

AI for Everyone : ปัญญาประดิษฐ์เพื่ออนาคตของทุกคน

โดย นางสาวเพ็ญภา ศีลาคำ
นักวิชาการแผนกภาพถ่ายปฏิบัติการ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับประเภทและกลไกการทำงานของ AI ในการยกระดับประสิทธิภาพการทำงานของภาครัฐ

๒. เพื่อสร้างความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์และแนวทางบริหารจัดการ AI ภายใต้กรอบธรรมาภิบาล เพื่อให้การประมวลผลข้อมูลภาครัฐมีความโปร่งใส ปลอดภัย และเท่าเทียม

สรุปเนื้อหา

ในปัจจุบันปัญญาประดิษฐ์ (Artificial Intelligence : AI) ได้เปลี่ยนผ่านจากเทคโนโลยีสมัยใหม่สู่การเป็นกลไกสำคัญในการขับเคลื่อนเศรษฐกิจและสังคมโลก โดยการทำงานพื้นฐานของ AI อยู่บนหลักการปรับเปลี่ยนข้อมูลดิบ (Raw Data) ให้กลายเป็นชุดข้อมูลเชิงโครงสร้างและรหัสฐานสองที่คอมพิวเตอร์สามารถประมวลผลได้ เช่น การเปลี่ยนลักษณะของลายนิ้วมือหรือม่านตาให้กลายเป็นรหัสเลข ๐ และ ๑ เพื่อเข้าสู่กระบวนการวิเคราะห์เชิงลึกและการตัดสินใจที่มีความแม่นยำ สำหรับในภาพรวมระดับมหภาค AI ได้เข้าไปเพิ่มประสิทธิภาพการทำงาน ลดข้อผิดพลาดและเร่งรัดการดำเนินงานในทุกอุตสาหกรรมหลัก โดยสามารถแบ่ง AI ออกเป็น ๓ ประเภท ตามระดับความสามารถ ดังนี้

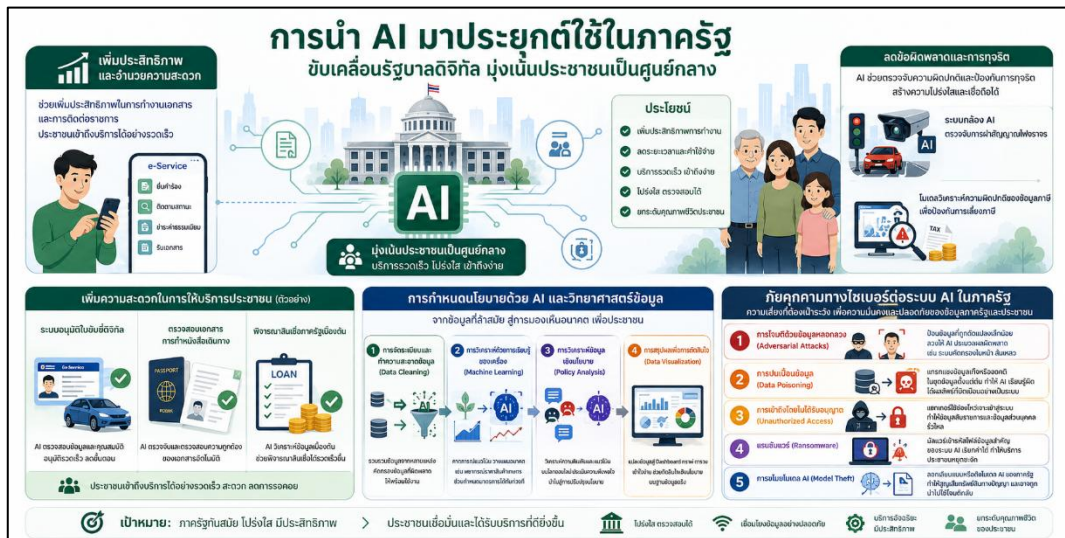
๑. Artificial Narrow Intelligence (ANI) หรือปัญญาประดิษฐ์แบบแคบ เป็น AI ที่ถูกออกแบบและฝึกฝนให้ทำงานในรูปแบบเฉพาะเจาะจงในขอบเขตที่จำกัดและมีความชำนาญเฉพาะด้าน เช่น ระบบสแกนลายนิ้วมือเพื่อระบุตัวตนและระบบขับเคลื่อนรถยนต์อัตโนมัติ เป็นต้น

๒. Artificial General AI (AGI) หรือ Strong AI เป็น AI ที่มีระดับสติปัญญาและความสามารถเทียบเท่ามนุษย์ สามารถเรียนรู้ ปรับตัว คิดวิเคราะห์ และทำงานได้หลายด้าน ซึ่งยังไม่มีอยู่จริงในปัจจุบันและเป็นเป้าหมายสำคัญที่นักวิจัยทั่วโลกกำลังเร่งพัฒนา

๓. Artificial Superintelligence (ASI) หรือปัญญาประดิษฐ์ขั้นยวดยิ่ง เป็นแนวคิดเชิงทฤษฎีในอนาคตที่ AI จะสามารถพัฒนาจนมีระดับความฉลาด ความคิดสร้างสรรค์ และสติปัญญาเหนือกว่ามนุษย์ โดยสามารถช่วยในการแก้ไขปัญหาวิกฤตระดับโลกที่ซับซ้อนเกินกว่าสติปัญญาของมนุษย์ เช่น การคิดค้นยารักษาโรคอุบัติใหม่ การจัดการความยากจน และการแก้ปัญหาภาวะโลกร้อน เป็นต้น

สำหรับการนำ AI มาประยุกต์ใช้ในภาครัฐถือเป็นแนวทางสำคัญในการปรับเปลี่ยนไปสู่รัฐบาลดิจิทัลที่มุ่งเน้นประชาชนเป็นศูนย์กลาง โดยมีประโยชน์ในการเพิ่มประสิทธิภาพและอำนวยความสะดวกในกระบวนการทำงานเอกสารและการติดต่อราชการส่งผลให้ประชาชนสามารถเข้าถึงบริการได้อย่างรวดเร็ว เช่น ระบบอนุมัติใบขับขี่ดิจิทัล การตรวจสอบเอกสารการทำหนังสือเดินทางและการพิจารณาสิทธิประโยชน์เบื้องต้น เป็นต้น นอกจากนี้ AI ยังสามารถลดข้อผิดพลาดและการทุจริต โดยใช้ระบบอัตโนมัติในการตรวจจับการกระทำผิดกฎหมาย เช่น ระบบกล้อง AI ตรวจจับการฝ่าสัญญาณไฟจราจร และการใช้โมเดลวิเคราะห์ความผิดปกติของข้อมูลภาษีเพื่อป้องกันการเลี่ยงภาษี เป็นต้น ดังภาพที่ ๑

ในอดีตการกำหนดนโยบายภาครัฐมักมีข้อจำกัดด้านการเข้าถึงข้อมูล เนื่องจากกระบวนการจัดเก็บและประมวลผลข้อมูลแบบดั้งเดิมต้องใช้เวลาอันส่งผลให้ข้อมูลที่น่ามาใช้อย่างมีประสิทธิภาพไม่สะท้อนสถานการณ์ปัจจุบัน โดยการประยุกต์ใช้ AI และวิทยาศาสตร์ข้อมูลได้เข้ามาช่วยแก้ไขข้อจำกัดนี้ ทำให้ภาครัฐสามารถ



ภาพที่ ๑ การนำ AI มาประยุกต์ใช้ในภาครัฐ

ที่มา : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัลสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

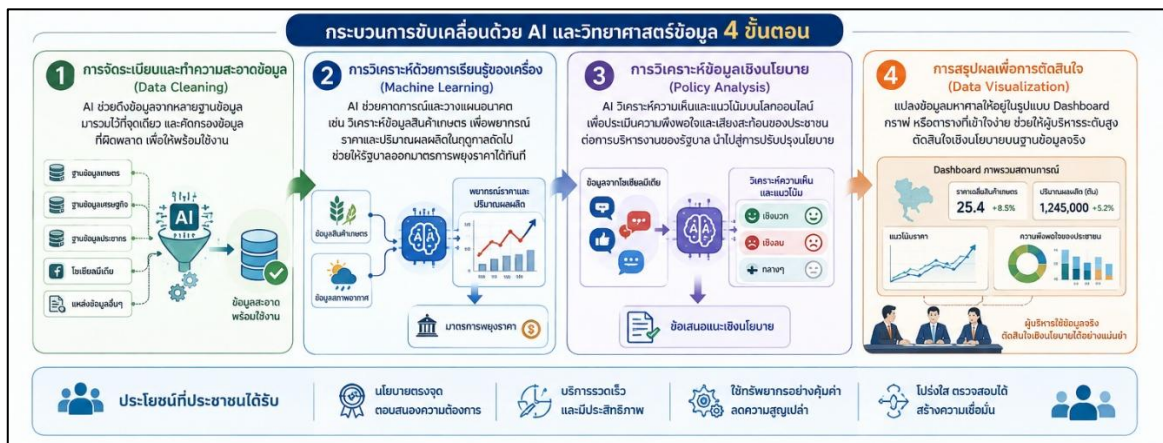
คาดการณ์แนวโน้ม มองเห็นปัญหาได้รวดเร็วขึ้น และตัดสินใจเชิงนโยบายได้อย่างแม่นยำ โดยมีกระบวนการขับเคลื่อนหลัก ๔ ขั้นตอน ดังนี้

๑. การจัดระเบียบและทำความสะอาดข้อมูล (Data Cleaning) เป็นการนำ AI เข้ามาช่วยในการดึงข้อมูล จากหลายฐานข้อมูลมารวมไว้ที่จุดเดียว และทำการคัดกรองข้อมูลที่ผิดพลาด เพื่อให้พร้อมสำหรับการนำไปใช้งาน

๒. การวิเคราะห์ด้วยการเรียนรู้ของเครื่อง (Machine Learning) เป็นการนำ AI มาช่วยในการคาดการณ์และวางแผนอนาคต เช่น การวิเคราะห์ข้อมูลสินค้าเกษตรเพื่อพยากรณ์ราคาและปริมาณผลผลิตในฤดูกาลถัดไป ช่วยให้รัฐบาลสามารถออกมาตรการการพุงราคาได้อย่างทันท่วงที

๓. การวิเคราะห์ข้อมูลเชิงนโยบาย (Policy Analysis) คือ การใช้ AI วิเคราะห์ความเห็นและแนวโน้มบนโลกออนไลน์ เพื่อประเมินความพึงพอใจและเสียงสะท้อนของประชาชนต่อการบริหารงานของรัฐบาล และนำไปสู่การปรับปรุงนโยบาย

๔. การสรุปผลเพื่อการตัดสินใจ (Data Visualization) คือ การแปลงข้อมูลมหาศาลให้อยู่ในรูปแบบของ Dashboard กราฟ หรือตารางที่เข้าใจง่าย ช่วยให้ผู้บริหารระดับสูงสามารถตัดสินใจเชิงนโยบายบนฐานข้อมูลจริง ดังภาพที่ ๒



ภาพที่ ๒ กระบวนการขับเคลื่อนด้วย AI

ที่มา : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัลสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

นอกเหนือจากโครงสร้างพื้นฐานของภาครัฐแล้ว Generative AI หรือ AI แบบสร้างสรรค์ ได้กลายเป็นเครื่องมือสำคัญที่ช่วยเพิ่มขีดความสามารถของภาคประชาชนในวงกว้าง โดยแบ่งออกเป็น ๔ มิติ ดังนี้

๑. มิติด้านการศึกษา เป็นการทำหน้าที่เป็นผู้สอนส่วนบุคคล ช่วยสรุปเนื้อหาบทเรียน ตัวข้อสอบ และอธิบายแนวคิดยาก ๆ ตามระดับความเข้าใจของผู้เรียน

๒. มิติด้านการทำงานและธุรกิจ เป็นการลดเวลาในการสร้างเอกสาร ร่างและตอบอีเมลธุรกิจ ตลอดจนการสร้างสรรคเนื้อหาสำหรับการตลาด รวมถึงการวิเคราะห์แนวโน้มของตลาดเพื่อออกแบบผลิตภัณฑ์และเขียนโฆษณา

๓. มิติด้านโปรแกรมเมอร์ เป็นการทำหน้าที่ผู้ช่วยเขียนโค้ดและช่วยตรวจสอบเพื่อแก้ไขจุดบกพร่องของซอฟต์แวร์ ซึ่งช่วยลดระยะเวลาในการพัฒนาเทคโนโลยี

๔. มิติด้านความบันเทิง เป็นการขยายขอบเขตจินตนาการผ่านการร่วมสร้างสรรค์ เช่น การแต่งนิยาย การประพันธ์ทำนองเพลงและการสร้างสรรคดีโอจากข้อความ เป็นต้น

แม้ว่า AI จะมีประโยชน์ทางด้านการบริหารจัดการ แต่การประมวลผลข้อมูลจำนวนมากของภาครัฐ ซึ่งครอบคลุมถึงข้อมูลที่ระบุตัวบุคคลได้ ข้อมูลทางการเงินและข้อมูลความมั่นคง ย่อมมีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ ภาครัฐจึงจำเป็นต้องมีมาตรการเฝ้าระวังและแนวทางรับมือกับรูปแบบภัยคุกคามทางไซเบอร์อย่างเหมาะสม โดยสามารถแบ่งรูปแบบภัยคุกคามทางไซเบอร์ออกเป็น ๕ รูปแบบ ดังนี้

๑. การโจมตีด้วยข้อมูลหลอกลวง (Adversarial Attacks) เป็นการป้อนข้อมูลที่ถูกดัดแปลงทางกายภาพหรือดิจิทัลเพียงเล็กน้อย เพื่อลวงให้ AI ประมวลผลผิดพลาด เช่น ระบบคัดกรองใบหน้าหรือระบบตรวจจับวัตถุทำงานล้มเหลว เป็นต้น

๒. การปนเปื้อนข้อมูล (Data Poisoning) เป็นการแทรกแซงและใส่ข้อมูลเท็จหรือข้อมูลที่เป็นอคติเข้าไปในชุดข้อมูลที่ใช้ฝึกฝนตั้งแต่ต้น ส่งผลให้กระบวนการเรียนรู้ของ AI เสียหายและได้ผลลัพธ์ที่บิดเบือนอย่างเป็นระบบ

๓. การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access) เป็นการที่แฮกเกอร์ใช้ประโยชน์จากช่องโหว่ของระบบที่มีการป้องกันต่ำเพื่อเจาะเข้าสู่ฐานข้อมูล ส่งผลให้ข้อมูลความลับราชการและข้อมูลส่วนบุคคลของประชาชนรั่วไหล

๔. แรนซัมแวร์ (Ransomware) เป็นการโจมตีด้วยมัลแวร์เรียกค่าไถ่ โดยการเข้ารหัสไฟล์ข้อมูลสำคัญของระบบ AI ทำให้ไม่สามารถใช้งานได้ ส่งผลให้ระบบบริการประชาชนหยุดชะงัก

๕. การขโมยโมเดล AI เป็นการลอกเลียนแบบหรือดิงเอาสถาปัตยกรรมและค่าน้ำหนักของโมเดล AI ของภาครัฐออกไป ส่งผลให้สูญเสียทรัพย์สินทางปัญญา อีกทั้งผู้ไม่หวังดียังสามารถหาช่องโหว่เพื่อโจมตีกลับ

สำหรับการนำ AI มาใช้ประมวลผลข้อมูลเพื่อการบริหารประชาชนของหน่วยงานภาครัฐจำเป็นต้องอยู่ภายใต้กรอบธรรมาภิบาล ๕ ประการ ดังนี้

๑. ความเป็นส่วนตัว (Data Privacy) คือ ข้อมูลของประชาชนต้องได้รับการคุ้มครองตามกฎหมาย ปลอดภัยจากการเข้าถึงโดยไม่ได้รับอนุญาต

๒. ความโปร่งใส (Transparency) คือ โมเดล AI ที่ใช้ตัดสินใจส่งผลกระทบต่อประชาชนต้องสามารถอธิบายที่มาของผลลัพธ์ได้

๓. ความเป็นธรรม (Fairness) คือ การที่ข้อมูลต้องไม่มีอคติเพื่อให้มั่นใจว่าประชาชนทุกคนได้รับการปฏิบัติอย่างเท่าเทียม

๔. ความปลอดภัยและความน่าเชื่อถือ (Safety & Reliability) คือ การที่ผลลัพธ์จาก AI ต้องผ่านการตรวจสอบความถูกต้องก่อนนำไปใช้งานจริง

๕. ความรับผิดชอบ (Accountability) คือ หากระบบ AI เกิดข้อผิดพลาดต้องมีการกำหนดตัวผู้รับผิดชอบทางกฎหมายและจริยธรรมอย่างชัดเจน

ในการพัฒนาภาครัฐสู่การเป็นองค์กรที่ขับเคลื่อนด้วย AI อย่างยั่งยืน จำเป็นต้องมีการวางโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยอย่างเป็นระบบ โดยมีแนวทางปฏิบัติหลัก ๓ ประการ ดังนี้

๑. การพัฒนามาตรฐานความปลอดภัยเฉพาะสำหรับ AI (AI-Specific Security Standards) เป็นการกำหนดโปรโตคอลและแนวปฏิบัติในการพัฒนา AI ที่ปลอดภัย ตั้งแต่ขั้นตอนการเก็บข้อมูล การฝึกฝนโมเดลไปจนถึงการจัดวางระบบ โดยใช้การเข้ารหัสขั้นสูงและโปรโตคอลสื่อสารที่มีความปลอดภัยทางไซเบอร์

๒. การเฝ้าระวังและตรวจจับเชิงรุก (Continuous Real-time Monitoring) เป็นการติดตั้งระบบตรวจจับภัยคุกคามอัตโนมัติที่ทำงานแบบเรียลไทม์ เพื่อตรวจสอบพฤติกรรมที่ผิดปกติของโมเดล AI และสกัดกั้นสัญญาณการโจมตี

๓. การเสริมสร้างขีดความสามารถและตระหนักรู้ (Capacity Building & Awareness) เป็นการมุ่งเน้นการฝึกอบรมบุคลากรภาครัฐและเจ้าหน้าที่ผู้รับผิดชอบระบบให้มีความรู้ความเข้าใจเท่าทันภัยคุกคามรูปแบบใหม่ทางไซเบอร์

ในการประยุกต์ใช้เทคโนโลยีควบคู่กับกรอบธรรมาภิบาลที่รัดกุมจะช่วยให้ภาครัฐสามารถใช้ประโยชน์จาก AI ในการยกระดับคุณภาพชีวิตของประชาชน ขับเคลื่อนเศรษฐกิจ และสร้างความมั่นคงปลอดภัยอย่างยั่งยืนในสังคม

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน

สามารถนำองค์ความรู้เรื่อง AI มาปรับใช้เพื่อปรับเปลี่ยนกระบวนการทำงานสู่ระบบดิจิทัลได้ โดยเริ่มตั้งแต่การปรับปรุงคุณภาพข้อมูลด้วยการจัดระเบียบและทำความสะอาดข้อมูลให้มีความถูกต้องและพร้อมใช้งาน จากนั้นนำระบบการเรียนรู้ของเครื่องมาช่วยในการคาดการณ์แนวโน้ม พยากรณ์สถานการณ์ หรือเตือนภัยล่วงหน้า เพื่อเตรียมมาตรการรับมือ นอกจากนี้ ยังสามารถใช้ Generative AI เข้ามาเป็นผู้ช่วยอัจฉริยะในการปฏิบัติงานประจำวัน เช่น การร่างเอกสารราชการ การสรุปเนื้อหาหายงาน การตอบอีเมล หรือการออกแบบเนื้อหาประชาสัมพันธ์ ซึ่งจะช่วยลดเวลาและขั้นตอนปฏิบัติงานได้

ประโยชน์ต่อตนเอง

๑. เพิ่มประสิทธิภาพและลดเวลาในการทำงาน
๒. ได้เรียนรู้และเข้าใจเทคโนโลยี AI และความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นทักษะสำคัญในยุคดิจิทัล
๓. สามารถคิดวิเคราะห์และแก้ปัญหาในงาน โดยใช้ข้อมูลจริงสนับสนุนแทนการใช้ความรู้สึกหรือประสบการณ์ส่วนตัว
๔. มีความตระหนักรู้ด้านความปลอดภัย เข้าใจรูปแบบภัยคุกคามไซเบอร์ ทำให้ระมัดระวังในการจัดการข้อมูล

ประโยชน์ต่อองค์กร

๑. กระบวนการทำงานมีความรวดเร็ว แม่นยำ และลดการใช้ทรัพยากรหรือการทำงานแบบซ้ำซ้อน
๒. ระบบ Data Visualization (Dashboard) สรุปข้อมูลให้เข้าใจง่าย ช่วยให้ผู้บริหารตัดสินใจเชิงนโยบายได้อย่างแม่นยำและทันสถานการณ์
๓. การบริหารจัดการ AI ภายใต้ธรรมาภิบาลช่วยให้องค์กรมีมาตรฐาน ตรวจสอบได้
๔. ระบบฐานข้อมูลมีความมั่นคงปลอดภัย

ประโยชน์ต่อสาธารณะ

๑. ประชาชนสามารถเข้าถึงบริการดิจิทัลได้สะดวกทุกที่และทุกเวลา
๒. การใช้ AI ที่มีธรรมาภิบาลช่วยให้มั่นใจได้ว่าประชาชนทุกคนจะได้รับการปฏิบัติอย่างเสมอภาคและเป็นธรรม
๓. ข้อมูลส่วนบุคคลมีความปลอดภัย
๔. สังคมมีความปลอดภัยและน่าอยู่ขึ้น

แหล่งที่มา

หลักสูตร : AI for Everyone : ปัญญาประดิษฐ์เพื่ออนาคตของทุกคน

บรรยายโดย : ผศ.ดร.วิลาวัลย์ อินทร์ชำนาญ คณบดี วิทยาลัยครีเอทีฟดีไซน์ แอนด์ เอ็นเตอร์เทนเมนต์ เทคโนโลยี มหาวิทยาลัยธุรกิจบัณฑิต

สถาบัน: สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัลสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

รูปแบบหลักสูตร : การเรียนออนไลน์ (TDGA e-learning)

ช่วงเวลาการฝึกอบรม : กรกฎาคม ๒๕๖๙