กรอบการกำกับดูแลการใช้งาน
ปัญญาประดิษฐ์ (Artificial Intelligence) และ
การเรียนรู้ของเครื่อง (Machine Learning) ในตลาดทุน

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
ธันวาคม 2566

สารบัญ

1. บทนำ

ด้วยปัจจุบันปัญญาประดิษฐ์ (Artificial Intelligence : AI) และการเรียนรู้ของเครื่อง (Machine Learning : ML) (AI/ML) มีการพัฒนาขึ้นอย่างรวดเร็ว เนื่องจากการเพิ่มขึ้นของข้อมูลอิเล็กทรอนิกส์และเครื่องคอมพิวเตอร์ที่มีประสิทธิภาพในการประมวลผลสูง สภาพแวดล้อมดังกล่าวได้สร้างโอกาสใหม่ให้แก่ผู้ประกอบธุรกิจในตลาดทุน (“ผู้ประกอบธุรกิจ”) ที่ต้องการนำ AI/ML มาใช้เพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการดำเนินงานขององค์กร ซึ่งสามารถแบ่งออกเป็น 2 ด้าน ได้แก่

(1) ด้านประสิทธิภาพและประสิทธิผลภายในองค์กร : AI/ML ช่วยติดตามและบริหารจัดการความเสี่ยงต่าง ๆ ในองค์กร สนับสนุนกระบวนการตัดสินใจ ตรวจจับความผิดปกติหรือเหตุอันควรสงสัย ซึ่งสามารถนำไปสู่การแก้ไขปัญหาได้อย่างทันท่วงที

(2) ด้านประสิทธิภาพและประสิทธิผลของการให้บริการลูกค้า : AI/ML ช่วยอำนวยความสะดวกแก่ลูกค้าของผู้ประกอบธุรกิจ และสนับสนุนการออกแบบกลยุทธ์การลงทุนที่เพิ่มโอกาสและความคาดหวังผลตอบแทนที่สูงขึ้น

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) สนับสนุนการนำเทคโนโลยีใหม่มาใช้ในภาคตลาดทุน และเล็งเห็นถึงความเสี่ยงที่เกี่ยวข้องกับการใช้งาน AI/ML จึงได้จัดทำคู่มือฉบับนี้ขึ้น เพื่อช่วยให้ผู้ประกอบธุรกิจตระหนักถึงความเสี่ยงและแนวทางการนำ AI/ML มาใช้งานอย่างเหมาะสม และเพื่อสร้างความเชื่อมั่นของประชาชนในการลงทุนในตลาดทุนไทย

ทั้งนี้ ความเสี่ยงจากการใช้งาน AI/ML ตลอดจนหลักการพื้นฐานในคู่มือฉบับนี้ เป็นการนำเสนอผลการศึกษาข้อมูลจากภายในและต่างประเทศ ซึ่งอาจยังไม่ครอบคลุมกับบางบริบทของการใช้งาน AI/ML และความเสี่ยงอื่น ๆ ที่อาจจะเกิดขึ้นได้ในอนาคตด้วยความก้าวหน้าทางเทคโนโลยี ทั้งฮาร์ดแวร์และซอฟต์แวร์ที่เปลี่ยนแปลงไปอย่างรวดเร็ว

2. บทนิยาม

คำศัพท์ที่ใช้ในคู่มือฉบับนี้ มีความหมายดังต่อไปนี้

อัลกอริทึม (Algorithm) หมายถึง ขั้นตอนและวิธีการในการประมวลผลเพื่อหาผลลัพธ์ที่ชัดเจนด้วยระบบคอมพิวเตอร์ หรือวิธีการอื่นใดในทำนองเดียวกัน

โมเดล (Model) หมายถึง แบบจำลองข้อมูลทางคณิตศาสตร์หรือโปรแกรมที่ถูกสร้างขึ้นจากอัลกอริทึมและถูกสอนโดยอาศัยชุดข้อมูลเพื่อให้มีความสามารถในการทำงานตามวัตถุประสงค์ที่กำหนด เช่น การพยากรณ์ผลการดำเนินธุรกิจ การแยกแยะชนิดของวัตถุ และการสร้างรูปภาพ เป็นต้น

ปัญญาประดิษฐ์ (Artificial Intelligence : AI) หมายถึง เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้คอมพิวเตอร์มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การให้เหตุผล และการแก้ไขปัญหา เป็นต้น ตามวัตถุประสงค์ที่มนุษย์กำหนด

การเรียนรู้ของเครื่อง (Machine Learning : ML) หมายถึง ปัญญาประดิษฐ์ (AI) ประเภทหนึ่งที่มีความสามารถในการเรียนรู้และปรับปรุงประสิทธิภาพการทำงานของตน โดยใช้อัลกอริทึมในการวิเคราะห์และเรียนรู้จากข้อมูลที่ได้รับจากการสอน หรือสภาพแวดล้อม

AI/ML หมายถึง เทคโนโลยีด้าน Artificial Intelligence หรือ Machine Learning ที่ช่วยสนับสนุนการทำงาน หรือทำงานตามวัตถุประสงค์ที่มนุษย์กำหนด

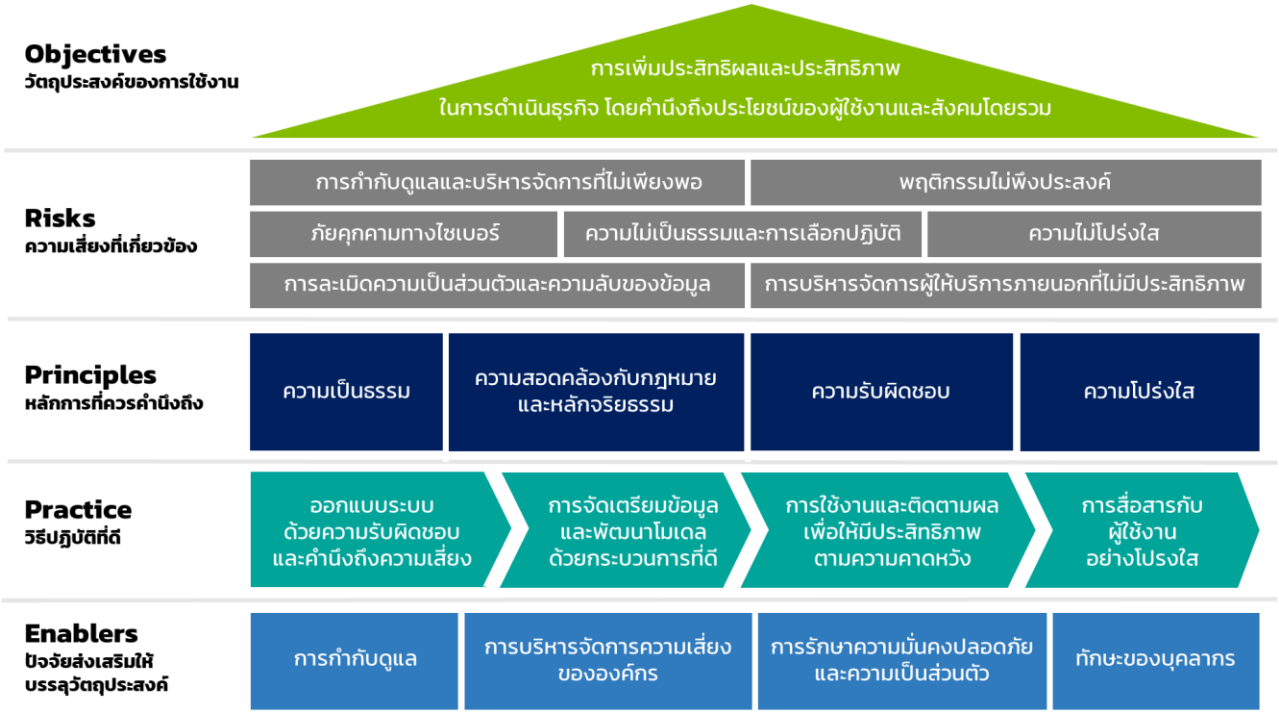
ปัญญาประดิษฐ์แบบรู้สร้าง (Generative AI) หมายถึง AI/ML ที่มีความสามารถในการสร้าง (Generate) ชุดข้อมูลใหม่ขึ้นมา ไม่ว่าจะเป็นข้อความ ภาพ เสียง Code และสารสนเทศอื่น ๆ จากการเรียนรู้ของโมเดลโดยมีตัวอย่างของ Generative AI ซึ่งเป็นที่รู้จักในวงกว้างคือ ChatGPT หรือ Google Bard เป็นต้น

ความเป็นธรรม (Fairness) หมายถึง การตัดสินใจที่อยู่บนพื้นฐานของความเท่าเทียม โดยไม่เลือกปฏิบัติกับบุคคลหรือสิ่งใด ๆ และหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) เช่น เพศ เชื้อชาติ ศาสนา และความเห็นทางการเมือง เป็นต้น ในกระบวนการตัดสินใจ เว้นแต่การกระทำดังกล่าวจะเป็นไปอย่างสมเหตุสมผล

จริยธรรม (Ethics) หมายถึง การออกแบบ พัฒนาและใช้งาน AI/ML ที่พฤติกรรมหรือผลจากการทำงานของ AI สอดคล้องกับกฎระเบียบ แนวปฏิบัติ หลักจริยธรรม หรือหลักการอันดีที่พึงปฏิบัติตามบริบทที่ AI/ML ถูกนำไปประยุกต์ใช้

ความโปร่งใส (Transparency) หมายถึง ความสามารถในการอธิบายเหตุการณ์ การกระทำ กระบวนการทำงาน และกิจกรรมต่าง ๆ เกี่ยวกับ AI/ML รวมถึงตรวจสอบย้อนหลังเหตุการณ์ที่เกิดขึ้นได้

3. กรอบการกำกับดูแลการใช้งาน AI/ML



ภาพประกอบ : กรอบการกำกับดูแลการใช้งาน AI/ML (AI/ML Governance Framework)

AI/ML เป็นเทคโนโลยีที่มีความซับซ้อน มีการพัฒนาอย่างรวดเร็ว และสามารถช่วยลดต้นทุนและเพิ่มประสิทธิภาพในการดำเนินธุรกิจได้อย่างมาก อย่างไรก็ดี การใช้งาน AI/ML สามารถก่อให้เกิดความเสี่ยงใหม่ที่เพิ่มขึ้นเช่นกัน ดังนั้น ก่อนตัดสินใจนำ AI/ML มาใช้งาน ผู้ประกอบธุรกิจควรเข้าใจถึงความเสี่ยงที่เกี่ยวข้องอย่างรอบด้านและจัดให้มีมาตรการควบคุมอย่างเหมาะสม ในคู่มือฉบับนี้จะอธิบายกรอบการกำกับดูแลการใช้งาน AI/ML (AI/ML Governance Framework) โดยประกอบด้วย 5 ส่วน ซึ่งสรุปได้ ดังนี้

3.1 วัตถุประสงค์ของการใช้งาน

การใช้งาน AI/ML เพื่อเพิ่มประสิทธิผลและประสิทธิภาพในการดำเนินธุรกิจ ควรมีวัตถุประสงค์ที่ชัดเจนและเหมาะสม โดยคำนึงถึงประโยชน์ต่อผู้ใช้งานและสังคมโดยรวม

3.2 ความเสี่ยงที่เกี่ยวข้อง

AI/ML เป็นเทคโนโลยีที่มีบทบาทสำคัญในการเพิ่มศักยภาพในการดำเนินธุรกิจด้วยความสามารถในการวิเคราะห์ข้อมูลและช่วยในการตัดสินใจ อย่างไรก็ดี การใช้งาน AI/ML ต้องมีการบริหารจัดการความเสี่ยงที่เกี่ยวข้องอย่างเหมาะสม เช่น ความเสี่ยงด้านการกำกับดูแลและบริหารจัดการที่ไม่เพียงพอ ด้านพฤติกรรมที่ไม่พึงประสงค์ ด้านภัยคุกคามทางไซเบอร์ ด้านความไม่เป็นธรรมและการเลือกปฏิบัติ ด้านความไม่โปร่งใส ด้านการละเมิดความเป็นส่วนตัวและความลับของข้อมูล และด้านการบริหารจัดการผู้ให้บริการภายนอกที่ไม่มีประสิทธิภาพ เป็นต้น

3.3 หลักการที่ควรคำนึงถึง

หลักการพื้นฐานที่ควรคำนึงถึงเพื่อให้การใช้งาน AI/ML บรรลุวัตถุประสงค์ที่กำหนดไว้ ได้แก่

(1) ความเป็นธรรม : ออกแบบและพัฒนา AI/ML โดยคำนึงถึงความเป็นธรรม ความเท่าเทียม และความหลากหลายทางสังคม เพื่อไม่ให้บุคคลหรือกลุ่มบุคคลบางส่วนได้รับการเลือกปฏิบัติ

(2) ความสอดคล้องกับกฎหมายและหลักจริยธรรม : ใช้งาน AI/ML อย่างสอดคล้องกับกฎหมายและหลักจริยธรรม โดยดำเนินการรวบรวมกฎหมายและหลักจริยธรรมที่เกี่ยวข้อง พิจารณาความเหมาะสมของการใช้งาน AI/ML และนำกฎหมายและหลักจริยธรรมไปเป็นพื้นฐานในการออกแบบ พัฒนา และใช้งาน AI/ML

(3) ความรับผิดชอบ : มีความรับผิดชอบต่อผลที่เกิดขึ้นจากการนำ AI/ML มาใช้งาน

(4) ความโปร่งใส : ใช้งาน AI/ML ด้วยความโปร่งใส โดยมีการให้ข้อมูลต่อผู้ใช้งานอย่างเพียงพอ และคำนึงถึงความสามารถของผู้ประกอบธุรกิจในการอธิบายขอบเขตและหลักการทำงานของ AI/ML พร้อมทั้งความสามารถในการตรวจสอบข้อมูลย้อนหลังสำหรับกิจกรรมที่เกิดขึ้น (Traceability)

3.4 วิธีปฏิบัติที่ดี

วิธีปฏิบัติในการใช้งาน AI/ML ให้มีประสิทธิภาพ ประกอบด้วย 4 ขั้นตอนหลัก ได้แก่

(1) การออกแบบระบบ โดยกำหนดวัตถุประสงค์ มาตรการควบคุมและแก้ไขความเสี่ยง หลักการใช้งาน และข้อกำหนดความต้องการในการพัฒนาระบบ

(2) การจัดเตรียมข้อมูลและพัฒนา AI/ML โดยจัดเตรียมข้อมูลให้มีคุณภาพ เหมาะสมกับวัตถุประสงค์ และสอดคล้องกับหลักการใช้งาน รวมถึงพัฒนาโมเดลด้วยอัลกอริทึมที่เหมาะสม

(3) การใช้งานและติดตามผล โดยทดสอบการทำงานในสภาพแวดล้อมเสมือนจริงก่อนนำ AI/ML ไปใช้งานจริง และติดตามทบทวนผลของการทำงานอย่างสม่ำเสมอ เพื่อให้ได้ผลที่มีประสิทธิภาพตามความคาดหวัง

(4) การสื่อสารกับผู้ใช้งาน โดยเปิดเผยข้อมูลที่เหมาะสม เพื่อให้ผู้ใช้งานเข้าใจการทำงานของ AI/ML และสามารถคาดการณ์ผลที่อาจเกิดขึ้น

3.5 ปัจจัยส่งเสริมให้บรรลุวัตถุประสงค์

การประยุกต์ใช้ AI/ML ให้บรรลุวัตถุประสงค์ที่กำหนดไว้ ต้องอาศัยปัจจัยหลายประการร่วมกัน โดยสิ่งสำคัญที่ช่วยให้บรรลุวัตถุประสงค์ได้ มีดังนี้

(1) การกำกับดูแล : ผู้ประกอบธุรกิจควรจัดให้มีกรอบการกำกับดูแล (Governance Framework) ที่ดี โดยมุ่งเน้นการมีส่วนร่วมของผู้บริหาร การกำหนดบทบาทหน้าที่ที่ชัดเจน รวมถึงมีการติดตามและประเมินผลการประยุกต์ใช้ AI/ML

(2) การบริหารจัดการความเสี่ยงขององค์กร : การจัดการความเสี่ยงด้าน AI/ML ที่ดีและสอดคล้องกับการบริหารจัดการความเสี่ยงขององค์กรจะช่วยเพิ่มโอกาสในการบรรลุ

วัตถุประสงค์ของการใช้งาน AI/ML ได้ โดยมีความเข้าใจความเสี่ยงที่เกี่ยวข้องกับ AI/ML กำหนดมาตรการควบคุมความเสี่ยง และติดตามความเสี่ยงอย่างเหมาะสม

(3) การรักษาความมั่นคงปลอดภัยและความเป็นส่วนตัว : ผู้ประกอบธุรกิจควรจัดให้มีนโยบายและมาตรการควบคุมที่เหมาะสมกับความเสี่ยง โดยคำนึงถึงองค์ประกอบหลักของการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ 3 ประการ ได้แก่ การรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพความพร้อมใช้งาน

(4) ทักษะของบุคลากร : ผู้ประกอบธุรกิจควรจัดให้มีบุคลากรที่รับผิดชอบในด้านการพัฒนา ทดสอบ นำไปใช้งาน และควบคุมดูแลการทำงานของ AI/ML ที่เพียงพอและเหมาะสมกับรูปแบบการใช้งาน AI/ML ขององค์กร

ทั้งนี้ รายละเอียดของ 5 ส่วนข้างต้น จะปรากฏในข้อ 4 – 8 ตามลำดับต่อไป

4. วัตถุประสงค์ของการใช้งาน

ปัจจุบัน AI/ML ได้รับการพัฒนาอย่างรวดเร็วและสามารถนำมาประยุกต์ใช้ได้หลากหลายรูปแบบในองค์กรต่าง ๆ เพื่อให้การใช้งาน AI/ML ประสบความสำเร็จ ผู้ประกอบธุรกิจจึงควรเริ่มจากการกำหนดวัตถุประสงค์ของการใช้งานที่ชัดเจนและเหมาะสม โดยคำนึงถึงโอกาสหรือประโยชน์ที่องค์กรจะได้รับ รวมถึงความเป็นไปได้ของการใช้งาน ซึ่งสามารถพิจารณาได้จากปัจจัยต่าง ๆ เช่น ต้นทุนในการลงทุนและดำเนินงาน ความสามารถทางเทคโนโลยี ความพร้อมของข้อมูล ความพร้อมของบุคลากรและทรัพยากรที่เกี่ยวข้อง เป็นต้น

ในการกำหนดวัตถุประสงค์ของการใช้งาน AI/ML นั้น ผู้ประกอบธุรกิจควรคำนึงถึงวัตถุประสงค์ในด้านการสร้างประโยชน์ต่อผู้ใช้งานและสังคมโดยรวม โดยการใช้งาน AI/ML จะต้องมีคุณสมบัติที่สำคัญ 2 ประการ ได้แก่

- **มีประโยชน์ (Beneficence) :** AI/ML ต้องก่อให้เกิดประโยชน์ต่อผู้ใช้งานและสังคมโดยรวม เช่น ช่วยให้ผู้ใช้งานสามารถตัดสินใจได้อย่างถูกต้องแม่นยำมากขึ้น ช่วยให้เข้าใจพฤติกรรมของลูกค้าและตลาดได้ดียิ่งขึ้น หรือช่วยให้ลูกค้าได้รับผลตอบแทนหรือความสะดวกสบายมากขึ้น เป็นต้น
- **ไม่ประพฤติผิด (Non-Malfeasance)** : AI/ML ต้องไม่สร้างความเดือดร้อนหรือความเสียหายต่อผู้ใด เช่น ไม่ละเมิดความเป็นส่วนตัว ไม่เลือกปฏิบัติ ไม่สร้างอคติ ไม่ก่อให้เกิดความเสี่ยงด้านความปลอดภัย เป็นต้น

ทั้งนี้ ผู้ประกอบธุรกิจควรให้ความสำคัญกับการกำหนดวัตถุประสงค์ของการใช้งาน AI/ML อย่างชัดเจนและเหมาะสม เพื่อให้สามารถใช้ประโยชน์จากเทคโนโลยี AI/ML ได้อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดแก่องค์กรและสังคมโดยรวม

จากการศึกษาข้อมูลทั้งในและต่างประเทศเทศพบว่า ในปัจจุบันผู้ประกอบธุรกิจมีการใช้ AI/ML เพื่อวัตถุประสงค์ในการเพิ่มประสิทธิผลและประสิทธิภาพของงาน ดังนี้

4.1 การบริหารจัดการกองทุน/การจัดการพอร์ต

การแข่งขันของตลาดทุนที่เพิ่มสูงขึ้น ส่งผลให้ผู้ประกอบธุรกิจที่ในอดีตจะเน้นการวิเคราะห์การลงทุนด้วยปัจจัยพื้นฐาน มีการขยายขอบเขตไปสู่การวิเคราะห์เชิงปริมาณตัวเลข (Quantitative Approach) ที่เพิ่มมากขึ้น โดยนำข้อมูลจากแหล่งต่าง ๆ มาประมวลผลโดย AI/ML เพื่อเพิ่มโอกาสในการสร้างผลตอบแทนที่สูงขึ้นและสร้างผลิตภัณฑ์ที่ดึงดูดความสนใจจากลูกค้า

การใช้งาน AI/ML สำหรับการจัดการกองทุนหรือการจัดพอร์ตยังถือเป็นเรื่องใหม่ โดยเริ่มต้นจากการนำ AI/ML มาใช้วิเคราะห์ข้อมูลการลงทุนเพื่อสนับสนุนการตัดสินใจของผู้จัดการกองทุนในการบริหารจัดการพอร์ต (Portfolio Management) โดยพิจารณาปัจจัยต่าง ๆ เช่น สภาวะเศรษฐกิจ ประเภทสินทรัพย์ ความเสี่ยงและผลตอบแทน เพื่อเพิ่มโอกาสให้ผลตอบแทนสูงสุด นอกจากนี้ ผู้ประกอบธุรกิจบางรายได้เริ่มนำ AI/ML มาใช้เพิ่มประสิทธิภาพการเลือกเส้นทางสำหรับส่งคำสั่งซื้อขายหลักทรัพย์หรือสินทรัพย์ต่าง ๆ (Broker Selection/Order Routing)

4.2 การให้บริการคำปรึกษาด้านการลงทุน

ในปัจจุบัน การให้บริการคำปรึกษาด้านการลงทุนมีการพัฒนาไปอย่างก้าวหน้า โดยผู้ประกอบธุรกิจได้นำเทคโนโลยี AI/ML มาใช้เพื่อเพิ่มประสิทธิภาพและประสิทธิผลของการให้บริการ ดังนี้

- การใช้อัลกอริทึมที่มีการกำหนดเงื่อนไขการตัดสินใจชัดเจน (Rule-Based Algorithm) ยังคงเป็นที่นิยมในการให้บริการคำปรึกษาด้านการลงทุนแบบอัตโนมัติผ่านระบบ Robot-Advisor เนื่องจากมีความชัดเจนและเข้าใจง่าย อย่างไรก็ตาม เทคโนโลยีด้านการวิเคราะห์ข้อมูลที่มีความก้าวหน้ามากยิ่งขึ้น ทำให้ผู้ประกอบธุรกิจสามารถพัฒนาโมเดลการลงทุนโดยใช้ AI/ML ที่มีความแม่นยำและมีประสิทธิภาพมากยิ่งขึ้น
- การวิเคราะห์ข้อมูลเชิงลึกและทำนายหรือคาดการณ์แนวโน้มของตลาดทุน โดย AI/ML สามารถประมวลผลข้อมูลจากแหล่งต่าง ๆ เช่น ข่าวสารด้านการเงินและเศรษฐกิจ และนโยบายด้านการเงินของประเทศต่าง ๆ เป็นต้น ร่วมกับข้อมูลในอดีต (Historical Data) เพื่อสร้างโมเดลการลงทุนที่สามารถคาดการณ์แนวโน้มของตลาดทุนได้แม่นยำยิ่งขึ้น อย่างไรก็ตาม โมเดลการลงทุนที่แนะนำโดย AI/ML ยังคงถูกใช้งานอยู่ในขอบเขตจำกัด และส่วนมากต้องอาศัยการมีส่วนร่วมของมนุษย์ (Manual Intervention) ในการทบทวนผล (Review) ที่ได้รับจาก AI/ML ก่อนที่จะนำไปให้คำแนะนำกับลูกค้าหรือนำไปจัดพอร์ตการลงทุน

4.3 การบริหารความเสี่ยง

AI/ML ช่วยให้ผู้ประกอบธุรกิจสามารถบริหารความเสี่ยงเกี่ยวกับการประกอบธุรกิจ เช่น ติดตามความเสี่ยงของลูกค้า (Customer's Risk Profile) ติดตามความเสี่ยงในการผิดชำระหนี้ (Potential Defaults) และติดตามพฤติกรรมอันต้องสงสัยของลูกค้าและพนักงานในองค์กร เป็นต้น ซึ่ง AI/ML สามารถช่วยให้ผู้ประกอบธุรกิจได้รับสัญญาณเตือนล่วงหน้า (Early-Warning Indicator) ก่อนที่ความเสี่ยงนั้นจะส่งผลกระทบต่อองค์กร

4.4 การคัดเลือกอัลกอริทึมที่ใช้ซื้อขาย

AI/ML สามารถใช้ในการวิเคราะห์ประสิทธิภาพของอัลกอริทึมการซื้อขาย และให้คำแนะนำในการเลือกอัลกอริทึมที่สามารถสร้างโอกาสให้ผลตอบแทนดีที่สุดในแต่ละภาวะตลาด ช่วยให้ผู้ประกอบธุรกิจสามารถให้บริการที่มีประสิทธิภาพและตรงความต้องการของลูกค้ามากยิ่งขึ้น

4.5 การให้บริการกับลูกค้า

AI/ML ถูกนำมาใช้เพื่อยกระดับบริการและสร้างประสบการณ์ที่ดีให้กับลูกค้า เช่น การใช้งานระบบถามตอบอัตโนมัติ (Chatbot) ที่สามารถตอบคำถามของลูกค้าโดยใช้ภาษาที่ดูเป็นธรรมชาติคล้ายมนุษย์ และให้บริการได้ตลอด 24 ชั่วโมง ทำให้ผู้ประกอบธุรกิจสามารถลดต้นทุนในการดำเนินงานด้านศูนย์บริการลูกค้า (Call Center)

4.6 การปฏิบัติตามกฎระเบียบ

AI/ML มีบทบาทในการช่วยปรับปรุงประสิทธิผลและประสิทธิภาพของการปฏิบัติตามกฎระเบียบ โดยช่วยในการป้องกัน เฝ้าระวัง และตรวจจับการกระทำที่อาจนำไปสู่การละเมิดกฎระเบียบต่าง ๆ แบบอัตโนมัติ ตัวอย่างของการใช้งาน AI/ML ในด้านการปฏิบัติตามกฎระเบียบ มีดังนี้

- การเปิดบัญชีและทำความรู้จักลูกค้า (Client Onboarding) : AI/ML ช่วยสนับสนุนกระบวนการรับลูกค้าในหลายมิติ เช่น การตรวจสอบใบหน้าของลูกค้าเทียบกับภาพถ่ายในเอกสารแสดงตน การตรวจจับการมีชีวิต (Liveness Check) ในขั้นตอนการรับลูกค้าผ่านช่องทางอิเล็กทรอนิกส์ ตลอดจนการเฝ้าระวังและติดตามรายชื่อบุคคลต้องห้ามทำธุรกรรมหรือบุคคลที่มีความเสี่ยงสูงได้อย่างเป็นปัจจุบัน เป็นต้น
- การตรวจจับการฉ้อโกง (Fraud Detection) : AI/ML สามารถวิเคราะห์ข้อมูลจำนวนมากเพื่อระบุรูปแบบและความผิดปกติที่อาจบ่งบอกถึงกิจกรรมการฉ้อโกง เช่น กิจกรรมการซื้อขายที่อาจไม่เป็นธรรม หรือการซื้อขายโดยอาจใช้ข้อมูลวงใน เป็นต้น
- การรายงานข้อมูลตามกฎระเบียบ : AI/ML สามารถช่วยสร้างรายงานข้อมูลต่อหน่วยงานกำกับดูแลแบบอัตโนมัติอย่างถูกต้องและทันเวลา เช่น การรายงานธุรกรรมที่เข้าข่ายต้องรายงานหน่วยงานทางกฎหมาย เป็นต้น
- การติดตามสัดส่วนการลงทุนของกองทุน (Investment Limitation) : AI/ML สามารถช่วยตรวจสอบและควบคุมให้สัดส่วนการลงทุนของกองทุนเป็นไปตามหลักเกณฑ์ที่กำหนดได้อย่างถูกต้องและมีประสิทธิภาพ

4.7 การสร้างข้อมูลเนื้อหา

Generative AI ถูกนำมาใช้ในการเพิ่มประสิทธิภาพหรือลดระยะเวลาในการปฏิบัติงานของผู้ประกอบธุรกิจ โดยมีการประยุกต์ใช้หรือแฝงเข้ากับกิจกรรมต่าง ๆ ตามข้อ 4.1 ถึง 4.6 ตัวอย่างเช่น การใช้ Generative AI เพื่อสังเคราะห์ข้อมูลสรุปภาวะตลาดสำหรับให้บริการแก่ลูกค้า หรือการใช้ Generative ในการทำบทวิเคราะห์ บทวิจัย หรือรายงานต่าง ๆ สำหรับใช้งานภายในองค์กร เป็นต้น

5. ความเสี่ยงที่เกี่ยวข้อง

AI/ML เป็นเทคโนโลยีที่กำลังมีบทบาทสำคัญในภาคตลาดทุน เนื่องจากมีศักยภาพสูงในการวิเคราะห์ข้อมูลและช่วยในการตัดสินใจ ซึ่งสามารถช่วยลดค่าใช้จ่ายและต้นทุนในการดำเนินธุรกิจ พร้อมทั้งเพิ่มประสิทธิภาพในการทำงานให้ดียิ่งขึ้น อย่างไรก็ดี การใช้งาน AI/ML ในการดำเนินธุรกิจย่อมนำมาซึ่งความเสี่ยงใหม่ ๆ ที่หากไม่มีการบริหารจัดการอย่างเหมาะสม อาจนำมาซึ่งความเสียหายด้านการเงิน ภาพลักษณ์องค์กร และเกิดการละเมิดกฎระเบียบที่เกี่ยวข้องได้

ความเสี่ยงจากการประยุกต์ใช้ AI/ML มีความหลากหลายและแตกต่างกันไปตามบริบทของการประยุกต์ใช้ AI/ML โดยมีตัวอย่างที่สำคัญ ดังนี้

5.1 ความเสี่ยงด้านการกำกับดูแลและบริหารจัดการที่ไม่เพียงพอ

นโยบายและกรอบการบริหารจัดการความเสี่ยงที่มีอยู่เดิมอาจไม่เพียงพอที่จะรองรับความเสี่ยงใหม่ ๆ ที่เกี่ยวข้องกับการใช้งาน AI/ML โดยเฉพาะ ดังนั้น ผู้ประกอบธุรกิจจึงจำเป็นต้องปรับปรุงนโยบายหรือมาตรการควบคุมความเสี่ยงให้ครอบคลุมการใช้งาน AI/ML อย่างเหมาะสม เช่น การกำหนดนโยบายและขั้นตอนในการบริหารจัดการความเสี่ยงจากการทำงานผิดพลาดของ AI/ML ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Risks) ความเสี่ยงด้านความไม่เป็นธรรมและการเลือกปฏิบัติ และความเสี่ยงด้านความไม่โปร่งใส เป็นต้น

5.2 ความเสี่ยงด้านพฤติกรรมไม่พึงประสงค์

คุณภาพและปริมาณของข้อมูลที่ใช้ในกระบวนการเรียนรู้ของ AI/ML มีความสำคัญอย่างยิ่งต่อผลและประสิทธิภาพของ AI/ML หากข้อมูลที่นำมาใช้งานมีคุณภาพและปริมาณที่ไม่เพียงพออาจทำให้ AI/ML ไม่สามารถให้ผลที่ถูกต้องและแม่นยำ หรือส่งผลให้ AI/ML มีพฤติกรรมที่ไม่พึงประสงค์หรือแสดงผลที่ไม่คาดคิด ตัวอย่างเช่น Chatbot ตอบสนองต่อคำถามของลูกค้า ด้วยข้อมูลที่ไม่ถูกต้อง ไม่เหมาะสม หรือมีอคติ ซึ่งอาจทำให้เกิดผลกระทบต่อลูกค้าและชื่อเสียงขององค์กรได้

5.3 ความเสี่ยงด้านภัยคุกคามทางไซเบอร์

การใช้เทคโนโลยีในการประกอบธุรกิจย่อมนำมาซึ่งความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้น ผู้ไม่ประสงค์ดีสามารถโจมตี AI/ML ได้ผ่านช่องโหว่ของระบบ หรือโจมตีข้อมูลซึ่งถูกใช้ในการสอน AI/ML เพื่อทำให้ AI/ML ทำงานผิดพลาด หยุดทำงาน หรือเกิดการรั่วไหลของข้อมูล ตัวอย่างเช่น Poisoning Attack ซึ่งเป็นการโจมตีโดยทำให้ข้อมูลที่ใช้สอนโมเดลปนเปื้อนด้วยข้อมูลที่ทำให้เกิดช่องโหว่เพื่อให้ผู้ไม่ประสงค์ดีสามารถบรรลุเป้าหมายที่ต้องการ และ Evasion Attack ซึ่งเป็นการโจมตีโมเดลโดยส่งข้อมูลที่ทำให้โมเดลประมวลผลแล้วทำงานผิดพลาดหรือหยุดทำงาน เป็นต้น

5.4 ความเสี่ยงด้านความไม่เป็นธรรมและการเลือกปฏิบัติ

การทำงานของ AI/ML อาจนำไปสู่ความไม่เป็นธรรมและการเลือกปฏิบัติ ซึ่งเกิดจากอคติที่มาจากการออกแบบและสร้างโมเดล (Bias Introduced by Engineering Decisions) หรือเกิดจากอคติที่มาจากข้อมูล (Data Bias) เช่น ข้อมูลที่ใช้ในการสอนโมเดล (Training Dataset) ไม่มีคุณภาพ ความหลากหลาย หรือปริมาณที่เพียงพอ เป็นต้น

5.5 ความเสี่ยงด้านความไม่โปร่งใส

ความโปร่งใสเป็นหนึ่งในปัจจัยสำคัญที่ช่วยให้ AI/ML มีความน่าเชื่อถือต่อผู้ใช้งาน อย่างไรก็ดี การทำความเข้าใจและอธิบายกระบวนการคิดคำนวณหรือการตัดสินใจของ AI/ML เป็นเรื่องที่ซับซ้อน ทำให้ในบางครั้ง ผู้พัฒนาระบบและผู้ใช้งานไม่สามารถทราบถึงวิธีการตัดสินใจหรือปัจจัยที่มีผลต่อการตัดสินใจของระบบ ส่งผลให้เกิดปัญหาด้านความเชื่อมั่นในการใช้งาน ซึ่งเป็นความท้าทายใหม่ที่เกิดขึ้นกับการใช้งาน AI/ML ดังนั้น เพื่อเพิ่มความโปร่งใสและความน่าเชื่อถือ กระบวนการพัฒนาและออกแบบระบบควรคำนึงถึงความสามารถในการอธิบายการทำงานของ AI/ML ต่อผู้ใช้งาน (Explainable AI/ML)[1] และการจัดเก็บหลักฐานเพื่อการตรวจสอบย้อนหลังได้ โดยเฉพาะกรณีที่ AI/ML ถูกใช้งานโดยไม่มีมนุษย์ควบคุมการตัดสินใจ นอกจากนี้ ควรมีการสื่อสารหรือแจ้งเตือนผู้ใช้งานเมื่อมีการใช้งาน AI/ML เพื่อช่วยให้ผู้ใช้งานตระหนักถึงความเสี่ยง และความน่าเชื่อถือของผลลัพธ์ เช่น สื่อสารให้ผู้ใช้งานทราบขณะสนทนากับระบบอัตโนมัติ เพื่อให้ผู้ใช้งานทราบถึงความเสี่ยงที่ได้รับคำตอบที่ไม่ตรงประเด็นหรือไม่ครบถ้วนสมบูรณ์ได้ เป็นต้น

5.6 ความเสี่ยงด้านการละเมิดความเป็นส่วนตัวและความลับของข้อมูล

การสอนโมเดลของ AI/ML หรือการใช้งาน AI/ML มีการประมวลผลข้อมูล Input จากผู้ใช้งาน ย่อมมีความเสี่ยงที่อาจเกิดขึ้นจากการละเมิดความเป็นส่วนตัวของลูกค้า (เจ้าของข้อมูล) และการเปิดเผยข้อมูลอันเป็นความลับขององค์กรโดยไม่พึงประสงค์ โดยเฉพาะในกรณีที่ผู้ประกอบธุรกิจไม่มีนโยบายหรือแนวปฏิบัติเกี่ยวกับการใช้งาน AI/ML และไม่มีการสร้างความตระหนักให้กับบุคลากรอย่างเพียงพอ อาจทำให้พนักงานมีการนำข้อมูลลับไปใช้งานกับ AI/ML ที่เปิดให้บริการกับสาธารณะ (เช่น ChatGPT) เพื่อสนับสนุนการทำงาน เช่น การนำข้อมูลลับเกี่ยวกับการประชุมภายในองค์กรส่งให้กับบริการ Generative AI สาธารณะเพื่อสร้างสรุปผลการประชุม เป็นต้น ซึ่งอาจก่อให้เกิดผลกระทบในด้านกฎหมายและสร้างความเสียหายทางธุรกิจ

5.7 ความเสี่ยงด้านการบริหารจัดการผู้ให้บริการภายนอกที่ไม่มีประสิทธิภาพ

การใช้งาน AI/ML ที่ต้องพึ่งพาผู้ให้บริการภายนอก (Third-Party Providers) เช่น ผู้พัฒนาโมเดลหรือผู้ให้บริการ AI/ML สำเร็จรูปหรือพร้อมใช้งาน เป็นต้น อาจส่งผลให้ความเสี่ยงโดยรวมของผู้ประกอบธุรกิจสูงขึ้น โดยเฉพาะกรณีที่ไม่มีการบริหารจัดการผู้ให้บริการภายนอกอย่างมีประสิทธิภาพ ตั้งแต่กระบวนการตรวจสอบคุณสมบัติผู้ให้บริการ การจัดทำข้อตกลงหรือสัญญา และการติดตามผลการดำเนินงานของผู้ให้บริการ

[1] หากผู้ประกอบธุรกิจมีการใช้งาน AI/ML ที่ไม่สามารถอธิบายการทำงานหรือการตัดสินใจของ AI/ML ได้ ผู้ประกอบธุรกิจควรคำนึงถึงแนวทางการจัดการปัญหา ข้อร้องเรียน หรือข้อพิพาทจากลูกค้า โดยคำนึงถึงผลประโยชน์ของลูกค้าเป็นสำคัญ

6. หลักการที่ควรคำนึงถึง

6.1 ความเป็นธรรม

AI/ML ควรถูกออกแบบและพัฒนาโดยคำนึงถึงความเป็นธรรม ความเท่าเทียม และความหลากหลายทางสังคม เพื่อไม่ให้บุคคลหรือกลุ่มบุคคลบางส่วนได้รับการเลือกปฏิบัติอย่างไม่สมเหตุสมผล รวมถึงให้โอกาสประชาชนทุกคน รวมถึงกลุ่มคนด้อยโอกาสและผู้ทุพพลภาพได้รับประโยชน์จาก AI/ML ได้อย่างทั่วถึงและเท่าเทียม

AI/ML อาจก่อให้เกิดผลที่ไม่เป็นธรรมได้จากสาเหตุหลัก 2 สาเหตุ ได้แก่

(1) อคติที่มาจากข้อมูล (Data Bias) เนื่องจากข้อมูลที่ใช้ในการสอนโมเดลเอนเอียง ไม่ครอบคลุมทุกกลุ่มประชากร หรือมีขนาดกลุ่มตัวอย่างที่ไม่เหมาะสม ทำให้เกิดการเลือกปฏิบัติ ตัวอย่างเช่น AI คัดเลือกผู้สมัครงานเพศชายมากกว่าเพศหญิง อันมีสาเหตุจากข้อมูลส่วนใหญ่ที่ใช้สอนโมเดลนั้นเป็นข้อมูลของเพศชาย จึงทำให้ AI ให้น้ำหนักในการเลือกผู้สมัครงานเพศชายมากกว่าผู้สมัครงานเพศหญิง เป็นต้น

(2) อคติที่มาจากการออกแบบและสร้างโมเดล (Bias Introduced by Engineering Decisions) ซึ่งอาจเกิดได้จากความผิดพลาดในการตัดสินใจของบุคคลที่เกี่ยวข้องในการออกแบบและสร้างโมเดล ทั้งโดยเจตนาและไม่เจตนา รวมถึงกระบวนการออกแบบและสร้างโมเดลที่ไม่มีมาตรการควบคุมที่เพียงพอ

การป้องกันเกิดอคติที่มาจากข้อมูล (Data Bias) สามารถทำได้โดยการเลือกข้อมูลที่ใช้ในกระบวนการสอนโมเดลด้วยความระมัดระวังและคำนึงถึงมาตรการ ดังนี้

- เลือกใช้แหล่งข้อมูลที่มีความน่าเชื่อถือและมีการเก็บรวบรวมอย่างถูกต้อง
- เลือกใช้ข้อมูลที่มีความหลากหลาย และครอบคลุมทุกกลุ่มประชากร
- เลือกใช้ข้อมูลที่มีขนาดของกลุ่มตัวอย่างที่สามารถสะท้อนหรือเป็นตัวแทนของประชากรได้อย่างสมเหตุสมผล
- มีความระมัดระวังในการใช้ข้อมูลที่มีความอ่อนไหว (Sensitive Data) หรือข้อมูลที่มีความเฉพาะของกลุ่มประชากรใดกลุ่มหนึ่ง เช่น เพศสภาพ เชื้อชาติ ศาสนา และความเห็นทางการเมือง เป็นต้น
- กำหนดชุดข้อมูลสำหรับการทดสอบแต่ละชุดให้มีความแตกต่างกันของกลุ่มประชากร เพื่อตรวจสอบว่า AI ยังคงตัดสินใจได้อย่างถูกต้อง ไม่เอนเอียงไปตามกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง
- ทดสอบโมเดลโดยการสุ่มข้อมูลที่คาดว่าจะส่งผลให้เกิดอคติเพื่อค้นหาความผิดพลาด และดำเนินการปรับปรุงแก้ไขต่อไป

สำหรับอคติที่มาจากการออกแบบและสร้างโมเดล (Bias Introduced by Engineering Decisions) สามารถป้องกันได้โดยกำหนดให้บุคลากรที่มีส่วนร่วมในกระบวนการสร้างโมเดลมีความหลากหลาย และมีกระบวนการสอบทาน (Review) และทดสอบ (Test) ในขั้นตอนการสร้างโมเดลที่ดี

รวมถึง (ในกรณีที่จำเป็น) จัดให้มีผู้เชี่ยวชาญด้านการประยุกต์ใช้ AI/ML ให้คำปรึกษา เพื่อให้สามารถมองเห็นความเสี่ยงที่อคติอาจเกิดขึ้นและกำหนดแนวทางการลดความเสี่ยงดังกล่าว

ทั้งนี้ หากผู้ประกอบธุรกิจมีการปฏิบัติต่อลูกค้าที่แตกต่างกันบนพื้นฐานของความสมเหตุสมผลและสามารถอธิบายเหตุผลได้ การกระทำดังกล่าวอาจถือว่ายังอยู่บนหลักของความเป็นธรรม โดยมีตัวอย่างเช่น การพิจารณาวงเงินกู้ยืมเพื่อการซื้อขายหลักทรัพย์ (Credit Limit) โดย AI/ML จะประมวลผลข้อมูลและความเสี่ยงจากปัจจัยต่าง ๆ ของลูกค้า (เช่น ฐานเงินเดือน และระยะเวลาการทำงาน) ซึ่งอาจทำให้ลูกค้าแต่ละรายได้รับวงเงินที่ไม่เท่ากัน หรือการแนะนำผลิตภัณฑ์ด้านการลงทุนโดย AI/ML อาจวิเคราะห์อายุและข้อมูลฐานะทางการเงินของลูกค้า เพื่อคัดเลือกผลิตภัณฑ์ที่เหมาะสม เป็นต้น

6.2 ความสอดคล้องกับกฎหมายและหลักจริยธรรม

การใช้ AI/ML ได้อย่างเหมาะสมและมีประสิทธิภาพนั้น จำเป็นต้องมีความสอดคล้องกับกฎหมายและหลักจริยธรรมที่เกี่ยวข้อง โดยผู้ประกอบธุรกิจควรดำเนินการ ดังนี้

(1) รวบรวมกฎหมายและหลักจริยธรรม ซึ่งรวมถึงหลักปฏิบัติ ค่านิยม พันธกิจ และนโยบายขององค์กรที่เกี่ยวข้องกับการใช้งาน AI/ML

(2) พิจารณาความเหมาะสมของการใช้งาน AI/ML โดยคำนึงถึงความสอดคล้องกับกฎหมายและหลักจริยธรรมตามข้อ (1)

(3) ใช้กฎหมายและหลักจริยธรรมตามข้อ (1) เป็นพื้นฐานในการออกแบบ พัฒนา และใช้งาน AI/ML ขององค์กร

ตัวอย่างของการนำหลักการด้านความสอดคล้องกับกฎหมายและหลักจริยธรรม ได้แก่

(1) การใช้งาน AI/ML ในการจัดการพอร์ตการลงทุนแบบอัตโนมัติ จะต้องเปิดเผยข้อมูลความเสี่ยงต่อลูกค้าด้วยข้อมูลที่ถูกต้องและไม่เสนอเกินความเป็นจริง สอดคล้องกับการปฏิบัติตามกฎระเบียบและนโยบายขององค์กร

(2) การใช้งาน AI/ML เพื่อสนับสนุนการคัดเลือกผู้สมัครงานที่มีศักยภาพ จะต้องไม่นำข้อมูลเพศสภาพมาเป็นปัจจัยในการตัดสินใจเลือกผู้สมัคร สอดคล้องกับหลักปฏิบัติขององค์กร (Code of Conduct) ที่ให้โอกาสการเข้าทำงานกับทุกเพศสภาพอย่างเท่าเทียมกัน

6.3 ความรับผิดชอบ

หลักการในด้านความรับผิดชอบนี้มุ่งที่การกำหนดความรับผิดชอบ (Accountability) และความเป็นเจ้าของ (Ownership) สำหรับกิจกรรมที่มีการใช้งาน AI/ML อย่างชัดเจน เพื่อให้การนำ AI/ML มาใช้งานเป็นไปอย่างมีประสิทธิผล

หลักการในด้านความรับผิดชอบแบ่งออกเป็น 2 ด้านที่สำคัญ ดังนี้

6.3.1 ความรับผิดชอบภายในองค์กร (Internal Accountability)

ผู้ประกอบธุรกิจที่มีการนำเทคโนโลยี AI/ML มาใช้งานควรขยายขอบเขตหน้าที่และความรับผิดชอบของผู้บริหารระดับสูง (Senior Management) ให้ครอบคลุม ดังนี้

(1) อนุมัตินโยบายการใช้งาน AI/ML

(2) อนุมัติรูปแบบของการประยุกต์ใช้ AI/ML รวมถึงโมเดลที่จะใช้งาน

(3) ติดตามผลของ AI/ML

(4) ติดตามความเสี่ยงที่อาจเกิดขึ้นจาก AI/ML

การมอบหมายอำนาจหน้าที่ในการตัดสินใจเกี่ยวกับ AI/ML ควรคำนึงถึงระดับของผลกระทบที่เกิดจากการตัดสินใจและความสอดคล้องกับกรอบการกำกับดูแลของผู้ประกอบธุรกิจ (Internal Governance Framework) ตัวอย่างเช่น ผู้ประกอบธุรกิจที่กำหนดให้ Chief Financial Officer (CFO) เป็นผู้มีอำนาจในการอนุมัติเรื่องการซื้อขายหน่วยลงทุน เมื่อผู้ประกอบธุรกิจนำ AI/ML มาใช้ส่งคำสั่งซื้อขายหน่วยลงทุนแบบอัตโนมัติ ผู้ประกอบธุรกิจควรกำหนดให้ CFO หรือผู้บริหารระดับสูงกว่า มีส่วนร่วมในการอนุมัติโมเดลของ AI/ML และข้อมูลที่ใช้งานโดย AI/ML เพื่อให้สอดคล้องกับกรอบการกำกับดูแลขององค์กร อย่างไรก็ดี หาก CFO มีความรู้ความเชี่ยวชาญ และประสบการณ์ด้าน AI/ML ที่ยังไม่เพียงพอ ผู้ประกอบธุรกิจสามารถแต่งตั้งที่ปรึกษาด้านการประยุกต์ใช้ AI/ML หรือแต่งตั้งคณะกรรมการที่มี CFO เป็นองค์ประกอบเพื่อรับผิดชอบในเรื่องดังกล่าวตามความเหมาะสม เป็นต้น

6.3.2 ความรับผิดชอบภายนอกองค์กร (External Accountability)

ผู้ประกอบธุรกิจควรกำหนดช่องทางการติดต่อเพื่อให้ผู้ใช้งาน ลูกค้า เจ้าของข้อมูลส่วนบุคคล หรือผู้ที่อาจได้รับผลกระทบจากการทำงานของ AI/ML สามารถติดต่อสอบถามข้อมูล ร้องเรียน และแจ้งประเด็นปัญหาหรือความผิดพลาดเกี่ยวกับการใช้งาน AI/ML ได้อย่างสะดวก ซึ่งจะช่วยให้ผู้ประกอบธุรกิจรับทราบประเด็นปัญหาและความผิดพลาดที่เกิดขึ้น และดำเนินการแก้ไขได้อย่างทันท่วงที

นอกจากนี้ คำถาม ข้อร้องเรียน ประเด็นปัญหา และความผิดพลาดต่าง ๆ ที่ได้รับแจ้งควรถูกรวบรวมและใช้ประโยชน์สำหรับ (1) การตรวจสอบและทบทวนการทำงานของ AI/ML (2) การปรับปรุงโมเดลและวิธีการใช้งานข้อลูกค้า (User Experience/User Interface) และ (3) การวางแผนป้องกันปัญหาที่อาจเกิดขึ้นในอนาคต

6.4 ความโปร่งใส

ความโปร่งใสเป็นหลักการที่สำคัญประการหนึ่งที่ผู้ประกอบธุรกิจควรคำนึงถึงในการใช้งาน AI/ML เนื่องจาก AI/ML เป็นเทคโนโลยีที่ซับซ้อนและยากในการเข้าใจกลไกการทำงาน แม้ว่าจะมีพัฒนาการด้านความแม่นยำที่เพิ่มมากขึ้นกว่าในอดีต แต่ข้อผิดพลาดจากการทำงานของ AI/ML ยังคงมีโอกาสเกิดขึ้นได้ในระดับที่มากน้อยแตกต่างกันไปตามโมเดลและข้อมูลที่ใช้งาน ดังนั้น การใช้งาน AI/ML จึงควรคำนึงถึงเรื่องความโปร่งใส โดยสามารถอธิบายได้ว่า AI/ML ถูกนำมาใช้ในกระบวนการ (Process) ใด และหลักการทำงานหรือการตัดสินใจของ AI/ML เป็นอย่างไร (Explainability) นอกจากนี้ ความโปร่งใสยังแสดงให้เห็นได้จากความสามารถในการตรวจสอบข้อมูลย้อนหลังสำหรับกิจกรรมที่เกิดขึ้น (Traceability) ว่าเป็นไปตามหลักการหรือความตั้งใจที่แจ้งไว้ต่อลูกค้าหรือไม่

ระดับของความโปร่งใสที่เหมาะสมในการเปิดเผยข้อมูลเกี่ยวกับการใช้งาน AI/ML นั้น ขึ้นอยู่กับบริบทและลักษณะของการใช้งาน AI/ML ผู้ประกอบธุรกิจควรพิจารณาการเปิดเผยข้อมูลดังต่อไปนี้ต่อลูกค้าอย่างเพียงพอและเหมาะสมกับความเสี่ยงของกิจกรรมที่มีการใช้งาน AI/ML

(1) ขอบเขตและข้อจำกัดของการใช้งาน

(2) ข้อมูลเบื้องต้นเกี่ยวกับการทำงานหรือความสามารถของ AI/ML ที่ผู้ใช้งานทั่วไปสามารถเข้าใจได้

(3) ชุดข้อมูลที่ใช้ในการทดสอบโมเดลและผลการทดสอบ (เช่น ผลิตภัณฑ์ที่ถูกใช้ในการทดสอบ ช่วงเวลาของข้อมูลที่ใช้ในการทดสอบ เงื่อนไขและวิธีการส่งคำสั่งการคำนวณค่าธรรมเนียมและภาษีในการทดสอบ และผลตอบแทนที่ได้รับ เป็นต้น)

(4) ข้อจำกัดหรือปัจจัยที่มีโอกาสทำให้ AI/ML ไม่สามารถให้ผลตามผลการทดสอบ

(5) ข้อตกลงเกี่ยวกับการใช้บริการ (Terms and Conditions) รวมถึงขอบเขตความรับผิดชอบของผู้ประกอบธุรกิจและลูกค้า

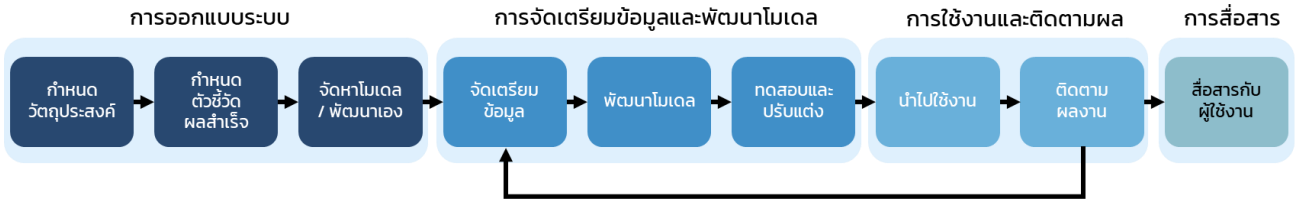
(6) การแก้ไขเปลี่ยนแปลงเกี่ยวกับ AI/ML และโมเดลที่มีนัยสำคัญ

นอกจากนี้ ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลที่เกี่ยวข้องกับกระบวนการสร้างและทดสอบโมเดล[2] หรือบันทึกเหตุการณ์ (Log) อย่างเพียงพอและเหมาะสมกับความเสี่ยงของการใช้งาน AI/ML เพื่อรองรับการตรวจสอบในภายหลังเมื่อพบประเด็นปัญหา หรือเมื่อได้รับการร้องขอจากลูกค้าหรือผู้ตรวจสอบ (Auditor) ตามความสมเหตุสมผล

[2] ตัวอย่างข้อมูลที่ควรจัดเก็บเช่น แหล่งที่มาของข้อมูล (Data Provenance) การประมวลผลหรือเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นกับข้อมูลในกระบวนการจัดเตรียมข้อมูล (Data Lineage) การออกแบบและการทำงานของอัลกอริทึม และชุดข้อมูลพร้อมกับผลลัพธ์ในกระบวนการสอน (Training) และทดสอบโมเดล (Test) เป็นต้น

7. วิธีปฏิบัติที่ดี

การใช้งาน AI/ML ให้สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ ต้องอาศัยวิธีปฏิบัติที่ดีในแต่ละขั้นตอนของการใช้งาน ดังนี้



ภาพประกอบ : วิธีปฏิบัติที่ดีในการใช้งาน AI/ML

7.1 การออกแบบระบบ

การออกแบบระบบที่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ ต้องผ่านการวิเคราะห์และนำวัตถุประสงค์ (ตามข้อ 4) มาตรการควบคุมและแก้ไขความเสี่ยงที่เกี่ยวข้อง (ตามข้อ 5) และหลักการใช้งาน (ตามข้อ 6) มาเปลี่ยนเป็นข้อกำหนดความต้องการในการพัฒนาระบบ (System Requirements) พร้อมทั้งเลือกใช้เครื่องมือหรือผลิตภัณฑ์ที่สามารถตอบสนองความต้องการดังกล่าวได้

เนื่องจากบริบทในการใช้งาน AI/ML และความพร้อมด้านบุคลากรที่แตกต่างกันในแต่ละองค์กร การเลือกใช้เครื่องมือหรือผลิตภัณฑ์จึงมีความแตกต่างกัน บางองค์กรอาจเลือกใช้ผลิตภัณฑ์ AI/ML ที่พร้อมใช้งาน (Off-the-shelf Products) หรือว่าจ้างหน่วยงานภายนอกมาดำเนินการทั้งหมด แต่ในขณะที่บางองค์กรมีความพร้อมและความเชี่ยวชาญในการสร้างโมเดลด้วยบุคลากรของตนเอง สิ่งสำคัญที่ผู้ประกอบธุรกิจทุกรายควรคำนึงถึงคือ ความรับผิดชอบต่อผลของ AI/ML จะยังคงอยู่ที่ผู้ประกอบธุรกิจโดยตรง ไม่ว่า AI/ML หรือโมเดลที่นำมาใช้งานอยู่ในรูปแบบใด ดังนั้น ผู้ประกอบธุรกิจควรมีการตรวจสอบให้มั่นใจได้ว่าโมเดลที่ใช้มีกระบวนการพัฒนาที่ดี สามารถทำงานได้อย่างมีประสิทธิภาพ และสามารถบรรลุวัตถุประสงค์ตามที่กำหนด

กรณีที่ผู้ประกอบธุรกิจใช้งาน AI/ML จากผู้ขายผลิตภัณฑ์ หรือมีการใช้บริการผู้ให้บริการภายนอก ผู้ประกอบธุรกิจควรมีความรู้และความเข้าใจถึงวิธีการทำงานของ AI/ML ดังกล่าวอย่างเพียงพอ ตลอดจนมีการกำกับดูแลความเสี่ยงที่อาจเกิดขึ้นจากบุคคลภายนอก (Third-party Management) อย่างเหมาะสม โดยพิจารณาดำเนินการดังต่อไปนี้ในระดับที่เหมาะสมกับบริบทของการใช้งาน AI/ML

(1) ตรวจสอบข้อมูลเกี่ยวกับผู้ขายผลิตภัณฑ์หรือผู้ให้บริการภายนอก (Due Diligence) ก่อนเริ่มใช้งาน และระหว่างใช้งานอย่างสม่ำเสมอ

(2) คัดเลือก AI/ML ที่จะนำมาใช้งานอย่างรัดกุม โดยทดสอบการทำงานของโมเดลอย่างเพียงพอเพื่อให้มั่นใจว่า ผลของ AI/ML มีความน่าเชื่อถือและมีประสิทธิภาพ

(3) ทำความเข้าใจเกี่ยวกับโมเดลที่นำมาใช้งาน เพื่อให้สามารถอธิบายการทำงานของโมเดลต่อลูกค้าได้ด้วยตนเอง โดยเฉพาะกรณีที่ AI/ML ถูกนำมาใช้งานแบบอัตโนมัติ และไม่มีเจ้าหน้าที่เข้ามามีส่วนร่วมในการตัดสินใจ (Human-out-of-the-Loop)

(4) จัดทำสัญญาการใช้งานที่ระบุขอบเขตของงาน ความรับผิดชอบ ข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) และตัวบ่งชี้ประสิทธิภาพการทำงาน (Key Performance Indicator) อย่างชัดเจน ทั้งนี้ รายละเอียดที่กำหนดในสัญญาควรเหมาะสมกับบริบทของการใช้งาน AI/ML

(5) จัดให้มีกระบวนการติดตามประสิทธิภาพการทำงานของ AI/ML และมีการปรับปรุงเปลี่ยนแปลงอย่างเหมาะสมเพื่อให้มั่นใจได้ว่าผลจากการใช้งานเป็นไปตามที่คาดหวัง

7.2 การจัดเตรียมข้อมูลและพัฒนาโมเดล

7.2.1 การจัดเตรียมข้อมูล

เนื่องจาก AI/ML จำเป็นต้องใช้ข้อมูลในการเรียนรู้และประมวลผลในการทำงาน ดังนั้น ผู้ประกอบธุรกิจจึงควรมีการจัดเตรียมข้อมูลที่ดี ซึ่งประกอบด้วยขั้นตอนพื้นฐานดังนี้

(1) การกำหนดคุณสมบัติและคุณภาพของข้อมูล : ผู้ประกอบธุรกิจควรกำหนดคุณสมบัติและคุณภาพของข้อมูลที่เหมาะสม เพื่อให้ AI/ML สามารถทำงานได้อย่างมีประสิทธิภาพตามเป้าหมายที่กำหนด โดยอาจพิจารณาจากประเภทของข้อมูลที่จำเป็น ขนาดของข้อมูล ความถูกต้องของข้อมูล และข้อมูลที่มีการจัดเก็บภายในช่วงเวลาที่ต้องการ (Time Series Data) เป็นต้น

(2) การรวบรวมและเชื่อมโยงข้อมูล : ผู้ประกอบธุรกิจควรรวบรวมและทำการเชื่อมโยงข้อมูลจากแหล่งต่าง ๆ (Data Integration) เพื่อให้ได้ข้อมูลครบถ้วนและครอบคลุมตามที่ต้องการ โดยภายหลังจากทำการเชื่อมโยงและรวบรวมข้อมูลเรียบร้อยแล้ว ควรมีการจัดเตรียมเอกสารเพื่อแสดงแหล่งที่มาของข้อมูล (Data Provenance) รวมถึงรายละเอียดการประมวลผลหรือการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นกับข้อมูลตลอดกระบวนการจัดเตรียมข้อมูล (Data Lineage) เพื่อประโยชน์ในการตรวจสอบย้อนกัน (Traceability) ในกรณีที่ AI/MLทำงานผิดพลาด

(3) การระบุประเภทของข้อมูล: การจัดเตรียมข้อมูลสำหรับการสอน ตรวจสอบ และทดสอบโมเดล ควรมีการระบุประเภทของข้อมูล (Data Labelling) อย่างถูกต้อง เพื่อให้ AI/ML มีข้อมูลและสามารถรับรู้ความหมายของข้อมูลได้อย่างถูกต้อง

(4) การประเมินคุณภาพของข้อมูล : ก่อนที่จะนำชุดข้อมูล (Dataset) ไปใช้สำหรับการสอน ตรวจสอบ และทดสอบโมเดลควรมีการประเมินคุณภาพของข้อมูล (Data Evaluation) และปรับปรุงข้อมูลให้มีคุณภาพตามหลักเกณฑ์ที่องค์กรกำหนด

(5) การคุ้มครองข้อมูลส่วนบุคคล : ในกรณีที่มีการใช้ข้อมูลส่วนบุคคลหรือข้อมูลที่อ่อนไหว (Sensitive Data) ผู้ประกอบธุรกิจควรมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม เพื่อลดความเสี่ยงในการรั่วไหลของข้อมูลส่วนบุคคล เช่น Access Control, Encryption, และ Anonymization เพื่อป้องกันการรั่วไหลข้อมูล

7.2.2 การพัฒนาโมเดล

กระบวนการพัฒนาโมเดลสำหรับ AI/ML ประกอบด้วยขั้นตอนพื้นฐาน 4 ขั้นตอน ได้แก่

(1) การเตรียมอัลกอริทึมสำหรับสร้างโมเดล

(2) การสอนโมเดลด้วยชุดข้อมูล (Training Dataset) ที่เตรียมไว้

(3) การตรวจสอบประสิทธิภาพของโมเดลด้วยชุดข้อมูลสำหรับตรวจสอบ (Validation Dataset) ซึ่งในขั้นตอนนี้โมเดลอาจถูกปรับแต่ง (Tuning) จนกว่าจะให้ผลที่มีประสิทธิภาพตามเป้าหมายที่ต้องการ และ

(4) การทดสอบโมเดลในขั้นตอนสุดท้ายก่อนการนำไปใช้งานจริง ด้วยชุดข้อมูลสำหรับทดสอบ (Testing Dataset) ซึ่งเป็นชุดข้อมูลที่ไม่ซ้ำกับ Training Dataset และ Validation Dataset

สำหรับ AI/ML ที่ถูกนำมาใช้งานในกระบวนการทางธุรกิจที่มีความเสี่ยงสูง ผู้ประกอบธุรกิจควรหลีกเลี่ยงการใช้งาน AI/ML หรือโมเดลที่มนุษย์ไม่สามารถควบคุมหรือระงับการทำงานใด ๆ ได้ (Human-out-of-the-Loop) และควรจัดให้ที่มีช่องทางให้มนุษย์เข้ามามีส่วนร่วมในการควบคุมการทำงานหรือการตัดสินใจของ AI/ML (Human-in-the-Loop หรือ Human-over-the-Loop[3]) หรือจัดให้มีกลไกฉุกเฉิน (Kill Switch) รองรับเหตุการณ์ผิดปกติ ซึ่งจะอนุญาตให้เจ้าหน้าที่ระงับการตัดสินใจหรือการทำงานของ AI/ML และแทรกแซงการดำเนินงานที่เกี่ยวข้องได้อย่างรวดเร็ว เพื่อจำกัดผลกระทบที่อาจเกิดขึ้นกับลูกค้าและสาธารณะ ทั้งนี้ Kill Switch ที่พัฒนาขึ้นต้องมีการกำหนดเงื่อนไขการใช้งาน (Activation) ที่ชัดเจน และได้รับการทดสอบอย่างเพียงพอก่อนนำไปใช้งานจริง

7.3 การใช้งานและติดตามผล

7.3.1 การใช้งาน

ก่อนการเริ่มนำ AI/ML ไปใช้งานจริง ผู้ประกอบธุรกิจควรทดสอบการทำงานของ AI/ML ในสภาพแวดล้อมเสมือนจริง (Pre-production Environment) เพื่อตรวจสอบความถูกต้องและประสิทธิภาพการทำงานของ AI/ML รวมถึงขีดความสามารถในการรองรับปริมาณการใช้งาน (Workload) และความสามารถในการตอบสนองภายในระยะเวลาที่ยอมรับได้ (Acceptable Latency Time)

เพื่อให้ AI/ML มีความพร้อมใช้งานหรือให้บริการได้อย่างต่อเนื่อง ผู้ประกอบธุรกิจควรจัดให้มีการบริหารจัดการความเปลี่ยนแปลง (Change Management) ที่ดี เพื่อช่วยลดผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง และเพื่อให้การเปลี่ยนแปลงที่เกิดขึ้นบรรลุเป้าหมายที่ตั้งไว้อย่างมีประสิทธิภาพ

---

[3] Human-in-the-Loop : เป็นการใช้งาน AI/ML ที่มนุษย์เข้ามามีส่วนร่วมในการควบคุมการทำงานหรือตัดสินใจทั้งหมด โดยมี AI/ML ทำหน้าที่ในการให้คำแนะนำหรือข้อมูล แต่ไม่สามารถทำงานหรือตัดสินใจในการดำเนินการใด ๆ ได้ โดยปราศจากมนุษย์
Human-over-the-Loop : เป็นการใช้งาน AI/ML ที่ AI/ML สามารถทำงานหรือตัดสินใจเองได้ แต่ยังต้องอาศัยมนุษย์ในการกำกับดูแล อีกทั้งมนุษย์สามารถเข้าควบคุมหรือระงับการทำงานเมื่อพบความผิดพลาดหรือมีเหตุจำเป็นได้

7.3.2 การติดตามผล

หลังจากนำ AI/ML ไปใช้งานจริง ผู้ประกอบธุรกิจควรมีการติดตามและประเมินประสิทธิภาพของ AI/ML ในด้านความสำเร็จตามวัตถุประสงค์ และประสิทธิภาพในการทำงานของ AI พร้อมทั้งปรับแต่งค่า (Model Tuning) เมื่อมีความจำเป็น เพื่อให้มั่นใจว่า AI/ML ยังสามารถทำงานได้อย่างถูกต้องและเป็นไปตามวัตถุประสงค์ที่กำหนดไว้ นอกจากนี้ ผู้ประกอบธุรกิจควรมีกระบวนการในการเฝ้าติดตามแหล่งข้อมูลหรือชุดข้อมูลใหม่ที่สามารถนำมาใช้ในการสอนโมเดลเพื่อปรับปรุงประสิทธิภาพของ AI/ML ให้ดีขึ้น

ในการติดตามการทำงานของ AI/ML ผู้ประกอบธุรกิจอาจใช้เครื่องมือที่ช่วยในการเฝ้าติดตามและรายงานผลโดยอัตโนมัติเพื่อกำหนดตัวชี้วัด (Specific Triggers) ที่บ่งชี้ความจำเป็นในการทบทวนและทดสอบโมเดลและข้อมูลที่ใช้งาน เช่น เครื่องมือติดตามและแจ้งเตือนเมื่อพอร์ตการลงทุนที่ใช้งาน AI/ML ให้ผลตอบแทนขาดทุนถึงระดับที่กำหนด หรือพอร์ตการลงทุนมีการเข้าซื้อหน่วยลงทุนใหม่ ๆ ที่ให้ผลตอบแทนที่ขาดทุนอย่างต่อเนื่อง (Low Accuracy Rate) ซึ่งต้องมีการตรวจหาความผิดปกติและปรับปรุงข้อบกพร่องต่อไป เป็นต้น

7.4 การสื่อสาร

การสื่อสารกับผู้ใช้งานด้วยข้อมูลที่เพียงพอ จะช่วยสร้างความเข้าใจและความมั่นใจต่อการใช้บริการของลูกค้า ในขณะเดียวกันการเปิดเผยข้อมูลในรายละเอียดที่มากเกินไป อาจส่งผลให้เกิดความสับสนหรือมีการอาศัยจุดอ่อนของ AI/ML เพื่อหาผลประโยชน์ส่วนตน ดังนั้น ผู้ประกอบธุรกิจควรพิจารณาอย่างรอบคอบในการเลือกข้อมูลที่จะเปิดเผยต่อสาธารณะ และใช้ภาษาที่สื่อสารให้ลูกค้าทั่วไปสามารถเข้าใจได้โดยง่าย โดยมีตัวอย่างดังนี้

(1) กรณีผู้ประกอบธุรกิจใช้งาน AI/ML เพื่อการให้บริการลูกค้าผ่านระบบรับส่งข้อความอิเล็กทรอนิกส์ (Electronic Messaging) เช่น อีเมล หรือ Chatbot ผู้ประกอบธุรกิจอาจเล็งเห็นถึงความเสี่ยงจากการที่ AI/ML ให้ข้อมูลที่ไม่ถูกต้องแม่นยำ ทำให้ลูกค้าเข้าใจผิดและสร้างความไม่พึงพอใจในการใช้บริการ ผู้ประกอบธุรกิจอาจเลือกที่จะแจ้งให้กับลูกค้าทราบในจุดเริ่มต้นการสนทนาว่า กำลังสนทนากับระบบอัตโนมัติ (AI/ML) เพื่อให้ลูกค้าสามารถคาดการณ์การกระทำต่าง ๆ ซึ่งผิดไปจากการสนทนากับมนุษย์ได้

(2) กรณีผู้ประกอบธุรกิจมีการใช้งาน AI/ML เพื่อตรวจจับพฤติกรรมการซื้อขายที่ไม่เป็นธรรม ผู้ประกอบธุรกิจอาจตัดสินใจที่จะไม่เปิดเผยข้อมูลเกี่ยวกับโมเดลและข้อมูลที่ใช้งาน เนื่องจากมีความเสี่ยงที่ผู้ไม่ประสงค์ดีจะอาศัยช่องโหว่เพื่อหลีกเลี่ยงการถูกตรวจจับ

นอกจากนี้ ในกรณีที่มีการใช้งาน AI/ML เพื่อให้คำแนะนำในการลงทุน การบริหารจัดการพอร์ตหรือกิจกรรมอื่นใดซึ่งมีความเสี่ยงที่อาจส่งผลกระทบด้านการเงินต่อลูกค้า ผู้ประกอบธุรกิจควรเปิดเผยข้อมูลเพื่อให้ผู้ลงทุนมีความเข้าใจ มีความระมัดระวังในการลงทุน และสามารถตัดสินใจบนข้อมูลที่เพียงพอ

8. ปัจจัยส่งเสริมให้บรรลุวัตถุประสงค์

การประยุกต์ใช้ AI/ML ให้บรรลุวัตถุประสงค์ที่กำหนดไว้ ต้องอาศัยวิธีปฏิบัติที่ดีในแต่ละขั้นตอนของการนำ AI/ML มาใช้งาน ดังนี้

8.1 การกำกับดูแล

การใช้งาน AI/ML อาจนำมาซึ่งความเสี่ยงใหม่ ๆ ซึ่งวิธีการกำกับดูแลและควบคุมความเสี่ยงที่มีอยู่เดิมอาจไม่เพียงพอ ผู้ประกอบธุรกิจจึงควรมีการประเมินความเสี่ยง[4] ของการใช้งาน AI/ML ภายใต้บริบท (Context) ขององค์กร และจัดให้มีกรอบการกำกับดูแลความเสี่ยงจากการใช้งาน AI/ML ที่ครอบคลุมเรื่อง[5] ดังนี้

(1) การกำหนดคณะกรรมการที่ทำหน้าที่กำหนดกลยุทธ์และนโยบายการใช้งาน AI/ML รวมถึงติดตามและประเมินผลการประยุกต์ใช้ AI/ML

(2) การกำหนดหน้าที่และความรับผิดชอบ (Role and Responsibility) ของบุคลากร และผู้มีส่วนได้เสียที่เกี่ยวข้อง (Stakeholders)

(3) การบริหารจัดการความเสี่ยงของการใช้งาน AI/ML ที่อยู่บนพื้นฐานของความรับผิดชอบต่อผู้ใช้งาน ลูกค้าและสังคมโดยรวม ซึ่งสอดคล้องกับการบริหารจัดการความเสี่ยงขององค์กร (Enterprise Risk Management)

ทั้งนี้ คณะกรรมการหรือที่ปรึกษาของคณะกรรมการของผู้ประกอบธุรกิจควรมีความรู้ความเชี่ยวชาญ หรือประสบการณ์ที่เกี่ยวข้องกับการประยุกต์ใช้ AI/ML อย่างเพียงพอ เพื่อให้สามารถเข้าใจความเสี่ยงของการใช้งาน AI/ML และสามารถกำกับดูแลความเสี่ยงได้อย่างมีประสิทธิผล

8.2 การบริหารจัดการความเสี่ยงขององค์กร

การบริหารจัดการความเสี่ยงขององค์กร (Enterprise Risk Management: ERM) เป็นกระบวนการที่ช่วยให้ผู้ประกอบธุรกิจระบุ ประเมิน และจัดการกับความเสี่ยงต่าง ๆ เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจที่ตั้งไว้ ERM สามารถช่วยเพิ่มโอกาสในการบรรลุวัตถุประสงค์ของการใช้งาน AI/ML ได้ ดังนี้

(1) สร้างความเข้าใจความเสี่ยงที่เกี่ยวข้องกับ AI/ML : ERM ช่วยให้ผู้ประกอบธุรกิจเข้าใจความเสี่ยงที่เกี่ยวข้องกับ AI/ML ได้อย่างครอบคลุม โดยพิจารณาปัจจัยต่าง ๆ เช่น ประเภทของความเสี่ยง ระดับความรุนแรงของความเสี่ยง และผลกระทบต่อองค์กร ความเข้าใจความเสี่ยงเหล่านี้จะช่วยให้องค์กรสามารถวางแผนและรับมือกับความเสี่ยงได้อย่างมีประสิทธิภาพ

(2) กำหนดมาตรการควบคุมความเสี่ยง : ERM ช่วยให้ผู้ประกอบธุรกิจกำหนดมาตรการควบคุมความเสี่ยงที่เหมาะสมกับความเสี่ยงที่ระบุไว้ มาตรการควบคุมความเสี่ยงเหล่านี้อาจรวมถึง

---

[4] ศึกษาเพิ่มเติมเกี่ยวกับการประเมินความเสี่ยงระบบปัญญาประดิษฐ์ได้จาก แนวปฏิบัติเกี่ยวกับมาตรฐานการใช้ปัญญาประดิษฐ์ version 1 จัดทำโดย ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย https://www.law.chula.ac.th/wp-content/uploads/2023/03/TAIG-20230222.pdf

[5] ศึกษาเพิ่มเติมเกี่ยวกับการกำหนดโครงสร้างหรือกรอบการกำกับดูแลความเสี่ยงจากการใช้งาน AI/ML ได้จากแนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาล สำหรับผู้บริหารองค์กร จัดทำโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ https://www.etda.or.th/getattachment/Our-Service/AIGC/AIGC/Ai_Gov_Guideline_edit.pdf.aspx?lang=th-TH

การพัฒนานโยบายและแนวปฏิบัติ การฝึกอบรมพนักงาน และการลงทุนในเทคโนโลยีความปลอดภัย

(3) ติดตามความเสี่ยง : ERM ช่วยให้ผู้ประกอบธุรกิจติดตามความเสี่ยงอย่างต่อเนื่อง เพื่อให้มั่นใจว่าความเสี่ยงเหล่านี้ยังคงอยู่ในระดับที่ยอมรับได้ การประเมินความเสี่ยงอย่างสม่ำเสมอจะช่วยให้องค์กรสามารถระบุความเสี่ยงใหม่ ๆ และปรับปรุงมาตรการควบคุมความเสี่ยงที่มีอยู่ได้อย่างมีประสิทธิภาพ

8.3 การรักษาความมั่นคงปลอดภัยและความเป็นส่วนตัว

การรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ และความเป็นส่วนตัวยังคงเป็นหัวใจสำคัญของการใช้งาน AI/ML เช่นเดียวกับการใช้งานเทคโนโลยีสารสนเทศอื่น ๆ โดยการออกแบบพัฒนา และใช้งาน AI/ML ควรคำนึงถึงความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ และความเป็นส่วนตัวเพื่อป้องกันการถูกโจมตีโดยผู้ไม่ประสงค์ดี และการใช้งาน AI/ML ที่ไม่เหมาะสม ซึ่งอาจส่งผลกระทบต่อลูกค้าและบุคคลที่เกี่ยวข้อง

ผู้ประกอบธุรกิจควรจัดให้มีนโยบายและมาตรการควบคุมที่เหมาะสมกับความเสี่ยง โดยคำนึงถึงองค์ประกอบหลักของการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ 3 ประการ ดังนี้

(1) การรักษาความลับ (Confidentiality) : รักษาความลับของข้อมูลในทุกขั้นตอนตั้งแต่การรวบรวมข้อมูล วิเคราะห์ข้อมูล และประมวลผลข้อมูล โดยให้สิทธิ์เข้าถึงข้อมูลเฉพาะแก่ผู้ที่มีสิทธิ์ และป้องกันการเข้าถึงข้อมูลโดยผู้ที่ไม่มีสิทธิ์หรือผู้ที่ไม่เกี่ยวข้อง

(2) การรักษาความถูกต้องครบถ้วน (Integrity) : มีมาตรการเพื่อป้องกันการแก้ไขหรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต เพื่อให้ข้อมูลมีความถูกต้องครบถ้วนและเชื่อถือได้อยู่เสมอ

(3) การรักษาสภาพความพร้อมใช้งาน (Availability) : บริการของ AI/ML ต้องสามารถเข้าถึงหรือใช้งานได้ เมื่อมีความจำเป็นต้องใช้ พร้อมทั้งสามารถใช้งานได้อย่างต่อเนื่อง (Continuity) โดยเฉพาะ AI/ML ที่ถูกใช้งานกับกระบวนการทางธุรกิจซึ่งมีความสำคัญสูง

หาก AI/ML มีการใช้งานข้อมูลส่วนบุคคลในการประมวลผล ผู้ประกอบธุรกิจควรมีการเก็บรักษาข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัย และจัดให้มีมาตรการรักษาข้อมูลส่วนบุคคลที่เหมาะสม เช่น มีการเข้ารหัสลับข้อมูล (Encryption) และมีการทำข้อมูลส่วนบุคคลให้เป็นข้อมูลนิรนาม (Data Anonymization) เป็นต้น เพื่อลดความเสี่ยงจากกรณีข้อมูลรั่วไหล

ทั้งนี้ เพื่อให้มั่นใจว่าการใช้งาน AI/ML เป็นไปตามนโยบายด้าน IT Security ขององค์กร ผู้ประกอบธุรกิจควรจัดให้มีการสอบตรวจสอบด้าน IT (IT Audit) ที่ครอบคลุมระบบ AI/ML โดยมีการปรับปรุงข้อตรวจพบต่าง ๆ ภายในระยะเวลาที่เหมาะสมกับความเสี่ยง

8.4 ทักษะของบุคลากร

การนำเทคโนโลยีมาใช้ในการประกอบธุรกิจ รวมถึงการใช้งาน AI/ML ที่ไม่เหมาะสมหรือไม่ถูกต้องอาจสร้างความเสียหายต่อการดำเนินธุรกิจได้ ดังนั้น ผู้ประกอบธุรกิจต้องดำเนินการเพื่อให้มั่นใจได้ว่าบุคลากรทุกระดับตั้งแต่ผู้ปฏิบัติงาน ไปจนถึงคณะกรรมการของผู้ประกอบธุรกิจมีความเข้าใจเพียงพอเกี่ยวกับการใช้งาน AI/ML

ผู้ประกอบธุรกิจควรจัดให้มีบุคลากรที่รับผิดชอบในด้านการพัฒนา ทดสอบ นำไปใช้งาน และควบคุมดูแลการทำงานของ AI/ML ที่เพียงพอและเหมาะสมกับรูปแบบการใช้งาน AI/ML ขององค์กร การขาดทักษะ ความเชี่ยวชาญ และประสบการณ์ด้าน AI/ML ของบุคลากรอาจส่งผลให้เกิดปัญหาในการบำรุงรักษา (Maintenance) และการพัฒนาประสิทธิภาพของโมเดลของ AI/ML ซึ่งจะทำให้ผู้ประกอบธุรกิจต้องพึ่งพาบุคคลภายนอก (Third Party) มากเกินไป (Over-Reliance) ดังนั้น ผู้บริหารระดับสูงและบุคลากรที่รับผิดชอบเกี่ยวกับการใช้งาน AI/ML ควรได้รับการเพิ่มพูนความรู้หรือการฝึกอบรมเพื่อให้เข้าใจถึงความท้าทาย ปัญหา และความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยี AI/ML และสามารถกำหนดมาตรการควบคุมความเสี่ยงอย่างเหมาะสมก่อนที่จะตัดสินใจนำ AI/ML มาใช้ในเชิงธุรกิจ

9. บรรณานุกรม

The International Organization of Securities Commissions (IOSCO). *The use of artificial intelligence and machine learning by market intermediaries and asset managers*. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. *เอกสารแนวปฏิบัติจริยธรรมปัญญาประดิษฐ์.* https://bact.cc/f/2022/11/202012-thailand-ai-ethics-guideline-mdes.pdf

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. *แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาล สำหรับผู้บริหารองค์กร*. https://www.etda.or.th/getattachment/Our-Service/AIGC/AIGC/Ai_Gov_Guideline_edit.pdf.aspx?lang=th-TH

Monetary Authority of Singapore. Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of AI and Data Analytics in Singapore's Financial Sector. https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/FEAT

De Nederlandsche Bank. *General principles for the use of Artificial Intelligence in the financial sector*. https://www.dnb.nl/media/jkbip2jc/general-principles-for-the-use-of-artificial-intelligence-in-the-financial-sector.pdf

The High-Level Expert Group on Artificial Intelligence (set up by the European Commission). *Ethics guidelines for trustworthy AI*. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

ธนาคารแห่งประเทศไทย. *Stages of AI/ML Development in Thai Banking Sector.* https://www.bot.or.th/th/research-and-publications/articles-and-publications/articles/Article_1Jan2022.html