

ปัญหากฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต¹

ร้อยตำรวจเอกภาณุพงศ์ ทองชล²

การศึกษาเรื่อง ปัญหากฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต มีวัตถุประสงค์เพื่อศึกษาความเป็นมา แนวคิด และทฤษฎีเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ศึกษากฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตของประเทศไทยและต่างประเทศ เพื่อศึกษาวิเคราะห์ปัญหากฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อศึกษาแนวทางการแก้ไขกฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ของไทยที่เหมาะสมและสามารถนำมาบังคับใช้ได้อย่างมีประสิทธิภาพ

จากการศึกษาทำให้ทราบว่าปัญหากฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต มีข้อสรุปดังนี้

ปัญหาเกี่ยวกับการส่งลิงก์ซอฟต์แวร์ที่เป็นอันตรายให้แก่ผู้เสียหาย เพื่อหลอกล่อให้ติดตั้งในโทรศัพท์มือถือ

มาตรา 10 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดไว้ว่า “ผู้ใดกระทำความผิดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

เมื่อพิจารณาถึงบทบัญญัติมาตรา 10 ข้างต้น เป็นความผิดฐานการรบกวนระบบคอมพิวเตอร์ โดยพบว่า การกระทำที่สามารถนำมาตรา 10 มาบังคับใช้ ได้แก่ การโจมตีแบบ DDoS (Distributed Denial of Service) หมายถึง การส่งคำขอเข้าระบบคอมพิวเตอร์เป็นจำนวนมากพร้อมกันจากหลายเครื่อง เพื่อทำให้ระบบไม่สามารถตอบสนองการทำงานตามปกติได้ ทำให้เว็บไซต์หรือบริการออนไลน์ล่ม ไม่สามารถ

¹ บทความนี้ เรียบเรียงจากการค้นคว้าอิสระ เรื่อง ปัญหากฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต โดยมีอาจารย์ที่ปรึกษาคือรองศาสตราจารย์ ดร. พันธุ์เทพ วิฑิตอนันท์ และคณะกรรมการสอบคือ ผู้ช่วยศาสตราจารย์ ดร. ชนกพร สุนนะเศรษฐกุล และผู้ช่วยศาสตราจารย์ ดร. ดนพร จรุงเกียรติ

² นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต (สงขลา) คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

ให้บริการได้ตามปกติ หรือการติดตั้งมัลแวร์หรือไวรัส เช่น การติดตั้งโปรแกรมที่เป็นอันตราย เช่น ไวรัสหรือมัลแวร์ในระบบคอมพิวเตอร์ของผู้อื่น ทำให้ระบบทำงานผิดปกติหรือหยุดการทำงานโดยสมบูรณ์ หรือการเจาะระบบและทำลายข้อมูล โดยการเจาะเข้าสู่ระบบคอมพิวเตอร์และทำการลบหรือแก้ไขข้อมูลที่สำคัญทำให้ระบบไม่สามารถทำงานได้ตามปกติ เช่น การลบไฟล์ระบบหรือการแก้ไขฐานข้อมูล หรือการขัดขวางการทำงานของเครือข่าย เช่น การทำให้การเชื่อมต่อเครือข่ายถูกขัดขวาง เช่น การปิดกั้นพอร์ตหรือการสร้างการเชื่อมต่อที่ผิดปกติ ทำให้การเชื่อมต่อระหว่างอุปกรณ์ในเครือข่ายทำงานไม่ได้ตามปกติ เป็นต้น³ เห็นได้ว่า การติดตั้งโปรแกรมที่เป็นอันตราย เช่น ไวรัสหรือมัลแวร์ในระบบคอมพิวเตอร์นั้น เป็นความผิดตามมาตรา ๓ ส่วนการกระทำของมิชฌาซีฟในการส่งข้อความหลอกลวงผ่านช่องทางสื่อสารโดยมีการแนบลิงก์ที่จะนำผู้เสียหายไปสู่การติดตั้งแอปพลิเคชันที่เป็นอันตรายนั้น เป็นการกระทำความผิดในลักษณะของการแจกจ่ายซอฟต์แวร์ที่เป็นอันตราย ซึ่งมีได้มีบทบัญญัติใด ได้กล่าวถึง ทั้งที่ การแจกจ่ายซอฟต์แวร์ที่เป็นอันตรายเป็นจุดเริ่มต้นในการนำไปสู่การกระทำความผิดอื่น ๆ

ผู้ศึกษาจึงทำการศึกษากฎหมายต่างประเทศ ประมวลกฎหมายอาญา (Crimes Act 1900 (NSW)) ของมลรัฐนิวเซาท์เวลส์ เครือรัฐออสเตรเลีย บัญญัติไว้ว่า “ผู้ใดครอบครองหรือควบคุมข้อมูลโดยมีเจตนาที่จะกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างร้ายแรง หรือมีเจตนาที่จะอำนวยความสะดวกในการกระทำความผิดดังกล่าว (ไม่ว่าจะเป็นตนเองหรือบุคคลอื่น) ถือว่ามีความผิด มีโทษจำคุกสูงสุดสามปี”⁴

ขณะเดียวกัน ประมวลกฎหมายอาญาแคลิฟอร์เนีย (California Penal Code) บัญญัติไว้ว่า “บุคคลใดที่มีเจตนาและโดยมิชอบจัดหา ใช้ มีในครอบครอง ผลิต ออกแบบ พัฒนา ทดสอบ หรือแจกจ่ายโปรแกรมคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ที่มีจุดประสงค์เพื่ออำนวยความสะดวกในการเข้าถึงโดยไม่ได้รับอนุญาตหรือเพื่อก่อให้เกิดความเสียหาย”⁵ และบทลงโทษผู้กระทำความผิดอาจถูกลงโทษจำคุกในเรือนจำของรัฐไม่เกินสามปี หรือจำคุกในเรือนจำของเคาน์ตีไม่เกินหนึ่งปี หรือปรับเงินไม่เกิน 10,000 ดอลลาร์ หรือทั้งจำทั้งปรับ⁶

ขณะที่ กฎหมายของราชอาณาจักรเนเธอร์แลนด์พบว่า การส่งลิงก์ซอฟต์แวร์ที่เป็นอันตรายให้แก่ผู้เสียหาย เพื่อหลอกล่อให้ติดตั้งในโทรศัพท์มือถือถือขึ้น เป็นความผิดตามกฎหมายอาญานเนเธอร์แลนด์ (Dutch Criminal Code) มาตรา 139d ที่กำหนดให้บุคคลใดที่มีเจตนาในการกระทำความผิด เตรียมการ หรืออำนวยความสะดวกในการกระทำความผิดร้ายแรง ผลิต จัดหา ขาย นำเข้า เผยแพร่ หรือทำให้มีโปรแกรมคอมพิวเตอร์

³ หนังสือพิมพ์คมชัดลึก, ลบด่วน 10 แอปพลิเคชัน อันตราย ดูดเงินหายเกลี้ยงบัญชี, [Online], available URL: <https://www.komchadluek.net/kom-lifestyle/it/555393.2567>(มีนาคม, 20).

⁴ Crimes Act 1900 (NSW), Section 308 F.

⁵ California Penal Code, Section 502(c)(6).

⁶ California Penal Code, Section 502(d)(1).

หรืออุปกรณ์อื่นใดที่ถูกออกแบบหรือปรับแต่งเพื่อใช้ในการกระทำความผิดร้ายแรงต้องรับโทษจำคุกไม่เกินสี่ปี หรือปรับเป็นเงินในระดับห้า⁷ ซึ่งหมายถึงค่าปรับสูงสุด 900,000 ยูโร ”⁸

จากการศึกษากฎหมายไทยและกฎหมายต่างประเทศซึ่งที่กล่าวไปข้างต้นพบว่า มาตรา 10 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยนั้น บัญญัติให้การกระทำด้วยประการใดโดยมิชอบ ที่ทำให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติให้เป็นความผิดตามกฎหมาย ซึ่งเห็นได้ว่าเป็นกรณีที่ผู้กระทำความผิดได้กระทำความผิดต่อระบบคอมพิวเตอร์ของผู้เสียหายโดยตรง แต่บทบัญญัติดังกล่าวมิได้ครอบคลุมถึงการส่งลิงก์ซอฟต์แวร์ที่เป็นอันตรายแก่ผู้เสียหาย เพื่อให้ผู้เสียหายทำการติดตั้งซอฟต์แวร์ที่เป็นอันตรายดังกล่าวด้วยตนเองแต่ประการใด กรณีจึงแตกต่างจากกฎหมายของสหรัฐอเมริกาและราชอาณาจักรเนเธอร์แลนด์ ที่มีการบัญญัติให้บุคคลที่ทำการเผยแพร่หรือส่งลิงก์ซอฟต์แวร์ที่เป็นอันตรายให้แก่บุคคลอื่นเป็นความผิด ขณะที่เครื่องรัฐออสเตรีย แม้จะมีได้กำหนดให้การส่งลิงก์ซอฟต์แวร์ที่เป็นอันตรายจะเป็นความผิดโดยตรง แต่หากพบว่าบุคคลดังกล่าวครอบครองข้อมูลที่มีเจตนากระทำความผิดก็สามารถนำบทบัญญัตินี้มาใช้บังคับได้อย่างครอบคลุมและสอดคล้องกับกฎหมายของนานาประเทศ

ด้วยเหตุนี้ ผู้ศึกษาจึงเห็นว่า ควรมีการกำหนดให้การส่งลิงก์ซอฟต์แวร์ที่เป็นอันตรายแก่ผู้เสียหาย เพื่อหลอกลวงให้ผู้ได้รับลิงก์ที่ส่งมานั้นทำการดาวน์โหลดไฟล์และติดตั้งไว้ในโทรศัพท์มือถือเป็นความผิด ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้กฎหมายของประเทศไทยสามารถนำมาใช้บังคับได้อย่างครอบคลุมและสอดคล้องกับกฎหมายของนานาประเทศ

ปัญหาเกี่ยวกับการเข้าควบคุมการใช้โทรศัพท์ของผู้เสียหายจากระยะไกล

⁷ Dutch Criminal Code, Section 139d.

⁸ ในระบบกฎหมายของเนเธอร์แลนด์ การปรับเป็นเงินในระดับต่างๆ จะถูกกำหนดตามหมวดหมู่ของการลงโทษปรับที่ระบุไว้ใน Dutch Criminal Code (Wetboek van Strafrecht) มาตรา 23 โดยมีการปรับตามระดับต่างๆ ดังนี้

ระดับที่หนึ่ง (Category 1) สูงสุด 450 ยูโร

ระดับที่สอง (Category 2) สูงสุด 4,500 ยูโร

ระดับที่สาม (Category 3) สูงสุด 45,000 ยูโร

ระดับที่สี่ (Category 4) สูงสุด 225,000 ยูโร

ระดับที่ห้า (Category 5) สูงสุด 900,000 ยูโร

ระดับที่หก (Category 6) ไม่มีการกำหนดสูงสุด ขึ้นอยู่กับความรุนแรงของคดีและการตัดสินของศาล

ดังนั้น การปรับเป็นเงินในระดับที่ห้า (Category 5) มีมูลค่าสูงสุดถึง 900,000 ยูโร ซึ่งเป็นการกำหนดบทลงโทษที่รุนแรงสำหรับการกระทำความผิดร้ายแรง เช่น การผลิตหรือแจกจ่ายซอฟต์แวร์ที่เป็นอันตรายที่มีเจตนาในการกระทำความผิดตามมาตรา 139d ของ Dutch Criminal Code

มาตรา 7 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้บัญญัติไว้ว่า “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนี้มิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ”

การกระทำความผิดอาญานั้นเป็นการกระทำที่ต่อเนื่อง ซึ่งแม้เป็นการกระทำครั้งเดียว แต่ผู้กระทำสามารถกระทำความผิดในหลายฐานความผิดได้โดยต้องพิจารณาในแต่ละกรณี เช่น การบุกรุกเข้าไปในบ้านพักอาศัยของผู้อื่น และมีการนำทรัพย์สินของผู้อื่นออกมาด้วย โดยเจ้าของทรัพย์สินมิได้ยินยอม นอกจากผู้กระทำมีความผิดฐานบุกรุกแล้ว ยังมีความผิดฐานลักทรัพย์ในเคสสถานอีกด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ก็เช่นเดียวกัน มักเป็นการกระทำที่ต่อเนื่องกัน โดยลักษณะของการกระทำความผิดสามารถแยกส่วนออกจากกันได้ และเพื่อให้เป็นไปตามหลักของกฎหมายอาญา ซึ่งห้ามนำกฎหมายที่มีลักษณะใกล้เคียงอย่างยิ่งมาบังคับใช้ การกระทำความผิดในแต่ละส่วนจึงควรมีการบัญญัติให้เป็นความผิดแยกต่างหากจากกัน

มาตรา 7 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กล่าวถึงเฉพาะการเข้าถึงระบบคอมพิวเตอร์เท่านั้น แต่ไม่ครอบคลุมไปถึงการเข้าควบคุมระบบคอมพิวเตอร์หรือควบคุมการใช้โทรศัพท์มือถือของผู้เสียหาย หรือทำให้ผู้เสียหายไม่สามารถควบคุมระบบคอมพิวเตอร์ของตนเองได้อีกต่อไป ดังนั้น จึงไม่มีความชัดเจนว่าจะสามารถนำบทบัญญัตินี้มาใช้กับกลุ่มมิจนาซีฟที่เข้าถึงระบบคอมพิวเตอร์โดยมีวัตถุประสงค์เพื่อเข้าควบคุมการใช้โทรศัพท์ของผู้เสียหาย เพื่อลักลอบโอนเงินออกจากบัญชีของผู้เสียหายผ่านทางแอปพลิเคชันของธนาคาร ทั้งที่การกระทำดังกล่าวสร้างความเสียหายแก่ผู้เสียหายเป็นอย่างมาก นอกจากนี้อัตราโทษที่กำหนดไว้ในมาตรานี้ ยังไม่ได้สัดส่วนกับความเสียหายที่เกิดขึ้น ทำให้ไม่มีประสิทธิภาพเพียงพอที่จะยับยั้งการกระทำความผิดในลักษณะดังกล่าว เพื่อคุ้มครองประชาชนจากอาชญากรรมเทคโนโลยีที่เกิดขึ้นได้

ทั้งนี้ บทบัญญัติ มาตรา 7 กล่าวถึงเฉพาะความผิดเกี่ยวกับการเข้าถึงข้อมูลระบบคอมพิวเตอร์ของบุคคลอื่นเท่านั้น แต่มิได้กล่าวถึงผลต่อเนื่องของการเข้าถึงนั้น กล่าวคือ เมื่อมิจนาซีฟสามารถหลอกลวงผู้เป็นเจ้าของระบบคอมพิวเตอร์หรือโทรศัพท์มือถือทำการติดตั้งซอฟต์แวร์ที่เป็นอันตราย โดยเมื่อทำการติดตั้งโปรแกรมแล้ว จะส่งผลทำให้มิจนาซีฟสามารถเข้าถึงข้อมูลต่าง ๆ ที่จัดเก็บไว้ในโทรศัพท์มือถือได้ นอกจากนั้น การทำงานของซอฟต์แวร์ที่เป็นอันตราย ยังมีผลทำให้ผู้เป็นเจ้าของโทรศัพท์มือถือสูญเสียการควบคุมโทรศัพท์มือถือของตนเอง โดยมีจนาซีฟสามารถเข้าควบคุมและใช้งานแทนตัวผู้เสียหายได้ แล้วกระทำการหลายประการที่ก่อให้เกิดความเสียหายแก่ผู้ใช้งาน เช่น การทำธุรกรรมทางการเงินในแอปพลิเคชันที่ติดตั้งอยู่ในโทรศัพท์มือถือ โดยการโอนเงินออกจากบัญชีของเจ้าของโทรศัพท์ด้วยระบบโมบายแบงก์กิ้ง เป็นต้น

เมื่อทำการศึกษากฎหมายต่างประเทศพบว่า กฎหมายของมลรัฐนิวเซาท์เวลส์ เครือรัฐออสเตรเลีย พบว่ากฎหมายอาญา (Crimes Act 1900 (NSW)) ได้บัญญัติเกี่ยวกับการทำให้การสื่อสารทางอิเล็กทรอนิกส์เสียหายโดยไม่ได้รับอนุญาต โดยมีสาระสำคัญคือ “บุคคลใดที่ทำให้ความเชื่อถือ ความปลอดภัย หรือการ

ทำงานของข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์หรือของเครือข่ายคอมพิวเตอร์หรือบริการการสื่อสารอิเล็กทรอนิกส์ใดๆ เสียหายโดยไม่ได้รับอนุญาตจะมีความผิดทางอาญา ต้องระวางโทษจำคุก 2 ปี⁹ ทั้งนี้บทบัญญัติมาตรานี้ สามารถนำมาใช้กับกรณีมิฉะนั้นเข้าควบคุมการใช้โทรศัพท์มือถือของผู้เสียหายจากระยะไกล ซึ่งเป็นการทำให้การสื่อสารทางอิเล็กทรอนิกส์เกิดความเสียหายโดยไม่ได้รับอนุญาตจากบุคคลที่เป็นเจ้าของระบบคอมพิวเตอร์

สำหรับการศึกษากฎหมายของมลรัฐแคลิฟอร์เนีย สหรัฐอเมริกาพบว่า การเข้าควบคุมการใช้โทรศัพท์ของผู้เสียหายจากระยะไกลโดยไม่ได้รับอนุญาต ถือเป็นการกระทำผิดกฎหมายตามประมวลกฎหมายอาญาแคลิฟอร์เนีย (California Penal Code) ความว่า "บุคคลใดที่มีเจตนาและโดย มีชอบเข้าถึงคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์โดยไม่มีสิทธิ์ จะมีความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต"¹⁰ สำหรับบทลงโทษกำหนดไว้ใน California Penal Code ต้องระวางโทษจำคุกในเรือนจำของรัฐไม่เกินสามปี หรือ จำคุกในเรือนจำของเคาน์ตีไม่เกินหนึ่งปี หรือปรับเงินไม่เกิน 10,000 ดอลลาร์ หรือทั้งจำทั้งปรับ และหากการกระทำผิดทำให้เกิดความเสียหายที่มีมูลค่ามากกว่า 10,000 ดอลลาร์ ผู้กระทำความผิดต้องระวางโทษเพิ่มขึ้นโดยจำคุกในเรือนจำของรัฐไม่เกินสี่ปี หรือปรับเงินไม่เกิน 25,000 ดอลลาร์ หรือทั้งจำทั้งปรับ¹¹

เมื่อทำการศึกษากฎหมายของราชอาณาจักรเนเธอร์แลนด์พบว่า การเข้าควบคุมการใช้โทรศัพท์ของผู้เสียหายจากระยะไกลนั้น กฎหมายอาญาเนเธอร์แลนด์ (Dutch Criminal Code) บัญญัติไว้ความว่า "บุคคลใดที่จงใจและโดยมีชอบเข้าถึงระบบคอมพิวเตอร์หรือส่วนหนึ่งส่วนใดของระบบคอมพิวเตอร์ ซึ่งมีมาตรการป้องกันการเข้าถึงโดยเฉพาะ จะมีความผิดฐานบุกรุกทางคอมพิวเตอร์ และต้องรับโทษจำคุกไม่เกินหนึ่งปี หรือปรับเป็นเงินในระดับที่สี่"¹² ซึ่ง Dutch Criminal Code (Wetboek van Strafrecht) มาตรา 23 ค่าปรับระดับสี่ หมายถึง ค่าปรับที่มีอัตราปรับขั้นสูง 225,000 ยูโร

เมื่อทำการศึกษาเปรียบเทียบกฎหมายไทยและกฎหมายต่างประเทศดังที่กล่าวไปข้างต้น เห็นได้ว่าทุกประเทศมีบทบัญญัติของกฎหมายที่ใกล้เคียงกันซึ่งกำหนดให้การเข้าถึงระบบคอมพิวเตอร์ของบุคคลอื่นที่มีมาตรการป้องกันเป็นการกระทำที่มีชอบด้วยกฎหมายเป็นความผิด และมีอัตราโทษใกล้เคียงกันคือ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปี ถึงสามปี แต่มีข้อพิจารณาคือ กฎหมายของสหรัฐอเมริกานั้น ได้คำนึงถึงความเสียหายที่เกิดขึ้นจากการเข้าถึงระบบคอมพิวเตอร์นั้นด้วย หากการเข้าถึงระบบคอมพิวเตอร์นั้นได้ก่อให้เกิดความเสียหายแก่เจ้าของระบบคอมพิวเตอร์มูลค่าตั้งแต่ 10,000 ดอลลาร์สหรัฐขึ้นไปผู้กระทำความผิดต้องระวางโทษ

⁹ Crimes Act 1900 (NSW), Section 308I .

¹⁰ Crimes Act 1900 (NSW), Section 502(c)(1).

¹¹ California Penal Code, Section 502(d).

¹² Dutch Criminal Code, Section 138ab.

หนักขึ้น ซึ่งมีข้อดีคือ เป็นการป้องปรามทำให้คนเกิดความเกรงกลัวต่อโทษที่หนักขึ้น ทำให้บรรลुวัตถุประสงค์ของการลงโทษทางอาญาคือการยับยั้งการกระทำความผิด

ผู้ศึกษาจึงเห็นว่า เมื่อมีการเข้าสู่ระบบคอมพิวเตอร์โดยมิชอบแล้ว หากบุคคลนั้นได้เข้าควบคุมระบบคอมพิวเตอร์แทนผู้เสียหาย และได้ไปซึ่งทรัพย์สินของผู้เสียหายก็ควรมีการกำหนดให้ผู้นั้นต้องระวางโทษที่หนักขึ้น

ปัญหาเกี่ยวกับการเปลี่ยนรหัสความปลอดภัยของแอปพลิเคชันต่าง ๆ ในโทรศัพท์มือถือของผู้เสียหาย

มาตรา 9 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดไว้ว่า “ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ” การบังคับใช้มาตรานี้มุ่งเน้นการปกป้องข้อมูลคอมพิวเตอร์ของผู้ใช้งานจากการถูกแก้ไข เปลี่ยนแปลง หรือทำลายโดยมิชอบ ซึ่งเป็นการรักษาความมั่นคงปลอดภัยในโลกดิจิทัล

ขณะเดียวกัน เมื่อนำมาวิเคราะห์ปัญหาเกี่ยวกับการควบคุมโทรศัพท์มือถือของบุคคลอื่นจากระยะไกลแล้ว พบว่า เมื่อมีจาชิปสามารถควบคุมการใช้งานโทรศัพท์มือถือของผู้เสียหายได้แล้ว กระบวนการต่อไปที่มิจาชิปมักดำเนินการคือ การเปลี่ยนรหัสความปลอดภัยของแอปพลิเคชันต่าง ๆ ในโทรศัพท์มือถือของผู้เสียหาย ถึงแม้ว่าการเปลี่ยนรหัสความปลอดภัยดังกล่าวนี้ ต้องมีการขอไค้ OTP แต่หน่วยงานส่งไค้ด ดังกล่าวมาให้ตามหมายเลขโทรศัพท์ที่ทำการติดตั้งแอปพลิเคชันนั้น ซึ่งมิจาชิปสามารถมองเห็นหน้าจอโทรศัพท์มือถือได้เช่นเดียวกับผู้ใช้งานโทรศัพท์มือถือ รวมถึงเป็นผู้ควบคุมการใช้งาน ดังนั้น การเปลี่ยนรหัสความปลอดภัยจึงสามารถดำเนินการได้โดยง่าย แล้วสร้างความเสียหายให้แก่ผู้เสียหายจากการทำธุรกรรมทางการเงินผ่านแอปพลิเคชันต่าง ๆ

ทั้งนี้องค์ประกอบของความผิดที่สำคัญของมาตรา 9 คือ “ข้อมูลคอมพิวเตอร์” แต่รหัส OTP ไม่มีความชัดเจนว่าถือเป็น “ข้อมูลคอมพิวเตอร์” เพราะข้อมูลคอมพิวเตอร์ตามมาตรา 9 นั้น หมายถึง ข้อมูลข้อความ คำสั่ง ชุดคำสั่ง หรืออื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ แต่รหัส OTP เป็นข้อมูลที่ถูกส่งมาจากหน่วยงานภายนอก มิได้อยู่ในระบบคอมพิวเตอร์แต่ประการใด นอกจากนี้ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งมีผลบังคับใช้มาตั้งแต่ พ.ศ. 2544 มีเจตนารมณ์เพื่อรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมือนกับการเป็นหนังสือ หรือหลักฐานเป็นหนังสือและรับรองวิธีการส่งและรับข้อมูลให้เป็นการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อส่งเสริมการทำเพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือและมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม ซึ่งเจตนารมณ์ของกฎหมายดังกล่าวมีความแตกต่างจากการบัญญัติกฎหมายว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ ดังนั้น จึงไม่เหมาะสมหากการบัญญัติเกี่ยวกับความผิดเกี่ยวกับคอมพิวเตอร์ ต้องนำพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาร่วมพิจารณาด้วย

เมื่อทำการศึกษากฎหมายของต่างประเทศพบว่า การเปลี่ยนรหัสความปลอดภัยของแอปพลิเคชันต่าง ๆ ในโทรศัพท์มือถือของผู้เสียหายโดยไม่ได้รับอนุญาต สามารถถูกดำเนินคดีภายใต้ Crimes Act 1900 (NSW) มลรัฐนิวเซาท์เวลส์ โดยการแก้ไขข้อมูลโดยไม่ได้รับอนุญาตโดยมีเจตนาให้เกิดความเสียหาย หรือการรบกวนการทำงานของคอมพิวเตอร์ จะมีความผิดและต้องรับโทษจำคุกไม่เกินสิบปี¹³ ทั้งนี้ มาตราดังกล่าวมุ่งเน้นการกระทำการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต โดยมีเจตนาให้เกิดความเสียหายหรือการรบกวนการทำงานของระบบคอมพิวเตอร์ โดยผู้กระทำความผิดมีบทลงโทษที่รุนแรง เนื่องจากมีเจตนาทำให้เกิดความเสียหายต่อบุคคลที่เป็นเจ้าของระบบคอมพิวเตอร์โดยตรง

สำหรับกฎหมายของสหรัฐอเมริกาพบว่า การกระทำที่เกี่ยวกับการเปลี่ยนแปลงหรือแก้ไขรหัสความปลอดภัยโดยไม่ได้รับอนุญาต สามารถพิจารณาว่า เป็นการกระทำที่ผิดกฎหมายภายใต้ California Penal Code ความว่า “บุคคลใดมีเจตนาและโดยมิชอบ ขโมย นำไปใช้ หรือดัดแปลงข้อมูลที่อยู่ในคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์โดยไม่มีสิทธิ”¹⁴ โดยอัตราโทษคือการจำคุกในเรือนจำของรัฐไม่เกินสามปี หรือจำคุกในเรือนจำของเคาน์ตีไม่เกินหนึ่งปี หรือปรับเงินไม่เกิน 10,000 ดอลลาร์ หรือทั้งจำทั้งปรับ

เมื่อทำการศึกษากฎหมายของราชอาณาจักรเนเธอร์แลนด์พบว่า การเปลี่ยนรหัสความปลอดภัยของแอปพลิเคชันต่าง ๆ ในโทรศัพท์มือถือ เป็นความผิดตามกฎหมายอาญาเนเธอร์แลนด์ (Dutch Criminal Code) ความว่า “บุคคลใดที่จงใจและโดยมิชอบทำลาย ทำให้เสียหาย ทำให้ไม่สามารถใช้งานได้ หรือแก้ไขเปลี่ยนแปลงข้อมูลที่ถูกเก็บรักษา ประมวลผล หรือส่งผ่านด้วยระบบคอมพิวเตอร์ หรือทำให้ข้อมูลดังกล่าวถูกลบ ทำให้ไม่สามารถใช้งานได้ หรือไม่สามารถเข้าถึงได้ จะมีความผิดฐานก่อวินาศกรรมข้อมูล และต้องรับโทษจำคุกไม่เกินสองปี หรือปรับเป็นเงินในระดับที่สี่”¹⁵ ซึ่ง Dutch Criminal Code (Wetboek van Strafrecht) กำหนดอัตราค่าปรับขั้นสูงของอัตราโทษปรับระดับสี่ ไว้ในหมายถึง ค่าปรับสูงสุดไม่เกิน 225,000 ยูโร¹⁶

จากการศึกษาบทกฎหมายไทยและกฎหมายต่างประเทศข้างต้น เห็นได้ว่า กฎหมายไทยมีความเหมือนกับ Crime Act 1900 (NSW) ในแง่ของเจตนาที่มุ่งปกป้องข้อมูลคอมพิวเตอร์จากการทำลายหรือแก้ไขโดยไม่มิสิทธิ แต่มีความแตกต่างในแง่ที่กฎหมายของเครือรัฐออสเตรเลีย ระบุรายละเอียดเพิ่มเติมเกี่ยวกับการกระทำที่เกี่ยวข้องกับระบบคอมพิวเตอร์เอาไว้โดยละเอียดมากกว่า เช่นเดียวกับการเปรียบเทียบกับ California Penal Code มาตรา 502(C)(2) ที่มีการกำหนดโทษสำหรับการเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาตและทำให้ข้อมูลดังกล่าวเกิดความเสียหายเช่นเดียวกัน แต่กฎหมายของแคลิฟอร์เนียอาจมี

¹³ Crimes Act 1900 (NSW) Crimes Act 1900 (NSW) Section 308C.

¹⁴ California Penal Code , Section 502(c)(2).

¹⁵ Dutch Criminal Code (Wetboek van Strafrecht), Section 350a.

¹⁶ Dutch Criminal Code (Wetboek van Strafrecht), Section 23.

รายละเอียดเพิ่มเติมเกี่ยวกับประเภทของข้อมูลและระบบที่ครอบคลุมมากกว่า ขณะที่กฎหมายอาญาของราชอาณาจักรเนเธอร์แลนด์ มีความเหมือนกันในแง่ของเจตนารมณ์ของกฎหมายที่ต้องการปกป้องข้อมูลคอมพิวเตอร์จากการถูกทำลายหรือแก้ไขโดยไม่ได้รับอนุญาต และมีความแตกต่างกันในแง่ที่กฎหมายของเนเธอร์แลนด์มีการระบุรายละเอียดเพิ่มเติมเกี่ยวกับประเภทของข้อมูลและระบบที่คุ้มครอง รวมถึงบทลงโทษซึ่งอาจแตกต่างกันไปตามความร้ายแรงของการกระทำความผิด

ผู้ศึกษาจึงเห็นว่า ควรมีการแก้ไขบทบัญญัติมาตรา 9 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้มีบทบัญญัติที่ชัดเจนยิ่งขึ้น เช่น ควรกำหนดให้การเปลี่ยนรหัสของมาตรการรักษาความปลอดภัยของระบบคอมพิวเตอร์ เป็นความผิดประการหนึ่งในมาตรา 9 ดังกล่าวนี้นอกจากจะทำให้การบัญญัติกฎหมายมีความชัดเจนแล้ว ยังอาจส่งผลทำให้การบังคับใช้กฎหมายมีประสิทธิภาพมากกว่าที่เป็นอยู่ในปัจจุบัน

การศึกษาเรื่อง การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ผู้ศึกษามีข้อเสนอแนะดังต่อไปนี้

1. ปัญหาเกี่ยวกับการส่งลิงก์ซอฟต์แวร์ที่เป็นอันตรายให้แก่ผู้เสียหาย เพื่อหลอกให้ติดตั้งในโทรศัพท์มือถือ

ผู้ศึกษาขอเสนอให้มีการเพิ่มเติมวรรคสองของ มาตรา 10 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยใช้ข้อความต่อไปนี้

มาตรา 10 “ผู้ใดกระทำความผิดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ผู้ใดเจตนาส่งซอฟต์แวร์ที่เป็นอันตรายแก่ผู้อื่น โดยมีวัตถุประสงค์ให้ผู้นั้นติดตั้งซอฟต์แวร์ที่เป็นอันตรายนั้นในระบบคอมพิวเตอร์ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

ทั้งนี้ เนื่องจากในปัจจุบันยังไม่มีบทบัญญัติใดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บัญญัติให้การส่งซอฟต์แวร์ที่เป็นอันตรายแก่ผู้อื่นให้เป็นความผิด ทั้งที่การกระทำความผิดดังกล่าวเป็นจุดเริ่มต้นของการกระทำความผิดอื่น ซึ่งรวมถึง การทำให้ระบบคอมพิวเตอร์ของผู้อื่นได้รับความเสียหาย หลังจากที่เหยื่อหลงเชื่อกลลวงของมิจฉาชีพแล้วทำการติดตั้งซอฟต์แวร์ดังกล่าว หากกฎหมายของประเทศไทยบัญญัติความผิดดังกล่าวไว้ นอกจากสามารถนำมาใช้บังคับใช้คุ้มครองประชาชนตั้งแต่ต้นเหตุแห่งปัญหาของการเกิดอาชญากรรมทางเทคโนโลยีแล้ว ยังทำให้กฎหมายไทยมีบทบัญญัติที่สอดคล้องกับกฎหมายของนานาประเทศอีกด้วย

2. ปัญหาเกี่ยวกับการเข้าควบคุมการใช้โทรศัพท์ของผู้เสียหายจากระยะไกล

ผู้ศึกษาขอเสนอให้มีการแก้ไขเพิ่มเติมวรรคสองของมาตรา 7 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยใช้ข้อความดังต่อไปนี้

มาตรา 7 “ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนี้มิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

การกระทำตามวรรคแรก หากมีผลเป็นการควบคุมระบบคอมพิวเตอร์แทนเจ้าของระบบคอมพิวเตอร์หรือแทนผู้มีอำนาจเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยชอบด้วยกฎหมาย ผู้นั้น ต้องระวางโทษจำคุกไม่เกินสี่ปี หรือปรับไม่เกินแปดหมื่นบาท หรือทั้งจำทั้งปรับ”

ทั้งนี้ เนื่องจากตามมาตรา 7 แห่ง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีบทบัญญัติเกี่ยวกับการกระทำความผิดเฉพาะในส่วนของการเข้าถึงเท่านั้น แต่ไม่รวมไปถึงการควบคุมการใช้งานแทนเจ้าของระบบคอมพิวเตอร์ การเพิ่มเติมกฎหมายดังกล่าวเพื่อให้ผู้กระทำความผิดเกี่ยวกับการเข้าสู่ระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบแล้ว หากบุคคลนั้นได้เข้าควบคุมระบบคอมพิวเตอร์แทนผู้เสียหาย และได้ไปซึ่งทรัพย์สินของผู้เสียหายได้รับโทษที่หนักขึ้น เพื่อให้บรรลุวัตถุประสงค์ของการลงโทษทางอาญาคือการป้องกันและยับยั้งการกระทำความผิด โดยนำอัตราโทษของกฎหมายสหรัฐอเมริกาที่บัญญัติให้ผู้กระทำความผิดต้องระวางโทษเพิ่มขึ้นสองเท่ามาใช้เป็นแนวทางในการบัญญัติโทษดังกล่าว

3. ปัญหาเกี่ยวกับการเปลี่ยนรหัสความปลอดภัยของแอปพลิเคชันต่าง ๆ ในโทรศัพท์มือถือของผู้เสียหาย

ผู้ศึกษาขอเสนอให้มีการแก้ไขเพิ่มเติม มาตรา 9 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยใช้ข้อความต่อไปนี้แทน

มาตรา 9 “ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นรวมถึงรหัสความปลอดภัยของระบบคอมพิวเตอร์โดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ทั้งนี้ เนื่องจากมาตรา 9 วรรคแรกนั้น ข้อมูลคอมพิวเตอร์ หมายถึงข้อมูลที่อยู่ในระบบคอมพิวเตอร์เท่านั้น ไม่รวมถึงรหัสความปลอดภัยของระบบคอมพิวเตอร์ที่ส่งมาจากหน่วยงานอื่น เพื่อให้บทบัญญัติดังกล่าวมีความชัดเจนยิ่งขึ้น โดยกำหนดให้การเปลี่ยนรหัสของมาตรการรักษาความปลอดภัยของระบบคอมพิวเตอร์ เป็นความผิดประการหนึ่งในมาตรา 9 นี้ นอกจากจะทำให้การบัญญัติกฎหมายที่มีโทษทางอาญามีความชัดเจนยิ่งขึ้นแล้ว ยังอาจส่งผลทำให้การบังคับใช้กฎหมายมีประสิทธิภาพมากกว่าที่เป็นอยู่ในปัจจุบัน

เอกสารอ้างอิง

ภาษาไทย

สรณันท์ จิระสุรัตน์ และคณะ. **Cyber Threats 2011** โดย ThaiCERT. กรุงเทพฯ : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 2554.

สำนักงานเลขาธิการวุฒิสภา. **พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พร้อมทั้งสรุปสาระสำคัญ ประวัติ ความเป็นมา กระบวนการ และขั้นตอนในการตราพระราชบัญญัตินี้** กล่าวของสภานิติบัญญัติแห่งชาติ. กรุงเทพฯ : สำนักงานเลขาธิการวุฒิสภา, 2549.

หยุด แสงอุทัย. **ความรู้เบื้องต้นเกี่ยวกับกฎหมายทั่วไป**. พิมพ์ครั้งที่ 21. กรุงเทพมหานคร : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2562.

หนังสือพิมพ์คมชัดลึก, **ลบด่วน 10 แอปพลิเคชัน อันตราย ดูดเงินหายเกลี้ยงบัญชี**, [Online], available URL: <https://www.komchadluek.net/kom-lifestyle/it/555393.2567>(มีนาคม, 20).

ภาษาต่างประเทศ

GeeksforGeeks. **Differed Between Conventional Crime and Cybercrime.**

<https://www.geeksforgeeks.org/difference-between-conventional-crime-and-cybercrime/2024> (May, 16).

Herbert L. Packer. **The Limits of the Criminal Sanction**. California : Stanford University Press, 1968.

James T. Graves. "Perception Versus Punishment in Cybercrime." **Journal of Criminal Law and Criminology** 109, 2 (2019), : 32.