



สำนักงานตำรวจแห่งชาติ
(Royal Thai Police)



สื่อการเรียนรู้ เพื่อสร้างความตระหนักรู้เกี่ยวกับการใช้งานโปรแกรม **AI** (ARTIFICIAL INTELLIGENCE)

หรือแอปพลิเคชัน



สถาบันส่งเสริมงานสอบสวน สำนักงานกฎหมายและคดี



สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร





หนังสือ ตร. ที่ 0011.45/3024 ลงวันที่ 30 กันยายน 2568

เรื่อง กำชับการปฏิบัติเกี่ยวกับการใช้โปรแกรมเพื่อช่วยเหลือในการทำสำนวนการสอบสวนคดีอาญา



สำนวนคดีอาญาต้องดำเนินการในลักษณะเป็นความลับ

หากพนักงานสอบสวนใช้โปรแกรมหรือแอปพลิเคชันที่เป็นแบบสาธารณะ ข้อมูลที่พนักงานสอบสวนบันทึกลงไปในส่วน อาจถูกนำไปรวมเป็นฐานข้อมูลของระบบ เพื่อใช้ในการประมวลผลสำหรับผู้ใช้งานที่เป็นบุคคลทั่วไป ทำให้ข้อมูลหรือข้อเท็จจริงในการทำสำนวนรั่วไหลได้



พนักงานสอบสวนต้องให้ความสำคัญต่อการจัดทำสำนวนการสอบสวนด้วยตนเองเป็นอันดับแรก หากพนักงานสอบสวนจะใช้โปรแกรมหรือแอปพลิเคชันช่วยในการปฏิบัติงาน จะต้องไม่ขัดต่อกฎหมายและระเบียบที่เกี่ยวข้อง และมีความปลอดภัย

โดยมีแนวทางดำเนินการ ดังนี้

- พิจารณาเลือกโปรแกรมหรือแอปพลิเคชันที่ใช้การเชื่อมโยงข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ ภายใน ตร. เป็นอันดับแรก
- พงส. ต้องไม่นำเข้าข้อมูลส่วนบุคคลของบุคคล และข้อมูลสำคัญในสำนวนการสืบสวนสอบสวนคดีอาญาเข้าสู่ระบบ เพื่อสรุป วิเคราะห์ ประมวลผลโดยเด็ดขาด ควรใช้เฉพาะการปฏิบัติงานในส่วนที่ไม่ส่งผลกระทบต่อคดีหรือเป็นการเล็กน้อยในการทำสำนวน
- หากมีความจำเป็นต้องใช้โปรแกรมหรือแอปพลิเคชันที่เปิดให้บริการสาธารณะ ให้ พงส. ศึกษา ตรวจสอบ และพิจารณาก่อนว่ามีมาตรฐาน มีความปลอดภัย และมีกฎระเบียบการทำงานของระบบที่จะไม่นำข้อมูลต่าง ๆ ของผู้ใช้งานนำไปรวมไว้ในฐานข้อมูลของระบบ รวมถึงการตั้งค่าการควบคุมข้อมูลก่อนเริ่มใช้งานด้วย
- หากหน่วยใดจะจัดทำโปรแกรมหรือแอปพลิเคชันในลักษณะช่วยสรุป วิเคราะห์ ประมวลผล โดยระบบปัญญาประดิษฐ์ จะต้องเสนอโครงการและสถาปัตยกรรมระบบมาให้ สทส. (ศทก.) ตรวจสอบรับรองก่อน





กฎหมาย ที่เกี่ยวข้อง



page 03

“สำนวนคดีอาญาเป็นข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐมิให้เปิดเผย ถือเป็นข้อราชการอันพึงสงวนเป็นความลับ เพราะเป็นเอกสารสำคัญในการสอบสวนพยานหลักฐานต่าง ๆ เพื่อนำตัวผู้กระทำผิดมาลงโทษ พนักงานสอบสวนจึงต้องสงวนไว้เป็นความลับอย่างยิ่งห้ามนำไปเปิดเผยเป็นอันขาด

ทั้งนี้ สำนวนการสอบสวนยังประกอบด้วยข้อมูลส่วนบุคคลของผู้เกี่ยวข้อง เช่น ผู้เสียหาย พยาน และผู้ต้องหา เป็นต้น ซึ่งได้รับความคุ้มครองตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเปิดเผยเป็นการทั่วไปต่อผู้ไม่มีหน้าที่เกี่ยวข้อง หากไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ”

01

พ.ร.บ.ข้อมูลข่าวสารของทางราชการ
พ.ศ.2540

02

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

03

ระเบียบว่าด้วยการรักษาความลับของทางราชการ
พ.ศ.2544 และที่แก้ไขเพิ่มเติม

04

ระเบียบ ตร. ว่าด้วยประมวลระเบียบการตำรวจ
ไม่เกี่ยวกับคดี ลักษณะที่ 29 ความลับ

ความตระหนักรู้เกี่ยวกับการนำปัญญาประดิษฐ์ (ARTIFICIAL INTELLIGENCE: AI) มาใช้ในการทำสำนวนการสอบสวน

ความเข้าใจพื้นฐาน เกี่ยวกับ AI

AI คือระบบที่สามารถประมวลผลข้อมูล เรียนรู้จากประสบการณ์ และทำงานบางอย่างแทนมนุษย์ เช่น การแปลงเสียงเป็นข้อความ การช่วยจัดเรียงเอกสาร หรือการแปลภาษา

ประโยชน์ของการใช้ AI ในการทำสำนวน

- ร่างเอกสารได้รวดเร็ว
- ช่วยในการตรวจสอบความสอดคล้องของข้อมูล
- ช่วยในการค้นหาข้อมูล พฤติกรรมซ้ำในคดีที่คล้ายกัน
- ลดภาระงานเอกสาร

ความเสี่ยงและข้อควรระวัง

- ข้อมูลลับและความเป็นส่วนตัว ห้ามนำข้อมูลคดีหรือข้อมูลส่วนบุคคลเข้าสู่ระบบ AI ที่ไม่ได้รับอนุญาตหรือไม่มีมาตรการป้องกันข้อมูล
- ความถูกต้องของข้อมูล AI อาจให้คำตอบหรือร่างข้อความที่ดูสมจริง แต่ไม่ถูกต้องตามข้อเท็จจริง หรือหลักกฎหมาย
- อคติของข้อมูล (Bias) - หาก AI ถูกฝึกจากข้อมูลที่มี อคติ อาจทำให้ผลการวิเคราะห์ที่ไม่เป็นกลาง หรือเกิดความไม่ยุติธรรม

แนวทางปฏิบัติที่เหมาะสม และควรตระหนักรู้

- AI เป็นผู้ช่วยไม่ใช่ผู้ตัดสินใจ - ต้องตรวจสอบและแก้ไขทุกข้อความที่ AI สร้างขึ้น ก่อนนำไปใช้จริง
- หลีกเลี่ยงการป้อนข้อมูลที่เป็นความลับหรือข้อมูลระบุตัวตน
- เลือกใช้ระบบ AI ที่ได้รับการรับรองจากหน่วยงานรัฐหรือผ่านมาตรฐานความปลอดภัยข้อมูล
- ผู้ใช้งาน AI ควรผ่านการอบรมการเทคโนโลยีดิจิทัลและกฎหมายไซเบอร์อย่างต่อเนื่อง



หลักการตั้งค่าเริ่มต้น อย่างปลอดภัย



การควบคุมการเข้าถึง (Access Control)

ให้กำหนดสิทธิ์การเข้าถึงเฉพาะเท่าที่จำเป็นจริง ๆ ผู้ที่ได้รับอนุญาตเท่านั้น
จึงจะสามารถเข้าดูหรือใช้งานข้อมูลและระบบปัญญาประดิษฐ์ได้ เพื่อลดความเสี่ยง
จากการเข้าถึงโดยไม่เหมาะสม



การพิสูจน์ตัวตน (Authentication)

ควรใช้การยืนยันตัวตนหลายขั้นตอน โดยเฉพาะสำหรับบัญชีผู้ดูแลระบบที่มีอำนาจ
จัดการระบบปัญญาประดิษฐ์ วิธีนี้ช่วยลดความเสี่ยงจากการถูกเข้าถึง
โดยไม่ได้รับอนุญาต เช่น การขโมยรหัสผ่านหรือข้อมูลยืนยันตัวตนอื่น ๆ



กระบวนการติดตั้งและใช้งาน

เมื่อเริ่มใช้งาน “ช่องทางเชื่อมต่อระบบ” หรือ API ควรกำหนดให้มีการตรวจสอบตัวตน
และสิทธิ์ของผู้ใช้อย่างเข้มงวดก่อนทุกครั้ง เพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาต
เข้ามาใช้งาน ควบคุมระบบ หรือดึงข้อมูลออกไปได้



การตรวจสอบและแก้ไขข้อมูลนำเข้า (Input Sanitization)

ควรตรวจสอบข้อมูลที่ใส่เข้ามาในระบบให้ถูกต้องตามรูปแบบที่ระบบรองรับ พร้อมปรับแก้
ข้อมูลให้อยู่ในขอบเขตที่ปลอดภัย เพื่อลดความเสี่ยงจากการถูกโจมตีหรือการส่งข้อมูล
ที่อาจทำให้ระบบทำงานผิดพลาด



การบันทึกล็อกและการเฝ้าระวัง

ควรเก็บข้อมูลบันทึกการทำงานของระบบ เช่น ข้อมูลที่ระบบรับเข้าและส่งออก รวมถึง
กิจกรรมที่ทำด้วยสิทธิ์ผู้ดูแลระบบ เพื่อนำไปใช้ตรวจสอบเหตุผิดปกติ ร่องรอยภัยคุกคาม
หรือการโจมตีที่อาจเกิดขึ้นในอนาคต



สำนักงานตำรวจแห่งชาติ
(Royal Thai Police)



ข้อควรระวัง/แนะนำ



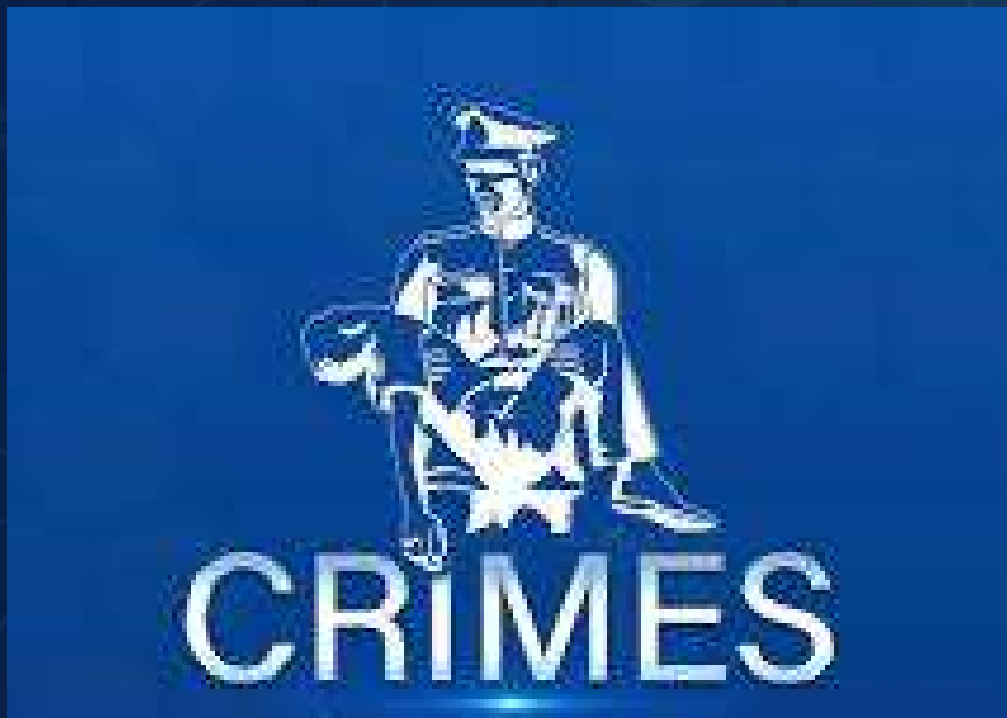
ไม่ใส่ข้อมูลส่วนตัว/ข้อมูลลงไปแชต หากจำเป็น ต้องทำ Data Masking (การปิดบังข้อมูล) การแทนค่าข้อมูลจริงด้วยค่าอื่น เช่น เปลี่ยนชื่อเป็น xxxx



- ใช้เวอร์ชันองค์กร (เช่น ChatGPT Team/Enterprise, Gemini for Workspace, Microsoft Copilot for M365) เนื่องจากมีฟีเจอร์ในการควบคุม
- การใช้ AI ผ่าน API (การใช้ช่องทางที่ทำให้ระบบงานหรือแอปพลิเคชันขององค์กร เชื่อมต่อกับระบบ AI ได้โดยตรง เพื่อส่งข้อมูลไปให้ระบบประมวลผล และรับผลลัพธ์ กลับมาอย่างเป็นระเบียบและปลอดภัย) เช่น การใช้ OpenAI API ควรกำหนด การตั้งค่าไม่ให้ระบบบันทึกข้อมูลการใช้งาน (log) เพื่อคุ้มครองข้อมูลของผู้ใช้
- ปิดการเก็บข้อมูลในตั้งค่า Settings เช่น ChatGPT → ปิด "Chat History & Training"
- ถ้าข้อมูลเป็นข้อมูลส่วนบุคคล ควรพิจารณาใช้ AI on-premise (กลุ่มเซิร์ฟเวอร์ ของหน่วยงานและสามารถควบคุมเองได้)



โปรแกรม “สำนวนอิเล็กทรอนิกส์”



เป็นโปรแกรมที่พัฒนา
อยู่บนแพลตฟอร์มของ
ระบบ CRIMES
ระบบเทคโนโลยีสารสนเทศ ตร.



มีระบบปกป้องภัยคุกคามทางดิจิทัล (Cybersecurity) เช่น การโจมตีการเข้าถึง โดยไม่ได้รับอนุญาตหรือการขโมยข้อมูล เพื่อรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล ซึ่งรวมถึงการใช้เทคโนโลยี กระบวนการ และการให้ความรู้แก่ผู้ใช้งาน เพื่อลดความเสี่ยง



ระบบเครือข่ายมีความปลอดภัย



มีคณะกรรมการ กำกับดูแล ตรวจสอบ ด้านความปลอดภัย ภายใต้การกำกับ
ดูแลสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
National Cyber Security Agency - NCSA



ศทก. อยู่ระหว่างพัฒนาระบบ Smart Crimes : ระบบสำนวนอิเล็กทรอนิกส์
อัจฉริยะ คาดว่าจะเปิดให้ใช้งานประมาณเดือน เม.ย.69





CRIMES ONLINE

CRIMES SEARCH

CRIMES Search

สำนวนอิเล็กทรอนิกส์

เชื่อมโยงข้อมูลกับหน่วยงานภายนอก

ข้อมูลบุคคล
พันโทฯ กรมราชทัณฑ์

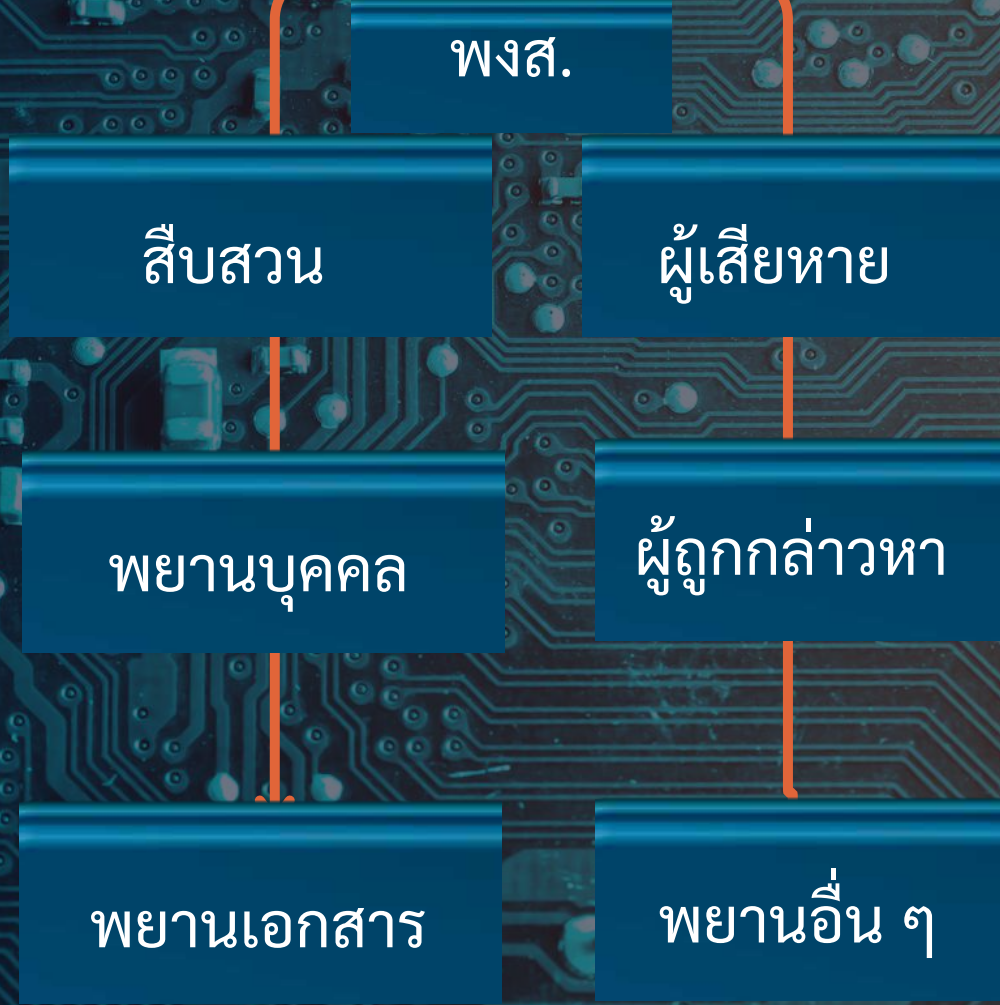
ข้อมูลทะเบียนราษฎร์
กรมการปกครอง

กระทรวงพาณิชย์

ข้อมูลยานพาหนะ
กรมการขนส่งทางบก

ธนาคารกรุงไทย

ข้อมูลหลักประกันสุขภาพ
(สปสช.)



สำนักงานอัยการสูงสุด 

สำนักงานศาลยุติธรรม 

การขอหมายจับออนไลน์
ผ่านระบบ AWIS

