วารสารราชภัฏ
Rajapark Journal (ISSN: 1905-2243)
ปีที่ 15 ฉบับที่ 39 มีนาคม – เมษายน 2564 – TCI กลุ่มที่ 2 มนุษยศาสตร์และสังคมศาสตร์ ปี 2563–2567

การปรับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม พ.ศ. 2560 กับการหลอกลวงเกี่ยวกับความสัมพันธ์เชิงความรักที่กระทำทางระบบคอมพิวเตอร์

The Application of Computer–related Crime Act (No.2) B.E. 2560 (2017) to the Online Romance Scam

[1]คณาธิป ทองรวีวงศ์ (Kanathip Thograweewong)
[2]ชลธิชา สมสอาด (Chonthicha Somsaard)
มหาวิทยาลัยเกษมบัณฑิต (Kasem Bendit University)
Email: [1]kanathip.tho@kbu.ac.th, [2]chonthicha.som@kbu.ac.th

Received January 20, 2021; **Revised** February 28, 2021; **Accepted** April 20, 2021

Abstract

Online Romance Scam can be classified as one type of computer related fraud which targets human perception or understanding by using fake or false computer data. Unlike other computer crime such as hacker, his scam does not affect computer security. This scam varies in method and pattern of behavior. The scope of this article was to analyze the application of computer related crime Act to the case of online romance scam. By classifying romance scam into 4 stages, the analysis indicated that computer related crime act could be applied in certain stage of Romance scam such as “Search for victim stage” which is limited to the method of imputing false or fake computer data to deceive the victim in a manner that could possibly affect public. As for relationship making stage and benefit seeking stage which involves the input of fake or false or obscene computer data, the scope of section 14 (1) (2) (4) of the computer related crime Act was restricted merely to the input of data to public. Thus, the interpersonal communication such as “Sexting” was not covered by the offence. Regarding the specific type of “Romance scam” such as “Online dating”, the article found certain limitations of applying section 14 of this Act as well. In addition, “Romance scam” could have relationships with other laws and could cause the victim to be an offender of other laws.

Keywords: Computer–Crime Act; Romance scam; Computer fraud

บทคัดย่อ

Romance scam ที่กระทำทางระบบคอมพิวเตอร์ จัดอยู่ในกลุ่มการฉ้อโกงหลอกลวงทางคอมพิวเตอร์ที่มุ่งหมายต่อการรับรู้หรือความเข้าใจของมนุษย์ โดยใช้ข้อมูลปลอมหรือเท็จ จึงไม่ส่งผลกระทบต่อคุณลักษณะด้านความปลอดภัยทางคอมพิวเตอร์เหมือนอาชญากรรมคอมพิวเตอร์อื่น พฤติกรรมนี้มีความหลากหลายทั้งในแง่ของรูปแบบและวิธีการ บทความนี้จึงศึกษาวิเคราะห์การปรับใช้ พ.ร.บ. คอมพิวเตอร์ กับ “Romance scam” ที่กระทำทางระบบคอมพิวเตอร์ พบว่าพระราชบัญญัตินี้ ไม่มีฐานความผิดเฉพาะสำหรับ “Romance scam” ส่วนฐานความผิดที่มีอยู่มีข้อจำกัดในการปรับใช้กับ “Romance scam” กล่าวคือ เมื่อวิเคราะห์ตามขั้นตอนการทำผิด พบว่า พ.ร.บ. คอมพิวเตอร์อาจนำมาใช้ได้บางขั้นตอน แต่มีข้อจำกัดหลายประการ เช่น ขั้นตอนการแสวงหาเหยื่อ มีข้อจำกัดเฉพาะการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบที่น่าจะทำให้ประชาชนเสียหาย ขั้นตอนการติดต่อสร้างความสัมพันธ์และขั้นตอนการแสวงประโยชน์ แม้ว่าจะเป็นการนำข้อมูลเท็จเข้าสู่ระบบหรือมีข้อมูลลามกแต่มาตรา 14 (1) (2) (4) ก็มีองค์ประกอบที่จำกัดเฉพาะการเผยแพร่ข้อมูลต่อสาธารณะหรือมีลักษณะที่ส่งผลกระทบต่อสาธารณะ ไม่ครอบคลุมการสื่อสารระหว่างบุคคล สำหรับ “Romance scam” บางประเภท เช่น ธุรกิจจัดหาคู่ออนไลน์ พบว่าสามารถปรับใช้ฐานความผิดตาม พ.ร.บ. คอมพิวเตอร์ ในบางกรณี เช่น ธุรกิจจัดหาคู่ที่จัดตั้งขึ้นเพื่อการหลอกลวง นอกจากนี้ “Romance scam” ยังมีความสัมพันธ์กับความผิดตามกฎหมายอื่นและอาจส่งผลให้เหยื่อเป็นผู้กระทำความผิดตามกฎหมายอื่นด้วย

คำสำคัญ: พ.ร.บ.คอมพิวเตอร์; การหลอกลวงเกี่ยวกับความสัมพันธ์เชิงความรัก; การฉ้อโกงหลอกลวงทางคอมพิวเตอร์

บทนำ

การหลอกลวงเกี่ยวกับความสัมพันธ์เชิงความรัก (เนื่องจากยังไม่มีกฎหมายกำหนดความผิดหรือกำหนดนิยามโดยเฉพาะ โดยอาจมีการใช้คำที่แตกต่างกัน เช่น ในทางปฏิบัติของเจ้าหน้าที่ตำรวจใช้คำว่า “แสร้งรักออนไลน์” (แต่ก็ไม่ใช่คำที่บัญญัติในกฎหมายโดยเฉพาะ ในที่นี้จึงใช้คำทับศัพท์ว่า “Romance scam”) เป็นอาชญากรรมชนิดหนึ่ง ซึ่ง จัดอยู่ในกลุ่มการฉ้อโกงหลอกลวง (Scam) โดยอาชญากรติดต่อสร้างความสัมพันธ์ในเชิงความรักกับเหยื่อ ทำให้เชื่อใจว่าอาชญากรมีความรักและประสงค์จะแต่งงานหรือใช้ชีวิตร่วมกัน จากนั้นอาชญากรจะใช้วิธีการต่าง ๆ เพื่อแสวงประโยชน์ เช่น อ้างเหตุต่าง ๆ ขอให้เหยื่อโอนเงินให้ เช่น อ้างเหตุจำเป็นด้านการเดินทางหรือค่าใช้จ่ายในการเดินทาง โดยเฉพาะกรณีเหยื่ออยู่ต่างประเทศ เหตุความเจ็บป่วยหรือเหตุจำเป็นอื่นเพื่อให้เหยื่อเห็นใจ (Nick Tilley & Aiden Sidebottom, 2017) การหลอกลวงอาจเกิดขึ้นครั้งเดียว (Hit and run) หรืออาจเกิดขึ้นอย่างต่อเนื่องผ่านความสัมพันธ์ที่ยาวนาน (Markus Jakobsson, 2016)

“Romance scam” มุ่งหลอกลวงมนุษย์โดยอาศัยจุดอ่อนในแง่ความเปราะบางทางจิตใจหรืออารมณ์ของเหยื่อ (Emotional vulnerability) (Federal Bureau of Investigation (FBI), 2017) “Romance scam” ไม่จำกัดว่าจะต้องเป็นการกระทำทางคอมพิวเตอร์เท่านั้น อย่างไรก็ตาม การสื่อสารข้อมูลคอมพิวเตอร์ส่งผลให้การหลอกลวงประเภทนี้แพร่หลายมากขึ้นโดยเฉพาะการกระทำข้ามพรมแดนของประเทศ เนื่องจากอาชญากรรมประเภทนี้เกี่ยวข้องกับการ

สร้างความสัมพันธ์จึงสามารถเกิดขึ้นในลักษณะต่อเนื่อง อันส่งผลกระทบต่อเหยื่อในระดับที่รุนแรงกว่าการหลอกลวงทรัพย์สินที่เกิดขึ้นแบบครั้งเดียว

เมื่อพิจารณาในแง่กฎหมาย พบว่าพระราชบัญญัติว่าด้วยกากระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่แก้ไขเพิ่มเติม พ.ศ. 2560 (ซึ่งต่อไปในบทความนี้จะใช้คำย่อว่า “พ.ร.บ. คอมพิวเตอร์”) ในส่วนของการฉ้อโกงหลอกลวงทางคอมพิวเตอร์ มีบทบัญญัติเกี่ยวข้องคือ มาตรา 14 (1) ที่บัญญัติว่า “ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูล คอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา” มาตรานี้มีวัตถุประสงค์ใช้สำหรับการป้องกันและปราบปรามการฉ้อโกงหลอกลวงทางคอมพิวเตอร์ ซึ่งโดยหลักแล้วรวมถึงการหลอกลวงในลักษณะ “Romance scam” ด้วย แม้ว่ามาตราดังกล่าวมีการแก้ไขปรับปรุงตามกฎหมายฉบับ พ.ศ. 2560 แต่เมื่อพิจารณาสภาพพฤติกรรมของ “Romance scam” ประกอบกับกฎหมายต่างประเทศแล้ว มีประเด็นว่า ความผิดฐานดังกล่าวครอบคลุมพฤติกรรมการฉ้อโกงทางคอมพิวเตอร์ที่มีรูปแบบหลากหลายรวมทั้ง “Romance scam” ได้เพียงใด จึงนำไปสู่การศึกษาวิเคราะห์เพื่อชี้ให้เห็นปัญหา อุปสรรคและข้อจำกัดในการปรับใช้มาตรา 14 (1) กับ “Romance scam” โดยมีขอบเขตการศึกษาในแง่พฤติกรรมจำกัดเฉพาะ “Romance scam” ที่กระทำทางระบบคอมพิวเตอร์ (Online Romance Scam) และมีขอบเขตด้านกฎหมายที่ศึกษาเฉพาะ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่แก้ไขเพิ่มเติม พ.ศ. 2560 เท่านั้น

การหลอกลวงเกี่ยวกับความสัมพันธ์เชิงความรัก (Romance scam) **ในบริบทของอาชญากรรมประเภทการฉ้อโกงหลอกลวงทางคอมพิวเตอร์**

“Romance scam” ที่เกิดขึ้นในสภาพแวดล้อมการสื่อสารข้อมูลคอมพิวเตอร์ จัดเป็นส่วนย่อยของอาชญากรรมประเภท “การฉ้อโกงหลอกลวงทางคอมพิวเตอร์” (Computer fraud) ดังนั้น บทความนี้จะเริ่มจากการศึกษาแนวคิดและหลักการของการฉ้อโกงหลอกลวงทางคอมพิวเตอร์ ซึ่งเป็นอาชญากรรมคอมพิวเตอร์ (Computer crime) หรือ อาชญากรรมไซเบอร์ (Cyber rime) ประเภทหนึ่งที่เกิดขึ้นแพร่หลายในระบบเศรษฐกิจดิจิทัลและมีขอบเขตกว้าง โดยสามารถจำแนกเป็น 4 กลุ่มพฤติกรรม (Kanathip Thongraweewong, 2021) ได้แก่

(1) การฉ้อโกงหลอกลวงทางคอมพิวเตอร์ที่มีเป้าหมายต่อการประมวลผลโดยอัตโนมัติของระบบหรือโปรแกรมคอมพิวเตอร์ เช่น การหลอกลวงซอฟท์แวร์หรือโปรแกรมที่ใช้วิเคราะห์ข้อมูล (Analytics software) ทั้งนี้เนื่องจาก มีซอฟท์แวร์หรือโปรแกรมที่นำปัจจัยต่างๆ มาประกอบการคำนวณ โดยประมวลผลและตัดสินใจโดยอัตโนมัติ หรือการใช้ปัญญาประดิษฐ์ (Artificial Intelligence หรือ AI) อาชญากรจึงใช้วิธีการทางเทคนิค เพื่อ หลอกลวงการทำงานโดยอัตโนมัติของซอฟท์แวร์หรือโปรแกรม โดยไม่ได้มุ่งหมายต่อการรับรู้ของมนุษย์ดังเช่นการหลอกลวงฉ้อโกงแบบดั้งเดิม

(2) การฉ้อโกงหลอกลวงในระบบการชำระเงินทางอิเล็กทรอนิกส์ เช่น การรับเงินหรือชำระเงินผ่านระบบอิเล็กทรอนิกส์ ผ่านโปรแกรมประยุกต์ (Application) หรือกระเป๋าเงินอิเล็กทรอนิกส์ (E-wallet)

(3) การฉ้อโกงหลอกลวงประเภท “Phishing” แม้ว่าโดยทั่วไปการฉ้อโกงหลอกลวงประเภทนี้คือการใช้วิธีการนำข้อมูลปลอมเข้าสู่ระบบ โดยมุ่งหมายได้มาซึ่งรหัสผ่านหรือข้อมูลส่วนตัวของเหยื่อ แต่มีความซับซ้อนในแง่เทคนิค

และจำแนกวิธีการกระทำได้หลากหลาย (Kanathip Thongraweewong, 2018) บางวิธีการไม่เกี่ยวข้องกับการนำข้อมูลปลอมหรือเท็จหลอกลวงมนุษย์ แต่เป็นการกระทำต่อระบบหรือโปรแกรมโดยอัตโนมัติ

(4) การฉ้อโกงหลอกลวงประเภท “Scam” จัดอยู่ในกลุ่มการฉ้อโกงหลอกลวงทางคอมพิวเตอร์ ซึ่งใช้ข้อมูลเท็จหลอกลวงมนุษย์ โดยแยกเป็นสองกลุ่มหลัก ได้แก่ (1) การหลอกลวงเกี่ยวกับธุรกิจหรือการลงทุน เช่น การหลอกลวงในรูปแบบ “Ponzi scam” ซึ่งคล้ายคลึงกับ แผนการแบบพีระมิด (Pyramid scheme) ในกรณีที่มีการนำเงินจากผู้เข้าร่วมมาจ่ายให้กันเป็นทอดๆ รวมทั้งมีการให้ค่าตอบแทนจากการแนะนำผู้อื่นเข้าร่วม (Recruiting) (Rustad, 2014) และ (2) การหลอกลวงเกี่ยวกับความสัมพันธ์ระหว่างบุคคล โดยเฉพาะความสัมพันธ์ในเชิงความรัก (Romance scam) โดยในบทความนี้มีขอบเขตศึกษาวิเคราะห์อาชญากรรมชนิดนี้ ซึ่งแม้ว่าจะคล้ายคลึงกับการหลอกลวงประเภท “Scam” ชนิดอื่นเนื่องจากอาศัยความไว้วางใจของเหยื่อและอาจนำไปสู่การได้มาซึ่งประโยชน์ทางการเงินเช่นกัน แต่ Romance scam อาศัยความไว้วางใจในระดับที่ลึกซึ้งกว่าเนื่องจากเชื่อมโยงกับความสัมพันธ์ในเชิงความรัก และอาจมีชื่อเรียกที่หลากหลาย เช่น Online dating scam, Sex scam เป็นต้น

การหลอกลวงเกี่ยวกับความสัมพันธ์เชิงความรัก(Romance scam) **ตามกรอบแนวคิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์**

กรอบแนวคิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ที่ใช้ในบทความนี้คือกรอบแนวคิดเกี่ยวกับเกณฑ์ความมั่นคงปลอดภัยของระบบและข้อมูลคอมพิวเตอร์ (Information security) ซึ่งพิจารณาโดยจำแนกคุณลักษณะ (Characteristics) 3 ประการ อันนำไปสู่เป้าหมายชองความมั่นคงปลอดภัยของระบบหรือข้อมูล (Set of security goals) (Cherdantseva and Hilton, 2013) ได้แก่

(1) “Confidentiality” หรือ “C” หมายถึง การรักษาความลับ ซึ่งมีความหมายสองนัย คือ (1) ความลับของข้อมูล (Data Confidentiality) ซึ่งจะไม่ถูกเข้าถึงหรือเปิดเผยโดยผู้ที่ไม่มีสิทธิ (Gattiker, 2004) (2) ความเป็นส่วนตัว (Privacy) หมายถึง เจ้าของข้อมูลเป็นผู้ควบคุมว่าข้อมูลของตนจะถูกเก็บรวบรวม ประมวลผล โดยบุคคลใด และภายใต้เงื่อนไขใด และอาจถูกส่งต่อให้บุคคลใด

(2) “Integrity” หรือ “I” หมายถึง การคงสภาพหรือบูรณภาพ ซึ่งมีความหมายสองนัยคือ 1) บูรณภาพของข้อมูล (Data integrity) ซึ่งมีความหมายว่าข้อมูลจะถูกเปลี่ยนแปลงได้เฉพาะกรณีที่กระทำโดยมีอำนาจ (National Research Council, 1991) 2) บูรณภาพของระบบ (System integrity) หมายถึง ระบบจะต้องปฏิบัติการได้ตามหน้าที่ที่กำหนด ไว้โดยปราศจากการแทรกแซงที่ไม่มีอำนาจ ในการรักษาบูรณภาพของระบบจะต้องอาศัยความสมบูรณ์เชิงตรรกะ (logical completeness) ของฮาร์ดแวร์และซอฟท์แวร์ที่เกี่ยวกับมาตรการป้องกันระบบจากการแทรกแซงด้วย (Longley and Shain, 1989)

(3) Availability หรือ “A” หมายถึง การที่ระบบพร้อมที่จะทำงานโดยไม่ปฏิเสธผู้ใช้ที่มีอำนาจ (Frawley, Miller and Miller, 2001) อาจเรียกว่า “ความพร้อมใช้งาน” โดยในความหมายอย่างกว้างรวมถึงระบบและข้อมูลคอมพิวเตอร์ด้วย

เมื่อนำกรอบแนวคิดนี้มาวิเคราะห์การฉ้อโกงหลอกลวงทางคอมพิวเตอร์ จำแนกได้ 2 กรณีคือ

– *การฉ้อโกงหลอกลวงทางคอมพิวเตอร์* ที่ส่งผลกระทบต่อคุณลักษณะด้านความปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์ เช่น การส่งชุดคำสั่งไปยังโปรแกรมเป้าหมายเพื่อให้ทำงานไปตามที่อาชญากรต้องการ เพื่อประมวลผลการจ่ายเงินหรือประโยชน์อื่นให้แก่อาชญากร ดังนี้ ส่งผลกระทบในการทำให้เกิดการแก้ไขเปลี่ยนแปลง

ข้อมูลหรือบูรณภาพของข้อมูล แต่ไม่เกี่ยวข้องกับการหลอกลวงบุคคลโดยตรง เมื่อพิจารณาตามพ.ร.บ.คอมพิวเตอร์ จะพบว่ามีฐานความผิดสำหรับการกระทำที่กระทบต่อคุณลักษณะด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ เช่น มาตรา 5–10 (Kanathip Thongraweewong, 2020)

– *การฉ้อโกงหลอกลวงทางคอมพิวเตอร์* ที่ไม่ส่งผลกระทบต่อคุณลักษณะด้านความปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์ กล่าวคือ การหลอกลวงที่มุ่งเน้นการหลอกลวงบุคคล โดยอาศัยระบบหรือคอมพิวเตอร์เป็นเครื่องมือหรือช่องทางการสื่อสาร แต่ไม่ส่งผลกระทบต่อคุณลักษณะด้านความลับ บูรณภาพ และ ความพร้อมใช้ ผู้กระทำจึงอาศัยข้อมูลเนื้อหาที่มนุษย์เข้าใจได้ เช่น ข้อมูลเท็จ บิดเบือน

สำหรับ “Romance scam” แม้กระทำทางคอมพิวเตอร์ แต่เป็นการฉ้อโกงหลอกลวงที่ไม่ส่งผลกระทบต่อคุณลักษณะด้านความปลอดภัยของระบบหรือข้อมูล เนื่องจากอาศัยข้อมูลเท็จเพื่อหลอกลวงเหยื่อเพื่อสร้างความสัมพันธ์ระหว่างบุคคล กล่าวคือ ผลกระทบจากข้อมูลเท็จที่นำเข้าสู่ระบบนั้นเกิดขึ้นกับความรู้และความเข้าใจตลอดจนปฏิกิริยาตอบสนองจากบุคคลผู้เป็นเหยื่อ โดยไม่ส่งผลให้ระบบหรือข้อมูลถูกแก้ไขหรือไม่สามารถใช้การได้แต่อย่างใด กล่าวคือ อาชญากรอาศัยสภาพแวดล้อมทางคอมพิวเตอร์เป็นช่องทางกระทำเท่านั้น

วิเคราะห์การปรับใช้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กับ การหลอกลวงเกี่ยวกับความสัมพันธ์เชิงความรัก (Romance scam)

เนื่องจาก “Romance scam” มีลักษณะและวิธีการหลากหลาย ตลอดจนสามารถแบ่งย่อยได้หลายประเภท บทความนี้จึงวิเคราะห์การปรับใช้กฎหมายสำหรับพฤติกรรมนี้โดยใช้สองวิธีการคือ การวิเคราะห์ตามขั้นตอนของพฤติกรรม และ การวิเคราะห์โดยจำแนกตามประเภทของพฤติกรรม

*วิเคราะห์การปรับใช้กฎหมายกับ **“Romance scam”** โดยวิธีการจำแนกขั้นตอนพฤติกรรม*

เมื่อพิจารณารูปแบบหรือวงจรพฤติกรรมของ Romance scam จะสามารถจำแนกขั้นตอนพฤติกรรมได้สี่ขั้นตอน เพื่อวิเคราะห์ปรับใช้กฎหมายในแต่ละขั้นตอนดังต่อไปนี้

1) ขั้นตอนการแสวงหาเหยื่อ กล่าวคือ การสืบค้นข้อมูลหรือแสวงหาเหยื่อจากสื่อออนไลน์ เช่น เว็บไซต์จัดหาคู่หรือสื่อสังคมออนไลน์ (Social media) ในขั้นตอนนี้อาจยังไม่เป็นความผิดตามกฎหมายหากเป็นการค้นหาข้อมูลที่บุคคลทั่วไปเข้าถึงได้ แต่หากเป็นการเข้าถึงระบบโดยมิชอบเพื่อได้ข้อมูลเหยื่อมาอาจเป็นความผิด มาตรา 5 มาตรา 7 ของ พ.ร.บ. คอมพิวเตอร์ แต่ในขั้นตอนนี้หากมี การนำข้อมูลบุคคลอื่นมาปลอมตัวเพื่อแอบอ้าง (Fake profile) (Rege, 2009) จะเป็นการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบตาม มาตรา 14 (1)

2) ขั้นตอนการสร้างความสัมพันธ์ กล่าวคือ อาชญากรติดต่อสร้างความรู้จัก นอกจากนี้ หากอาชญากรรู้จักเหยื่อผ่านทางการสนทนาเป็นกลุ่ม อาจทำการชักชวนให้เหยื่อมาทำการสนทนาในช่องทางส่วนบุคคล เช่น ผ่านโปรแกรมสนทนาระหว่างเหยื่อกับอาชญากรรม เมื่อพิจารณาสภาพลักษณะพฤติกรรมของการกระทำในขั้นตอนนี้จะเป็นการยากที่จะจำแนกความแตกต่างจากการติดต่อสร้างความสัมพันธ์ระหว่างบุคคลในสังคมออนไลน์ จึงยังไม่เป็นความผิดตามกฎหมายและไม่มีมาตรการทางกฎหมายที่จะคุ้มครองหรือป้องกันเหยื่อในขั้นตอนนี้

อย่างไรก็ตาม การสื่อสารสร้างความสัมพันธ์อาจเป็นความผิดตาม พ.ร.บ. คอมพิวเตอร์ มาตรา 14 หากเนื้อหาที่สื่อสารเป็นเนื้อหาผิดกฎหมาย (Illegal content) แต่จากการศึกษาพบว่า มาตรา 14 มีข้อจำกัดในการปรับใช้กับพฤติกรรมในขั้นตอนนี้ด้วยเหตุสองประการคือ

(1) Romance scam ในขั้นตอนการสื่อสารสร้างความสัมพันธ์ อาจยังไม่สามารถบ่งชี้ได้ว่าเป็นการนำข้อมูล “เท็จ หรือ บิดเบือน” เข้าสู่ระบบ เนื่องจากเป็นเพียงการสื่อสารข้อมูลในลักษณะให้ความหวัง ความรู้สึก เท่านั้น

(2) พฤติกรรมในขั้นตอนนี้เป็นการสื่อสารระหว่างบุคคลโดยไม่เผยแพร่ต่อสาธารณะ จึงไม่เข้าองค์ประกอบความผิดเกี่ยวกับเนื้อหาตามมาตรา 14 ซึ่งในหลายอนุมาตรมีเงื่อนไขว่าต้องเป็นเนื้อหาที่มีการเผยแพร่ต่อสาธารณะหรือมีลักษณะผลกระทบต่อสาธารณะ เช่น ข้อมูลเท็จตามมาตรา 14 (2) ต้องเป็นกรณีที่น่าจะทำให้ประชาชนตื่นตระหนกหรือกระทบต่อความมั่นคงของรัฐ จึงไม่รวมถึงข้อมูลเนื้อหาหลอกลวงเฉพาะบุคคล สำหรับข้อมูลคอมพิวเตอร์อันลามกตามมาตรา 14 (4) มีองค์ประกอบจำกัดเฉพาะการสื่อสารที่ประชาชนทั่วไปอาจเข้าถึงได้ จึงไม่รวมถึงการสื่อสารสร้างความสัมพันธ์ระหว่างอาชญากรกับเหยื่อโดยส่งข้อมูลทางเพศระหว่างกัน (Sexting) แต่ทั้งนี้หากมีการส่งข้อมูลลามกเด็กหรือครอบครองสื่อลามกเด็กอาจเป็นความผิดกฎหมายอาญาซึ่งไม่อยู่ในขอบเขตการศึกษาของบทความนี้

3) ขั้นตอนการแสวงประโยชน์ทางทรัพย์สิน โดยอาชญากรอาจเริ่มจากสิ่งเล็กน้อย เช่น ขอสิ่งของ ของขวัญ เพื่อเป็นการทดสอบเหยื่อ จากนั้นจะขอเงินจำนวนที่มากขึ้นโดยอ้างเหตุจำเป็นต่าง ๆ (Whitty Monica T & Buchanan Tom, 2012) เช่น ขอเงินค่าเดินทางจากต่างประเทศไปพบเหยื่อ อ้างเหตุความจำเป็นหรือเดือดร้อนเพื่อขอยืมเงิน ขั้นตอนนี้แม้เป็นการนำข้อมูลเท็จเข้าสู่ระบบ แต่หากข้อเท็จจริงปรากฏว่าเป็นการสื่อสารหลอกลวงเฉพาะเหยื่อ จะไม่เป็นความผิดมาตรา 14 (4) เพราะไม่มีพฤติการณ์ที่ประชาชนทั่วไปน่าจะเกิดความเสียหาย แต่อาจเป็นความผิดฐานฉ้อโกงตามกฎหมายอาญาซึ่งไม่อยู่ในขอบเขตการศึกษานี้

เนื่องจากลักษณะพิเศษของ Romance scam คือความสัมพันธ์ระหว่างบุคคล โดยอาจเกิดขึ้นผ่านกระบวนการสร้างความสัมพันธ์ที่ยาวนานกว่า “Scam” ชนิดอื่น (Jakobsson, 2016) การเรียกร้องทรัพย์สินจึงมีลักษณะต่อเนื่องหรือเป็นวงจรการหลอกลวง (cycle of lures) (IC3 (Internet Crime Complaint Center), 2007) ดังนั้นในช่วงความสัมพันธ์อาจมีการเรียกทรัพย์สินหลายครั้งด้วยเหตุที่เชื่อมโยงกันหรืออ้างเหตุใหม่ ในทางกฎหมายอาจเป็นการฉ้อโกงตามกฎหมายอาญาหลายกรรมต่างกัน

4) ขั้นตอนการแสวงประโยชน์ต่อเนื่องหลังจากเหยื่อรู้ตัว โดยปกติวงจรของพฤติกรรม Romance scam จะยุติลงเมื่อเหยื่อรู้ตัวว่าถูกหลอกและตัดสินใจยุติการให้ประโยชน์แก่อาชญากร อย่างไรก็ตาม ในบางกรณี แม้ว่าอาชญากรรู้ว่าเหยื่อรู้ตัวแล้ว แต่ยังคงดำเนินการแสวงประโยชน์จากเหยื่อต่อไป ขั้นตอนนี้อาจจัดเป็น “คลื่นที่สอง” (Second wave of romance scam) (Whitty and Buchanan, 2012) เช่น อาชญากรยอมรับว่าในครั้งแรกตั้งใจหลอกลวงแต่ต่อมาเกิดความรักเหยื่อจริงๆ หรือ ปลอมตัวเป็นบุคคลที่สาม เช่น อ้างเป็นเจ้าหน้าที่มาอธิบายเหตุผลที่อาชญากรไม่มาพบเหยื่อตามที่นัดหมายเพราะป่วยหนักต้องการเงิน หรือ นำข้อมูลทางเพศที่ได้จากเหยื่อในขั้นตอนการพูดคุยมาข่มขู่เรียกทรัพย์สิน ในส่วนนี้จะเกี่ยวข้องกับอาชญากรรมประเภทอื่น เช่น การขู่คุกคามทางเพศ (Sextortion) ซึ่งอาจเป็นความผิดตามกฎหมายอาญา เช่นรีดเอาทรัพย์ หรือความผิดต่อเสรีภาพ ซึ่งไม่อยู่ในขอบเขตการศึกษานี้ ในแง่ของ พ.ร.บ. คอมพิวเตอร์ การกระทำของ “Romance scam” ในขั้นตอนนี้จะเกี่ยวข้องกับ การวิเคราะห์การปรับใช้กฎหมายโดยจำแนกตามขั้นตอนของพฤติกรรม เป็นกรอบการวิเคราะห์ซึ่ง สามารถนำไปประยุกต์ใช้กับ “Romance scam” ประเภทต่างๆ ที่อาจมีลักษณะและวิธีการแตกต่างกันไป

*วิเคราะห์การปรับใช้กฎหมายกับ **“Romance scam”** ตามประเภทของพฤติกรรม*

เนื่องจาก “Romance scam” มีลักษณะและรายละเอียดที่แตกต่างกันในแต่ละกรณี นอกจากการปรับใช้กฎหมายโดยจำแนกตามขั้นตอนพฤติกรรมดังกล่าวในหัวข้อ 4.1 แล้ว ในหัวข้อนี้จะวิเคราะห์ การปรับใช้กฎหมายโดยจำแนกตามประเภทของ “Romance scam” ซึ่งจะเลือกนำประเภทของ “ธุรกิจจัดหาคู่ออนไลน์” มาศึกษาวิเคราะห์

ธุรกิจบริการจัดหาคู่ทั้งที่ให้บริการในประเทศและธุรกิจจัดหาคู่สมรสระหว่างประเทศ (International marriage agencies) จัดเป็นธุรกิจที่ถูกต้องตามกฎหมายของหลายประเทศ ธุรกิจเหล่านี้ อาจให้บริการทั้งทางระบบคอมพิวเตอร์ (Online dating sites) โดยมีระดับการให้บริการแตกต่างกันไป เช่น จัดให้มีระบบฐานข้อมูลสำหรับสมาชิกบริการคัดเลือกจับคู่ที่เหมาะสมโดยการประมวลข้อมูล หรือเพียงให้บริการในฐานะตัวกลางติดต่อระหว่างสมาชิก อย่างไรก็ตาม ธุรกิจดังกล่าวอาจมีความสัมพันธ์กับ Romance scam ในสองกรณีดังนี้

กรณีที่หนึ่ง ธุรกิจการจัดหาคู่ออนไลน์ที่มีลักษณะเป็น Romance scam ในกรณีนี้ผู้ให้บริการมีเจตนาแสวงประโยชน์โดยมิชอบ เช่น บริการจัดหาคู่ระหว่างประเทศที่ให้บริการทางสื่อออนไลน์ โดยเสนอว่าจะจัดหาให้มีการแต่งงาน แต่แท้จริงแล้วเป็นการจัดส่งให้ไปถูกกักขังและให้บริการทางเพศ กรณีนี้อาจเรียกว่า”Marriage scam” และเชื่อมโยงกับอาชญากรรมอื่น เช่น การค้ามนุษย์ (Federal Bureau of Investigation (FBI), 2017) เมื่อวิเคราะห์การปรับใช้ พ.ร.บ. คอมพิวเตอร์ ธุรกิจจัดหาคู่กรณีนี้เป็นการนำข้อมูลเท็จหลอกลวงบุคคลทั่วไปทางอินเทอร์เน็ตอันเป็นความผิดตาม มาตรา 14 (1)

กรณีที่สอง ธุรกิจการจัดหาคู่ออนไลน์ที่ผู้ประกอบธุรกิจไม่มีส่วนเกี่ยวข้องกับ Romance scam แต่ถูกใช้เป็นช่องทางหรือเครื่องมือของอาชญากร เช่น อาชญากรสมัครสมาชิกใช้บริการหาคู่ออนไลน์เพื่อติดต่อสร้างความสัมพันธ์และให้ความหวังว่าจะแต่งงานกับเหยื่อ ต่อมาเมื่อเหยื่อหลงเชื่อจึงเริ่มหลอกลวงทรัพย์สินจากเหยื่อ (Rege, 2009)

เมื่อวิเคราะห์การปรับใช้ พ.ร.บ. คอมพิวเตอร์ กรณีนี้ อาชญากรผู้หลอกลวงอาจมีความผิด มาตรา 14 (1) สำหรับพฤติกรรมการเผยแพร่ข้อมูลเท็จที่อาจกระทบต่อประชาชนทั่วไป เช่น การนำโปรไฟล์ปลอมไปเผยแพร่ในเว็บไซต์หาคู่ที่เข้าถึงได้โดยบุคคลทั่วไป ในส่วนของผู้ให้บริการเว็บไซต์หาคู่ อยู่ในความหมายของ ผู้ให้บริการ โดยจัดเป็นผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น จึงอาจต้องรับผิดตาม มาตรา 15 สำหรับเนื้อหาที่ผู้ใช้งานนำเข้าสู่ระบบ หากเนื้อหานั้นเป็นความผิด มาตรา 14 อย่างไรก็ตาม หากผู้ให้บริการพิสูจน์ว่าได้ดำเนินการตามหลักแจ้งเตือนและระงับเนื้อหา(Notice and takedown) ตาม มาตรา 15 และประกาศกระทรวงแล้วก็ได้รับยกเว้นโทษ

จากความสัมพันธ์กับธุรกิจจัดหาคู่ออนไลน์ จะเห็นได้ว่า Romance scam อาจใช้ในความหมายที่แคบลงสำหรับพฤติกรรมหลอกลวงเกี่ยวกับการหาคู่สมรสหรือการแต่งงาน จึงอาจเรียกว่า “Dating scam หรือ Marriage scam” หรือ “Mail-order bride” โดยการกระทำหลักคือ ชักจูงให้เหยื่อหลงเชื่อด้วยการอ้างเหตุเกี่ยวกับการจัดหาคู่ที่จะนำไปสู่การสมรสหรือสร้างครอบครัว นอกจากนี้ยังอาจเกี่ยวข้องกับความผิดตามกฎหมายอื่น เช่น การเข้าเมือง การสัญญาว่าจะจัดการเพื่อให้ได้วีซ่าสำหรับเข้าประเทศ

Romance scam กับ อาชญากรรมชนิดอื่น

ลักษณะสำคัญของ Romance scam คือ การหลอกลวงโดยอาศัยความเชื่อใจและความคาดหวังบนพื้นฐานของความรักจึงอาจนำไปสู่ Scam ชนิดอื่นได้อย่างหลากหลาย เช่น การหลอกลวงเงิน การหลอกลวงให้ร่วมลงทุน การหลอกลวงให้ร่วมทำธุรกิจที่ผิดกฎหมายอื่น เป็นต้น นอกจากนี้ Romance scam ยังมีความเกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์อื่น เช่น การโจรกรรมข้อมูลเอกลักษณ์หรือข้อมูลระบุตัวตน (Identity theft) โดยเฉพาะในขั้นตอนที่

อาชญากรแอบอ้างหรือปลอมตัวเป็นคนอื่นเพื่อพูดคุยสร้างความสัมพันธ์กับเหยื่อ เช่น อ้างว่าเป็นผู้หญิง โดยนำภาพโปรไฟล์ของผู้อื่นมาแสดงให้เหยื่อหลงเชื่อ การอ้างว่าเป็นผู้ทำงานในธุรกิจจัดหานักแสดงหรือโฆษณา อ้างว่าเป็นเจ้าหน้าที่รัฐ นักธุรกิจ ฯลฯ วิธีการเช่นนี้เข้าองค์ประกอบฐาน นำข้อมูลปลอมหรือเท็จเข้าสู่ระบบคอมพิวเตอร์ แต่หากเป็นการหลอกลวงเหยื่อโดยเจาะจงอาจไม่ใช่พฤติการณ์ที่น่าจะเสียหายแก่ประชาชนตาม มาตรา 14 (1)

นอกจากนี้ Romance scam บางกรณีส่งผลให้เหยื่อกลายเป็นผู้กระทำผิดตามกฎหมายอื่น กล่าวคือ เมื่อเหยื่อหลงเชื่อแล้ว อาชญากรอาจใช้เหยื่อเป็นเครื่องมือกระทำผิดอื่น เช่น ให้เหยื่อเป็นผู้รับหรือส่งเงินที่อาชญากรได้มาโดยมิชอบ (Money mule) (Jakobsson, 2016) ให้เหยื่อมีส่วนในการซื้อขายสินค้าหนีภาษีหรือสินค้าผิดกฎหมาย ฯลฯ เหยื่อจึงอาจเป็นตัวการร่วมกับอาชญากรในการกระทำผิดตามกฎหมายต่าง ๆ กฎหมายฟอกเงิน กฎหมายภาษี เช่น การฉ้อโกงหลอกลวงในแผนการอื่นของอาชญากรต่อไป

สรุป

Romance scam ที่กระทำทางระบบคอมพิวเตอร์ จัดอยู่ในกลุ่มการฉ้อโกงหลอกลวงทางคอมพิวเตอร์ในลักษณะเดียวกับ “Scam” ซึ่งเป็นการหลอกลวงที่มุ่งหมายต่อการรับรู้หรือความเข้าใจของมนุษย์ โดยใช้ข้อมูลปลอมหรือเท็จ จึงไม่ส่งผลกระทบต่อคุณลักษณะด้านความปลอดภัยทางคอมพิวเตอร์ดังเช่นอาชญากรรมคอมพิวเตอร์อื่น พฤติกรรมนี้มีความหลากหลายทั้งในแง่ของรูปแบบและวิธีการ บทความนี้จึงศึกษาวิเคราะห์การปรับใช้ พ.ร.บ. คอมพิวเตอร์ กับ “Romance scam” ที่กระทำทางระบบคอมพิวเตอร์ โดยมีวิธีการวิเคราะห์สองแนวทาง คือ การวิเคราะห์การปรับใช้ พ.ร.บ. คอมพิวเตอร์ กับ “Romance scam” โดยจำแนกตามขั้นตอนของพฤติกรรม กล่าวคือ จำแนกลักษณะร่วม (Common character) ของ “Romance scam” แต่ละประเภท ออกเป็น 4 ขั้นตอน ซึ่งพบว่า พ.ร.บ. คอมพิวเตอร์ อาจนำมาใช้กับ Romance scam ได้บางขั้นตอนของพฤติกรรม เช่น ขั้นตอนการแสวงหาเหยื่อ แต่ก็มีข้อจำกัดเฉพาะการแสวงหาเหยื่อโดยมีพฤติกรรมการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบที่น่าจะทำให้ประชาชนเสียหาย เช่น การนำข้อมูลของผู้อื่นมาใช้แสดงประวัติบนเว็บไซต์เพื่อหลอกลวงให้เหยื่อหลงเชื่อ สำหรับขั้นตอนการติดต่อสร้างความสัมพันธ์และขั้นตอนการแสวงประโยชน์ แม้ว่าจะเป็นการนำข้อมูลเท็จเข้าสู่ระบบแต่มาตรา 14 (1) (2) ก็มีองค์ประกอบที่จำกัดเฉพาะการเผยแพร่ข้อมูลต่อสาธารณะหรือมีลักษณะที่ส่งผลกระทบต่อสาธารณะ

การวิเคราะห์การปรับใช้ พ.ร.บ. คอมพิวเตอร์ กับ “Romance scam” โดยจำแนกตามประเภท ซึ่งในที่นี้กล่าวถึงกรณี ธุรกิจจัดหาคู่ออนไลน์ ซึ่งพบว่า พ.ร.บ. คอมพิวเตอร์ อาจนำมาปรับใช้ได้บางกรณี เช่น ธุรกิจจัดหาคู่ที่จัดตั้งขึ้นเพื่อการหลอกลวง สำหรับธุรกิจจัดหาคู่ที่ไม่มีวัตถุประสงค์หลอกลวงก็อาจเกี่ยวข้องกับความผิดตามมาตรา 14 เช่น การนำข้อมูลผู้อื่นมาแสดงในเว็บไซต์จัดหาคู่อันเป็นการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบตามมาตรา 14 (1) สรุปได้ว่า พ.ร.บ. คอมพิวเตอร์ มีฐานความผิดที่สามารถปรับใช้กับอาชญากรรมที่กระทำทางระบบคอมพิวเตอร์หลายรูปแบบ แต่ในกรณีของ “Romance scam” นั้นไม่มีฐานความผิดเฉพาะและฐานความผิดที่มีอยู่มีข้อจำกัดในการปรับใช้กับ “Romance scam” โดยเฉพาะในขั้นตอนการติดต่อสร้างความสัมพันธ์กับเหยื่อ

ข้อเสนอแนะ

จากผลการวิเคราะห์จะเห็นได้ว่า ในกรณีของ “Romance scam” พ.ร.บ. คอมพิวเตอร์ ไม่มีฐานความผิดเฉพาะและฐานความผิดที่มีอยู่โดยเฉพาะมาตรา 14 สามารถปรับใช้กับ “Romance scam” อย่างมีข้อจำกัดทั้งในแง่ขั้นตอนและประเภทของพฤติกรรม ผู้เขียนจึงมีข้อเสนอแนะสองแนวทางดังนี้

แนวทางที่หนึ่ง แก้ไข พ.ร.บ. คอมพิวเตอร์ โดยเพิ่มบทบัญญัติเกี่ยวกับ “Romance scam” โดยเฉพาะ แยกต่างหากจากมาตรา 14 โดยมีองค์ประกอบครอบคลุมทั้ง 4 ขั้นตอนของการกระทำ

แนวทางที่สอง แก้ไข พ.ร.บ. คอมพิวเตอร์ เพื่อให้ฐานความผิดมีขอบเขตจำกัดเฉพาะอาชญากรรมคอมพิวเตอร์ที่แท้จริง (Pure cybercrime) ซึ่งกระทบต่อคุณลักษณะด้านความปลอดภัยทางคอมพิวเตอร์ (CIA) โดยในกรณีมาตรา 14 นั้น ควรแก้ไขเพื่อแยกการฉ้อโกงหลอกลวงทางคอมพิวเตอร์ซึ่งไม่ส่งผลกระทบต่อคุณลักษณะด้านความปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์ ดังเช่น “Romance scam” ออกจากฐานความผิดมาตรานี้ เนื่องจากสามารถปรับใช้กฎหมายอื่น เช่น ความผิดฐานฉ้อโกง ตามประมวลผลกฎหมายอาญาได้อยู่แล้ว

References

Cherdantseva, Y., & Hilton, J. (2013). Information Security and Information Assurance: The Discussion about the Meaning, Scope and Goals, In *Organizational, Legal, and Technological Dimensions of Information System Administrator*, Almeida, F. Portelal. (Eds.). Hershey, PA: IGI Global. Pp.167–198.

Federal Bureau of Investigation (FBI). (2017). *Romance scam.* Retrieved June 9, 2019, from https://www.fbi.gov/news/stories/romance–scams

Frawley, K., Miller, D. W., & Miller, C. (2001). State of Security Features for Medical Information. In *Information Technology for the Practicing Physician*, section Security of Medical Information, Joan M. Kiel. (Eds.). Springer. Pp. 247–253.

Gattiker, Urs E. (2004). *The Information Security Dictionary.* Kluwer Academic Publisher.

IC3 (Internet Crime Complaint Center). (2007). *Internet Crime Report*. Retrieved June 9, 2019, from http://www.ic3.gov/media/annualreport/2007_IC3 Report.pdf

Jakobsson, M. (2016). *Case study: Romance Scams,* In Understanding Social Engineering Based Scams, Springer. Retrieved June 9, 2019, from https://www.springer.com/gp/book /9781493964550#aboutBook

Longley, D., & Shain, M. (1989). *Data and Computer Security: A Dictionary of Terms and Concepts*. London: Palgrave Macmillan, UK.

National Research Council. (1991). *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: The National Academies Press.

Rege, A. (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud, *International Journal of Cyber Criminology*, *3*(2), 494–512.

Rustad, M. (2014). *Global Internet Law (Hornbook Series)*. St. Paul, MN: West Academic Publishing.

Thongraweewong, K. (2018). Legal Limitations Relating to the Application of Thai Computer–related Crime Act of B.E. 2560 in the Case of "Phishing", paper presented in *the 9th International Science, Social Science, Engineering and Energy Conference I–SEEC 2018*, Bangkok, Thailand.

Thongraweewong, K. (2020). *Computer Crimes Law, Volume 1: Offences against computer and data security*. Bangkok: Nititham.

Thongraweewong, K. (2021). *Computer Crimes Law, Volume 2: Offences against Computer Fraud, Spam and other offences*. Bangkok: Nititham.

Tilley, N., & Sidebottom, A. (2017). *Handbook of Crime Prevention and Community Safety* (2nd ed.). London: Routledge.

Whitty, M.T., & Buchanan, T. (2012). The Online Romance Scam: A Serious Cybercrime. *Cyber Psychology, Behavior, and Social Networking*, 15(3), 181–183.