

Stages of AI/ML Development in Thai Banking Sector



หากพิจารณาจำกัดความของปัญญาประดิษฐ์ หรือ **Artificial Intelligence (AI)** แล้ว ส่วนใหญ่จะหมายถึง ศาสตร์แขนงหนึ่งที่ทำให้คอมพิวเตอร์มีความสามารถคิด วิเคราะห์ เรียนรู้ หรือตอบสนองได้ด้วยตัวเอง ซึ่งศาสตร์นี้ เกิดขึ้นและถูกนำมาใช้นานกว่า 50 ปีแล้ว และด้วยในปัจจุบันที่ เทคโนโลยีการประมวลผลก้าวหน้าขึ้น ทำให้ระบบสามารถ รวบรวมและวิเคราะห์ข้อมูลปริมาณมากและซับซ้อนได้ใน เวลาอันรวดเร็ว รวมทั้งได้ข้อมูลที่มีคุณภาพดีขึ้น ประกอบ กับการพัฒนาของ AI ที่ก้าวหน้าขึ้นมากในรูปแบบที่เรียกว่า การเรียนรู้ของเครื่องจักรหรือ Machine Learning (ML) ที่ทำให้คอมพิวเตอร์สามารถเรียนรู้ ปรับตัว และทำงานได้ ด้วยตนเองด้วย ML algorithm ผ่านการเรียนรู้และปรับปรุง ผลลัพธ์การทำงานจากรูปแบบของ input ที่ใส่เข้าไป ทำให้ ช่วยเพิ่มประสิทธิภาพในการทำงาน ML จึงเข้ามาเป็นอีก หนึ่งในตัวเร่งสำคัญที่ให้เทคโนโลยีด้าน AI ถูกนำมา ประยุกต์ใช้ในชีวิตประจำวัน และสนับสนุนการทำธุรกิจ มากขึ้น

ในปัจจุบันคงปฏิเสธได้ยากว่า AI ได้ถูกนำมาใช้ใน หลากหลายรูปแบบ และเข้ามาเป็นส่วนหนึ่งของชีวิตประจำวัน มากขึ้น เช่น ระบบผู้ช่วยอัจฉริยะอย่าง Siri หรือ Alexa

รถยนต์ขับเคลื่อนอัตโนมัติ (self-driving car) หรือแม้แต่ ปัญญาประดิษฐ์อย่าง Alpha Go ที่สามารถเอาชนะมนุษย์ใน การแข่งขันหมากล้อม ก็ล้วนเป็นผลมาจากเทคโนโลยี AI ทั้งนี้

ในภาคการธนาคารเองก็เช่นเดียวกัน AI ถูกนำมาใช้ใน หลากหลายผลิตภัณฑ์หรือบริการทางการเงินในรูปแบบใหม่ที่ แตกต่างออกไป ใช้เพื่อปรับปรุงผลิตภัณฑ์หรือบริการที่มีอยู่แล้ว ให้ดียิ่งขึ้น ทั้งการให้บริการลูกค้า การเพิ่มความสามารถของระบบ และในการด้านบริหารจัดการความเสี่ยงของภาคการธนาคาร

บทความนี้จะกล่าวถึง AI ในมิติที่เฉพาะเจาะจงมาที่ ML เป็นหลัก ทั้งในด้านรูปแบบการนำ AI/ML ไปประยุกต์ในภาคการ ธนาคาร ความเสี่ยงและสิ่งสำคัญที่ต้องคำนึงถึง และแนวทางการ พัฒนา AI/ML ในภาคการธนาคารของไทยในระยะถัดไป

1

รูปแบบการนำ AI/ML ไปประยุกต์ในภาคการธนาคาร

ภาคการธนาคารประยุกต์นำ AI/ML มาใช้ในหลากหลายรูปแบบ โดยสามารถจัดรูปแบบตามวัตถุประสงค์ของผลิตภัณฑ์หรือบริการ ได้เป็น 3 กลุ่มหลัก ดังนี้

1) กลุ่มงานให้บริการแก่ลูกค้า

เป็นการนำ AI/ML เข้ามาช่วยนำเสนอผลิตภัณฑ์บริการ หรือให้ความช่วยเหลือแก่ลูกค้า เพื่อให้ตรงกับความต้องการของลูกค้ามากที่สุด ดังจะเห็นได้จากธนาคารหลายแห่งมีบริการในลักษณะนี้ เช่น บริการ **Robo Advisor** ซึ่งทำให้คอมพิวเตอร์สามารถแนะนำการลงทุนหรือผลิตภัณฑ์ทางการเงินที่สอดคล้องกับพฤติกรรมและรูปแบบการดำเนินชีวิตของลูกค้าแต่ละราย รวมถึงบริการให้ข้อมูล ตอบข้อสงสัยหรือให้ความช่วยเหลือแก่ลูกค้าผ่านช่องทางออนไลน์ที่เรียกว่า **แชทบอท (Chatbot)** ซึ่งช่วยทำให้การตอบสนองต่อลูกค้าทำได้รวดเร็วและตรงกับความต้องการมากขึ้น

2) กลุ่มงานเพื่อเพิ่มความสามารถของระบบ

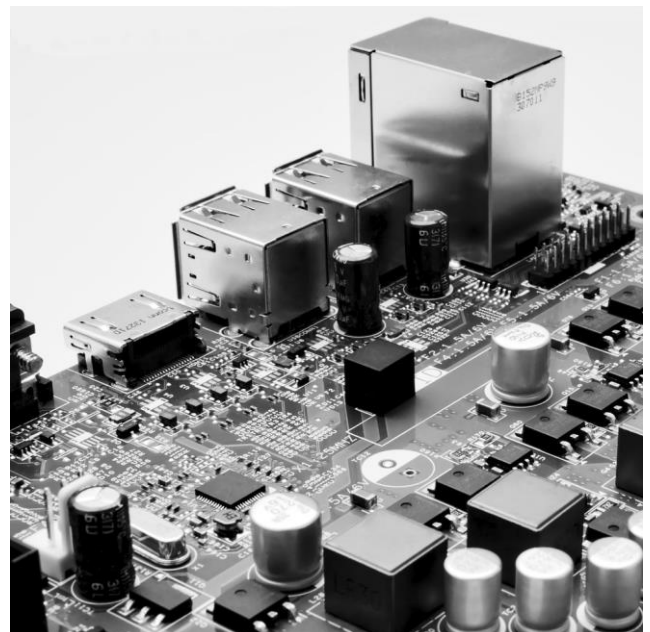
นำ AI/ML มาใช้เพื่อยกระดับการทำงานภายในให้มีประสิทธิภาพและรวดเร็วมากขึ้น เช่น ใช้ในด้านการ **ตรวจสอบความถูกต้องครบถ้วนของเอกสาร** ต่าง ๆ ก่อนนำไปประมวลผล หรือ **การพิสูจน์และยืนยันตัวตนดิจิทัล** ของลูกค้าที่ติดต่อเข้ามาด้วยการวิเคราะห์จากเสียงและคำพูดทางโทรศัพท์

3) กลุ่มงานด้านบริหารจัดการความเสี่ยง

ธนาคารนำ AI/ML มาช่วยในการประเมินความเสี่ยงของลูกค้าด้วยปัจจัยที่แตกต่าง หลากหลายและสะท้อนพฤติกรรมหรือความเสี่ยงมากขึ้น เช่น การวิเคราะห์ความเสี่ยงของลูกค้าจากรูปแบบการใช้สินเชื่อและบริการ การประเมินราคาสินทรัพย์ และการบริหารจัดการหนี้ เป็นต้น ซึ่งช่วยให้ธนาคารสามารถ **ประเมินความเสี่ยงในการให้สินเชื่อ** ของลูกค้าแต่ละรายได้แม่นยำและรวดเร็วขึ้น นอกจากนี้ AI/ML ยังถูกนำมาใช้ในการ **ตรวจจับการทุจริต** ในรูปแบบที่ซับซ้อน

และคาดการณ์รูปแบบการทุจริตใหม่ ๆ ได้อีกด้วยในปัจจุบันธนาคารในประเทศไทยพบว่าการนำ AI/ML เข้ามาใช้ในผลิตภัณฑ์และบริการทางการเงินของธนาคารอยู่บ้างแล้ว และมีแนวโน้มที่เพิ่มขึ้นอย่างต่อเนื่อง จากสถิติการรายงานข้อมูลการใช้เทคโนโลยี AI/ML ในปี 2564 พบว่ามีปริมาณการใช้งานเพิ่มขึ้นประมาณ 2.5 เท่า เมื่อเทียบกับปีก่อน โดยส่วนใหญ่อยู่ในกลุ่มผลิตภัณฑ์หรือบริการที่มีความเสี่ยงต่ำ เช่น บริการ Chatbot หรือ บริการ Robo Advisor นอกจากนี้ยังพบแนวโน้มเพิ่มขึ้นในการนำ AI/ML มาใช้ในงานที่มีความเสี่ยงหรือผลกระทบที่สูงมากขึ้น เช่น การวิเคราะห์ความเสี่ยงลูกค้าเพื่อพิจารณาอนุมัติสินเชื่อ หรือใช้วิเคราะห์แนวโน้มของภัยคุกคามไซเบอร์ เป็นต้น

นอกจากนี้ **ธนาคารแห่งประเทศไทยได้นำ AI/ML มาประยุกต์ใช้ในงานหลายด้านด้วยกัน** ตั้งแต่การช่วยตรวจหาธนบัตรที่ไม่สมบูรณ์ระหว่างการผลิต การจัดกลุ่มเอกสารที่มาจากหลากหลายแห่งและมีรูปแบบที่ไม่แน่นอน ไปจนถึงการคาดการณ์ทิศทางการส่งออกของประเทศ และใช้สนับสนุนงานตรวจสอบสถาบันการเงินของไทย



2 | ความเสี่ยงและสิ่งสำคัญที่ต้องคำนึงถึง

แม้ว่าการนำ AI/ML มาใช้จะก่อให้เกิดประโยชน์อย่างมากตามที่ได้กล่าวข้างต้น แต่ก็ยังมีสิ่งที่ต้องคำนึงถึงในการนำ AI/ML ไปใช้เช่นกัน เช่น 1) ความเท่าเทียมกันและการไม่เลือกปฏิบัติ 2) ความรับผิดชอบ 3) ความโปร่งใสและการอธิบายได้ 4) ความเป็นส่วนตัว 5) ความมั่นคงปลอดภัยด้าน IT และ 6) ความเชื่อถือได้

1) ความเท่าเทียมกันและการไม่เลือกปฏิบัติ (Fairness and Nondiscrimination)

ปัจจุบันการไม่เลือกปฏิบัติเป็นประเด็นที่มีความสำคัญเนื่องด้วยมีผลกระทบต่อมนุษย์เราโดยตรง เช่น การรับสมัครงานที่อาจเลือกพิจารณาเฉพาะผู้ที่จบการศึกษาจากบางมหาวิทยาลัย การกำหนดอัตราดอกเบี้ยของกลุ่มคนที่มีอาชีพที่ไม่มีรายได้ประจำที่อาจสูงกว่าอาชีพที่มีรายได้ประจำ หรือการเลือกปฏิบัติในการรักษาคนไข้ที่มีกำลังทรัพย์แตกต่างกับคนไข้กลุ่มอื่น จึงมีการนำเอาเทคโนโลยีด้าน AI/ML มาใช้ เพื่อลดอคติที่เกิดจากมนุษย์ ให้เกิดความเท่าเทียม และการไม่เลือกปฏิบัติ อย่างไรก็ตาม การใช้เทคโนโลยีดังกล่าวก็ยังสามารถก่อให้เกิดความไม่เท่าเทียมหรือการเลือกปฏิบัติได้ โดยทางออกส่วนหนึ่ง คือ **ลดการใช้ข้อมูลที่ไม่เป็นกลางหรืออคติ (bias) ให้ได้มากที่สุด** ซึ่งปัจจุบันมีหลากหลายวิธีในการลด bias เช่น การสุ่มกลุ่มตัวอย่างข้อมูล (sampling) ให้กระจายตัวและสะท้อนถึงประชากร (population) อย่างเหมาะสม การนำเครื่องมือมาช่วยวิเคราะห์และตรวจสอบการเกิด bias ในแต่ละขั้นตอน รวมถึง การใช้ความเห็นจากผู้เชี่ยวชาญในหลากหลายศาสตร์ เพื่อให้ได้มุมมองที่ครบถ้วนรอบด้าน และช่วยลดการเกิด bias โดยไม่ตั้งใจ

นอกจากนี้ บางครั้งในการพัฒนาแบบจำลอง ควรให้ความสำคัญกับการนำข้อมูลหรือปัจจัยที่มีความอ่อนไหว เช่น เพศ หรือสีผิว มาใช้ในการพัฒนาหรือตัดสินใจทั้งทางตรงและทางอ้อม เนื่องจากจะนำไปสู่การเลือกปฏิบัติได้

ดังเช่น ในสหราชอาณาจักรมีการออกกฎหมายห้ามนำข้อมูลด้านเพศมาใช้ในการพิจารณา แต่ในทางปฏิบัติบางแบบจำลองยังสามารถใช้ปัจจัยอื่นมาใช้เพื่อระบุเพศได้โดยอ้อม ซึ่งเรื่องนี้ก็ยังคงทำให้เกิดปัญหาการเลือกปฏิบัติเช่นเดิมและเป็นสิ่งที่ต้องหาทางแก้ไขต่อไป

2) ความรับผิดชอบ (Accountability)

AI/ML เป็นเทคโนโลยีใหม่และเพิ่งได้รับความนิยมใช้งานแพร่หลายไม่นาน ทำให้ยังมีความคลุมเครือในเรื่องความรับผิดชอบ (liability) และความรับผิดชอบทางกฎหมาย (legal responsibility) โดยที่ผ่านมามีผลกระทบจากข้อผิดพลาดของระบบที่เกิดขึ้น มนุษย์ยังคงเป็นผู้รับผิดชอบ แม้ว่าคน ๆ นั้นจะเข้าไปมีส่วนเกี่ยวข้องเพียงเล็กน้อย หรือมีส่วนร่วมโดยไม่ได้ตั้งใจก็ตาม ดังเช่น ในปี 2561 ในรัฐ Arizona มีเหตุการณ์รถขับเคลื่อนอัตโนมัติ (autonomous car) ของบริษัทแห่งหนึ่งเกิดอุบัติเหตุทำให้มีผู้เสียชีวิต ส่งผลให้บริษัทถูกฟ้อง ซึ่งหลังการพิจารณาคดี ศาลตัดสินให้บริษัทผู้ผลิตรถยนต์ไม่มีความผิด แต่ผู้ที่นั่งอยู่ในรถซึ่งทำหน้าที่ดูแลความปลอดภัยตกเป็นจำเลย และต้องรับผิดชอบหากทำให้ผู้อื่นเสียชีวิตโดยความประมาทจากการจับยานพาหนะ และอีกกรณีหนึ่ง ในปี 2562 เศรษฐีชาวฮ่องกงสูญเสียเงินกว่า 20 ล้านเหรียญจากการลงทุนโดยระบบอัตโนมัติ ซึ่งท้ายที่สุดเขาก็ทำเรื่องฟ้องร้องบริษัทที่ขายระบบนั้นให้แก่เขา

ดังนั้น ควรมีการกำหนดความรับผิดชอบ มีกระบวนการซึ่งมีผู้ที่รับผิดชอบผลการดำเนินงานของระบบอย่างชัดเจน เพื่อให้มั่นใจว่าการพัฒนาระบบได้ผ่านการพิจารณา คำนึงถึงผลที่จะตามมา และไม่เกิดความคลุมเครือในด้านความรับผิดชอบ

นอกจากนี้ ในบางกรณีการนำเทคโนโลยี AI/ML มาใช้งาน แทนมนุษย์ อาจส่งผลกระทบต่อการใช้งานหรือการลดจำนวนพนักงาน ดังนั้นองค์กรจำเป็นต้องจัดเตรียมการพัฒนาทักษะและบริหารจัดการบุคลากรที่เหมาะสมเพื่อลดผลกระทบดังกล่าว

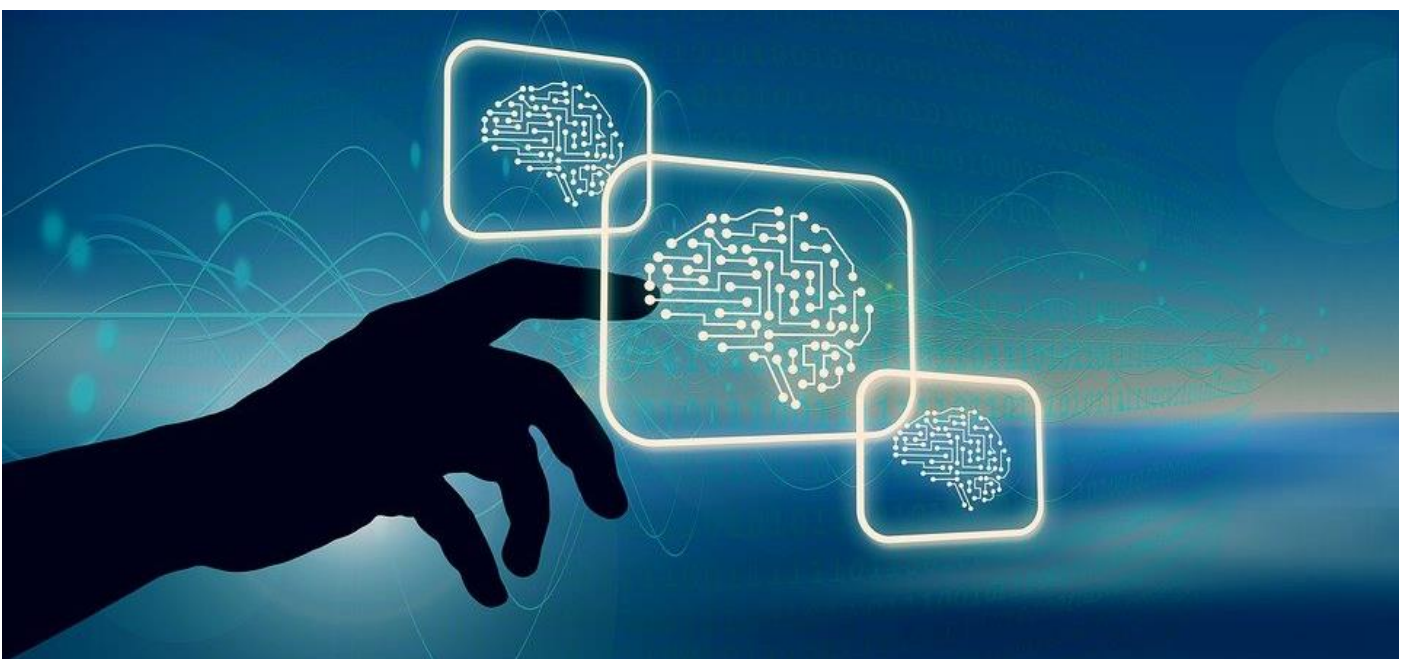
3) ความโปร่งใส และการอธิบายได้ (Transparency and Explainability)

โดยพื้นฐาน AI/ML เป็นเทคโนโลยีที่มีความซับซ้อน และยากต่อการอธิบายถึงกระบวนการคิดคำนวณหรือการตัดสินใจ ซึ่งในหลายกรณีผู้พัฒนาหรือผู้ใช้งานไม่ทราบว่า AI/ML มีกระบวนการตัดสินใจอย่างไร หรือมีปัจจัยอะไรบ้างที่มีผลต่อการตัดสินใจ ซึ่งเป็นปัญหาของทั้งผู้พัฒนา ผู้บริหารในองค์กร ผู้กำกับดูแล รวมถึงผู้ใช้งาน ถึงความเชื่อมั่นของการนำ AI/ML ไปใช้ในงานที่ต้องการความชัดเจนและความโปร่งใส

ดังนั้น ในการพัฒนาจำเป็นต้องคำนึงถึงวิธีการ แนวทางหรือรูปแบบในการอธิบายการทำงานของ AI/ML ให้ได้อย่างเหมาะสม อีกทั้งกระบวนการสื่อสาร หรือแจ้งเตือนให้แก่ผู้ใช้งานเพื่อให้ทราบว่ากำลังใช้งานหรือสนทนากับระบบอัตโนมัติ เพื่อแสดงความโปร่งใสและไม่ก่อให้เกิดความเข้าใจผิด

4) ความเป็นส่วนตัว (Privacy)

สำหรับการพัฒนา AI/ML นั้น ในบางครั้งมีการใช้ข้อมูลส่วนบุคคลเข้ามาเกี่ยวข้องด้วย ซึ่งในปัจจุบัน หลายประเทศมีกฎหมายที่เข้ามาควบคุมไม่ให้เกิดการละเมิดความเป็นส่วนตัวของผู้ใช้หรือผู้ให้ข้อมูล ไม่ว่าจะเป็นทั้งในประเทศไทยหรือสากล เช่น ข้อกำหนดของสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (GDPR) พระราชบัญญัติประกันสุขภาพแบบพกพา และความรับผิดชอบ (HIPAA) ที่กล่าวถึงการคุ้มครองข้อมูลของกลุ่มสาธารณสุข หรือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของประเทศไทยที่บัญญัติมาเพื่อกำกับดูแลการนำข้อมูลส่วนบุคคลไปใช้ เป็นต้น ซึ่งกฎหมายเหล่านี้ส่งผลโดยตรงที่นำข้อมูลไปพัฒนาโมเดล AI/ML เช่น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งต้องได้รับอนุญาต (consent) จากเจ้าของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน รวมถึงสิทธิ์ของเจ้าของข้อมูลที่สามารถขอให้ลบหรือทำลายข้อมูลของตนเองได้ (right to erasure) เป็นต้น



ดังนั้นผู้พัฒนาจำเป็นต้องคำนึงถึงความเหมาะสมของ
เฟืองไว และหลักเกณฑ์ดังกล่าว โดยต้องพิจารณาใช้ข้อมูล
เท่าที่จำเป็น (least privilege) ระบุวัตถุประสงค์ที่ชัดเจน
ว่านำข้อมูลไปใช้ในเรื่องใด พิจารณาการใช้เทคนิค data
masking และ data anonymization เพื่อช่วยปกปิดข้อมูล
ส่วนบุคคลที่สำคัญ

5) ความมั่นคงปลอดภัยด้าน IT (IT Security)

การรักษาความมั่นคงปลอดภัยยังคงเป็นสิ่งทีทุกภาค
ส่วนต้องให้ความสำคัญ เนื่องจากเทคโนโลยี AI/ML นั้น
อาศัยระบบ IT เป็นพื้นฐานทำให้ยังมีความเสี่ยงด้าน
เทคโนโลยีสารสนเทศ (IT Risk) ตามมาด้วย ผู้พัฒนาจึง
ต้องคำนึงถึงการรักษาความมั่นคงปลอดภัยของระบบ ซึ่ง
ควรประกอบไปด้วย 3 มิติ ดังนี้

- **การรักษาความลับของข้อมูล** โดยในทุกขั้นตอนตั้งแต่
ของข้อมูล การเก็บรวบรวม วิเคราะห์ และประมวลผล
ต้องคงไว้ซึ่งความลับของข้อมูลไม่ให้ผู้ที่ไม่มีสิทธิ์หรือ
ผู้ที่ไม่เกี่ยวข้องสามารถเข้าถึงได้
- **ความถูกต้องของข้อมูล** ที่ต้องควบคุมไม่ให้เกิด
แก้ไขได้โดยไม่ได้รับอนุญาต เพื่อให้ระบบและข้อมูล
มีความถูกต้องและเชื่อถือได้อยู่เสมอ
- **ความพร้อมใช้ของระบบ** ระบบควรสามารถให้บริการ
ได้อย่างต่อเนื่อง โดยเฉพาะอย่างยิ่งกับระบบงานสำคัญ
และมีผลกระทบสูง ทั้งในด้านของจำนวนผู้ใช้งานและ
ความเชื่อมั่น

ดังนั้นผู้พัฒนาจำเป็นต้อง**จัดให้มีการกำหนดมาตรฐาน**
การรักษาความปลอดภัยให้ครบถ้วน ตั้งแต่การค้นหา
และการประเมินช่องโหว่ (vulnerability assessment)
การทดสอบเจาะระบบ (penetration test) การรักษา
ความมั่นคงปลอดภัยของข้อมูลตามระดับความสำคัญ
รวมถึงการบริหารจัดการความเสี่ยงจากการใช้บริการ
จากผู้ให้บริการภายนอกอย่างเหมาะสม

6) ความเชื่อถือได้ (Reliability)

ระบบที่ดีควรคงความสามารถในการทำงานได้ตามที่
ออกแบบและเริ่มใช้งานตั้งแต่แรก ทนทานต่อการเปลี่ยนแปลง
ของสภาพแวดล้อม (robustness) รวมถึงยังคงทำงานได้
อย่างถูกต้อง หากถูกโจมตีแบบ adversarial attack ซึ่งเป็น
เทคนิคการหลอกให้ AI/ML ทำงานผิดพลาด เช่น การใส่
ข้อมูลรบกวน (noise) เข้าไป หรือ การดัดแปลงข้อมูลบางส่วน
เพื่อทำให้ระบบตรวจสอบความแท้จริงของเอกสารทำงาน
ผิดพลาด เป็นต้น

ดังนั้น ผู้พัฒนา**ควรจัดให้มีกระบวนการ ทดสอบ หรือ**
เครื่องมือ เพื่อใช้ทดสอบความเชื่อถือได้ และปรับปรุงคุณภาพ
อย่างเป็นประจำสม่ำเสมอ รวมถึง **จัดให้มีผู้เชี่ยวชาญภายนอก**
มาช่วยตรวจสอบ และประเมินประสิทธิภาพ เพื่อให้มั่นใจว่า
ระบบยังสามารถทำงานได้ตามที่กำหนดไว้ และอยู่ในระดับ
ความเสี่ยงที่เหมาะสมยอมรับได้

3 | แนวทางการพัฒนา AI/ML ในภาคการธนาคารของไทย

ที่ผ่านมาหลายธนาคารในไทยได้พัฒนาและประยุกต์ใช้ AI/ML ในผลิตภัณฑ์และบริการทางการเงินอย่างต่อเนื่อง อย่างไรก็ตาม ยังมีอีกหลากหลายด้านที่ยังจำเป็นต้องพัฒนา ส่งเสริม และผลักดันเพิ่มเติมในมิติต่าง ๆ เช่น

1) ส่งเสริมการสร้างความรู้และบุคลากรในการพัฒนา

ความรู้ ความเข้าใจในการพัฒนาเทคโนโลยี รูปแบบการนำไปประยุกต์ใช้ ความเสี่ยงหรือข้อจำกัดต่าง ๆ จากการนำ AI/ML มาใช้ เป็นเรื่องที่ผู้ที่เกี่ยวข้องในแต่ละด้าน ไม่ว่าจะเป็นด้านธุรกิจ ด้านพัฒนาระบบ ด้านกำกับดูแล ความเสี่ยง หรือด้านตรวจสอบ จำเป็นต้องเรียนรู้และพัฒนาในเรื่องนี้ เพื่อให้การใช้ AI/ML เกิดประสิทธิภาพ ตรงกับวัตถุประสงค์ และอยู่ในระดับความเสี่ยงที่เหมาะสม

นอกจากนี้ การสร้างบุคลากรที่มีความรู้และทักษะในเรื่องนี้ เป็นสิ่งจำเป็น และยิ่งขาดแคลนอยู่มาก

เนื่องมาจากหลักการ และวิธีคิดในการพัฒนา AI/ML แตกต่างจากการพัฒนาระบบแบบเดิม ๆ อีกทั้งยังมีความรู้ในศาสตร์หลาย ๆ แขนง เช่น พื้นฐานวิทยาการคอมพิวเตอร์ การพัฒนาโปรแกรมและการวิเคราะห์ข้อมูล (programming and data analytics) หรือสถิติ และความน่าจะเป็น (probability and statistic) เป็นต้น

ทั้งนี้ ธนาคารแห่งประเทศไทยจะร่วมส่งเสริมให้เกิดกลุ่มความร่วมมือในเรื่อง AI/ML ในภาคการเงิน และการธนาคารอย่างเป็นรูปธรรม พัฒนาองค์ความรู้ในแต่ละระดับทั้งระดับผู้บริหารระดับสูง ผู้พัฒนา หรือผู้ปฏิบัติงานและการเพิ่มจำนวนบุคลากรในด้านนี้ให้เพิ่มมากขึ้นอีกด้วย

2) ส่งเสริมความเข้าใจความเข้าใจเทคโนโลยี AI/ML ของประชาชนผู้ใช้งาน

นอกจากการส่งเสริมความรู้ให้แก่ผู้พัฒนาแล้ว ในภาคประชาชนเองก็ควรได้รับพัฒนาความรู้ในการใช้เครื่องมือ อุปกรณ์ และเทคโนโลยีที่เกี่ยวข้องกับ AI/ML เช่น ตระหนักรู้ว่ากำลังสนทนากับ Chatbot เป็นต้น

รวมถึง ในฐานะผู้ใช้งาน ควรมีความตระหนักรู้ถึงความสำคัญของข้อมูลส่วนบุคคล เข้าใจในวัตถุประสงค์และสิทธิต่าง ๆ เมื่อกำหนดนำข้อมูลส่วนบุคคลไปใช้

3) ส่งเสริมให้เกิดคุณภาพและปริมาณข้อมูลที่เหมาะสม

หนึ่งในปัจจัยสำคัญที่จะส่งผลให้ AI/ML สามารถทำงานได้อย่างมีประสิทธิภาพ ชาญฉลาด และตรงตามวัตถุประสงค์ที่ต้องการ คือ คุณภาพและปริมาณของข้อมูล ซึ่งควรได้รับการส่งเสริมให้มีการพัฒนาด้านข้อมูลอย่างต่อเนื่องในหลากหลายด้าน เช่น

- **รูปแบบของข้อมูล:** ควรกำหนดรูปแบบของข้อมูลที่สามารถนำไปใช้ ไม่ว่าจะเป็นการใช้ข้อมูลเชิงโครงสร้าง (structure data) หรือ ข้อมูลที่ไม่มีโครงสร้าง (unstructured data) เช่น ไฟล์เสียง รูปภาพ รวมทั้งช่วงเวลาการเกิดข้อมูล และการกระจายตัวของข้อมูล
- **แหล่งที่มาของข้อมูล:** ใช้ข้อมูลจากแหล่งที่น่าเชื่อถือไม่ว่าจะเป็นจากภายในองค์กรเอง หรือจากหน่วยงานภายนอก
- **คุณภาพของข้อมูล:** ใช้ข้อมูลที่มีความถูกต้องและครบถ้วนข้อมูล
- **การรักษาความปลอดภัยและความเป็นส่วนตัว:** กำหนดชั้นความลับและสิทธิการเข้าถึง และการปกปิดข้อมูลส่วนตัว
- **ปริมาณข้อมูล:** ส่งเสริมการใช้จำนวนข้อมูลที่มากเพียงพอ และครอบคลุมในมิติสำคัญ

4) กำหนดหลักเกณฑ์ในการกำกับดูแลในภาคการธนาคาร

ด้วยเทคโนโลยี AI/ML เป็นเทคโนโลยีที่มีความซับซ้อน พัฒนาการอย่างรวดเร็ว อีกทั้งยังไม่มีรูปแบบที่ตายตัว ทำให้การออกกฎเกณฑ์ และวิธีการกำกับดูแลยังมีความท้าทายอยู่มากในการสร้างสมดุลระหว่างการส่งเสริมการใช้เทคโนโลยี และการบริหารจัดการความเสี่ยง ดังนั้น หน่วยงานกำกับดูแลทางการเงินในแต่ละประเทศจึงมีแนวทางในการดำเนินการในเรื่องนี้ที่แตกต่างกัน เช่น คณะกรรมาธิการยุโรป (European Commission) ธนาคารกลางอังกฤษ (Bank of England) หรือ ธนาคารกลางฮ่องกง (Hong Kong Monetary Authority) ใช้ผลสำรวจจากสถาบันการเงินต่าง ๆ ในเรื่องเกี่ยวกับการนำ AI/ML มาใช้ เพื่อสื่อสารให้ทราบถึงทิศทาง รูปแบบการพัฒนา สิ่งที่เป็นอุปสรรคหรือความเสี่ยงที่ต้องคำนึงถึง ในขณะที่ยังคง เช่น ธนาคารกลางสิงคโปร์ (Monetary Authority of Singapore) กำหนดกรอบหลักการ การพัฒนา AI/ML เพื่อเป็นแนวทางพื้นฐานที่ควรใช้พิจารณาในการพัฒนา และคำนึงถึงในการนำ AI/ML มาใช้

สำหรับประเทศไทยนั้น มีการกำหนดแนวทางกำกับดูแลอยู่บ้างแล้ว เช่น หลักการและแนวทางจริยธรรมปัญญาประดิษฐ์ของประเทศไทย (Digital Thailand – AI Ethics Guideline) โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำหรับการพัฒนาและใช้งานปัญญาประดิษฐ์ รวมถึง หลักเกณฑ์ในเรื่อง AI/ML ในภาคการธนาคารนั้น **ธนาคารแห่งประเทศไทยอยู่ระหว่างศึกษาและดำเนินการร่วมกับภาคการธนาคาร หน่วยงานที่เกี่ยวข้องต่าง ๆ เพื่อให้การกำกับดูแลความเสี่ยงไปควบคู่กับการส่งเสริมให้เกิดการพัฒนาในเรื่องนี้** อย่างไรก็ตาม หนทางนี้ภาคการธนาคารสามารถประยุกต์กฎหมายและหลักเกณฑ์ที่เกี่ยวข้องมาใช้อ้างอิงเป็นแนวทางการบริหารจัดการความเสี่ยงจากการใช้ AI/ML ได้ เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2563 ที่มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคล ทำให้การพัฒนาเทคโนโลยี AI/ML ที่จำเป็นต้องนำข้อมูลส่วนบุคคลมาใช้งานจะต้องมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่นำมาใช้ให้เหมาะสม และเพียงพอ หรือหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) ซึ่งครอบคลุมการบริหารจัดการความเสี่ยงและการรักษาความมั่นคงปลอดภัยด้าน IT เป็นต้น



ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ธนาคารแห่งประเทศไทย

Email : ITSupervision@bot.or.th