การคุ้มครองสิทธิในอัตลักษณ์ส่วนบุคคลจากเทคโนโลยี Deepfake

The Protection of Personal Identity Rights against Deepfake Technology

อนุเทพ สุขศรีวงศ์

Anuthep Snookering*

ณัชญากัญจน์ รัตนวรกานต์

Nashayagal Rattanavorragant**

*อาจารย์ ดร. สังกัด สำนักวิชานิติศาสตร์ มหาวิทยาลัยแม่ฟ้าหลวง

**อาจารย์ ดร. สังกัด สาขาวิชานิติศาสตร์ คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง

บทคัดย่อ

บทความนี้มีวัตถุประสงค์เพื่อวิเคราะห์ปัญหาและช่องว่างของกฎหมายไทยในการคุ้มครองสิทธิในอัตลักษณ์ส่วนบุคคลจากเทคโนโลยีดีพเฟค (Deepfake) ซึ่งเป็นสื่อสังเคราะห์ที่สร้างหรือดัดแปลงด้วยปัญญาประดิษฐ์จนมีความสมจริงยากแก่การแยกแยะจากของจริง ก่อให้เกิดการขโมยอัตลักษณ์ การฉ้อโกง การหมิ่นประมาท ข่าวปลอม และสื่อลามกอนาจารโดยไม่ยินยอม บทความนี้ใช้วิธีการศึกษาเชิงเอกสารจากตัวบทกฎหมาย คำพิพากษา และเอกสารทางวิชาการทั้งในและต่างประเทศ จากการศึกษา พบว่า กฎหมายไทยที่ใช้บังคับอยู่ยังไม่สามารถคุ้มครองสิทธิในอัตลักษณ์จากดีพเฟคได้อย่างมีประสิทธิภาพ เนื่องจากประการแรก ประเทศไทยยังไม่มีกฎหมายเฉพาะว่าด้วยดีพเฟคหรือปัญญาประดิษฐ์ การคุ้มครองจึงอาศัยการปรับใช้กฎหมายเดิมหลายฉบับอย่างกระจัดกระจายและเป็นการแก้ปัญหาเฉพาะหน้า ประการที่สอง กฎหมายไทยมีช่องว่างเชิงโครงสร้างที่สำคัญ คือ การไม่ได้รับรอง “สิทธิในอัตลักษณ์ของบุคคล” เป็นการเฉพาะ เมื่อเปรียบเทียบกับสหภาพยุโรป ซึ่งมี EU Artificial Intelligence Act เป็นกฎหมายควบคุมการใช้ปัญญาประดิษฐ์อย่างเป็นระบบ โดยมีการจัดระดับความเสี่ยง องค์กรที่ดูแล และการกำหนดบทลงโทษที่ชัดเจน ซึ่งอาจนำมาปรับใช้เป็นต้นแบบในประเทศไทยได้ บทความนี้จึงเสนอแนะให้ประเทศไทยบัญญัติกฎหมายเฉพาะที่กำหนดนิยามดีพเฟค องค์กรกำกับดูแล เกณฑ์ประเมินความเสี่ยง บทลงโทษทางแพ่งและอาญาที่ชัดเจน

คำสำคัญ: ดีพเฟค; สิทธิในอัตลักษณ์ของบุคคล; ปัญญาประดิษฐ์

Abstract

This article aims to analyze the problems and legal gaps in Thai law regarding the protection of the right to personal identity from deepfake technology which is synthetic media created or modified using artificial intelligence to such a realistic degree that it is difficult to distinguish from the genuine subject. Such technology facilitates to identity theft, fraud, defamation, fake news, and non-consensual pornography. This article employs a documentary research methodology, drawing upon legal texts, court judgments, and academic literature from both domestic and international sources. The study found that existing Thai laws do not effectively protecting the right to identity from deepfakes. Firstly, Thailand currently lacks specific legislation addressing deepfakes or artificial intelligence; consequently, protection relies on the fragmented application of various existing laws and ad hoc legal interpretation. Secondly, Thai law contains a significant structural gap: the failure to specifically recognize the “Personal Identity Rights”. Compared to the European Union, which has enacted the EU Artificial Intelligence Act, a comprehensive legal framework regulating artificial intelligence by establishing risk classification framework, regulatory authorities and clear penalties and which could serve as a model for Thailand. Therefore, this article proposes that Thailand enact specific legislation defining the term "deepfake", establishing a regulatory body, risk classification, and clear civil and criminal penalties.

Keywords: Deepfake; Personal Identity Rights; artificial intelligence

1.บทนำ

ความก้าวหน้าของเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ได้เปลี่ยนแปลงรูปแบบการสร้างและเผยแพร่ข้อมูลดิจิทัลอย่างมีนัยสำคัญ โดยเฉพาะการพัฒนาเทคโนโลยีสื่อสังเคราะห์ (Synthetic Media) หรือที่เรียกว่า “ดีพเฟค” (Deepfake) ซึ่งอาศัยเทคนิคการเรียนรู้เชิงลึก (Deep Learning) ในการสร้างหรือดัดแปลงภาพ เสียง และวิดีโอให้มีความสมจริงจนยากต่อการแยกแยะจากข้อมูลจริง แม้เทคโนโลยีดังกล่าวจะก่อให้เกิดประโยชน์ในด้านอุตสาหกรรมภาพยนตร์ การศึกษา การแพทย์ และการสื่อสาร แต่ในอีกด้านหนึ่งก็เปิดโอกาสให้เกิดการนำไปใช้ในทางที่ละเมิดสิทธิของบุคคลอย่างกว้างขวาง

ปัญหาที่เกิดจากดีพเฟคมิได้จำกัดอยู่เพียงการเผยแพร่ข้อมูลอันเป็นเท็จ หากแต่ส่งผลกระทบโดยตรงต่อสิทธิในอัตลักษณ์ของบุคคล (Personal Identity Rights) ซึ่งครอบคลุมภาพ ใบหน้า เสียง ชื่อ และข้อมูลชีวมิติที่สามารถระบุตัวบุคคลได้ การนำอัตลักษณ์ของบุคคลไปสร้างหรือดัดแปลงโดยปราศจากความยินยอมอาจนำไปสู่การฉ้อโกง การหมิ่นประมาท การสร้างข่าวปลอม การแสวงหาประโยชน์ทางการค้าโดยมิชอบ ตลอดจนการผลิตสื่อลามกอนาจารสังเคราะห์ ซึ่งก่อให้เกิดความเสียหายต่อชื่อเสียง ศักดิ์ศรี ความเป็นส่วนตัว และความมั่นคงปลอดภัยของบุคคลทั้งยังสร้างความท้าทายต่อกระบวนการยุติธรรมในการพิสูจน์ข้อเท็จจริงและการเยียวยาความเสียหาย

แม้ว่าประเทศไทยจะมีกฎหมายหลายฉบับที่สามารถนำมาปรับใช้กับการกระทำที่เกี่ยวข้องกับดีพเฟค ได้แก่ รัฐธรรมนูญแห่งราชอาณาจักรไทย ประมวลกฎหมายแพ่งและพาณิชย์ ประมวลกฎหมายอาญา พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่กฎหมายเหล่านี้ล้วนถูกตราขึ้นก่อนการเกิดขึ้นของเทคโนโลยีดีพเฟค จึงเป็นเพียงการปรับใช้บทบัญญัติเดิมเพื่อแก้ไขปัญหาเฉพาะกรณี ส่งผลให้การคุ้มครองมีลักษณะกระจัดกระจายขาดความเป็นเอกภาพ และยังมีช่องว่างสำคัญในประเด็นการคุ้มครองสิทธิในอัตลักษณ์ของบุคคล การกำหนดฐานความรับผิด และการเยียวยาทางแพ่งแก่ผู้เสียหาย

ในขณะเดียวกัน หลายประเทศได้เริ่มพัฒนากฎหมายหรือมาตรการเฉพาะเพื่อกำกับดูแลปัญญาประดิษฐ์และดีพเฟค โดยเฉพาะสหภาพยุโรปซึ่งได้ตรา EU Artificial Intelligence Act (EU AI Act) เพื่อกำกับดูแลระบบปัญญาประดิษฐ์ตามระดับความเสี่ยง แม้กฎหมายดังกล่าวจะมิได้มุ่งคุ้มครองผู้เสียหายจากดีพเฟคโดยตรง แต่ก็สะท้อนแนวโน้มของกฎหมายสมัยใหม่ที่ให้ความสำคัญกับการกำกับดูแลเทคโนโลยีเชิงป้องกัน ควบคู่กับการสร้างความโปร่งใสและความรับผิดของผู้พัฒนาและผู้ให้บริการระบบปัญญาประดิษฐ์

บทความนี้มีวัตถุประสงค์เพื่อวิเคราะห์ปัญหาและช่องว่างของกฎหมายไทยในการคุ้มครองสิทธิในอัตลักษณ์ส่วนบุคคลจากเทคโนโลยีดีพเฟค ศึกษาขอบเขตการบังคับใช้ของกฎหมายไทยที่เกี่ยวข้อง เปรียบเทียบแนวทางการกำกับดูแลของสหภาพยุโรปภายใต้ EU AI Act และเสนอแนวทางในการพัฒนากฎหมายไทยให้สามารถคุ้มครองสิทธิของบุคคลและกำกับดูแลการใช้เทคโนโลยีดีพเฟคได้อย่างเหมาะสม โดยใช้วิธีการศึกษาเชิงเอกสารจากกฎหมาย คำพิพากษา และเอกสารวิชาการทั้งในและต่างประเทศ

“ดีพเฟค” (Deepfake) คืออะไร

“ดีพเฟค” (Deepfake) คือ เทคโนโลยีสื่อสังเคราะห์ (Synthetic Media) ได้รับการพัฒนาขึ้นโดยอาศัยเทคนิคการเรียนรู้เชิงลึก (Deep Learning) และโครงข่ายประสาทเทียมแบบปฏิปักษ์ (Generative Adversarial Networks – GANs) หน้าที่ของ GANs คือ การสร้างข้อมูลออกมา สำหรับการที่จะสร้างข้อมูลออกมาได้นั้น GANs จะประกอบไปด้วย 2 ส่วน คือ Generator ที่ทำหน้าที่สร้างข้อมูลให้ตรงกับคุณสมบัติ และเป้าหมาย เช่น ขนาด สี รูปทรงโครงสร้าง ผิววัตถุ และ Discriminator ที่จะตรวจสอบว่า Generator สร้างข้อมูลออกมาใกล้เคียงกับเป้าหมายที่สนใจหรือไม่[1]

[1] Nut Chukamphaeng. 2019. GANs: อะไรคือ Generative Adversarial Networks. https://medium.com/@nutorbitx/gans-%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3%E0%B8%84%E0%B8%B7%E0%B8%AD-generative-adversarial-networks-7973ae70db70

เทคโนโลยีดังกล่าวมีความสามารถในการวิเคราะห์ เรียนรู้ และเลียนแบบลักษณะเฉพาะทางกายภาพและพฤติกรรมของบุคคล ไม่ว่าจะเป็นใบหน้า ท่าทาง น้ำเสียง และบุคลิกภาพ แล้วนำมาสร้างสรรค์หรือดัดแปลงเป็นสื่อดิจิทัลที่มีความสมจริงจนแทบไม่สามารถแยกแยะออกจากสื่อต้นฉบับที่เกิดขึ้นจริงได้

ความก้าวหน้าของเทคโนโลยีนี้ สะท้อนให้เห็นอย่างชัดเจนในนิยามทางกฎหมายระดับสากล โดยสหภาพยุโรปได้ให้คำนิยามของ “Deepfake” ไว้ในกฎหมายปัญญาประดิษฐ์ (The EU Artificial Intelligence Act) ว่าเป็น “เนื้อหาภาพ เสียง หรือวิดีโอที่สร้างหรือดัดแปลงโดยระบบปัญญาประดิษฐ์ ซึ่งมีลักษณะคล้ายกับบุคคล วัตถุ สถานที่ หรือหน่วยงานที่มีอยู่จริง และมีแนวโน้มที่จะทำให้บุคคลทั่วไปเข้าใจผิดว่าเป็นของจริงหรือความจริง”

ในอดีต การสร้างดีพเฟคจำกัดอยู่เฉพาะในกลุ่มผู้เชี่ยวชาญด้านวิทยาการคอมพิวเตอร์หรือสตูดิโอภาพยนตร์ขนาดใหญ่ที่มีทรัพยากรสูง ทว่าในปัจจุบันเครื่องมือและแอปพลิเคชันสำหรับสร้างดีพเฟคได้รับการพัฒนาให้ใช้งานง่ายและเข้าถึงได้ทั่วไปผ่านสมาร์ตโฟนและอินเทอร์เน็ต การเข้าถึงที่ง่ายดายนี้ทำให้อัตราการแพร่กระจายของดีพเฟคเพิ่มขึ้นเป็นทวีคูณ นำไปสู่ความเสี่ยงที่หลากหลายและส่งผลกระทบในวงกว้าง เช่น การฉ้อโกงทางการเงิน การหมิ่นประมาทเพื่อทำลายชื่อเสียง การสร้างสื่อลามกอนาจาร โดยปราศจากความยินยอม และการเผยแพร่ข่าวปลอม (Fake News) เพื่อบิดเบือนกระบวนการประชาธิปไตยและการเลือกตั้ง[2]

การคุ้มครองอัตลักษณ์ของบุคคล

อัตลักษณ์ (Identity) ในทางจิตวิทยาสังคม หมายถึง ความสำนึกของแต่ละบุคคลว่าตนเองมีความแตกต่างจากผู้อื่นมากน้อยเพียงไร[3] แนวคิดเรื่อง "สิทธิในบุคลิกภาพ"

---

[2] Judge, E. F., & Korhani, A. M. (2021). Deepfakes, Counterfeits, and Personality. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3893890

[3] วิภูพงศ์ จิระประภูศักดิ์. (2558). การศึกษาวัฒนธรรมย่อยและการวิเคราะห์อัตลักษณ์ ของกลุ่มเฮฟวี่เมทัล กรณีศึกษากลุ่มเฮฟวี่เมทัลในเขตอำเภอเมืองเชียงใหม่ = A Study of subculture and identity analysis of

(personality rights หรือ droits de la personnalité ในระบบกฎหมายภาคพื้นยุโรป) เป็นกลุ่มสิทธิที่คุ้มครองคุณลักษณะอันเป็นแก่นแห่งความเป็นบุคคล ได้แก่ ภาพ (image) เสียง (voice) ชื่อ (name) และลักษณะเฉพาะตัวอื่น ๆ ที่ทำให้บุคคลหนึ่งแตกต่างจากบุคคลอื่น สิทธินี้มีลักษณะสองมิติที่ดำรงอยู่ควบคู่กัน คือ มิติเชิงศักดิ์ศรี (dignitary dimension) ซึ่งคุ้มครองความเป็นปัจเจกบุคคล[4] โดยไม่ผูกติดอยู่กับเงื่อนไขว่าจะต้องมีการกล่าวข้อความเท็จ ที่ทำให้เสื่อมเสียชื่อเสียง ดีพเฟคที่นำใบหน้าของบุคคลไปใช้ในบริบท ที่มิได้ทำให้เสียชื่อเสียงแต่อย่างใด เช่น การนำไปใช้โฆษณาสินค้าโดยไม่ได้รับอนุญาต ก็ยังคงเป็นการละเมิดสิทธิในบุคลิกภาพได้ ในขณะที่อาจไม่เข้าองค์ประกอบความผิดฐานหมิ่นประมาท กับมิติเชิงทรัพย์สิน (proprietary dimension) ซึ่งคุ้มครองมูลค่าทางเศรษฐกิจจากการแสวงประโยชน์จากอัตลักษณ์ ในระบบกฎหมายอเมริกันมิติหลังนี้ตกผลึกเป็น “สิทธิในการเผยแพร่ตน” (right of publicity) ขณะที่ในระบบกฎหมายภาคพื้นยุโรปทั้งสองมิติมักรวมอยู่ในกรอบสิทธิในบุคลิกภาพอันเดียวกัน[5]

ภาพของบุคคลสามารถสื่อได้ถึงบุคคลในภาพ การใช้ดีพเฟคโดยไม่ได้รับความยินยอมเพื่อสร้างภาพบุคคลอื่น ไม่ว่าจะเป็นภาพนิ่งหรือภาพเคลื่อนไหว ย่อมกระทบสิทธิในอัตลักษณ์ของบุคคลในภาพ ตามพระราชบัญญัติลิขสิทธิ์ภาพนิ่งจะได้รับความคุ้มครองในส่วนของงานศิลปกรรม ส่วนภาพเคลื่อนไหวจะได้รับความคุ้มครองในส่วนของงานโสตทัศนวัสดุหรืองานภาพยนตร์[6] หากนำภาพนิ่งหรือภาพเคลื่อนไหวอันมีลิขสิทธิ์ของบุคคลอื่นมาดัดแปลง ย่อมเป็นการละเมิดลิขสิทธิ์ของเจ้าของลิขสิทธิ์[7] ในภาพนั้นพระราชบัญญัติลิขสิทธิ์ไม่ได้คุ้มครองบุคคลในภาพ ภาพถ่ายของบุคคลถือว่า

---

heavy metal group: A Case study of heavy metal group in Mueang, Chiang Mai / วิภูพงศ์ จิระประภูศักดิ์. เชียงใหม่ บัณฑิตวิทยาลัย มหาวิทยาลัยเชียงใหม่.

[4] P, J. (2025). Navigating the legal framework for deepfake technology in the era of intellectual property and personal rights. International Journal for Multidisciplinary Research, 7(2). https://doi.org/10.36948/ijfmr.2025.v07i02.37887

[5] Judge, E. F., & Korhani, A. M. (2021). อ้างแล้ว

[6] พระราชบัญญัติลิขสิทธิ์ พ.ศ.2537 มาตรา 4

[7] พระราชบัญญัติลิขสิทธิ์ พ.ศ.2537 มาตรา 27 มาตรา 28

เป็นข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของบุคคลในภาพ เพราะข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม ผู้เก็บรวบรวมหรือใช้ภาพถ่ายของบุคคลถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคล[8] หากผู้ควบคุมข้อมูลส่วนบุคคลนำภาพของบุคคลอื่นไปใช้โดยที่บุคคลในภาพมิได้ยินยอมก็จะเป็นความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล[9] ภาพบุคคลหากมีการดัดแปลงแก้ไขโดยไม่ได้รับความยินยอมในประการที่จะทำให้เกิดความเสียหายต่อบุคคลในภาพแล้วนำเข้าสู่ระบบคอมพิวเตอร์ก็อาจมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์[10] ภาพบุคคลหากมีการดัดแปลงเป็นภาพลามกอนาจารก็จะเป็นความผิดอาญาตามประมวลกฎหมายอาญาในกรณีภาพลามกอนาจารเด็กอายุไม่เกิน 18 ปี จะมีโทษหนักขึ้นความผิดอาญาดังกล่าวเป็นความผิดอันยอมความมิได้[11]

เสียงของบุคคลสามารถสื่อได้ถึงบุคคลเจ้าของเสียงนั้น ธนาคารหลายแห่งได้ใช้เทคโนโลยีการจดจำเสียง (Voice Biometrics) เพื่อประโยชน์ในการยืนยันลูกค้า เทคโนโลยีนี้ทำงานโดยการเปรียบเทียบคุณสมบัติในตัวอย่างเสียงที่กำหนดกับเทมเพลต “พิมพ์เสียง” ที่ได้รับจากการบันทึกก่อนหน้า[12] การใช้ดีพเฟคสร้างเสียงบุคคลอื่นสามารถสร้างเสียงที่ฟังดูเหมือนเสียงจริงของบุคคลอื่นได้ และอาจกระทบสิทธิในอัตลักษณ์ของบุคคลเจ้าของเสียง โดยอาจนำไปสู่การฉ้อโกงในระบบการเงินได้ อันเป็นความผิดตามกฎหมายอาญา[13] และเป็นการละเมิดตามกฎหมายแพ่งได้[14]

ชื่อของบุคคลสามารถสื่อได้ถึงบุคคลเจ้าของชื่อนั้น ชื่อทำหน้าที่เป็นสัญลักษณ์เฉพาะตัวของบุคคล ชื่อและนามสกุลเป็นข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง

---

[8] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 6

[9] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 27 มาตรา 79

[10] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14(1) มาตรา 16

[11] ประมวลกฎหมายอาญา มาตรา 287 มาตรา 287/1 มาตรา 1(17)

[12] iProov. (2023). Voice Biometrics For Private Banking and Wealth Management: ความรู้สึกปลอดภัยที่ผิดพลาด? https://www.iproov.com/th/blog/voice-biometrics-false-security

[13] ประมวลกฎหมายอาญา มาตรา 342

[14] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล สิทธิในการใช้ชื่อได้รับความคุ้มครองตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 18 หากมีบุคคลอื่นนำชื่อไปใช้โดยมิได้รับอนุญาตจนทำให้เจ้าของชื่อเสื่อมเสียประโยชน์ เจ้าของชื่อก็สามารถฟ้องร้องขอให้ศาลสั่งระงับความเสียหาย เรียกค่าสินไหมทดแทนได้[15]

นอกจากนั้น ดีฟเฟคยังมีการละเมิดความเป็นส่วนตัวในสองระดับ คือ ระดับที่หนึ่ง ความเป็นส่วนตัวของข้อมูล (informational privacy) เนื่องจากการสร้างดีฟเฟคจำเป็นต้องอาศัยข้อมูลชีวมิติ (biometric data) คือ ภาพใบหน้าและคลื่นเสียง ซึ่งโดยธรรมชาติเป็นข้อมูลที่บ่งชี้ตัวบุคคลและไม่อาจเปลี่ยนแปลงได้ และระดับที่สอง คือ ความเป็นส่วนตัวในความสงบสุขแห่งชีวิต (privacy as seclusion) และความเป็นส่วนตัวเชิงตัดสินใจ (decisional privacy) ที่ถูกล่วงล้ำเมื่อบุคคลถูกประกอบสร้างให้ปรากฏในสถานการณ์ที่ตนมิได้กระทำ[16] ความเป็นส่วนตัวเป็นสิทธิได้รับความคุ้มครองตามรัฐธรรมนูญ[17]

ดีพเฟคกับความผิดฐานฉ้อโกง

ความผิดฐานฉ้อโกง คือ การหลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จหรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม และหากมีการแสดงตนเป็นบุคคลอื่นในการฉ้อโกงนั้นก็จะมีโทษหนักขึ้น การแสดงข้อความอันเป็นเท็จต่อประชาชนหรือด้วยการปกปิดความจริงซึ่งควรบอกให้แจ้งแก่ประชาชนจะเป็นความผิดฐานฉ้อโกงประชาชน ซึ่งจะมีโทษหนักและเป็นความผิดอันมิอาจยอมความได้ (ความผิดฐานฉ้อโกงอื่นที่ไม่ใช่ฐานฉ้อโกงประชาชนสามารถยอมความได้)[18]

---

[15] คำพิพากษาศาลฎีกาที่ 802/2558 และฎีกาที่ 4432/2553

[16] Han, M. (2024). The infringement of deepfake technology on personal privacy and legal protection: A discussion based on Article 1032 of the Civil Code. Journal of Education, Humanities and Social Sciences. https://doi.org/10.54097/s0a47e08

[17] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 32

[18] ประมวลกฎหมายอาญา มาตรา 341-343 และมาตรา 348

รายงานเหตุการณ์ดีพเฟคไตรมาสที่ 1 ประจำปี 2025 (Q1 2025 Deepfake Incident Report) จัดโดย Resemble AI 2025 ระบุว่าช่วงไตรมาสแรกของปี 2568 มีการหลอกลวงจากการใช้เทคโนโลยีดีพเฟคในโลก มากกว่า 163 เหตุการณ์ สร้างมูลค่าความเสียหายสูงถึง 200 ล้านดอลลาร์สหรัฐ (หรือประมาณ 6,500 ล้านบาท) โดยภูมิภาคที่มีการหลอกลวงมากสุด คือ อเมริกาเหนือ 38% เอเชีย 27% ยุโรป 21% และภูมิภาคอื่น ๆ 14% ซึ่งกลุ่มเป้าหมายหลายหลักในการหลอกลวง ประกอบด้วย บุคคลที่มีชื่อเสียง นักการเมืองและนักธุรกิจ กลุ่มนักการเมือง และภาคประชาชน โดยเฉพาะกลุ่มผู้หญิง และเด็ก อีกทั้งยังมีกลุ่มองค์กร มีทั้งภาคเอกชน องค์กรภาครัฐ และสถาบันการศึกษา เป็นต้น โดยแนวทางการหลอกลวงมีทั้ง ใช้วิดีโอ 46% ใช้ภาพ 32% และเสียง 22%[19]

ดีพเฟคกับสื่อลามกอนาจาร

สื่อลามกอนาจารสังเคราะห์เป็นปัญหาที่มีพบมากสุดที่เกิดจากดีพเฟค โดยผู้เสียหายส่วนใหญ่เป็นผู้หญิงและเด็กผู้หญิง[20] (Meti, 2026; Flynn et al., 2025) สร้างความเสียหายทางจิตใจ (trauma) ความเสียหายต่อชื่อเสียงการถูกกีดกันทางสังคม (social ostracism) และการถูกผลักออกจากโอกาสทางเศรษฐกิจ (economic exclusion)[21] สื่อลามกอนาจาร ไม่ได้มีคำนิยามไว้เป็นการเฉพาะแต่มีการให้คำนิยามคำว่า สื่อลามกอนาจารเด็ก ไว้ในประมวลกฎหมายอาญา มาตรา 1(17) ซึ่งเมื่อนำมาพิจารณาโดยเทียบเคียงกับมาตรา 287(1) แล้วคำว่า “สื่อลามกอนาจาร” จะหมายความว่า วัตถุหรือสิ่งที่แสดงให้รู้หรือเห็นถึงการกระทำทางเพศของบุคคลโดยรูป เรื่อง

[19] สภาองค์กรของผู้บริโภค. 2568. ภัยดีพเฟคพุ่ง หลังคนดังถูกปลอมหน้า – เสียง เอไอใช้หลอกเต็มรูปแบบ. https://www.tcc.or.th/deepfake-scam/

[20] Meti, V. (2026). Can women's dignity endure the deepfake era? Non-consensual intimate imagery and the fragility of personality rights in India. *Lex Is Us Law Journal*. https://doi.org/10.65393/liuv5112

[21] Kugler, M., & Pace, C. (2021). Deepfake privacy: Attitudes and regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3781968

หรือลักษณะสามารถสื่อไปในทางลามกอนาจาร ไม่ว่าจะอยู่ในรูปแบบของเอกสาร ภาพเขียน ภาพพิมพ์ ภาพระบายสี สิ่งพิมพ์ รูปภาพ ภาพโฆษณา เครื่องหมาย รูปถ่าย ภาพยนตร์ แถบบันทึกเสียง แถบบันทึกภาพ หรือรูปแบบอื่นใดในลักษณะทำนองเดียวกัน และให้หมายความรวมถึงวัตถุหรือสิ่งต่าง ๆ ข้างต้นที่จัดเก็บในระบบคอมพิวเตอร์ หรือในอุปกรณ์อิเล็กทรอนิกส์อื่นที่สามารถแสดงผลให้เข้าใจความหมายได้ ตามแนวคำพิพากษาศาลฎีกาสื่อลามกอนาจารหมายรวมถึงภาพที่แม้ไม่เห็นอวัยวะเพศชัดเจนแต่ก็มีลักษณะส่อไปในด้านยั่วยุกามารมณ์ เช่น ภาพหญิงเปลือยตลอดร่าง แม้จะมีผ้าบางใสหรือตาข่ายผ้าปกปิดอวัยวะเพศ แต่พอเห็นอวัยวะเพศได้บ้างถือได้ว่าเป็นภาพอันลามก ไม่ใช่ภาพศิลปะที่แสดงถึงส่วนสัดความสมบูรณ์ของร่างกาย[22]

ความผิดเกี่ยวกับสื่อลามกอนาจาร ในประมวลกฎหมายอาญาจะรวมถึงการทำ ผลิต มีไว้ นำเข้า การแจกจ่ายหรือเพื่อการแสดงอวดแก่ประชาชน การให้เช่าและช่วยการทำให้แพร่หลาย ดังนั้น ไม่ว่าจะเป็นผู้ผลิต ผู้ค้าผู้นำเข้า หรือผู้ครอบครองกฎหมายล่วงเอาผิดทั้งสิ้น กรณีเป็นสื่อลามกอนาจารเด็กอายุไม่เกิน 18 ปี จะมีโทษหนักขึ้น กรณีเป็นสื่อลามกอนาจารเกี่ยวข้องพระมหากษัตริย์ พระราชินี รัชทายาท หรือผู้สำเร็จราชการแทนพระองค์ก็จะเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร[23] ในกรณีที่มีการแต่งกายหรือใช้เครื่องหมายที่แสดงว่าเป็นภิกษุ สามเณร นักพรต หรือนักบวชในศาสนาจะเป็นความผิดที่เกี่ยวกับศาสนาด้วย[24] หากมีนำสื่อลามกอนาจารเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ที่ประชาชนทั่วไปอาจเข้าถึงได้ก็จะมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14(4) ด้วย

ในประเทศไทยได้เคยมีกลุ่มลับในแอปพลิเคชัน ใช้ชื่อกลุ่มว่า "ชุมชนช่างตัดเสื้อ" มีสมาชิกในกลุ่มมากกว่า 120,000 คน โดยกลุ่มนี้จะใช้ AI เข้ามาตัดต่อรูปภาพดารา

---

[22] ThaiDeka. คำพิพากษาศาลฎีกาที่ 3510/2531. https://deka.in.th/deka/2531-3510-105530, คำพิพากษาศาลฎีกาที่ 6301/2533. https://deka.in.th/deka/2533-6301-110201

[23] ประมวลกฎหมายอาญา มาตรา 112

[24] ประมวลกฎหมายอาญา มาตรา 208

ก่อนจะเปิดขายในราคาภาพละ 50 บาท อีกทั้งยังพบว่า ผู้ต้องหายังเปิดให้เช่าโปรแกรมที่ใช้ในการตัดต่ออีกด้วย โดยคิดค่าเช่าวันละ 300 บาท มีเงินหมุนเวียนบัญชีกว่า 800,000 บาท ภายหลังกลุ่มลับนี้ถูกตำรวจจับกุมดำเนินคดีจากข้อมูลการสืบสวน พบว่าดารานักแสดงสาวชื่อดังถูกนำภาพอนาจารไปขายถึง 46 คน ในจำนวนนี้มีดาราดัง เช่น มายด์และอ๊ะอายวง 4EVE บุ๋ม ปนัดดา ดีเจต้นหอม ในกรณีนี้ตำรวจได้มีการตั้งข้อหาการกระทำผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จเข้าสู่คอมพิวเตอร์และแจกจ่ายหรือขายภาพลามกอนาจาร[25]

ในประเทศอินเดียหญิงแม่บ้านธรรมดาคนหนึ่งในเมืองดิบรูการห์ รัฐอัสสัม ถูกอดีตแฟนหนุ่มของเธอนำภาพลักษณ์ของตนไปสร้างบัญชีอินสตาแกรมชื่อ Babydoll Archi (บาบีดอลล์ อาร์ชี) มียอดผู้ติดตาม 1.4 ล้านคน อดีตแฟนหนุ่มได้ใช้เครื่องมืออย่าง ChatGPT และ Dzine เพื่อสร้างตัวตนเสมือนด้วย AI วีดีโอหนึ่งที่กลายเป็นไวรัลโด่งดังในอินเดียเป็นภาพเธอในชุดส่าหรีสีแดง เต้นด้วยท่าทางยั่วยวนใจตามจังหวะเพลงโรมาเนียนที่ชื่อ "Dame Un Grr" ส่วนอีกภาพหนึ่งแสดงภาพเธอโพสต์ท่าทางกับเคนดรา ลัสท์ (Kendra Lust) ดาวภาพยนตร์ผู้ใหญ่ชาวอเมริกัน ต่อมาอดีตแฟนหนุ่มถูกจับและดำเนินคดีในข้อหาที่เกี่ยวข้องกับการคุกคามทางเพศ การแพร่กระจายสื่อลามก หมิ่นประมาท ทำให้บุคคลเสื่อมเสียชื่อเสียง ปลอมตัวเป็นผู้อื่นเพื่อหลอกลวง และก่ออาชญากรรมออนไลน์ ซึ่งมีโทษจำคุกสูงสุดถึง 10 ปี[26]

ดีพเฟคกับข่าวปลอม

ข่าวปลอม หรือ Fake News คือ ข่าวหรือข้อมูลที่นำไปสู่ความเข้าใจผิดและไม่ตั้งอยู่บนพื้นฐานความจริง โดยข่าวปลอมเป็นการจงใจให้ข้อมูลที่ผิดพลาด

[25] ไทยพีบีเอส. 2567. "มายด์ 4 EVE" ร้องถูกตัดต่อภาพอนาจาร พบ 46 ดาราโดนด้วย. https://www.thaipbs.or.th/news/content/335822

[26] บีบีซี นิวส์ไทย. 2025. เปิดคดีคลิปลวงดีพเฟค (Deepfake) สาวอินเดียถูกขโมยตัวตนไปสร้างคลิปอนาจารด้วยเอไอ. https://www.bbc.com/thai/articles/czdv909gvpjo.

และหวังผลประโยชน์จากความเข้าใจผิดนั้น ซึ่งผู้ที่ขาดทักษะในการจำแนกข้อเท็จจริงมีโอกาสถูกยั่วยุให้หลงเชื่อข่าวปลอมได้โดยง่าย[27]

การสร้างข่าวปลอมและนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จเข้าสู่คอมพิวเตอร์จะมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14 หากข่าวนั้นทำให้บุคคลอื่นเสียหายต่อชื่อเสียงก็จะมีความผิดฐานหมิ่นประมาท การสร้างข่าวปลอมโดยใช้ดีพเฟคสามารถทำได้โดยการปลอมเป็นบุคคลที่น่าเชื่อถือชักจูงคนไปลงทุน เล่นการพนัน กดลิงค์ที่ไม่ปลอดภัย เป็นต้น

EU Artificial Intelligence Act

เทคโนโลยีดีพเฟคเป็นส่วนหนึ่งของเทคโนโลยีปัญญาประดิษฐ์ ซึ่งสหภาพยุโรปได้สร้าง EU Artificial Intelligence Act หรือ EU AI Act เป็นกฎหมายของสหภาพยุโรปมีสถานะเป็น “ระเบียบ” (Regulation) มิใช่ “ทิศทาง” (Directive) ผลในทางกฎหมายคือ บทบัญญัติมีผลใช้บังคับโดยตรง (directly applicable) ในรัฐสมาชิกทั้ง 27 ประเทศ โดยไม่ต้องอาศัยการอนุวัติการเป็นกฎหมายภายในของแต่ละรัฐ EU AI Act เป็นกรอบกฎหมายที่ควบคุมเทคโนโลยีปัญญาประดิษฐ์อย่างเป็นระบบฉบับแรกของโลก[28]

EU AI Act จะมีการควบคุมปัญญาประดิษฐ์ตามระดับความเสี่ยงโดยแบ่งออกเป็น 4 ระดับ คือ

ระดับที่หนึ่ง ความเสี่ยงที่ยอมรับไม่ได้ (unacceptable risk) ตามมาตรา 5 ซึ่งเป็นการกระทำที่ต้องห้ามโดยเด็ดขาด ได้แก่ การให้คะแนนทางสังคม (social scoring) โดยหน่วยงานรัฐ ระบบ AI ที่ใช้เทคนิคบงการพฤติกรรมแบบจิตใต้สำนึก (subliminal/manipulative techniques) การจดจำอารมณ์ (emotion recognition) ในสถานที่ทำงาน

---

[27] ชยพล ธานีวัฒน์. การบังคับใช้กฎหมายเพื่อรับมือกับข่าวปลอม (Fake News). https://old.parliament.go.th/ewtadmin/ewt/elaw_parcy/ewt_dl_link.php?nid=2439

[28] European Commission. (n.d.). Regulatory framework on artificial intelligence (AI Act). Shaping Europe's Digital Future. Retrieved June 27, 2026, from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

และสถานศึกษา และการระบุอัตลักษณ์บุคคลด้วยข้อมูลชีวมิติจากระยะไกลแบบเรียลไทม์ในพื้นที่สาธารณะเพื่อการบังคับใช้กฎหมาย โดยมีข้อยกเว้นที่จำกัดและเข้มงวด

ระดับที่สอง ความเสี่ยงสูง (high risk) ได้แก่ ระบบที่ระบุไว้ในภาคผนวก (Annex) ของกฎหมาย เช่น ระบบที่ใช้ในการคัดเลือกบุคลากร การประเมินเครดิต โครงสร้างพื้นฐานดิจิทัลที่สำคัญ การบังคับใช้กฎหมาย และการควบคุมพรมแดน ระบบในระดับนี้มิได้ถูกห้าม แต่ต้องผ่านการประเมินความสอดคล้อง (conformity assessment) การจัดการความเสี่ยง การกำกับดูแลคุณภาพข้อมูล การจัดทำเอกสารทางเทคนิค การบันทึกร่องรอย (logging) ความโปร่งใส การกำกับดูแลโดยมนุษย์ (human oversight) และการขึ้นทะเบียนในฐานข้อมูลของสหภาพยุโรป

ระดับที่สาม ความเสี่ยงจำกัด (limited risk) ซึ่งหน้าที่หลักคือความโปร่งใสตามมาตรา 50 โดยเฉพาะหน้าที่แจ้งให้ผู้ใช้ทราบว่ากำลังปฏิสัมพันธ์กับระบบ AI เช่น แชตบอต และหน้าที่ติดป้ายกำกับเนื้อหาที่สร้างหรือดัดแปลงด้วย AI รวมถึงสื่อสังเคราะห์ประเภท deepfake และ

ระดับที่สี่ ความเสี่ยงน้อยหรือไม่มีนัยสำคัญ (minimal risk) ซึ่งไม่มีหน้าที่บังคับ แต่ส่งเสริมการปฏิบัติตามประมวลความประพฤติโดยสมัครใจ

ด้านการบังคับใช้ EU AI Act สถาปนาสำนักงานปัญญาประดิษฐ์แห่งยุโรป (European AI Office) ภายใต้คณะกรรมาธิการยุโรปเป็นองค์กรกำกับหลักในระดับสหภาพ โดยเฉพาะสำหรับหน้าที่ของผู้ให้บริการ Global Partnership on Artificial Intelligence หรือ GPAI ควบคู่กับคณะกรรมการปัญญาประดิษฐ์ (AI Board) และหน่วยงานผู้มีอำนาจระดับชาติของแต่ละรัฐสมาชิก[29]

ในด้านบทลงโทษ EU AI Act กำหนดโทษปรับทางปกครองในระดับสูงตามมาตรา 99 โดยการกระทำที่ต้องห้ามมีโทษปรับสูงสุดถึง 35 ล้านยูโร หรือร้อยละ 7 ของยอดผลประกอบการทั่วโลกต่อปี แล้วแต่จำนวนใดจะสูงกว่า การไม่ปฏิบัติตามข้อกำหนดของระบบความเสี่ยงสูงมีโทษปรับสูงสุด 15 ล้านยูโร หรือร้อยละ 3

[29] GDPR Local. (2025, November 19). EU AI Act summary: Europe's AI regulation. https://gdprlocal.com/eu-ai-act-summary/

และการให้ข้อมูลอันเป็นเท็จต่อหน่วยงานมีโทษสูงสุด 7.5 ล้านยูโร หรือร้อยละ 1 ซึ่งเป็นเพดานโทษที่สูงกว่า General Data Protection Regulation หรือ GDPR อย่างมีนัยสำคัญ โดยมีเพดานที่ผ่อนปรนสำหรับวิสาหกิจขนาดกลาง ขนาดย่อม และสตาร์ตอัป[30]

นอกจากนี้ เช่นเดียวกับ GDPR AI Act มีผลนอกอาณาเขต (extraterritorial reach) ตามมาตรา 2 กล่าวคือ กฎหมายใช้บังคับแก่ผู้ให้บริการที่นำระบบ AI ออกสู่ตลาดสหภาพยุโรป หรือให้บริการในสหภาพยุโรป ตลอดจนกรณีที่ผลลัพธ์ (output) ของระบบถูกนำไปใช้ในสหภาพยุโรป โดยไม่คำนึงว่าผู้ให้บริการจะตั้งอยู่ที่ใด[31] คุณลักษณะนี้ก่อให้เกิดสิ่งที่นักวิชาการเรียกว่า "ปรากฏการณ์บรัสเซลส์" (Brussels effect) ที่ทำให้มาตรฐานของยุโรปกลายเป็นจุดอ้างอิงโดยพฤตินัยสำหรับผู้ประกอบการและผู้กำกับดูแลนอกสหภาพ[32]

สถานการณ์การกำกับดูแลปัญญาประดิษฐ์ของประเทศไทย

ประเทศไทยยังไม่มีกฎหมายเฉพาะว่าด้วยปัญญาประดิษฐ์ที่มีผลใช้บังคับเหมือนสหภาพยุโรป การกำกับดูแลปัจจุบันยังคงตั้งอยู่บนฐานของกฎหมายเดิมมาปรับใช้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ ETDA จัดทำ (ร่าง) พระราชบัญญัติว่าด้วยการส่งเสริมและสนับสนุนนวัตกรรมปัญญาประดิษฐ์แห่งประเทศไทย พ.ศ.....” “(ร่าง) ประกาศเรื่องศูนย์ทดสอบนวัตกรรมปัญญาประดิษฐ์ (AI Sandbox)”

---

[30] Legiscope. (2026, May 23). EU AI Act deadlines 2026–2027: Compliance calendar + fines. https://www.legiscope.com/blog/eu-ai-act-timeline-deadlines.html

[31] Legiscope. Loc. cit.

[32] European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

และ “(ร่าง) ประกาศเรื่องการประเมินความเสี่ยงจากการใช้ระบบปัญญาประดิษฐ์”[33] แต่ปัจจุบันก็ยังมิได้มีการบัญญัติเป็นกฎหมาย

ข้อเสนอแนะในการแก้ไขปัญหาดีพเฟค

1. ประเทศไทยควรมีการบัญญัติกฎหมายเฉพาะในการควบคุมเทคโนโลยีปัญญาประดิษฐ์ โดยกำหนดองค์กรเฉพาะในดูแลควบคุม กำหนดเกณฑ์การประเมินความเสี่ยง ตลอดจนกำหนดบทลงโทษทั้งทางแพ่งและทางอาญาที่มากพอและเหมาะสมในการควบคุม โดยอาจใช้แนวทางของ EU AI Act มาเป็นต้นแบบ

2. ควรมีการกำหนดนิยามคำว่า “ดีพเฟค” ที่ชัดเจนควรมีการรวบรวมฐานความผิดที่เกิดจากดีพเฟคไว้ในกฎหมายเฉพาะฉบับเดียว

[33] ไทยรัฐ. (2567, 5 มกราคม). ยุคแห่งปัญญาประดิษฐ์ รวบรวมกฎหมายและการกำกับดูแล AI ในไทยไปถึงไหนแล้ว?. https://www.thairath.co.th/money/tech_innovation/digital_transformation/2752978

บรรณานุกรม

European Commission. (n.d.). Regulatory framework on artificial intelligence (AI Act). Shaping Europe's Digital Future. Retrieved June 27, 2026, from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

GDPR Local. (2025, November 19). EU AI Act summary: Europe's AI regulation. https://gdprlocal.com/eu-ai-act-summary/

Han, M. (2024). The infringement of deepfake technology on personal privacy and legal protection: A discussion based on Article 1032 of the Civil Code. Journal of Education, Humanities and Social Sciences. https://doi.org/10.54097/s0a47e08

https://www.thairath.co.th/money/tech_innovation/digital_transformation/2752978

iProov. (2023). Voice Biometrics For Private Banking and Wealth Management: ความรู้สึกปลอดภัยที่ผิดพลาด?. https://www.iproov.com/th/blog/voice-biometrics-false-security

Judge, E. F., & Korhani, A. M. (2021). Deepfakes, Counterfeits, and Personality. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3893890

Kugler, M., & Pace, C. (2021). Deepfake privacy: Attitudes and regulation. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3781968

Legiscope. (2026, May 23). EU AI Act deadlines 2026–2027: Compliance calendar + fines. https://www.legiscope.com/blog/eu-ai-act-timeline-deadlines.html

Meti, V. (2026). Can women's dignity endure the deepfake era? Non-consensual intimate imagery and the fragility of personality rights in India. Lex Is Us Law Journal. https://doi.org /10.65393/liuv5112

Nut Chukamphaeng. 2019. GANs: อะไรคือGenerativeAdversarialNetworks. https://medium.com/@nutorbitx/gans-%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3%E0%B8%84%E0%B8%B7%E0%B8%AD-generative-adversarial-networks-7973ae70db70

P, J. (2025). Navigating the legal framework for deepfake technology in the era of intellectual property andpersonal rights. International Journal for Multidisciplinary Research, 7(2). https://doi.org/10.36948/ijfmr.2025.v07i02.37887

ThaiDeka. คำพิพากษาศาลฎีกาที่ 3510/2531. https://deka.in. th/deka/2531-3510-105530, คำพิพากษาศาลฎีกาที่ 6301/2533. https://deka.in.th/deka/2533-6301-110201

ชยพล ธานีวัฒน์. การบังคับใช้กฎหมายเพื่อรับมือกับข่าวปลอม (Fake News). https://old.parliament.go.th/ewtadmin/ewt/elaw_parcy/ewt_dl_link.php?nid=2439

ไทยพีบีเอส. 2567. "มายด์ 4 EVE" ร้องถูกตัดต่อภาพอนาจาร พบ 46 ดาราโดนด้วย https://www. thaipbs.or.th/news/content/335822

ไทยรัฐ. (2567, 5 มกราคม). ยุคแห่งปัญญาประดิษฐ์ รวบรวมกฎหมายและการกำกับดูแล AI ในไทย ไปถึงไหนแล้ว?https://www.thairath.co.th/money/tech_innovation/digital_transformation/2752978

บีบีซี นิวส์ไทย. 2025. เปิดคดีคลิปลวงดีพเฟค (Deepfake) สาวอินเดียถูกขโมยตัวตนไปสร้างคลิปอนาจารด้วยเอไอhttps://www.bbc.com/thai/articles/czdv909gvpjo.

วิภูพงศ์ จิระประภูศักดิ์. (2558). การศึกษาวัฒนธรรมย่อยและการวิเคราะห์อัตลักษณ์ของกลุ่มเฮฟวี่เมทัล กรณีศึกษากลุ่มเฮฟวี่เมทัลในเขตอำเภอเมืองเชียงใหม่ = A Study of subculture and identity analysis of heavy metal group: A Case study of heavy metal group in Mueang, Chiang Mai / วิภูพงศ์ จิระประภูศักดิ์. เชียงใหม่ บัณฑิตวิทยาลัย มหาวิทยาลัยเชียงใหม่.

สภาองค์กรของผู้บริโภค. 2568. ภัยดีพเฟคพุ่ง หลังคนดังถูกปลอมหน้า – เสียงเอไอใช้หลอกเต็มรูปแบบ. https://www.tcc.or.th/deepfake-scam/