การฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์

Artificial Intelligence in Identity Fraud

เมธิ์ธีรฎา ธรรมไชยพงษ์[1]

Meteerada Tamchipong

อัจฉรียา ชูตินันทน์[2]

Achariya Chutinun

[1] นักศึกษา หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์

Graduate Student of Master of Law, Pridi Banomyong Faculty of Law, Dhurakij Pundit University

[2] รองศาสตราจารย์ คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์

Associate Professor in Pridi Banomyong Faculty of Law, Dhurakij Pundit University

บทคัดย่อ

ความเจริญก้าวหน้าทางด้านเทคโนโลยีการสื่อสาร โดยเฉพาะเทคโนโลยีปัญญาประดิษฐ์ การพัฒนาเครื่องมือที่สามารถสร้างภาพ เสียง และวิดีโอที่มีความสมจริงสูงในปัจจุบัน ส่งผลให้รูปแบบการก่ออาชญากรรมเปลี่ยนแปลงไปจากเดิมอย่างมีนัยสำคัญ โดยเฉพาะการฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์เพื่อหลอกลวงบุคคลที่กระทำได้อย่างแนบเนียนและซับซ้อน จนเป็นอุปสรรคต่อการข่มขู่ ยับยั้ง ป้องกัน ปราบปราม หรือการนำตัวผู้กระทำความผิดมาลงโทษ โดยผู้กระทำผิดจำนวนมากมักมีความรู้ความชำนาญในการใช้เทคโนโลยีดังกล่าว และมีวัตถุประสงค์เพื่อแสวงหาทรัพย์สินหรือผลประโยชน์จากผู้อื่นโดยมิชอบ ซึ่งอาชญากรรมในลักษณะนี้ไม่เพียงแต่ก่อให้เกิดความเสียหายแก่ผู้เสียหายโดยตรง แต่ยังกระทบต่อระบบเศรษฐกิจ ความมั่นคงของประเทศ และความเชื่อมั่นของประชาชนต่อระบบการทำธุรกรรมทางอิเล็กทรอนิกส์ที่เป็นโครงสร้างพื้นฐานของสังคมยุคดิจิทัล ทั้งนี้ โอกาสในการเกิดความเสียหายมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง เนื่องจากเทคโนโลยีที่ใช้ก่ออาชญากรรมมีความซับซ้อนยิ่งขึ้น และสามารถนำไปใช้ซ้ำหรือขยายผลในวงกว้างด้วยต้นทุนที่ต่ำ เมื่อประกอบกับความสามารถในการซ่อนตัวผ่านช่องทางออนไลน์ ยิ่งทำให้การติดตามจับกุมผู้กระทำผิดทำได้ยาก ส่งผลให้การกระทำผิดในลักษณะนี้ทวีความรุนแรงและสร้างความเสียหายต่อสังคมอย่างต่อเนื่อง

การฉ้อโกงและการฉ้อโกงโดยการปลอมแปลงตัวตนเป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่งซึ่งมีพัฒนาการที่ซับซ้อนขึ้นอย่างต่อเนื่อง แม้ยังคงอาศัยวิธีการหลอกลวงเป็นหลัก แต่เมื่อผนวกกับเทคโนโลยีปัญญาประดิษฐ์ (AI) กลับยิ่งเพิ่มศักยภาพของการปลอมแปลงให้แนบเนียนและน่าเชื่อถือมากขึ้น โดยอาชญากรอาจแสดงตนเป็นเจ้าหน้าที่รัฐ บุคคลมีชื่อเสียง หรือสมาชิกครอบครัวของเหยื่อ ผ่านสื่อปลอมในรูปแบบเสียง ภาพ หรือวิดีโอ โดยดำเนินการผ่านอินเทอร์เน็ตเป็นหลัก ทำให้สามารถเข้าถึงเหยื่อได้จำนวนมากภายในระยะเวลาอันสั้น โดยเฉพาะกลุ่มเสี่ยง เช่น ผู้สูงอายุ หรือผู้ที่ไม่คุ้นชินกับเทคโนโลยี ที่สำคัญคือ แม้ความเสียหายจะมีมูลค่าสูงและก่อให้เกิดผลกระทบต่อระบบดิจิทัลในวงกว้าง แต่กฎหมายอาญาของไทยยังไม่มีบทบัญญัติที่กำหนดความผิด หรือเหตุเพิ่มโทษสำหรับการฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์ไว้โดยเฉพาะ การดำเนินคดีในกรณีดังกล่าวจึงต้องอาศัยบทบัญญัติเก่าที่มีอยู่เดิม ได้แก่ ประมวลกฎหมายอาญามาตรา 342(1) หรือมาตรา 343 วรรคสอง ประกอบมาตรา 342 แล้วแต่กรณี รวมถึงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 14(1) ซึ่งยังไม่สามารถรองรับความซับซ้อนและความร้ายแรงของพฤติกรรมที่ใช้เทคโนโลยีปัญญาประดิษฐ์เป็นเครื่องมือในการกระทำความผิดได้อย่างมีประสิทธิภาพ

งานวิจัยนี้จึงมุ่งวิเคราะห์ปัญหาทางกฎหมายที่เกิดจากการที่บทบัญญัติปัจจุบันไม่สามารถรองรับการกระทำความผิดที่มีลักษณะซับซ้อนและร้ายแรงมากขึ้น ศึกษาหลักการและแนวคิดเกี่ยวกับเหตุฉกรรจ์ การกำหนดโทษทางอาญา และเปรียบเทียบกับกฎหมายของต่างประเทศ ได้แก่ สาธารณรัฐฝรั่งเศส สหรัฐอเมริกา และสหราชอาณาจักร ซึ่งมีแนวทางเฉพาะในการควบคุมการใช้เทคโนโลยี Deepfake เพื่อการแอบอ้างตัวตนหรือหลอกลวง โดยข้อเสนอสำคัญของงานวิจัยนี้ คือ การกำหนด “เหตุเพิ่มโทษ” สำหรับความผิดฐานฉ้อโกงโดยการปลอมแปลงตัวตนด้วย

ปัญญาประดิษฐ์โดยบัญญัติไว้ในบทบัญญัติเฉพาะ เช่น มาตรา 342/1 แห่งประมวลกฎหมายอาญา เพื่อให้สามารถยกระดับการฉ้อโกงในลักษณะดังกล่าวเป็นความผิดที่มีลักษณะร้ายแรง พร้อมเพิ่มอัตราโทษให้เหมาะสม ซึ่งจะช่วยให้กฎหมายไทยมีความทันสมัย สอดคล้องกับสถานการณ์จริง และสามารถป้องกัน ปราบปราม และยับยั้งอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพ อันจะนำไปสู่ความเป็นธรรมและความสงบเรียบร้อยในสังคมโดยรวม

คำสำคัญ: การฉ้อโกง, การปลอมแปลงตัวตน, ปัญญาประดิษฐ์, เหตุฉกรรจ์

Abstract

Recent developments in communication technology, especially in the field of artificial intelligence (“AI”), have paved the way for a new generation of tools capable of producing images, audio, and video with striking realism. These breakthroughs have upended traditional criminal methods, notably in the area of artificial intelligence in identity fraud. Criminals are now harnessing AI to craft fake identities with remarkable precision, thereby undermining well-established mechanisms for deterrence, prevention, and prosecution. Many offenders have honed their technical skills and are primarily motivated to unlawfully secure assets or benefits; as a result, victims not only suffer direct harm, but the economic system, national security, and public trust in digital transactions also face destabilizing pressures. The natural complexity of these modern technologies, paired with their low cost of replication and the capacity for anonymous online operation, only serves to complicate efforts to track and capture those responsible, intensifying the adverse impact on society.

Fraud and identity fraud are evolving as a form of economic crime. While traditional deceptive practices often depended on relatively simple schemes, the integration of AI now confers an air of authenticity and heightened complexity upon the forgeries. Offenders can assume the identities of government officials, celebrities, or even close family members by using artificially generated sounds, images, or video, methods that are primarily disseminated over the internet. This rapid and far-reaching approach to deception tends to target vulnerable groups, such as the elderly or individuals with limited digital savvy. Critically, even though the financial repercussions are increasingly severe and the ripple effects on digital systems are profound, Thai criminal law still lacks specific provisions that directly address the use of AI in identity fraud or that outline appropriate aggravating factors. Currently, authorities rely on existing legal measures such as

Section 342(1) or Section 343 Paragraph 2 in combination with Section 342 of the Criminal Code, as the case may be, along with Section 14(1) of the Computer-Related Crimes Act, B.E. 2560 (2017), which remain inadequate for capturing the full extent and gravity of crimes that employ AI as a tool.

This research sets out to scrutinize the legal challenges emerging from the limitations of current statutory frameworks in handling the increasingly intricate and severe spectrum of AI-enabled identity fraud. The analysis delves into the underlying principles that guide the imposition of aggravating circumstances in criminal penalties, while also offering a comparative look at the legal systems in France, the United States, and the United Kingdom, jurisdictions that have introduced tailored measures to address the misuse of deepfake technology for fraudulent impersonation. The principal recommendation advanced by this study is the introduction of a dedicated legal provision that would establish explicit aggravating factors for Artificial Intelligence in Identity Fraud by adding a new subsection (for example, Section 342/1 of the Criminal Code). Such reform is envisioned to reclassify these offenses as more serious, with penalties that appropriately reflect their heightened danger, thereby ensuring that Thai law remains up to date with contemporary realities and is more effective in preventing, controlling, and deterring technology-driven criminal conduct, all in the service of maintaining justice and social order.

Keywords: Identity Fraud, Artificial Intelligence, Aggravating Factors

1. บทนำ

การกำหนดบทลงโทษในทางอาญามีรากฐานจากแนวคิดเรื่อง “ความสมควรลงโทษ” ซึ่งสะท้อนความร้ายแรงของการกระทำที่กระทบต่อความสงบเรียบร้อยของสังคม โดยเฉพาะในกรณีที่มีเหตุฉกรรจ์ซึ่งแสดงถึงพฤติการณ์ที่รุนแรงหรือสร้างผลกระทบร้ายแรงต่อบุคคลหรือสาธารณะ การกำหนดอัตราโทษจึงต้องสอดคล้องกับระดับอันตรายที่เกิดขึ้น ซึ่งมีเป้าหมายทั้งในเชิงตอบโต้ ยับยั้ง และป้องกันการกระทำผิดตามแนวคิดของ Classical School, Deterrence Theory และ Utilitarianism

ในบริบทปัจจุบัน เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence – AI) ได้เปลี่ยนแปลงรูปแบบของอาชญากรรม โดยเฉพาะการฉ้อโกงผ่านการปลอมแปลงตัวตน ซึ่งผู้กระทำความผิดสามารถใช้ AI สร้างเสียง ภาพหรือวิดีโอปลอมได้อย่างสมจริง เช่น Deepfake หรือ Voice Cloning เพื่อนำไปหลอกลวงให้โอนเงินหรือให้ข้อมูลสำคัญ โดยการกระทำผ่านระบบอิเล็กทรอนิกส์และอินเทอร์เน็ตสามารถดำเนินการได้อย่างรวดเร็ว เข้าถึงเหยื่อได้

จำนวนมาก และหลบเลี่ยงการตรวจจับได้ง่าย ก่อให้เกิดความเสียหายต่อทรัพย์สิน ความเชื่อมั่นของประชาชน และระบบเศรษฐกิจในวงกว้าง

แม้ประเทศไทยจะมีกฎหมายอาญาและกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ที่กำหนดความผิดฐานฉ้อโกงไว้ เช่น ประมวลกฎหมายอาญา มาตรา 341–348 และพระราชบัญญัติคอมพิวเตอร์ฯ มาตรา 14(1) และ 16 แต่กฎหมายดังกล่าวไม่ได้บัญญัติถึงการปลอมแปลงตัวตนด้วย AI ไว้อย่างเฉพาะเจาะจง อีกทั้งอัตราโทษที่มีอยู่ยังไม่สะท้อนถึงขนาดของความเสียหายหรือจำนวนผู้เสียหายได้เพียงพอ จึงไม่สามารถข่มขู่หรือยับยั้งผู้กระทำผิดได้อย่างมีประสิทธิภาพ ยิ่งเมื่อพิจารณาว่าเทคโนโลยี AI มีต้นทุนต่ำและสามารถนำไปใช้ซ้ำได้อย่างกว้างขวาง โอกาสในการเกิดความเสียหายจึงมีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง

คดีตัวอย่างที่เกิดขึ้นในประเทศไทย เช่น การใช้ AI ปลอมแปลงใบหน้าและเสียงเพื่อแสดงตนเป็นเจ้าหน้าที่รัฐ โทรหลอกเหยื่อให้โอนเงิน หรือปลอมเสียงของบุคคลในครอบครัวเพื่อหลอกยืมเงิน ล้วนสะท้อนถึงความสามารถของ AI ในการหลอกลวงอย่างแนบเนียน และแสดงให้เห็นถึงข้อจำกัดของกฎหมายในการรับมือกับอาชญากรรมยุคดิจิทัล นอกจากนี้ บทบัญญัติว่าด้วยเหตุฉกรรจ์ในกฎหมายไทย เช่น มาตรา 342 แห่งประมวลกฎหมายอาญา ยังเน้นเฉพาะการแสดงตนเป็นผู้อื่นหรืออาศัยความอ่อนแอของผู้ถูกหลอก โดยไม่พิจารณาถึงขนาดของความเสียหายหรือการใช้เทคโนโลยีขั้นสูง

ยิ่งไปกว่านั้น ความผิดฐานฉ้อโกงดังกล่าวมักกระทำอย่างเป็นระบบ ข้ามพรมแดน และซ่อนร่องรอยได้ดี จึงมีอัตราการจับกุมและลงโทษต่ำ ผู้กระทำความผิดจำนวนมากจึงไม่เกรงกลัวต่อโทษทางกฎหมาย และเห็นว่าความเสี่ยงในการถูกจับต่ำกว่าผลประโยชน์ที่ได้รับ

จากปัญหาดังกล่าว ทำให้เห็นว่า กฎหมายอาญาและกฎหมายคอมพิวเตอร์ของไทยยังไม่สามารถรองรับพฤติการณ์ความผิดแบบใหม่ที่เกิดขึ้นจากการใช้ AI ได้อย่างมีประสิทธิภาพและเป็นธรรม ความจำเป็นในการพิจารณาปรับปรุงกฎหมายให้สอดคล้องกับสภาพสังคมปัจจุบันจึงเป็นเรื่องเร่งด่วน ทั้งในด้านการบัญญัติฐานความผิดใหม่หรือการกำหนดเหตุเพิ่มโทษอย่างเหมาะสม สอดคล้องกับบทบัญญัติตามรัฐธรรมนูญ มาตรา 77 ที่กำหนดให้รัฐใช้โทษอาญาเฉพาะในกรณีที่มีความร้ายแรงและเพื่อประโยชน์สาธารณะโดยแท้จริง

2. หลักกฎหมายแนวคิดและทฤษฎีที่เกี่ยวข้องกับการฉ้อโกง โดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์

การฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์ (Artificial Intelligence – AI) เป็นปรากฏการณ์อาชญากรรมสมัยใหม่ที่มีลักษณะซับซ้อนและยากต่อการรับมือด้วยแนวทางทางกฎหมายแบบเดิม บทนี้จึงมุ่งอธิบายพื้นฐานทางทฤษฎีและแนวคิดสำคัญที่เกี่ยวข้อง ทั้งในด้านกฎหมายอาญาและเทคโนโลยี AI เพื่อวางรากฐานสำหรับการเสนอแนะแนวทางการปรับปรุงกฎหมายในบทถัดไป

2.1 แนวคิดและทฤษฎีทางกฎหมายอาญา

1) ความรับผิดทางอาญาและนิติสมบัติ แนวคิดพื้นฐานในการกำหนดความรับผิดทางอาญาต้องตั้งอยู่บนหลักการที่ว่ากฎหมายอาญามีไว้เพื่อคุ้มครอง “นิติสมบัติ” เช่น ชีวิต ร่างกาย และทรัพย์สิน โดยแนวคิดของ Prof. Claus Roxin[3] ได้เสนอให้กฎหมายอาญาเป็นมาตรการสุดท้าย (ultima ratio) ที่ใช้เฉพาะเมื่อกฎหมายประเภทอื่นไม่สามารถคุ้มครองสิทธิเหล่านั้นได้อย่างเพียงพอ

2) หลักความชอบด้วยกฎหมายและการได้สัดส่วนของโทษ หลัก nullum crimen, nulla poena sine lege เป็นหลักประกันว่าความผิดและโทษต้องกำหนดไว้ล่วงหน้าในกฎหมาย และต้องตีความอย่างเคร่งครัด นอกจากนี้ หลักความได้สัดส่วน (proportionality) ยังเน้นว่าบทลงโทษต้องสอดคล้องกับความร้ายแรงของพฤติกรรม ซึ่งได้รับการสนับสนุนโดยทฤษฎีสำคัญ เช่น

- ทฤษฎีเจตจำนงอิสระ[4]: เน้นการรับผิดตามเจตนาและการเลือกกระทำของผู้กระทำผิด
- ทฤษฎีอรรถประโยชน์นิยม[5]: พิจารณาบทลงโทษเพื่อผลประโยชน์สูงสุดของสังคม
- ทฤษฎีการลงโทษเพื่อข่มขู่ยับยั้ง[6]: มุ่งลดการกระทำผิดซ้ำโดยการข่มขู่ทางกฎหมาย

3) ประเภทของความผิดอาญาและการดำเนินคดี ในระบบกฎหมายไทย ความผิดแบ่งเป็น “อาญาแผ่นดิน” และ “อันยอมความได้” ซึ่งมีผลต่ออำนาจการดำเนินคดีของรัฐ ความผิดฐานฉ้อโกงโดยการปลอมแปลงตัวตนด้วย AI แม้ปัจจุบันจะเป็นความผิดอันยอมความได้ (ตามมาตรา 348) แต่ด้วยลักษณะการกระทำที่รุนแรงและกระทบสาธารณะในวงกว้าง จึงมีข้อเสนอให้ยกระดับเป็นความผิดอาญาแผ่นดิน

4) หลักการลงโทษทางอาญา[7] การลงโทษในระบบกฎหมายมีทั้งบทบัญญัติของฝ่ายนิติบัญญัติ และการปรับใช้ของฝ่ายตุลาการ โดยการคำนึงถึงเหตุภาววิสัยในการลงโทษ[8] (ความเสียหายที่เกิดขึ้น) และการคำนึงถึงเหตุอัตวิสัยในการลงโทษ[9] (พฤติการณ์ของผู้กระทำ)

5) แนวคิดที่ต้องรับโทษหนักขึ้นเนื่องจากฉกรรจ์[10] สำหรับพฤติการณ์ที่ร้ายแรงเป็นพิเศษ การเพิ่มโทษจากเหตุฉกรรจ์สะท้อนหลักความได้สัดส่วนของโทษกับความร้ายแรงของพฤติการณ์แห่งการกระทำ โดยเฉพาะในกรณีที่มีเจตนาเลวร้ายหรือผลกระทบรุนแรง โดย Beccaria เสนอว่า[11]บทลงโทษควรหนักขึ้นเมื่อการกระทำนั้นละเมิดต่อความสงบของสังคมในระดับสูง โดยในกฎหมายไทย แนวคิดนี้ปรากฏในมาตรา 342 แห่งประมวลกฎหมายอาญา ที่เพิ่ม

---

[3] สุรสิทธิ์ แสงวิโรจนพัฒน์, “หลักเกณฑ์การกำหนดความผิดทางอาญาตามกฎหมายต่างประเทศ,” เล่มที่ 77 บทบัณฑิตย์ นิตยสารของเนติบัณฑิตยสภา, น. 125, 128 (เมษายน-มิถุนายน 2564).

[4] อัจฉรียา ชูตินันทน์, อาจชญาวิทยาและทัณฑวิทยา, พิมพ์ครั้งที่ 5 (กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2566), น. 218.

[5] *เพิ่งอ้าง*, น. 237.

[6] *เพิ่งอ้าง*, น. 238.

[7] ปกป้อง ศรีสนิท, กฎหมายอาญาชั้นสูง, พิมพ์ครั้งที่ 4 (กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2566), น. 227.

[8] *เพิ่งอ้าง*, น. 231.

[9] *เพิ่งอ้าง*, น. 227-233.

[10] ชยธร วิชาโคตร, “ปัญหากฎหมายเกี่ยวกับความผิดฐานฉ้อโกง,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2552), น. 140.

[11] *เพิ่งอ้าง*, น. 140.

โทษกรณีแสดงตนเป็นผู้อื่นหรืออาศัยความอ่อนแอของผู้เสียหาย ถือเป็นการใช้เหตุฉกรรจ์เพื่อสะท้อนระดับความอันตรายของผู้กระทำและป้องกันมิให้เกิดการกระทำซ้ำ

2.2 แนวคิดเกี่ยวกับปัญญาประดิษฐ์และบทบาทในอาชญากรรม

ในยุคที่เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) พัฒนาไปอย่างรวดเร็ว ระบบต่าง ๆ ที่สามารถเลียนแบบกระบวนการคิดและพฤติกรรมของมนุษย์ได้ถูกนำมาใช้ในชีวิตประจำวันอย่างกว้างขวาง ทั้งในการสื่อสาร การแพทย์ การคมนาคม รวมถึงการรักษาความปลอดภัย จะเห็นว่ามนุษย์พึ่งพาและใช้ประโยชน์จากปัญญาประดิษฐ์อย่างมาก[12]อย่างไรก็ตาม เทคโนโลยีเดียวกันนี้กลับถูกนำไปใช้ในทางที่ผิด เช่น การปลอมแปลงตัวตนเพื่อหลอกลวงเหยื่อผ่านโลกออนไลน์ ซึ่งก่อให้เกิด “อาชญากรรมทางเทคโนโลยี” รูปแบบใหม่ที่กฎหมายแบบดั้งเดิมยังไม่สามารถรองรับได้อย่างมีประสิทธิภาพ

1) ความหมายและคุณลักษณะของปัญญาประดิษฐ์

AI (Artificial Intelligence) แปลเป็นภาษาไทยได้ว่า “ปัญญาประดิษฐ์” คือความสามารถของ เครื่องจักรที่เลียนแบบพฤติกรรมความฉลาดหรือปัญญาจากมนุษย์ โดยการจำลองพฤติกรรมของ มนุษย์ผนวกกับกระบวนการประมวลผลความรู้ความเข้าใจของคอมพิวเตอร์[13] AI จึงเป็นเทคโนโลยีที่ทำให้ระบบคอมพิวเตอร์สามารถเลียนแบบความสามารถทางปัญญาของมนุษย์ เช่น การคิด วิเคราะห์ เรียนรู้จากข้อมูล หรือแม้แต่การตัดสินใจด้วยตนเองโดยไม่ต้องมีการสั่งงานแบบตายตัวในทุกขั้นตอน

จากเดิมที่ AI เคยถูกมองว่าเป็นเรื่องไกลตัวหรือมีอยู่เพียงในนิยายวิทยาศาสตร์ ปัจจุบันกลับกลายเป็นเทคโนโลยีที่แทรกซึมอยู่ในชีวิตประจำวันของคนทั่วไปอย่างแนบเนียน ไม่ว่าจะเป็นระบบช่วยแนะนำเนื้อหาในแอปดูหนังหรือโซเชียลมีเดีย, ระบบปลดล็อกใบหน้าบนโทรศัพท์มือถือ, หรือแม้แต่เสียงพูดตอบกลับจากผู้ช่วยเสมือน เช่น Siri หรือ Google Assistant ล้วนเป็นตัวอย่างของ AI ที่ใช้งานจริงและแพร่หลายอยู่รอบตัวเราทุกวัน

อย่างไรก็ตาม ความสามารถอันชาญฉลาดของ AI ที่ถูกพัฒนาขึ้นเพื่ออำนวยความสะดวกแก่ผู้คน ก็เปรียบเสมือนดาบสองคม เมื่อถูกนำไปใช้ในทางที่ผิด โดยเฉพาะในรูปแบบของปัญญาประดิษฐ์ที่เรียกว่า Deepfake ซึ่งเป็นหนึ่งในรูปแบบของ AI ที่น่ากังวลมากที่สุดในเชิงอาชญากรรม โดยเป็น AI ที่สามารถสร้างใบหน้า เสียง และตัวตน ที่สังเคราะห์ใหม่ขึ้นมาเป็นอัตลักษณ์ของบุคคลอื่น หรือตามแต่ที่ผู้ใช้ต้องการได้อย่างแนบเนียนจนยากที่จะแยกความจริงออกจากของปลอม โดย AI ชนิดนี้ มักมีการนำไปใช้ในอุตสาหกรรมความบันเทิง รวมถึงสื่อดิจิทัลที่สร้างสรรค์ต่าง ๆ เช่น ฟิลเตอร์หน้าใสในวีดีโอคอล โปรแกรมเปลี่ยนเสียง แอปสลับใบหน้า เป็นต้น แต่เมื่อผู้กระทำผิดเล็งเห็นความสามารถของ AI ชนิดนี้ จึงกลับกลายเป็นเครื่องมือสำคัญของผู้กระทำผิดในการแอบอ้างตัวตนบุคคล

---

[12] อารีย์น่าร์ อาแว และ ภาณุวัฒน์ นนท์ตุลา, “ปัญหาทางกฎหมายเรื่องความรับผิดทางเสียหายที่ปัญญาประดิษฐ์ก่อขึ้น,” วารสารกฎหมายและสังคมรังสิต, ปีที่ 5, ฉบับที่ 1, น. 31, 31 (มกราคม - เมษายน 2566).

[13] เหมือน สุขมาตย์, “ความรับผิดทางอาญาของปัญญาประดิษฐ์,” วารสารนิติศาสตร์ มหาวิทยาลัยราชภัฏอุบลราชธานี, ปีที่ 7, ฉบับที่ 2, น. 37, 38 (กรกฎาคม - ธันวาคม 2562).

อื่น เพื่อหลอกลวงหรือฉ้อโกงในรูปแบบใหม่ที่อาศัยความแนบเนียนเป็นจุดแข็ง และสร้างความเสียหายได้ในวงกว้าง โดยเฉพาะเมื่อผสานกับช่องทางสื่อสารออนไลน์ที่รวดเร็วและเข้าถึงได้ง่าย เช่น การเปลี่ยนใบหน้าของบุคคลหนึ่งในวิดีโอต่าง ๆ รวมถึงวีดีโอคอลให้กลายเป็นอีกคน หรือการสร้างสังเคราะห์เสียงพูดเป็นเสียงพูดของผู้อื่น เช่น บุคคลที่มีชื่อเสียง เจ้าหน้าที่ตำรวจ[14] หรือแม้กระทั่งคนในครอบครัวของเหยื่อ[15]มาทำการหลอกลวงเหยื่อให้โอนเงิน เป็นต้น

ความสามารถในการจำลองตัวตนบุคคลได้อย่างแนบเนียนนี้ ส่งผลให้ AI ไม่ได้เป็นเพียงเครื่องมือทางวิทยาการ แต่กลายเป็น เครื่องมือทางอาญา ที่ผู้กระทำผิดใช้เพื่อจงใจก่อให้เกิดความเข้าใจผิด หลอกลวง และแสวงหาผลประโยชน์โดยมิชอบในลักษณะที่เกินกว่าศักยภาพของเทคโนโลยีแบบเก่า รวมถึงปกปิดตัวตนเพื่อให้ยากต่อการจับกุม ปัจจุบันมีรูปแบบของการหลอกลวงหลายกรณี สำหรับบทความนี้จึงวิเคราะห์ถึงรูปแบบการปลอมแปลงที่เกี่ยวข้องกับการฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์

2) รูปแบบของการปลอมแปลงฉ้อโกงโดยปลอมแปลงตัวตนด้วย AI

AI ได้รับการประยุกต์ใช้ในการฉ้อโกงโดยการปลอมแปลงตัวตนในหลายรูปแบบ ซึ่งล้วนมีจุดร่วมคือ ความสมจริง ความแนบเนียน และการเข้าถึงเหยื่อในวงกว้าง โดยสามารถจำแนกรูปแบบสำคัญได้ 3 ประเภทหลัก ดังนี้

ก. การปลอมแปลงวิดีโอ (Deepfake): ผู้กระทำผิดใช้วิดีโอปลอมที่แสดงภาพบุคคลมีชื่อเสียง หรือเจ้าหน้าที่รัฐ เพื่อสร้างความน่าเชื่อถือในการขอข้อมูลหรือเงิน เช่น การปลอมวิดีโอคอลเป็นตำรวจหลอกให้เหยื่อโอนเงิน

ข. การสร้างตัวตนปลอม (Synthetic Identities): ใช้ AI สร้างภาพใบหน้าหรือบัญชีโซเชียลมีเดียของบุคคลที่ไม่มีตัวตนอยู่จริง เพื่อเปิดบัญชีธนาคาร หรือหลอกให้เหยื่อเชื่อว่ากำลังติดต่อกับบุคคลนั้นจริง ๆ

ค. การปลอมแปลงเสียงและเอกสารดิจิทัล: เทคโนโลยีเลียนแบบเสียงสามารถใช้โทรหลอกลวง เช่น แอบอ้างเป็นญาติผู้เสียหาย หรือปลอมแปลงเอกสารทางราชการเพื่อสมัครบริการทางการเงิน เป็นต้น

แนวโน้มดังกล่าวสะท้อนให้เห็นว่า AI ได้เปลี่ยนบทบาทจากการเป็นผู้ช่วยของมนุษย์ไปสู่การเป็นเครื่องมือของการแอบอ้างและหลอกลวง ที่ทรงพลังในบริบทของอาชญากรรม โดยเฉพาะการฉ้อโกงผ่านโลกดิจิทัล ซึ่งถือเป็นหัวใจสำคัญของปัญหาที่บทความนี้มุ่งวิเคราะห์และเสนอแนวทางทางกฎหมายเพื่อรับมืออย่างเป็นระบบ

3) บทบัญญัติกฎหมายไทยที่เกี่ยวข้อง

แม้ในปัจจุบันกฎหมายไทยยังไม่มีบทบัญญัติเฉพาะที่กำหนดความผิดเกี่ยวกับการฉ้อโกงโดยใช้ปัญญาประดิษฐ์โดยตรง แต่สามารถประยุกต์ใช้กฎหมายที่มีอยู่เดิมเพื่อดำเนินคดีกับผู้กระทำความผิดในบางกรณีได้ โดยเฉพาะในกรณีที่มีการปลอมแปลงตัวตนหรือข้อมูลเพื่อแสวงหาประโยชน์ทางทรัพย์สิน ซึ่งเกี่ยวข้องกับกฎหมายสำคัญดังต่อไปนี้

ก. ประมวลกฎหมายอาญา

[14] ไทยพีบีเอสนิวส์, “จับแก๊งคอลเซ็นเตอร์ รับบทตำรวจปลอมผ่านเอไอ,” สืบค้นเมื่อวันที่ 5 กรกฎาคม 2568, จาก https://youtu.be/1rSETal8ab8.

[15] ข่าวช่องวัน. “เตือนภัย! โทรปลอมเสียงคนในครอบครัวหลอกโอนเงิน,” สืบค้นเมื่อวันที่ 5 กรกฎาคม 2568, จาก https://youtu.be/9Sri6s8qPZ0.

มาตรา 341 กำหนดความผิดฐานฉ้อโกง โดยบัญญัติว่าผู้ใดกระทำโดยทุจริตหรือหลอกลวงผู้อื่นด้วยข้อความอันเป็นเท็จ หรือปกปิดข้อความจริง ซึ่งควรต้องบอก แล้วเอาทรัพย์สินของผู้อื่นไป ถือเป็นความผิดทางอาญา

มาตรา 342 บัญญัติเพิ่มโทษสำหรับกรณีฉ้อโกงที่มีลักษณะเป็นเหตุฉกรรจ์ ได้แก่ แสดงตนเป็นคนอื่น และอาศัยความปัญญาของผู้ถูกหลอกลวงซึ่งเป็นเด็กหรืออาศัยความอ่อนแอจิตของผู้ถูกหลอกลวง

มาตรา 343 กำหนดให้ความผิดฐานฉ้อโกงที่กระทำต่อประชาชนทั่วไปหรือประชาชนจำนวนมาก เป็นความผิดที่มีโทษร้ายแรงกว่าการฉ้อโกงทั่วไป

มาตรา 348 บัญญัติให้ความผิดฐานฉ้อโกงเป็นความผิดอันยอมความได้ เว้นแต่เป็นกรณีที่บัญญัติไว้ในมาตรา 343 ซึ่งเป็นความผิดอาญาแผ่นดิน

ข. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ 2 พ.ศ. 2560

มาตรา 14 วรรคหนึ่ง (1) กำหนด ห้ามนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จ โดยมีลักษณะเป็นการหลอกลวงหรืออาจก่อให้เกิดความเสียหายแก่ประชาชน

มาตรา 16 กำหนด ห้ามนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งภาพของบุคคลที่ถูกตัดต่อหรือดัดแปลง โดยมีลักษณะที่อาจทำให้เจ้าของภาพเสียหายหรืออับอาย

ค. กฎหมายอื่นที่เกี่ยวข้อง

การปลอมแปลงตัวตนด้วย AI ยังอาจละเมิดกฎหมายอื่น เช่น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA), พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ แต่กฎหมายทั้งสองฉบับดังกล่าวไม่ได้มีบทบัญญัติที่กล่าวถึงการฉ้อโกงและความเสียหายเชิงทรัพย์สินโดยตรง โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะมุ่งเน้นไปที่การคุ้มครองข้อมูลส่วนบุคคล และ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ จะมุ่งเน้นไปที่ความน่าเชื่อถือของข้อมูลทางอิเล็กทรอนิกส์มากกว่า กฎหมายทั้งสองฉบับเหล่านี้จึงไม่ใช่กฎหมายหลักในความผิดฐานนี้ แต่เป็นกฎหมายเสริมที่ศาลสามารถนำกฎหมายเหล่านี้มาปรับใช้ร่วมกับกฎหมายอาญาและกฎหมายคอมพิวเตอร์เพื่อเพิ่มโทษหรือขยายขอบเขตความผิดในคดีนั้นๆได้

อย่างไรก็ดี กฎหมายเหล่านี้ยังไม่สามารถรับมือกับลักษณะเฉพาะของการฉ้อโกงโดยใช้ AI ได้อย่างครอบคลุม จึงมีความจำเป็นในการบัญญัติกฎหมายเฉพาะเพื่อให้สอดรับกับภัยคุกคามทางเทคโนโลยีในยุคปัจจุบัน

3. ความผิดฐานฉ้อโกงโดยการปลอมแปลงตัวตนตามกฎหมายของต่างประเทศ

แม้การฉ้อโกงโดยใช้ AI จะเป็นภัยคุกคามรูปแบบใหม่ แต่ก็เป็นปัญหาสากลที่หลายประเทศเผชิญร่วมกัน บทบัญญัติกฎหมายในหลายระบบและหลายประเทศ จึงได้พัฒนาแนวทางเพื่อตอบโต้การปลอมแปลงตัวตนผ่านเทคโนโลยี เช่น Deepfake และการสร้างข้อมูลเทียม บทนี้มุ่งศึกษากฎหมายที่เกี่ยวข้องจากฝรั่งเศส สหรัฐอเมริกา และสหราชอาณาจักร เพื่อแสดงให้เห็นถึงแนวทางการรับมือของประเทศต่าง ๆ ที่สามารถนำมาเป็นบทเรียนสำหรับการพัฒนากฎหมายไทยในบทต่อไป

3.1 สาธารณรัฐฝรั่งเศส

สาธารณรัฐฝรั่งเศสใช้ระบบกฎหมายซีวิลลอว์ ซึ่งถือหลักว่าหากไม่มีบทบัญญัติกฎหมายกำหนดไว้ การกระทำนั้นไม่ถือเป็นความผิด แม้ยังไม่มีกฎหมายเฉพาะเกี่ยวกับการฉ้อโกงโดยใช้ปัญญาประดิษฐ์ (AI) แต่กฎหมายที่มีอยู่สามารถบังคับใช้กับพฤติกรรมลักษณะดังกล่าวได้

1) ความผิดฐานฉ้อโกง

มาตรา 313-1[16] แห่ง Code pénal บัญญัติความผิดฐานฉ้อโกงไว้ว่า การหลอกลวงบุคคลโดยใช้ชื่อปลอม แสดงความสามารถอันเป็นเท็จ หรือการปิดบังฐานะที่แท้จริง หรือใช้วิธีมิชอบด้วยกฎหมาย เพื่อให้ผู้อื่นหลงเชื่อและโอนทรัพย์สิน ถือเป็นความผิด มีโทษจำคุก 5 ปี และปรับ 375,000 ยูโร

มาตรา 313-2[17] เพิ่มโทษเมื่อกระทำต่อกลุ่มเปราะบาง โดยเจ้าหน้าที่รัฐ หรือในนามองค์กร เช่น องค์กรการกุศล หรือหากกระทำในรูปแบบองค์กรอาชญากรรม โทษสูงสุดคือจำคุก 10 ปี และปรับ 1,000,000 ยูโร

มาตรา 313-3[18] กำหนดให้การพยายามกระทำผิดต้องรับโทษเช่นเดียวกับความผิดสำเร็จ

2) ความผิดฐานแอบอ้างตัวตน

---

[16] Penal Code Section 1: Fraud Article 313-1

Fraudulent obtaining is the act of deceiving a natural or legal person by the use of a false name or a fictitious capacity, by the abuse of a genuine capacity, or by means of unlawful manoeuvres, thereby to lead such a person, to his prejudice or to the prejudice of a third party, to transfer funds, valuables or any property, to provide a service or to consent to an act incurring or discharging an obligation.

Fraudulent obtaining is punished by five years' imprisonment and a fine of €375,000.

[17] The penalties are increased to seven years' imprisonment and a fine of 750,000 euros when the fraud is committed:

1. By a person holding public authority or entrusted with a public service mission, in the exercise or on the occasion of the exercise of their functions or mission;

2. By a person who wrongfully assumes the status of a person holding public authority or entrusted with a public service mission;

3. By a person who solicits the public for the issuance of securities or for the collection of funds for humanitarian or social assistance purposes;

4. To the detriment of a person whose particular vulnerability, due to their age, illness, infirmity, physical or mental impairment, or pregnancy, is apparent or known to the perpetrator; 4 bis to the detriment of a person subjected to psychological or physical coercion, within the meaning of Article 223-15-3, and whose condition is known to the perpetrator;

5. To the detriment of a public entity, a social protection organization, or an entity entrusted with a public service mission, for the purpose of obtaining an allowance, benefit, payment, or undue advantage.

The penalties are increased to ten years' imprisonment and a fine of 1,000,000 euros when the fraud is committed as part of an organized group.

[18] Code pénal Article 313-3 (paragraph 1)

Attempt to commit the offences set out under this section of the present code is subject to the same penalties.

The provisions of article 311-12 are applicable to the misdemeanour of fraudulent obtaining.

มาตรา 226-4-1 บัญญัติว่า การแอบอ้างเป็นบุคคลอื่นหรือใช้ข้อมูลที่สามารถระบุตัวบุคคลได้ โดยเจตนาเพื่อรบกวนความสงบสุขหรือทำให้เสียชื่อเสียง ต้องระวางโทษจำคุก 1 ปี และปรับ 15,000 ยูโร และหากกระทำผ่านเครือข่ายออนไลน์ก็มีโทษเท่ากัน

3) ความผิดเกี่ยวกับอาชญากรรมไซเบอร์

มาตรา 323-3[19] กำหนดว่า การแทรกแซงข้อมูลในระบบประมวลผลอัตโนมัติ เช่น การนำเข้าสู่ระบบ แก้ไข ส่งข้อมูลโดยฉ้อฉล การสกัด การถือครอง การทำซ้ำ การส่ง การลบ หรือการฉ้อฉลแก้ไขข้อมูลที่มีอยู่ มีโทษจำคุก 5 ปี และปรับ 150,000 ยูโร และหากเป็นระบบของรัฐ โทษจะเพิ่มเป็นจำคุก 7 ปี และปรับ 300,000 ยูโร

3.2 สหรัฐอเมริกา

แม้สหรัฐอเมริกาจะยังไม่มีกฎหมายเฉพาะสำหรับการฉ้อโกงโดยใช้ AI แต่กฎหมายที่มีอยู่สามารถนำมาใช้ดำเนินคดีได้ โดยเฉพาะกฎหมายของรัฐบาลกลาง ได้แก่

1) กฎหมายว่าด้วยการฉ้อโกง (Federal Fraud Statutes)

- Wire Fraud (18 U.S.C. § 1343)[20]

กำหนดโทษสำหรับการใช้ระบบสื่อสารอิเล็กทรอนิกส์ เช่น โทรศัพท์ อีเมล หรือวิดีโอคอล เพื่อหลอกลวงให้ผู้อื่นโอนทรัพย์สิน โดยมีองค์ประกอบ ได้แก่ (1) มีแผนฉ้อโกง, (2) ใช้การสื่อสารทางอิเล็กทรอนิกส์, และ (3) เกิดความเสียหายต่อทรัพย์สิน

เนื่องจากการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์ (AI) มักใช้ผ่านระบบสื่อสารออนไลน์ จึงเข้าข่ายความผิดนี้ โดยมีโทษสูงสุดจำคุก 20 ปี และอาจเพิ่มเป็น 30 ปีหากเกี่ยวข้องกับสถาบันการเงินหรือหน่วยงานของรัฐ

2) กฎหมายว่าด้วยการปลอมแปลงตัวตน (Identity Theft Laws)

---

[19] Code pénal Article 323-3

Fraudulently introducing data into an automated processing system, extracting, holding, reproducing, transmitting, deleting, or fraudulently modifying the data it contains is punishable by five years' imprisonment and €150,000 fine.

When this offense has been committed against an automated personal data processing system implemented by the State, the penalty is increased to seven years' imprisonment and a fine of €300,000.

[20] 18 U.S.C. § 1343

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation occurs in relation to, or involving any benefit authorized, transported, transmitted, transferred, disbursed, or paid in connection with, a presidentially declared major disaster or emergency (as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122)), or affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

- Identity Theft (18 U.S.C. § 1028)

ครอบคลุมการปลอมแปลง สร้าง หรือใช้ข้อมูลระบุตัวตนของผู้อื่น เช่น บัตรประชาชนหรือใบขับขี่ เพื่อฉ้อโกง ปัญญาประดิษฐ์ที่ใช้สร้างภาพหรือเสียงปลอม (deepfake) เพื่อหลอกเหยื่อ เช่น ในกรณี Romance Scams ที่ผู้กระทำผิดใช้ภาพและเสียงปลอมด้วย AI หลอกเยื่อให้ตกหลุมรัก เพื่อหลอกให้ส่งเงินหรือข้อมูลส่วนตัว เข้าข่ายความผิดตามมาตรานี้

- Aggravated Identity Theft (18 U.S.C. § 1028A)

เพิ่มโทษสำหรับผู้ที่ใช้ข้อมูลระบุตัวตนของผู้อื่นโดยมิชอบ ระหว่างกระทำอาชญากรรมร้ายแรง เช่น การฉ้อโกงทางการเงิน โดยกำหนดโทษจำคุกเพิ่มอีก 2 ปี (หรือ 5 ปีหากเกี่ยวข้องกับการก่อการร้าย)

3) กฎหมายระดับมลรัฐ: แคลิฟอร์เนีย

แม้มลรัฐแคลิฟอร์เนียยังไม่มีกฎหมายเฉพาะเกี่ยวกับการใช้ AI หรือ Deepfake ในการกระทำความผิด แต่กฎหมายที่มีอยู่สามารถประยุกต์ใช้กับการปลอมแปลงตัวตนทางดิจิทัลได้ โดยเฉพาะ

มาตรา 528.5[21] แห่ง California Penal Code กำหนด ห้ามปลอมแปลงตัวตนผ่านสื่ออิเล็กทรอนิกส์เพื่อข่มขู่ คุกคาม หรือฉ้อโกง มีโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000 ดอลลาร์ หรือทั้งจำทั้งปรับ พร้อมสิทธิในการฟ้องแพ่งของผู้เสียหาย

มาตรา 530.5 แห่ง California Penal Code กำหนด ห้ามใช้ข้อมูลส่วนบุคคล เช่น ชื่อ หรือเลขประจำตัวของผู้อื่นโดยมิชอบ เพื่อวัตถุประสงค์ทางอาญา ใช้ได้เฉพาะเมื่อเหยื่อเป็นบุคคลจริง หากมีเหยื่อหลายรายหรือกระทำผิดซ้ำ โทษจะรุนแรงขึ้น

3.3 สหราชอาณาจักร

---

[21] California Code, Penal Code - PEN § 528.5

(a) Notwithstanding any other provision of law, any person who knowingly and without consent credibly impersonates another actual person through or on an Internet Web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person is guilty of a public offense punishable pursuant to subdivision (d).

(b) For purposes of this section, an impersonation is credible if another person would reasonably believe, or did reasonably believe, that the defendant was or is the person who was impersonated.

(c) For purposes of this section, “electronic means” shall include opening an e-mail account or an account or profile on a social networking Internet Web site in another person's name.

(d) A violation of subdivision (a) is punishable by a fine not exceeding one thousand dollars ($1,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(e) In addition to any other civil remedy available, a person who suffers damage or loss by reason of a violation of subdivision (a) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief pursuant to paragraphs (1), (2), (4), and (5) of subdivision (e) and subdivision (g) of Section 502.

(f) This section shall not preclude prosecution under any other law.

สหราชอาณาจักรใช้ระบบกฎหมายคอมมอนลอว์ (Common Law) หรือเป็นจารีตประเพณี (Customary) โดยรัฐสภาได้บัญญัติกฎหมายเกี่ยวกับความผิดฐานฉ้อโกงมาตั้งแต่ปี ค.ศ. 1757 ซึ่งต่อมาได้มีการปรับปรุงแก้ไขและพัฒนาเรื่อยมา อย่างไรก็ตาม การฉ้อโกงเป็นเรื่องที่ทุกคนในสังคมยอมรับว่าการกระทำเช่นนั้นเป็นการกระทำที่ต้องห้ามและขัดต่อความรู้สึกทางศีลธรรมของคนในสังคมหรือที่เรียกว่า“ ความผิดในตัวเอง”(mala in se) ในปัจจุบันรัฐสภาสหราชอาณาจักรตราพระราชบัญญัติการฉ้อโกง The Fraud Act 2006 มาใช้บังคับแทนการป้องกันและควบคุมอาชญากรรม (Criminalise)[22]

สำหรับการฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์นั้น แม้ว่าสหราชอาณาจักรจะยังไม่มีกฎหมายเฉพาะที่ว่าด้วยการกระทำผิดโดยใช้ปัญญาประดิษฐ์โดยตรง แต่กฎหมายอาญาที่มีอยู่ก็สามารถถูกนำมาใช้ดำเนินคดีกับการฉ้อโกงในลักษณะนี้ได้ โดยเฉพาะอย่างยิ่งกฎหมายที่เกี่ยวข้องกับการฉ้อโกงทางการเงินและการปลอมแปลงตัวตน ซึ่งสามารถใช้บังคับกับกรณีที่เทคโนโลยีถูกนำมาเป็นเครื่องมือในการกระทำผิด กฎหมายสำคัญที่เกี่ยวข้องในกรณีนี้ ได้แก่

1) Fraud Act 2006 กฎหมายฉบับนี้กำหนดความผิดฐานฉ้อโกงไว้ 3 ประเภท ได้แก่

มาตรา 2[23]: *Fraud by False Representation* – การแสดงข้อความเท็จโดยเจตนาเพื่อให้ได้มาซึ่งประโยชน์

มาตรา 3[24]: Fraud by Failing to Disclose Information – การละเว้นไม่เปิดเผยข้อมูลที่ควรต้องเปิดเผย

---

[22] กมลรัตน์ ภาษีผล, “ความผิดฐานฉ้อโกงในวิธีการทางอิเล็กทรอนิกส์ให้เป็นเหตุฉกรรจ์,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิต, 2566) น. 69.

[23] Fraud Act 2006 Section 2

(1) A person is in breach of this section if he—

(a) dishonestly makes a false representation, and

(b) intends, by making the representation—

(i)to make a gain for himself or another, or

(ii)to cause loss to another or to expose another to a risk of loss.

(2) A representation is false if—

(a) it is untrue or misleading, and

(b) the person making it knows that it is, or might be, untrue or misleading.

(3) “Representation” means any representation as to fact or law, including a representation as to the state of mind of—

(a) the person making the representation, or

(b) any other person.

(4) A representation may be express or implied.

(5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

[24] Fraud Act 2006 Section 3

A person is in breach of the section if he—

มาตรา 4: Fraud by Abuse of Position – การใช้อำนาจหน้าที่ในทางที่ผิดเพื่อแสวงหาประโยชน์

บทบัญญัติดังกล่าวสามารถประยุกต์ใช้กับการกระทำผิดที่ใช้ AI เป็นเครื่องมือ เช่น การปลอมแปลงตัวตนเจ้าหน้าที่รัฐผ่าน Deepfake (มาตรา 2) หรือการปกปิดตัวตนจริงผ่านเทคโนโลยีเพื่อหลอกลวงทางการเงิน (มาตรา 3) โดยกฎหมายกำหนดโทษสูงสุดจำคุก 10 ปี หรือปรับ หรือทั้งจำทั้งปรับ

2) กฎหมายอื่นที่เกี่ยวข้อง นอกเหนือจาก Fraud Act ยังมีกฎหมายเสริมที่อาจเกี่ยวข้อง ได้แก่:

Identity Documents Act 2010: กรณีการครอบครองหรือใช้เอกสารแสดงตนปลอม

Data Protection Act 2018 (มาตรา 170): กรณีการจัดเก็บหรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

Computer Misuse Act 1990: ความผิดเกี่ยวกับการเข้าถึงหรือดัดแปลงข้อมูลทางอิเล็กทรอนิกส์โดยมิชอบ

กฎหมายเหล่านี้แม้มิได้มุ่งคุ้มครองทรัพย์สินโดยตรง แต่สามารถใช้ประกอบการพิจารณาคดีกรณีที่มีการใช้ AI ในการปลอมแปลงตัวตนหรือเข้าถึงข้อมูลเพื่อประโยชน์ทางการเงินโดยมิชอบ

4. วิเคราะห์เปรียบเทียบความผิดฐานฉ้อโกงโดยการปลอมแปลงตัวตนตามกฎหมายของประเทศไทยกับของต่างประเทศ

การฉ้อโกงโดยการปลอมแปลงตัวตนเป็นอาชญากรรมทางเศรษฐกิจที่มีมานาน แต่เทคโนโลยีปัญญาประดิษฐ์ (AI) ได้เพิ่มความซับซ้อนและความแนบเนียนในการกระทำผิด ทำให้เหยื่อตกเป็นเป้าหมายได้ง่ายขึ้น แม้กรณีดังกล่าวจะเกิดขึ้นเพิ่มขึ้นในประเทศไทย แต่ยังไม่มีกฎหมายเฉพาะที่รองรับ กฎหมายไทยยังคงต้องอาศัยบทบัญญัติทั่วไปเกี่ยวกับความผิดฐานฉ้อโกง การปลอมแปลงเอกสาร และการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งยังไม่เพียงพอในการรับมือกับการฉ้อโกงโดยใช้ AI บทนี้จึงนำเสนอการวิเคราะห์กฎหมายไทยที่เกี่ยวข้อง พร้อมเปรียบเทียบกับกฎหมายของสาธารณรัฐฝรั่งเศส สหรัฐอเมริกา และสหราชอาณาจักร เพื่อชี้ให้เห็นช่องว่างทางกฎหมาย และเสนอมาตรการที่ควรปรับปรุงให้สอดคล้องกับลักษณะอาชญากรรมยุคดิจิทัล

4.1 วิเคราะห์ขอบเขตของกฎหมายไทยที่เกี่ยวข้องกับความผิดฐานฉ้อโกงโดยการปลอมแปลงตัวตนของประเทศไทย

ปัจจุบัน กฎหมายไทยยังไม่มีบทบัญญัติเฉพาะที่รองรับการฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์ (AI) โดยตรง การดำเนินคดีจึงต้องอาศัยมาตรา 342 และ 343 ของประมวลกฎหมายอาญา ซึ่งกล่าวถึงการฉ้อโกงโดยการแสดงตนเป็นคนอื่น และการฉ้อโกงประชาชน รวมถึงมาตรา 14 และ 16 ของ

(a) dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and

(b) intends, by failing to disclose the information—

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ที่เกี่ยวกับการนำข้อมูลปลอมหรือภาพที่ถูกตัดต่อเข้าสู่ระบบคอมพิวเตอร์ อย่างไรก็ดี กฎหมายดังกล่าวยังไม่ครอบคลุมลักษณะเฉพาะของการฉ้อโกงโดยใช้ AI ซึ่งมีความซับซ้อน เข้าถึงเหยื่อได้จำนวนมาก และหลีกเลี่ยงการตรวจจับได้ง่าย ส่งผลให้การบังคับใช้กฎหมายไม่มีประสิทธิภาพเพียงพอ การปรับปรุงกฎหมายให้รองรับเทคโนโลยีใหม่นี้จึงเป็นเรื่องเร่งด่วนและจำเป็น

4.2 ปัญหากฎหมายไทยเกี่ยวกับการฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์

เทคโนโลยี AI โดยเฉพาะ Deepfake และ Voice Cloning ได้กลายเป็นเครื่องมือสำคัญของอาชญากรในการปลอมแปลงตัวตนเพื่อฉ้อโกงผ่านอินเทอร์เน็ต สร้างความเสียหายทางทรัพย์สินและบั่นทอนความเชื่อมั่นในระบบดิจิทัล ตัวอย่างในไทยพบการปลอมเสียงคนในครอบครัวหลอกให้โอนเงิน[25]และการใช้วิดีโอปลอมสวมรอยเป็นตำรวจ[26]แม้กฎหมายไทย เช่น ประมวลกฎหมายอาญา มาตรา 341–348 และ พ.ร.บ.คอมพิวเตอร์ พ.ศ. 2560 มาตรา 14(1) และ 16 จะสามารถใช้บังคับกับบางกรณีได้ แต่ยังไม่มีบทบัญญัติใดที่ระบุการฉ้อโกงด้วย AI ไว้อย่างเฉพาะเจาะจง ทำให้การบังคับใช้กฎหมายไม่มีประสิทธิภาพเพียงพอในการยับยั้งอาชญากรรมที่ซับซ้อนและแพร่หลายมากขึ้น นอกจากนี้กฎหมายที่มีอยู่ยังไม่สอดคล้องกับลักษณะเฉพาะของความผิดในยุคเทคโนโลยี เช่น ความแนบเนียนในการกระทำ ความเสียหายในวงกว้าง และความยากในการติดตามตัวผู้กระทำผิด จึงจำเป็นต้องมีการปรับปรุงกฎหมายให้ครอบคลุมการฉ้อโกงโดยใช้ AI อย่างชัดเจน เพื่อให้การลงโทษได้สัดส่วนกับความร้ายแรงของความผิด และป้องกันอาชญากรรมยุคใหม่ได้อย่างมีประสิทธิภาพ

4.3 วิเคราะห์เปรียบเทียบความผิดฐานฉ้อโกงโดยการปลอมแปลงตัวตนตามกฎหมายของประเทศไทยกับต่างประเทศ

แม้แต่ละประเทศจะยังไม่มีกฎหมายเฉพาะเกี่ยวกับการฉ้อโกงโดยใช้ปัญญาประดิษฐ์ แต่ต่างก็ใช้บทบัญญัติเดิมมาปรับใช้กับกรณีดังกล่าว โดยอาศัยการตีความให้ครอบคลุมพฤติกรรมใหม่ที่เกี่ยวกับ AI และ Deepfake

ในสาธารณรัฐฝรั่งเศส การกระทำดังกล่าวอาจเข้าข่ายความผิดตาม มาตรา 313-1 ของ Code Pénal ว่าด้วยการฉ้อโกง และหากกระทำต่อกลุ่มเปราะบางหรือโดยองค์กรอาชญากรรม อาจเพิ่มโทษตาม มาตรา 313-2 นอกจากนี้ มาตรา 226-4-1 ว่าด้วยการแอบอ้างตัวตน สามารถใช้ประกอบเพื่อเพิ่มโทษได้

ในสหรัฐอเมริกา ใช้ 18 U.S.C. § 1343 (Wire Fraud) ดำเนินคดีในกรณีหลอกลวงผ่านระบบอิเล็กทรอนิกส์ รวมถึง Deepfake Fraud และใช้ § 1028 และ § 1028A กับการปลอมแปลงและใช้ข้อมูลระบุตัวตนของผู้อื่นโดยมิชอบ โดยเพิ่มโทษเมื่อกระทำร่วมกับอาชญากรรมร้ายแรง

---

[25] ข่าวช่องวัน, “แก๊งคอลฯ ปลอมเสียงเป็นลูกหลอกแม่โอนเงิน,” สืบค้นเมื่อวันที่ 5 กรกฎาคม 2568, จาก https://www.youtube.com/watch?v=nBpFS0KBdQ8

[26] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, “เตือนภัย! มิจฉาชีพใช้ AI สร้าง Deepfake หลอกลวงปลอมเป็นตำรวจ,” สืบค้นเมื่อวันที่ 5 กรกฎาคม 2568, จาก https://www.youtube.com/watch?v=766pPepQ7jY

ในมลรัฐแคลิฟอร์เนีย การปลอมแปลงตัวตนทางออนไลน์อาจผิดตาม Penal Code § 528.5 ส่วนการใช้ข้อมูลส่วนบุคคลโดยมิชอบเพื่อฉ้อโกงเข้าข่าย § 530.5 แม้ยังไม่ครอบคลุม AI โดยตรง แต่สามารถนำมาประยุกต์ใช้ได้

ในสหราชอาณาจักร แม้ไม่มีบทบัญญัติเฉพาะเกี่ยวกับ AI Fraud แต่ Fraud Act 2006 มาตรา 2, 3 และ 4 กำหนดความผิดเกี่ยวกับการแสดงข้อความเท็จ การปกปิดข้อมูล และการใช้อำนาจหน้าที่ในทางที่ผิด ซึ่งสามารถตีความครอบคลุมถึงการใช้เทคโนโลยี Deepfake เพื่อหลอกลวงได้ และอาจใช้ Computer Misuse Act 1990 เป็นกฎหมายประกอบเพิ่มเติม

ในประเทศไทย การฉ้อโกงโดยการปลอมแปลงตัวตนด้วย AI ยังต้องพึ่งพามาตรา 342 และ 343 ของประมวลกฎหมายอาญา และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 เช่น มาตรา 14 และ 16 ซึ่งยังไม่มีความเฉพาะเจาะจงและขาดความทันสมัยเมื่อเทียบกับลักษณะความผิดในยุคดิจิทัล

4.4 วิเคราะห์สถานการณ์และกรณีศึกษาในต่างประเทศที่เกี่ยวกับการฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์

การปลอมแปลงตัวตนด้วย AI เช่น deepfake ได้กลายเป็นเครื่องมือในการฉ้อโกงที่แพร่หลายในระดับสากล ตัวอย่างคดีสำคัญ เช่น กรณีในสหราชอาณาจักรและสหรัฐอาหรับเอมิเรตส์ที่มีการปลอมเสียงผู้บริหารเพื่อหลอกโอนเงินหลายล้านยูโร รวมถึงคดีในฮ่องกงที่ใช้วิดีโอปลอมหลอกโอนเงินกว่า 900 ล้านบาท นอกจากนี้ ในสหรัฐฯ มีรายงานว่ามีการแพร่ระบาดของกลโกงประเภท “เสียงหลอกลวง” ที่ผู้ปกครองได้รับสายโทรศัพท์ซึ่งใช้เสียงเลียนแบบลูกหลานของตนซึ่งร้องขอความช่วยเหลือฉุกเฉินเพื่อหลอกให้ผู้ปกครองโอนเงิน ซึ่งในสหรัฐฯ มีรายงานว่ากลโกงประเภทหลอกว่าเป็นหลานทางโทรศัพท์เหล่านี้ทำให้เหยื่อสูญเงินรวมเกือบ $1.9 ล้านดอลลาร์ในปี 2023[27]เป็นต้น

เพื่อตอบโต้ภัยคุกคามนี้ หลายประเทศได้แก้ไขหรือออกกฎหมายใหม่ เช่น สาธารณรัฐฝรั่งเศสตรา SREN Law ปี 2024 ให้การเผยแพร่สื่อปลอมที่สร้างจาก AI โดยไม่แจ้งว่าเป็นสื่อปลอมถือเป็นความผิดทางอาญา รัฐแคลิฟอร์เนียของสหรัฐฯ ห้ามใช้ deepfake ในการหาเสียง และเปิดช่องให้ฟ้องคดีแพ่งกรณี deepfake ลามกอนาจารได้ถึง $150,000 ส่วนสหราชอาณาจักรแม้ไม่มีกฎหมายเฉพาะ แต่ใช้ Fraud Act 2006 และ Online Safety Act 2023 รับมือกรณีลักษณะนี้

กรณีเหล่านี้สะท้อนให้เห็นว่า การฉ้อโกงด้วย AI สร้างความเสียหายรุนแรงและยากต่อการตรวจจับ ประเทศไทยจึงควรเร่งบัญญัติกฎหมายเฉพาะเพื่อให้การบังคับใช้กฎหมายมีประสิทธิภาพ ทันสมัย และคุ้มครองประชาชนได้อย่างแท้จริงในยุคดิจิทัล

[27] California Department of Justice, “Attorney General Bonta warns Californians: AI-generated scams are widespread and tricky to spot. State of California,” Retrieved 5 July 2025, From https://oag.ca.gov/news/press-releases

4.5 เหตุผลและความจำเป็นในการกำหนดเหตุเพิ่มโทษในการฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์

การฉ้อโกงโดยใช้ปัญญาประดิษฐ์ (AI) มีความซับซ้อนและแนบเนียนกว่าการฉ้อโกงทั่วไปอย่างมีนัยสำคัญ ผู้กระทำสามารถปลอมแปลงภาพ เสียง หรือบุคลิกบุคคลที่เหยื่อไว้วางใจ และดำเนินการหลอกลวงผ่านระบบออนไลน์ตลอด 24 ชั่วโมง ทำให้โอกาสในการก่อเหตุสูงขึ้น จำนวนเหยื่อขยายตัวรวดเร็ว และความเสียหายทางเศรษฐกิจมีมูลค่าสูงขึ้นอย่างมาก ขณะเดียวกัน ผู้กระทำยังสามารถปกปิดตัวตนด้วยเทคโนโลยีขั้นสูง ทำให้การติดตามจับกุมทำได้ยากยิ่ง ส่งผลให้บทลงโทษตามกรอบเดิมไม่เพียงพอต่อการป้องปรามหรือข่มขู่ยับยั้ง

เมื่อพิจารณาตามหลัก “เหตุเพิ่มโทษ” หรือ “เหตุฉกรรจ์” ที่เน้นความร้ายแรงของการกระทำและผลกระทบต่อสังคม การฉ้อโกงโดยใช้ AI จึงควรได้รับการพิจารณาให้มีบทลงโทษสูงขึ้นใน 4 ด้านหลัก ได้แก่

1) การเพิ่มโทษเนื่องจากจำนวนผู้เสียหายและโอกาสในการกระทำความผิด ปัญญาประดิษฐ์ (AI) ช่วยให้ผู้กระทำผิดสามารถเข้าถึงเหยื่อจำนวนมากได้รวดเร็วผ่านช่องทางออนไลน์หรืออินเทอร์เน็ตที่ประชาชนเข้าถึงได้ตลอดเวลา ทำให้โอกาสในการกระทำความผิดมากขึ้น ประกอบกับความสามารถของปัญญาประดิษฐ์เองที่สามารถปลอมแปลงตัวตนได้อย่างแนบเนียน ทำให้มีผู้หลงเชื่อและตกเป็นเหยื่อมากขึ้น มากกว่าการฉ้อโกงโดยวิธีการทั่วๆไป

2) การเพิ่มโทษจากมูลค่าของความเสียหายที่เกิดขึ้นจากการกระทำความผิด การใช้ AI ทำให้การหลอกลวงดูน่าเชื่อถือและเกิดผลได้จริง มูลค่าความเสียหายที่เกิดขึ้นจึงมักสูงกว่าอาชญากรรมในรูปแบบเดิมอย่างมาก และขยายผลได้ในวงกว้าง

3) ความยากในการติดตามจับกุมตัวผู้กระทำความผิด เนื่องจากปัญญาประดิษฐ์ในปัจจุบันมีความสามารถสูงและสามารถปลอมแปลงตัวตนได้อย่างแนบเนียนทั้งภาพและเสียง ผู้กระทำผิดจึงอาศัยความสามารถของปัญญาประดิษฐ์ในการปกปิดและปลอมแปลงตัวตนผ่านช่องทางอินเทอร์เน็ตและช่องทางออนไลน์ ส่งผลทำให้เกิดความยากต่อการติดตามจับกุมตัวผู้กระทำความผิดมากกว่าการปลอมแปลงตัวตนโดยวิธีการธรรมดา

4) การเพิ่มโทษจากระดับความร้ายแรงและความน่าตำหนิของการกระทำเมื่อเทียบกับการฉ้อโกงโดยการปลอมแปลงตัวตนกรณีทั่วไป

การฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์ (AI) ต้องใช้ทักษะขั้นสูงและการวางแผนที่ซับซ้อน แสดงถึงเจตนาแน่วแน่และความสามารถในการก่ออาชญากรรมขั้นสูง นอกจากนี้ การใช้ปัญญาประดิษฐ์ยังส่งผลให้การกระทำความผิดมีประสิทธิภาพมากขึ้น ทั้งในด้านการหลอกลวงให้เกิดผล ความเสียหายที่เกิดขึ้น และโอกาสในการกระทำซ้ำ ซึ่งทั้งหมดนี้สะท้อนให้เห็นถึง “ระดับความร้ายแรงของผลแห่งการกระทำ” ที่มากกว่าการฉ้อโกงโดยการปลอมแปลงตัวตนในรูปแบบทั่วไปอย่างชัดเจน เมื่อพิจารณาเปรียบเทียบกับการปลอมแปลงตัวตนในลักษณะทั่วไป เช่น การใช้บัตรประชาชนปลอม หรือการแอบอ้างชื่อโดยไม่มีเครื่องมือทางเทคโนโลยีเข้าช่วย จะเห็นว่าการกระทำดังกล่าวมักเกิดจากช่องโหว่ในระบบ หรือใช้วิธีการง่าย ๆ ที่ไม่มีความซับซ้อนและความเสียหายในวงกว้าง

เท่ากับการใช้ปัญญาประดิษฐ์สมควรได้รับการพิจารณาให้เป็นเหตุเพิ่มโทษเพื่อความเป็นธรรมและสอดคล้องกับนโยบายป้องกันอาชญากรรมสมัยใหม่

โดยสรุป การฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์ (AI) มีลักษณะเฉพาะที่ก่อให้เกิดผลกระทบอย่างรุนแรงและแตกต่างจากการฉ้อโกงแบบเดิมอย่างชัดเจน การกำหนดให้เป็นเหตุเพิ่มโทษจึงเป็นมาตรการจำเป็นเพื่อปกป้องสังคมและตอบสนองต่อความร้ายแรงของอาชญากรรมในยุคเทคโนโลยี

4.6 การกำหนดให้การฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์เป็นความผิดอาญาแผ่นดิน

ในระบบกฎหมายไทย ความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญามักจัดเป็นความผิดอาญาส่วนตัว ที่ยอมความได้ โดยให้ความสำคัญกับสิทธิของผู้เสียหายรายบุคคลเป็นหลัก อย่างไรก็ตาม การฉ้อโกงโดยใช้ปัญญาประดิษฐ์ได้พัฒนาไปสู่รูปแบบที่ซับซ้อนและส่งผลกระทบวงกว้าง ทั้งในด้านจำนวนผู้เสียหาย มูลค่าความเสียหาย และความเสียหายเชิงโครงสร้างต่อความมั่นคงของระบบดิจิทัลและเศรษฐกิจโดยรวม จึงไม่อาจถือเป็นการละเมิดสิทธิส่วนบุคคลเพียงอย่างเดียวอีกต่อไป

พฤติการณ์ของการกระทำดังกล่าวมักมีลักษณะซ่อนเร้น ยากแก่การตรวจพบ และอาศัยเทคโนโลยีที่มีประสิทธิภาพสูงในการปลอมแปลงตัวตน ส่งผลให้เกิดอุปสรรคในการดำเนินคดีหากต้องรอการร้องทุกข์จากผู้เสียหาย อีกทั้งยังเปิดโอกาสให้ผู้กระทำผิดสามารถใช้วิธีข่มขู่หรือล่อลวงเหยื่อเพื่อหลีกเลี่ยงความรับผิดได้

ด้วยเหตุนี้ จึงมีความจำเป็นในการยกระดับความผิดดังกล่าวให้เป็นความผิดอาญาแผ่นดิน เพื่อให้รัฐสามารถดำเนินคดีได้แม้ไม่มีการร้องทุกข์ ทั้งยังช่วยเพิ่มประสิทธิภาพในการป้องกัน ปราบปราม และยับยั้ง การกระทำความผิด โดยเฉพาะในบริบทที่จำนวนผู้เสียหายและมูลค่าความเสียหายมีแนวโน้มสูงขึ้นอย่างต่อเนื่อง

แนวทางนี้สอดคล้องกับหลักการในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 77 และพระราชบัญญัติหลักเกณฑ์การจัดทำร่างกฎหมายและการประเมินผลสัมฤทธิ์ของกฎหมาย พ.ศ. 2562 ที่มุ่งให้กฎหมายมีความทันสมัย สอดคล้องกับสภาพการณ์ และสามารถรับมือกับอาชญากรรมรูปแบบใหม่ได้อย่างมีประสิทธิภาพ อีกทั้งยังสอดรับกับทิศทางของกฎหมายในต่างประเทศ เช่น สาธารณรัฐฝรั่งเศส สหรัฐอเมริกา และสหราชอาณาจักร ที่มีการขยายขอบเขตของกฎหมายอาญาเพื่อครอบคลุมอาชญากรรมที่เกิดจากการใช้เทคโนโลยีปัญญาประดิษฐ์

5. ข้อเสนอแนะ

จากการศึกษาพบว่า การฉ้อโกงโดยการปลอมแปลงตัวตนด้วยปัญญาประดิษฐ์เป็นปัญหาที่ทวีความรุนแรงขึ้นอย่างต่อเนื่อง เนื่องจากเทคโนโลยี AI ทำให้การปลอมแปลงมีความแนบเนียนและเข้าถึงได้ง่าย ส่งผลให้เกิดความเสียหายต่อทรัพย์สินและความเชื่อมั่นของประชาชนในวงกว้าง โดยเฉพาะเมื่อผู้กระทำแอบอ้างเป็นเจ้าหน้าที่รัฐหรือบุคคลใกล้ชิดกับเหยื่อ

อย่างไรก็ดี กฎหมายไทยในปัจจุบันยังไม่มีบทบัญญัติเฉพาะที่รองรับการกระทำความผิดในลักษณะดังกล่าว ทำให้การบังคับใช้ต้องอาศัยบทบัญญัติทั่วไปในประมวลกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ซึ่งมีข้อจำกัดทั้งในด้านขอบเขตของความผิด อัตราโทษ และลักษณะของความเป็นความผิดอาญาแผ่นดิน

ด้วยเหตุนี้ ผู้เขียนจึงเสนอแนวทางปรับปรุงกฎหมายไทยเพื่อให้สามารถรองรับและจัดการกับปัญหาการฉ้อโกงโดยการปลอมแปลงตัวตนด้วย AI ได้อย่างมีประสิทธิภาพ ดังนี้

5.1 การเพิ่มเหตุฉกรรจ์ในมาตรา 342/1 แห่งประมวลกฎหมายอาญา

เสนอให้บัญญัติมาตรา 342/1 กำหนดให้การฉ้อโกงโดยการปลอมแปลงตัวตนด้วย AI เป็นเหตุฉกรรจ์ของความผิดฐานฉ้อโกง โดยระบุว่า

“ถ้าการกระทำความผิดฐานฉ้อโกงตามมาตรา 341 ผู้กระทำปลอมแปลงตัวตนโดยใช้ปัญญาประดิษฐ์ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท”

การกำหนดบทบัญญัตินี้จะช่วยให้การบังคับใช้กฎหมายมีความชัดเจน สอดคล้องกับลักษณะการกระทำผิดในยุคดิจิทัล และสะท้อนให้เห็นถึงระดับความร้ายแรงของการใช้เทคโนโลยีในการกระทำผิด

5.2 การกำหนดให้เป็นความผิดอาญาแผ่นดินตามมาตรา 348

เสนอให้แก้ไขมาตรา 348 โดยเพิ่มให้ความผิดตามมาตรา 342/1 เป็นความผิดอาญาแผ่นดินเช่นเดียวกับมาตรา 343 โดยมีข้อความว่า:

“ความผิดในหมวดนี้ นอกจากความผิดตามมาตรา 343 และมาตรา 342/1 เป็นความผิดอันยอมความได้”

การแก้ไขนี้จะปิดช่องโหว่ที่อาจเปิดโอกาสให้ผู้กระทำผิดหลีกเลี่ยงความรับผิด และจะส่งผลให้เจ้าหน้าที่รัฐสามารถดำเนินคดีได้แม้ไม่มีคำร้องทุกข์จากผู้เสียหาย ช่วยยับยั้ง ป้องกัน และปราบปรามการกระทำความผิดได้อย่างมีประสิทธิภาพ

บรรณานุกรม

ภาษาไทย

กมลรัตน์ ภาษีผล. “ความผิดฐานฉ้อโกงในวิธีการทางอิเล็กทรอนิกส์ให้เป็นเหตุฉกรรจ์.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิต, 2566.

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. “เตือนภัย! มิจฉาชีพใช้ AI สร้าง Deepfake หลอกลวงปลอมเป็นตำรวจ.” จาก https://www.youtube.com/watch?v=766pPepQ7jY, 5 กรกฎาคม 2568.

ข่าวช่องวัน. “แก๊งคอลฯ ปลอมเสียงเป็นลูกหลอกแม่โอนเงิน.” จาก https://www.youtube.com/watch?v=nBpFS0KBdQ8, 5 กรกฎาคม 2568.

ข่าวช่องวัน. “เตือนภัย! โทรปลอมเสียงคนในครอบครัวหลอกโอนเงิน.” จาก https://youtu.be/9Sri6s8qPZ0, 5 กรกฎาคม 2568.

ชยธร วิชาโคตร. “ปัญหากฎหมายเกี่ยวกับความผิดฐานฉ้อโกง.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2552.

ไทยพีบีเอสนิวส์. “จับแก๊งคอลเซ็นเตอร์ รับบทตำรวจปลอมผ่านเอไอ.” จาก https://youtu.be/1rSETal8ab8, 5 กรกฎาคม 2568.

ปกป้อง ศรีสนิท. กฎหมายอาญาชั้นสูง. พิมพ์ครั้งที่ 4. กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2566.

สุรสิทธิ์ แสงวิโรจนพัฒน์. “หลักเกณฑ์การกำหนดความผิดทางอาญาตามกฎหมายต่างประเทศ.” เล่มที่ 77 บทบัณฑิตย์ นิตยสารของเนติบัณฑิตยสภา. 125 (เมษายน-มิถุนายน 2564): 128.

เหมือน สุขมาตย์. “ความรับผิดทางอาญาของปัญญาประดิษฐ์.” วารสารนิติศาสตร์ มหาวิทยาลัยราชภัฏอุบลราชธานี. ปีที่ 7, ฉบับที่ 2 37(กรกฎาคม - ธันวาคม 2562): 38.

อัจฉรียา ชูตินันทน์. อาจชญาวิทยาและทัณฑวิทยา. พิมพ์ครั้งที่ 5. กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2566.

อารีย์น่าร์ อาแว และ ภาณุวัฒน์ นนท์ตุลา. “ปัญหาทางกฎหมายเรื่องความรับผิดทางเสียหายที่ปัญญาประดิษฐ์ก่อขึ้น.” วารสารกฎหมายและสังคมรังสิต, ปีที่ 5, ฉบับที่ 1 31(มกราคม - เมษายน 2566): 31.

ภาษาต่างประเทศ

California Department of Justice. “Attorney General Bonta warns Californians: AI-generated scams are widespread and tricky to spot. State of California.” https://oag.ca.gov/news/ press-releases, 5 July 2025.