคุกคามรูปแบบใหม่ ๆ ที่อาจเกิดขึ้นในอนาคต

๑.๓ ข้อห้ามและการกระทำความผิดทางไซเบอร์ (มาตรา ๑๐ ถึงมาตรา ๑๖)

(๑) กำหนดแนวทางและมาตรการคุ้มครองโดยให้หัวหน้าหน่วยงานส่วนกลางที่เกี่ยวข้องจัดทำแนวทางปฏิบัติเพื่อคุ้มครองโครงสร้างพื้นฐานที่อยู่ภายใต้การกำกับดูแล และมีคำสั่งให้ดำเนินการมาตรการคุ้มครองเพิ่มเติมได้

^{๑๑} 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.

(๒) กำหนดข้อห้ามการบุกรุกโครงสร้างพื้นฐานที่สำคัญ เช่น การเข้าถึงระบบโดยไม่มีสิทธิ การทำลายข้อมูลหรือใช้โปรแกรมที่เป็นอันตราย หรือการระดมส่งสัญญาณโจมตีการทำงานของโครงสร้างพื้นฐาน

(๓) กำหนดหน้าที่ในการแจ้งเตือนและมาตรการเยียวยา โดยเมื่อองค์กรบริหารจัดการพบว่ามีเหตุหรืออุบัติการณ์เกี่ยวกับการโจมตีโครงสร้างพื้นฐานเกิดขึ้น 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)” แยกตามกลุ่มอุตสาหกรรมเพื่อทำหน้าที่ให้ข้อมูลเกี่ยวกับสาเหตุและแนวทางแก้ไข และการบริหารจัดการระบบวิเคราะห์และแจ้งเตือนภัยแบบทันที

๑.๕ บทลงโทษ (มาตรา ๒๘ ถึงมาตรา ๓๐)

(๑) โทษอาญา: บุคคลซึ่งบุกรุกหรือรบกวนการดำเนินงานของโครงสร้างพื้นฐานด้านข้อมูลสารสนเทศและการสื่อสารต้องระวางโทษจำคุกไม่เกิน ๑๐ ปี หรือปรับไม่เกิน ๑๐๐ ล้านบาท

(๒) โทษปรับทางปกครอง: กรณีบุคคลซึ่งไม่ปฏิบัติตามคำสั่งกักกันระบบหรือไม่วิเคราะห์ช่องโหว่ตามที่กฎหมายกำหนด ระวางโทษปรับตั้งแต่ ๕ ล้านบาท ถึง ๕๐ ล้านบาทแล้วแต่กรณี

๔. Framework Act on National Informatization^{๑๒}

วัตถุประสงค์^{๑๓}

กฎหมายว่าด้วยโครงสร้างพื้นฐานการสร้างสังคมสารสนเทศแห่งชาติมีวัตถุประสงค์เพื่อขับเคลื่อนไปสู่สังคมที่อยู่บนพื้นฐานของความรู้และข้อมูลสารสนเทศอย่างยั่งยืน ยกระดับคุณภาพชีวิตของประชาชนโดยการกำหนดทิศทางพื้นฐานและนโยบายที่จำเป็นเพื่อทำให้เป็นสังคมสารสนเทศระดับชาติ

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

๑.๑ บทนิยามคำว่า “การสร้างสังคมสารสนเทศแห่งชาติ (National Informatization)” หมายความว่า การส่งเสริมการนำเทคโนโลยีสารสนเทศมาใช้โดยหน่วยงานระดับชาติ หน่วยงานท้องถิ่น หรือสถาบันหรือองค์กรใดที่สนับสนุนการดำเนินกิจกรรมผ่านกระบวนการ

^{๑๒} Act No. 14572, Mar. 14, 2017

^{๑๓} 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.

สารสนเทศนี้ คำว่า “การคุ้มครองข้อมูลสารสนเทศ (protection of information)” หมายความว่า การจัดทำมีมาตรการการบริหารจัดการและเทคนิคที่จะป้องกันความเสียหาย การดัดแปลง หรือการรั่วไหลใด ๆ ของข้อมูลที่อาจเกิดขึ้นมาจากกระบวนการจัดเก็บ 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) เพื่อสนับสนุนการพัฒนานโยบายในการส่งเสริมข้อมูลสารสนเทศระดับชาติ และการสร้างสรรค์วัฒนธรรมด้านสารสนเทศระดับชาติ

๑.๓ การส่งเสริมการเป็นสังคมสารสนเทศแห่งชาติ (มาตรา ๑๕ ถึงมาตรา ๒๘)

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

๑.๔ การป้องกันผลกระทบเชิงลบของข้อมูลสารสนเทศแห่งชาติ (มาตรา ๒๙ ถึงมาตรา ๔๒)

รัฐมีหน้าที่จัดทำแผนระดับชาติเพื่อป้องกันปัญหาการติดอินเทอร์เน็ต โดยจัดตั้งศูนย์ให้คำปรึกษาและบำบัดผู้ติดอินเทอร์เน็ต และอาจออนุมัติ “Green Internet Certification” แก่ผู้ให้บริการซึ่งมีมาตรการป้องกันการติดอินเทอร์เน็ต รับรองการเข้าถึงและใช้งานอินเทอร์เน็ตของผู้สูงอายุและผู้ทุพพลภาพ กำหนดนโยบายเพื่อรับประกันความปลอดภัยในการเผยแพร่ข้อมูลตลอดทั้งกระบวนการ กำหนดมาตรฐานและความน่าเชื่อถือของระบบการคุ้มครองข้อมูลสารสนเทศ กำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล และกำหนดมาตรฐานทางจริยธรรมไซเบอร์ที่เหมาะสม

๑.๕ การยกระดับโครงสร้างพื้นฐานข้อมูลสารสนเทศและการสื่อสาร (มาตรา ๔๓ ถึงมาตรา ๔๗)

รัฐอาจจัดตั้งเครือข่ายความเร็วสูงเพื่อให้องค์กรที่ไม่แสวงหากำไรสามารถนำไปใช้งานได้ ในราคาประหยัด ขยายความร่วมมือด้านการให้บริการเครือข่ายดิจิทัล และสนับสนุนหน่วยงานของรัฐให้ใช้โครงสร้างพื้นฐานข้อมูลสารสนเทศและการสื่อสารที่ทันสมัย

๕. Electronic Government Act^{๑๔}

วัตถุประสงค์^{๑๕}

กฎหมายว่าด้วยรัฐบาลอิเล็กทรอนิกส์มีวัตถุประสงค์เพื่อส่งเสริมการพัฒนา รัฐบาลอิเล็กทรอนิกส์อย่างมีประสิทธิภาพ เพิ่มประสิทธิภาพ ความโปร่งใส และความเป็นประชาธิปไตย ในการบริหารราชการแผ่นดิน รวมถึงการพัฒนาคุณภาพชีวิตของประชาชนโดยกำหนดหลักการ พื้นฐาน กระบวนการ วิธีการดำเนินงาน และเรื่องอื่นที่เกี่ยวข้องกับการบริหารราชการแผ่นดิน ด้วยวิธีการทางอิเล็กทรอนิกส์

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

๑.๑ หลักการของรัฐบาลอิเล็กทรอนิกส์ (มาตรา ๔) หน่วยงานของรัฐต้อง คำนึงถึงการสร้างความเชื่อมั่นในการรักษาความปลอดภัยและความน่าเชื่อถือของระบบสารสนเทศ (information systems) และการคุ้มครองข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัว

๑.๒ แผนแม่บทรัฐบาลอิเล็กทรอนิกส์ (มาตรา ๕) หน่วยงานกลางมีหน้าที่ จัดทำแผนแม่บทรัฐบาลอิเล็กทรอนิกส์ทุกห้าปี โดยรวบรวมแผนงานของหน่วยงานต่าง ๆ เพื่อใช้เป็น กรอบในการพัฒนา การดำเนินงาน และการขับเคลื่อนรัฐบาลอิเล็กทรอนิกส์ของประเทศ

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

๑.๔ การกระทำที่ต้องห้าม (มาตรา ๓๕) กฎหมายกำหนดห้ามบุคคลกระทำการ ในลักษณะที่เป็นการปลอมแปลง ดัดแปลง ทำลาย ลบข้อมูลของหน่วยงานภาครัฐ หรือใช้ระบบ สารสนเทศเพื่อการแบ่งปันข้อมูลโดยไม่มีเหตุอันสมควร ตลอดจนเปิดเผยหรือเผยแพร่โปรแกรม ที่ทำให้สามารถดัดแปลงหรือลบข้อมูลของหน่วยงานภาครัฐได้

๑.๕ การจัดทำมาตรการรักษาความปลอดภัยสำหรับเครือข่ายข้อมูลสารสนเทศ และการสื่อสาร (มาตรา ๕๖) หน่วยงานของรัฐต้องจัดทำมาตรการเพื่อรักษาความปลอดภัยและ ความน่าเชื่อถือของเครือข่ายข้อมูลสารสนเทศและการสื่อสาร รวมถึงข้อมูลเกี่ยวกับการบริหาร ราชการ เพื่อป้องกันการปลอมแปลง การรั่วไหล หรือการทำลายเอกสารอิเล็กทรอนิกส์

๑.๖ การป้องกันและการตอบสนองต่อความล้มเหลวของระบบ (มาตรา ๕๖-๒) หัวหน้าหน่วยงานของรัฐมีหน้าที่จัดทำมาตรการป้องกันและตอบสนองต่อความล้มเหลวของระบบ เพื่อให้การทำงานและการจัดการระบบข้อมูลมีประสิทธิภาพ

^{๑๔} Act No. 14914, Oct. 24, 2017

^{๑๕} 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.

๑.๗ การกำกับดูแลระบบสารสนเทศ (มาตรา ๕๗) หัวหน้าหน่วยงานของรัฐ มีหน้าที่กำหนดให้มีการตรวจสอบและติดตามการดำเนินงานของระบบสารสนเทศเพื่อแก้ไขและ ประกันความปลอดภัยของระบบดังกล่าว

๑.๘ บทกำหนดโทษ (มาตรา ๗๖) กำหนดโทษจำคุกและโทษปรับสำหรับผู้ซึ่ง ละเมิดการรักษาความปลอดภัยทางไซเบอร์ เช่น การทำลายข้อมูลทางปกครอง ระวังโทษจำคุก ไม่เกิน ๑๐ ปี หรือกรณีที่มีการเข้าถึงข้อมูลสารสนเทศโดยมิชอบ ระวังโทษจำคุกไม่เกิน ๕ ปีหรือ ปรับไม่เกิน ๕๐ ล้านบาท เป็นต้น

b. Electronic Financial Transactions Act^{๑๖}

วัตถุประสงค์^{๑๗}

กฎหมายว่าด้วยธุรกรรมทางการเงินอิเล็กทรอนิกส์มีวัตถุประสงค์เพื่อสร้างความ เชื่อมั่นในความปลอดภัยและความน่าเชื่อถือของธุรกรรมทางการเงินอิเล็กทรอนิกส์โดยการกำหนด ความสัมพันธ์ในแง่ของกฎหมายให้มีความชัดเจน ตลอดจนอำนวยความสะดวกทางการเงินแก่ประชาชน และส่งเสริมการพัฒนาทางเศรษฐกิจของประเทศด้วยการวางรากฐานการพัฒนาอุตสาหกรรมทางการเงิน อิเล็กทรอนิกส์ได้อย่างเหมาะสม

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

๑.๑ บทนิยามคำว่า “โครงสร้างพื้นฐานทางการเงินทางอิเล็กทรอนิกส์ (Electronic Financial Infrastructure)” หมายความว่า ระบบการประมวลผลข้อมูลที่ใช้ใน ธุรกรรมทางการเงินอิเล็กทรอนิกส์และเครือข่ายข้อมูลสารสนเทศและการสื่อสาร และคำว่า “การละเมิด ทางอิเล็กทรอนิกส์ (electronic infringement)” หมายความว่า การโจมตีโครงสร้างพื้นฐาน ทางการเงินอิเล็กทรอนิกส์ด้วยวิธีการต่าง 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) สถาบันการเงินและ ผู้ประกอบธุรกิจมีหน้าที่ปฏิบัติตามมาตรฐานที่ Financial Services Commission (FSC) กำหนด ทั้งใน ด้านทรัพยากรมนุษย์ สิ่งอำนวยความสะดวก อุปกรณ์อิเล็กทรอนิกส์ และค่าใช้จ่ายในการทำธุรกรรม ทางอิเล็กทรอนิกส์ต่าง ๆ ให้มีความปลอดภัยและน่าเชื่อถือ รวมถึงต้องมีการจัดทำแผนงานด้าน เทคโนโลยีสารสนเทศเป็นประจำทุกปีและเสนอต่อ FSC

๑.๓ การแต่งตั้งเจ้าหน้าที่ด้านความปลอดภัยสารสนเทศ และการวิเคราะห์ และประเมินช่องโหว่ (มาตรา ๒๑-๒ และมาตรา ๒๑-๓) กำหนดให้สถาบันการเงินหรือผู้ประกอบ ธุรกิจแต่งตั้งเจ้าหน้าที่ด้านความปลอดภัยสารสนเทศ (chief information security officer) เพื่อรับผิดชอบการจัดการด้านความปลอดภัยแก่ธุรกิจทางการเงินอิเล็กทรอนิกส์และเทคโนโลยี สารสนเทศ ตลอดจนกำหนดให้สถาบันการเงินและผู้ประกอบธุรกิจการเงินอิเล็กทรอนิกส์มีหน้าที่

^{๑๖} Act No. 21205, Dec. 17, 2026

^{๑๗} 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.

วิเคราะห์และประเมินเหตุที่มีความเกี่ยวข้องกับโครงสร้างพื้นฐานทางการเงินอิเล็กทรอนิกส์และรายงานต่อ FSC

๑.๔ การห้ามละเมิดทางอิเล็กทรอนิกส์ การแจ้งและตอบโต้เหตุละเมิด (มาตรา ๒๑-๔ ถึงมาตรา ๒๑-๖) กฎหมายกำหนดห้ามการเข้าถึงโครงสร้างพื้นฐานทางการเงินอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต ห้ามการติดตั้งโปรแกรม เช่น ไวรัสคอมพิวเตอร์ หรือมัลแวร์ โดยมีวัตถุประสงค์เพื่อทำลายข้อมูลหรือขัดขวางการทำงานของโครงสร้างพื้นฐานดังกล่าว และในกรณีมีเหตุละเมิดอันทำให้ระบบไม่สามารถทำงานต่อไปได้ สถาบันการเงินและผู้ประกอบธุรกิจทางการเงินอิเล็กทรอนิกส์ย่อมมีหน้าที่แจ้งให้ 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^{๑๘}

วัตถุประสงค์^{๑๙}

กฎหมายว่าด้วยสำนักงานข่าวกรองแห่งสาธารณรัฐเกาหลีมีวัตถุประสงค์เพื่อกำหนดเรื่องที่เกี่ยวข้องกับการจัดระเบียบองค์กรและกำหนดขอบเขตหน้าที่ของสำนักงานข่าวกรองแห่งชาติ ตลอดจนการปฏิบัติการกิจด้านความมั่นคงแห่งชาติให้เป็นไปอย่างมีประสิทธิภาพ

สาระสำคัญที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

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

๑.๒ อำนาจในการสืบสวนสอบสวน (มาตรา ๕) กำหนดให้พนักงานของ NIS มีอำนาจในการสืบสวนสอบสวนและเข้าถึงเอกสาร การเก็บตัวอย่าง การร้องขอข้อมูลเพิ่มเติมได้

๑.๓ บทกำหนดโทษ (มาตรา ๒๑ ถึงมาตรา ๒๓) กำหนดโทษกรณีฝ่าฝืนกฎหมายประกอบด้วยโทษจำคุกและพักใช้ใบอนุญาตแล้วแต่ฐานความผิดเป็นรายกรณี

^{๑๘} Act No. 18519, Oct. 19, 2021

^{๑๙} 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.

๔. บทสรุป

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