# บันทึกข้อความ

**ส่วนราชการ** สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ โทร. ๑๓๘๐๘ (รองฯ จุมพล)

**ที่** สม ๐๑๐๐/๑๙๓ **วันที่** ๕ มีนาคม ๒๕๖๙

**เรื่อง** แนวปฏิบัติเบื้องต้นในการใช้ระบบปัญญาประดิษฐ์ (AI) ในการปฏิบัติงาน

เรียน ผอ.สนย./ผอ.สคส.๑/ผอ.สคส.๒/ผอ.สำนักงาน กสม. พื้นที่ภาคใต้

ด้วยปรากฏว่ามีเจ้าหน้าที่เริ่มนำเทคโนโลยี AI (Artificial Intelligence) มาประยุกต์ใช้ในการปฏิบัติงานในสำนัก/สำนักงานกันอย่างแพร่หลาย เพื่อยกระดับประสิทธิภาพการดำเนินงานด้านสิทธิมนุษยชนให้ครอบคลุม รวดเร็ว และมีคุณภาพยิ่งขึ้น อย่างไรก็ตาม การใช้ระบบ AI จำเป็นต้องอยู่บนพื้นฐานของความปลอดภัย ความถูกต้อง ความโปร่งใส และความรับผิดชอบ เพื่อมิให้เกิดผลกระทบต่อสิทธิและเสรีภาพของประชาชน

ในการนี้ เพื่อป้องกันมิให้เกิดความเสี่ยงหรือความเสียหายต่อสิทธิของประชาชน และความน่าเชื่อถือขององค์กร หากเจ้าหน้าที่ขาดความรู้ความเข้าใจที่ถูกต้อง ดังนั้น จึงขอกำหนดแนวปฏิบัติเบื้องต้นในการใช้ระบบ AI สำหรับให้เจ้าหน้าที่ถือปฏิบัติโดยเคร่งครัด ดังต่อไปนี้

**๑. ห้ามนำข้อมูลที่ระบุตัวตนของผู้ร้องเรียนหรือผู้เสียหายเข้าสู่ระบบ AI สาธารณะโดยเด็ดขาด**

ข้อมูลส่วนบุคคล ได้แก่ ชื่อ-นามสกุล เลขประจำตัวประชาชน ที่อยู่ หมายเลขโทรศัพท์ หรือข้อมูลใด ๆ ที่สามารถระบุตัวตนของบุคคลได้ เป็นข้อมูลที่ได้รับความคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ การนำข้อมูลดังกล่าวเข้าสู่ระบบ AI สาธารณะ อาจก่อให้เกิดความเสี่ยงต่อการรั่วไหลของข้อมูลและอาจเป็นการละเมิดสิทธิของผู้ร้องเรียน

**ตัวอย่าง** กรณีที่เจ้าหน้าที่ต้องการให้ AI ช่วยสรุปคำร้องเรียนของนายสมชาย ใจดี เลขบัตรประชาชน ๓-๑๐๐๑-๐๐๐๐๐-๐๐-๐ ที่อยู่ ๑๒๓ ถ.พระราม ๙ นั้น ห้าม พิมพ์ชื่อ-นามสกุลจริงของผู้ร้อง แต่ให้แทนที่ข้อมูลดังกล่าวเป็น “ผู้ร้อง” หรือ “นาย ก” และ “ที่อยู่ในกรุงเทพมหานคร” ก่อนนำเนื้อหาไปใส่ในระบบ AI

**๒. ต้องตรวจสอบความถูกต้องของผลลัพธ์จาก AI ทุกครั้งก่อนนำไปใช้ในงานทางการ**

ระบบ AI อาจสร้างข้อมูลที่ดูน่าเชื่อถือแต่ผิดพลาดได้ โดยเฉพาะในเรื่องตัวเลข สถิติ การอ้างอิงกฎหมาย มาตราหรือข้อความจากอนุสัญญาระหว่างประเทศ รวมทั้งเหตุการณ์ที่เกิดขึ้นภายหลังจากวันที่ระบบ AI ได้รับการฝึกฝนมา ซึ่งอาจล้าสมัยหรือไม่สอดคล้องกับสถานการณ์ปัจจุบัน

**ตัวอย่าง** AI อาจอ้างว่า “มาตรา ๔๔ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย ๒๕๖๐ รับรองสิทธิในทรัพย์สิน” ซึ่งความเป็นจริงมาตราดังกล่าวเป็นเรื่องอื่น เจ้าหน้าที่ต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำไปอ้างอิงในรายงานหรือหนังสือราชการทุกครั้ง ห้ามอ้างอิงข้อมูลจาก AI โดยมิได้ตรวจสอบ

/๓. ต้องระมัด...

**๓. ต้องระมัดระวังอคติ และการเลือกปฏิบัติ (Algorithmic Bias) ที่อาจซ่อนอยู่ในผลลัพธ์ของ AI**

เจ้าหน้าที่ต้องวิเคราะห์ผลลัพธ์จาก AI อย่างมีวิจารณญาณ เพื่อไม่ให้เกิดการเลือกปฏิบัติต่อกลุ่มเป้าหมาย เนื่องจากระบบ AI ได้รับการฝึกฝนจากข้อมูลจำนวนมหาศาล ซึ่งอาจสะท้อนอคติทางสังคม วัฒนธรรม เพศ ชาติพันธุ์ ศาสนา หรือฐานะทางเศรษฐกิจที่มีอยู่ในสังคม ผลลัพธ์จาก AI ที่เกี่ยวข้องกับกลุ่มชนกลุ่มน้อย ผู้พิการ แรงงานข้ามชาติ หรือกลุ่มเปราะบางอื่น ๆ เจ้าหน้าที่ต้องพิจารณาด้วยความระมัดระวังและรอบคอบเป็นพิเศษ

**ตัวอย่าง** หากสั่งให้ AI วิเคราะห์สถิติอาชญากรรม แล้ว AI สรุปว่า “กลุ่มแรงงานข้ามชาติมีแนวโน้มกระทำผิดสูงกว่า” เจ้าหน้าที่ต้องตรวจสอบว่าข้อมูลนั้นเป็นอคติของระบบหรือไม่ เพื่อไม่ให้รายงานนำไปสู่การตีตรา (Stigma)

**๔. ห้ามอัปโหลดไฟล์เอกสารที่มีชั้นความลับ หรือเอกสารภายในสำนักงานฯ เข้าสู่ระบบ Cloud ของ AI ภายนอก**

**ตัวอย่าง** หนังสือแจ้งข้อเท็จจริงที่กำหนดชั้นความลับมาจากหน่วยงานที่เกี่ยวข้อง ห้ามอัปโหลดไฟล์ทั้งฉบับเพื่อให้ AI ย่อความหรือประมวลผล แต่ควรสรุปเฉพาะประเด็นหรือข้อมูลที่สามารถเปิดเผยได้ด้วยตนเอง

**๕. การระวังข้อมูลลวงหรือที่เรียกกันทั่วไปว่าอาการ “หลอน” (AI Hallucination)**

เจ้าหน้าที่พึงระลึกว่า AI สามารถสร้างข้อมูลที่ดูน่าเชื่อถือแต่ไม่มีอยู่จริงขึ้นมาได้ (Fake citations)

**ตัวอย่าง** AI อาจอ้างรายงานการตรวจสอบ ที่ ๒๓๗๕/๒๕๖๕ ซึ่งในฐานข้อมูลไม่มีเลขรายงานฉบับนี้ หรืออ้างอิงเอกสารทางวิชาการที่ไม่มีอยู่จริง เจ้าหน้าที่ต้องตรวจสอบความถูกต้องของข้อมูลทุกครั้ง

**๖. ความเป็นปัจจุบันของข้อมูล โดยเฉพาะอย่างยิ่งข้อกฎหมาย**

เจ้าหน้าที่ต้องตระหนักว่า AI ส่วนใหญ่มีฐานข้อมูลที่จำกัดถึงช่วงเวลาหนึ่งเท่านั้น และอาจไม่ทราบกฎหมายที่เพิ่งประกาศใช้บังคับ

**ตัวอย่าง** กฎหมายลำดับรองที่ประกาศในราชกิจจานุเบกษาเมื่อเดือนที่แล้ว AI อาจยังไม่ทราบ เจ้าหน้าที่จึงต้องตรวจสอบข้อมูลด้วยตนเองจาก website ของราชกิจจานุเบกษา หรือแหล่งข้อมูลของส่วนราชการที่เกี่ยวข้อง

**๗. หลักสิทธิมนุษยชน และหลักความเป็นกลาง ห้ามใช้ AI ตัดสินใจขั้นสุดท้ายในกรณีที่มีผลกระทบต่อสิทธิเสรีภาพของบุคคล**

การใช้ AI ร่างความเห็นต้องยึดถือความเป็นกลางและหลักการสิทธิมนุษยชน การวินิจฉัยว่ามีการละเมิดสิทธิมนุษยชนหรือไม่ ตลอดจนการเสนอข้อเสนอแนะที่มีผลต่อบุคคลหรือกลุ่มบุคคลใด ต้องอาศัยความรู้และทักษะของของเจ้าหน้าที่/ผู้บังคับบัญชาที่เข้าใจบริบทสังคม กฎหมาย และมิติสิทธิมนุษยชนอย่างรอบด้าน AI สามารถเป็นเครื่องมือช่วยวิเคราะห์ข้อมูลเบื้องต้นได้เท่านั้น

/ตัวอย่าง...

**ตัวอย่าง** การร่างความเห็นเรื่องเสรีภาพในการชุมนุม เจ้าหน้าที่ต้องไม่ใช้ Prompt ที่มีลักษณะชี้นำให้ AI เขียนสนับสนุนหรือโจมตีฝ่ายหนึ่งฝ่ายใด แต่ต้องเน้นหลัก “สิทธิ” และ “ข้อจำกัด” ตามกฎหมาย AI อาจช่วยสรุปข้อเท็จจริงจากคำร้องเรียนและระบุมาตรากฎหมายที่เกี่ยวข้องได้ แต่การวินิจฉัยว่ากรณีใดเป็นการละเมิดสิทธิมนุษยชน หรือข้อเสนอแนะต่อหน่วยงานที่เกี่ยวข้อง ต้องเป็นการตัดสินใจของเจ้าหน้าที่/ผู้บังคับบัญชา/กสม. เท่านั้น

**๘. ควรพัฒนาทักษะการใช้ AI อย่างต่อเนื่องและแลกเปลี่ยนความรู้กับเพื่อนร่วมงาน**

เทคโนโลยี AI มีการพัฒนาอย่างรวดเร็ว เจ้าหน้าที่ทุกคนควรติดตามความเปลี่ยนแปลงและพัฒนาทักษะของตนเองให้ทันสมัยอยู่เสมอ เพื่อให้สามารถใช้ AI ได้อย่างมีประสิทธิภาพ ปลอดภัย และสอดคล้องกับพันธกิจของสำนักงาน รวมทั้งเผยแพร่ความรู้ที่ได้รับแก่เพื่อนร่วมงานด้วย

**ตัวอย่าง** เจ้าหน้าที่ที่ค้นพบวิธีใช้ AI เพื่อสรุปรายงานได้อย่างมีประสิทธิภาพ ควรบันทึก Prompt และขั้นตอนที่ใช้ แล้วนำไปแบ่งปันในการประชุมกลุ่มงาน/สำนัก หรือรวบรวมไว้เป็นคลังความรู้ของกลุ่มงาน/สำนัก เพื่อให้เพื่อนร่วมงานทุกคนได้ใช้ประโยชน์ร่วมกัน

ทั้งนี้ หากเจ้าหน้าที่ได้ใช้ AI ในส่วนที่เป็นสาระสำคัญของการปฏิบัติงาน ต้องตรวจสอบความถูกต้องของเนื้อหาอย่างรอบคอบทุกครั้ง และควรแจ้งให้ผู้บังคับบัญชาทราบด้วย เพื่อให้ผู้บังคับบัญชาเพิ่มความระมัดระวังและใช้ดุลพินิจในการตรวจสอบความถูกต้อง (Double-Check) ในส่วนที่ AI ประมวลผลเป็นพิเศษ ป้องกันความผิดพลาดทางเทคนิคที่อาจเกิดขึ้นได้

จึงเรียนมาเพื่อโปรดแจ้งเจ้าหน้าที่เพื่อถือปฏิบัติโดยเคร่งครัดต่อไป

(นายจุมพล ขุนอ่อน)

รองเลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ