

AI for Everyone : ปัญญาประดิษฐ์เพื่ออนาคตของทุกคน

โดย นายเจนภพ สี่แดง
นักวิชาการแผนกที่ภาพถ่ายปฏิบัติการ

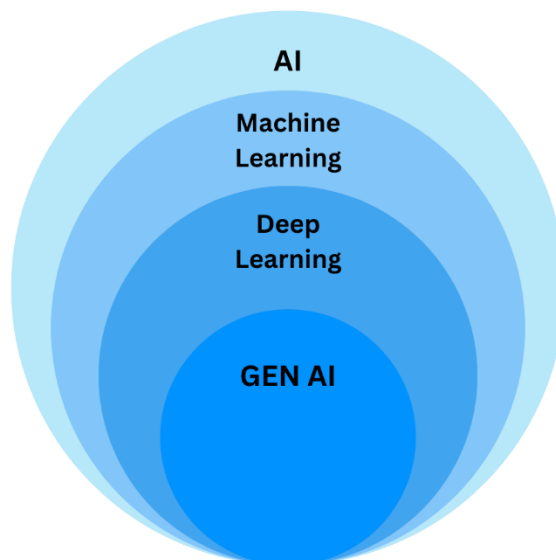
วัตถุประสงค์

๑. เรียนรู้และทำความเข้าใจกับ AI เบื้องต้น
๒. เพื่อให้เข้าใจความหมายของปัญญาประดิษฐ์และประโยชน์ของ AI
๓. เพื่อให้สามารถนำ AI มาประยุกต์ใช้สำหรับบริการภาครัฐ

สรุปเนื้อหา

AI หรือปัญญาประดิษฐ์กำลังเข้ามามีบทบาทอย่างมากในการเปลี่ยนแปลงโลกในหลายมิติ ทั้งในด้านเศรษฐกิจ เทคโนโลยี และวิถีชีวิต โดย AI เข้ามาสนับสนุนให้การทำงานรวดเร็วและแม่นยำขึ้น ลดต้นทุน และสร้างรูปแบบธุรกิจรูปแบบใหม่ ในขณะเดียวกันก็ผลักดันให้เกิดนวัตกรรม เช่น การแพทย์อัจฉริยะ รถยนต์ไร้คนขับและการเข้ามามีบทบาทในการจัดการแนวความสะอาดในชีวิตประจำวัน รวมทั้งเปิดโอกาสทางการศึกษาในการเข้าถึงข้อมูลการเรียนรู้จากต่างประเทศและการศึกษาทางไกลได้ง่ายขึ้น ทำให้ผู้คนเข้าถึงความสะดวกสบายมากขึ้น นอกจากนี้ AI ยังเข้ามามีบทบาทกับงานในหน่วยงานภาครัฐ เช่น การลดขั้นตอนในการให้บริการทำให้เกิดความสะดวกรวดเร็วในการบริการและการเข้าถึงข้อมูลของทางภาครัฐ อย่างไรก็ตาม การเติบโตของ AI ก็สร้างความท้าทายด้านความเป็นส่วนตัว ความปลอดภัยและการเปลี่ยนแปลงในตลาดแรงงาน จึงจำเป็นต้องใช้ควบคู่กับการกำกับดูแลและจริยธรรมเพื่อให้เกิดประโยชน์สูงสุดต่อสังคมและโลกในอนาคต

๑. คำศัพท์พื้นฐานเกี่ยวกับ AI



รูปที่ ๑ องค์ประกอบของ AI

ที่มา <https://www.disruptignite.com/blog/what-is-ai-artificial-intelligence>

๑.๑ Artificial Intelligence (AI) – ปัญญาประดิษฐ์

เป็นเทคโนโลยีที่ออกแบบให้คอมพิวเตอร์หรือเครื่องจักรมีความสามารถในการ “คิด วิเคราะห์ ตัดสินใจ และเรียนรู้” เหมือนหรือใกล้เคียงกับมนุษย์ โดยอาศัยข้อมูลและอัลกอริทึมเป็นพื้นฐานในการทำงาน โดยประเภทของ AI แบ่งได้หลัก ๆ ๓ ระดับตามความสามารถดังนี้

๑. AI เฉพาะด้าน (Narrow AI หรือ Weak AI) เป็น AI ที่ถูกออกแบบให้ทำงานเฉพาะเรื่องได้อย่างดีเยี่ยม แต่ไม่สามารถทำงานอื่นนอกเหนือจากที่ถูกฝึก เช่น ระบบแปลภาษาออนไลน์ กล้องจดจำใบหน้าหรือระบบแนะนำสินค้าในแพลตฟอร์มซื้อขายสินค้า

๒. AI อนุเคราะห์ (General AI หรือ Strong AI) เป็น AI ที่มีความสามารถใกล้เคียงกับมนุษย์ สามารถคิด วิเคราะห์ และเรียนรู้เพื่อแก้ปัญหาได้หลากหลายด้านเหมือนคน ปัจจุบันยังเป็นเพียงแนวคิดและอยู่ในขั้นวิจัย

๓. AI เหนือมนุษย์ (Super AI) เป็น AI ที่ฉลาดและมีความสามารถเหนือกว่ามนุษย์ทุกด้าน ทั้งด้านความคิดสร้างสรรค์ การแก้ปัญหา และการตัดสินใจ ซึ่งยังไม่มีในปัจจุบัน และเป็นหัวข้อถกเถียงด้านจริยธรรมและความปลอดภัยในอนาคต

๑.๒ Machine Learning (ML) – การเรียนรู้ของเครื่อง

เป็นสาขาหนึ่งของ AI ที่เน้นให้คอมพิวเตอร์สามารถเรียนรู้จากข้อมูลด้วยตัวเองโดยไม่ต้องเขียนคำสั่งทุกขั้นตอน เช่น การทำนายผลลัพธ์จากข้อมูลเก่า หรือการจำแนกรูปภาพและข้อความ ML สร้างโมเดลทางคณิตศาสตร์ที่เรียนรู้จากตัวอย่างข้อมูล

๑.๓ Deep Learning (DL) – การเรียนรู้เชิงลึก

เป็นเทคนิคของ Machine Learning ที่ใช้โครงข่ายประสาทเทียมหลายชั้น (Neural Networks) เพื่อวิเคราะห์ข้อมูลซับซ้อน เช่น ภาพ เสียง หรือข้อความ DL สามารถจับความสัมพันธ์เชิงซ้อนของข้อมูลได้ดีกว่า Machine Learning แบบดั้งเดิม และเป็นเทคโนโลยีเบื้องหลัง Generative AI

๑.๔ Generative AI – ปัญญาประดิษฐ์สร้างสรรค์

เป็น AI ที่สามารถสร้างเนื้อหาใหม่ได้เอง เช่น ข้อความ ภาพ เสียง วิดีโอ หรือชุดคำสั่งโปรแกรม โดยเรียนรู้จากข้อมูลจำนวนมากในฐานข้อมูล ตัวอย่างเช่น การสร้างภาพวาดจากคำสั่งข้อความหรือเขียนบทความอัตโนมัติ โดย Generative AI ทำให้คอมพิวเตอร์สามารถสร้างสรรค์ผลงานใหม่คล้ายมนุษย์

๒. ประโยชน์ของ AI ในภาครัฐ



รูปที่ ๒ AI ในการให้บริการของภาครัฐ

ที่มา <https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/Articles/AI-in-Government-Services.aspx>

AI เข้ามามีบทบาทที่สำคัญที่ช่วยให้หน่วยงานภาครัฐสามารถทำงานได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น ลดขั้นตอนที่ซ้ำซ้อน และลดการใช้เอกสารกระดาษด้วยการปรับเปลี่ยนมาเป็นระบบดิจิทัล เช่น การยื่นคำร้องออนไลน์ที่ใช้ AI ตรวจสอบความถูกต้องของข้อมูลอัตโนมัติ การจัดหมวดหมู่และส่งต่อเรื่องไปยังหน่วยงานที่เกี่ยวข้องอย่างแม่นยำ ทำให้ประชาชนได้รับบริการเร็วขึ้น อีกทั้ง AI ยังช่วยเพิ่มประสิทธิภาพการทำงานของเจ้าหน้าที่ เช่น การค้นหาข้อมูล การตรวจสอบเอกสารหรือการตอบคำถามทั่วไป ทำให้เจ้าหน้าที่สามารถมุ่งเน้นกับงานที่ต้องใช้การตัดสินใจเชิงลึกและการแก้ปัญหาได้มากขึ้น ส่งผลให้คุณภาพการบริการโดยรวมสูงขึ้น ลดค่าใช้จ่าย ลดความผิดพลาด และสร้างความโปร่งใสในการดำเนินงานของภาครัฐโดยยึดหลักแนวทาง Citizen Centric ในการบริหารจัดการภาครัฐ

Citizen Centric คือ แนวคิดหรือแนวทางการให้บริการของภาครัฐและองค์กร ที่มุ่งเน้น “ประชาชนเป็นศูนย์กลาง” (People-first approach) หมายถึง การออกแบบนโยบาย ระบบ หรือบริการ โดยเริ่มจากความต้องการ ประสบการณ์ และความสะดวกของประชาชนเป็นหลัก มากกว่าการมองจากมุมมองของหน่วยงานหรือเจ้าหน้าที่

๓. ข้อควรระวังในการใช้ AI ในภาครัฐ

การนำปัญญาประดิษฐ์ (AI) มาใช้ในภาครัฐมีศักยภาพสูงในการเพิ่มประสิทธิภาพการทำงาน ลดขั้นตอนซ้ำซ้อน และยกระดับการให้บริการประชาชนให้รวดเร็วและตรงตามความต้องการมากขึ้น แต่การใช้งานก็มีข้อควรระวังหลายประการ โดยเฉพาะในเรื่องความปลอดภัย ความเป็นธรรมและความรับผิดชอบของหน่วยงาน

ประเด็นแรกคือเรื่อง การคุ้มครองข้อมูลประชาชน ภาครัฐถือครองข้อมูลส่วนบุคคลจำนวนมาก เช่น ข้อมูลบัตรประชาชน ประวัติการรักษาพยาบาล ข้อมูลภาษี หรือข้อมูลการเดินทาง ซึ่งหาก AI นำข้อมูลเหล่านี้ไปประมวลผลโดยไม่มีมาตรการปกป้องที่ดี อาจทำให้เกิดการรั่วไหล การถูกขโมยหรือการนำไปใช้ในทางที่ไม่เหมาะสมได้ ดังนั้นต้องมีการเข้ารหัสข้อมูล (Data Encryption) การกำหนดสิทธิ์การเข้าถึง (Access Control) และปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (เช่น PDPA หรือ GDPR) อย่างเคร่งครัด

ประเด็นที่สองคือเรื่อง Responsibility หรือความรับผิดชอบของหน่วยงาน แม้ AI จะช่วยตัดสินใจหรือทำงานบางอย่างได้อัตโนมัติ แต่ความรับผิดชอบขั้นสุดท้ายยังคงอยู่ที่มนุษย์หรือเจ้าหน้าที่ของรัฐ หากเกิดข้อผิดพลาดหรือความเสียหายจากการใช้ AI หน่วยงานต้องมีความชัดเจนว่าใครเป็นผู้รับผิดชอบ และต้องมีกลไกการตรวจสอบและอุทธรณ์ เพื่อให้ประชาชนสามารถทักท้วงและตรวจสอบได้ อีกทั้งในเรื่องความถูกต้องและความน่าเชื่อถือของข้อมูลที่ AI ใช้ เพราะหากข้อมูลที่นำมาฝึกสอนมีความผิดพลาด ไม่ครบถ้วน หรือมีอคติ (Bias) ก็อาจทำให้ผลลัพธ์ของ AI ไม่ยุติธรรม หรือเลือกปฏิบัติต่อประชาชนบางกลุ่มโดยไม่ตั้งใจ เช่น การใช้ AI ในการคัดเลือกผู้ขอรับสวัสดิการ หากข้อมูลฝึกสอนมีความลำเอียง อาจทำให้บางกลุ่มถูกปฏิเสธโดยไม่เป็นธรรม

ประการสุดท้ายคือ ความปลอดภัยทางไซเบอร์ (Cybersecurity) เนื่องจากระบบ AI ที่เชื่อมต่อกับฐานข้อมูลภาครัฐมีความเสี่ยงต่อการถูกโจมตีหรือเจาะระบบ จึงต้องมีการทดสอบความปลอดภัยเป็นประจำ ใช้ระบบป้องกันการโจมตีขั้นสูง และมีแผนรับมือหากเกิดเหตุไม่คาดคิด เพื่อไม่ให้บริการของรัฐหยุดชะงักหรือสร้างความเสียหายต่อประชาชน

๔. รูปแบบการโจมตีทางไซเบอร์ที่ภาครัฐต้องระวัง

๔.๑ การโจมตีด้วยข้อมูลที่หลอกลวง (Deceptive Data Attacks) เป็นการส่งข้อมูลเทียมหรือหลอกลวงเข้าสู่ระบบของภาครัฐหรือ AI เพื่อให้ผลลัพธ์การวิเคราะห์ผิดพลาด เช่น การสร้างข้อมูลบิดเบือนเพื่อตัดสินใจผิด ระบบอาจประเมินความเสี่ยงผิด หรือให้บริการประชาชนไม่ถูกต้อง ส่งผลกระทบต่อความน่าเชื่อถือของหน่วยงาน

๔.๒ การปนเปื้อนข้อมูล (Data Poisoning) เป็นการแทรกข้อมูลที่ผิดหรือมีอคติเข้าไปในชุดข้อมูลที่ AI ใช้ฝึกสอน ทำให้โมเดลเรียนรู้ผิดพลาดและตัดสินใจไม่ถูกต้อง ตัวอย่างเช่น การเผยแพร่ข่าวปลอม (Fake News) ที่เข้าไปในฐานข้อมูล ทำให้ระบบวิเคราะห์ข้อมูลประชาชนหรือสื่อสารกับประชาชนผิดพลาด

๔.๓ การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access) เกิดจากผู้ไม่หวังดีเจาะระบบเข้าถึงข้อมูลหรือบริการของรัฐบาลโดยไม่ได้รับอนุญาต เช่น ข้อมูลส่วนบุคคล เอกสารสำคัญ หรือระบบบริการประชาชน การเข้าถึงโดยไม่ได้รับอนุญาตนี้อาจนำไปสู่การขโมยข้อมูล แก้ไขข้อมูล หรือปิดกั้นการให้บริการ

๔.๔ แรนซัมแวร์ (Ransomware) เป็นการโจมตีที่ผู้โจมตีเข้ารหัสไฟล์หรือระบบของภาครัฐแล้วเรียกค่าไถ่ ทำให้บริการสำคัญของรัฐ เช่น ระบบภาษี ระบบทะเบียนราษฎร หรือระบบสาธารณสุขหยุดชะงัก การป้องกันต้องมีการสำรองข้อมูลอย่างสม่ำเสมอ และใช้ระบบความปลอดภัยขั้นสูง

๔.๕ การขโมยโมเดล AI (AI Model Theft) ในยุคที่ภาครัฐใช้ AI โมเดลเองก็เป็นเป้าหมายของ แฮ็กเกอร์ ผู้โจมตีอาจขโมยโมเดลเพื่อใช้ประโยชน์เชิงพาณิชย์ หรือสร้างความเสียหาย เช่น การสร้างโมเดลปลอมที่เลียนแบบระบบของรัฐ หรือเรื่องข้อมูลที่สำคัญของประชาชน

๕. แนวทางการเพิ่มความปลอดภัยให้ระบบ AI ของภาครัฐ

การใช้ AI ในภาครัฐช่วยเพิ่มประสิทธิภาพในการให้บริการประชาชนและการบริหารงาน แต่เนื่องจากระบบ AI ต้องประมวลผลข้อมูลจำนวนมากและบางครั้งเป็นข้อมูลสำคัญหรืออ่อนไหว จึงต้องมีมาตรการ ด้านความปลอดภัยที่เข้มงวดเพื่อป้องกันการโจมตีและความเสี่ยงต่าง ๆ โดยสามารถดำเนินการได้ดังนี้

๕.๑ พัฒนามาตรฐานความปลอดภัยเฉพาะ AI และการเข้ารหัส โดยกำหนดมาตรฐานความปลอดภัยเฉพาะสำหรับระบบ AI ทั้งในส่วนของการเก็บข้อมูล การประมวลผล และการส่งข้อมูล ใช้เทคโนโลยีเข้ารหัส (Encryption) และโปรโตคอลการสื่อสารที่ปลอดภัยเพื่อป้องกันข้อมูลจากการถูกดักจับหรือแก้ไข นอกจากนี้ควรกำหนดมาตรฐานการจัดการโมเดล AI ให้สามารถตรวจสอบและควบคุมการเข้าถึงได้อย่างเข้มงวด

๕.๒ การเฝ้าระวังและตรวจจับภัยคุกคามอย่างต่อเนื่อง โดยระบบ AI ของภาครัฐมีการเฝ้าระวังภัยคุกคามแบบเรียลไทม์ (Real-time Threat Monitoring) เพื่อสามารถตรวจจับพฤติกรรมที่ผิดปกติ เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การโจมตีแบบฟิชซิง หรือการฝังข้อมูลอันตรายในระบบ การติดตั้งระบบแจ้งเตือนอัตโนมัติและการวิเคราะห์เหตุการณ์อย่างต่อเนื่องจะช่วยลดความเสี่ยงจากการโจมตีและเพิ่มความปลอดภัยของระบบ

๕.๓ การฝึกอบรมและสร้างความตระหนักรู้ให้กับเจ้าหน้าที่ บุคลากรของภาครัฐเป็นจุดอ่อนที่สำคัญในการรักษาความปลอดภัย AI จึงต้องมีการฝึกอบรมเจ้าหน้าที่ให้รู้จักภัยคุกคามทางไซเบอร์ วิธีการป้องกัน และแนวทางปฏิบัติเมื่อเกิดเหตุฉุกเฉิน รวมถึงสร้างความตระหนักรู้เรื่องความปลอดภัยดิจิทัลให้เจ้าหน้าที่ทุกระดับเข้าใจความสำคัญของการรักษาความปลอดภัยของระบบ AI

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน

การนำองค์ความรู้ด้านปัญญาประดิษฐ์ (AI) ไปปรับใช้ในการปฏิบัติงานมีประโยชน์อย่างมากในปัจจุบัน เนื่องจาก AI สามารถช่วยเพิ่มประสิทธิภาพการทำงาน ลดขั้นตอนที่ซ้ำซ้อน และทำให้การประมวลผลข้อมูลจำนวนมากเป็นไปอย่างรวดเร็วและแม่นยำ นอกจากนี้ยังสนับสนุนการให้บริการที่ตอบสนองต่อความต้องการของประชาชนหรือผู้ใช้ได้ดียิ่งขึ้น อีกทั้งยังช่วยยกระดับคุณภาพงานบริการให้มีความโปร่งใส ลดค่าใช้จ่าย และสร้างนวัตกรรมใหม่ ๆ ในการปฏิบัติงาน เช่น การเขียนโค้ดในการช่วยประมวลผลชั้นข้อมูลเชิงพื้นที่เชิงเลข การสร้าง Model ในการประมวลผลในการจัดการข้อมูลขนาดใหญ่ เป็นต้น

ประโยชน์ต่อตนเอง

๑. ช่วยส่งเสริมการเรียนรู้และพัฒนาศักยภาพของตนเองในด้านเทคโนโลยี
๒. เพิ่มประสิทธิภาพในการปฏิบัติงานและลดภาระงานที่ซ้ำซ้อน
๓. สนับสนุนการตัดสินใจ วางแผน และวิเคราะห์ข้อมูลในการทำงาน

ประโยชน์ต่อองค์กร

๑. เพิ่มประสิทธิภาพและความรวดเร็วในการให้บริการประชาชน ลดความซ้ำซ้อนและขั้นตอนที่ไม่จำเป็น
๒. ช่วยในการวิเคราะห์และประมวลผลข้อมูลจำนวนมากเพื่อสนับสนุนการวางนโยบายและการตัดสินใจและนำไปสู่การปฏิบัติ
๓. เสริมสร้างความโปร่งใสและความรับผิดชอบในการดำเนินงานของหน่วยงานรัฐ
๔. สนับสนุนการจัดการทรัพยากรและระบบงานภาครัฐอย่างมีประสิทธิภาพ ลดค่าใช้จ่ายและความสูญเสียจากความผิดพลาด

ประโยชน์ต่อสาธารณะ

๑. ช่วยให้ประชาชนเข้าถึงบริการสาธารณะได้รวดเร็ว แม่นยำ และสะดวกมากยิ่งขึ้น
๒. ยกระดับคุณภาพชีวิตโดยช่วยลดความเสี่ยง เพิ่มความปลอดภัย และส่งเสริมความสะอาดสบายในชีวิตประจำวัน

แหล่งที่มา

หลักสูตร : AI for Everyone : ปัญญาประดิษฐ์เพื่ออนาคตของทุกคน

บรรยายโดย : ผู้ช่วยศาสตราจารย์ ดร.วิลาวัลย์ อินทร์ชำนาญ

สถาบัน: สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (Thailand Digital Government Academy)

รูปแบบหลักสูตร : การเรียนออนไลน์ (E-Learning)

ช่วงเวลาการฝึกอบรม : สิงหาคม ๒๕๖๘