วารสารนิติศาสตร์
มหาวิทยาลัยธรรมศาสตร์
THAMMASAT LAW JOURNAL

ชื่อเรื่อง : มาตรการกากับดูแลการใช้งานระบบปัญญาประดิษฐ์

ชื่อผู้แต่ง : พัฒนาพร โกวพัฒนกิจ, ปิยะบุตร บุญอร่ามเรือง

การอ้างอิงที่แนะนำ : พัฒนาพร โกวพัฒนกิจ, ปิยะบุตร บุญอร่ามเรือง, ‘มาตรการกากับดูแลการใช้งานระบบปัญญาประดิษฐ์’ (2567) 53(1) วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 112.

โครงการวารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ เลขที่ 2 ถนนพระจันทร์ แขวงพระบรมมหาราชวัง เขตพระนคร กรุงเทพมหานคร 10200 โทร. 02 613 2109 อีเมล tu.lawjournal@tu.ac.th

มาตรการกำกับดูแลการใช้งานระบบปัญญาประดิษฐ์*

Regulation on Artificial Intelligence Deployment

พัฒนาพร โกวพัฒนกิจ
รองศาสตราจารย์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
Patanaporn Kowpatanakit
Associate Professor, Faculty of Law, Chulalongkorn University
ปิยะบุตร บุญอร่ามเรือง
รองศาสตราจารย์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
Piyabutr Bunaramrueang
Associate Professor, Faculty of Law, Chulalongkorn University

วันที่รับบทความ 10 กรกฎาคม 2566; วันแก้ไขบทความ 11 พฤศจิกายน 2566; วันตอบรับบทความ 23 มกราคม 2567

บทคัดย่อ

ประเด็นข้อกังวลการใช้งานระบบปัญญาประดิษฐ์นั้น ที่จริงแล้วไม่ใช่ประเด็นทางเทคนิคที่เข้าใจยากหรือเป็นประเด็นที่ขัดขวางการพัฒนา แต่เป็นเรื่องการประเมินและติดตามและผลกระทบเป็นสำคัญ กล่าวคือ มาตรการประเมินและติดตามอย่างไรที่เหมาะสม และเมื่อไหร่ที่ควรจะประเมินและติดตาม เพื่อให้เกิดผลสัมฤทธิ์ด้านการพัฒนาที่พึงปรารถนา โดยเฉพาะประเด็นอคตินั้นย่อมไม่มีใครต้องการให้เกิดขึ้น แต่หากไม่มีการบริหารจัดการความเสี่ยงที่ดีพอ ก็อาจจะกลายเป็นปัญหาใหญ่ได้

* บทความนี้ปรับปรุงมาจากงานบางส่วนของโครงการจัดทำระเบียบ มาตรการ และมาตรฐานที่เกี่ยวข้องกับปัญญาประดิษฐ์ (Artificial Intelligence: AI) เสนอต่อ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (2565).

ดังนั้น จึงเป็นที่มาที่กล่าวได้ว่า ทั่วโลกเริ่มให้ความสำคัญและเริ่มออกแนวทางการกำกับดูแลการใช้งานปัญญาประดิษฐ์ โดยจำแนกได้เป็น 2 ลักษณะ ได้แก่ การกำกับดูแลแบบทั่วไป (general regulation) และการกำกับดูแลเฉพาะเรื่อง (sector-specific regulation)

คำสำคัญ : ปัญญาประดิษฐ์, การกำกับดูแล, การประเมินความเสี่ยง, การประเมินเทคโนโลยี

Abstract

Concerns on artificial intelligence (AI) are neither technical nor impedimental to technological progress. It is about assessing and monitoring for what and when would be appropriate to regulate with desirable advancement. Especially, nobody would accept systemic bias to exist in any AI system. Without proper risk management, the bias would become a major problem unintentionally. It is therefore an increasing awareness and movement at moment to introduce AI regulations around the world which include general regulation and sector-specific regulation.

Keywords: Artificial Intelligence, regulation, risk assessment, technology assessment

1. ข้อกังวลกับแนวทางการประเมินเทคโนโลยี

ปัจจุบัน การใช้งานระบบปัญญาประดิษฐ์เป็นที่ยอมรับและใช้งานกันอย่างกว้างขวาง โดยเฉพาะสถานการณ์ที่โลกได้รู้จักกับระบบปัญญาประดิษฐ์เพื่อการสร้างใหม่ (จากชุดข้อมูลที่มีอยู่เดิม) หรือที่เรียกว่า “Generative AI” อันเป็นที่มาของความตื่นเต้นของพัฒนาการก้าวกระโดดทางเทคโนโลยีครั้งใหญ่นี้ เช่น ChatGPT ที่สามารถโต้ตอบคำถามแบบบทสนทนาอย่างลื่นไหลจนเริ่มมองกันว่าเป็นยุคต่อไปของระบบสืบค้นข้อมูลทางเว็บไซต์ หรือแม้กระทั่งสามารถใช้ทำการบ้านและสอบแทนมนุษย์ได้ หรือ DALL-E ที่สามารถสร้างภาพกราฟิกใหม่จากอินพุต (input) ข้อความได้อย่างน่าทึ่ง ทำให้เกิดความกังวลเรื่องลิขสิทธิ์และงานศิลปะ เป็นต้น[1] และเช่นเดียวกับทุกเทคโนโลยีและความตื่นเต้นครั้งใหม่บนโลกจะนำมาพร้อมกับความกังวลทางสังคม และหลายครั้งนำไปสู่ประเด็นปัญหาใหม่ที่เรายังไม่เข้าใจมาก่อน ซึ่งสำหรับกรณี ChatGPT ก็นำมาซึ่งความกังวลเกี่ยวกับการศึกษาที่ศาสตราจารย์ชอมสกี้เรียกว่า “การลอกเลียนวรรณกรรมขั้นสูง” (hi-tech plagiarism)[2] หรือบางท่านก็เรียกว่า “เฟ้นสุ่มเจรจาอย่างนกแก้ว” (stochastic parrots)[3] อันแสดงให้เห็นลักษณะของปัญหาและระดับความเข้าใจที่จำเป็นต้องมีในการใช้งานระบบปัญญาประดิษฐ์

โดยบทความนี้จะได้นำเสนอเป็น 4 ส่วนตามลำดับ โดยอธิบายข้อกังวลของการใช้งานระบบปัญญาประดิษฐ์นี้ในฐานะที่เป็นเทคโนโลยีใหม่ในส่วนแรกนี้ และแสดงให้เห็นว่าข้อกังวลดังกล่าวไม่ใช่เรื่องใหม่ แต่เคยเกิดขึ้นมาแล้วกับเทคโนโลยีในอดีต ซึ่งจะนำไปสู่การจัดการด้วยการประเมินเทคโนโลยีเพื่อการจัดการความเสี่ยง ส่วนที่สองจะได้อธิบายประเด็นทั่วไปในการประเมินการใช้งานระบบปัญญาประดิษฐ์เพื่อเข้าสู่รายละเอียดที่สำคัญของการประเมินในปัจจุบัน ส่วนที่สามจะได้อธิบายประเด็นเฉพาะภาคอุตสาหกรรมของการใช้งานระบบปัญญาประดิษฐ์เพื่อให้เห็นแนวโน้มการกำกับดูแล

---

[1] ดู John Naughton, ‘ChatGPT Isn’t a Great Leap Forward, It’s an Expensive Deal with the Devil’ (The Observer, 4 February 2023) <https://www.theguardian.com/commentisfree/2023/feb/04/chatgpt-isnt-a-great-leap-forward-its-an-expensive-deal-with-the-devil> สืบค้นเมื่อ 3 กรกฎาคม 2566; Laurie Clarke, ‘When AI Can Make Art – What Does It Mean for Creativity?’ (The Observer, 12 November 2022) <https://www.theguardian.com/technology/2022/nov/12/ when-ai-can-make-art-what-does-it-mean-for-creativity-dall-e-midjourney> สืบค้นเมื่อ 3 กรกฎาคม 2566.

[2] EduKitchen, ‘Chomsky on ChatGPT, Education, Russia and the Unvaccinated’ (21 January 2023) <https://www.youtube.com/watch?v=IgxzcOugvEI> สืบค้นเมื่อ 3 กรกฎาคม 2566.

[3] Emily M. Bender and others, ‘On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?’, *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2021) <https://dl.acm.org/doi/10.1145/3442188.3445922> สืบค้นเมื่อ 2 กรกฎาคม 2566.

เฉพาะที่เกิดขึ้นพร้อม ๆ กันด้วย เพื่อให้ผู้อ่านได้เห็นภาพใหญ่ของการกำกับดูแลเทคโนโลยีใหม่ว่ามีลักษณะอย่างไร เพื่อนำไปสู่ส่วนสุดท้ายที่จะสรุปและนำเสนอว่ามีมาตรการจัดการความเสี่ยงเชิงป้องกันแบบทั่วไปประกอบกับมาตรการแบบอื่น ๆ อย่างไร อนึ่ง ผู้เขียนมุ่งเน้นอธิบายและนำเสนอเพียงมุมมองการกำกับดูแลการใช้งานระบบปัญญาประดิษฐ์เท่านั้น ซึ่งจะเป็นการพุ่งเป้าไปที่การประเมินและการจัดการความเสี่ยงเป็นสำคัญ ไม่รวมถึงประเด็นแวดล้อมอื่น ๆ ที่เกี่ยวข้องสำคัญ อาทิ ประเด็นการส่งเสริมและการลงทุน ประเด็นการมีส่วนร่วมของภาคอุตสาหกรรม หรือประเด็นสัญญาอัตโนมัติ ซึ่งล้วนเป็นประเด็นสำคัญที่ควรต้องมีบทความอธิบายแยกไปต่างหากในแต่ละประเด็นต่อไป

ที่จริงแล้วความกังวลเกี่ยวกับปัญญาประดิษฐ์ไม่ใช่ของใหม่ อย่างน้อยกรณีของแชทบอท (chatbot) เคยเกิดขึ้นมาก่อนหน้านี้แล้วตั้งแต่ปี 1966 ในชื่อ Eliza[4] ที่ขณะนั้นก็สร้างความตื่นเต้นในลักษณะเดียวกันกับ ChatGPT ที่คนเริ่มมีความกังวลและมองว่ามีความใกล้เคียงมนุษย์[5] ปัจจุบันมีการถกเถียงถึงประเด็นปัญหาทางสังคมและเศรษฐกิจดังกล่าวอย่างกว้างขวาง[6] แต่โดยสรุปอาจกล่าวได้ว่ามีความกังวลทางสังคมที่อาจเรียกได้ว่าเป็นประเด็นทางจริยธรรมใน 3 ประเด็นหลัก[7] ได้แก่

- ความเป็นส่วนตัวและการเฝ้าระวัง (privacy and surveillance) เพราะระบบปัญญาประดิษฐ์จำเป็นต้องประมวลผลข้อมูลจำนวนมหาศาล โดยเฉพาะกรณีที่ใช้ในการเฝ้าระวัง เช่น กล้องวงจรปิด

---

[4] Joseph Weizenbaum, 'ELIZA' (Communications of the ACM, 1966) <https://redirect.cs.umbc.edu/courses/331/ papers/eliza.html> สืบค้นเมื่อ 4 กรกฎาคม 2566; 'Eliza (Elizabot.Js)' (mass:werk) <https://www.masswerk.at/elizabot/ #ELIZA> สืบค้นเมื่อ 4 กรกฎาคม 2566.

[5] John Naughton (เชิงอรรถ 1).

[6] ดู Julia Bossmann, 'Top 9 Ethical Issues in Artificial Intelligence' (World Economic Forum, 21 October 2016) <https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/> สืบค้นเมื่อ 4 กรกฎาคม 2566; 'Artificial Intelligence' (UNESCO) <https://www.unesco.org/en/artificial-intelligence> สืบค้นเมื่อ 7 กรกฎาคม 2566; 'OECD AI Principles Overview' (The OECD Artificial Intelligence Policy Observatory) <https://oecd.ai/en/> สืบค้นเมื่อ 4 กรกฎาคม 2566; George Lawton, 'Generative AI Ethics: 8 Biggest Concerns' (Enterprise AI, 18 April 2023) <https://www.techtarget.com/searchenterpriseai/tip/Generative-AI-ethics-8-biggest-concerns> สืบค้นเมื่อ 4 กรกฎาคม 2566; Vincent C. Müller, 'Ethics of Artificial Intelligence and Robotics' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Summer 2021, Metaphysics Research Lab, Stanford University 2021) <https://plato.stanford.edu/archives/sum2021/entries/ethics-ai/> สืบค้นเมื่อ 4 กรกฎาคม 2566.

[7] Christina Pazzanese, 'Ethical Concerns Mount as AI Takes Bigger Decision-Making Role' (*Harvard Gazette*, 26 October 2020) <https://news.harvard.edu/gazette/story/2020/10/ethical-concerns-mount-as-ai-takes-bigger-decision-making-role/> สืบค้นเมื่อ 3 สิงหาคม 2565.

ที่สามารถตรวจจับลักษณะของรูปร่างและการแต่งกาย และอาจรวมถึงใบหน้า ที่มีความสุ่มเสี่ยงจะกระทบสิทธิขั้นพื้นฐานของมนุษย์ กรณีเช่นนี้จึงมีความจำเป็นอย่างมากที่จะต้องระมัดระวังและใช้งานตามที่จำเป็น

- อคติและการเลือกปฏิบัติ (bias and discrimination) เพราะระบบปัญญาประดิษฐ์เป็นกลไกที่ทำหน้าที่ตัดสินใจโดยอัตโนมัติไปตามข้อมูลที่ได้รับ ซึ่งเกิดจากวิธีการที่มนุษย์กำหนดเป็นเบื้องต้น แต่อาจไม่ได้ติดตามตรวจสอบโดยตลอด และมีความเป็นไปได้ว่าการตัดสินใจหลายกรณีอาจกระทบต่อสิทธิขั้นพื้นฐานของมนุษย์โดยไม่ได้ตั้งใจหรือทราบถึงผลร้ายที่จะเกิดขึ้นเช่นนั้นมาก่อน เช่น กรณีที่ระบบอาจประเมินเครดิตของบุคคลไปอย่างมีอคติตามเชื้อชาติเพราะข้อมูลเดิมที่ระบบใช้ในการฝึกปรากฏอคติเช่นนั้นอยู่เดิมก่อนแล้วในสังคม กรณีเช่นนี้จึงมีความจำเป็นที่จะต้องระมัดระวังตั้งแต่ในขั้นการออกแบบระบบให้แน่ใจว่าไม่มีอคติเช่นว่านั้น[8]

- บทบาทการตัดสินใจโดยมนุษย์ (role of human judgment) เพราะระบบปัญญาประดิษฐ์ทำงานโดยอัตโนมัติแทนมนุษย์ และอาจถึงขนาดว่าตัดสินใจไปตามสถานการณ์ที่เหมาะสมแทนมนุษย์ อย่างไรก็ดี เมื่อระบบปัญญาประดิษฐ์สามารถตัดสินใจเองได้ ย่อมนำมาสู่คำถามสำคัญว่าจะมีบทบาทของมนุษย์อย่างไร เช่น ระบบต่าง ๆ ดั้งเดิมที่มุ่งเน้นให้มีมนุษย์อยู่ท่ามกลางกระบวนการที่จะสามารถมีเวลาเพียงพอที่จะยับยั้งการทำงานของระบบได้ ณ ขณะที่เกิดปัญหา หรือที่เรียกว่า “human in the loop” แต่ในสถานการณ์ที่ใช้ระบบปัญญาประดิษฐ์อาจแตกต่างออกไปเพราะการตัดสินใจนั้นอยู่ในหลักเสี้ยววินาทีที่มนุษย์ไม่มีความสามารถจะทำเช่นนั้นได้

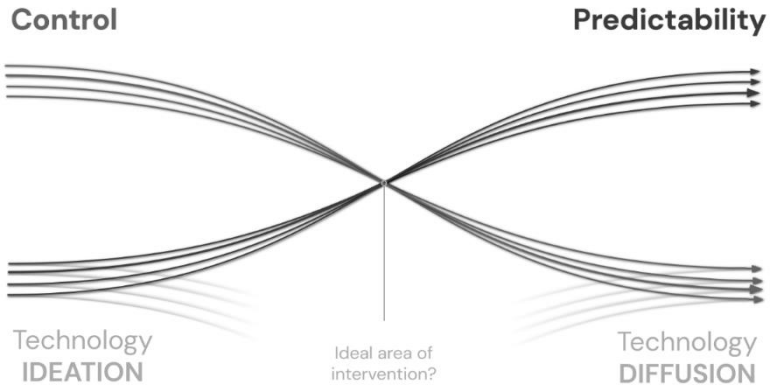
นอกจากนี้ยังมีความกังวลอื่น ๆ ทางสังคม เช่น การว่างงานที่มีแนวโน้มจะเกิดขึ้นจากการใช้ระบบปัญญาประดิษฐ์เข้ามาทดแทน หรือปัญหาการบิดเบือนหรือสร้างข้อมูลเท็จอันเนื่องมาจากการทำงานของระบบเพื่อบรรลุเป้าหมายที่กำหนดให้โต้ตอบโดยอาจสร้างข้อมูลเท็จขึ้นมาให้ผู้ใช้งานพึงพอใจ หรือความกังวลว่าระบบปัญญาประดิษฐ์จะกลายเป็นภัยแก่มนุษยชาติได้หากไม่มีการควบคุมดูแล เป็นต้น[9]

---

[8] ‘อคติ’ ในที่นี้หมายถึง ผลลัพธ์ของการประมวลผลที่ไม่พึงประสงค์เพราะไม่ได้ตรวจสอบให้ดีพอหรือระมัดระวังให้ดีพอในเชิงข้อมูลหรือกระบวนการ ในบางที่อาจเรียกใช้คำว่า อคติ แต่หมายถึงผลลัพธ์ที่แตกต่างไปตามกลุ่มเพศหรือพฤติกรรมบางประการที่มีลักษณะค่อนข้างเฉพาะ เช่น Cirillo D and others, ‘Sex and Gender Differences and Biases in Artificial Intelligence for Biomedicine and Healthcare’ (2020) 3 npj Digital Medicine 1 เป็นต้น, อย่างไรก็ดี นัยดังกล่าวไม่ใช่อคติในความหมายที่อธิบายในที่นี้ ดูรายละเอียดความหมายเพิ่มเติมในส่วนต่อไป.

[9] ดู Sharad Gandhi, ‘Social Concerns About Artificial Intelligence’ (Medium, 9 June 2018) <https://medium.com/ @sharad.gandhi/social-concerns-about-artificial-intelligence-93e939b88a8c> สืบค้นเมื่อ 3 สิงหาคม 2565; Josh Taylor and Alex Hern, ‘“Godfather of AI” Geoffrey Hinton Quits Google and Warns over

ภาพที่ 1 แสดงระดับความสามารถในการควบคุม (Control) เปรียบเทียบระดับความสามารถในการคาดหมายผลกระทบ (Predictability) ตามช่วงเวลา



ที่มา : Vourdaki A, 'What Is the Collingridge Dilemma and Why Is It Important for Tech Policy?' (*Demos Helsinki*, 15 February 2022), adapted from Fabio Besti and Francesco Samore, 'Responsibility Driven Design for the Future Self-Driving Society' (Giannino Bassetti Foundation 2022).

อย่างไรก็ดี ประเด็นความกังวลเหล่านี้ย่อมมีเกิดขึ้นเมื่อมีเทคโนโลยีใหม่ที่เราอาจจะยังไม่คุ้นเคยและไม่เข้าใจดีพอ นำมาสู่ความพยายามที่จะควบคุมหรือกำกับดูแลเทคโนโลยีดังกล่าว ซึ่งที่จริงแล้วก็เกิดขึ้นกับเทคโนโลยีใหม่ ๆ ในอดีตมาแล้วทั้งสิ้น ดังแสดงตามภาพข้างต้นในลักษณะปัญหาทางสองแพร่งของคอลลิงกริดจ์ (Collingridge Dilemma) ที่ว่า "ถ้ามันเปลี่ยนง่าย เราก็ไม่รู้ตัวว่าจะต้องทำอะไร แต่พอรู้ตัวว่าต้องทำอะไรซักอย่าง การจะเปลี่ยนแปลงนั้นก็ยากแล้ว"[10] หรืออีกนัยหนึ่งกล่าวได้ว่า การเปลี่ยนแปลงหรือกำกับดูแลเทคโนโลยีในช่วงเริ่มต้นที่ยังไม่มีการใช้งานอย่างกว้างขวาง

Dangers of Misinformation' (The Guardian, 2 May 2023) <https://www.theguardian.com/technology/2023/may/02/geoffrey-hinton-godfather-of-ai-quits-google-warns-dangers-of-machine-learning> สืบค้นเมื่อ 5 สิงหาคม 2566; Chris Vallance, 'AI Risks Leading Humanity to "extinction," Experts Warn' (NBC News, 30 May 2023) <https://www.nbcnews.com/tech/tech-news/ai-risks-leading-humanity-extinction-experts-warn-rcna86791> สืบค้นเมื่อ 5 กรกฎาคม 2566; 'Elon Musk among Experts Urging a Halt to AI Training' (BBC News, 29 March 2023) <https://www.bbc.com/news/technology-65110030> สืบค้นเมื่อ 5 กรกฎาคม 2566; 'How to Worry Wisely about Artificial Intelligence' (The Economist, 20 April 2023) <https://www.economist.com/ leaders/2023/04/20/how-to-worry-wisely-about-artificial-intelligence> สืบค้นเมื่อ 5 กรกฎาคม 2566.

[10] David Collingridge, *The Social Control of Technology* (St Martin's Press 1980) 11.

นั้นง่าย แต่เราก็จะยังไม่ทราบว่าสังคมจะได้รับผลกระทบอย่างไร ต่อเมื่อเทคโนโลยีนั้นได้รับการใช้งานอย่างกว้างขวาง เราก็จะทราบดีถึงผลกระทบของเทคโนโลยีนั้น แต่เมื่อนั้นก็ยากแล้วที่จะเปลี่ยนแปลงอะไร

ตัวอย่างที่น่าจะเด่นชัดที่สุดในเรื่องนี้ ได้แก่ พัฒนาการของเทคโนโลยีอินเทอร์เน็ต ที่แต่เดิมนั้นไม่มีใครคาดคิดว่าจะมีผลกระทบเชิงลบทางสังคม ทำให้ในระยะแรก ณ จุดเริ่มต้นของอินเทอร์เน็ตได้ออกแบบโดยโครงสร้างพื้นฐานเป็นโครงข่ายที่ไม่มีระบบรักษาความปลอดภัย (unsecured network) ซึ่งที่จริงแล้วก็เป็นคุณลักษณะพื้นฐานของระบบแบบเปิดที่ต้องการส่งเสริมให้มีการพัฒนาและขยายตัวอย่างรวดเร็ว การรักษาความมั่นคงปลอดภัยนั้นอาจไปอยู่ที่อุปกรณ์หรือเครื่องคอมพิวเตอร์ปลายทางเป็นสำคัญ ทำให้ในช่วงแรก 1980s มีการเติบโตของอินเทอร์เน็ตอย่างรวดเร็ว แต่ภายหลังทำให้เกิดปัญหาการโจมตีและฉ้อโกงกันทางอินเทอร์เน็ตและค่อย ๆ เพิ่มปริมาณแพร่หลายมากอย่างในปัจจุบัน ทำให้เราเห็นผลกระทบที่เป็นจุดอ่อนของเทคโนโลยีอย่างชัดเจน[11] หากเรารู้ว่าจะมีผลกระทบเช่นนี้ก่อนแต่แรก อินเทอร์เน็ตก็อาจจะไม่ใช่อินเทอร์เน็ตอย่างที่เรารู้จักในทุกวันนี้

แนวทางหนึ่งที่ใช้เป็นเครื่องมือสำคัญมาแล้วในการพิจารณากำกับดูแลเทคโนโลยีใหม่ให้เท่าทันอย่างเหมาะสม คือ “การประเมินเทคโนโลยี” หรือ TA (Technology Assessment)[12] โดยแนวทางสำคัญที่เป็นพื้นฐานของการประเมินก็คือการประเมินความเสี่ยงและผลกระทบด้านต่าง ๆ ซึ่ง

---

[11] ดู Bradley Fidler, ‘Cybersecurity Governance: A Prehistory and Its Implications’ (2017) 19 Digital Policy, Regulation and Governance 449; Craig Timberg, ‘The Real Story of How the Internet Became so Vulnerable’ (Washington Post, 30 May 2015) <http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/> สืบค้นเมื่อ 7 กรกฎาคม 2566; CBS News, ‘DARPA: Nobody’s Safe on the Internet - CBS News’, (60 Minutes, 8 February 2015) <https://www.cbsnews.com/news/darpa-dan-kaufman-internet-security-60-minutes/> สืบค้นเมื่อ 7 กรกฎาคม 2566.

[12] Ad Hoc Expert Group (AHEG), ‘First Draft of the Recommendation on the Ethics of Artificial Intelligence - UNESCO Digital Library’ (UNESCO, 2020) SHS/BIO/AHEG-AI/2020/4 REV.2 <https://unesdoc.unesco.org/ark:/48223/ pf0000373434> สืบค้นเมื่อ 8 กรกฎาคม 2566; AI Council, ‘AI Roadmap’ (UK Government 2021) <https://www.gov.uk/government/publications/ai-roadmap> สืบค้นเมื่อ 8 กรกฎาคม 2566; Rafael A. Calvo, Dorian Peters and Stephen Cave, ‘Advancing Impact Assessment for Intelligent Systems’ (2020) 2 Nature Machine Intelligence 89; Roger Clarke, ‘Principles and Business Processes for Responsible AI’ (2019) 35 Computer Law & Security Review 410; Bernd Carsten Stahl and others, ‘A Systematic Review of Artificial Intelligence Impact Assessments’ [2023] Artificial Intelligence Review <https://doi.org/10.1007/s10462-023-10420-8> สืบค้นเมื่อ 8 กรกฎาคม 2566; ‘Technology Assessment: Artificial Intelligence: Emerging Opportunities, Challenges, and Implications’ (*U.S. Government Accountability Office*, 28 March 2018) <https://www.gao.gov/products/gao-18-142sp> สืบค้นเมื่อ 8 กรกฎาคม 2566.

TA พยายามจะมองไปให้ไกลกว่าเพียงแค่ผลกระทบแต่ไปให้ถึงวิสัยทัศน์และแรงจูงใจที่ขับเคลื่อนพัฒนาการทางเทคโนโลยีซึ่งโดยสภาพเป็นภารกิจของฝ่ายนิติบัญญัติ[13] [14] และในอดีตก็จะมองว่ารัฐบาลซึ่งเป็นฝ่ายบริหารจะมี “การประเมินความเสี่ยง” หรือ RA (Risk Assessment) เป็นเครื่องมือหลักในการกำกับดูแล อย่างไรก็ดีปัจจุบัน TA และ RA ถูกใช้เป็นเครื่องมือร่วมกันและหลอมรวมกันเป็นส่วนมากเพราะปัจจัยการประเมินความเสี่ยงเป็นสำคัญ[15] ในมุมการกำกับดูแลในที่นี้จะได้กล่าวเฉพาะการประเมินความเสี่ยงที่เป็นเครื่องมือของการกำกับดูแลเฉพาะตามประเด็นที่ตอบโจทย์ข้อกังวลทางสังคมหรือจริยธรรมเท่านั้น จะไม่ได้พูดถึงแนวทางการส่งเสริมหรือขับเคลื่อนตามปัจจัยอื่น ๆ

2. ประเด็นทั่วไปเกี่ยวกับการประเมินระบบปัญญาประดิษฐ์

ในเชิงนิยามของปัญญาประดิษฐ์ปัจจุบันค่อนข้างมีความชัดเจนแล้ว โดย NIST (National Institute for Science and Technology) เป็นหน่วยงานที่รับผิดชอบกำหนดมาตรฐานสำคัญต่าง ๆ ทางเทคโนโลยีของสหรัฐอเมริกา รวมถึงประเด็นเกี่ยวกับ AI ก็เช่นเดียวกัน[16] โดยอ้างอิงนิยามความหมายว่า *“[ปัญญาประดิษฐ์ คือ] กลุ่มของระบบซอฟต์แวร์ขนาดใหญ่ที่รับสัญญาณจากสภาพแวดล้อมและดำเนินการส่งผลลัพธ์ตามสภาพแวดล้อมนั้น เช่น ข้อมูล การคาดการณ์ ข้อแนะนำ การจัดประเภท หรือการตัดสินใจที่ส่งผลต่อสภาพแวดล้อมที่กำลังมีปฏิสัมพันธ์อยู่ด้วยกันพร้อม ๆ กับการส่งออกผลลัพธ์อื่น ๆ”*[17]

---

[13] Rinie van Est, Bart Walhout and Frans Brom, ‘Risk and Technology Assessment’ in Sabine Roeser and others (eds), *Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk* (Springer Netherlands 2012) <https://doi.org/10.1007/978-94-007-1433-5_43> สืบค้นเมื่อ 8 กรกฎาคม 2566; Raija Koivisto and others, ‘Integrating Future-Oriented Technology Analysis and Risk Assessment Methodologies’ (2009) 76 Technological Forecasting and Social Change 1163.

[14] Anne De Piante Henriksen, ‘A Technology Assessment Primer for Management of Technology’ (1997) 13 International Journal of Technology Management 615, ซึ่งประกอบไปด้วยวิธีการประเมินต่าง ๆ รวมถึงการวิเคราะห์ทางเศรษฐกิจ (Economic Analysis) การวิเคราะห์การตัดสินใจ (Decision Analysis) การวิเคราะห์ระบบ (System Analysis) การคาดการณ์ทางเทคโนโลยี (Technological Forecasting) การติดตามข้อมูล (Information Monitoring) การประเมินผลสัมฤทธิ์ทางเทคนิค (Technical Performance Assessment) การประเมินความเสี่ยงหรือ RA (Risk Assessment) การวิเคราะห์ตลาด (Market Analysis) และการวิเคราะห์ผลกระทบหรือปัจจัยภายนอก (Externalities/Impact Analysis).

[15] Rinie van Est, Bart Walhout and Frans Brom (เชิงอรรถ 13).

[16] Reva Schwartz and others, ‘Towards a Standard for Identifying and Managing Bias in Artificial Intelligence’ (2022) <https://www.nist.gov/publications/towards-standard-identifying-and-managing-bias-artificial-intelligence> สืบค้นเมื่อ 22 มิถุนายน 2565. *hereafter* “NIST Bias Guidance.”

[17] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2020).

ในปี 2019 OECD ได้เสนอนิยามของระบบปัญญาประดิษฐ์ว่าหมายถึง

> ระบบที่ใช้เครื่องจักรที่สามารถทำการคาดการณ์ ให้คำแนะนำ หรือตัดสินใจที่มีอิทธิพลต่อสภาพแวดล้อมจริงหรือเสมือนตามชุดของวัตถุประสงค์ที่กำหนดไว้โดยมนุษย์ โดยใช้เครื่องและ/หรือมนุษย์ในการนำเข้าวัตถุดิบหรือข้อมูล (Input) เพื่อ :
>
> (1) รับรู้สภาพแวดล้อมจริงและ/หรือเสมือน
>
> (2) สกัดและตกผลึกการรับรู้ดังกล่าวเป็นแบบจำลองต่าง ๆ ผ่านการวิเคราะห์ในลักษณะอัตโนมัติ (เช่น ร่วมกับการเรียนรู้ของเครื่องหรือการทำงานด้วยมือ); และ
>
> (3) ใช้การอนุมานหรือการคาดคะเนตามหลักเหตุผลด้วยแบบจำลอง (model inference) เพื่อกำหนดตัวเลือกสำหรับข้อมูลหรือการกระทำ โดยระบบ AI ต่าง ๆ จะได้รับการออกแบบให้ทำงานด้วยระดับความเป็นอิสระ (autonomy) ที่แตกต่างกัน[18]

ในเชิงเทคนิค มีวิธีการที่ใช้ในการทำงานของระบบปัญญาประดิษฐ์มากมายหลายวิธี และมีการจำแนกประเภทได้อย่างหลากหลาย[19] แต่ไม่ว่าจะอย่างไร นิยามข้างต้นของ NIST ซึ่งเป็นความหมายอย่างกว้างเป็นที่ยอมรับอ้างอิงมากที่สุด และปรากฏในกฎหมายงบประมาณของสหรัฐอเมริกา ดังต่อไปนี้

> ปัญญาประดิษฐ์เป็นระบบเครื่องจักรโดยเฉพาะระบบคอมพิวเตอร์ที่สามารถคาดคะเน ให้คำแนะนำ หรือตัดสินใจในสิ่งแวดล้อมจริงหรือสิ่งแวดล้อมเสมือนจริงตามวัตถุประสงค์ที่มนุษย์กำหนดได้ โดยระบบปัญญาประดิษฐ์ใช้เครื่องจักรและข้อมูลที่ป้อนเข้าโดยมนุษย์ที่สามารถ

---

[18] OECD, 'Scoping the OECD AI Principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO)' (OECD, 2019) <https://www.oecd-ilibrary.org/science-and-technology/scoping-the-oecd-ai-principles_d62f618a-en> สืบค้นเมื่อ 22 มิถุนายน 2565.

[19] *See* Aryan Pegwar, 'What Is the Difference between Artificial Intelligence (AI), Machine Learning (ML) and Data Science' (Medium, 13 April 2020) <https://medium.com/@rkt10952/what-is-the-difference-between-artificial-intelligence-ai-machine-learning-ml-and-data-science-42af1fde4cc1> สืบค้นเมื่อ 4 กรกฎาคม 2566; Steve Juumta, 'What Is Artificial Intelligence? An Informed Definition' (Emerj Artificial Intelligence Research, 21 December 2018) <https://emerj.com/ai-glossary-terms/what-is-artificial-intelligence-an-informed-definition/> accessed 4 July 2023; A. L. Samuel, 'Some Studies in Machine Learning Using the Game of Checkers' (1959) 3 IBM Journal of Research and Development 210; Pagani M and Champion R, 'Making Sense of the AI Landscape' [2020] *Harvard Business Review* <https://hbr.org/2020/11/making-sense-of-the-ai-landscape> สืบค้นเมื่อ 4 กรกฎาคม 2566.

(ก) รับรู้สิ่งแวดล้อมจริงและเสมือนจริง

(ข) วิเคราะห์ข้อมูลที่เป็นนามธรรมทำให้เป็นรูปธรรมโดยอัตโนมัติ และ

(ค) ใช้แบบโครงสร้างจำลองสร้างตัวเลือกสำหรับข้อมูลหรือการปฏิบัติการ[20]

สหภาพยุโรปก็ได้มีร่างกฎหมายการกำกับดูแลการใช้งานระบบปัญญาประดิษฐ์ ซึ่งก็ได้มีการกำหนดนิยามความหมายของระบบปัญญาประดิษฐ์ในลักษณะเดียวกันเอาไว้ว่า *"ระบบปัญญาประดิษฐ์ (AI System) หมายถึง ซอฟต์แวร์ที่พัฒนาขึ้นด้วยเทคนิคและวิธีการอย่างน้อยหนึ่งอย่างที่ระบุไว้ในภาคผนวก 1*[21] *และสามารถสร้างผลลัพธ์ เช่น เนื้อหา การคาดคะเน คำแนะนำ หรือการตัดสินใจที่มีอิทธิพลต่อสภาพแวดล้อมที่พวกเขาโต้ตอบด้วย สำหรับชุดวัตถุประสงค์ที่กำหนดโดยมนุษย์"*[22]

โดยสรุปปัญญาประดิษฐ์หรือระบบปัญญาประดิษฐ์ทำงานอยู่บนองค์ประกอบ 3 ประการสำคัญ ได้แก่

(1) รับรู้สิ่งแวดล้อมจริงและเสมือนจริง

(2) ดำเนินการส่งผลลัพธ์ตามสภาพแวดล้อมโดยอัตโนมัติ เช่น ข้อมูล การคาดการณ์ ข้อแนะนำ การจัดประเภท หรือการตัดสินใจที่ส่งผลต่อสภาพแวดล้อมที่กำลังมีปฏิสัมพันธ์อยู่

(3) ใช้แบบจำลองสร้างตัวเลือกสำหรับข้อมูลหรือการปฏิบัติการที่กำหนดวัตถุประสงค์โดยมนุษย์

จะเห็นได้ว่า นิยามดังกล่าวไม่ได้ลงประเด็นที่เกี่ยวกับวิธีการทางเทคนิคหรือความซับซ้อนของระบบแต่อย่างใด ประเด็นทางเทคนิค เช่น เป็นระบบที่ใช้วิธีการแบบมีผู้ดูแลหรือไม่ (supervised or unsupervised) หรือเป็นระบบที่ใช้วิธีการทางสถิติหรือหลักเกณฑ์เชิงตรรกะหรือไม่ ล้วนไม่ใช่ประเด็นของการพิจารณาว่าเป็นปัญญาประดิษฐ์หรือไม่ในมุมมองการกำกับดูแล

---

[20] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 5002 (2021).

[21] EU AI Act, Annex I, กำหนดไว้ดังนี้ : -

(a) การเรียนรู้ของเครื่อง รวมถึงการเรียนรู้แบบมีผู้ดูแล ไม่มีผู้ดูแลและแบบเสริมกำลังการเรียนรู้ โดยใช้วิธีการที่หลากหลายรวมถึงการเรียนรู้เชิงลึก (Deep Learning)

(b) แนวทางเชิงตรรกะและฐานความรู้ รวมถึงการแทนค่าความรู้ การเขียนโปรแกรมเชิงอุปนัย (ตรรกะ) ฐานความรู้ การอนุมานและกลไกนิรนัย การให้เหตุผล (เชิงสัญลักษณ์) และระบบผู้เชี่ยวชาญ

(c) วิธีการทางสถิติ การประมาณค่าแบบเบย์ วิธีการค้นหาและการเพิ่มประสิทธิภาพ.

[22] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final, *hereafter* "EU AI Act".

ในประเด็นที่เกี่ยวกับการประเมินความเสี่ยง ในปี 2022 OECD จึงได้แนะนำกรอบแนวทางการประเมินความเสี่ยงประเมินความเสี่ยงของการใช้งานระบบปัญญาประดิษฐ์ 5 ประการ[23] ได้แก่

(1) ผู้คนและโลก (People and Planet) เป็นมิติที่พิจารณาถึงผลกระทบ (โดยเฉพาะอย่างยิ่งในเชิงบวกหรือสนับสนุน) ของระบบปัญญาประดิษฐ์ที่เชื่อถือได้และมีมนุษย์เป็นศูนย์กลางและเน้นประโยชน์ต่อผู้คนและโลก ซึ่งรวมถึงสิทธิมนุษยชน สิ่งแวดล้อม และบริบททางสังคมอื่น ๆ โดยเฉพาะอย่างยิ่งที่นอกเหนือจากประโยชน์ทางเศรษฐกิจ

(2) บริบททางเศรษฐกิจ (Economic Context) เป็นมิติพิจารณาถึงสภาพแวดล้อมที่มีการนำระบบปัญญาประดิษฐ์ไปใช้งานในภาคส่วนหรือองค์กรหนึ่ง ๆ เช่น การประยุกต์ใช้ในอุตสาหกรรมที่เกี่ยวกับสุขภาพ การเงิน และการผลิต หรืออาจพิจารณาในแง่ของการใช้งานในทางธุรกิจ ผลกระทบที่อาจจะเกิดขึ้น และขนาดของผลกระทบนั้น รวมถึงวุฒิภาวะของเทคโนโลยีที่ใช้ประกอบด้วย

(3) ข้อมูลและอินพุต (Data & Inputs) เป็นมิติที่พิจารณาข้อมูลและอินพุตที่ใช้โดยระบบปัญญาประดิษฐ์เพื่อสร้างตัวแทนของสภาพแวดล้อม โดยพิจารณารวมถึงที่มาของข้อมูล ไม่ว่าจะเป็นข้อมูลที่ครอบครองโดยภาคเอกชน ข้อมูลที่เปิดเผยต่อสาธารณะโดยภาครัฐ หรือข้อมูลส่วนบุคคล รวมถึงวิธีการเก็บรวบรวมข้อมูลด้วยเครื่องและ/หรือคน โครงสร้างและรูปแบบของข้อมูลและคุณสมบัติของข้อมูล ซึ่งอาจต้องพิจารณาถึงลักษณะของข้อมูลที่เก็บทั้งในเชิงเนื้อหา ความถี่ และความละเอียดของข้อมูล

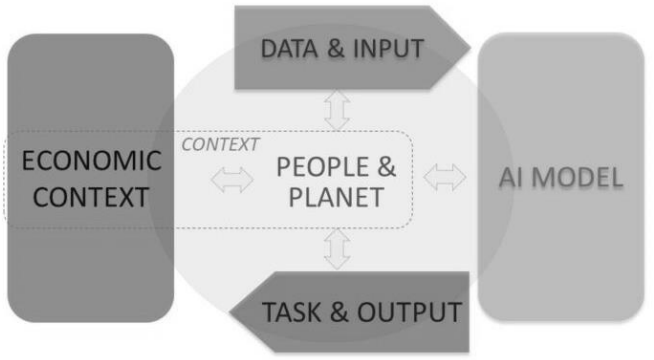
(4) แบบจำลองปัญญาประดิษฐ์ (Model) เป็นมิติของแบบจำลองปัญญาประดิษฐ์ที่เป็นตัวแทน สภาพแวดล้อมภายนอกทั้งหมดหรือบางส่วนโดยใช้การคำนวณของระบบปัญญาประดิษฐ์ ซึ่งครอบคลุมองค์ประกอบต่าง ๆ ของสภาพแวดล้อม เช่น กระบวนการ วัตถุ ความคิด ผู้คน และ/หรือปฏิสัมพันธ์ในโลกแห่งความเป็นจริง ซึ่งรวมถึงสมมติฐานเกี่ยวกับความเป็นจริง (model) โดยเฉพาะในแง่ของความสามารถในการอธิบายถึงปัจจัยที่ส่งผลต่อการตัดสินใจ หรือผลลัพธ์การประมวลผลของระบบปัญญาประดิษฐ์ได้

(5) งานและผลลัพธ์ (Tasks & Outputs) เป็นมิติของงานที่ระบบดำเนินการ เช่น การทำให้เป็นส่วนบุคคล (personalisation) หรือการรับรู้ (recognition) และผลลัพธ์ของระบบนั้นซึ่งรวมถึงการส่งอิทธิพลต่อบริบท โดยเฉพาะอย่างยิ่งการนำระบบมาใช้ในบริบทหรือสภาพแวดล้อมที่แตกต่างจากข้อมูลหรืออินพุตนั้นอาจทำให้เกิดผลที่ไม่คาดหมาย อาทิ การเลือกปฏิบัติ (discrimination) หรือความผิดพลาดที่ไม่ได้คาดหมาย (unexpected errors)

---

[23] OECD, 'OECD Framework for the Classification of AI Systems' (OECD, 2022) <https://www.oecd-ilibrary.org/ science-and-technology/oecd-framework-for-the-classification-of-ai-systems_cb6d9eca-en> สืบค้นเมื่อ 8 กรกฎาคม 2566.

ภาพที่ 2 แสดงความสัมพันธ์ของมิติการประเมินการใช้งานระบบปัญญาประดิษฐ์



ที่มา: OECD, 'OECD Framework for the Classification of AI Systems' (OECD 2022)

ในปีเดียวกัน NIST ก็ได้เผยแพร่เอกสารสำคัญอันเป็นส่วนหนึ่งของความพยายามที่จะสร้างกรอบมาตรฐานการพัฒนาระบบ AI ที่เชื่อถือได้ ได้แก่ แนวปฏิบัติเกี่ยวกับการจัดการอคติของระบบ AI หรือ "NIST Bias Guidance" โดยระบุว่ามีความเป็นไปได้ที่ระบบ AI จะมีอคติอย่างน้อย 3 ประการ[24]

- อคติของระบบ (Systemic Bias) โดยระบุว่า หมายถึง ผลจากกระบวนการและทางปฏิบัติของหน่วยงานที่ดำเนินการไปในทางที่ส่งผลให้กลุ่มทางสังคมบางกลุ่มได้รับประโยชน์หรือได้เปรียบกว่ากลุ่มอื่นที่เสียประโยชน์หรือเสียเปรียบ ซึ่งสถานการณ์นี้อาจเกิดขึ้นได้จากชุดข้อมูลที่ใช้ในการฝึกระบบ AI

- อคติของการประมวลผล (Statistical and Computational Biases) โดยระบุว่าหมายถึง ผลจากชุดตัวอย่างข้อมูลที่ไม่เหมาะสมที่จะเป็นตัวแทนของกลุ่มประชาการที่ต้องการ ซึ่งสถานการณ์นี้มักจะเกิดขึ้นจากการฝึกระบบ AI ด้วยข้อมูลประเภทเดียวซึ่งไม่สามารถอนุมานหรือขยายผลให้ใช้ได้กับชุดข้อมูลอื่น

- อคติของมนุษย์ (Human Bias) โดยระบุว่าหมายถึง ความผิดพลาดที่เกิดจากข้อจำกัดของมนุษย์ที่อยู่บนพื้นฐานของการคาดการณ์และการการคาดคะเนที่เป็นการตัดสินใจที่เร็วกว่าและง่ายกว่า ซึ่งอคติดังกล่าวเป็นพื้นฐานของการตัดสินใจของมนุษย์ เพียงแค่การทำความเข้าใจอคติดังกล่าวไม่เพียงพอที่จะควบคุมอคตินี้ได้

โดย NIST แนะนำให้ผู้พัฒนาระบบปรับใช้แนวทางที่คำนึงถึงสภาพทางสังคมและเทคโนโลยี (socio-technical approach) เพราะเทคโนโลยีเพียงอย่างเดียวไม่เพียงพอที่จะจัดการกับผลกระทบทางสังคมของระบบ AI ได้ จำเป็นต้องคำนึงถึงคุณค่าและพฤติกรรมของข้อมูล ผู้คนที่ต้องมีปฏิสัมพันธ์

[24] NIST Bias Guidance (เชิงอรรถ 16) 6-9.

กับระบบ และปัจจัยที่ซับซ้อนเชิงโครงสร้างองค์กรที่เกี่ยวข้องกับการออกแบบ พัฒนา และนำไปใช้งาน[25] และให้ข้อแนะนำ 8 ประการ[26] ดังนี้

- การติดตามตรวจสอบ (Monitoring) ได้แก่ การจัดให้มีระบบติดตามตรวจสอบเพิ่มเติม เพื่อคอยเตือนไปยังผู้รับผิดชอบหากว่าตรวจพบโอกาสที่จะเกิดปัญหา

- การรับแจ้งเพื่อแก้ไข (Recourse Channels) ได้แก่ การจัดให้มีช่องทางในการสื่อสารที่ผู้ใช้งานสามารถแจ้งเหตุหรือบอกกล่าวเกี่ยวกับผลร้ายที่อาจจะเกิดขึ้นเพื่อหาแนวทางแก้ไขผลกระทบนั้น

- นโยบายและกระบวนการ (Policies and Procedures) ได้แก่ การจัดทำนโยบายและกระบวนการภายในเป็นลายลักษณ์อักษรเพื่อกำหนดบทบาทความรับผิดชอบและกระบวนการในแต่ละขั้นตอนของการพัฒนา AI

- การจัดทำเอกสาร (Documentation) ได้แก่ การจัดทำเอกสารต้นแบบที่สร้างมาตรฐานของการพัฒนาพร้อมระบุคำอธิบายต่าง ๆ ของระบบเพื่อให้ผู้รับผิดชอบตรวจสอบสามารถเข้าใจและพิจารณาดำเนินการต่อสิ่งที่อาจจะเกิดขึ้นได้อย่างเหมาะสมกับความเสี่ยง

- ความรับผิดชอบ (Accountability) ได้แก่ การจัดให้มีบุคลากรหรือทีมงานรับผิดชอบโดยเฉพาะต่อการจัดการอคติของระบบ AI

- วัฒนธรรมและการปฏิบัติ (Culture & Practice) ได้แก่ การที่หน่วยงานให้ความสำคัญกับการจัดการความเสี่ยงแม้ไม่ได้มีเขียนระบุไว้ที่ใดก็ตาม ซึ่งมักจะปรากฏในรูปแบบของการให้ผู้เชี่ยวชาญมาตรวจสอบและตั้งคำถามต่อการพัฒนาระบบ (effective challenge) และการจัดให้มีระบบจัดการความเสี่ยงแบบ 3 lines of defense

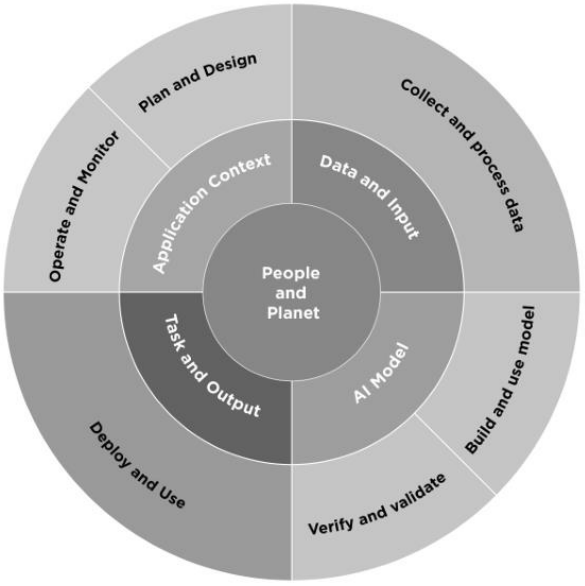
- การจัดการความเสี่ยง (Risk Mitigation, Risk Tiering & Incentive Structures) ได้แก่ ความเข้าใจว่าหัวใจของการจัดการความเสี่ยงอยู่ที่การลดความเสี่ยง (risk mitigation) ไม่ใช่การหลีกเลี่ยงความเสี่ยง (risk avoidance) กล่าวคือ ยอมรับว่ามีความเป็นไปได้ที่จะเกิดเหตุการณ์ที่ไม่พึงประสงค์แต่พร้อมที่จะเผชิญเหตุและแก้ไขปัญหานั้น

- การแลกเปลี่ยนข้อมูล (Information Sharing) ได้แก่ การแบ่งปันข้อมูลภายในหน่วยงานเกี่ยวกับเหตุการณ์หรือผลกระทบจากอคติของระบบ AI จะช่วยยกระดับของการจัดการความเสี่ยงและลดความผิดพลาดที่อาจเกิดขึ้นได้

[25] NIST Bias Guidance (เชิงอรรถ 16) 10-11.

[26] NIST Bias Guidance (เชิงอรรถ 16) 42-47.

ภาพที่ 3 แสดงความสัมพันธ์ของวงจรกระบวนการใช้งานกับมิติการประเมินระบบปัญญาประดิษฐ์



ที่มา : NIST AI 100-1 (AI RMF 1.0)

ในเดือนมกราคมปี ค.ศ. 2023 NIST ก็ได้เผยแพร่กรอบการจัดการความเสี่ยงของระบบปัญญาประดิษฐ์ หรือ AI RMF 1.0 (AI Risk Management Framework) โดยมีวัตถุประสงค์เพื่อให้หน่วยงานหรือองค์กรสามารถสร้างกรอบแนวทางการจัดการความเสี่ยงของระบบปัญญาประดิษฐ์และสามารถวิเคราะห์ผลกระทบรวมถึงบอกคุณลักษณะของระบบที่ไว้วางใจต่าง ๆ ได้ ซึ่งหมายถึงการบริหารจัดการให้มีความสมเหตุสมผลและน่าเชื่อถือ (valid and reliable) ความปลอดภัย (safe) ความมั่นคง (secure) ความทนทาน (resilient) ความโปร่งใสและรับผิดชอบ (accountable and transparent) ความสามารถในการอธิบายและแปลความหมายได้ (explainable and interpretable) การคุ้มครองความเป็นส่วนตัว (privacy) และความเป็นธรรมที่ไม่มีอคติ (fair) โดยกำหนดภารกิจหลัก 4 ประการในเรื่องนี้ ได้แก่[27]

(1) ทิศทางชัดเจน (GOVERN) เป็นภารกิจที่หน่วยงานจะต้องกำหนดหรือสร้างเป็นนโยบายหรือวัฒนธรรมขององค์กรให้ชัดเจนที่จะบริหารจัดการความเสี่ยงการใช้งานระบบปัญญาประดิษฐ์ตลอดทุกขั้นตอนและผูกพันทุกคนที่มีมีส่วนเกี่ยวข้อง

[27] 'AI Risk Management Framework' (NIST 2023) NIST AI 100-1 <https://www.nist.gov/itl/ai-risk-management-framework> สืบค้นเมื่อ 9 กรกฎาคม 2566.

(2) เห็นภาพใหญ่ (MAP) เป็นภารกิจที่ทุกกรณีของการพัฒนาหรือใช้งานระบบปัญญาประดิษฐ์ ทุกฝ่ายจะต้องเข้าใจบริบทและกิจกรรมที่เกี่ยวข้องทั้งหมด เพราะหากฝ่ายหนึ่งฝ่ายใดไม่เข้าใจภาพใหญ่ของการใช้งานก็จะทำให้ไม่สามารถคาดการณ์หรือประเมินความเสี่ยงที่อาจจะเกิดขึ้นได้ เจตนาที่ดีในตอนเริ่มต้นก็อาจจะต้องเสียไปเพราะการดำเนินการในช่วงต่อมาได้

(3) ชี้วัดรายประเด็น (MEASURE) เป็นภารกิจที่หน่วยงานจะต้องกำหนดตัวชี้วัดและวิธีการประเมินความเสี่ยงต่าง ๆ ซึ่งจะเป็นผลต่อเนื่องมาจากภารกิจ MAP และ MANAGE

(4) ตั้งเกณฑ์และติดตาม (MANAGE) เป็นภารกิจที่หน่วยงานจะต้องมีการจัดลำดับความสำคัญของความเสี่ยงและจัดสรรทรัพยากรเพื่อการประเมินและชี้วัดต่าง ๆ ตามรอบระยะเวลาที่กำหนดเพื่อให้บรรลุวัตถุประสงค์ที่เป็นเป้าหมายสำคัญ

ภาพที่ 4 ระดับความเสี่ยงของระบบปัญญาประดิษฐ์ตาม EU AI Act

ที่มา : Regulatory framework proposal on artificial intelligence | Shaping Europe’s digital future, https://digital-strategy.ec.europa.eu/es/node/9745 (last visited Jun 11, 2022).

โดยสอดคล้องกับแนวทางที่กล่าวมา ร่างกฎหมายการกำกับดูแลการใช้งานระบบปัญญาประดิษฐ์ของสหภาพยุโรปก็ได้กำหนดระดับความเสี่ยงไว้ดังต่อไปนี้

- ความเสี่ยงที่ยอมรับไม่ได้ (Unacceptable risk) ระบบปัญญาประดิษฐ์ประเภทนี้ถือเป็นภัยคุกคามต่อความปลอดภัย ความเป็นอยู่ และสิทธิของประชาชนอย่างชัดเจน ตัวอย่างเช่น ระบบการให้คะแนนทางสังคมที่กระทำโดยรัฐบาล เป็นต้น

- ความเสี่ยงสูง (High risk) ระบบปัญญาประดิษฐ์ประเภทนี้จะต้องอยู่ภายใต้ภาระหน้าที่ที่เข้มงวดก่อนที่จะนำระบบปัญญาประดิษฐ์ความเสี่ยงสูงออกสู่ตลาด โดยมีเกณฑ์ที่จะต้องผ่านการทดสอบดังนี้

  - ระบบการประเมินและบรรเทาความเสี่ยงที่เพียงพอ
  - ชุดข้อมูลคุณภาพสูงที่ป้อนให้กับระบบเพื่อลดความเสี่ยงและผลการเลือกปฏิบัติ
  - การบันทึกกิจกรรม/เหตุการณ์เพื่อให้แน่ใจว่าสามารถติดตามผลได้
  - เอกสารรายละเอียดที่ให้ข้อมูลทั้งหมดที่จำเป็นในระบบและวัตถุประสงค์ของระบบสำหรับหน่วยงานกำกับดูแลในการประเมินการปฏิบัติตาม
  - ข้อมูลที่ชัดเจนและเพียงพอแก่ผู้ใช้
  - มาตรการควบคุมดูแลที่เหมาะสมของมนุษย์เพื่อลดความเสี่ยง
  - ความยืดหยุ่น ความปลอดภัย และความแม่นยำในระดับสูง

- ความเสี่ยงจำกัด (Limited risk) มีหน้าที่ที่จะต้องทำตามหลักความโปร่งใส (transparency) ตัวอย่างเช่น ระบบแชทบอท (Chatbots)

- ความเสี่ยงน้อยที่สุด (Minimal Risk) ไม่มีภาระหน้าที่ที่จะต้องทำตามหลักเกณฑ์หรือนโยบายใด ๆ

จะเห็นได้ว่าแนวทางการประเมินความเสี่ยงได้ถูกนำมาใช้ในการประเมินเทคโนโลยีปัญญาประดิษฐ์เป็นการทั่วไปแล้วอย่างชัดเจน ข้อสังเกตประการสำคัญ ณ ที่นี้ก็คือ ไม่ใช่กรณีที่จะกำกับแบบระบบใบอนุญาต แต่เป็นการนำเอากรอบแนวคิดการประเมินความเสี่ยงและการประเมินเทคโนโลยีมาใช้ และเป็นการใช้แบบทั่วไปโดยไม่จำกัดเฉพาะเจาะจงในลักษณะการใช้งานอย่างใดอย่างหนึ่งเป็นการเฉพาะ อย่างไรก็ดี มีการใช้งานระบบปัญญาประดิษฐ์ในอุตสาหกรรมหรือการใช้งานเฉพาะบางประเภทที่จำเป็นและเริ่มมีการกำกับดูแลเฉพาะแล้ว

3. ประเด็นเฉพาะภาคอุตสาหกรรมเกี่ยวกับการประเมินระบบปัญญาประดิษฐ์

จากที่ได้กล่าวมาแล้ว แนวทางกำกับดูแลปัญญาประดิษฐ์จึงเน้นไปที่การประเมินความเสี่ยงและจัดการความเสี่ยงของเทคโนโลยีเป็นสำคัญโดยได้ยกตัวอย่างมาตการจัดการความเสี่ยงแบบทั่วไป ในส่วนนี้จะได้แสดงให้เห็นแนวโน้มการประเมินและการจัดการความเสี่ยงอีกลักษณะหนึ่งซึ่งเน้นไปที่การกำกับดูแลในรายละเอียดเฉพาะของแต่ละภาคอุตสาหกรรม (sector-specific) ที่มีความสำคัญของแต่ละประเทศต่อไปนี้

(1) แนวการกำกับดูแลการใช้งานปัญญาประดิษฐ์ในยานยนต์อัตโนมัติ

ปัจจุบัน กฎเกณฑ์ที่เกี่ยวข้องกับการใช้ยานยนต์อัตโนมัติยังไม่มีแนวทางที่เป็นหลักสากลในการกำกับดูแลเรื่องนี้ เนื่องจากสภาพการใช้รถ การใช้ถนน และข้อบังคับกฎจราจรของแต่ละประเทศมีความแตกต่างกัน แต่เนื่องจากมีพัฒนาการและเทคโนโลยีที่ก้าวหน้าในภาคอุตสาหกรรมนี้มาก ทำให้มีแนวทางในการกำกับดูแลการใช้งานปัญญาประดิษฐ์ในยานยนต์อัตโนมัติอยู่พอสมควร ซึ่งยังคงต้องสอดคล้องตามกฎหมายจราจรและกฎหมายที่เกี่ยวข้องกับยานยนต์ โดยมีตัวอย่างมาตรการกำกับดูแลปัญญาประดิษฐ์ในยานยนต์อัตโนมัติในต่างประเทศ ตามตารางต่อไปนี้

ตารางที่ 1 ตัวอย่างมาตรการกำกับดูแลปัญญาประดิษฐ์ในยานยนต์อัตโนมัติในต่างประเทศ

สหรัฐอเมริกา
นโยบายยานยนต์อัตโนมัติของรัฐบาลกลาง (Federal Automated Vehicles Policy) ออกโดยสำนักงานความปลอดภัยด้านการจราจรบนทางหลวงแห่งชาติ หรือ NHTSA (National Highway Traffic Safety Administration) เพื่อกำหนดแนวทางเกี่ยวกับการออกแบบ การพัฒนา การทดสอบ และการใช้งานยานพาหนะอัตโนมัติขั้นสูงก่อนที่จะมีการนำเข้าสู่ตลาด สำหรับกฎเกณฑ์ที่เกี่ยวกับการกำกับดูแลโดยเฉพาะนั้นจะขึ้นอยู่กับกฎหมายของแต่ละรัฐ ซึ่งมีทั้งในลักษณะของการออกเป็นกฎหมายเพื่อกำกับดูแลโดยเฉพาะ หรือเป็นการออกคำสั่งของผู้ว่าการรัฐ โดยแต่ละรัฐจะกำหนดและอนุญาตให้สามารถนำยานยนต์อัตโนมัติมาใช้บนถนนสาธารณะได้ในลักษณะของการทดสอบหรือการใช้งานจริง ซึ่งกฎหมายของแต่ละรัฐอาจมีข้อกำหนดเพิ่มเติมเกี่ยวกับการขอรับใบอนุญาต ข้อกำหนดเกี่ยวกับการใช้งานบนท้องถนน รวมถึงข้อกำหนดเกี่ยวกับการทำสัญญาประกันภัย[28]
ญี่ปุ่น
กระทรวงที่ดิน โครงสร้างพื้นฐาน การขนส่ง และการท่องเที่ยว (Ministry of Land, Infrastructure, Transport and Tourism หรือ MLIT) จัดทำแนวปฏิบัติเกี่ยวกับเทคโนโลยีเพื่อความปลอดภัยของยานพาหนะที่ขับเคลื่อนโดยอัตโนมัติ (Guidelines for the Safety Technologies of Automated Vehicles) โดยระบุถึงข้อกำหนดด้านความปลอดภัยสำหรับยานยนต์อัตโนมัติ ต่อมาได้มีการแก้ไขปรับปรุงกฎหมาย 2 ฉบับ ได้แก่ กฎหมายการจราจรทางบก (Road Traffic Act หรือ RTA) และกฎหมายเกี่ยวกับยานพาหนะขนส่งทางบก (Road Transport Vehicle Act

[28] NCSL, 'Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation' (National Conference of State Legislatures, 2020) <https://www.ncsl.org/transportation/autonomous-vehicles> สืบค้นเมื่อ 9 กรกฎาคม 2566.

หรือ RTVA) เพื่อให้ครอบคลุมถึงการใช้ยานยนต์อัตโนมัติ ซึ่งปัจจุบันกฎหมายกำหนดให้สามารถใช้ยานยนต์อัตโนมัติตามมาตรฐานของ SAE ระดับที่ 3 มาขับขี่บนถนนสาธารณะ และสามารถใช้ยานยนต์อัตโนมัติ ระดับที่ 4 ได้ในพื้นที่ที่มีจำนวนประชากรไม่มาก และต้องได้รับอนุญาตจากหน่วยงานด้านความปลอดภัยสาธารณะในพื้นที่นั้น ๆ รวมถึงกำหนดหลักเกณฑ์ต่าง ๆ เกี่ยวกับมาตรฐานความปลอดภัยและการใช้งานยานยนต์อัตโนมัติ

อิสราเอล

กรอบนโยบายยานยนต์อัตโนมัติ (Autonomous Vehicle Policy Framework) ซึ่งกำหนดถึงกรอบแนวทางและนโยบายเกี่ยวกับยานยนต์อัตโนมัติ

ในปี ค.ศ. 2018 กระทรวงคมนาคมและความปลอดภัยทางถนนได้แก้ไขกฎจราจรให้อำนาจเจ้าหน้าที่ควบคุมการจราจรอนุมัติการผ่อนผันและอนุญาตให้ใช้งานยานยนต์อัตโนมัติ รวมถึงกำหนดหลักเกณฑ์เกี่ยวกับการขออนุญาตจากหน่วยงานที่เกี่ยวข้องก่อนที่จะนำยานยนต์อัตโนมัติมาทดสอบหรือใช้บนท้องถนน

ออสเตรเลีย

ประเทศออสเตรเลียมีแนวปฏิบัติที่เกี่ยวข้องกับยานยนต์อัตโนมัติ ดังนี้

1. แนวปฏิบัติสำหรับรถยนต์อัตโนมัติ (National Enforcement Guidelines for Automated Vehicles) จัดทำโดยคณะกรรมการขนส่งแห่งชาติ (National Transport Commission) กำหนดแนวทางในการนำหลักการควบคุมรถยนต์อย่างเหมาะสมที่กำหนดไว้ใน Australian Road Rule 297 ว่าควรจะนำมาใช้กับยานยนต์อัตโนมัติอย่างไรบ้าง

2. แนวปฏิบัติสำหรับการทดสอบรถยนต์อัตโนมัติในออสเตรเลีย 2020 (Guidelines for Trials of Automated Vehicles in Australia 2020) จัดทำโดยคณะกรรมการขนส่งแห่งชาติ (National Transport Commission) และหน่วยงานด้านความร่วมมือด้านการขนส่งระหว่างออสเตรเลียและนิวซีแลนด์ (Austroads) เพื่อกำหนดแนวปฏิบัติสำหรับการขออนุญาตทดสอบรถยนต์อัตโนมัติบนท้องถนน

ปัจจุบันมีการจัดทำร่างกฎหมายว่าด้วยความปลอดภัยของรถยนต์อัตโนมัติ (Automated Vehicle Safety Law: AVSL) โดยมีหลักเกณฑ์เกี่ยวกับการกำกับดูแลความปลอดภัยของรถยนต์อัตโนมัติ เช่น การกำหนดหน่วยงานที่มีหน้าที่อนุมัติการนำเข้ารถยนต์อัตโนมัติและพิจารณาด้านคุณภาพความปลอดภัย การกำหนดหน่วยงานกำกับดูแลการรับรองความปลอดภัยของรถยนต์อัตโนมัติ และกำหนดหน่วยงานที่มีอำนาจหน้าที่เกี่ยวข้องกับการจดทะเบียน การออกใบอนุญาตขับขี่รถยนต์ และหน้าที่ในการตรวจสอบความปลอดภัย

สาธารณรัฐประชาชนจีน
ประเทศจีนมีการจัดทำมาตรฐานที่เกี่ยวข้องกับยานยนต์อัตโนมัติหลายฉบับ ได้แก่ 1. มาตรฐานแห่งชาติสำหรับการทดสอบยานยนต์ขับขี่อัตโนมัติ กำหนดถึงมาตรฐานระดับชาติสำหรับการทดสอบรถยนต์ไร้คนขับอัจฉริยะบนท้องถนน 2. มาตรฐานการขับขี่อัตโนมัติ กำหนดถึงเกณฑ์มาตรฐานสำหรับผู้ผลิตรถยนต์ในการพัฒนาเทคโนโลยีแห่งอนาคต 3. มาตรฐานระดับการขับขี่อัตโนมัติสำหรับยานพาหนะ กำหนดถึงมาตรฐาน 6 ระดับของการขับขี่อัตโนมัติสำหรับยานพาหนะในประเทศจีน ตั้งแต่ระดับ L0 ที่ต้องอาศัยคนขับเป็นส่วนใหญ่ ไปจนถึง L5 ที่เป็นระบบอัตโนมัติในการขับขี่เต็มรูปแบบ นอกจากนี้ ยังมีกฎหมายที่เกี่ยวข้องกับการกำกับดูแล คือ ข้อบังคับทางปกครองเกี่ยวกับการทดสอบยานยนต์ทางถนนที่เชื่อมต่อระบบอัจฉริยะ (เพื่อทดลองใช้) (Administrative Regulations on Intelligent Connected Vehicle Road Test (for Trial Implementation) โดยใช้กำกับดูแลความปลอดภัยสำหรับการทดสอบยานยนต์ทางถนนที่ติดตั้งเครือข่ายอัจฉริยะ โดยกำกับดูแลทั้งผู้ขับขี่ รถทดสอบ ถนนที่ทดสอบ ตลอดจนช่วงเวลาที่ทดสอบ ตั้งแต่เริ่มประกาศการทดสอบจนถึงจัดทำรายงานสรุปการทดสอบหลังจากการทดสอบเสร็จสิ้นและส่งให้หน่วยงานกำกับดูแลของรัฐ
สหภาพยุโรป
สหภาพยุโรปมีกฎเกณฑ์ด้านความปลอดภัยทั่วไปของยานพาหนะ (Vehicle General Safety Regulation) ซึ่งกำหนดมาตรการด้านความปลอดภัยทางท้องถนนและกำหนดกรอบทางกฎหมายสำหรับการอนุญาตให้ใช้ยานยนต์อัตโนมัติภายในสหภาพยุโรป[29]

ที่มา : โครงการจัดทำระเบียบ มาตรการ และมาตรฐานที่เกี่ยวข้องกับปัญญาประดิษฐ์ (Artificial Intelligence: AI) (2565)

(2) แนวการกำกับดูแลการใช้งานปัญญาประดิษฐ์ในอากาศยานไร้คนขับ

ปัจจุบันหลายประเทศเริ่มมีมาตรการกำกับอากาศยานไร้คนขับและเริ่มมีการใช้งานจริงในภาคส่วนต่าง ๆ แต่ส่วนใหญ่ยังไม่มีกฎหมายกำกับอากาศยานไร้คนขับที่ควบคุมโดยปัญญาประดิษฐ์ (AI drones) เป็นการเฉพาะ ซึ่งยังคงต้องสอดคล้องตามกฎหมายการบินและอากาศยานที่มีอยู่เดิมของแต่ละประเทศเป็นสำคัญ โดยมีตัวอย่างมาตรการกำกับดูแลปัญญาประดิษฐ์ในเทคโนโลยีที่เกี่ยวข้องกับอากาศยานไร้คนขับในต่างประเทศ ตามตารางต่อไปนี้

[29] 'New Vehicle General Safety Regulation' (European Commission, 6 July 2022) <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4312> สืบค้นเมื่อ 9 กรกฎาคม 2566.

ตารางที่ 2 ตัวอย่างมาตรการกำกับดูแลปัญญาประดิษฐ์ในเทคโนโลยีที่เกี่ยวข้องกับอากาศยานไร้คนขับในต่างประเทศ

สหรัฐอเมริกา
โครงการนำร่องการบูรณาการระบบอากาศยานไร้คนขับ (Unmanned Aircraft Systems Integration Pilot Program) เป็นโครงการของสำนักงานการบินกลาง หรือ Federal Aviation Administration (FAA) โดยมีวัตถุประสงค์เพื่อส่งเสริมความปลอดภัยในการใช้งานอากาศยานไร้คนขับ และให้มีการใช้งานในภาคส่วนต่าง ๆ เช่น ภาคการเกษตร ภาคธุรกิจ ภารกิจฉุกเฉิน การรับส่งผู้โดยสาร และกิจการอื่น ๆ
ญี่ปุ่น
ประเทศญี่ปุ่นมีกฎหมายที่ควบคุมการใช้อากาศยานไร้คนขับหรือโดรน คือ Civil Aeronautics Act ซึ่งกำหนดถึงประเภทของโดรนที่สามารถใช้งานได้ กำหนดพื้นที่ห้ามบินผ่าน รวมทั้งกำหนดถึงข้อปฏิบัติสำหรับผู้ใช้งาน อย่างไรก็ตาม กฎหมายฉบับนี้ยังไม่ได้กำหนดครอบคลุมถึงการใช้งานอากาศยานไร้คนขับที่ควบคุมโดยระบบปัญญาประดิษฐ์
อิสราเอล
ปัจจุบันประเทศอิสราเอลยังไม่มีกฎหมายที่กำกับดูแลการใช้งานอากาศยานไร้คนขับที่ควบคุมโดยระบบปัญญาประดิษฐ์โดยเฉพาะ
ออสเตรเลีย
ปัจจุบันประเทศออสเตรเลียมีกฎหมายที่ควบคุมการใช้งานอากาศยานไร้คนขับหรือโดรน แต่ยังไม่มีกฎหมายที่กำกับดูแลการใช้งานอากาศยานไร้คนขับที่ควบคุมโดยระบบปัญญาประดิษฐ์โดยเฉพาะ
สาธารณรัฐประชาชนจีน
ปัจจุบันประเทศสาธารณรัฐประชาชนจีนมีกฎหมายที่ควบคุมการใช้งานอากาศยานไร้คนขับหรือโดรน แต่ยังไม่มีกฎหมายที่กำกับดูแลการใช้งานอากาศยานไร้คนขับที่ควบคุมโดยระบบปัญญาประดิษฐ์โดยเฉพาะ
สหภาพยุโรป
สำหรับอากาศยานไร้คนขับหรือโดรน สหภาพยุโรปมีกฎเกณฑ์ที่กำหนดกรอบเกี่ยวกับความปลอดภัยในการใช้งานโดรนของบุคคลทั่วไป คือ EU Regulations 2019/947 and 2019/945[30] ซึ่งโดรนที่

[30] 'Civil Drones (Unmanned Aircraft)' (EASA, 22 June 2023) <https://www.easa.europa.eu/en/domains/civil-drones> สืบค้นเมื่อ 9 กรกฎาคม 2566.

ควบคุมโดยระบบปัญญาประดิษฐ์ (Autonomous drone) จะถูกจัดอยู่ในประเภท Specific category หรือ Certified category ซึ่งต้องปฏิบัติตามกฎเกณฑ์และได้รับอนุญาตจากหน่วยงานที่เกี่ยวข้องก่อนจึงจะสามารถใช้งานได้

ที่มา : โครงการจัดทำระเบียบ มาตรการ และมาตรฐานที่เกี่ยวข้องกับปัญญาประดิษฐ์ (Artificial Intelligence: AI) (2565)

(3) แนวการกำกับดูแลการใช้งานปัญญาประดิษฐ์ในเทคโนโลยีจดจำใบหน้า

ปัจจุบันได้มีการนำเทคโนโลยีจดจำใบหน้ามาใช้มากยิ่งขึ้น ซึ่งอาจส่งผลกระทบในทางที่ไม่ดีที่ก่อให้เกิดการละเมิดความเป็นส่วนตัวได้ เช่น การให้คะแนนทางสังคม (social scoring) หรือกรณีที่อาจส่งผลในทางที่ดี ตัวอย่างเช่น การติดตามหาบุคคลสูญหาย หรือติดตามผู้กระทำความผิดที่ได้มีการออกหมายจับแล้ว ซึ่งหากขาดการกำกับดูแลเทคโนโลยีจดจำใบหน้าแล้ว ย่อมทำให้เกิดการนำเทคโนโลยีดังกล่าว ไปใช้ในทางที่ก่อให้เกิดผลเสียได้ สำหรับประเทศไทยในปัจจุบันยังไม่มีการกำกับดูแลเกี่ยวกับการใช้ปัญญาประดิษฐ์ในเทคโนโลยีจดจำใบหน้าโดยเฉพาะ ตัวอย่างมาตรการกำกับดูแลปัญญาประดิษฐ์ในเทคโนโลยีที่เกี่ยวข้องกับเทคโนโลยีจดจำใบหน้าในต่างประเทศ ตามตารางดังต่อไปนี้

ตารางที่ 3 ตัวอย่างมาตรการกำกับดูแลปัญญาประดิษฐ์ในเทคโนโลยีที่เกี่ยวข้องกับเทคโนโลยีจดจำใบหน้าในต่างประเทศ

สหรัฐอเมริกา
กฎหมายเพื่อกำกับดูแลการใช้งานเทคโนโลยีการจดจำใบหน้า โดยออกเป็นกฎหมายระดับรัฐ เช่น BIPA (Illinois Biometric Information Privacy Act), CCPA (California Consumer Privacy Act), POST (New York Public Oversight of Surveillance Technology Act) เป็นต้น
ญี่ปุ่น
ประเทศญี่ปุ่นยังไม่มีกฎเกณฑ์เฉพาะเกี่ยวกับการกำกับดูแลการใช้เทคโนโลยีจดจำใบหน้าหรือเทคโนโลยีชีวมิติในการระบุตัวตน อย่างไรก็ตาม มีแนวคิดเกี่ยวกับการกำกับดูแลตามที่กำหนดไว้ในนโยบายการกำกับดูแลปัญญาประดิษฐ์ในประเทศญี่ปุ่น 1.1 (AI Governance in Japan 1.1)
อิสราเอล
ประเทศอิสราเอลยังไม่มีกฎเกณฑ์เฉพาะสำหรับการกำกับดูแลการใช้เทคโนโลยีจดจำใบหน้าหรือเทคโนโลยีชีวมิติในการระบุตัวตน ทั้งนี้ มีแนวคิดเกี่ยวกับการนำระบบจดจำใบหน้ามาใช้ในพื้นที่

สาธารณะ โดย Israel National Cyber Directorate (INCD) เสนอแนวนโยบายและข้อเสนอเกี่ยวกับการกำกับดูแล คือ Facial Recognition in Israel's Public Places Policy Principles & a Call for Regulation[31]
ออสเตรเลีย
ประเทศออสเตรเลียยังไม่มีกฎเกณฑ์เฉพาะและแนวปฏิบัติเกี่ยวกับการกำกับดูแลการใช้เทคโนโลยีจดจำใบหน้าหรือเทคโนโลยีชีวมิติในการระบุตัวตน อย่างไรก็ตาม การจัดเก็บข้อมูลชีวมิติจะอยู่ภายใต้การกำกับดูแลของกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
สาธารณรัฐประชาชนจีน
ประเทศสาธารณรัฐประชาชนจีนยังไม่มีกฎเกณฑ์เกี่ยวกับการกำกับดูแลการใช้เทคโนโลยีจดจำใบหน้าหรือเทคโนโลยีชีวมิติในการระบุตัวตนโดยเฉพาะ ทั้งนี้ มีร่างระเบียบว่าด้วยการบริหารการสังเคราะห์เชิงลึกของบริการข้อมูลทางอินเทอร์เน็ต (Draft of Provisions on the Management of Deep Synthesis in Internet Information Service) ซึ่งจะควบคุมผู้ให้บริการสังเคราะห์เชิงลึกที่อาจมีการนำข้อมูลทางชีวมิติมาใช้งาน
สหภาพยุโรป
สหภาพยุโรปกำหนดให้การใช้เทคโนโลยีชีวมิติระยะไกลในการระบุตัวตนโดยใช้ระบบปัญญาประดิษฐ์เป็นการใช้ระบบปัญญาประดิษฐ์ที่มีความเสี่ยงสูงซึ่งต้องมีกฎเกณฑ์การกำกับดูแลที่เข้มงวดก่อนที่จะนำมาใช้ ทั้งนี้มีการกำหนดแนวปฏิบัติสำหรับการใช้เทคโนโลยีการจดจำใบหน้า คือ Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement[32]

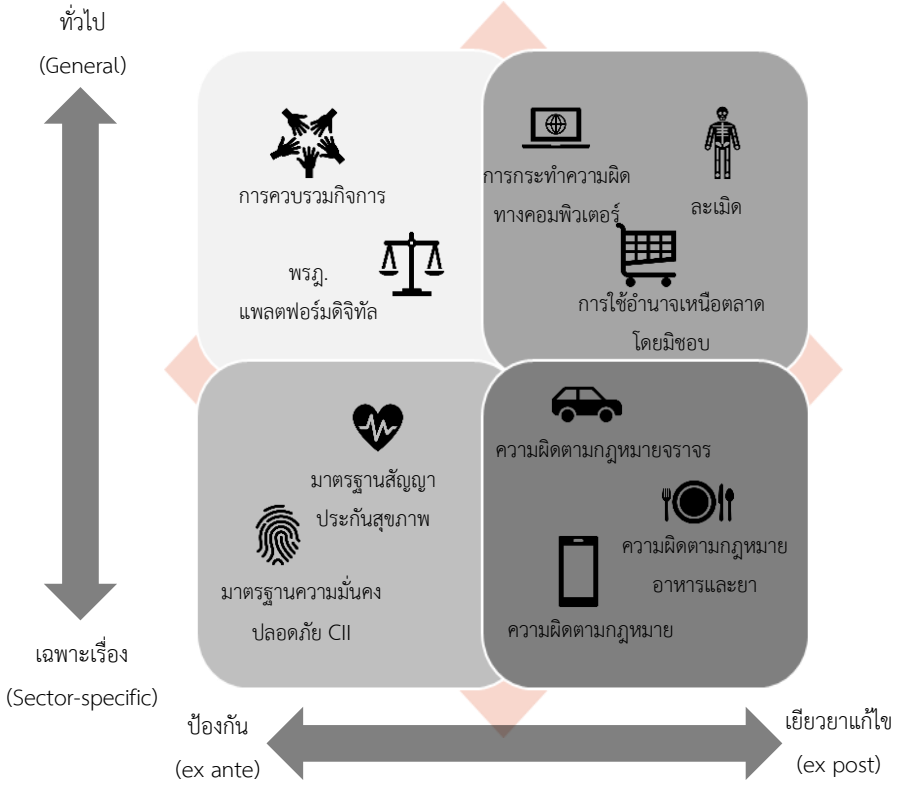
ที่มา : โครงการจัดทำระเบียบ มาตรการ และมาตรฐานที่เกี่ยวข้องกับปัญญาประดิษฐ์ (Artificial Intelligence: AI) (2565)

[31] The Identity and Biometric Applications Unit, 'Facial Recognition in Israel's Public Places Policy Principles & a Call for Regulation' <https://www.gov.il/BlobFolder/generalpage/face_recognition/he/Facial Recognition in Public Places - INCD.pdf> สืบค้นเมื่อ 9 กรกฎาคม 2566.

[32] European Data Protection Board, 'Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement' <https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement _en_1.pdf> สืบค้นเมื่อ 9 กรกฎาคม 2566.

4. มาตรการกำกับดูแลการใช้งานระบบปัญญาประดิษฐ์

ภาพที่ 5 ลักษณะของมาตรการกำกับดูแล (Regulatory Framework)



ที่มา : โครงการจัดทำระเบียบ มาตรการ และมาตรฐานที่เกี่ยวข้องกับปัญญาประดิษฐ์ (Artificial Intelligence: AI) (2565)

จะเห็นได้ว่า ประเด็นข้อกังวลการใช้งานระบบปัญญาประดิษฐ์นั้น ที่จริงแล้วไม่ใช่ประเด็นทางเทคนิคหรือเป็นประเด็นที่ขัดขวางการพัฒนา แต่เป็นเรื่องการใช้งานและผลกระทบเป็นสำคัญ กล่าวคือ เป็นเรื่องที่ต้องการการบริหารจัดการที่ดีควบคู่ไปกับการพัฒนา โดยเฉพาะประเด็นอคตินั้นในทางเทคนิคก็มีวัตถุประสงค์เดียวกันที่ไม่ต้องการจะให้เกิดขึ้น แต่หากไม่มีการบริหารจัดการที่ดีพอก็อาจจะกลายเป็นปัญหาใหญ่ได้ ดังนั้น จึงเป็นที่มาที่กล่าวได้ว่า ทั่วโลกเริ่มให้ความสำคัญและเริ่มออกแนวทางการกำกับดูแลการใช้งานปัญญาประดิษฐ์

จากภาพจะเห็นได้ว่า มาตรการกำกับดูแลสามารถพิจารณาแยกได้เป็น 2 ลักษณะ ดังนี้

(1) ในเชิงบริบทการกำกับดูแล (แกนแนวตั้งตามภาพ) เป็นลักษณะเฉพาะเจาะจง (specificity) ของการกำกับดูแล กล่าวคือ

- กรณีการกำกับดูแลโดยทั่วไป (general) เป็นการกำกับดูแลแบบหลักการแม่บทที่ปรับใช้ได้กับทุกกรณีที่เกี่ยวข้องโดยไม่แตกต่างกัน เช่น ละเมิด หรือการกระทำความผิดทางคอมพิวเตอร์ ที่ใช้หลักการเดียวกัน ไม่แตกต่างไปตามสภาพหรือบริบทของกรณี

- การกำกับดูแลเฉพาะเรื่อง (sector-specific) เป็นการกำกับดูแลที่มีหลักเกณฑ์เฉพาะของเรื่องที่ไม่สามารถนำไปใช้ได้กับบริบทอื่น ๆ เช่น มาตรฐานสัญญาประกันสุขภาพ การกระทำความผิดตามกฎหมายจราจร ซึ่งเป็นเรื่องเฉพาะเจาะจง ไม่สามารถเอามาตรฐานสัญญาประกันสุขภาพไปใช้ในเรื่องอื่นได้ เป็นต้น

(2) ในเชิงระยะเวลา (แกนแนวนอนตามภาพ) เป็นการกำกับดูแลที่แตกต่างกันตามระยะเวลาที่เกิดขึ้น โดยพิจารณาเอาเหตุการณ์ที่ไม่พึงประสงค์ที่ต้องการจะกำกับดูแลมาเป็นแกนกลาง

- มาตรการป้องกัน (*ex ante*) เป็นการกำกับดูแลที่เกิดขึ้นก่อนด้วยวัตถุประสงค์ที่ต้องการจะหลีกเลี่ยงหรือบริหารจัดการไม่ให้มีเหตุการณ์ไม่พึงประสงค์ เช่น การควบรวมกิจการ หรือมาตรฐานสัญญาต่าง ๆ ล้วนเป็นเครื่องมือเพื่อป้องกันทั้งสิ้น โดยทั่วไปแล้วจะมีมาตรการป้องกันในกรณีพิจารณาแล้วมีประสิทธิภาพมากกว่าที่จะมีการบริหารจัดการเพื่อหลีกเลี่ยงไม่ให้มีเหตุการณ์ไม่พึงประสงค์เกิดขึ้น ซึ่งโดยทั่วไปแล้วก็จะต้องเป็นกรณีที่มีความชัดเจนเพียงพอและสามารถใช้หลักการบริหารความเสี่ยงเข้ามาดำเนินการได้ตามสมควร เครื่องมือทางกฎหมายในเรื่องนี้ เช่น การกำหนดมาตรฐาน การประเมินความเสี่ยง และการสร้างแนวปฏิบัติ เป็นต้น

- มาตรการเยียวยาแก้ไข (*ex post*) เป็นการกำกับดูแลที่เกิดขึ้นหลังมีเหตุการณ์ไม่พึงประสงค์ เช่น ฐานความผิดตามกฎหมายต่าง ๆ มาตรการประเภทนี้ถือเป็นมาตรการพื้นฐานดั้งเดิมทางกฎหมาย เพราะโดยทั่วไปแล้วเราไม่สามารถจะใช้มาตรการป้องกันกับทุก ๆ เรื่องได้ และโดยสภาพก็อาจจะมีต้นทุนมากไม่คุ้มค่าต่อการดำเนินการ เครื่องมือทางกฎหมายในเรื่องนี้จึงเป็นการกำหนดฐานความผิดและค่าเสียหายเป็นสำคัญ

จากภาพรวมของการกำกับดูแลการใช้งานระบบปัญญาประดิษฐ์จะเห็นได้ว่ามาตรการกำกับดูแลสามารถพิจารณาแยกได้เป็น 4 ลักษณะ ดังนี้

(1) มาตรการป้องกันแบบทั่วไป กล่าวคือ เป็นการกำกับดูแลแบบหลักการแม่บทที่ปรับใช้ได้กับทุกกรณีที่เกี่ยวข้อง (general) โดยเน้นที่การป้องกัน (ex ante) และการบริหารความเสี่ยงเป็นสำคัญ เพื่อไม่ให้เกิดเหตุการณ์ที่ไม่พึงประสงค์ เช่น การควบรวมกิจการ หรือมาตรฐานสัญญาต่าง ๆ ล้วนเป็นเครื่องมือเพื่อป้องกันทั้งสิ้น โดยทั่วไปแล้วจะมีมาตรการป้องกันในกรณีพิจารณาแล้วมีประสิทธิภาพมากกว่าที่จะมีการบริหารจัดการเพื่อหลีกเลี่ยงไม่ให้มีเหตุการณ์ไม่พึงประสงค์เกิดขึ้น ซึ่งโดยทั่วไปแล้วจะต้องเป็นกรณีที่มีความชัดเจนเพียงพอและสามารถใช้หลักการบริหารความเสี่ยงเข้ามาดำเนินการได้ตามสมควร เครื่องมือทางกฎหมายในเรื่องนี้ เช่น การกำหนดมาตรฐาน

การประเมินความเสี่ยง และการสร้างแนวปฏิบัติ เป็นต้น มาตรการนี้จึงเน้นให้ผู้ใช้งานมีความระมัดระวังแต่เนื่องจากเป็นมาตรการทั่วไปที่ทุกภาคอุตสาหกรรมต้องมี จึงเป็นมาตรการขั้นต่ำเป็นหลัก

(2) มาตรการป้องกันแบบเฉพาะเรื่อง กล่าวคือ เป็นการกำกับดูแลเชิงป้องกัน (*ex ante*) ที่มีหลักเกณฑ์เฉพาะของเรื่องเฉพาะอุตสาหกรรม (sector-specific) ที่ไม่สามารถนำไปใช้ได้กับบริบทอื่น ๆ เช่น มาตรฐานสัญญาประกันสุขภาพ การกระทำความผิดตามกฎหมายจราจร ซึ่งเป็นเรื่องเฉพาะเจาะจงไม่สามารถเอามาตรฐานสัญญาประกันสุขภาพไปใช้ในเรื่องอื่นได้ เป็นต้น

(3) มาตรการเยียวยาแก้ไขแบบทั่วไป กล่าวคือ เป็นการกำกับดูแลที่เกิดขึ้นเมื่อมีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นแล้ว (ex post) เป็นการทั่วไป (general) เช่น ฐานความผิดตามกฎหมายแม่บทอย่างกฎหมายอาญาและกฎหมายปกครอง หรือความรับผิดทางแพ่ง เป็นต้น มาตรการประเภทนี้ถือเป็นมาตรการพื้นฐานดั้งเดิมทางกฎหมาย เพราะโดยทั่วไปแล้วเราไม่สามารถจะใช้มาตรการป้องกันกับทุก ๆ เรื่องได้ และโดยสภาพก็อาจจะมีต้นทุนมากไม่คุ้มค่าต่อการดำเนินการ เครื่องมือทางกฎหมายในเรื่องนี้จึงเป็นการกำหนดฐานความผิดและค่าเสียหายเป็นสำคัญเป็นมาตรการที่เกิดขึ้น

(4) มาตรการเยียวยาแก้ไขแบบเฉพาะเรื่อง กล่าวคือ เป็นมาตรการเยียวยาแก้ไข (*ex post*) ที่หลักกฎหมายพื้นฐานและหลักทั่วไปไม่สามารถใช้ได้อย่างมีประสิทธิภาพ จึงจำเป็นต้องกำหนดฐานความผิดและค่าเสียหายเฉพาะเรื่อง (sector-specific) ขึ้นมา เช่น ฐานความผิดตามกฎหมายสื่อสาร ฐานความผิดตามกฎหมายอาหารและยา เป็นต้น

การใช้งานระบบปัญญาประดิษฐ์นั้นมีอยู่ทั้งในบริบทแบบทั่วไป (general) และบริบทเฉพาะเรื่อง (sector-specific) โดยประเด็นที่ได้รับความสนใจมากในปัจจุบันได้แก่ ยานยนต์อัตโนมัติ และอากาศยานไร้คนขับ ซึ่งจำเป็นที่หน่วยงานกำกับดูแลเฉพาะเรื่อง ได้แก่ กรมขนส่งทางบก และสำนักงานการบินพลเรือน จะต้องมีมาตรการเฉพาะที่เกี่ยวข้องกับปัญญาประดิษฐ์ เพราะเป็นเรื่องที่มีรายละเอียดเฉพาะเรื่องอย่างเจาะจงบริบทที่ไม่เกี่ยวข้องกับส่วนงานอื่น และเน้นหนักไปที่มาตรการเชิงป้องกันเป็นสำคัญ เพราะเป็นประเด็นด้านความปลอดภัยเป็นหลัก ขณะที่ประเด็นแบบเทคโนโลยีจดจำใบหน้าก็จำเป็นที่หน่วยงานอย่างสำนักงานตำรวจแห่งชาติ หรือหน่วยงานทางปกครอง เช่น กรุงเทพมหานครจะต้องมีมาตรการเฉพาะเข้ามากำกับดูแลการใช้งานเช่นกัน

บทความนี้จึงเสนอให้จัดการความเสี่ยงของเทคโนโลยีด้วยมาตรการกำกับป้องกันทั้งในบริบทแบบทั่วไป (general) และบริบทเฉพาะเรื่อง (sector-specific) ซึ่งปัจจุบันยังขาดกรอบการกำกับดูแลแม่บทที่เป็นมาตรการป้องกันแบบทั่วไป ที่กฎหมายแบบทั่วไป สามารถตราออกมาเพื่อกำหนดมาตรฐานขั้นต่ำเชิงป้องกันได้ โดยสอดคล้องกับมาตรฐานสากล ซึ่งเรื่องนี้จากการศึกษาพบว่ามีช่องทางที่สามารถทำได้โดยออกเป็นพระราชกฤษฎีกาภายใต้พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 โดยไม่ต้องตราเป็นพระราชบัญญัติ ในลักษณะเดียวกันกับพระราชกฤษฎีกาการประกอบธุรกิจ

บริการแพลตฟอร์มดิจิทัลที่ต้องแจ้งให้ทราบ พ.ศ. 2565 และพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565 ซึ่งมีหลักการทำนองเดียวกันในเชิงป้องกันเป็นการทั่วไป เช่นนี้ ก็จะทำให้มีมาตรการที่ทำหน้าที่เป็นมาตรการป้องกันแบบทั่วไปที่กำหนดมาตรฐานขั้นต่ำเอาไว้ซึ่งจะทำให้เกิดกรอบการกำกับดูแลเชิงการบริหารความเสี่ยงในภาพรวม เพื่อที่จะให้หน่วยงานกำกับดูแลเฉพาะเรื่องสามารถออกมาตรการเฉพาะของตนต่อยอดต่อไป

อนึ่ง มีการศึกษาในอีกลักษณะหนึ่งของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[33] ที่เสนอร่างพระราชบัญญัติว่าด้วยการส่งเสริมและสนับสนุนนวัตกรรมปัญญาประดิษฐ์แห่งประเทศไทย พ.ศ. .... โดยมีวัตถุประสงค์เชิงเนื้อหา 5 ประการ ได้แก่ (1) ศูนย์ทดสอบนวัตกรรมปัญญาประดิษฐ์ (2) การแบ่งปันข้อมูล (3) การสร้างมาตรฐาน AI (4) การประเมินความเสี่ยง (5) การกำหนดมาตรฐานของสัญญาระหว่างผู้ให้บริการกับผู้ใช้ผลิตภัณฑ์หรือบริการ AI ทำให้ผลการศึกษาดังกล่าวจึงเสนอเป็นออกพระราชบัญญัติ แตกต่างจากที่เสนอในบทความนี้ที่เสนอออกเป็นเพียงพระราชกฤษฎีกาเพื่อให้ได้เฉพาะส่วนมาตรการกำกับดูแลเชิงป้องกันแบบทั่วไปเท่านั้น

[33] โครงการเพื่อการศึกษา หารือ และรับฟังความคิดเห็นเกี่ยวกับการกำกับดูแลและส่งเสริมเทคโนโลยีสมัยใหม่ ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ดำเนินการโดย บริษัท เบเคอร์ แอนด์ แม็คเคนซี่ จำกัด และคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.