รายงานวิจัยฉบับสมบูรณ์

โครงการศึกษาการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้เพื่อป้องกันและปราบปรามอาชญากรรม

โดย

ผู้ช่วยศาสตราจารย์ ดร. สุพัตรา แผนวิชิต

มหาวิทยาลัยสุโขทัยธรรมาธิราช

ได้รับทุนวิจัยจากกองทุนวิทยาศาสตร์ วิจัยและนวัตกรรม ประจำปี 2564

สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.)

กันยายน 2565

ชื่อเรื่อง โครงการศึกษาการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้เพื่อป้องกันและปราบปรามอาชญากรรม

ชื่อผู้วิจัย ผู้ช่วยศาสตราจารย์ ดร. สุพัตรา แผนวิชิต

ปีที่แล้วเสร็จ 2565

บทคัดย่อ

การศึกษาวิจัยครั้งนี้มีวัตถุประสงค์ 1) เพื่อศึกษานวัตกรรมและเทคโนโลยีเกี่ยวกับข้อมูลขนาดใหญ่ (Big Data) และการนำข้อมูลขนาดใหญ่มาใช้ประโยชน์ในการป้องกันและปราบปรามอาชญากรรมทั้งด้านการเฝ้าระวังและติดตามด้านการป้องกันและปราบปรามด้านการสืบสวนสอบสวนและด้านพยานหลักฐาน 2) เพื่อศึกษากฎหมายที่เกี่ยวข้อง ปัญหาและข้อจำกัดในการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในระบบงานยุติธรรมด้านการป้องกันและปราบปรามอาชญากรรม ทั้งข้อจำกัดด้านกฎหมายด้านความพร้อมของหน่วยงานและบุคลากร รวมทั้งผลกระทบต่อสิทธิของเจ้าของข้อมูล 3) เพื่อวิเคราะห์รูปแบบและแนวทางการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) ในการป้องกันและปราบปรามการอาชญากรรมของต่างประเทศ 4) เพื่อเสนอแนะแนวทางแก้ไขกฎหมายเพื่อรองรับการนำข้อมูลขนาดใหญ่มาใช้ประโยชน์ในการป้องกันและปราบปรามอาชญากรรมของภาครัฐ และ 5) เพื่อเสนอแนะแนวทางเตรียมความพร้อมของหน่วยงานบังคับใช้กฎหมายเพื่อสนับสนุนการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปรามอาชญากรรมเพื่อประสิทธิภาพสูงสุด

ระเบียบวิธีการวิจัย ประกอบด้วย การวิจัยเอกสาร (Documentary research) การสัมภาษณ์เชิงลึก (In-depth Interview) การประชุมกลุ่มย่อย (Focus Group) และการจัดสัมมนาเพื่อรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้องและผู้มีส่วนได้เสีย

ผลการศึกษาพบว่า ข้อมูลขนาดใหญ่ (Big Data) มีประโยชน์ต่อระบบงานยุติธรรมในหลายด้านทั้งการเฝ้าระวังและติดตาม การป้องกันและปราบปราม การสืบสวนสอบสวน รวบรวมพยานหลักฐาน โดยเฉพาะการนำข้อมูลขนาดใหญ่มาใช้เป็นเครื่องมือวิเคราะห์ความเสี่ยงของการเกิดอาชญากรรม เพื่อให้สามารถวางมาตรการป้องกันและปราบปรามอาชญากรรมได้อย่างมีประสิทธิภาพ แต่ในปัจจุบันประเทศไทยยังมีปัญหาและข้อจำกัดในการใช้ข้อมูลขนาดใหญ่หลายประการ อาทิ ข้อจำกัดด้านกฎหมาย ผลกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล ข้อจำกัดด้านเทคโนโลยีและการใช้ประโยชน์จากข้อมูล ข้อจำกัดด้านการจัดเก็บและเชื่อมโยงฐานข้อมูล ผู้วิจัยจึงได้เสนอแนวทางแก้ไขปัญหาโดยการแก้ไขเพิ่มเติมพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 โดยกำหนดเพิ่มส่วนที่เกี่ยวกับการบริหารจัดการข้อมูลขนาดใหญ่เพื่อป้องกันและปราบปรามอาชญากรรม กำหนดหลักเกณฑ์การเชื่องโยงข้อมูล การจัดทำบัญชีรายการข้อมูล (Data Catalog) การวิเคราะห์ข้อมูลแนวโน้มอาชญากรรม รวมถึงให้หน่วยงานภาครัฐสามารถเข้าถึงข้อมูลและแลกเปลี่ยนข้อมูลกับภาคเอกชนเพื่อนำไปใช้ประโยนช์ในภารกิจด้านการป้องกันและปราบปรามอาชญากรรมได้

คำสำคัญ ข้อมูลขนาดใหญ่ ป้องกัน ปราบปราม อาชญากรรม

Title: Project on Study of Introduction of Big Data to Prevention and Suppression of Crimes

Researcher: Asst. Prof. Dr. Supatra Phanwichit

Year of Completion: 2022

Abstract

The objectives of this research are: 1) to study innovations and technologies relating to big data, and introduction of big data to use in preventing and suppressing crimes, both for monitoring and following up crime prevention and suppression, investigation and gathering evidence; 2) to study laws relevant to problems and limits in use of big data for preventing and suppressing crimes, either legal restrictions, readiness of agencies and human resources, as well as impact on rights of the data subjects; 3) to analyze forms and approaches to use of big data for preventing and suppressing crimes in foreign countries; 4) to propose an approach to amending laws for supporting use of big data for preventing and suppressing crimes in the public sector; and 5) to propose an approach to preparing law enforcement agencies for supporting use of big data for preventing and suppressing crimes, as to achieve the highest efficiency.

The research methodology comprises of documentary research, in-depth interview, focus group, and seminar for hearing opinions from competent agencies and stakeholders.

The study shows that big data are beneficial to the justice system in various respects, including monitoring and following up crimes, preventing and suppressing crimes, investigation, gathering evidence, as to enable efficient crime prevention and suppression measures. However, at the present, Thailand still experiences several problems with and restrictions in use of big data, for example, legal restriction, impact on rights of the data subjects, technological restrictions and use of data, restrictions of storage and connection of databases. Therefore, the researcher proposes an approach to solving the problems by amending Digitalization of Public Administration and Services Delivery Act, B.E. 2562 (2019), adding a part concerning administration of big data for preventing and suppressing crimes, stipulating criteria for connecting data, data cataloging, analysis of data for criminal tendency, as well as allowing public agencies to access and exchange data with the private sector for using the data in missions of crime prevention and suppression.

Keyword: Big Data , Prevention , Suppression , Crime

สารบัญ

บทที่ 1
บทนำ

1. หลักการและเหตุผล

เศรษฐกิจดิจิทัล (Digital Economy) หมายถึง การขับเคลื่อนเศรษฐกิจของประเทศโดยใช้เทคโนโลยีสารสนเทศและการสื่อสารมาสร้างอาชีพหรือกิจกรรมทางเศรษฐกิจ หรือเรียกว่าเทคโนโลยีดิจิทัล เพื่อให้ทันยุคสมัย อันเป็นกลไกสำคัญในการขับเคลื่อนการปฏิรูปกระบวนการผลิตการดำเนินธุรกิจ การค้า การบริการ การศึกษา การสาธารณสุข การบริหารราชการแผ่นดิน รวมทั้งกิจกรรมทางเศรษฐกิจและสังคมอื่น ๆ ที่ส่งผลต่อการพัฒนาทางเศรษฐกิจและการพัฒนาคุณภาพชีวิตของคนในสังคม เพราะเศรษฐกิจดิจิทัลจะช่วยการลดทุนการผลิต อำนวยความสะดวกในการให้บริการและการลงทุนในธุรกิจ ทำให้ธุรกิจขยายตัวกว้างมากขึ้นและมีลักษณะข้ามพรมแดน ส่งผลต่อการขยายตัวของการจ้างงาน ซึ่งความก้าวหน้าทางเทคโนโลยีสารสนเทศดังกล่าวได้ถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสาร ส่งผลให้เกิดปริมาณของข้อมูลขนาดใหญ่ที่มีจำนวนข้อมูลมหาศาลในทุกรูปแบบทุกมิติ การนำข้อมูลขนาดใหญ่ดังกล่าวมาประมวลและวิเคราะห์จะทำให้ได้ผลที่นำมาใช้ประโยชน์ได้อย่างมหาศาล ข้อมูลขนาดใหญ่จึงเป็นเครื่องมือที่มีประสิทธิภาพในการช่วยให้รัฐบาลพัฒนาคุณภาพชีวิตความเป็นอยู่ของประชาชนให้ดียิ่งขึ้น โดยเฉพาะในการป้องกันและปราบปรามอาชญากรรม ผลที่ได้จากการวิเคราะห์ข้อมูลขนาดใหญ่สามารถช่วยในการทำงานของหน่วยงานบังคับใช้กฎหมายได้ตั้งแต่การวิเคราะห์ความเสี่ยงหรือโอกาสที่จะเกิดอาชญากรรมไปจนถึงการกำหนดมาตรการในการป้องกันอาชญากรรมเพราะสามารถนำมาใช้เป็นเครื่องมือในการหารูปแบบและโอกาสในการเกิดอาชญากรรม เป็นการทำนายเหตุการณ์ล่วงหน้าเพื่อป้องกันและลดอัตราการเกิดอาชญากรรมได้

ข้อมูลขนาดใหญ่ (Big Data) นับเป็นนวัตกรรมทางเทคโนโลยีที่มีประโยชน์อย่างมาก เพราะเป็นเครื่องมือของภาครัฐในการขับเคลื่อนการบริหารงานอย่างมีประสิทธิภาพและทันต่อการเปลี่ยนแปลงทางเทคโนโลยี ในด้านการแก้ไขปัญหาอาชญากรรม การใช้ข้อมูลขนาดใหญ่เป็นเครื่องมือในการช่วยเก็บข้อมูลและวิเคราะห์ความเสี่ยงของการเกิดอาชญากรรม เพื่อให้สามารถวางมาตรการป้องกันและปราบ ปรามอาชญากรรมได้อย่างตรงจุดมากขึ้น สำหรับประเทศไทยข้อมูลขนาดใหญ่ (Big Data) ยังไม่ถูกนำมาใช้ประโยชน์ในกระบวนการยุติธรรมทางอาญาอย่างเป็นรูปธรรม เนื่องจากยังขาดกลไกกฎหมายที่ชัดเจน ทั้งที่การวิเคราะห์ข้อมูลขนาดใหญ่มีประโยชน์ต่อระบบงานยุติธรรมในหลายด้าน ไม่ว่าในด้านการเฝ้าระวังและติดตาม ด้านการป้องกันและปราบปราม ด้านการสืบสวนสอบสวน หรือด้านพยานหลักฐาน ดังนั้น ภาครัฐ

ควรให้ความสำคัญกับการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในระบบงานยุติธรรมเพื่อป้องกันและปราบปรามอาชญากรรม อาทิ การใช้วิเคราะห์ข้อมูลการเกิดอาชญากรรม ความเสี่ยงเพื่อเฝ้าระวังการเกิดอาชญากรรม วิเคราะห์พฤติกรรมของผู้กระทำความผิดและแนวโน้มการเกิดอาชญากรรม การสืบหาบุคคลและยานพาหนะ การวิเคราะห์ความเชื่อมโยงของพยานหลักฐานเพื่อประโยชน์ในงานสอบสวน และในขณะเดียวกับภาครัฐจะต้องตระหนักถึงความสำคัญของสิทธิส่วนบุคคลของประชาชน รวมถึงการสร้างหลักประกันแก่ประชาชนต่อเรื่องความเสี่ยงในการใช้ข้อมูลและเทคโนโลยีอย่างต่อเนื่อง ด้วยเหตุดังกล่าวจึงนำมาสู่แนวคิดการวิจัยเพื่อเสนอแนวทางให้ภาครัฐสามารถนำข้อมูลขนาดใหญ่มาใช้เพื่อประโยชน์ในการป้องกันและปราบปรามอาชญากรรมให้มีประสิทธิภาพ โดยการแก้ไขข้อจำกัดด้านกฎหมาย การวางแนวทางใช้ข้อมูลเพื่อให้เกิดผลในเชิงการป้องกันอาชญากรรม โดยเน้นกระบวนการมีส่วนร่วมของประชาชนผ่านกระบวนการแลกเปลี่ยนข้อมูลและการใช้ข้อมูลร่วมกัน โดยคำนึงถึงหลักประกันของประชาชนเกี่ยวกับสิทธิของเจ้าของข้อมูล

การศึกษาวิจัยนี้เป็นองค์ความรู้ใหม่ด้านการนำนวัตกรรมมาใช้ในกระบวนการยุติธรรมทางอาญา เป็นการพัฒนางานวิจัยด้านกฎหมายในมิติที่ทันต่อเทคโนโลยีและสังคมดิจิทัล โดยผลที่ได้จากการการวิจัยคือข้อเสนอแนะแนวทางแก้ไขกฎหมายเพื่อลดข้อจำกัดการนำนวัตกรรมและเทคโนโลยีข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ในระบบงานยุติธรรมด้านการป้องกันและปราบปรามอาชญากรรม รัฐบาลและหน่วยงานที่เกี่ยวข้องสามารถนำผลการศึกษาวิจัยไปใช้ในการกำหนดนโยบายและยุทธศาสตร์ที่เกี่ยวข้อง และเป็นการนำนวัตกรรมมาใช้ประโยชน์ต่อการสร้างการมีส่วนร่วมของประชาชนกับภาครัฐในการป้องกันและปราบปรามอาชญากรรม ก่อให้เกิดประโยชน์ในเชิงเศรษฐกิจและสังคม เพราะช่วยลดภาระภาครัฐ ทั้งด้านงบประมาณ กำลังพล ด้านอุปกรณ์เครื่องมือและลดต้นทุนในการดูแลผู้ต้องขังในเรือนจำ ทำให้รัฐมีความมั่นคงทางเศรษฐกิจมากขึ้น ปัญหาอาชญากรรมลดลง สังคมมีความสงบสุขและประชาชนมีความปลอดภัยในชีวิตและทรัพย์สิน โดยในงานวิจัยจะทำการศึกษาเปรียบเทียบกับแนวทางของต่างประเทศที่มีการนำข้อมูลขนาดใหญ่มาใช้อย่างมีประสิทธิภาพ เพื่อนำมาวิเคราะห์และประมวลผลเป็นแนวทางแก้ไขกฎหมายและการเตรียมความพร้อมของภาครัฐเพื่อสนับสนุนการนำนวัตกรรมและเทคโนโลยี Big Data มาใช้ในการป้องกันและปราบปรามอาชญากรรมในประเทศไทย

2. วัตถุประสงค์

1) เพื่อศึกษานวัตกรรมและเทคโนโลยีเกี่ยวกับข้อมูลขนาดใหญ่ (Big Data) และการนำข้อมูลขนาดใหญ่มาใช้ประโยชน์ในการป้องกันและปราบปรามอาชญากรรม ทั้งด้านการเฝ้าระวังและติดตาม ด้านการป้องกันและปราบปราม ด้านการสืบสวนสอบสวนและด้านพยานหลักฐาน

2) เพื่อศึกษากฎหมายที่เกี่ยวข้อง ปัญหาและข้อจำกัดในการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในระบบงานยุติธรรมด้านการป้องกันและปราบปรามอาชญากรรม ทั้งข้อจำกัดด้านกฎหมาย ด้านความพร้อมของหน่วยงานและบุคลากร รวมทั้งผลกระทบต่อสิทธิของเจ้าของข้อมูล

3) เพื่อวิเคราะห์รูปแบบและแนวทางการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) ในการป้องกันและปราบปรามการอาชญากรรมของต่างประเทศ

4) เพื่อเสนอแนะแนวทางแก้ไขกฎหมายเพื่อรองรับการนำข้อมูลขนาดใหญ่มาใช้ประโยชน์ในการป้องกันและปราบปรามอาชญากรรมของภาครัฐ

5) เพื่อเสนอแนะแนวทางเตรียมความพร้อมของหน่วยงานบังคับใช้กฎหมายเพื่อสนับสนุนการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปรามอาชญากรรมเพื่อประสิทธิภาพสูงสุด

3. กรอบการวิจัย

การวิจัยเป็นการวิเคราะห์เพื่อกำหนดแนวทางที่เป็นรูปธรรมในการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) ในการป้องกันและปราบปรามอาชญากรรม เนื่องจากในประเทศไทยยังขาดความชัดเจนและมีข้อจำกัดหลายประการ ในการรวบรวม วิเคราะห์และบริหารจัดการข้อมูลขนาดใหญ่ งานวิจัยจึงมุ่งสร้างแนวทางการลดข้อจำกัดของกฎหมาย นำไปสู่การแก้ไขกฎหมายและกำหนดยุทธศาสตร์ของหน่วยงานที่เกี่ยวข้องต่อไป โดยเน้นการส่งเสริมให้ประชาชนทุกคนได้มีส่วนร่วมในการป้องกันและปราบปรามอาชญากรรมอย่างแท้จริง โดยประชาชนจะมีส่วนร่วมตั้งแต่กระบวนการให้ข้อมูล การแลกเปลี่ยนข้อมูลและการใช้ประโยชน์จากข้อมูลร่วมกันระหว่างภาครัฐและประชาชน

4. สมมติฐานงานวิจัย

ปัจจุบันภาครัฐให้ความสำคัญต่อการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ให้เกิดประโยชน์กับประเทศในหลายด้านโดยเฉพาะในด้านเศรษฐกิจ แต่ในการป้องกันและปราบปรามอาชญากรรม ทั้งการเฝ้าระวังและติดตาม การป้องกันและปราบปราม การสืบสวนสอบสวนและด้านพยานหลักฐาน การนำข้อมูล

ขนาดใหญ่มาใช้ประโยชน์ยังมีปัญหาและข้อจำกัดหลายประการ อาทิ ข้อจำกัดด้านกฎหมาย ผลกระทบต่อสิทธิของเจ้าของข้อมูล ความพร้อมของหน่วยงานและบุคลากร ดังนั้น การศึกษาและวิเคราะห์เพื่อเสนอแนวทางการแก้ไขกฎหมายและกำหนดมาตรการการนำข้อมูลขนาดใหญ่ในการป้องกันและปราบปรามอาชญากรรม โดยศึกษาจากบทเรียนและแนวทางที่ดีของต่างประเทศ จะเป็นการเตรียมความพร้อมของหน่วยงานบังคับใช้กฎหมายเพื่อสนับสนุนการนำข้อมูลขนาดใหญ่มาใช้เพื่อให้เกิดประสิทธิภาพและประโยชน์สูงสุด ส่งผลดีต่อการลดปัญหาอาชญากรรม และลดภาระและงบประมาณภาครัฐในการป้องกันและปราบปรามอาชญากรรม

5. แผนการดำเนินงานวิจัย

แผนงาน/กิจกรรม	ระยะเวลา (เดือน)											
	1	2	3	4	5	6	7	8	9	10	11	12
ศึกษา รวบรวมข้อมูลทบทวนวรรณกรรมและข้อมูลจากหน่วยงานที่เกี่ยวข้อง	■	■	■									
ดำเนินการเก็บรวบรวมข้อมูลโดยการสัมภาษณ์เชิงลึก				■								
ดำเนินการเก็บรวบรวมข้อมูลโดยการประชุมกลุ่มย่อย					■	■						
สรุปและวิเคราะห์ผลจากการเก็บรวบรวบข้อมูล							■	■				
ประมวลผลและวิเคราะห์ผลการศึกษาของประเทศไทยเปรียบเทียบกับต่างประเทศ									■			
จัดทำข้อเสนอแนะแนวแก้ไขกฎหมายหรือกำหนดมาตรการเพื่อนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ในระบบงานยุติธรรมด้านการป้องกันและปราบปรามอาชญากรรม										■		
การจัดสัมมนารับฟังความคิดเห็น											■	
สรุปผลจากการรับฟังความคิดเห็นและแก้ไขรายงานวิจัย											■	
จัดทำรายงานวิจัยฉบับสมบูรณ์												■

6. ประโยชน์ที่คาดว่าจะได้รับ

การวิจัยนี้มีขอบเขตในการจัดทำแนวทางแก้ไขกฎหมายเพื่อวางกรอบการในการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปราบอาชญากรรมอย่างเป็นรูปธรรม ซึ่งแนวทางและข้อเสนอแนะดังกล่าวจะก่อให้เกิดประโยชน์ในหลายด้าน ดังนี้

1) ด้านเศรษฐกิจ ข้อมูลขนาดใหญ่ถือเป็นทรัพยากรที่มีคุณค่าทางเศรษฐกิจ เมื่อนำข้อมูลดังกล่าวมาใช้อย่างเหมาะสมเพื่อประโยชน์ในการเฝ้าระวัง ติดตามผู้กระทำความผิดและการป้องกันและปราบปรามอาชญากรรม จะช่วยลดภาระของภาครัฐ ทั้งด้านงบประมาณ ด้านกำลังพล ด้านอุปกรณ์เครื่องมือและลดต้นทุนในการดูแลผู้ต้องขังในเรือนจำ ทำให้ประเทศไทยมีความมั่นคงทางเศรษฐกิจจากการป้องกันและปราบปรามปัญหาอาชญากรรมที่มีประสิทธิภาพ

2) ด้านสังคม การมีมาตรการเฝ้าระวัง มาตรการป้องกันและปราบปรามอาชญากรรมที่รวดเร็ว ทันต่อสถานการณ์ มีประสิทธิภาพ จะทำให้อาชญากรรมลดน้อยลง ลดปัญหาภัยคุกคามที่เกิดต่อประชาชน เกิดความสงบสุข ความเป็นระเบียบเรียบร้อยและความปลอดภัยของสังคมและประชาชน

3) ด้านการมีส่วนร่วมของประชาชน ภาคประชาชนและสังคมจะเป็นแรงขับเคลื่อนสำคัญในการป้องกันและปราบปรามอาชญากรรม โดยจะมีส่วนร่วมในการสร้างข้อมูล แลกเปลี่ยนข้อมูลและการใช้ข้อมูล ขนาดใหญ่ร่วมกันระหว่างภาครัฐ ภาคเอกชนและประชาชน

4) ด้านวิชาการ งานวิจัยนี้เป็นองค์ความรู้ใหม่ด้านการนำนวัตกรรมมาใช้ในกระบวนการยุติธรรมทางอาญา หน่วยงานรัฐสามารถนำไปใช้เป็นแนวทางในการกำหนดนโยบายและยุทธศาสตร์ที่เกี่ยวข้อง และบุคคลทั่วไปสามารถนำไปใช้ประโยชน์หรืออ้างอิงทางวิชาการได้

บทที่ 2

ทบทวนวรรณกรรม

ในส่วนของการทบทวนวรรณจะกล่าวถึง แนวคิดและทฤษฎีที่เกี่ยวกับประเด็นวิจัย ประกอบด้วย แนวคิดนโนบาย Thailand 4.0 แนวคิดการปฏิรูปประเทศ แนวคิดตามยุทธศาสตร์ชาติและแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ยุทธศาสตร์สำนักงานตำรวจแห่งชาติ 20 ปี (พ.ศ. 2561 - 2580) แนวคิดและทฤษฎีการป้องกันและปราบปรามอาชญากรรม และแนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และแนวคิดการกำกับดูแลข้อมูลภาครัฐ (Government Data Governance) และเนื้อหาเกี่ยวกับการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้กับภารกิจในการป้องกันและปราบปรามอาชญากรรม ตลอดจนกฎหมายที่เกี่ยวข้อง รายละเอียดดังนี้

1. แนวคิดและทฤษฎีที่เกี่ยวข้อง

1.1 แนวคิดนโยบาย Thailand 4.0

เป็นวิสัยทัศน์เชิงนโยบายการพัฒนาเศรษฐกิจของประเทศไทยหรือโมเดลพัฒนาเศรษฐกิจของรัฐบาล ซึ่งมุ่งเน้นในเรื่องการพัฒนาสู่ “ความมั่นคง มั่งคั่ง และยั่งยืน”ด้วยการสร้าง “ความเข้มแข็งจากภายใน” ขับเคลื่อนตามแนวคิด “ปรัชญาเศรษฐกิจพอเพียง” ผ่านกลไก “ประชารัฐ” ทั้งนี้ การดำเนินการปรับเปลี่ยนให้ประเทศไทยสามารถมุ่งสู่ Thailand 4.0 ได้เป็นผลสำเร็จ จำเป็นต้องขับเคลื่อนผ่านกลไกภาครัฐ โดยได้กำหนดยุทธศาสตร์ชาติ 20 ปี เพื่อให้ภาครัฐปรับตัวให้เข้ากับเศรษฐกิจและสังคมยุค Digital นอกจากนี้ ยังยกระดับประสิทธิภาพการทำงานของรัฐบาลเข้าสู่การเป็นรัฐบาล Digital ที่มีการทำงานแบบอัจฉริยะ ให้บริการโดยมีประชาชนเป็นศูนย์กลาง และขับเคลื่อนให้เกิดการเปลี่ยนแปลงได้อย่างแท้จริงโดยอยู่บนพื้นฐานของการบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration) การนำเทคโนโลยีและอุปกรณ์ Digital มาสนับสนุนการปฏิบัติงาน (Smart Operations) ที่ประหยัดและคุ้มค่า และการยกระดับงานบริการภาครัฐให้ตรงกับความต้องการของประชาชนที่เปลี่ยนแปลงอยู่ตลอดเวลา (Citizen-centric Services) นโยบายดังกล่าว เป็นโอกาสที่เอื้อให้กระบวนการยุติธรรมซึ่งเป็นส่วนหนึ่งขององค์กรภาครัฐ ต้องทำการปฏิรูปงานใหม่ตามโมเดล Government 4.0 เพื่อให้มีความก้าวหน้าในเชิงรุกและมีประสิทธิภาพ รองรับการขับเคลื่อนประเทศเข้าสู่ยุค THAILAND 4.0

1.2 แนวคิดการปฏิรูปประเทศ

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ประกอบไปด้วย 16 หมวด 279 มาตรา มีจุดเด่นประการหนึ่งคือ การให้ความสำคัญกับการปฏิรูปประเทศ โดยบัญญัติให้การปฏิรูปประเทศเป็นหนึ่งหมวดในรัฐธรรมนูญ (หมวด 16 มาตรา 257 – มาตรา 261) และได้บัญญัติถึงเป้าหมายของการปฏิรูปประเทศไว้ 3 ประการ คือ 1) ประเทศชาติมีความสงบเรียบร้อย มีความสามัคคีปรองดอง มีการพัฒนาอย่างยั่งยืนตามหลักปรัชญาของเศรษฐกิจพอเพียง และมีความสมดุลระหว่างการพัฒนาด้านวัตถุกับการพัฒนาด้านจิตใจ 2) สังคมมีความสงบสุข เป็นธรรมและมีโอกาสอันทัดเทียมกันเพื่อขจัดความเหลื่อมล้ำ และ 3) ประชาชนมีความสุข มีคุณภาพชีวิตที่ดี และมีส่วนร่วมในการพัฒนาประเทศและการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข โดยกำหนดให้มีการดำเนินการปฏิรูปประเทศอย่างน้อยใน 7 ด้าน ได้แก่ ด้านการเมือง ด้านการบริหารราชการแผ่นดิน ด้านกฎหมาย ด้านกระบวนการยุติธรรม ด้านการศึกษา ด้านเศรษฐกิจ และด้านอื่น ๆ ดังนั้น กระบวนการยุติธรรมต้องดำเนินการปฏิรูปกระบวนการยุติธรรมเพื่อให้บรรลุเป้าหมายตามที่กำหนดไว้ในรัฐธรรมนูญและต้องดำเนินการปฏิรูปให้สอดคล้องกับยุทธศาสตร์ชาติและเป็นไปตามแผนที่กำหนด

1.3 แนวคิดตามยุทธศาสตร์ชาติและแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ

ประเทศไทยมียุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580) ที่รัฐบาลได้จัดทำขึ้นในกรอบระยะ 20 ปี เพื่อใช้เป็นกรอบทิศทางระยะยาวในการพัฒนาประเทศ โดยกำหนดเป้าหมายอนาคตประเทศไทยปี 2580 “ประเทศมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจ พอเพียง” ประกอบด้วย ยุทธศาสตร์ 6 ยุทธศาสตร์ โดยกำหนดการขับเคลื่อนเพื่อนำไปสู่การปฏิบัติเป็นระยะ ๆ ละ 5 ปี ได้แก่

1) ยุทธศาสตร์ด้านความมั่นคง

2) ยุทธศาสตร์ด้านการสร้างความสามารถในการแข่งขัน

3) ยุทธศาสตร์ด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์

4) ยุทธศาสตร์ด้านการสร้างโอกาสและความเสมอภาคทางสังคม

5) ยุทธศาสตร์ด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรต่อสิ่งแวดล้อม

6) ยุทธศาสตร์ด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ

สำหรับแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ. 2560 – 2564) จะเป็นแนวทางการพัฒนารองรับยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580) เพื่อเตรียมความพร้อมและวางรากฐานในการยกระดับประเทศไทยให้เป็นประเทศที่พัฒนาแล้ว โดยตอบสนองวัตถุประสงค์และเป้าหมายการพัฒนาตามยุทธศาสตร์ชาติ ในระยะเวลา 5 ปี จำนวน 10 ยุทธศาสตร์ ซึ่งประกอบด้วย ยุทธศาสตร์ชาติ 6 ยุทธศาสตร์ตามที่ได้กล่าวมาและอีก 4 ยุทธศาสตร์ที่เป็นกลไกสนับสนุนให้การดำเนินการตามยุทธศาสตร์ทั้ง 6 ด้านสัมฤทธิ์ผล ประกอบด้วย

1) ยุทธศาสตร์การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์

2) ยุทธศาสตร์การพัฒนาวิทยาศาสตร์ เทคโนโลยี วิจัยและนวัตกรรม

3) ยุทธศาสตร์การพัฒนาภาคเมืองและพื้นที่เศรษฐกิจ และ

4) ยุทธศาสตร์ความร่วมมือระหว่าง ประเทศเพื่อการพัฒนา

แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 จะเป็นแผนแรกที่ถูกใช้ให้เป็นกลไกเชื่อมโยงสู่การขับเคลื่อนการพัฒนา โดยได้กำหนดแนวทางการพัฒนาที่เกี่ยวกับกระบวนการยุติธรรมอยู่ใน 2 ยุทธศาสตร์ ได้แก่ ยุทธศาสตร์ที่ 2 การสร้างความเป็นธรรมและลดความเหลื่อมล้ำในสังคม โดยเพิ่มโอกาสให้กับกลุ่มเป้าหมายประชากรร้อยละ 40 ที่มีรายได้ต่ำสุดให้สามารถเข้าถึงบริการที่มีคุณภาพของรัฐ ซึ่งรวมถึงการเข้าถึงกระบวนการยุติธรรมด้วย และได้กำหนดตัวชี้วัด ให้มีการเข้าถึงกระบวนการยุติธรรมของกลุ่มประชากรที่มีฐานะยากจนเพิ่มขึ้น ยุทธศาสตร์ที่ 4 การบริหารจัดการในภาครัฐ การป้องกันการทุจริตประพฤติมิชอบ และธรรมาภิบาลในสังคมไทย โดยปฏิรูปกฎหมายและกระบวนการยุติธรรมให้มีความทันสมัยเป็นธรรม และสอดคล้องกับ ข้อบังคับสากลหรือข้อตกลงระหว่างประเทศ เพื่อคุ้มครองสิทธิเสรีภาพของประชาชนอย่างเสมอภาค ผู้มีส่วนได้ส่วนเสียมีความมั่นใจ ยอมรับ และปฏิบัติตามกติกา เอื้อต่อภารกิจภาครัฐ การลงทุนและดำเนินธุรกิจ ภาคเอกชน ดึงดูดการลงทุนจากต่างประเทศ ลดความเหลื่อมล้ำ และเพิ่มคุณภาพชีวิตของประชาชน ตลอดจนมีการบังคับใช้กฎหมายอย่างเคร่งครัด และมีประสิทธิภาพ รวมทั้งการวินิจฉัยคดีมีความถูกต้อง รวดเร็ว โปร่งใส และเป็นธรรม ตามหลักนิติธรรมและลดปริมาณผู้กระทำผิดในที่ควบคุม

1.4 ยุทธศาสตร์สำนักงานตำรวจแห่งชาติ 20 ปี (พ.ศ. 2561 - 2580)

ยุทธศาสตร์สำนักงานตำรวจแห่งชาติ 20 ปี (พ.ศ. 2561 - 2580) ฉบับนี้ จึงเป็นนโยบายและกรอบแนวทางในการบริหารและการปฏิบัติงานของสำนักงานตำรวจแห่งชาติ ซึ่งทุกหน่วยในสังกัด และข้าราชการตำรวจทุกนายจะต้องนำไปสู่การปฏิบัติเพื่อบรรลุสู่วิสัยทัศน์ “เป็นองค์กรบังคับใช้กฎหมาย ที่

ประชาชนเชื่อมั่นศรัทธา” และเป็นส่วนสำคัญในการสนับสนุนการพัฒนาประเทศให้เป็นไปตามเป้าหมายของยุทธศาสตร์ชาติต่อไป

ยุทธศาสตร์สำนักงานตำรวจแห่งชาติ 20 ปีประกอบด้วย 4 ยุทธศาสตร์ ได้แก่

1) การเสริมสร้างความมั่นคงของสถาบันหลักของชาติและการรักษาความมั่นคงภายในประเทศ
2) การเพิ่มศักยภาพในการบังคับใช้กฎหมาย การอำนวยความยุติธรรมทางอาญาและการให้บริการประชาชนอย่างเสมอภาคเป็นธรรม
3) การมีส่วนร่วมของภาคประชาชนในการรักษาความสงบเรียบร้อยของสังคมอย่างยั่งยืน
4) การพัฒนาองค์กรให้ทันสมัย มุ่งสู่ความเป็นเลิศ

สำหรับในส่วนที่เกี่ยวข้องกับการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปรามอาชญากรรมจะอยู่ในยุทธศาสตร์ที่ 2 และยุทธศาสตร์ที่ 4 รายละเอียดดังนี้

ยุทธศาสตร์ที่ 2 การเพิ่มศักยภาพในการบังคับใช้กฎหมาย การอำนวยความยุติธรรมทางอาญา และการให้บริการประชาชนอย่างเสมอภาคเป็นธรรม

ประเด็นยุทธศาสตร์ที่ 2.1 การป้องกันปราบปรามอาชญากรรมและการบังคับใช้กฎหมาย

กลยุทธ์

2.1.1 รักษาความปลอดภัยในชีวิตและทรัพย์สินของประชาชน โดยมุ่งเน้นการป้องกันอาชญากรรม

2.1.1.1 เพิ่มประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรม

2.1.1.2 พัฒนาระบบฐานข้อมูลและนำเทคโนโลยีที่ทันสมัยมาใช้ในการแก้ไขปัญหาอาชญากรรม

ยุทธศาสตร์ที่ 4 การพัฒนาองค์กรให้ทันสมัย มุ่งสู่ความเป็นเลิศ

ประเด็นยุทธศาสตร์ที่ 4.5. การยกระดับมาตรฐานการปฏิบัติงานให้มีความทันสมัย รองรับนโยบาย ประเทศไทย 4.0

กลยุทธ์

4.5.1 เพิ่มสมรรถนะขององค์กรในการตอบสนองต่อประชาชนในสถานการณ์ หรือภาวะฉุกเฉินให้สะดวกและรวดเร็ว

4.5.2 พัฒนาระบบการป้องกัน ติดตาม เฝ้าระวังและวิเคราะห์เหตุคุกคามทางเทคโนโลยีและนวัตกรรมดิจิทัล และจัดตั้งศูนย์ประสานงาน ด้าน Cyber crime

4.5.3 สร้างและพัฒนาระบบฐานข้อมูลกลางขององค์กร (Big Data) ให้ครอบคลุมทุกหน่วยงานและทันสมัย เพื่อสนับสนุนภารกิจตำรวจได้อย่างมีประสิทธิภาพและเชื่อมโยงกับส่วนราชการอื่นได้

4.5.4 พัฒนาและปรับวิธีการปฏิบัติงานระบบการบริหารจัดการด้านข้อมูล ข่าวสาร และการบริการประชาชนให้ทันสมัย โดยนำนวัตกรรม เทคโนโลยีและระบบการทำงานที่เป็นดิจิทัลมาใช้ในการบริหาร และการตัดสินใจ

4.5.5 พัฒนาศักยภาพและการจัดการความรู้ของบุคลากรทุกระดับชั้น ในด้านเทคโนโลยีนวัตกรรมดิจิทัล

4.5.6 กำหนดกรอบอัตราและจัดหาวัสดุอุปกรณ์ เครื่องมือเครื่องใช้ที่ทันสมัย ยานพาหนะทั้งทางบก ทางน้ำ ทางอากาศ ตลอดจนอาคารที่ทำการและที่พักอาศัย ให้เพียงพอและเหมาะสมต่อการปฏิบัติงาน

1.5 แนวคิดและทฤษฎีที่เกี่ยวข้องกับการป้องกันอาชญากรรม

แนวความคิดของ Brantingham และ Faust ได้กล่าวไว้ว่า การป้องกันปัญหาอาชญากรรมสามารถที่จะกระทำได้สามแนวทางด้วยกัน คล้ายๆ กับการป้องกันโรคหรือสุขภาพของคนเราการป้องกันเช่นว่านี้ คือ การป้องกันในขั้นแรก (Primary prevention) การป้องกันในระยะที่สอง (Secondary prevention) และ การป้องกันในขั้นที่สาม (Tertiary prevention) การป้องกันโรคในขั้นตอนแรก คือ การให้วัคซีนป้องกันโรค รวมทั้งการให้คำแนะนำการดูแลรักษาสุขภาพร่างกายให้ถูกสุขอนามัย โดยเจ้าหน้าที่สาธารณสุขเป็นผู้ให้คำแนะนำ การป้องกันในขั้นที่สอง คือ การป้องกันที่นอกเหนือจากการป้องกันที่สังคมหรือรัฐได้กระทำอยู่แล้วในเวลานั้น และนอกจากนั้น จะต้องมุ่งความสนใจไปที่ผู้ป่วยแต่ละรายรวมทั้งสถานการณ์ของโรคที่ปรากฏให้เห็นเด่นชัดว่า เป็นอาการของโรคที่เกิดขึ้นแล้ว รวมไปถึงการค้นหาสมมติฐานของโรคในแต่ละโรค และจะต้องมีระบบเตรียมการในการตรวจหาสมมติฐานของโรคดังกล่าวเป็นอย่างดีด้วย การป้องกันในขั้นที่สาม คือ การป้องกันในส่วนที่เหลือจากขั้นที่หนึ่ง และขั้นที่สอง คือ การป้องกันจากผู้ป่วยที่เป็นโรคชัดเจน หรืออาจจะกล่าวอีกนัยหนึ่งว่าเป็นการเยียวยารักษาผู้ป่วยให้หายขาด ไม่ให้เป็นโรคอีกครั้ง การป้องกันปัญหา

อาชญากรรมก็เช่นเดียวกันสามารถจะนำรูปแบบและวิธีการป้องกันโรคในทางการแพทย์มาใช้กับการป้องกันดังกล่าวนี้ได้[1]

การป้องกันอาชญากรรมในขั้นแรก (Primary Crime Prevention)

รูปแบบในการป้องกันปัญหาอาชญากรรมในขั้นนี้มีหลายรูปแบบ ในที่นี้จะหมายถึง การออกแบบสิ่งแวดล้อม (Environment design) การเฝ้าระวังของเพื่อนบ้าน (Neighborhood watch and citizen patrol) การเรียนรู้เกี่ยวกับอาชญากรรมและการป้องกันอาชญากรรม (Education about crime and crime prevention) ระบบความปลอดภัยส่วนบุคคล (Private securely)

- การออกแบบสิ่งแวดล้อม (Environment design) หมายถึง เทคนิคต่างๆ ในการป้องกันปัญหาอาชญากรรม เป้าหมายของเทคนิคเหล่านี้ก็เพื่อทำให้ผู้กระทำผิดได้ยากยิ่งขึ้น นอกจากนั้นยังหมายรวมถึงการเฝ้าระแวดระวังให้กับประชาชนผู้อยู่อาศัย การสร้างความรู้สึกปลอดภัยในชีวิตและทรัพย์สินของประชาชนให้แพร่หลายออกไปมากยิ่งขึ้น การวางแผนในการปลูกสร้างอาคารที่อยู่อาศัยให้ง่ายต่อการมองเห็น การติดตั้งแสงสว่างให้เพียงพอและการติดตั้งแบบการล็อคประตูให้แข็งแรงมั่นคง และการทำเครื่องหมายลงบนทรัพย์สินของตนเองเพื่อให้ง่ายต่อการแยกแยะและจดจำ

- การเฝ้าระวังของเพื่อนบ้าน (Neighborhood watch and citizen patrol) หมายถึง การเฝ้าระแวดระวังและการจัดสายตรวจเพื่อนบ้านเพื่อออกตรวจตรา และคอยสอดส่องดูแลซึ่งกันและกันเป็นการเพิ่มขีดความสามารถของชุมชนให้เสี่ยงต่อภัยอาชญากรรมให้ลดน้อยถอยลงการเรียนรู้เกี่ยวกับอาชญากรรมและการป้องกันอาชญากรรม (Education about crime and crime prevention) หมายถึง กิจกรรมต่างๆ ของงานยุติธรรมทางอาญาทั้งหลายทั้งปวงย่อมเกี่ยวข้องกับการป้องกันปัญหาอาชญากรรมในขั้นแรกทั้งนั้น อย่างเช่น กิจกรรมของเจ้าหน้าที่ตำรวจ การปรากฏตัวของเจ้าหน้าที่ตำรวจ ณ ที่ใดที่หนึ่งย่อมทำให้ประชาชนลดความหวาดกลัวอาชญากรรมลงไปในตัวด้วย ทางด้านงานศาลและงานราชทัณฑ์ก็เช่นเดียวกัน ศาลและราชทัณฑ์ช่วยให้ผู้กระทำผิดยอมรับถึงความเสี่ยงต่อการกระทำผิดของตนเองเพิ่มมากขึ้นเรื่อยๆ เหล่านี้ล้วนแต่เกี่ยวข้องกับการป้องกันในขั้นแรกทั้งสิ้น ส่วนภาครัฐก็จะมีส่วนเกี่ยวข้องกับการป้องกันในขั้นแรกเหมือนหน่วยงานในกระบวนการยุติธรรมอื่นๆ คือ มีส่วนช่วยให้

[1] Brantingham and Faust .(1976) A Conceptual Model of Crime Prevention . Crime Delinquency 22 , 1976 , pp 284-296 . อ้างถึงใน อุนิษา เลิศโตมรสกุล และ ผศ.ดร.ชาญคณิต กฤตยา สุริยะมณี, การศึกษาหาแนวทางในการป้องกันอาชญากรรมแบบไม่เป็นทางการ: กรณีศึกษาในเขตกรุงเทพมหานคร , กรุงเทพ : สำนักงานกิจการยุติธรรม , 2552 , หน้า 17.

ข้อมูลที่แท้จริงเกี่ยวกับความรุนแรงของอาชญากรรมในปัจจุบันที่หน่วยงานยุติธรรมต่างๆ จะต้องเข้าควบคุมและแก้ไข ซึ่งจะทำให้ประชาชนทั่วไปสามารถยอมรับความจริงอันนั้นได้

- ระบบความปลอดภัยส่วนบุคคล (Private securely) นั้น ก็มีส่วนเกี่ยวข้องกับการป้องกันในขั้นแรกเหมือนกัน คือ มีส่วนเกี่ยวข้องในรูปของการสนับสนุนหรือมีส่วนช่วยเหลือหน่วยงานในกระบวนการยุติธรรมทางอาญาต่างๆ อย่างเป็นทางการในการข่มขวัญและยับยั้งการกระทำผิดของอาชญากร

การป้องกันอาชญากรรมในเบื้องต้นหรือขั้นแรกจะเกี่ยวข้องกับประเด็นปัญหาทางสังคมอย่างวงกว้าง ซึ่งประเด็นปัญหาเหล่านี้ย่อมต้องเกี่ยวข้องกับปัญหาอาชญากรรมและพฤติกรรมเบี่ยงเบน กล่าวคือ การป้องกันปัญหาเหล่านี้บางครั้งต้องป้องกันทางสังคม (Social prevention)กิจกรรมในการป้องกันทางสังคมเหล่านี้ได้แก่ การแก้ไขปัญหาการว่างงาน การแก้ไขปัญหาการด้อยการศึกษา การแก้ไขปัญหาความยากจน นอกจากนั้น กิจกรรมเหล่านี้ยังหมายรวมถึงการแก้ไขพฤติกรรมเบี่ยงเบน โดยเน้นไปที่สาเหตุการเกิดพฤติกรรมดังกล่าว ซึ่งมีผลทำให้ปัญหาอาชญากรรมและความหวาดกลัวต่ออาชญากรรมลดลงตามไปด้วย อย่างไรก็ตาม การป้องกันปัญหาอาชญากรรมในขั้นแรกนี้ นอกจากจะเป็นการพยายามที่จะหลีกเลี่ยงพฤติกรรมเบี่ยงเบนและพฤติกรรมอาชญากรรมดังกล่าวนี้แล้ว การติดตามพฤติกรรมดังกล่าวยังรวมทั้งการตกเป็นผู้เสียหายหรือเหยื่ออาชญากรรม (Victimization) อาจเป็นหนทางหนึ่งที่ลดความหวาดกลัวต่อปัญหาอาชญากรรมลงได้ [2]

<u>การป้องกันอาชญากรรมในขั้นที่สอง</u> (Secondary Crime Prevention)

หมายถึง การพยายามที่จะเข้าใจถึงศักยภาพในการกระทำผิดของผู้กระทำผิดแล้วพยายามที่จะแทรกแซงหรือยับยั้งการกระทำผิดนั้นๆ หรือกล่าวได้อีกนัยหนึ่งว่า การป้องกันในขั้นที่สองนี้หมายถึง ความสามารถของสังคมและกระบวนการยุติธรรมในการที่จะกำหนดประเด็นปัญหาและการคาดคะเนหรือทำนายปัญหาที่เป็นอยู่ในเวลานั้นได้อย่างถูกต้องแม่นยำมากน้อยเพียงใด เพราะการเข้าแทรกแซงปัญหาผู้กระทำผิดนั้นได้ ส่วนใหญ่มาจากการที่ได้คาดคะเนหรือทำนายปัญหาจากตัวผู้กระทำผิดนั้นๆ เป็นหลัก

---

[2] Brantingham and Faust .(1976) A Conceptual Model of Crime Prevention . <u>Crime Delinquency</u> 22 , 1976 , pp 284-296 . อ้างถึงใน อุนิษา เลิศโตมรสกุล และ ผศ.ดร.ชาญคณิต กฤตยา สุริยะมณี, <u>การศึกษาหาแนวทางในการป้องกันอาชญากรรมแบบไม่เป็นทางการ: กรณีศึกษาในเขตกรุงเทพมหานคร</u> , กรุงเทพ : สำนักงานกิจการยุติธรรม , 2552 , หน้า 18.

ซึ่งรูปแบบในการป้องกันในขั้นที่สองนี้ก็คือ รูปแบบที่เรียกว่า การป้องกันจากสถานการณ์ที่เป็นจริงในเวลานั้น (Situational prevention) การป้องกันดังกล่าวนี้คือ การกำหนดประเด็นปัญหาให้แคบลงหรือเด่นชัดขึ้น แล้วเข้าทำการแทรกแซงแก้ไขปัญหานั้นๆ ให้ได้ผล รูปแบบในการป้องกันดังกล่าวนี้จะเกี่ยวข้องกับการเปลี่ยนแปลงแก้ไขในระบบการตรวจตราสอดส่องในชุมชน (Surveillance) รวมไปถึงการเปลี่ยนแปลงแก้ไขกิจกรรมที่สำคัญอื่นๆ ที่เกี่ยวข้องกับเรื่องนี้ด้วย กิจกรรมอันหนึ่งที่สำคัญ และมีความสัมพันธ์อย่างมากและมีความเหมาะสมกับการป้องกันในขั้นนี้มากที่สุดคือ กิจกรรมที่เรียกว่า “ตำรวจชุมชน” (Community Policing) ซึ่งเป็นวิธีการที่ต้องอาศัยชุมชนเข้ามาร่วมแก้ไขปัญหานั้นโดยตรง โดยเฉพาะการอาศัยเพื่อนบ้านเข้ามาแก้ไขปัญหาดังกล่าว อาจกล่าวได้ว่า วิธีการนี้เป็นวิธีการหนึ่งที่เหมาะสมในการป้องกันอาชญากรรมในขั้นที่สองนี้มากที่สุด การป้องกันปัญหาอาชญากรรมในขั้นที่สองนี้ได้ลอกเลียนแบบวิธีการในการป้องกันในขั้นแรกหลายวิธีการด้วยกัน แต่การป้องกันในขั้นนี้ก็มีข้อแตกต่างไปจากการป้องกันในแรกตรงที่ว่าการป้องกันในขั้นที่สอง เป็นการป้องกันจากสภาพปัญหาอาชญากรรมที่ปรากฏให้เห็นเด่นชัดหรือชัดเจนแล้วจึงพยายามเข้าดำเนินการแก้ไขปัญหาดังกล่าวนั้น แต่การป้องกันในขั้นที่หนึ่งสามารถป้องกันได้ตั้งแต่สภาพของปัญหานั้นยังไม่เกิด และการป้องกันในขั้นที่สองนี้ไม่เพียงแต่จะป้องกันปัญหาอาชญากรรมหลักๆ ดังที่ได้กล่าวแล้วเท่านั้นยังหมายรวมไปถึงการป้องกันการกระทำผิดของเด็กและเยาวชน รวมทั้งพฤติกรรมเบี่ยงเบนต่างๆ ที่เป็นอันตรายต่อสังคมด้วย ซึ่งจะเชื่อมโยงกับพฤติกรรมเบี่ยงเบนอื่นๆ อีกหลายรูปแบบ

<u>การป้องกันอาชญากรรมในขั้นที่สาม</u> (Tertiary Crime Prevention)

การป้องกันอาชญากรรมในขั้นนี้เป็นเรื่องของกระบวนการยุติธรรมที่จะต้องเข้ามาดำเนินการในเรื่องดังกล่าว อย่างเช่น การจับกุมของเจ้าหน้าที่ตำรวจ การสั่งฟ้องหรือไม่ฟ้องของพนักงานอัยการและการควบคุมกักขัง การบำบัดแก้ไขฟื้นฟูผู้กระทำผิดของเจ้าหน้าที่ราชทัณฑ์เหล่านี้ เป็นต้น การป้องกันในขั้นนี้ หัวใจหลักของการป้องกันคือ การป้องกันการกระทำผิดซ้ำ (Recidivism) ของผู้กระทำผิดไม่ให้กระทำผิดซ้ำขึ้นมาอีก กลยุทธ์หรือยุทธวิธีในการป้องกันในขั้นนี้ มีสองวิธีด้วยกัน วิธีแรกเรียกว่า การข่มขู่ยับยั้งเป็นกรณีพิเศษ (Specific deterrence) ส่วนวิธีที่สองเรียกว่า การลดความสามารถของผู้กระทำผิด (Incapacitation)

การข่มขู่ยับยั้งเป็นกรณีพิเศษ (Specific deterrence) หมายถึง ความพยายามที่จะป้องกันผู้ที่กระทำผิดไม่ให้กระทำผิดในรูปแบบอื่นๆ ขึ้นมาอีก เป็นการวางบทกำหนดโทษแก่ผู้กระทำผิดเอาไว้ซึ่งจะทำให้ผู้กระทำผิดหวาดกลัวและรู้สึกสูญเสียอิสรภาพตามมาตรการลดความสามารถของผู้กระทำ

ผิด (Incapacitation) เป็นการป้องกันอาชญากรรมมิให้เกิดขึ้นมาอีกในอนาคต โดยอาศัยการควบคุมผู้กระทำผิดแต่ละคนในช่วงเวลาใดเวลาหนึ่งเป็นหลักวิธีการควบคุมที่เป็นที่รู้จักกันแพร่หลายและเป็นหัวใจหลักของการลดขีดความสามารถของผู้กระทำผิดก็คือ การจำคุกหรือการกักขัง (Incapacitation) ซึ่งเป็นวิธีการที่จะสกัดกั้นการกระทำผิดของผู้กระทำผิดมิให้กระทำผิดขึ้นมาอีกในช่วงเวลาใดเวลาหนึ่ง ส่วนวิธีการควบคุมอื่นๆ ของ Incapacitation คือ วิธีการที่เรียกว่า การตรวจตราอย่างเข้มงวด (Intensive supervision) และการติดตามด้วยเครื่องมืออิเล็กทรอนิกส์ Electronic monitoring [3]

1.6 แนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

แนวคิดการคุ้มครองข้อมูลส่วนบุคคลตามกรอบการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดโดยองค์การร่วมมือและพัฒนาทางเศรษฐกิจ (OECD : The Organization for Economic Cooperation and Development) ใน OECD's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Dats มีหลักพื้นฐาน 8 ประการ กล่าวคือ 1) หลักข้อจำกัดในการเก็บรวบรวมข้อมูล 2) หลักคุณภาพของข้อมูล 3) หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ 4) หลักข้อจำกัดในการนำไปใช้ 5) หลักการรักษาความมั่นคงปลอดภัยข้อมูล 6) หลักการเปิดเผยข้อมูล 7) หลักการมีส่วนร่วมของบุคคล 8) หลักความรับผิดชอบ สำหรับประเทศไทยมีกฎหมายที่เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นสิทธิมนุษยชนขั้นพื้นฐานในปัจจุบันภายใต้หลักตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 กฎหมายที่ตราขึ้นเป็นกฎหมายกลางเพื่อคุ้มครองข้อมูลส่วนบุคคลคือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายเกี่ยวข้องอีกหลายฉบับ อาทิ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.7 แนวคิดการกำกับดูแลข้อมูลภาครัฐ (Government Data Governance)

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ได้กำหนดให้หน่วยงานภาครัฐทุกแห่งมีหน้าที่ในการกำกับดูแลข้อมูลขององค์กรให้ถูกต้องตรงกัน สมบูรณ์เป็น

[3] อุนิษา เลิศโตมรสกุล และ ผศ.ดร.ชาญคณิต กฤตยา สุริยะมณี, การศึกษาหาแนวทางในการป้องกันอาชญากรรมแบบไม่เป็นทางการ: กรณีศึกษาในเขตกรุงเทพมหานคร , กรุงเทพ : สำนักงานกิจการยุติธรรม , 2552 , หน้า 19- 20.

ปัจจุบัน ปลอดภัยและพร้อมใช้ตามกรอบธรรมาภิบาลข้อมูล (Data Governance Framework) ของสำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) โดยมีวัตถุประสงค์เพื่อนำไปสู่การให้บริการตามภารกิจขององค์กรอย่างมีประสิทธิภาพและสนับสนุนให้เกิดการใช้ประโยชน์ข้อมูลเชิงวิเคราะห์ประกอบการตัดสินใจวางแผนบริหารงาน การจัดทำยุทธศาสตร์และกำหนดนโยบายรวมทั้งการพัฒนากระบวนการทำงาน ทำให้มีประสิทธิภาพและเพิ่มความสามารถในการให้บริการประชาชนได้อย่างเป็นรูปธรรม นอกจากนี้ การกำกับดูแลข้อมูลที่เหมาะสมจะเอื้อให้หน่วยงานภาครัฐสามารถแลกเปลี่ยนข้อมูลระหว่างกันได้อย่างมีมาตรฐาน และพร้อมสำหรับการให้บริการข้อมูลเปิด (Open Data) อันจะเป็นประโยชน์แก่สาธารณะ

กรอบธรรมาภิบาลข้อมูลมีจุดประสงค์หลักเพื่อกำกับให้ข้อมูลมีความน่าเชื่อถือ ได้รับการกำกับดูแลอย่างเป็นระบบ และได้รับการปรับปรุงสม่ำเสมอ โดยเน้นให้ข้อมูล มีคุณภาพ ถูกต้อง สมเหตุสมผลเป็นปัจจุบัน ครบถ้วนสมบูรณ์และสอดคล้องกัน แนวทางการกำกับดูแลข้อมูลมีทั้งสิ้น 4 ขั้นตอน ดังต่อไปนี้[4]

1) การวางโครงสร้างบุคลากรและระบุความรับผิดชอบ (Organization and Stewardship)

การบริหารจัดการเรื่องธรรมาภิบาลข้อมูลนั้นมีความซับซ้อนและมีงานต่อเนื่องทั้งในมิติของการกำหนดกฎเกณฑ์นโยบาย และการวางระบบสารสนเทศเพื่อการกำกับดูแล ข้อมูลให้เป็นไปตามนโยบายองค์กร ดังนั้น การวางโครงสร้างบุคลากรเพื่อเป็นคณะกรรมการข้อมูล (Data Committee) ที่เหมาะสมจึงมีความจำเป็น โครงสร้างคณะกรรมการข้อมูลควรประกอบด้วยบุคลากร 3 กลุ่ม คือ

• ผู้บริหารระดับกลางและระดับสูงขององค์กร มีหน้าที่ในการประเมิน (Assess) และอนุมัติ (Approve) นโยบายด้านการกำกับดูแลข้อมูลขององค์กร ซึ่งควรมีการทบทวนเป็นระยะ ๆ เพื่อปรับให้ทันสมัย รวมทั้งมีหน้าที่ในการตัดสินใจเรื่องที่เกี่ยวข้องกับข้อมูลในมิติต่าง ๆ โดยเฉพาะการตัดสินใจเลือกหน่วยงานเจ้าของข้อมูล (Data Owner) สำหรับชุดข้อมูลที่มีการเก็บซ้ำซ้อนภายในองค์กร ทั้งนี้เพื่อให้เกิดความสอดคล้องของข้อมูลสำหรับการวิเคราะห์

• ตัวแทนกลุ่มผู้ใช้ข้อมูลหรือผู้มีส่วนเกี่ยวข้องหลัก (User/Stakeholder) จากส่วนงานต่าง ๆ มีหน้าที่ในการกำหนดสิทธิการเข้าถึงชุดข้อมูลของบุคลากรภายในและภายนอก รวมทั้งกำหนด

[4] สถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ (GBDi) , กรอบการวิเคราะห์ข้อมูลขนาดใหญ่ภาครัฐ (Government Big Data Analytics Framework), 2563, หน้า 34-40 ,

กฎเกณฑ์ในการกำกับดูแลชุดข้อมูลที่ส่วนงานตนเป็นเจ้าของและร่างนโยบาย เงื่อนไขการอนุมัติใช้ข้อมูลของบุคลากรภายนอกองค์กร

• เจ้าหน้าที่สารสนเทศข้อมูล (Data Custodian) มีหน้าที่ในการพัฒนา จัดหาระบบสารสนเทศเพื่อกำกับดูแลข้อมูลและจำกัดสิทธิในการเข้าถึงข้อมูลอย่างเป็นรูปธรรมตามนโยบายที่กำหนด

นอกจากนี้ คณะกรรมการข้อมูลยังมีหน้าที่ในการกำหนดโจทย์จากปัญหาหรือความท้าทายของแต่ละฝ่าย แผนกหรือส่วนงาน เพื่อใช้เป็นจุดตั้งต้นในการระบุชุดข้อมูลสำคัญขององค์กร และกำหนดผู้ควบคุมข้อมูล (Data Controller) ผู้ใช้ข้อมูล (Data User) และ ผู้ประมวลข้อมูล (Data Processor) สำหรับแต่ละชุดข้อมูลรวมทั้งมีหน้าที่ในการทำงานร่วม กับบริกรข้อมูล (Data Steward) เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยอีกด้วย

2) การจัดทำนโยบายการบริหารจัดการข้อมูล (Data Management Policy)

สิ่งที่คณะกรรมการข้อมูลต้องดำเนินการในลำดับแรกคือการกำหนดนโยบาย เพื่อการบริหารจัดการข้อมูลอย่างเป็นระบบแบ่งได้เป็น 4 มิติหลัก ดังนี้

1) การจัดการวงจรชีวิตข้อมูล (Data Lifecycle) : ดำเนินการวางกลไก เพื่อจัดการข้อมูลตามวงจรชีวิตที่เริ่มจากการสร้าง (Create) จัดเก็บ (Store) ใช้ประโยชน์ (Use) สำรองข้อมูล (Archive) และทำลายข้อมูล (Destroy) โดยระบุกระบวนการและกฎเกณฑ์ที่จำเป็นในแต่ละช่วงชีวิตของข้อมูลสำหรับชุดข้อมูลดิจิทัลขององค์กร ทั้งนี้ เพื่อประสิทธิภาพในการบริหารจัดการ คณะกรรมการข้อมูลสามารถเริ่มจากการนำร่องชุด ข้อมูลสำคัญบางส่วนก่อนเพื่อลดความยุ่งยากและประหยัดงบประมาณ ในช่วงแรกควรเลือกส่วนงานนำร่องและรายชุดข้อมูลเพื่อจัดทำ “รายการชุดข้อมูล” หรือ Data Catalog โดยมีการใส่ “รายละเอียดชุดข้อมูล” (Metadata) ตามที่ สพร.กำหนด

2) การวางนโยบายด้านความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy) : ร่างนโยบายด้านการป้องกันข้อมูลในบริบทของการรักษาความลับ ความพร้อมใช้งาน ความถูกต้องของข้อมูลตามมาตรฐาน ISO/ IEC27001 มีรายละเอียดดังนี้

• การรักษาความลับ (Confidentiality) หมายถึง การรักษาข้อมูลตามสภาพของการจัดชั้นความลับและมีการกำหนดสิทธิการเข้าถึงชุดข้อมูลอย่างชัดเจนตามระดับชั้นความลับโดยส่วนงานที่เป็นเจ้าของข้อมูล ทั้งนี้กฎการใช้ข้อมูลรวมถึงการเพิ่ม ลบ แก้ไข ประมวลผล นำไปใช้ แลกเปลี่ยนและเปิดเผยข้อมูล ซึ่งต้องสอดคล้องกับกฎหมาย เงื่อนไข และข้อกำหนดต่าง ๆ รวมถึงการคำนึงถึงมูลค่า

ความสำคัญและ ความอ่อนไหวของข้อมูล การกำหนดกฎเกณฑ์ที่เป็นรูปธรรมที่ชัดเจน จะทำให้เจ้าหน้าที่สารสนเทศข้อมูลสามารถพัฒนาเงื่อนไขหรือข้อกำหนดในโปรแกรมทำให้ควบคุมการเข้าถึงเพื่อรักษาความลับและลดความเสี่ยงของการถูกคุกคาม เพื่อเป็นการป้องกันการดัดแปลง แก้ไข แต่งเติม โดยไม่ได้รับอนุญาต และการรั่วไหลของข้อมูลอีกด้วย

• ความพร้อมใช้งาน (Availability) หมายถึง การพร้อมในการใช้งานอยู่เสมอ ผู้ใช้งานสามารถใช้ข้อมูลตามสิทธิได้ทันทีและได้อย่างต่อเนื่อง รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ที่ไม่คาดคิด

• ความถูกต้องของข้อมูล (Integrity) หมายถึง การคงสภาพของข้อมูลหรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูกเปลี่ยนแปลงโดยผู้ไม่มีสิทธิ เช่น ข้อมูลที่ใช้จะต้องเป็นข้อมูลที่ถูกต้องอย่างแท้จริง ไม่มีการดัดแปลงหรือแก้ไข

3) การประกันคุณภาพของข้อมูล (Data Quality Assurance) : เพื่อประกันความน่าเชื่อถือของข้อมูลและประสิทธิภาพของการนำข้อมูลไปใช้คณะกรรมการข้อมูลควรมีการวางแผนการด้านการประกันคุณภาพข้อมูลโดยมีการระบุเกณฑ์การวัดคุณภาพสำหรับ ข้อมูลแต่ละชุดและมีการกำหนด KPIs ที่ใช้วัดคุณภาพ รวมถึงกลไกการตรวจสอบคุณภาพที่ชัดเจนเป็นระบบ เพื่อเป็นการตรวจสอบผลลัพธ์หรือความสำเร็จจากการกำกับดูแลข้อมูล องค์ประกอบในการประเมินคุณภาพตามกรอบการกำกับดูแลข้อมูลของ สพร. ประกอบด้วย

• ข้อมูลมีความถูกต้อง (Accuracy) ขึ้นอยู่กับวิธีการที่ใช้ในการควบคุมข้อมูลนำเข้า และการควบคุมการประมวลผล ซึ่งวิธีการควบคุม การประมวลผล ได้แก่ การตรวจสอบยอดรวมที่ได้จากการประมวลผลแต่ละครั้ง หรือการตรวจสอบผลลัพธ์ที่ได้จากการประมวลผลด้วยเครื่องคอมพิวเตอร์ ส่วนการควบคุมการนำเข้าสามารถใช้วิธีสุ่มตรวจข้อมูลได้

• ข้อมูลมีความครบถ้วน (Completeness) ข้อมูลบางประเภทหากไม่ครบถ้วนก็จัดเป็นข้อมูลด้อยคุณภาพได้เช่นกัน เช่น ข้อมูลประวัติผู้รับการรักษาพยาบาล หากไม่มีหมู่เลือดของผู้รับการรักษาพยาบาล จะไม่สามารถใช้ได้ในกรณีที่ต้องการข้อมูลหมู่เลือดของผู้รับการรักษาพยาบาล

• ข้อมูลมีความต้องกัน (Consistency) หมายถึงค่าของข้อมูลในชุดเดียวกัน ควรสอดคล้องกับค่าในชุดข้อมูลอื่น หากมีการดึงข้อมูลสองค่าจากชุดข้อมูลต่างแหล่งกัน ข้อมูลต้องไม่ขัดแย้งกัน

• ข้อมูลมีความเป็นปัจจุบัน (Timeliness) หมายถึง ผู้ใช้สามารถนำเอาผลลัพธ์ที่ได้ไปใช้ได้ทันเวลา นั่นคือ จะต้องมีการจัดเก็บข้อมูลที่รวดเร็ว เพื่อให้ทันความต้องการของผู้ใช้

• ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy) หมายถึง ระดับของข้อมูลที่บริหารจัดการต้องนำเสนอได้ตรงและมีประสิทธิภาพสามารถใช้งานได้ตามวัตถุประสงค์

• ข้อมูลมีความพร้อมใช้ (Availability) หมายถึง ข้อมูลมีความพร้อมในการใช้งานอยู่เสมอ เข้าถึงได้ง่าย ใช้งานได้จริงและใช้งานได้ตลอดเวลา

4) การแลกเปลี่ยนข้อมูล (Data Exchange) : การแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอกองค์กรจะเป็นรูปธรรมได้นั้น คณะกรรมการข้อมูลต้องมีการวางนโยบาย ที่ชัดเจน โดยมีการจัดทำข้อกำหนดและเงื่อนไข (Terms and Conditions) ที่จะใช้สำหรับการแลกเปลี่ยนข้อมูลทั้งการส่งออกและนำเข้าข้อมูล มีมาตรการและกลไกการแลกเปลี่ยนข้อมูล รวมถึงประเด็นเรื่องความจำเป็นในการเข้ารหัส (Encrypt) และผู้ดูแลจัดเก็บกุญแจ ถอดรหัส (Key) กรณีข้อมูลมีชั้นความลับ นโยบายและแนวทางที่ชัดเจนจะลดความเสี่ยงให้ ส่วนงานสารสนเทศข้อมูลและสนับสนุนให้การบริหารจัดการแลกเปลี่ยนข้อมูลมีประสิทธิภาพ ประเด็นเรื่องการเชื่อมโยงแลกเปลี่ยนข้อมูลตามกรอบการกำกับดูแลข้อมูลของ สพร.กำหนดหัวข้อไว้ดังนี้

• กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัยคุณภาพข้อมูลและผู้ประสานงานหรือศูนย์ติดต่อ

• กำหนดกระบวนการในการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้ชัดเจน เริ่มต้นตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอน ระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

• กำหนดเมทาดาต้าของชุดข้อมูลที่ต้องการเชื่อมโยงและแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

• ทำสัญญาอนุญาตหรือข้อตกลงในการเชื่อมโยงและแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

• กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

• บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

• สามารถตรวจสอบได้ว่าการเชื่อมโยงและแลกเปลี่ยนได้ดำเนินการ อย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติกระบวนการเชื่อมโยง และแลกเปลี่ยนและมาตรฐานตามที่กำหนด

3) การตรวจประเมินธรรมาภิบาลข้อมูล (Audit)

องค์กรควรมีหน่วยงานภายในที่ได้รับมอบหมายให้ตรวจสอบธรรมาภิบาลข้อมูล (Internal Auditor) เพื่อเป็นการประกันคุณภาพโดยการตรวจสอบผลลัพธ์และความสำเร็จจากการกำกับดูแลข้อมูล นอกจากนี้ หน่วยงานกลางภาครัฐโดยสำนักงานสถิติแห่งชาติ (สสช.) และ สพร. (External Auditor) จะมีกระบวนการตรวจสอบด้านธรรมาภิบาลข้อมูลหน่วยงานภาครัฐเพื่อเป็นการประกันคุณภาพอีกต่อหนึ่งโดยองค์ประกอบ ในการตรวจประเมินคุณภาพ ประกอบด้วย

• การปฏิบัติตามการจัดการความเสี่ยงด้านข้อมูล (DataRisk Management) ตามนโยบายบริหารความเสี่ยงที่กำหนดโดยคณะกรรมการข้อมูล

• การปฏิบัติตามระเบียบและกฎหมายที่เกี่ยวข้องกับข้อมูล (Law and Regulation Compliance)

• การตรวจสอบคุณภาพข้อมูล (Data Quality Audit) เป็นการตรวจสอบกระบวนการที่เกี่ยวข้องกับข้อมูล

4) การสร้างความตระหนักและองค์ความรู้ในองค์กร (Building Knowledge and Awareness)

การกำกับดูแลข้อมูลเป็นสิ่งที่ทุกคนในองค์กรต้องให้ความร่วมมือ หากบุคลากรในองค์กรไม่มีความเข้าใจในวัตถุประสงค์ของการกำกับดูแลข้อมูล หรือไม่ตระหนักถึงความสำคัญของการกำกับดูแลข้อมูลก็จะส่งผลให้การดำเนินการด้านนี้ไม่มีประสิทธิผลและไม่เกิดประโยชน์อย่างแท้จริง ดังนั้นองค์กรควรมีแผนและนโยบายในการสร้างความตระหนักรู้ รวมทั้งให้ความรู้เกี่ยวกับธรรมาภิบาลข้อมูล และมีการกระตุ้นให้บุคลากรทุกส่วนให้ความ สำคัญและมีโอกาสได้นำความรู้ที่ได้ไปปรับใช้ในการทำงาน โดยมีการจัดอบรมหลักสูตรที่รวมถึงการสร้างองค์ความรู้(Program Coverage) การวัดผล (Measurement) และความต่อเนื่อง (Ongoing) ของการดำเนินงานด้านธรรมาภิบาลข้อมูล

2. กฎหมายเกี่ยวข้องกับการนำข้อมูลขนาดใหญ่มาใช้ในการป้องกันและปราบปรามอาชญากรรม

2.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตราขึ้นเพราะความก้าวหน้าทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็วและแนวโน้มเกิดการละเมิดสิทธิในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวมีเพิ่มมากขึ้น โดยเฉพาะการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์หรือเปิดเผยโดยมิชอบหรือโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล เพื่อประโยชน์ในทางการค้า หรือเพื่อประโยชน์ในการนำข้อมูลส่วนบุคคลไปใช้ในการกระทำความผิดต่าง ๆ เช่น การฉ้อโกง การหมิ่นประมาท เป็นต้น ซึ่งปัญหาเหล่านี้ย่อมส่งผลกระทบต่อความเชื่อมั่นในการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามนโยบายของรัฐบาล ดังนั้น ประเทศไทยจึงจำเป็นต้องมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เพื่อสร้างกลไกการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นมาตรฐานเดียวกันและสอดคล้องกับมาตรฐานที่เป็นสากล โดยต้องไม่สร้างภาระหน้าที่แก่ผู้เกี่ยวข้องจนกลายเป็นข้อจำกัดหรืออุปสรรคในการประกอบธุรกิจการค้าหรือการให้บริการของภาคส่วนต่าง ๆ จนเกินสมควร เพื่อแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ โดยกฎหมายจะมีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 เป็นไปตามพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ฉบับที่ 2) พ.ศ. 2564

หลักการพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีขอบเขตบังคับใช้กับทุกองค์กรที่มีการ เก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) กล่าวคือ กฎหมายกำหนดหน้าที่ในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลในการเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลของผู้อื่น การโอนข้อมูล การรักษาความปลอดภัยของข้อมูล การให้สิทธิตรวจสอบ แก้ไข ลบแก่เจ้าของข้อมูลส่วนบุคคล ซึ่งผู้ควบคุมข้อมูลจำเป็นต้องปฏิบัติให้ถูกต้องตามกฎหมาย อาทิ เรื่องการขอความยินยอม (Consent Form) การจัดให้มีนโยบายความเป็นส่วนตัว (Privacy Policy) และต้องเตรียมความพร้อมเพื่อจัดให้มีเอกสาร สัญญา และกระบวนการต่าง ๆ รวมทั้งหน้าที่ในการกำหนดมาตรการรักษาความปลอดภัยของข้อมูลตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด เช่น ผู้ควบคุมข้อมูลส่วนบุคคลต้องขอความความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (มาตรา 19) ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (มาตรา 24 หรือมาตรา 26) ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำ

การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง (มาตรา 27) เว้นแต่เป็นกรณีที่กฎหมายกำหนดให้สามารถกระทำได้ เป็นต้น ดังนั้น องค์กรจำเป็นต้องดำเนินการให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อวางแนวปฏิบัติในการเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลของผู้อื่น การโอนข้อมูล การรักษาความปลอดภัยของข้อมูล กระบวนการรองรับการใช้สิทธิของเจ้าของข้อมูล รวมทั้งตรวจสอบและจัดทำเอกสารกฎหมายที่เกี่ยวข้องตามที่กฎหมายกำหนด

สาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โครงสร้างของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล แบ่งเป็น 7 หมวด โดยสรุปดังนี้

- บทบัญญัติทั่วไป (มาตรา 1 – มาตรา 7) เป็นส่วนที่กำหนดเกี่ยวกับเรื่องผลบังคับใช้ของกฎหมาย และ บทนิยามตามพระราชบัญญัตินี้

- หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ระบุกฎเกณฑ์ คุณสมบัติ รวมถึงอำนาจหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล หมวดนี้แบ่งเนื้อหาออกเป็น 4 ส่วน คือ

ส่วนที่ 1 บททั่วไป (มาตรา 19-มาตรา 21) วางเงื่อนไขเกี่ยวกับฐานหรือเหตุของการประมวลผลข้อมูลส่วนบุคคลเช่นเดียวกับ GDPR ที่เรียกว่า “Lawful processing of personal data” โดยเงื่อนไขหลักของการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลคือต้องขอความยินยอมจากเจ้าของข้อมูล เว้นแต่เข้าเหตุอื่นที่กฎหมายกำหนด เช่น การปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ส่วนที่ 2 การเก็บรวบรวมข้อมูล (มาตรา 22 – มาตรา 26) บทบัญญัติในส่วนนี้ขยายความฐานหรือเหตุในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลทั่วไป และ ข้อมูลส่วนบุคคลชนิดพิเศษตามที่ระบุในมาตรา 26 เช่น ข้อมูลสุขภาพ ข้อมูลชีวภาพ รวมถึงหลักเกณฑ์เกี่ยวกับการแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ (Privacy notice or privacy statement)

ส่วนที่ 3 การใช้และการเปิดเผยข้อมูลส่วนบุคคล (มาตรา 27 – มาตรา 29) บทบัญญัติส่วนนี้กำหนดหลักเกณฑ์ในเรื่องการใช้ และ เปิดเผยข้อมูลส่วนบุคคล ซึ่งเป็นจุดที่แตกต่างจาก GDPR ที่กำหนดรวมการใช้และเปิดเผยอยู่ในความหมายของการ “ประมวลผลข้อมูลส่วนบุคคล” (Processing)

- หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล (มาตรา 30 – 42) บทบัญญัติส่วนนี้กำหนดในเรื่องของสิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น สิทธิขอเข้าถึง สิทธิขอแก้ไข สิทธิขอคัดค้าน สิทธิขอลบข้อมูล หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

- หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 43 – มาตรา 70) กำหนดจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อำนาจหน้าที่ของสำนักงาน รวมถึงคุณสมบัติของพนักงานเจ้าหน้าที่ของสำนักงาน

- หมวด 5 การร้องเรียน (มาตรา 71 – มาตรา 78) กำหนดหลักเกณฑ์และขั้นตอนการร้องเรียนเกี่ยวกับการฝ่าฝืน หรือ ไม่ปฏิบัติตามพระราชบัญญัตินี้รวมทั้งกระบวนการระงับข้อพิพาทเช่นการไกล่เกลี่ย

- หมวด 6 ความรับผิดทางแพ่ง (มาตรา 77 – มาตรา78) กำหนดการเยียวยาความเสียหายของเจ้าของข้อมูลจากการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามพระราชบัญญัตินี้ รวมถึงการกำหนดให้ศาลมีอำนาจพิจารณาให้ผู้ฝ่าฝืนชำระค่าสินไหมทดแทนเชิงลงโทษ (Punitive damage)

- หมวด 7 บทกำหนดโทษ แบ่งเป็น 2 ส่วนคือ

ส่วนที่ 1 โทษอาญา (มาตรา 79 – มาตรา 81)

ส่วนที่ 2 โทษทางปกครอง (มาตรา 82 – มาตรา 90)

- บทเฉพาะกาล (มาตรา 91 – มาตรา 96) กำหนดเรื่องการจัดการของหน่วยงานรัฐในระหว่างพระราชบัญญัตินี้ยังไม่มีผลบังคับและวางหลักเกี่ยวกับข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมมาก่อนที่พระราชบัญญัตินี้มีผลใช้บังคับ

2.2 พระราชบัญญัติตำรวจแห่งชาติ พ.ศ. 2547

ฐานอำนาจตามกฎหมายที่สำนักงานตำรวจแห่งชาติในการใช้ประโยชน์จากข้อมูลขนาดใหญ่ในการป้องกันและปราบปรามอาชญากรรม ได้แก่ พระราชบัญญัติตำรวจแห่งชาติ พ.ศ. 2547 บัญญัติให้สำนักงานตำรวจแห่งชาติมีอำนาจหน้าที่เกี่ยวกับการป้องกันและปราบปราม การกระทำความผิดทางอาญา รักษาความสงบเรียบร้อย ความปลอดภัยของประชาชนและความมั่นคงของราชอาณาจักร และปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของข้าราชการตำรวจ หรือสำนักงานตำรวจแห่งชาติ ตามความในมาตรา 6 (3) (4) และ (5)[5]

[5] พระราชบัญญัติตำรวจแห่งชาติ พ.ศ. 2547 “มาตรา 6 สำนักงานตำรวจแห่งชาติเป็นส่วนราชการมีฐานะเป็นนิติบุคคลอยู่ในบังคับบัญชาของนายกรัฐมนตรี และมีอำนาจหน้าที่ดังต่อไปนี้

(1) รักษาความปลอดภัยสำหรับองค์พระมหากษัตริย์ พระราชินี พระรัชทายาท ผู้สำเร็จราชการแทนพระองค์ พระบรมวงศานุวงศ์ ผู้แทนพระองค์ และพระราชอาคันตุกะ

ประกอบกับอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญาที่บัญญัติความหมายของคำว่า “การสืบสวน” หมายความถึงการแสวงหาข้อเท็จจริงและหลักฐานซึ่งพนักงานฝ่ายปกครองหรือตำรวจได้ปฏิบัติไปตามอำนาจและหน้าที่ เพื่อรักษาความสงบเรียบร้อยของประชาชน และเพื่อที่จะทราบรายละเอียดแห่งความผิด และ “การสอบสวน” หมายความถึงการรวบรวมพยานหลักฐานและการดำเนินการทั้งหลายอื่นตามบทบัญญัติแห่งประมวลกฎหมายนี้ ซึ่งพนักงานสอบสวนได้ทำไปเกี่ยวกับความผิดที่กล่าวหา เพื่อที่จะทราบข้อเท็จจริงหรือพิสูจน์ความผิดและเพื่อจะเอาตัวผู้กระทำผิดมาฟ้องลงโทษ และบัญญัติให้ตำรวจมีอำนาจในการสืบสวนคดีอาญาหรือบัญญัติให้พนักงานสอบสวนมีอำนาจออกหมายเรียกบุคคลเพื่อประโยชน์แห่งการรวบรวมหลักฐาน ตามความในมาตรา 2 (10)[6] และ (11)[7] และมาตรา 17[8]

2.3 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ในปัจจุบันมีกฎหมายที่เกี่ยวข้องกับการบริหารจัดการข้อมูลขนาดใหญ่ภาครัฐ ได้แก่ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 โดยกฎหมายฉบับนี้จะช่วยในการขับเคลื่อนให้เกิดการปฏิรูปการบริหารราชการแผ่นดินและการบริการประชาชนตามบทบัญญัติแห่งรัฐธรรมนูญและตามยุทธศาสตร์ชาติ โดยยกระดับการบริหารงานและการให้บริการภาครัฐจากรูปแบบเดิมไปสู่

---

(2) ดูแลควบคุมและกำกับการปฏิบัติงานของข้าราชการตำรวจซึ่งปฏิบัติการตามประมวลกฎหมายวิธีพิจารณาความอาญา

(3) ป้องกันและปราบปรามการกระทำความผิดทางอาญา

(4) รักษาความสงบเรียบร้อย ความปลอดภัยของประชาชนและความมั่นคงของราชอาณาจักร

(5) ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของข้าราชการตำรวจหรือสำนักงานตำรวจแห่งชาติ

(6) ช่วยเหลือการพัฒนาประเทศตามที่นายกรัฐมนตรีมอบหมาย

(7) ปฏิบัติการอื่นใดเพื่อส่งเสริมและสนับสนุนให้การปฏิบัติการตามอำนาจหน้าที่ตาม (1) (2) (3) (4) หรือ (5) เป็นไปอย่างมีประสิทธิภาพ ...”

[6] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (10) “การสืบสวน” หมายความถึงการแสวงหาข้อเท็จจริงและหลักฐานซึ่งพนักงานฝ่ายปกครองหรือตำรวจได้ปฏิบัติไปตามอำนาจและหน้าที่ เพื่อรักษาความสงบเรียบร้อยของประชาชนและเพื่อที่จะทราบรายละเอียดแห่งความผิด

[7] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (11) “การสอบสวน” หมายความถึงการรวบรวมพยานหลักฐานและการดำเนินการทั้งหลายอื่นตามบทบัญญัติแห่งประมวลกฎหมายนี้ ซึ่งพนักงานสอบสวนได้ทำไปเกี่ยวกับความผิดที่กล่าวหา เพื่อที่จะทราบข้อเท็จจริงหรือพิสูจน์ความผิดและเพื่อจะเอาตัวผู้กระทำผิดมาฟ้องลงโทษ

[8] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 17 พนักงานฝ่ายปกครองหรือตำรวจมีอำนาจทำการสืบสวนคดีอาญาได้

การดำเนินการและให้บริการผ่านระบบดิจิทัล ทั้งนี้ โดยมีระบบการทำงานแบบบูรณาการและมีการเชื่อมโยงข้อมูลระหว่างหน่วยงานของรัฐโดยใช้เทคโนโลยีดิจิทัลอย่างมั่นคงปลอดภัย รวมทั้งยังมีการเปิดเผยข้อมูลเปิดภาครัฐผ่านระบบดิจิทัลเพื่อให้การใช้ประโยชน์ในข้อมูลเป็นไปอย่างคุ้มค่า อันจะส่งผลให้การบริหารราชการแผ่นดินและการให้บริการประชาชนของหน่วยงานของรัฐเป็นไปอย่างมีประสิทธิภาพ รวดเร็ว ลดขั้นตอน เปิดเผย และโปร่งใส ประชาชนจะได้รับประโยชน์ทั้งในแง่ของความสะดวกในการรับบริการจากภาครัฐและยังสามารถตรวจสอบการดำเนินงานของหน่วยงานของรัฐได้ นอกจากนี้ การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัลยังมีส่วนสำคัญในการขับเคลื่อนการพัฒนาประเทศในด้านต่าง ๆ ให้มีความเจริญก้าวหน้ามากยิ่งขึ้น[9]

กฎหมายนี้กำหนดให้หน่วยงานของรัฐมีหน้าที่ต้องดำเนินการให้เป็นไปตามแผนพัฒนารัฐบาลดิจิทัล รวมทั้งมาตรฐาน ข้อกำหนด หลักเกณฑ์และวิธีการที่กำหนดขึ้นตามกฎหมายเพื่อให้หน่วยงานของรัฐเกิดการพัฒนาระบบการทำงานและระบบข้อมูลด้วยเทคโนโลยีดิจิทัลอย่างสอดคล้องเชื่อมโยงกัน เพื่อเพิ่มประสิทธิภาพการบริหารงานและการให้บริการภาครัฐ โดยมีคณะกรรมการพัฒนารัฐบาลดิจิทัลที่มีนายกรัฐมนตรีเป็นประธานทำหน้าที่กำกับดูแล รวมถึงขับเคลื่อนภารกิจและแผนพัฒนารัฐบาลดิจิทัลตามกฎหมายนี้

หน่วยงานที่อยู่ภายใต้กฎหมายฉบับนี้ ได้แก่ หน่วยงานของรัฐต่างๆ ทั้งราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การมหาชน รัฐสภา ศาล องค์กรอิสระตามรัฐธรรมนูญ องค์กรอัยการ สถาบันอุดมศึกษาของรัฐ และหน่วยงานอิสระของรัฐ แต่สำหรับกรณีของศาล กฎหมายนี้มุ่งหมายให้ครอบคลุมเพียงในส่วนที่ไม่เกี่ยวกับการพิจารณาอรรถคดี ส่วนหน่วยงานของรัฐสภาก็มุ่งหมายเฉพาะหน่วยงานธุรการของรัฐสภาเท่านั้น

สาระสำคัญกำหนดไว้ในมาตรา 4 กล่าวคือ เพื่อให้การบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวกรวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน ให้หน่วยงานของรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัลโดยมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล โดยมุ่งหมายในการเพิ่ม

---

[9] สำนักงานคณะกรรมการกฤษฎีกา, บันทึกวิเคราะห์สรุปสาระสำคัญของร่างพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. .... , สืบค้นเมื่อ 6 กุมภาพันธ์ 2564
https://www.krisdika.go.th/data/comment/comment_lawdraft/2561/2065_2561_0126.htm

ประสิทธิภาพและอำนวยความสะดวกในการให้บริการและการเข้าถึงของประชาชน และในการเปิดเผยข้อมูลภาครัฐต่อสาธารณะและสร้างการมีส่วนร่วมของทุกภาคส่วน

สรุปสาระสำคัญของพระราชบัญญัติฯ

1) กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบของเทคโนโลยีดิจิทัล โดยมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล โดยมุ่งหมายในการเพิ่มประสิทธิภาพและอำนวยความสะดวกในการให้บริการประชาชน และในการเปิดเผยข้อมูลภาครัฐต่อสาธารณะและสร้างการมีส่วนร่วมของทุกภาคส่วน

2) กำหนดให้มีแผนพัฒนาระบบรัฐบาลดิจิทัลเพื่อกำหนดกรอบและทิศทางการบริหารงานภาครัฐและการจัดทำบริการสาธารณะในรูปแบบของเทคโนโลยีดิจิทัลที่สอดคล้องกับวัตถุประสงค์ตามพระราชบัญญัตินี้ ยุทธศาสตร์ชาติ และแผนระดับชาติที่เกี่ยวข้อง โดยหน่วยงานของรัฐต้องดำเนินการตามแผนพัฒนาระบบรัฐบาลดิจิทัล รวมทั้งต้องจัดทำหรือปรับปรุงแผนปฏิบัติการหรือแผนงานของหน่วยงานของรัฐให้สอดคล้องกับแผนพัฒนาระบบรัฐบาลดิจิทัล

3) กำหนดให้มีคณะกรรมการพัฒนาระบบรัฐบาลดิจิทัลเพื่อทำหน้าที่จัดทำแผนพัฒนาระบบรัฐบาลดิจิทัลเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาอนุมัติ กำหนดนโยบาย หลักเกณฑ์ วิธีการ และมาตรฐานในการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัลตามพระราชบัญญัตินี้ ตลอดจนกำกับและติดตามให้หน่วยงานของรัฐมีการดำเนินการให้เป็นไปตามแผนพัฒนาระบบรัฐบาลดิจิทัล

4) กำหนดให้สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ทำหน้าที่เป็นหน่วยงานกลางในการอำนวยการ สนับสนุน และส่งเสริมการดำเนินงานเกี่ยวกับการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล และทำหน้าที่อำนวยการและสนับสนุนการปฏิบัติงานตามที่คณะกรรมการพัฒนาระบบรัฐบาลดิจิทัลมอบหมาย รวมทั้งรับผิดชอบงานธุรการและวิชาการของคณะกรรมการพัฒนาระบบรัฐบาลดิจิทัล

5) กำหนดให้หน่วยงานของรัฐมีหน้าที่ต้องจัดทำข้อมูลตามภารกิจให้อยู่ในรูปแบบข้อมูลดิจิทัล จัดทำกระบวนการหรือการดำเนินงานทางดิจิทัลเพื่อการบริหารราชการแผ่นดินและการให้บริการประชาชน จัดให้มีระบบการรับชำระเงินจากประชาชนผ่านระบบดิจิทัลเพิ่มอีกช่องทางหนึ่งจัดให้มีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล จัดให้มีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการเข้าสู่บริการดิจิทัลของหน่วยงานของรัฐ จัดให้มีการพัฒนาทักษะบุคลากรภาครัฐให้มีความรู้ความสามารถในการดำเนินงานด้านการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล โดยต้องมีการทบทวนและประเมินแผนการ

ดำเนินงาน นโยบาย และแนวปฏิบัติเกี่ยวกับการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัลของหน่วยงานของรัฐอย่างน้อยปีละหนึ่งครั้ง

6) กำหนดให้มีการแลกเปลี่ยนหรือเชื่อมโยงข้อมูลดิจิทัลระหว่างหน่วยงานของรัฐตามหลักเกณฑ์และวิธีการที่คณะกรรมการพัฒนาระบบรัฐบาลดิจิทัลกำหนด รวมทั้งกำหนดหน้าที่หน่วยงานของรัฐผู้รับข้อมูลดิจิทัลให้ดูแลรักษาข้อมูลและใช้ข้อมูลโดยไม่ทำให้สาระสำคัญของข้อมูลดังกล่าวผิดจากความเป็นจริง โดยมีศูนย์แลกเปลี่ยนข้อมูลกลางแห่งชาติในสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ทำหน้าที่ในการประสานและสนับสนุนการแลกเปลี่ยนข้อมูลและเชื่อมโยงข้อมูลระหว่างหน่วยงานของรัฐและหน่วยงานที่เกี่ยวข้อง

7) กำหนดให้หน่วยงานของรัฐสามารถขอเชื่อมโยงข้อมูลส่วนบุคคลจากหน่วยงานของรัฐแห่งอื่นที่มีข้อมูลส่วนบุคคลในความครอบครองเพื่อนำมาวิเคราะห์หรือประมวลผลได้ แต่ห้ามเปิดเผยต่อสาธารณะและกระทำการใดอันทำให้เจ้าของข้อมูลนั้นได้รับความเสียหาย

8) กำหนดให้หน่วยงานของรัฐเปิดเผยข้อมูลตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบดิจิทัลต่อสาธารณะ โดยต้องให้ประชาชนทั่วไปสามารถเข้าถึงได้อย่างเสรีและไม่เสียค่าใช้จ่าย โดยมีศูนย์กลางข้อมูลเปิดภาครัฐในสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ทำหน้าที่ประสานข้อมูลจากหน่วยงานของรัฐและเปิดเผยแก่ประชาชน และข้อมูลที่นำมาเปิดเผยดังกล่าวต้องเป็นไปในแนวทางและมาตรฐานเดียวกันตามที่คณะกรรมการพัฒนาระบบรัฐบาลดิจิทัลกำหนด [10]

9) กำหนดให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล

ศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล โดยจะไม่กระทบต่อความร่วมมือระหว่างหน่วยงานของรัฐที่ได้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลกันอยู่ก่อนแล้ว โดยเฉพาะระบบการเชื่อมโยงแลกเปลี่ยนข้อมูลเฉพาะด้านเพื่อการบริหารงานราชการ เช่น การเชื่อมโยงแลกเปลี่ยนข้อมูลทรัพยากรน้ำ เป็นต้น ทั้งนี้

[10] เรื่องเดียวกัน

ศูนย์แลกเปลี่ยนข้อมูลกลางจะมีการพัฒนารูปแบบการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างหน่วยงานรัฐที่ลดกระบวนการและขั้นตอนเดิมๆ โดยเฉพาะการทำบันทึกข้อตกลงความร่วมมือ (MOU) และมีกลไกที่ทำให้การเปิดเผยและเข้าถึงข้อมูลระหว่างหน่วยงานของรัฐมีความโปร่งใสตรวจสอบได้ โดยลดความกังวลด้านความรับผิดทางกฎหมายของหน่วยงานที่เป็นเจ้าของข้อมูล เนื่องด้วยกฎหมายฉบับนี้มีเจตนารมณ์ต้องการให้หน่วยงานของรัฐเกิดการบูรณาการฐานข้อมูลของภาครัฐทุกหน่วยงานเข้าด้วยกันให้เป็นระบบข้อมูล เพื่อประโยชน์ในการบริหารราชการแผ่นดินและอำนวยความสะดวกให้แก่ประชาชน โดยการนำเทคโนโลยีดิจิทัลมาใช้เป็นเครื่องมือในการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน

10) เพื่อให้การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัลเป็นไปตามวัตถุประสงค์และเกิดการบูรณาการร่วมกัน กำหนดให้หน่วยงานของรัฐจัดทำธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงานและดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ โดยธรรมาภิบาลข้อมูลภาครัฐ คือ การกำหนดกฎเกณฑ์หรือระเบียบแบบแผนของหน่วยงานของรัฐในเรื่องการบริหารจัดการบรรดาข้อมูลที่อยู่ในความครอบครองของหน่วยงานของรัฐตลอดช่วงชีวิตของข้อมูล เพื่อให้ข้อมูลมีคุณภาพสามารถนำมาใช้ประโยชน์รวมถึงเชื่อมโยงแลกเปลี่ยนระหว่างหน่วยงานได้ มีการกำหนดสิทธิ หน้าที่และความรับผิดชอบของผู้มีส่วนเกี่ยวข้องในหน่วยงานที่สามารถเข้าถึงหรือใช้ประโยชน์ในข้อมูล และต้องมีการกำหนดหลักเกณฑ์เพื่อคุ้มครองสิทธิในข้อมูลส่วนบุคคลของประชาชนตลอดจนความมั่นคงปลอดภัยของข้อมูลที่สำคัญของรัฐ ทั้งนี้ คณะกรรมการพัฒนารัฐบาลดิจิทัลจะจัดทำธรรมาภิบาลข้อมูลภาครัฐที่เป็นกรอบใหญ่ หลังจากนั้นหน่วยงานของรัฐมีหน้าที่จัดทำธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน และต้องดำเนินการให้เป็นไปตามข้อปฏิบัติในธรรมาภิบาลข้อมูลภาครัฐที่กำหนดขึ้น[11]

2.4 กฎหมายเกี่ยวกับการกำหนดนโยบายและการขับเคลื่อนการพัฒนาระบบดิจิทัลในภาครัฐ

(1) พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560 ซึ่งบัญญัติหลักการและกลไกในการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของประเทศ โดยให้มีนโยบาย และแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมและกองทุนพัฒนาดิจิทัล เพื่อเศรษฐกิจและสังคมเป็นกลไก

[11] ข้อมูลจากเว็บไซต์ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) , www.dga.or.th , สืบค้นเมื่อ 17 พฤศจิกายน 2563.

สำคัญ เพื่อการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร ในด้านดิจิทัลอย่างเป็นระบบอันจะนำไปสู่การพัฒนาทั้งทางด้านเศรษฐกิจและสังคมของประเทศ

(2) พระราชบัญญัติสภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย พ.ศ. 2562 ซึ่งจัดตั้งสภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย มีวัตถุประสงค์ในการเป็นตัวแทน ของสมาชิกผู้ประกอบธุรกิจหรืออุตสาหกรรมดิจิทัล ในการเสนอความเห็น ประสานงาน และสนับสนุนการดำเนินงานด้านนโยบายระหว่างภาครัฐและเอกชนเกี่ยวกับธุรกิจหรืออุตสาหกรรม ดิจิทัล รวมทั้งเสนอความเห็นและข้อเสนอแนะต่อภาครัฐในเรื่องกฎหมายที่เกี่ยวข้องกับธุรกิจ หรืออุตสาหกรรมดิจิทัล

(3) พระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562 ซึ่งจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ มีวัตถุประสงค์ในการส่งเสริมและสนับสนุนการพัฒนา ธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์ของประเทศ เพื่อเป็นกลไกในการขับเคลื่อน นโยบายและแผนของรัฐด้านธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์ รวมทั้งส่งเสริมให้เกิด การพัฒนามาตรฐานและกฎเกณฑ์ในการใช้งานเทคโนโลยีดิจิทัลเพื่อให้ระบบงานเทคโนโลยีดิจิทัลต่าง ๆ เชื่อมโยงกันได้อย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และมีความน่าเชื่อถือ

(4) พระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. 2561 ซึ่งจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เป็นหน่วยงานกลางของระบบรัฐบาลดิจิทัล ทำหน้าที่ให้บริการส่งเสริมและสนับสนุนการดำเนินงานของหน่วยงานของรัฐ และหน่วยงานอื่นที่เกี่ยวกับการพัฒนารัฐบาลดิจิทัล ตั้งแต่โครงสร้างพื้นฐานทางเทคโนโลยีดิจิทัล แอปพลิเคชันพื้นฐานเกี่ยวกับรัฐบาลดิจิทัล รวมทั้งจัดทำมาตรฐาน หลักเกณฑ์ และวิธีการทางเทคโนโลยีดิจิทัลเพื่อให้สามารถเชื่อมโยงข้อมูลและระบบการทำงานระหว่างกันของหน่วยงานได้

3. การใช้ข้อมูลขนาดใหญ่ (Big Data) กับภารกิจในการป้องกันและปราบปรามอาชญากรรม

ข้อมูลขนาดใหญ่ (Big Data) คือ ข้อมูลขนาดใหญ่ หรือมีปริมาณมาก หรือข้อมูลจำนวนมากมหาศาล ทุกเรื่อง ทุกแง่มุม ทุกรูปแบบ ซึ่งอาจเป็นข้อมูลที่มีโครงสร้างชัดเจน (Structured Data) เช่น ข้อมูลที่เก็บอยู่ในตารางข้อมูลต่างๆ หรืออาจเป็นข้อมูลกึ่งมีโครงสร้าง (Semi-Structured Data) เช่น ล็อกไฟล์ (Log files) หรือแม้กระทั่งข้อมูลที่ไม่มีโครงสร้าง (Unstructured Data) เช่น ข้อมูลการโต้ตอบปฏิสัมพันธ์ผ่านสังคมเครือข่าย (Social Network) เช่น Facebook, twitter หรือ ไฟล์จำพวกมีเดีย เป็นต้น ซึ่งอาจจะเป็นข้อมูลภายในองค์กรและภายนอกที่มาจากการติดต่อระหว่างองค์กร หรือจากทุกช่องทางการ

ติดต่อกับลูกค้า แต่ทั้งหมดนี้ก็ยังคงเป็นเพียงข้อมูลดิบที่รอการนำมาประมวลและวิเคราะห์เพื่อนำผลที่ได้มาสร้างมูลค่าทางธุรกิจ ข้อมูลเหล่านี้อาจจะไม่ได้อยู่ในรูปแบบที่องค์กรสามารถนำไปใช้ได้ทันที แต่อาจมีข้อมูลที่เป็นประโยชน์ต่อองค์กรบางอย่างแฝงอยู่[12]

คุณสมบัติของข้อมูลขนาดใหญ่ (Big Data)

เทคโนโลยี Big Data ประกอบด้วยฮาร์ดแวร์และซอฟต์แวร์ที่ควบรวม (integrate) จัดระเบียบ (organize) บริหารจัดการ (manage) และนำเสนอข้อมูล (present) ที่มีลักษณะเป็น 3 V ดังต่อไปนี้

ปริมาณ (volume) คือขนาดของข้อมูล ซึ่งการวัดว่า “มาก” หรือ “น้อย” นั้นไม่ได้มีตัวเปรียบเทียบที่แน่นอน ขึ้นอยู่กับแต่ละอุตสาหกรรม องค์กร หรือแอพพลิเคชัน โดยในความเป็นจริงแล้วขนาดมิได้สำคัญเท่ากับอัตราการเพิ่มขึ้นของข้อมูลเมื่อเทียบกับวิธีการแบบดั้งเดิม

ความหลากหลาย (variety) คือประเภทของตัวข้อมูลและแหล่งที่มาของข้อมูลที่แตกต่างกัน ซึ่งนี่คือลักษณะสำคัญของข้อมูลที่กำลังเป็นเปลี่ยนไป ความท้าทายที่มาพร้อมกับการเปลี่ยนแปลงนี้คือการจัดเก็บ วิเคราะห์ และดึงเอาข้อมูลเชิงลึก (insight) ออกมาจากข้อมูลเหล่านี้

ความเร็ว (velocity) คือความเร็วของการเปลี่ยนแปลงของข้อมูล ซึ่งส่งผลให้เทคโนโลยีการวิเคราะห์ข้อมูลที่มีความสามารถในการวิเคราะห์ในช่วงเวลาสั้น ๆ นั่นคือในระดับนาที มิใช่ระดับชั่วโมงหรือระดับวัน กลายเป็นเทคโนโลยีสำคัญสำหรับองค์กรที่ต้องการตอบสนองต่อสภาพตลาดและความต้องการของลูกค้าที่เปลี่ยนไปอย่างรวดเร็ว หรือแม้กระทั่งการตรวจจับหลักฐานการทุจริตต่าง ๆ[13]

ปัจจุบันสำนักงานตำรวจแห่งชาติได้มีการนำระบบเทคโนโลยีสารสนเทศที่ใช้สนับสนุนการปฏิบัติงานตามภารกิจดังต่อไปนี้

1) ระบบตรวจสอบลายพิมพ์นิ้วมืออัตโนมัติ (AFIS) และระบบทะเบียนประวัติอาชญากร (CDOS) สามารถตรวจสอบได้ว่า บุคคลที่พิมพ์มือ ส่งมาตรวจพิสูจน์เคยกระทำผิดทางอาญามาก่อนแล้วหรือไม่ ถ้ามีกระทำความผิดในเรื่องใด เป็นต้น

---

[12] ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม , Bid Data, สืบค้นเมื่อ 15 ธันวาคม 2563, https://www.ops.go.th/main/index.php/knowledge-base/article-pr/657-big-data.

[13] สำนักงานส่งเสริมเศรษฐกิจดิจิทัล, “รู้จักกับบิ๊กดาต้า Big Data Ecosystems” สืบค้นเมื่อ 3 พฤศจิกายน 2563, https://www.depa.or.th/th/article-view/big-data-ecosystems.

2) ระบบคอมพิวเตอร์ประกอบภาพใบหน้าคนร้าย (PICASSO) ใช้เพื่อหาภาพสเก็ตคนร้ายหรือผู้ต้องสงสัย เพื่อนำไปสู่การออกหมายเรียก หมายจับ หรือการจับตัวคนร้ายต่อไป

3) ระบบการติดต่อสื่อสารและควบคุมรถสายตรวจ C3I และรถยนต์ไฟฟ้าตรวจการณ์อัจฉริยะ (Smart Patrol Car) โดยศูนย์วิทยุมีคู่สายจำนวนมาก ทำให้สามารถรับแจ้งเหตุจากสถานีตำรวจหรือรถยนต์สายตรวจได้อย่างรวดเร็วและมีประสิทธิภาพ เมื่อรับแจ้งเหตุแล้วศูนย์วิทยุสามารถสั่งการและควบคุมเจ้าหน้าที่และรถสายตรวจให้เข้าระงับเหตุได้อย่างรวดเร็ว พร้อมทั้งแจ้งข้อมูลอาชญากรรม สถิติและกำลังพลที่มีในระบบให้แก่เจ้าหน้าที่ตำรวจในขณะออกไประงับเหตุได้ พร้อมทั้งบันทึก จัดเก็บข้อมูล สถิติอาชญากรรมเข้าสู่ระบบและให้ข้อมูลที่เป็นประโยชน์แก่ผู้บังคับบัญชาเพื่อการสั่งการหรืออำนวยการต่อเจ้าหน้าที่สายตรวจในขณะออกไประงับเหตุได้

4) ระบบสารสนเทศของสำนักงานตำรวจแห่งชาติ (POLIS) มีระบบงาน 6 กลุ่มประกอบด้วยข้อมูลจำนวน 26 ฐานข้อมูล ในขณะที่ระบบ Crime ซึ่งเป็นระบบสารสนเทศข้อมูลอาชญากรรมที่คล้ายคลึงกันดำเนินการโดยสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สามารถจำแนกผู้ใช้เป็น 5 กลุ่ม ได้แก่

1) กลุ่มระบบงานบันทึก (Data Entry)

2) กลุ่มระบบงานสืบค้นข้อมูล (Data Search)

3) กลุ่มระบบงานบริการข้อมูลอิเล็กทรอนิกส์ (e-Data Services)

4) กลุ่มระบบแจ้งเตือน (Alarm & Alert Services)

5) กลุ่มระบบงานบริหารจัดการข้อมูลและระบบ (Data & System Management)

ทั้งนี้ระบบ POLIS และระบบ Crime มีวัตถุประสงค์เพื่อการจัดเก็บข้อมูล ควบคุมข้อมูล และระบบตรวจสอบข้อมูลที่ส่วนกลางหรือที่สำนักงานตำรวจแห่งชาติ โดยให้บริการข้อมูลอิเล็กทรอนิกส์ต่อเจ้าหน้าที่ตำรวจผู้ปฏิบัติงานและผู้บริหาร สามารถใช้และเข้าถึงระบบฐานข้อมูล สามารถสืบค้นข้อมูลได้

5) ระบบ E-COP เป็นการรวบรวมการให้บริการด้านเอกสารอิเล็กทรอนิกส์ โดยทำหน้าที่ศูนย์กลางในการรวบรวมข้อมูลและสนับสนุนการปฏิบัติงานราชการของเจ้าหน้าที่ตำรวจในสังกัดได้อย่างครอบคลุม มีความง่ายในการใช้ ทำให้การทำงานมีความสะดวกรวดเร็ว ประหยัดค่าใช้จ่าย มีความโปร่งใสตรวจ สอบได้ ในการส่งเอกสารระหว่างหน่วยต่างๆ นอกจากนี้ ยังช่วยลดจำนวนบุคลากรด้านการรับส่งเอกสาร ตลอดจนสามารถให้บริการแก่ประชาชนได้อย่างรวดเร็วทันต่อเหตุการณ์

6) ระบบ I2 เป็นโปรแกรมใช้เพื่อวิเคราะห์เครือข่ายอาชญากรรมและเชื่อมโยงเหตุการณ์ พยาน หลักฐาน บุคคล มือถือ บัญชีธนาคาร รถยนต์และอื่นๆ เพื่อใช้งานด้านการสืบสวน เป็นการแยกองค์ประกอบความสัมพันธ์ในแต่ละส่วนออกมาเป็นแผนผัง (Mind Map) สร้างเส้นเวลา (Timeline) ตลอดจนการเชื่อมโยงทางโทรศัพท์ ทางการเงิน บุคคลทาง Facebook ทำให้งานที่มีความยุ่งยาก ซับซ้อนให้ดูเรียบง่าย กระชับและนำกราฟิกมาใช้ในการนำเสนอแสดงความสัมพันธ์ของสิ่งต่างๆ ที่นำเข้าสู่โปรแกรมออกมาเป็นแผนภูมิแสดงความ สัมพันธ์ที่เรียกว่า Link Chart ได้

7) ระบบกล้องวงจรปิด (CCTV) สามารถบันทึกเหตุการณ์ โดยภาพนิ่ง ภาพเคลื่อนไหว เสียงได้ตลอดเวลา เมื่อมีเหตุการณ์เกิดขึ้นสามารถดูเหตุการณ์ย้อนหลังได้และเป็นพยานหลักฐานในการพิจารณาคดีได้ ทั้งนี้ เพื่อทราบถึงการกระทำผิดทางอาญา ตลอดจนทำให้ทราบถึงผู้กระทำผิดทางอาชญากรรมนั้นด้วย

8) ระบบจำแนกลักษณะบุคคล (Bio-Metrics) เป็นระบบที่จัดเก็บลักษณะอัตลักษณ์ของบุคคลทางกายภาพ ได้แก่ ลายพิมพ์นิ้วมือจำนวน 10 นิ้ว และระบบจดจำใบหน้า (Face Recognition) แล้วส่งข้อมูลเข้าสู่ระบบคอมพิวเตอร์ จัดเก็บไว้ในแม่ข่าย (Server) เมื่อปฏิบัติงานก็นำลายพิมพ์นิ้วมือและรายละเอียดของใบหน้าทำการเปรียบเทียบกับฐานข้อมูลเดิมในแม่ข่ายเพื่อตรวจสอบ ยืนยันตัวบุคคลและตรวจสอบบุคคลต้องห้าม (Blacklist) ทำให้ป้องกันการปลอมแปลงเอกสารหรือหนังสือเดินทาง ตรวจสอบผู้ก่อการร้ายข้ามชาติ ตรวจสอบผู้ต้องหาหลบหนี ตรวจสอบบุคคลต้องห้าม สร้างมาตรฐานความปลอดภัยในการพิสูจน์ตัวบุคคล ยกระดับการตรวจคนเข้าเมืองเทียบเท่าระดับสากล สร้างความประทับใจและความเชื่อมั่นให้กับนักลงทุนต่างชาติและนักท่องเที่ยวต่างชาติ ทั้งนี้ ระบบจำแนกลักษณะบุคคล (Bio-Metrics) สามารถลดต้นทุนการจัดการ โดยใช้เวลาในการตรวจสอบอัตลักษณ์น้อย ทำให้อำนวยความสะดวกแก่ผู้เข้าและออกประเทศรวมถึงนักท่องเที่ยวได้อย่างมีประสิทธิภาพ[14]

9) ระบบ crimes หรือ Criminal Record Information and Management Enterprise System หรือระบบสารสนเทศของสำนักงานตำรวจแห่งชาติ ระบบใหม่เป็นระบบที่รวมรวมข้อมูลคดีแบบละเอียด ทำให้เป็นแหล่งข้อมูลที่มีค่าอย่างมาก ใช้ในงานป้องกัน ปราบปราม สืบสวน สอบสวน นอกจากนี้ระบบยังวิเคราะห์ข้อมูลและออกรายงานในรูปแบบที่ผู้บริหารสามารถนำไปประกอบการตัดสินใจ วางแผนและกำหนดนโยบายได้อย่างมั่นใจอีกด้วย ซึ่งนับว่าเป็นระบบที่มีประโยชน์อย่างมากต่องานตำรวจ

---

[14] สมญัติ คำปาละ, การวิเคราะห์การใช้และประโยชน์ ระบบข้อมูลขนาดใหญ่ของ สำนักงานตำรวจแห่งชาติ, วารสารสหวิทยาการ วิทยาลัยสหวิทยาการ มหาวิทยาลัยธรรมศาสตร์ , ปีที่ 17 ฉบับที่ 1 (มกราคม 2563 – มิถุนายน 2563) , หน้า 106 – 109.

ระบบ crimes เกิดขึ้นจากการที่สำนักงานเทคโนโลยีสารสนเทศและการสื่อสารได้จัดทำโครงการพัฒนาเทคโนโลยีสารสนเทศสถานีตำรวจ เพื่อพัฒนาและเพิ่มประสิทธิภาพให้กับสถานีตำรวจทั่วประเทศและหน่วยงานที่มีอำนาจในการสืบสวนสอบสวนคดีอาญา ซึ่งในปัจจุบันยังขาดการสนับสนุนเทคโนโลยีสารสนเทศที่ทันสมัยในการปฏิบัติหน้าที่โดยจะทำการเชื่อมโยงเครือข่ายระหว่างหน่วยงานที่มีอำนาจในการสืบสวนสอบสวนของสำนักงานเทคโนโลยีสารสนเทศและการสื่อสารกับหน่วยงานกลางที่มีหน้าที่บันทึกและจัดเก็บข้อมูลที่จำเป็นสำหรับงานสืบสวนสอบสวน เพื่อให้หน่วยงานที่มีอำนาจในการสืบสวนสอบสวนสามารถบันทึก จัดเก็บและเรียกใช้ข้อมูลจากฐานข้อมูลกลางเดียวกันได้เสร็จสิ้น ณ หน่วยงานนั้นๆ และสามารถประสานงานแลกเปลี่ยนข้อมูลระหว่างหน่วยงานอย่างรวดเร็ว ลดความซ้ำซ้อนของการนำเข้าและการจัดเก็บข้อมูล เป็นวิธีลดขั้นตอนและระยะเวลาการปฏิบัติงานและรองรับการที่จะประสานงานแลกเปลี่ยนข้อมูลร่วมกับหน่วยงานต่างๆในกระบวนการยุติธรรม และหน่วยงานอื่นๆ ซึ่งจะมีขึ้นในอนาคต การจัดหาระบบคอมพิวเตอร์ในโครงการพัฒนาเทคโนโลยีสารสนเทศสถานีตำรวจเป็นงานที่ต้องอาศัยความรู้และประสบการณ์เฉพาะด้านเนื่องจากระบบงานดังกล่าวใช้เทคโนโลยีสมัยใหม่ที่มีความซับซ้อน ในการออกแบบเพื่อให้สนองรับต่อความต้องการใช้ระบบของสถานีตำรวจการจัดหาระบบต้องเสียเวลา การจัดเตรียมและดำเนินการอย่างมากจะต้องทำโดยความรอบคอบและระมัดระวังโดยอาศัยความรู้ทางศาสตร์เกี่ยวกับเครือค่ายระบบคอมพิวเตอร์การบริหารและดำเนินโครงการ

ขอบเขตการทำงานของระบบ CRIMES มีดังนี้

- ระบบบันทึกข้อมูล คดีอาญาทั่วไป คดีอุบัติเหตุจราจร เหตุทรัพย์หาย เหตุรถหาย เหตุคนหายพลัดหลง เหตุคนตาย ไม่ทราบชื่อ แผนประทุษกรรม เหตุที่ต้องรายงาน
- ระบบบันทึกและติดตามบุคคลพ้นโทษ
- ระบบการออกคำขอหมายจับ ประกาศสืบจับ และถอนประกาศสืบจับ
- ระบบการออกคำขอต่างๆ เช่น หมายจับ ผัดฟ้อง ฝากขัง
- ระบบบันทึกการปล่อยตัวชั่วคราวและการให้ประกันตัว
- ระบบการขออายัดตัวและการรับรองการอายัดตัว
- ระบบบันทึกผลการตรวจสอบประวัติ

- ระบบรับเอกสารอิเล็กทรอนิกส์ (e-Form)[15]

จากข้างต้น ระบบเทคโนโลยีที่มีรูปแบบการทำงานที่เป็นการใช้ข้อมูลขนาดใหญ่ (Big Data) ในงานของตำรวจ ได้แก่ ระบบกล้องวงจรปิด ทำให้เกิดประโยชน์กับสำนักงานตำรวจแห่งชาติหลายประการคือ

1) ระบบกล้องวงจรปิดป้องกันการกระทำผิดทางอาญา เมื่อติดกล้องวงจรปิดตามสถานที่ต่างๆ เมื่อผู้ที่จะกระทำผิดทางอาญา พบเห็นกล้องวงจรปิด จะทำให้เกิดความกลัวที่จะถูกบันทึกว่าได้กระทำผิด บางส่วนจึงไม่กล้ากระทำผิดทางอาญา หรือเลิกล้มความตั้งใจที่จะกระทำความผิดนั้นๆ

2) ระบบกล้องวงจรปิดช่วยในการปราบปรามผู้กระทำผิดทางอาญา ได้แก่

(2.1) ระบบกล้องวงจรปิด ช่วยบันทึกข้อมูลเหตุการณ์ต่างๆ ได้ ประมาณ 1 เดือน หรือ 30 วัน หลังจากนั้นจึงบันทึกซ้ำ เมื่อมีการกระทำผิดทางอาญา สามารถตรวจสอบย้อนหลังทำให้ทราบว่ามีการกระทำผิดทางอาญาเกิดขึ้น

(2.2) ระบบกล้องวงจรปิด สามารถตรวจสอบย้อนหลังได้ว่า เมื่อมีการกระทำผิดทางอาญาเกิดขึ้น ใครเป็นผู้กระทำผิด ซึ่งนำไปสู่การจับกุมผู้กระทำผิดได้อย่างรวดเร็ว

(2.3) ข้อมูลที่บันทึกได้จากกล้องวงจรปิด สามารถนำมาเป็นพยานหลักฐานในการพิจารณาคดี นำไปสู่การลงโทษผู้กระทำความผิดได้

(2.4) ข้อมูลที่บันทึกได้จากกล้องวงจรปิด สามารถเป็นพยานหลักฐานในการพิจารณาคดีได้ในเวลานาน หากมีการเก็บข้อมูลอย่างถูกต้องและปลอดภัย โดยเป็นพยานหลักฐานได้ดีกว่าพยานบุคคลที่เห็นเหตุการณ์เนื่องจากเมื่อระยะเวลาผ่านไปเป็นเวลานาน พยานบุคคลไม่สามารถจดจำหรืออาจจะลืมเหตุการณ์ต่างๆ ได้

3) ระบบกล้องวงจรปิดทำให้เฝ้าตรวจได้ตลอดเวลา ตลอด 24 ชั่วโมง ต่อวันและเฝ้าได้หลายจุดหรือหลายๆ สถานที่ ซึ่งทำให้เฝ้าตรวจได้ดีกว่าเจ้าหน้าที่ตำรวจ สายตรวจ ที่ไม่สามารถตรวจได้ตลอด 24 ชั่วโมงต่อวัน ทำให้เกิดประสิทธิภาพการทำงานได้ดีกว่าการทำงานของบุคคล

4) การใช้ระบบกล้องวงจรปิดบันทึกเหตุการณ์ตามสถานที่ต่างๆ ทำให้เกิดความประหยัดได้ดีกว่าการใช้เจ้าหน้าที่สายตรวจ เพราะระบบกล้องวงจรปิดเป็นการลงทุนที่ต่ำกว่า ไม่มีค่าล่วงเวลา ไม่มี

---

[15] สำนักงานเทคโนโลยีและการสื่อสาร สำนักงานตำรวจแห่งชาติ , คู่มืออบรมหลักสูตรพนักงานสอบสวน, “การใช้งานระบบสารสนเทศข้อมูลอาชญากรรมสำนักงานตำรวจแห่งชาติ, 2559, หน้า 3-4.

การเบิกค่าเบี้ยเลี้ยง ไม่มีการเบิกค่ารักษาพยาบาล ไม่มีการเบิกค่าเล่าเรียนบุตร ไม่มีเงินประจำตำแหน่ง คงมีเพียงแต่ค่าซ่อมบำรุงตามโปรแกรมการดูแลตามระยะเวลาเท่านั้น

5) ทำให้การให้บริการมีความถูกต้อง น่าเชื่อถือ โดยระบบเทคโนโลยีสารสนเทศที่เป็นข้อมูลขนาดใหญ่สามารถตรวจสอบทำให้เกิดความถูกต้อง มีความผิดพลาดการตรวจสอบอยู่ในระดับต่ำมาก ทำให้เกิดความน่าเชื่อถือและความเชื่อมั่นในการให้บริการ

6) ระบบกล้องวงจรปิดทำให้มีข้อมูลขนาดใหญ่ เมื่อนำมาวิเคราะห์ ทำให้สามารถทำนายอนาคต (Prediction)[16] การนำสิ่งที่เกิดขึ้นในอดีตและสิ่งที่กำลังทำในปัจจุบันมาวิเคราะห์และสังเคราะห์ข้อมูลระบบข้อมูลขนาดใหญ่ เพื่อทำนายสิ่งที่จะเกิดขึ้นในอนาคต เช่น ระบบเทคโนโลยีสารสนเทศด้านสภาพภูมิอากาศ มาวิเคราะห์สภาพอากาศ แล้วทำนายสภาพอากาศในวันรุ่งขึ้นหรือวันอื่นๆ ในอนาคต หรือสำนักงานตำรวจแห่งชาติ ใช้ระบบเทคโนโลยีสารสนเทศวิเคราะห์ข้อมูลอาชญากรรม เพื่อทำนายอนาคตว่าอาชญากรรมจะเกิดอย่างไร เกิดที่ไหน เมื่อใด เป็นต้น[17]

สำหรับฐานข้อมูล Big Data ของหน่วยงานรัฐที่สามารถเชื่อมโยงและใช้ประโยชน์ด้านการป้องกันอาชญากรรมได้ อาทิ[18]

- ระบบการสืบค้นข้อมูลหมายจับในรูปแบบเว็บเซอร์วิส (Web Service) ของสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร ที่มีการเชื่อมโยงข้อมูลดังกล่าวผ่านระบบการบูรณาการฐานข้อมูลประชาชนและบริการภาครัฐ (Linkage Center) ของกรมการปกครองไว้เรียบร้อยแล้ว หากหน่วยงานใดต้องการเชื่อมโยงและใช้ข้อมูลหมายจับ ดังกล่าวสามารถขอเชื่อมโยงข้อมูลจากระบบผ่านระบบการบูรณาการฐานข้อมูล ประชาชนและบริการภาครัฐได้โดยตรง

---

[16] ธันยวุฒิ อักขระสมชีพ. (2562). Big Data คืออะไร Data Science คืออะไร มีข้อมูลอยู่จะเริ่มอย่างไร ในทีมต้องมีใคร [ออนไลน์]. สืบค้นเมื่อวันที่ : 20 มกราคม 2563, จาก https://medium.com/@thanyavuth/bigdata-และ-data-science-คืออะไร-ทีมต้องมีใครบ้างมีข้อมูลอยู่จะเริ่มอ ย่างไร-2cb7fec385a3 อ้างถึงใน สมญัติ คำปาละ, การวิเคราะห์การใช้และประโยชน์ ระบบข้อมูลขนาดใหญ่ของ สำนักงานตำรวจแห่งชาติ, หน้า 114.

[17] สมญัติ คำปาละ, การวิเคราะห์การใช้และประโยชน์ ระบบข้อมูลขนาดใหญ่ของ สำนักงานตำรวจแห่งชาติ, หน้า 113-114.

[18] สภาความมั่นคงแห่งชาติ, แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ 1 (พ.ศ. 2563 – 2565), https://www.nsc.go.th/wp-content/uploads/2020/03/AcPlan-Data-Integration.pdf สืบค้นเมื่อ 16 พฤศจิกายน 2564.

- ระบบของตำรวจภูธรภาค 9 เชื่อมโยงกับฐานข้อมูลกลาง สขว.กอ.รมน. ภาค 4 สน. การเชื่อมโยงต้องได้รับอนุญาตจาก กอ.รมน. ได้แก่ ข้อมูลหมายจับตามพระราชกำหนดการบริหารราชการในสถานการณ์ ฉุกเฉิน พ.ศ. 2548 ข้อมูลหมายจับตาม ป.วิ.อาญา ข้อมูลรายชื่อแกนนำร่วม ข้อมูลอาวุธปืนที่ใช้ก่อเหตุ ข้อมูลอาวุธปืนที่สูญหายและได้คืน ข้อมูลอู่ซ่อมรถ จำหน่ายอะไหล่ รถมือสอง ข้อมูลร้านจำหน่ายโทรศัพท์/ซิมการ์ด ข้อมูลร้านจำหน่ายอุปกรณ์ อิเล็กทรอนิกส์และวัสดุก่อสร้าง ข้อมูลวัตถุ ระเบิดและโรงโม่ และข้อมูลการโจรกรรมรถ

- ระบบฐานข้อมูลทะเบียนรถยนต์ของกรมการขนส่งทางบก ที่ได้พัฒนาระบบสารสนเทศที่ใช้ในการจัดเก็บข้อมูลทะเบียนรถ ฐานข้อมูลทะเบียนรถในปัจจุบันได้จัดเก็บข้อมูลประกอบด้วย เลขทะเบียนรถ เลขตัวรถ เลขเครื่องยนต์ประเภทรถ ยี่ห้อรถ แบบรุ่น วันที่จดทะเบียน สถานะรถ และสีรถ เป็นต้น

- ระบบฐานข้อมูลด้านการข่าว สำนักข่าวกรองแห่งชาติ ศูนย์ประสานข่าวกรองแห่งชาติ (ศป.ข.) ดำเนินการพัฒนาระบบฐานข้อมูลด้านการข่าว โดยในระยะที่ 1 การเตรียมความพร้อมด้านโครงสร้างพื้นฐาน และการพัฒนาระบบจัดเก็บข้อมูลข่าวสาร ระบบการติดต่อสื่อสารทั้งส่วนกลางและส่วนภูมิภาคด้วยเทคโนโลยีดิจิทัล สำหรับระยะที่ 2 มีการเชื่อมโยงฐานข้อมูลกับหน่วยสมาชิกในประชาคมข่าวกรองเป็นโครงการนำร่อง และระยะที่ 3 การเชื่อมโยงฐานข้อมูลกับหน่วยสมาชิกในประชาคมข่าวกรองต่อเนื่องจากระยะที่ 2 และการพัฒนาระบบวิเคราะห์การนำข้อมูลมาใช้ประโยชน์จัดทำรายงานในรูปแบบต่าง ๆ ตามความต้องการของผู้ใช้ประโยชน์

ในการจัดทำฐานข้อมูลขนาดใหญ่และวิเคราะห์อาชญากรรมมีประโยชน์ในหลายประการด้วยกัน กล่าวคือ[19]

1. ด้านการสืบสวน ระบบฐานข้อมูลประวัติอาชญากรมีประโยชน์ในด้านการสืบสวน เช่น ในกรณีที่เจ้าทุกข์หรือพยาน สามารถจดจำลักษณะและใบหน้าของผู้กระทำความผิดได้ สามารถช่วยสืบค้นหาตัวผู้กระทำความผิดได้จากงานด้านทะเบียนประวัติอาชญากร ในลักษณะของงานด้านสารบบ ภาพถ่ายคนร้าย หรือสมุดภาพคนร้าย การสเก็ตช์ภาพคนร้ายและการประกอบใบหน้าบุคคล หรือในกรณีที่ทราบชื่อผู้กระทำความผิดหรือสามารถจดจำตำหนิรูปพรรณบางอย่างของผู้กระทำความผิดได้ หรือทราบเพียงข้อมูลและวิธีการดำเนินการของผู้กระทำความผิด ก็สามารถใช้งานทะเบียนประวัติอาชญากรในการช่วยสืบค้นได้

[19] ภาสกร เจนประวิทย์, การจัดทำฐานข้อมูลและวิเคราะห์อาชญากรรมเบื้องต้นของศูนย์ปฏิบัติการคดีพิเศษภาค 4 , https://www.dsi.go.th/th/Detail/การจัดทำฐานข้อมูลและวิเคราะห์อาชญากรรมเบื้องต้นของศูนย์ปฏิบัติการคดีพิเศษภาค-4 , เข้าถึงเมื่อ 15 เมษายน 2564.

จากการค้นหาดัชนีชื่อกลาง ดัชนีตำหนิรูปพรรณ ตำหนิแผลเป็น รอยสักหรือสิ่งพิกลพิการภายในร่างกาย หรือค้นหาด้วยดัชนีวิธีการ เช่น ในกรณีที่ผู้กระทำความผิดนำทรัพย์สินไปจำนำ งานด้านระบบฐานข้อมูลทะเบียนประวัติอาชญากรสามารถช่วยตรวจสอบและค้นหาได้จากการตรวจสอบลายพิมพ์นิ้วมือในต้นขั้วของตั๋วจำนำ ค้นหาด้วยดัชนีลายพิมพ์นิ้วมือเดียวและตรวจสอบรายชื่อได้จากดัชนีชื่อกลาง หรือในกรณีที่พบทรัพย์สินของกลางแต่ไม่ทราบตัวผู้เป็นเจ้าของและถ้ามีการแจ้งความไว้ที่สถานีตำรวจ ก็สามารถสืบค้นหาได้จากดัชนีทรัพย์สินที่ถูกประทุษร้าย การตรวจสอบตัวผู้กระทำความผิดที่หลบหนีจากการจับกุมตัวของเจ้าหน้าที่ งานด้านทะเบียนประวัติอาชญากรก็สามารถช่วยสืบหาตัวด้วยการออกประกาศหมายจับและจัดส่งให้แก่สถานีตำรวจทั่วราชอาณาจักรเพื่อติดตามจับกุมตัวผู้กระทำความผิดต่อไปได้

2. ด้านการสอบสวน ระบบฐานข้อมูลประวัติอาชญากร จะช่วยในการตรวจสอบลายพิมพ์นิ้วมือของผู้ต้องหา เพื่อที่ต้องการทราบว่าผู้ต้องหานั้น เคยกระทำความผิดหรือมีคดีเคยต้องโทษมาก่อนหรือไม่ และช่วยในการตรวจสอบประวัติการทำแผนประทุษกรรมของผู้ต้องหา เพื่อตรวจสอบผู้ต้องหาว่าเคยกระทำความผิดมาก่อนด้วยวิธีการใด และเคยต้องโทษคดีความใดบ้าง นอกจากนั้นระบบฐานข้อมูลทะเบียนประวัติอาชญากร ยังช่วยตรวจสอบดัชนีการประกาศสืบจับตัวผู้กระทำความผิดทางคดีอาญา หรืออยู่ในระหว่างหลบหนีจากการจับกุม และช่วยตรวจสอบสายพิมพ์นิ้วมือของศพ เพื่อใช้ในการสืบสวนสอบสวนหาตัวผู้กระทำผิดต่อไป

3. ด้านการป้องกันปราบปราม มีประโยชน์ในการจัดทำประวัติผู้ต้องหาตามหมายจับ ผู้ต้องขังในเรือนจำ และบุคคลที่พ้นโทษ พร้อมจัดส่งไปยังสำนักงานตำรวจแห่งชาติและหน่วยงานที่เกี่ยวข้องที่บุคคลที่พ้นโทษมีภูมิลำเนาอยู่ เพื่อเป็นการแจ้งให้เจ้าหน้าที่ตำรวจท้องที่รับทราบ และจัดเก็บข้อมูลของบุคคลที่พ้นโทษเอาไว้ พร้อมกับคอยสอดส่องดูแลพฤติกรรมและความเคลื่อนไหว ถ้าหากบุคคลที่พ้นโทษไปแล้วกระทำความผิดอีกครั้ง ก็สามารถนำเอาข้อมูลและรายละเอียดต่างๆมาใช้ในการสืบสวนและปราบปรามต่อไป

4. การจัดเก็บข้อมูลที่เกี่ยวข้องกับอาชญากรรมของประเทศไทย

ปัจจุบันการจัดเก็บข้อมูลอาชญากรรมของประเทศไทย เป็นการจัดเก็บข้อมูลโดยหน่วยงานในกระบวนการยุติธรรมที่มีลักษณะต่างคนต่างเก็บรวบรวมข้อมูลสถิติต่าง ๆ ที่ผ่านเข้าออกขั้นตอนของกระบวนงานในส่วนของตนเอง ได้แก่ สถิติอาชญากรรมของตำรวจ สถิติคดีที่เข้าสู่การพิจารณาของศาลชั้นต้น สถิติผู้ต้องขังที่ราชทัณฑ์ดูแล สถิติคดีที่เกี่ยวข้องกับการที่ผู้กระทำความผิดผ่านเข้าสู่กระบวนการงาน

ของหน่วยงานต่าง ๆ ในกระบวนการยุติธรรมแต่ละหน่วยงาน โดยจัดทำเป็นรายปีและยังขาดความเชื่อมโยงระหว่างหน่วยงานในกระบวนการยุติธรรมและยังขาดการบริหารจัดการข้อมูลเชิงระบบเพื่อรับมือกับอาชญากรรมในปัจจุบันและในอนาคต[20] โดยปัจจุบันมีหน่วยงานที่มีการเก็บข้อมูลสถิติเกี่ยวกับอาชญากรรม ได้แก่ สำนักงานตำรวจแห่งชาติ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม กรมราชทัณฑ์สำนักงานกิจการยุติธรรมกระทรวงยุติธรรม

วิธีการจัดเก็บข้อมูลของแต่ละหน่วยงาน จะมีการจัดเก็บรายละเอียดของอาชญากรรมแตกต่างกันตามภารกิจของหน่วยงาน กล่าวคือ

สำนักงานตำรวจแห่งชาติ จะเก็บข้อมูลสถิติคดีเกี่ยวกับข้อมูลผู้กระทำความผิด รายละเอียดพฤติการณ์แห่งคดีซึ่งจะจัดเก็บข้อมูลตามเนื้อหาและองค์ประกอบความผิดของกฎหมายในเรื่องนั้น ๆ ข้อมูลเกี่ยวกับเหยื่อหรือผู้เสียหายจากการกระทำความผิด โดยมีการเก็บรวบรวมและทำสถิติคดีตามฐานความผิดคดีอาญาของคดี 4 กลุ่มคือ ฐานความผิดเกี่ยวกับชีวิต ร่างกายและเพศ ฐานความผิดเกี่ยวกับทรัพย์ ฐานความผิดพิเศษและคดีความผิดที่รัฐเป็นผู้เสียหายของแต่ละพื้นที่ทั่วประเทศ

สำนักงานอัยการสูงสุด มีการจัดเก็บข้อมูลเกี่ยวกับสถิติคดีที่รับมา และสถิติการสั่งฟ้องและสั่งไม่ฟ้องคดี โดยจำแนกตามรายภาคและประเภทสำนวนคดี ได้แก่ ความอาญาปรากฏตัวผู้ต้องหาที่ส่งตัวมา ความอาญาปรากฏตัวผู้ต้องหาที่ไม่ได้ส่งตัวมา (เว้นแต่คดีเปรียบเทียบ) ความอาญาปรากฏตัวผู้ต้องหาที่ไม่ได้ส่งตัวมา (เฉพาะคดีเปรียบเทียบ) ความอาญาไม่ปรากฏผู้กระทำผิด ความอาญาแก้ต่าง ชันสูตรพลิกศพ และสำนวนฟื้นฟูสมรรถภาพผู้ติดยาเสพติด

สำนักงานศาลยุติธรรม สำนักงานศาลยุติธรรมมีการจัดเก็บข้อมูลสถิติคดีของศาลทั่วราชอาณาจักร แยกประเภทคดีตามเขตอำนาจศาล โดยแยกออกเป็นคดีที่เข้าสู่การพิจารณาของศาล คดีที่พิพากษาแล้วเสร็จและคดีที่อยู่ระหว่างการพิจารณาของศาล โดยแยกประเภทคดีตามเขตอำนาจศาลและชั้นศาล ตัวอย่างเช่น ศาลชั้นต้น มีการจัดเก็บข้อมูลแบ่งออกเป็นคดีแพ่ง คดีพาณิชย์ คดีผู้บริโภค คดีสิ่งแวดล้อม คดีอาญา คดียาเสพติด คดีค้ามนุษย์ คดีนักท่องเที่ยว (อาญา) คดีทุจริตฯ (แพ่ง) คดีทุจริตฯ (อาญา) คดีเยาวชนฯ (แพ่ง) คดีเยาวชนฯ (อาญา) คดีภาษีอากร คดีแรงงาน คดีทรัพย์สิน (แพ่ง) คดีทรัพย์สิน (อาญา) คดีล้มละลาย คดีฟื้นฟูกิจการ เป็นต้น

---

[20] จุฑารัตน์ เอื้ออำนวย , การสำรวจสถิติอาชญากรรมในประเทศไทยและข้อเสนอเพื่อพัฒนาการกระบวนการยุติธรรมยุคใหม่ , วารสารกระบวนการยุติธรรม เล่มที่ 2 ปีที่ 1 , หน้า 11.

กรมราชทัณฑ์ มีการจัดเก็บรวบรวมสถิติที่เกี่ยวกับจำนวนนักโทษเด็ดขาด ผู้ต้องขัง เยาวชนที่ฝากขัง ผู้ถูกกักกันและผู้ต้องกักขัง และการเก็บสถิติเกี่ยวกับการกระทำความผิดซ้ำ

สำนักงานกิจการยุติธรรม กระทรวงยุติธรรม มีการจัดทำรายงานสถานการณ์อาชญากรรมและกระบวนการยุติธรรม เป็นข้อมูลทางสถิติที่เกี่ยวข้องกับอาชญากรรมและกระบวนการยุติธรรมในประเทศไทย โดยจำแนกเป็นหมวดหมู่ ได้แก่ สถานการณ์อาชญากรรม สถิติคดีอาญาและการดำเนินงานในชั้นตำรวจ กระบวนการดำเนินคดี สถิติการดำเนินคดีอาญาในชั้นพนักงานอัยการและกระบวนการพิจารณาคดีในชั้นศาล กระบวนการหลังการพิจารณาคดีสถิติการบังคับโทษในเรือนจำ การสั่งคุมประพฤติและการปฏิบัติต่อเด็กและเยาวชนที่กระทำผิด และการให้ความช่วยเหลือและการคุ้มครองสิทธิด้านกระบวนการยุติธรรม ทั้งนี้เนื้อหาในแต่ละส่วนประกอบด้วยสถิติเกี่ยวกับสถานการณ์อาชญากรรมและกระบวนการยุติธรรมในด้านต่างๆ ซึ่งได้รับการบันทึกและเก็บรวบรวมโดยหน่วยงานในกระบวนการยุติธรรม ได้แก่ สำนักงานตำรวจแห่งชาติ (กองแผนงาน อาชญากรรม) สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม (สำนักแผนงานและงบประมาณ กลุ่มงานส่วนระบบข้อมูลสถิติ) กรมราชทัณฑ์กรมคุมประพฤติ (กองยุทธศาสตร์และแผนงาน) กรมพินิจและคุ้มครองเด็กและเยาวชน กรมคุ้มครองสิทธิและเสรีภาพ (สำนักงานช่วยเหลือทางการเงินแก่ผู้เสียหายในคดีอาญา กลุ่มงานพัฒนาระบบไกล่เกลี่ยข้อพิพาท กลุ่มงานให้คำปรึกษากฎหมายและส่งเสริมสิทธิผู้ต้องหา) และสถาบันนิติวิทยาศาสตร์[21] และในส่วนของการเก็บข้อมูลคดีอาญา ประกอบด้วยเนื้อหาเกี่ยวกับฐานความผิด ในคดีอาญา 4 กลุ่ม ได้แก่ กลุ่มข้อหาฐานความผิดเกี่ยวกับชีวิต ร่างกายและเพศ กลุ่มข้อหาฐานความผิดเกี่ยวกับทรัพย์ กลุ่มข้อหาฐานความผิดพิเศษ และกลุ่มข้อหาคดีความผิดที่รัฐเป็นผู้เสียหาย

จะเห็นได้ว่า การใช้ประโยชน์จากข้อมูลที่เกี่ยวข้องกับอาชญากรรมดังกล่าวของแต่ละหน่วยงาน เป็นการใช้ประโยชน์จากข้อมูลในเชิงสถิติตามภารกิจของหน่วยงาน โดยอาจมีการนำข้อมูลสถิติมาใช้วิเคราะห์เพื่อประโยชน์ในเชิงนโยบาย แต่ไม่ได้มีการนำข้อมูลดังกล่าวมาวิเคราะห์ในลักษณะของการใช้ประโยชน์ด้านการป้องกันและปราบปรามอาชญากรรมในแต่ละพื้นที่ แต่ละช่วงเวลา ซึ่งประเด็นนี้เป็นเรื่องใหม่สำหรับประเทศไทย ผู้วิจัยจึงได้ศึกษาถึงแนวทางการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) ในด้านการป้องกันและปราบปรามอาชญากรรมของต่างประเทศมาวิเคราะห์เป็นแนวทางสำหรับประเทศไทย รายละเอียดปรากฏในบทที่ 4 ของรายงานวิจัย

---

[21] สำนักงานกิจการยุติธรรม กระทรวงยุติธรรม , รายงานสถานการณ์อาชญากรรมและกระบวนยุติธรรม ประจำปี 2562 , 2562, หน้า 3.

บทที่ 3
ระเบียบวิธีวิจัย

ผู้วิจัยใช้ระเบียบวิธีวิจัยในการเก็บรวบรวมข้อมูลและวิเคราะห์ข้อมูลเป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ประกอบด้วย การวิจัยเอกสาร (Documentary Research) การสัมภาษณ์เชิงลึก (In-depth Interview) การประชุมกลุ่มย่อย (Focus group) และการสัมมนารับฟังความคิดเห็น

1. การวิจัยเอกสาร (Documentary research)

การดำเนินการวิจัยโดยการวิจัยเอกสาร เป็นการรวบรวมข้อมูลที่เกี่ยวข้องกับงานวิจัยจากเอกสารที่เกี่ยวข้อง ทั้งจากแหล่งข้อมูลปฐมภูมิ (Primary Sources) ประกอบด้วย ตัวบทกฎหมาย กฎกระทรวง ระเบียบและคำสั่ง ข้อบังคับของกระทรวง ทบวง กรม หรือหน่วยงานราชการต่างๆ รวมถึงคำพิพากษาต่างๆ และจากแหล่งข้อมูลทุติยภูมิ (Secondary Sources) ประกอบด้วย ตำรากฎหมาย รายงานการวิจัย ตำรา บทความในวารสาร เอกสารการสัมมนา และข้อมูลจากอินเตอร์เน็ตในรูปแบบของเว็บไซต์ เอกสารที่เกี่ยวข้องนี้มีทั้งเอกสารไทยและต่างประเทศ ซึ่งส่วนหนึ่งของการวิจัยเอกสารนี้จะปรากฏอยู่ในบทการทบทวนวรรณกรรมและเป็นข้อมูลที่ใช้ในการวิเคราะห์ร่วมกับข้อมูลจากการสัมภาษณ์เชิงลึกและการจัดประชุมกลุ่มย่อย

2. การสัมภาษณ์เชิงลึก)In-depth Interview(

ดำเนินการสัมภาษณ์เชิงลึก (In-depth Interview) โดยมีผู้ให้ข้อมูลสำคัญ (Key Informant) เป็นผู้ทรงคุณวุฒิ จำนวนทั้งสิ้น 10 ท่าน ทั้งนี้ หลักเกณฑ์ในการเลือกผู้ทรงคุณวุฒิเพื่อเป็นผู้ให้ข้อมูลสำคัญ ใช้การเลือกแบบเจาะจง (Purposive sampling) โดยพิจารณาถึงการได้ข้อมูลที่ครอบคลุมประเด็นสำคัญเกี่ยวกับแนวทางการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปรามอาชญากรรมในประเทศไทย โดยจะดำเนินการสัมภาษณ์เชิงลึกผู้ที่เกี่ยวข้องโดยตรงและส่งแบบสัมภาษณ์ล่วงหน้า เพื่อให้ได้มาซึ่งข้อมูลที่จะใช้ในการวิเคราะห์ร่วมกับวิธีการวิจัยวิธีอื่น

2.1 ประชากรสัมภาษณ์

ผู้ให้ข้อมูลสำคัญ ได้แก่ ผู้แทนหน่วยงานที่มีภารกิจเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมและการใช้นำข้อมูลขนาดใหญ่ภาครัฐ ได้แก่

1) สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ จำนวน 2 คน
2) สำนักงานกฎหมายและคดี สำนักงานตำรวจแห่งชาติ จำนวน 2 คน
3) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีจำนวน 2 คน
4) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจจำนวน 2 คน
5) สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
6) สถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ

2.2 เครื่องมือในการเก็บรวบรวมข้อมูล

ดำเนินการเก็บรวบรวมข้อมูลโดยใช้แบบสัมภาษณ์เชิงลึก ประกอบด้วยคำถามดังนี้

1) ท่านทำงานในตำแหน่งอะไร งานที่ทำเกี่ยวข้องกับข้อมูลขนาดใหญ่ (Big Data) หรือไม่
2) หน่วยงานของท่านมีภารกิจที่เกี่ยวกับการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) อย่างไร และปัจจุบันหน่วยงานมีการนำข้อมูลขนาดใหญ่มาใช้ประโยชน์มากน้อยเพียงใด
3) ท่านมีความเห็นอย่างไรต่อหากมีการนำข้อมูลขนาดใหญ่ (Big Data) มาวิเคราะห์เพื่อลดการเกิดอาชญากรรมและปรามปรามการกระทำความผิด
4) ท่านคิดว่าในปัจจุบันกฎหมายมีข้อจำกัดในการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ในส่วนของการป้องกันและปราบปรามอาชญากรรมหรือไม่อย่างไร
5) ท่านคิดว่าภาครัฐควรกำหนดขอบเขตการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ของภาครัฐไว้แค่ไหน เพียงใด
6) ท่านคิดว่าภาครัฐควรมีหลักประกันเกี่ยวกับสิทธิของเจ้าของข้อมูลอย่างไร

7) ท่านมีความเห็นหรือข้อเสนอแนะในการแก้ไขกฎหมายเพื่อนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ในระบบงานยุติธรรมด้านการป้องกันและปราบปรามอาชญากรรมอย่างไร
8) ท่านคิดว่าความเห็นหรือข้อเสนอแนะเกี่ยวกับการบริหารจัดการข้อมูลขนาดใหญ่ของภาครัฐอย่างไร

3. การจัดประชุมกลุ่มย่อย (Focus Group)

ดำเนินการจัดประชุมกลุ่มย่อย (Focus Group) ในประเด็นปัญหา อุปสรรคและแนวทางการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปรามอาชญากรรมในประเทศไทย โดยพื้นที่ในการเก็บรวบรวมข้อมูลได้แก่ กรุงเทพมหานคร จังหวัดเชียงใหม่ จังหวัดชลบุรี จำนวนครั้งละ 30 คน

3.1 กลุ่มประชากร

เป็นกลุ่มประชากรผู้ที่มีส่วนได้เสีย (Stakeholders) ในการบังคับใช้กฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมและการบริหารข้อมูลขนาดใหญ่ภาครัฐมีดังนี้

กลุ่มที่ 1 กลุ่มหน่วยงานด้านเทคโนโลยีดิจิทัล ได้แก่ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมสำนักงานนวัตกรรมแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล

กลุ่มที่ 2 กลุ่มหน่วยงานในกระบวนการยุติธรรมทางอาญา ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม

กลุ่มที่ 3 กลุ่มภาคเอกชนและตัวแทนภาคประชาชน

3.2 เครื่องมือในการเก็บรวบรวมข้อมูล

ดำเนินการเก็บรวบรวมข้อมูลโดยใช้แบบแสดงความเห็น ระบุประเด็นคำถาม ดังนี้

1) ท่านมาจากหน่วยงานใด และงานที่ทำเกี่ยวข้องกับข้อมูลขนาดใหญ่ (Big Data) หรือไม่

2) หน่วยงานของท่านมีภารกิจที่เกี่ยวกับการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) อย่างไร และปัจจุบันหน่วยงานมีการนำข้อมูลขนาดใหญ่มาใช้ประโยชน์มากน้อยเพียงใด
3) ท่านมีความเห็นอย่างไรต่อหากมีการนำข้อมูลขนาดใหญ่ (Big Data) มาวิเคราะห์เพื่อลดการเกิดอาชญากรรมและปรามปรามการกระทำความผิด
4) ท่านคิดว่าในปัจจุบันกฎหมายมีข้อจำกัดในการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ในส่วนของการป้องกันและปราบปรามอาชญากรรมหรือไม่อย่างไร
5) ท่านคิดว่าภาครัฐควรกำหนดขอบเขตการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ของภาครัฐไว้แค่ไหน เพียงใด
6) ท่านคิดว่าภาครัฐควรมีหลักประกันเกี่ยวกับสิทธิของเจ้าของข้อมูลอย่างไร
7) ท่านมีความเห็นหรือข้อเสนอแนะในการแก้ไขกฎหมายเพื่อนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ในระบบงานยุติธรรมด้านการป้องกันและปราบปรามอาชญากรรมอย่างไร
8) ท่านคิดว่าความเห็นหรือข้อเสนอแนะเกี่ยวกับการบริหารจัดการข้อมูลขนาดใหญ่ของภาครัฐอย่างไร

4. การจัดสัมมนารับฟังความคิดเห็น

ดำเนินการจัดสัมมนารับฟังความคิดเห็น เพื่อนำเสนอผลการศึกษาของชุดโครงการวิจัยและรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้องและผู้มีส่วนได้เสีย และนำผลการรับฟังความคิดเห็นมาพิจารณาประกอบเพื่อแก้ไขปรับปรุงรายงานการวิจัยฉบับสมบูรณ์ โดยมีผู้เข้าร่วมสัมมนามาจากหน่วยงานที่เกี่ยวข้องและผู้ที่มีส่วนได้เสีย (Stakeholders) ใน 3 กลุ่มคือ

กลุ่มที่ 1 กลุ่มหน่วยงานด้านเทคโนโลยีดิจิทัล ได้แก่ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมสำนักงานนวัตกรรมแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล

กลุ่มที่ 2 กลุ่มหน่วยงานในกระบวนการยุติธรรมทางอาญา ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กองบังคับการปราบปรามการกระทำ

ความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม

กลุ่มที่ 3 กลุ่มภาคเอกชนและตัวแทนภาคประชาชน

กลุ่มที่ 4 นักวิชาการและผู้ทรงคุณวุฒิ

5. เครื่องมือในการวิจัย

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลตามวิธีการวิจัยเชิงคุณภาพที่ระบุไว้ มีดังนี้

1) การสัมภาษณ์เชิงลึก (In-depth Interview) เครื่องมือการวิจัย ได้แก่ แบบสัมภาษณ์เชิงลึก (ระบุประเด็นสัมภาษณ์ที่กำหนดไว้ล่วงหน้า)
2) การจัดประชุมกลุ่มย่อย (Focus Group) เครื่องมือการวิจัย ได้แก่ แบบแสดงความเห็น (ระบุประเด็นตามคำถามการวิจัย)

6. การวิเคราะห์ข้อมูล

ในส่วนของการวิเคราะห์ข้อมูลงานวิจัย ผู้วิจัยจะทำการสังเคราะห์และวิเคราะห์ข้อมูลเชิงคุณภาพ โดยวิเคราะห์จากเนื้อหาที่ได้จากการวิจัยเอกสาร และวิเคราะห์จากข้อมูล ความเห็นและข้อเสนอแนะที่ได้จากการเก็บรวบรวมข้อมูลโดยการสัมภาษณ์เชิงลึก การประชุมกลุ่มย่อย รวมทั้งจากการสัมมนารับฟังความเห็น เพื่อนำมาเป็นแนวทางเสนอแนะด้านกฎหมายในการการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปรามอาชญากรรม เพื่อให้หน่วยงานที่เกี่ยวข้องนำแนวทางดังกล่าวไปใช้ประโยชน์ตามภารกิจของตนต่อไป

บทที่ 4
รูปแบบและแนวทางการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) ในการป้องกันและปราบปรามการอาชญากรรมของต่างประเทศ

ในส่วนนี้เป็นการศึกษารูปแบบและแนวทางการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) ในการป้องกันและปราบปรามการอาชญากรรมของสหรัฐอเมริกา สหราชอาณาจักร และประเทศแคนนาดา เพื่อนำมาเป็นแนวทางพิจารณาข้อกฎหมายที่เกี่ยวข้องของไทยและเพื่อประโยชน์ในการประยุกต์ใช้เทคโนโลยีข้อมูลขนาดใหญ่ในภารกิจการป้องกันและปราบปรามอาชญากรรม

1. สหรัฐอเมริกา

1.1 ความเป็นมา

สหรัฐอเมริกาได้มีการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big data) ในกระบวนการยติธรรมทางอาญามาอย่างยาวนาน โดยในปี ค.ศ. 1967 คณะกรรมการประธานาธิบดีว่าด้วยการบังคับใช้กฎหมายและการบริหารงานยุติธรรม (President's Commission on Law Enforcement and Administration of Justice) ได้ส่งเสริมให้มีการนำเทคโนโลยีใหม่ๆ มาใช้วิเคราะห์ข้อมูลขนาดใหญ่ (Big data) ในงานระบบยุติธรรมทางอาญาเพื่อปรับปรุงระบบให้มีประสิทธิภาพและมีความยุติธรรมมากยิ่งขึ้น ซึ่งในช่วงเวลานั้นลักษณะการปฏิบัติงานของเจ้าหน้าที่เพื่อรักษากฎหมายเป็นไปในรูปแบบการปฏิบัติงานตรวจตราแบบสุ่ม (random patrol) ปฏิบัติการเผชิญเหตุเร็ว (rapid response) และการสืบสวนเชิงรับ (reactive investigations) ต่อมามีการศึกษาวิจัยพบว่าการปฏิบัติงานในรูปแบบการปฏิบัติงานตรวจตราแบบสุ่ม (random patrol) ซึ่งเป็นกลยุทธ์ที่เจ้าหน้าที่ตำรวจนำมาปรับใช้ในการปฏิบัติงาน ณ ขณะนั้นส่งผลต่อการป้องกันและปราบรามเหตุอาชญากรรมได้น้อย พร้อมเสนอแนะให้เปลี่ยนการปฏิบัติงานจากเชิงรับเป็นเชิงรุกโดยใช้แนวปฏิบัติงานเพื่อรักษากฎหมายบนพื้นฐานของข้อมูลหลักฐาน เช่น การบริหารจุดเสี่ยง (hot spots policing)[22]

---

[22] Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

ระบบกระบวนการยุติธรรมทางอาญาของประเทศสหรัฐอเมริกามีการเจริญเติบโตอย่างรวดเร็วมาตั้งแต่ปี ค.ศ. 1972 ซึ่งปีนี้ถือเป็นยุคของการเปลี่ยนผ่านหรือปรับเปลี่ยนข้อมูล (Data) แบบอนาล็อก (Analog) ไปเป็นดิจิทัล (Digital) โดยระบบกระบวนการยุติธรรมทางอาญาได้มีการนำการวิเคราะห์ข้อมูลขนาดใหญ่ด้วยคอมพิวเตอร์หรือที่เรียกว่า การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analysis) โดยใช้เทคโนโลยีเข้ามาปรับใช้ในการดำเนินงานกระบวนการยุติธรรมทางอาญา[23] ในหลายๆ ด้าน อาทิ หน่วยงานบังคับใช้กฎหมายได้เริ่มปรับใช้ข้อมูลขนาดใหญ่ในการปฏิบัติหน้าที่ป้องกันและปราบปรามอาชญากรรมในหลายๆ ด้าน เช่น การดำเนินงานด้านเฝ้าระวังติดตามต่างๆ โดยเจ้าหน้าที่ตำรวจ รวมถึง การออกตรวจตรา การสืบสวน และการวิเคราะห์อาชญากรรม โดยกรอบการดำเนินงานในด้านดังกล่าวของเจ้าหน้าที่ตำรวจจะเปลี่ยนไปตามข้อพิจารณาหารือในระดับนโยบาย กฎหมาย ข้อบังคับ และองค์ความรู้ทางวิชาการ ต่างๆ ที่เหมาะสมกับสภาพการณ์ในแต่ละช่วงเวลา ทั้งนี้ในช่วงปี ค.ศ. 1990 และต้นปี ค.ศ. 2000 ได้มีการนำแนวคิดการใช้สถิติโดยคอมพิวเตอร์มาปรับใช้ในการปฏิบัติงานของเจ้าหน้าที่ตำรวจทั่วประเทศสหรัฐอเมริกาโดยเริ่มจากนครนิวยอร์กเป็นที่แรก ซึ่งแนวคิดนี้เป็นแนวคิดด้านการบริหารจัดการที่มุ่งหาการระบุรูปแบบอาชญากรรม การหาจำนวน การสร้างแรงจูงใจในการปฏิบัติงานของเจ้าหน้าที่ตำรวจ และการอำนวยการใช้ทรัพยากรแก่ตำรวจ มากยิ่งกว่านั้นประเทศสหรัฐอเมริกาได้ให้ความสำคัญกับการปรับปรุงการเก็บรวบรวมข้อมูลยุติธรรมทางอาญาและการแลกเปลี่ยนข้อมูลยุติธรรมทางอาญามากยิ่งขึ้น[24] โดยเฉพาะอย่างยิ่งภายหลังจากการเกิดเหตุวินาศกรรม 11 กันยายน หรือ 9/11 ที่ถูกมองว่าเป็นความล้มเหลวชุมชนด้านการข่าวของสหรัฐ ซึ่งภายหลังจากเหตุวินาศกรรมดังกล่าว ทฤษฎีการพยากรณ์อาชญากรรมล่วงหน้า (Predictive policing theory) เข้ามามีบทบาทสำคัญในด้านงานข่าวกรองของสหรัฐฯ มีการริเริ่มแนวทางปฏิบัติหรือกลยุทธ์ต่างๆ ในหน่วยงานบังคับใช้กฎหมายโดยใช้ทฤษฎีการพยากรณ์อาชญากรรมล่วงหน้า (Predictive policing theory) เป็นพื้นฐาน ซึ่งบทบาทของหน่วยงานที่เกี่ยวข้องกับการปรับใช้แนวทางปฏิบัติหรือกลยุทธ์ต่างๆ โดยใช้ทฤษฎีดังกล่าวเป็นพื้นฐานมีหลายหน่วยงาน อาทิ หน่วยงานระดับท้องถิ่น (local) หน่วยงานระดับรัฐ (state) หน่วยรัฐบาลกลาง (federal governments) หน่วยงานอื่นๆ ผู้ออกแบบรูปแบบเครื่องมือ/

---

[23] Brayne, S. (2017, August). Big Data Surveillance: The Case of Policing, Vol. 82(5) 977–1008. Retrieved from American Sociological Review: http://users.soc.umn.edu/~uggen/Brayne_ASR_17.pdf

[24] Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

เทคโนโลยีสำหรับการพยากรณ์อาชญากรรมล่วงหน้า บริษัทผู้ผลิตหรือพัฒนา/ผู้ขาย นักวิจัย และที่ปรึกษาต่างๆ เป็นต้น ทั้งนี้กรมตำรวจส่วนท้องถิ่นเป็นส่วนงานที่ได้รับการจัดสรรงบประมาณจากรัฐบาลกลางเพื่อริเริ่มทดลองแนวทางปฏิบัติดังกล่าวมากที่สุด ดังจะเห็นได้จากในปี ค.ศ. 2011 กรมตำรวจนครลอสแอนเจลิสได้รับการจัดสรรงบประมาณจำนวน 3 ล้านดอลลาห์สหรัฐจากกระทรวงยุติธรรมแห่งสหรัฐอเมริกา U.S. Department of Justice (DOJ) เพื่อดำเนินแผนปฏิบัติงานด้านการวิเคราะห์ข้อมูลขนาดใหญ่เพื่อการพยากรณ์อาชญากรรมล่วงหน้าในหลายปี และในปี ค.ศ. 2015 กรมตำรวจเมืองไมอามี่ได้รับการจัดสรรงบประมาณจำนวน 600,000 ดอลลาห์สหรัฐ เพื่อดำเนินการในแผนปฏิบัติงานด้านการวิเคราะห์ข้อมูลขนาดใหญ่เช่นเดียวกันกับกรมตำรวจนครลอสแอนเจลิส ส่วนเมืองขนาดเล็กอื่นๆ จะได้รับเครื่องมือที่เป็นนวัตกรรมเทคโนโลยีใหม่ด้านการพยากรณ์อาชญากรรมไปใช้ภายหลังจากที่กรมตำรวจเมืองใหญ่ๆ ได้ดำเนินการทดลองใช้เครื่องมือดังกล่าวนำร่องไปก่อน อย่างไรก็ดีมีบางเมืองที่ได้นวัตกรรมเทคโนโลยีดังกล่าวไปใช้ในการดำเนินงานแล้ว คือ เมืองชิคาโก รัฐอิลลินอยส์ (Chicago, IL) มมฟิส รัฐเทนเนสซี (Memphis, TX) นครลอสแอนเจลิส รัฐแคลิฟอร์เนีย (Los Angeles, CA) ซานตาครูซ รัฐแคลิฟอร์เนีย (Santa Cruz, CA) มินนีแอโพลิส รัฐมินนิโซตา(Minneapolis, MN) เมืองปาล์มบีช รัฐฟลอริดา (Palm Beach, FL) แดลลัส รัฐเทกซัส (Dallas, TX) มืองแวนคูเวอร์ รัฐบริติชโคลัมเบีย ประเทศแคนาดา (Vancouver; British Columbia, Canada), ชาร์ลอตต์ รัฐนอร์ทแคโรไลนา (Charlotte-Mecklenburg, NC) เมืองแนชวิลล์ รัฐเทนเนสซี (Nashville, TN) เมืองเกลนเดล รัฐแอริโซนา (Glendale, AZ) เมืองออเรนจ์ตะวันออก รัฐนิวเจอร์ซีย์ (East Orange, NJ) บอลทิมอร์ รัฐแมริแลนด์(Baltimore, MD) นครนิวยอร์ก รัฐนิวยอร์ก (New York City, NY) เมืองฟิลาเดลเฟีย รัฐเพนซิลเวเนีย (Philadelphia, PA) เมืองไมอามี่ รัฐฟลอริดา (Miami, FL) เมืองนิวคาสเซิล รัฐเดลาแวร์ (New Castle, DE) ลิงคอล์น รัฐเนแบรสกา (Lincoln, NE) และ and เมืองมอนเตวิเดโอ รัฐมินนิโซตา (Montevideo, MN)[25]

รัฐบาลกลางพิจารณาสนับสนุนงบประมาณเพื่อการเก็บข้อมูลอาชญากรรมที่เป็นปัจจุบัน ไปยังสถานีตำรวจท้องถิ่นทั่วประเทศดังกล่าวข้างต้นเนื่องจากเห็นว่าเจ้าหน้าที่ตำรวจที่ปฏิบัติงานในรัฐต่างๆ ถือเป็นกลุ่มผู้ปฏิบัติงานส่วนหน้าที่เผชิญกับเหตุก่อการร้ายต่างๆ โดยงบประมาณที่ถูกจัดสรรแก่หน่วยงานบังคับใช้กฎหมายทั่วประเทศนั้นมีวัตถุประสงค์เพื่อจัดตั้งศูนย์ข่าวกรอง ให้เป็นสถานที่สำหรับการทำงานร่วมกันของ

[25] Brayne, S. (2017, August). Big Data Surveillance: The Case of Policing, Vol. 82(5) 977–1008. Retrieved from American Sociological Review: http://users.soc.umn.edu/~uggen/Brayne_ASR_17.pdf

หลายหน่วยงานและผู้ปฏิบัติงานสหวิชาชีพต่างๆ เพื่อดำเนินการรวบรวมข้อมูลจากทั้งแหล่งข้อมูลของภาครัฐและเอกชน โดยหน่วยงานบริหารกลางและท้องถิ่นได้ร่วมมือกับบริษัทเทคโนโลยีเพื่อยกระดับการเก็บข้อมูลและสมรรถนะการวิเคราะห์ข้อมูลอาชญากรรม เช่น มีการร่วมมือกับบริษัท Palantir (Palantir software company) ซึ่งเป็นบริษัทผลิตซอฟต์แวร์ที่สนับสนุนงบประมาณการผลิตซอฟ์ตแวร์บางส่วนโดยหลายองค์กร อาทิ องค์กรไม่แสวงหาผลกำไร In-Q-Tel (In-Q-Tel American Non-profit Organization) ธุรกิจเงินร่วมลงทุน ของหน่วยข่าวกรองอาญาของหน่วยสืบราชการลับกลางแห่งสหรัฐฯ (Criminal Intelligence Agency's (CIA's) venture capital firm) ให้ทำหน้าที่ออกแบบซอฟต์แวร์เพื่อการวิเคราะห์ข้อมูลที่แต่เดิมถูกใช้ในงานป้องกันราชอาณาจักร แต่ปัจจุบันบริษัท Palantir ได้ออกแบบซอฟต์แวร์ลักษณะดังกล่าวให้กับทั้งภาครัฐและเอกชนที่มีวัตถุประสงค์ในการใช้อย่างหลากหลาย เช่น บริษัท J.P. Morgan ใช้ในวัตถุประสงค์เชิงพาณิชย์ หน่วยงานบริหารกลางต่างๆ ใช้ในงานของรัฐ เช่น หน่วยสืบราชการลับกลางแห่งสหรัฐฯ (CIA) สำนักงานสอบสวนกลางแห่งสหรัฐอเมริกา (Federal Bureau of Investigation) สำนักงานตรวจคนเข้าเมืองและศุลกากรสหรัฐอเมริกา (U.S. Immigration and Customs Enforcement; ICE) กระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security) รวมถึงหน่วยงานบังคับใช้กฎหมายท้องถิ่นในสหรัฐฯ เช่น กรมตำรวจนครลอสแอนเจลิส (Los Angeles Police Department; LAPD) อนึ่ง การสนับสนุนงบประมาณจากหน่วยสอบสวนกลางแก่หน่วยงานบังคับใช้กฎหมายในท้องถิ่นมีวัตถุประสงค์หลักเพื่อปรับใช้และพัฒนาการปฏิบัติงานด้านการบังคับใช้กฎหมายโดยมีการริเริ่มใช้ข้อมูลขนาดใหญ่เข้ามาเป็นเครื่องมือในการปฏิบัติหน้าที่ต่างๆ อาทิ การปฏิบัติงานบนพื้นฐานของข้อมูลหลักฐาน กลยุทธ์การปฏิบัติงานด้วยการใช้ข้อมูลเป็นพื้นฐานเพื่อการขับเคลื่อนกลยุทธ์ (Data-Driven Strategy)[26]

อย่างไรก็ดี การนำข้อมูลขนาดใหญ่มาปรับใช้ในงานของภาครัฐและเอกชนยังมีข้อห่วงใยที่ยังไม่สามารถหาข้อสรุปได้ สืบเนื่องจากในปัจจุบันมีหลายองค์กรผู้เป็นเจ้าของโดเมนซึ่งถือเป็นบุคคลที่สามที่จัดทำการเก็บข้อมูลส่วนตัวของผู้ใช้ อาทิ โรงพยาบาล ที่พิจารณานำข้อมูลขนาดใหญ่มาปรับใช้ประโยชน์ในหลายๆ ด้านเพิ่มมากขึ้นแต่การพัฒนาระบบการรักษาความปลอดภัยของผู้ใช้ (User) ที่ยังไม่รัดกุมเพียงพอเพราะอาจต้องใช้งบประมาณในการลงทุนจำนวนมาก ส่งผลให้ความเสี่ยงการละเมิดข้อมูลความเป็นส่วนตัวของผู้ใช้งานมีโอกาสเพิ่มมากขึ้นตามไปด้วย มากไปกว่านั้นการจัดการข้อมูลความเป็นส่วนตัวที่โดยบุคลากรที่เกี่ยวข้องที่

[26] Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

ยังขาดความรู้ความเข้าใจในการจัดการข้อมูลผู้ใช้ที่เหมาะสมอาจก่อให้เกิดการรั่วไหลของข้อมูลซึ่งอาจมีผู้ไม่หวังดีนำข้อมูลความเป็นส่วนตัวของผู้ใช้ไปคุกคาม[27] หาผลประโยชน์ต่อไปได้

กล่าวได้ว่าในปัจจุบันประเทศสหรัฐอเมริกามีการนำเทคโนโลยีใหม่ๆ เข้ามาวิเคราะห์ข้อมูลขนาดใหญ่เพื่อช่วยเพิ่มประสิทธิภาพและความน่าเชื่อถือของข้อมูลในงานบังคับใช้กฎหมายเพื่อการป้องกันและปราบปรามอาชญากรรมในด้านต่างๆ อาทิ การนำทรัพยากรในหน่วยงานบังคับใช้กฎหมายที่มีอยู่อย่างจำกัดมาใช้อย่างมีประสิทธิภาพมากขึ้น การปรับปรุงการพยากรณ์และการป้องกันยับยั้งเหตุอาชญากรรมเชิงรุกเพื่อลดอัตราการเกิดอาชญากรรม[28] เป็นสำคัญ อีกทั้งเจ้าหน้าที่บังคับใช้กฎหมายในสถาบันยุติธรรมทางอาญาต่างๆ ในประเทศสหรัฐอเมริกามีการใช้เทคโนโลยีปัญญาประดิษฐ์ (AI : Artificial Intelligence) เป็นเครื่องมือในการวิเคราะห์ข้อมูลขนาดใหญ่เพื่อการพยากรณ์อาชญากรรมอย่างเป็นพื้นฐานการปฏิบัติงานประจำวัน อาทิ หน่วยงานบังคับใช้กฎหมาย ผู้พิพากษา คณะกรรมการพักการลงโทษ ผู้บัญชาการตำรวจ ตำรวจสายตรวจ ผลลัพธ์ที่ได้จากการวิเคราะห์ข้อมูลขนาดใหญ่โดยเทคโนโลยีปัญญาประดิษฐ์จะช่วยให้เจ้าหน้าที่บังคับใช้กฎหมายต่างๆ มีข้อมูลที่ครอบคลุมของผู้ต้องสงสัย ผู้กระทำความผิด และนักโทษทัณฑ์บน ซึ่งข้อมูลเชิงการสันนิษฐานที่แสดงผลแก่เจ้าหน้าที่บังคับใช้กฎหมายโดยอัตโนมัติเหล่านี้จะแสดงผลได้อย่างปราศจากอคติ เพราะระบบเทคโนโลยีได้ทำการวิเคราะห์ข้อมูลขนาดใหญ่บนหลักการที่ ปลอดค่านิยม (Value-Free) ความเป็นกลางทางด้านความเชื่อศาสนา (rigorous—neutral) ความเสถียร (consistent) ซึ่งจะช่วยให้เจ้าหน้าที่ผู้ปฏิบัติงานสามารถเกิดการตัดสินใจในระดับองค์กรแบบมีหลักฐานเป็นพื้นฐานได้มากกว่าเดิม[29]

---

[27] Mehmood, Abid & Natgunanathan, Iynkaran & Xiang, Yong & Hua, Guang & Guo, Song. (2016). Protection of Big Data Privacy. Retrieved from researchgate: https://www.researchgate.net/publication/301716085_Protection_of_Big_Data_Privacy

[28] Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

[29] Shapiro, A. (2019, September). Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. Retrieved from Surveillance & Society. Vol 17 No 3/4 (2019): Visibilities and New Models of Policing : https://www.researchgate.net/publication/338419815_Predictive_Policing_for_Reform_Indeterminacy_and_Intervention_in_Big_Data_Policing

1.2 แนวทางในการใช้ข้อมูลขนาดใหญ่ (Bid data) ในการป้องกันและปราบปรามอาชญากรรม

ภาครัฐและเอกชนในประเทศสหรัฐเมริกาได้มีการใช้ประโยชน์จากข้อมูลขนาดใหญ่ผ่านการวิเคราะห์ข้อมูลนวัตกรรมเทคโนโลยีเพื่อวัตถุหลายๆ ด้าน เช่น การพยากรณ์ปรากฏการณ์ทางสังคม (social phenomenon) ตัวอย่างเช่น เว็บไซต์ดีไซน์ดอทคอม (Decide.com) แสดงผลการคาดคะเน (predicts) ข้อมูลด้านราคาของสินค้าอิเล็กทรอนิกส์ในอนาคต (price of electronic products) เว็บไซต์โอบาม่าดอทคอม (Obama.com) ได้วิเคราะห์ข้อมูลขนาดใหญ่เพื่อพยากรณ์ผลการเลือกตั้งประธานาธิบดีล่วงหน้า[30] เป็นต้น ทั้งนี้รวมถึงวัตถุประสงค์ด้านการใช้เพื่อพยากรณ์อาชญากรรมของรัฐด้วย โดยประเทศสหรัฐอเมริกาได้พัฒนากลยุทธ์การป้องกันและปราบปรามอาชญากรรมขึ้นจากแนวคิดการพยากรณ์อาชญากรรมล่วงหน้าโดยใช้เทคโนโลยีเป็นเครื่องมือในการวิเคราะห์ข้อมูลขนาดใหญ่เพื่อลดอัตราการเกิดอาชญากรรมมาตั้งแต่ช่วงปี ค.ศ. 2000 และตามหลักแนวคิดการพยากรณ์อาชญากรรมล่วงหน้า (Predictive Policing Theory) เจ้าหน้าที่ผู้บังคับใช้กฎหมายจะได้รับข้อมูลเชิงแนวทางการดำเนินงานเพื่อการพยากรณ์อาชญากรรมล่วงหน้าด้วยกัน 3 ด้าน คือ 1) การคาดคะเนผู้ที่มีโอกาสก่อเหตุอาชญากรรมล่วงหน้า (Methods for predicting offenders) 2) การระบุคุณลักษณะผู้กระทำความผิดล่วงหน้า (predicting perpetrators' identities) และ 3) การพยากรณ์ผู้ที่มีโอกาสเป็นเหยื่ออาชญากรรมล่วงหน้า (Methods for predicting victims)[31]

ปัจจุบันหน่วยงานบังคับใช้กฎหมายในประเทศสหรัฐอเมริกาใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big data) ผ่านเครื่องมือต่างๆ ที่ผลิตจากเทคโนโลยีในโลกยุคโลกาภิวัฒน์เพื่อช่วยเสริมประสิทธิภาพและเพิ่มความน่าเชื่อถือของข้อมูลสำหรับใช้ในการปฏิบัติงานป้องกันและปราบปรามอาชญากรรม อาทิ ระบบสารสนเทศอาชญากรรม (Crime information systems) ซอฟต์แวร์ และสื่อสังคมออนไลน์ (Social media) บนเครือข่ายอินเตอร์เน็ต เจ้าหน้าที่บังคับใช้กฎหมายได้มีการใช้ประโยชน์ข้อมูลขนาดใหญ่ที่ผ่านการประมวลผลด้วยระบบคอมพิวเตอร์ในหลากหลายด้านเริ่มตั้งแต่ การดำเนินงานด้านเฝ้าระวังติดตาม การออกตรวจตรา การสืบสวน การวิเคราะห์อาชญากรรม และการบริหารความเสี่ยง ในงานเฝ้าระวังติดตาม ซึ่งงานเฝ้าระวังติดตามนี้สามารถจำแนกออกเป็น 2 ประเภทหลัก ได้แก่ การเฝ้าระวังเฉพาะเจาะจง (directed

---

[30] TaeHeon Moon, SunYoung Heo, SangHo Lee. (2014). Ubiquitous Crime Prevention System (UCPS) for a Safer City. Retrieved from ScienceDirect, Procedia Environmental Sciences, Volume 22, 2014: https://www.sciencedirect.com/science/article/pii/S1878029614001753?via%3Dihub

[31] Brayne, Rosenblat, & Boyd. (2015, October). Predictive Policing. Retrieved from datacivilrights.org: https://datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf

surveillance) และการเฝ้าระวังไม่เฉพาะเจาะจงผ่านเทคโนโลยี (dragnet surveillance)[32] อนึ่ง นวัตกรรมเทคโนโลยีที่เจ้าหน้าที่ตำรวจในประเทศสหรัฐอเมริกาใช้เป็นเครื่องมือในการประมวลผลข้อมูลขนาดใหญ่เพื่อคาดคะเนการเกิดอาชญากรรมล่วงหน้าในปัจจุบันมีอยู่อย่างหลากหลาย โดยนวัตกรรมที่เป็นที่นิยมและน่าสนใจมีรายละเอียดดังต่อไปนี้

1.2.1 ระบบสารสนเทศอาชญากรรม (Crime information systems)[33]

ระบบสารสนเทศอาชญากรรมที่ถูกนำมาใช้ประโยชน์ในโลกยุคปัจจุบันถูกแบ่งออกเป็น 2 ประเภท คือ 1. ระบบเว็บไซต์ และ 2. ระบบโทรศัพท์เคลื่อนที่ โดยในระบบแรกจะมีวิธีการสืบค้นข้อมูลโดยการค้นหาข้อมูลในเว็บไซต์ โดยใช้ Keyword หรือ คำสำคัญ เพื่อเป็นสืบค้นเนื้อหาสารสนเทศต่างๆ รวมถึงข้อมูลอาชญากรรม ส่วนอีกระบบหนึ่งคือระบบโทรศัพท์เคลื่อนที่จะมี Mobile Application หรือโปรแกรมที่อำนวยความสะดวกในด้านต่างๆ ที่ออกแบบมาสำหรับใช้บนสมาร์ทโฟน อาทิ บนสมาร์ทโฟนระบบปฏิบัติการไอโอเอส (iOS) มีชื่อเดิมว่า iPhone OS จะสามารถเข้าถึงโปรแกรมประยุกต์ได้ผ่านทาง APP Store ส่วนโทรศัพท์เคลื่อนที่ระบบปฏิบัติการแอนดรอยด์ (Android) จะสามารถเข้าถึงได้จากโปรแกรมประยุกต์ต่างๆ อาทิ KT Olleh, SKT store และอื่นๆ เป็นต้น ถือเป็นเครื่องมือในระบบสารสนเทศอาชญากรรม ทั้งนี้การพัฒนาโปรแกรมประยุกต์บนอุปกรณ์สื่อสารเคลื่อนที่มักมีการเปลี่ยนแปลงไปอย่างรวดเร็วตามกระแสโลกาภิวัตน์และการเติบโตของเทคโนโลยีในโครงข่ายอินเตอร์เน็ตที่ทำให้โลกเกิดการเชื่อมโยงผ่านการรับส่งข้อมูลจำนวนมหาศาลได้อย่างรวดเร็ว ในขณะเดียวก็มีการบันทึกข้อมูลการติดต่อสื่อสารไว้บนอินเทอร์เน็ตผ่านระบบการเก็บข้อมูลที่สามารถเข้าถึงได้จากทั่วทุกหนแห่งทั่วโลก

ในประเทศสหรัฐอเมริกามีการใช้ระบบสารสนเทศอาชญากรรม (Crime information systems) เพื่อการป้องกันและปราบปรามอาชญากรรมอย่างกว้างขวางในหลายๆ รัฐ อาทิ เมืองซานฟรานซิสโก (San Francisco) ในรัฐแคลิฟอร์เนีย หน่วยราชการมีการใช้ระบบเว็บไซต์และระบบโทรศัพท์เคลื่อนที่ เพื่อเผยแพร่

---

[32] Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

[33] TaeHeon Moon, SunYoung Heo, SangHo Lee. (2014). Ubiquitous Crime Prevention System (UCPS) for a Safer City. Retrieved from ScienceDirect, Procedia Environmental Sciences, Volume 22, 2014: https://www.sciencedirect.com/science/article/pii/S1878029614001753?via%3Dihub

ข้อเท็จจริงต่างๆ สำหรับเตือนภัยประชาชนหรือป้องกันอาชญากรรม (Crime prevention) อาทิ เว็บไซต์ดาต้าเอสเอฟ หรือ Data SF '(http://sanfrancisco.crimespotting.org/)' ของสำนักงานตำรวจในรัฐแคลิฟอร์เนียที่ให้บริการข้อมูลแก่ประชาชนในพื้นที่ด้วยกันหลากหลายด้าน เช่น ด้านอัตราการเกิดอาชญากรรม แผนที่ ชื่อถนน ข้อมูลทางหลวง และสำนักงานตำรวจในพื้นที่ที่สามารถให้บริการประชาชน ข้อมูลดังกล่าวจะช่วยให้เกิดความตระหนักรู้ภัยและลดความเสี่ยงจากเหตุอาชญากรรมเพราะประชาชนสามารถที่จะใช้แหล่งข้อมูลในระบบสาระสนเทศของทางการเพื่อค้นหาข้อมูลพื้นที่ ๆ ที่เกิดเหตุอาชญากรรมล่าสุด อีกทั้งประชาชนยังสามารถนำข้อมูลที่ได้มาต่อยอดเพื่อค้นหาชื่อเขตพื้นที่ ๆ และค้นหาอันดับการเกิดเหตุอาชญากรรมจากสูงไปต่ำได้ โดยใช้เขตพื้นที่เป็นฐาน รวมถึงยังสามารถค้นหาข้อมูลการเกิดอาชญากรรมในพื้นที่โดยรอบได้อีกด้วย นอกจากนี้ยังมีบรณาการทำงานร่วมกับตำรวจในการเผยแพร่รายงานอาชญากรรม (Crime Reports) ในเว็บไซต์ '(https://www.crimereports.com/)' เพื่อให้บริการข้อมูลแก่ประชาชนอย่างเป็นทางการเกี่ยวกับข้อมูลอาชญากรรมของ 15 รัฐ ในประเทศสหรัฐอเมริกา โดยในเว็บไซต์ดังกล่าวจะมีการวิเคราะห์ข้อมูลอาชญากรรมที่เกิดขึ้นในเดือนที่ผ่านมาและทำการเผยแพร่ผลการวิเคราะห์ข้อมูลดังกล่าวแก่สาธารณะชนทราบบนหน้าเว็บไซต์ ในขณะเดียวกันก็ยังมีการพัฒนาประแกรมประยุกต์ ที่สามารถเชื่อมโยงผู้ใช้เพื่อรับบริการการแจ้งเตือนต่างๆ จากทางราชการผ่านจดหมายอิเล็กทรอนิกส์ หรือโทรศัพท์เคลื่อนที่ได้

1.2.2 สื่อสังคมออนไลน์ (Social media)[34]

เจ้าหน้าที่ตำรวจในประเทศสหรัฐอเมริกาได้มีการนำข้อมูลขนาดใหญ่จากแหล่งสื่อสังคมออนไลน์ (Social media) มาใช้ในการปฏิบัติหน้าที่ด้านงานการสืบสวนเพื่อการวิเคราะห์อาชญากรรม การคาดคะเนอาชญากรรมล่วงหน้า และสร้างความตระหนักรู้สถานการณ์ให้แก่ประชาชน ตลอดจนมีการนำข้อมูลขนาดใหญ่จากแหล่งดังกล่าวมาปรับใช้ในการดำเนินคดีด้วยอีกทางหนึ่ง ดังตัวอย่างเช่น เจ้าหน้าที่ตำรวจในนครลอสแอนเจลิส (Los Angeles Police Department; LAPD) ได้มีการอธิบายถึงระบบ "automatic data grazing" ในระยะทดลองว่าเป็นระบบที่ช่วยแสวงหาข้อมูลที่มีลักษณะความเหมือน (similarities) ในคดีต่างๆ ที่ข้ามขอบเขตอำนาจศาล (cross jurisdictional boundaries) ซึ่งส่งผลให้เจ้าพนักงานสืบค้นหาข้อมูล

[34] Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

ในอดีตที่ถูกบันทึกไว้ในศาลไม่พบเนื่องจากแต่ละหน่วยงานมีการบันทึกข้อมูลแบบแยกกันทำให้ไม่สามารถนำข้อมูลในระบบออกมาใช้ได้ทันสถานการณ์ หรือที่เรียกว่า “Jurisdictional data silos” อนึ่งจากการวิจัยแบบสำรวจขององค์การตำรวจอาชญากรรมระหว่างประเทศ แห่งสำนักงานอธิบดีกรมตำรวจ ในปี ค.ศ. 2015 (International Association of Chiefs of Police) รายงานว่าหน่วยงานในสำนักงานกรมตำรวจกว่า 96% ใช้สื่อสังคมออนไลน์ (Social media) เพื่อบรรลุวัตถุประสงค์ต่างๆ ในการปฏิบัติงาน จากสำนวนการฟ้องในพื้นที่นครนิวยอร์กพบว่าหลักฐานประกอบในสำนวนฟ้อง (indictment documents) คิดเป็นกว่า 48% มาจากกิจกรรมที่เผยแพร่บนสื่อสังคมออนไลน์หรือมีการติดต่อสื่อสารผ่านสื่อสังคมออนไลน์ กรมตำรวจนครนิวยอร์กได้ริเริ่มกลยุทธ์ “Operation Crew Cut” ซึ่งเป็นกลยุทธ์การติดตามบัญชีสื่อสังคมออนไลน์ของสมาชิกแก๊งผู้ต้องสงสัย (suspected gang members) ก่อนจะมีการก่ออาชญากรรมเกิดขึ้น โดยกลยุทธ์นี้ตำรวจแห่งนครนิวยอร์กได้ใช้สื่อสังคมออนไลน์เชื่อมโยงและมีปฏิสัมพันธ์ระหว่างกลุ่มผู้ต้องสงสัยเพื่อสร้างความสัมพันธ์รายคนต่อในโลกแห่งความเป็นจริง อย่างไรก็ดีแม้กลยุทธ์การใช้โซเชี่ยลมีเดีย “social media policing” จะมีส่วนช่วยในการวิเคราะห์ข้อมูลขนาดใหญ่จากแหล่งสื่อสังคมออนไลน์รูปแบบต่างๆ อาทิ การสกัดข้อมูล (Data mining) จากทวิตเตอร์ (Twitter) เพื่อตรวจหากิจกรรมของกลุ่มบุคคลที่มีความเสี่ยงจะก่ออาชญากรรมนั้นถูกจัดว่าเป็นการสืบหาข้อมูลในชุดข้อมูลขนาดเล็กซึ่งชุดข้อมูลขนาดเล็กนี้เป็นข้อมูลที่เข้าถึงได้ง่าย สามารถนำไปใช้ต่อได้ และเชื่อมโยงกับผู้คนได้ทันที แต่ในการสืบค้นนั้น ยังคงจำเป็นต้องใช้มนุษย์ในการสืบค้นป้อนข้อมูล เพราะระบบไม่สามารถดำเนินการได้เองโดยอัตโนมัติ

นอกการนำข้อมูลขนาดใหญ่มาใช้ในงานสืบสวนแล้ว ข้อมูลขนาดใหญ่ยังถูกนำมาปรับใช้เพื่อการข่าวกรองสำหรับขับเคลื่อนการดำเนินคดีและบังคับใช้กฎหมาย (intelligence-driven prosecution) โดยศาลในประเทศสหรัฐอเมริกาใช้ประโยชน์จากข้อมูลขนาดใหญ่โดยผ่านเทคโนโลยีเพื่อการคาดการณ์อาชญากรรมล่วงหน้า (Predictive technology) เพื่อคำนวนหาความน่าจะเป็นในด้านการกระทำความผิดซ้ำ (recidivism) สำหรับช่วยประกอบการตัดสินใจของผู้บังคับใช้กฎหมายที่ดำเนินงานในด้านที่เกี่ยวข้องกับการประกันตัว การพิพากษาวางโทษ การพักการลงโทษ[35] นอกจากนี้ สำนักงานอัยการเขตแมนฮัตตันเป็นอีกหน่วยงานหนึ่งที่ได้ปรับใช้ข้อมูลขนาดใหญ่เพื่อการข่าวกรองสำหรับขับเคลื่อนการดำเนินคดีและบังคับใช้กฎหมาย (intelligence-driven prosecution) โดยหน่วยกลยุทธ์อาชญากรรม สำนักงานอัยการเขตแมน

[35] Sarah Brayne, Angèle Christin. (2020). Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts, Social Problems, spaa004, https://doi.org/10.1093/socpro/spaa004

ฮัตตันได้ทดลองงานดำเนินคดีโดยจำลองรูปแบบคดีขึ้นมาในหัวข้อ “primary crime drivers” ในละแวกบ้าน มีการนำซอฟต์แวร์ “target tracker” ซึ่งเป็นโปรแกรมเกี่ยวกับการติดตามความก้าวหน้าและประเมินผลไปใช้กับผู้ใช้งานรายบุคคลในผู้ที่มีภาพถ่าย ประวัติอาชญากรรม และข้อมูลส่วนตัวอื่นๆ อยู่ในระบบ ผลปรากฏว่าโปรแกรมไม่สามารถทำให้กลุ่มเป้าหมายถูกจับกุมได้ตามหลักฐานที่มีอยู่ในระบบ แต่หากเป้าหมายเคยถูกจับกุมมาก่อนระบบจะมีการแจ้งเตือนโดยอัตโนมัติไปที่สำนักงานอัยการทำให้อัยการสามารถตรวจสอบข้อมูลต่างๆ ได้ตั้งแต่ในระยะแรกๆ อาทิ ข้อมูลด้านการขอประกันตัว การฝากขังก่อนการพิจารณาคดี โทษปรับ และข้อพิจารณาโทษหนัก การนำซอฟต์แวร์ดังกล่าวมาปรับใช้ในงานดำเนินคดีถือเป็นเทคโนโลยีใหม่ที่ช่วยเสริมการปฏิบัติงานของพนักงานอัยการให้สามารถตอบสนองได้ทันต่อสถานการณ์ซึ่งเป็นสิ่งที่ไม่สามารถทำได้ในอดีตมาก่อน[36]

1.2.3 ซอฟต์แวร์กระบวนการคำสั่งหรือเงื่อนไขที่สร้างไว้แบบทีละขั้นตอนสำหรับการพยากรณ์อาชญากรรมล่วงหน้า (Algorithmic predictive policing)[37]

ในงานเฝ้าระวัง (Surveillance) เพื่อการป้องกันและปราบปรามอาชญากรรม เจ้าหน้าที่บังคับใช้กฎหมายในสหรัฐฯ ได้นำข้อมูลขนาดใหญ่มาใช้ประโยชน์ผ่านกระบวนการคำสั่งที่สร้างไว้แบบทีละขั้นตอนหรืออัลกอริทึม (Algorithm) สำหรับการพยากรณ์อาชญากรรมล่วงหน้า (Algorithmic predictive policing) เพื่อเป็นเครื่องมือในการคาดคะเนการคุณลักษณะบุคคล (Individual) หรือพื้นที่ (Areas) /สถานที่ (Places) ที่มีโอกาสจะเกิดเหตุอาชญากรรมล่วงหน้า โดยรูปแบบงานเฝ้าระวังสามารถแบ่งออกเป็น 2 ประเภทหลักได้ดังนี้ คือ 1. การเฝ้าระวังแบบเฉพาะเจาะจง (directed surveillance) และ 2. การเฝ้าระวังไม่เฉพาะเจาะจงผ่านเทคโนโลยี (dragnet surveillance) ซึ่งทั้ง 2 รูปแบบมีความแตกต่างกันคือ การเฝ้าระวังแบบเฉพาะเจาะจง (directed surveillance) จะให้ความสำคัญกับการตรวจและติดตามเฉพาะเจาะจงรายบุคคล (individuals) และสถานที่ (places) ที่มีความเสี่ยงนำไปสู่การเกิดอาชญากรรม ส่วนการเฝ้าระวัง

---

[36] Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

[37] Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

ไม่เฉพาะเจาะจงผ่านเทคโนโลยี (dragnet surveillance) จะเป็นการเฝ้าระวังที่ไม่เฉพาะเจาะจงกลุ่มบุคคลหรือหลักภูมิศาสตร์ใดๆ แต่จะเป็นการเก็บรวบรวมข้อมูลของประชาชนทุกคนในภาพรวม (everyone) ดังมีนักวิชาการได้ให้นิยามการเฝ้าระวัง (Surveillance) ไว้ว่าเป็น “การเก็บข้อมูลและวิเคราะห์ข้อมูลประชากรศาสตร์เพื่อกำกับควบคุมพฤติกรรมของประชาชนหมู่มากให้อยู่ในกรอบกฎเกณฑ์ของสังคม”[38] ดังมีรายละเอียดต่อไปนี้

1. การเฝ้าระวังแบบเฉพาะเจาะจง (Directed surveillance)

กระบวนการคำสั่งหรือเงื่อนไขที่สร้างไว้แบบทีละขั้นตอนสำหรับการพยากรณ์อาชญากรรมล่วงหน้า (Algorithmic predictive policing) ซึ่งถูกนิยามไว้อย่างกว้างขวางว่าเป็นระบบการปฏิบัติการทางตรรกะ หรือคณิตศาสตร์ (Logical Operations) ที่สามารถระบุ/กำหนดเหตุการณ์ (specified sequence) ได้อย่างเป็นทางการโดยการป้อนคำสั่งแบบทีละขั้นตอนเพื่อให้เกิดการประมวลผลข้อมูลแสดงตัวเลือกเพื่อการตัดสินใจอัตโนมัติ (automate decisions) โดยระบบคอมพิวเตอร์[39] ถือเป็นกลยุทธ์การดำเนินงานเฝ้าระวังที่ถูกปรับใช้มากที่สุด เครื่องมือในการพยากรณ์อาชญากรรมล่วงหน้านี้จะสามารถให้ข้อมูลเชิงแนวทางการปฏิบัติงานแก่เจ้าหน้าที่ตำรวจก่อนออกปฏิบัติการ อัลกอริทึมจะประมวลผลข้อมูลขนาดใหญ่และแสดงผลข้อมูลด้านบุคคล (Whom) และสถานที่ (Where) เพื่อเป็นประโยชน์ในการตัดสินใจ (police decision making) สำหรับการคาดคะเนคุณลักษณะผู้ต้องสงสัยที่แนวโน้มโน้มจะก่ออาชญากรรมล่วงหรือสถานที่ที่มีโอกาสจะเกิดเหตุอาชญากรรมในอนาคตของเจ้าหน้าที่ตำรวจต่อไป โดยในรายละเอียดจะได้กล่าวในหัวข้อต่อไป อนึ่งสถานีตำรวจในประเทศสหรัฐอเมริกามีการปรับใช้ซอฟต์แวร์กระบวนการคำสั่งหรือเงื่อนไขที่สร้างไว้แบบทีละขั้นตอนสำหรับการพยากรณ์อาชญากรรมล่วงหน้า (Algorithmic predictive policing) อย่างแพร่หลาย จากผลการวิจัยสำรวจ (Survey) เกี่ยวกับการปรับใช้เครื่องมือดังกล่าวของหน่วยงานในกรมตำรวจประเทศสหรัฐอเมริกาจำนวน 200 แห่งในปี ค.ศ. 2014 พบว่ามีหน่วยงานในสังกัดกรมตำรวจที่ใช้เครื่องมือกระบวนการคำสั่งหรือเงื่อนไขที่สร้างไว้แบบทีละขั้นตอนสำหรับการพยากรณ์อาชญากรรมล่วงหน้า (Algorithmic predictive policing) ในงานเฝ้าระวัง โดยคิดเป็น 38% จากหน่วยงาน

---

[38] Haggerty KD, Ericson RV. 2006. The New Politics of Surveillance and Visibility. P.3. Toronto: Univ. Toronto Press

[39] Barocas S, Rosenblat A, boyd d, Gangadharan SP, Yu C. (2014, October). Data & civil rights: technology primer. Retrieved from Data & Civil Rights: Why “Big Data” Is a Civil Rights Issue, Washington, DC: https://papers. ssrn.com/sol3/papers.cfm?abstract_id=2536579

ในกรมตำรวจจำนวน 200 แห่ง ส่วนอีก 70% มีกำหนดการว่าจะปรับใช้เครื่องมือดังกล่าวในการดำเนินงานด้านการเฝ้าระวังในปี ค.ศ. 2017[40]

เทคโนโลยีกระบวนการคำสั่งหรือเงื่อนไขที่สร้างไว้แบบทีละขั้นตอนสำหรับการพยากรณ์อาชญากรรมล่วงหน้า (Algorithmic predictive policing) ถือเป็นเทคโนโลยีที่ใช้ในกลยุทธ์การปฏิบัติการต่างๆ ของเจ้าหน้าที่ตำรวจในประเทศสหรัฐอเมริกา รวมถึงกลยุทธ์ด้านการดำเนินงานเฝ้าระวังแบบเฉพาะเจาะจง (Directed Surveillance) ซึ่งสามารถจำแนกออกเป็น 2 กลยุทธ์หลักๆ ได้แก่ 1.1 กลยุทธ์การเฝ้าระวังแบบมีสถานที่เป็นฐานเพื่อการพยากรณ์อาชญากรรมล่วงหน้า (Place-based predictive policing) และ 1.2 กลยุทธ์การเฝ้าระวังแบบมีบุคคลเป็นฐานเพื่อการพยากรณ์อาชญากรรมล่วงหน้า (Person-based predictive policing) มีรายละเอียดปรากฏดังต่อไปนี้

1.1 กลยุทธ์การเฝ้าระวังแบบมีสถานที่เป็นฐานเพื่อการพยากรณ์อาชญากรรมล่วงหน้า (Place-based predictive policing)

กลยุทธ์นี้เป็นการคาดคะเนช่วงระยะเวลาและสถานที่ที่มีโอกาสจะเกิดเหตุอาชญากรรมได้สูงในอนาคตโดยใช้ข้อมูลประวัติอาชญากรรมในอดีต (retrospective crime data) ป้อนเข้าไปในซอฟต์แวร์ที่ใช้กระบวนการเงื่อนไขที่สร้างไว้แบบทีละขั้นตอน หรืออัลกอริทึม (Algorithm) เป็นพื้นฐานในการพยากรณ์ โดยซอฟต์แวร์อัลกอริทึมเพื่อการวิเคราะห์ข้อมูขขนาดใหญ่ในการพยากรณ์อาชญากรรมล่วงหน้าที่เป็นที่นิยมในปัจจุบัน คือ ซอฟต์แวร์เพร็ดโพลอัลกอริทึม (PredPol’s algorithm) และซอฟต์แวร์ฮันช์แล็บ (HunchLab) อนึ่ง ปัจจุบันมีหน่วยงานในสังกัดกรมตำรวจของสหรัฐอเมริกาจำนวน 60 หน่วยงานที่ใช้ซอฟต์แวร์เพร็ดโพลอัลกอริทึม (PredPol’s algorithm) เป็นเครื่องมือในการคาดคะเนช่วงเวลาและสถานที่เสี่ยงจะเกิดอาชญากรรมในอนาคต โดยหน่วยงานในสังกัดกรมตำรวจที่มีการปรับใช้เครื่องมือดังกล่าวมากที่สุด คือกรมตำรวจนครลอสแอนเจลิส ทั้งนี้บริษัทผู้พัฒนาซอฟต์แวร์อัลกอริทึมการพยากรณ์อาชญากรรมล่วงหน้า (predictive policing company) ที่ใหญ่ที่สุดคือบริษัทเพร็ดโพล “PredPol” ซึ่งเป็นผู้สร้างซอฟต์แวร์เพร็ดโพลอัลกอริทึม (PredPol’s algorithm) โดยซอฟต์แวร์อัลกอริทึมนี้จะใช้ข้อมูลขนาดใหญ่จากระบบการบริหารจัดการเกี่ยวกับการบันทึกข้อมูล (record management systems) ของกรมตำรวจมาวิเคราะห์เพื่อการพยากรณ์อาชญากรรม โดยข้อมูลที่มีอยู่ในฐานข้อมูลของกรมตำรวจในด้านสถานที่

[40] Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

(location) ประเภท (type) เวลาที่เกิดอาชญากรรม (time of crimes) จะถูกป้อนเข้าไปในซอฟต์แวร์อัลกอริทึมดังกล่าว จากนั้นข้อมูลจะถูกวิเคราะห์ด้วยซอฟต์แวร์เพร็ดโพลอัลกอริทึม (PredPol's algorithm) นวัตกรรมซอฟต์แวร์นี้จะแสดงผลการพยากรณ์การเกิดอาชญากรรมในรูปแบบการเกิดซ้ำในละแวกใกล้เคียง (near-repeat model) โดยจะให้ข้อมูลเชิงลึกด้านพื้นที่ เช่นสถานที่ใดที่เคยมีเหตุอาชญากรรมเกิดขึ้นระบบจะประมวลผลและแสดงข้อมูลพื้นทีละแวกใกล้เคียง (surrounding area) ให้เป็นพื้นที่ที่มีความเสี่ยงจะเกิดเหตุอาชญากรรมประเภทเดิมขึ้นได้อีกเป็นครั้งที่สองแก่เจ้าหน้าที่ตำรวจลาดตระเวนทราบ[41]

นอกจากนี้ เพร็ดโพลอัลกอริทึม (PredPol's algorithm) ยังสร้างผลิตภัณฑ์ซึ่งเป็นชุดเดียวกับซอฟต์แวร์เพร็ดโพลอัลกอริทึมเพื่อการใช้งานร่วมกันในการเสริมประสิทธิภาพการพยากรณ์และการป้องกันการเกิดอาชญากรรมโดยมีการผลิตกล่องจุดตรวจเพื่อการคาดการณ์อาชญากรรม (predictive boxes) ขนาด 500 ×500 ตารางฟุต ตั้งไว้ในเขตพื้นที่ความรับผิดชอบของตำรวจในพื้นที่ที่มีขนาดเล็กแต่มีอาณาเขตความรับผิดชอบทับซ้อนกัน (overlaying small areas) ตามกลยุทธ์ดังกล่าวได้มีการส่งเสริมให้เจ้าหน้าที่ตำรวจสายตรวจใช้เวลาในการลาดตระเวนพื้นที่ในจุดที่มีกล่องจุดตรวจเพื่อการพยากรณ์ (predictive boxes) อยู่ให้มากขึ้น มีการกำหนดให้ตำรวจสายตรวจดำเนินการลงบันทึกระยะเวลานาทีที่ปฏิบัติหน้าที่ลาดตระเวนด้วยตนเอง (self-reported) ณ กล่องจุดตรวจเพื่อการพยากรณ์ลงบนคอมพิวเตอร์ที่ติดตั้งอยู่ในรถลาดตระเวณของสายตรวจ (in-car computers) อย่างไรก็ดีระยะเวลาในการลาดตระเวณ ณ กล่องจุดตรวจเพื่อการพยากรณ์ ขึ้นอยู่กับดุลยพินิจ (discretion) ของเจ้าหน้าที่ตำรวจสายตรวจ[42]

ตามทฤษฎีการเกิดอาชญากรรมในพื้นที่เดิมซ้ำ (near-repeat theory) เชื่อว่าเมื่ออาชญากรรมเคยเกิดขึ้นในพื้นที่ใดๆ แล้ว พื้นที่นั้นๆ อาจมีโอกาสเกิดอาชญากรรมขึ้นซ้ำได้อีก ดังนั้นแล้วเพื่อให้เกิดการป้องกับเหตุอาชญากรรมในพื้นที่เสี่ยง ทฤษฎีนี้ได้เสนอแนะให้เจ้าหน้าที่ตำรวจสายตรวจใช้ยุทธวิธีแทรกแซง (police intervention) โอกาสที่อาจจะเกิดอาชญากรรมซ้ำในพื้นที่เดิมโดยการออกลาดตระเวนในพื้นที่ที่เคยมีเหตุอาชญากรรมเกิดขึ้นเพื่อระงับยับยั้งโอกาสที่ผู้กระทำความผิดจะบุกรุก

---

[41] G. O. Mohler, M. B. Short, Sean Malinowski, Mark Johnson, G. E. Tita, Andrea L. Bertozzi & P. J. Brantingham (2015) Randomized Controlled Field Trials of Predictive Policing, Journal of the American Statistical Association, 110:512, 1399-1411, DOI: 10.1080/01621459.2015.1077710

[42] Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

(break-ins) พื้นที่เดิมที่เคยก่อเหตุอาชญากรรมไว้แล้วเนื่องจากผู้กระทำความผิด (offenders) มักจะก่อเหตุซ้ำในพื้นที่ที่คุ้นเคย (familiar areas) และการปรากฏตัวของเจ้าหน้าที่ตำรวจ (Police presence) นำไปสู่การลดอัตราการก่อเหตุอาชญากรรมของกลุ่มคนที่มีโอกาสสูงที่จะก่ออาชญากรรมและลดความสูญเสียที่อาจจะเกิดแก่เหยื่ออาชญากรรมล่วงหน้าได้[43]

มากยิ่งกว่านั้น ซอฟต์แวร์ฮันช์แล็บ (HunchLab) เป็นอีกหนึ่งเครื่องมือหลักหรือซอฟต์แวร์หลัก (major predictive policing software) ที่เจ้าหน้าที่ตำรวจในสหรัฐอเมริกาใช้เพื่อการพยากรณ์อาชญากรรม ระบบปฏิบัติการของซอฟต์แวร์ฮันช์แล็บ (HunchLab) [44] มีรูปแบบการทำงานที่สร้างจากแนวคิด “Risk Terrain Model” ซึ่งเป็นแนวคิดที่ใช้กลยุทธ์เชิงภูมิศาสตร์ (GIS techniques) อธิบายถึงวิธีการหาความสัมพันธ์ (Relationship) หรือความเชื่อมโยงระหว่างคุณลักษณะเชิงพื้นที่ (spatial features) ที่อาจนำไปสู่การก่อเหตุอาชญากรรม[45] ดังกล่าวแล้วซอฟต์แวร์ฮันช์แล็บ (HunchLab) จะใช้แนวคิด“Risk Terrain Model” ในการอธิบายถึงความสัมพันธ์ของตัวแปรดังนี้ สังคม (social) พฤติกรรม (behavioral) และปัจจัยเสี่ยงทางกายภาพ (Physical Risk Factor) ในทางกลับกันเมื่อเปรียบเทียบกับรูปแบบเพร็ดโพล (PredPol’s parsimonious model) จะพบว่ารูปแบบฮันช์ (HunchLab’s models) จะมีช่วงตัวแปรที่กว้างและหลากหลาย (wider range of variables)[46] อาทิ ความหลากหลายด้ารประชากรศาสตร์ (population density) สถานที่ประเภทบาร์ (location of bars) โบสถ์ (churches) จุดขนส่ง (transportation hubs) และข้อมูลการสำรวจจำนวนประชากร (census data) อนึ่งในปี ค.ศ. 2017 มีหน่วยงานในสังกัดกรมตำรวจนำซอฟต์แวร์ฮันช์แล็บ (HunchLab) ไปปรับใช้ในการปฏิบัติงานอยู่ด้วยกันหลายหน่วยงาน เช่น กรมตำรวจเมืองฟิลาเดลเฟีย (Philadelphia Police Department) กรมตำรวจเมืองไมอามี่ (Miami Police

---

[43] Brayne, Rosenblat, & Boyd, (2015, October). Predictive Policing. Retrieved from datacivilrights.org: https://datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf

[44] Brayne, S. (2017, August). Big Data Surveillance: The Case of Policing, Vol. 82(5) 977–1008. Retrieved from American Sociological Review: http://users.soc.umn.edu/~uggen/Brayne_ASR_17.pdf

[45] Caplan, J. M. & Kennedy, L. W. (Eds.) 2011. Risk Terrain Modeling Compendium. Newark, NJ: Rutgers Center on Public Security. Retrieved from riskterrainmodeling.com: https://www.rutgerscps.org/uploads/2/7/3/7/27370595/riskterrainmodelingcompendium_caplankennedy2011.pdf

[46] Brayne, Rosenblat, & Boyd, (2015, October). Predictive Policing. Retrieved from datacivilrights.org: https://datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf

Department) กรมตำรวจนครนิวยอร์ก (New York Police Department; NYPD) และอื่นๆ เป็นต้น มีการสนับสนุนว่าการใช้อัลกอริทึมเพื่อการคาดคะเนอาชญากรรมผ่านซอฟต์แวร์จะช่วยให้ทรัพยากรถูกนำมาใช้อย่างมีประสิทธิภาพมากกว่าเดิมเพราะการอ้างอิงข้อมูลจากการประมวลผลโดยอัลกอริทึม ข้อมูลที่ได้จะเป็นข้อมูลที่ปราศจากอคติ จากการศึกษาวิจัยด้านการนำข้อมูลขนาดใหญ่มาใช้ในกรมตำรวจนครลอสแอนเจลิสในปี ค.ศ 2017 พบว่าเจ้าหน้าที่ตำรวจผู้ปฏิบัติงานมีความเห็นสนับสนุนการนำข้อมูลขนาดใหญ่มาใช้ในงาน โดยผู้บังคับการตำรวจนครลอสแอนเจลิสได้อธิบายว่าการปฏิบัติงานของเจ้าหน้าที่ตำรวจที่ใช้การอ้างอิงจากข้อมูล (relying on data) มากกว่าการตีความของมนุษย์ (human interpretation) ในด้านรูปแบบอาชญากรรม (crime patterns) นั้น สามารถช่วยให้เจ้าหน้าที่ตำรวจใช้ทรัพยากรในการปฏิบัติงานได้อย่างมีประสิทธิภาพมากกว่าเดิม[47] อย่างไรก็ดีจากการศึกษาภาคสนาม (Field Trial) ในปีค.ศ. 2015 พบว่าการนำซอฟต์แวร์เพร็ดโพลอัลกอริทึม (PredPol's algorithm) มาใช้ในการวิเคราะห์ข้อมูลขนาดใหญ่เพื่อการพยากรณ์อาชญากรรมล่วงหน้าโดยมีเจ้าหน้าที่ตำรวจสายตรวจเป็นผู้ปรับใช้ผลการวิเคราะห์ข้อมูลที่ได้รับจากซอฟต์แวร์ดังกล่าวในการปฏิบัติงาน ส่งผลต่อการลดจำนวนการเกิดเหตุอาชญากรรม (crime volume) ได้น้อยแต่มีนัยยะสำคัญทางสถิติ (statistically significant reductions)[48]

1.2 กลยุทธ์การเฝ้าระวังแบบมีบุคคลเป็นฐานเพื่อการพยากรณ์อาชญากรรมล่วงหน้า (Person-based predictive policing)

ด้วยกลยุทธ์การเฝ้าระวังแบบมีบุคคลเป็นฐานเพื่อการพยากรณ์อาชญากรรมล่วงหน้า (Person-based predictive policing) จะให้ความสำคัญกับการคาดคะเนการเกิดอาชญากรรมอุกฉกรรจ์ (Violent Crime) ล่วงหน้า โดยหน่วยงานบังคับใช้กฎหมาย (Law enforcement) ใช้วิธีการเชิงวิเคราะห์ (Analytical approach) ข้อมูลขนาดใหญ่ใน 2 วิธี คือ การวิเคราะห์เครือข่ายทางสังคม (Analysis of social network) และการวิเคราะห์ปัจจัยที่มีความเสี่ยงแบบถดถอย (regression analysis of risk factors) เพื่อ

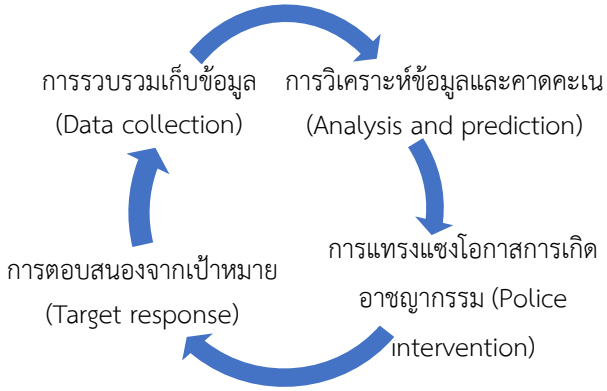
---

[47] Brayne, S. (2017, August). Big Data Surveillance: The Case of Policing, Vol. 82(5) 977–1008. Retrieved from American Sociological Review: http://users.soc.umn.edu/~uggen/Brayne_ASR_17.pdf

[48] Mohler, George & Short, M. & Malinowski, Sean & Johnson, Mark & Tita, George & Bertozzi, Andrea & Brantingham, P. (2015, October). Randomized Controlled Field Trials of Predictive Policing. Retrieved from Journal of the American Statistical Association: https://www.tandfonline.com/doi/abs/10.1080/01621459.2015.1077710?journalCode=uasa20

คาดคะเนคุณลักษณะในรายบุคคลที่มีความเสี่ยงสูงสุดที่จะลงมือก่ออาชญากรรม (highest-risk individuals) หรือบุคคลที่มีโอกาสจะเป็นเหยื่ออาชญากรรม ทั้งนี้ตามข้อสันนิษฐานที่ได้ตั้งไว้ว่ากลุ่มคนที่มีโอกาสในการก่ออาชญากรรมและกลุ่มคนที่มีความเสี่ยงจะกลายเป็นเหยื่ออาชญากรรมความรุนแรงจะคิดเป็นสัดส่วนที่น้อยจากจำนวนประชากรทั้งหมด ดังนั้นสามารถวิเคราะห์ข้อมูลแบบเฉพาะเจาะจงเป็นรายบุคคลได้ ตัวอย่างเช่น ตามรายงานของธรรมเนียบขาวด้านข้อมูลขนาดใหญ่ กรมตำรวจเมืองชิคาโก้ (Chicago) ได้ปรับใช้แนวทางการคาดคะเนความเสี่ยงในผู้ที่มีโอกาสก่ออาชญากรรม (Police modeling risk) โดยการทดลองนำข้อมูลจากเครือข่ายทางสังคม (social network) ของประชากรที่ไม่มีประวัติการก่ออาชญากรรม มาวิเคราะห์เพื่อคาดคะเนคุณลักษณะของบุคคลที่มีโอกาสสูงเกี่ยวข้องกับแก๊งที่ก่อคดีฆาตกรรม (gang-related murders) พบว่าไม่พบคุณลักษณะที่เป็นที่ประจักษ์เพื่อการระบุตัวตนของผู้กระทำความผิดที่เกี่ยวข้องกับคดีฆาตกรรมแต่หลังจากการวิเคราะห์ข้อมูลขนาดใหญ่ในกลุ่มเป้าหมายดังกล่าวเจ้าหน้าที่ตำรวจสามารถสกัดจำนวนผู้ที่อาจมีโอกาสก่อเหตุฆาตกรรมได้ในจำนวน 400 คนจากกลุ่มประชากรเป้าหมายทั้งหมด ซึ่งทั้ง 400 คนเป็นผู้ที่มีรายชื่ออยู่ในบันทึกสาธารณะ (public record) และอาจมีความเสี่ยงจะถูกตั้งข้อหา (charges) และถูกตัดสินลงโทษ (convictions) ในอนาคต หลักการดำเนินงานภายหลังจากการระบุกลุ่มผู้ที่มีโอกาสสูงในการก่ออาชญากรรมคือ เจ้าหน้าที่ตำรวจสามารถดำเนินการอย่างจริงจังในการแทรกแซงโอกาสในการประกอบอาชญากรรม (aggressive interventions) ของกลุ่มบุคคลที่มีความเสี่ยงจะก่อเหตุ เช่น การลาดตระเวน (patrolling) ไปในพื้นที่ที่กลุ่มเสี่ยงอาศัยอยู่และเข้าไปสอบถามพูดคุยกับกลุ่มบุคคลเหล่านั้นหรือสมาชิกในครอบครัวของบุคคลที่ถูกจัดอยู่ในกลุ่มเสี่ยงที่จะก่อเหตุอาชญากรรม[49] ทั้งนี้ กลยุทธ์การเฝ้าระวังแบบมีบุคคลเป็นฐานเพื่อการพยากรณ์อาชญากรรมล่วงหน้า (Person-based predictive policing) หรือกลยุทธ์การเฝ้าระวังแบบมีสถานที่เป็นพื้นฐานเพื่อการพยากรณ์อาชญากรรมล่วงหน้า (Place-based predictive policing) มีขั้นตอนหลักในการพยากรณ์อาชญากรรมล่วงหน้า (stages in the practice of predictive policing) เหมือนกันใน 4 ขั้นตอนคือ 1) การรวบรวมเก็บข้อมูล (Data collection) 2) การวิเคราะห์ข้อมูลและคาดคะเน (Analysis and prediction) 3) การแทรงแซงโอกาสการเกิดอาชญากรรมของเจ้าหน้าที่ตำรวจ (Police intervention) และ 4) การตอบสนองจากเป้าหมาย (Target response) ดังมีรายละเอียดปรากฏตามตารางวงกลมที่ 1

[49] Brayne, Rosenblat, & Boyd. (2015, October). Predictive Policing. Retrieved from datacivilrights.org: https://datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf



ตารางวงกลมที่ 1: ขั้นตอนการพยากรณ์อาชญากรรมล่วงหน้าแบบมีบุคคลและสถานที่เป็นฐาน[50]

2. การเฝ้าระวังแบบไม่เฉพาะเจาะจงผ่านเทคโนโลยี (Dragnet surveillance)

การเฝ้าระวังแบบไม่เฉพาะเจาะจงผ่านเทคโนโลยี (Dragnet surveillance) เป็นการเฝ้าระวังโดยใช้เทคโนโลยีวิเคราะห์ข้อมูลขนาดใหญ่ของประชาชนโดยไม่เฉพาะเจาะจงกลุ่มหรือจำกัดแค่บุคคลผู้ที่มีความเสี่ยงจะก่อเหตุอาชญากรรม โดยเครื่องมือที่ได้รับความนิยมมากที่สุดชนิดหนึ่งที่ใช้ในงานเฝ้าระวังแบบไม่เฉพาะเจาะจงผ่านเทคโนโลยี (Dragnet surveillance) คือระบบตรวจจับและอ่านป้ายทะเบียนรถโดยอัตโนมัติ (Automatic License Plate Reader; ALPR) ซึ่งเป็นนวัตกรรมทางเทคโนโลยีที่สามารถเรียกใช้ประโยชน์ได้ในทันที (static) เช่นขณะอยู่กลางสี่แยกไฟแดง และพกพาเคลื่อนที่ได้ (mobile) เช่น สามารถติดตั้งไว้ในรถของตำรวจสายตรวจ ระบบตรวจจับและอ่านป้ายทะเบียนรถโดยอัตโนมัติ (Automatic License Plate Reader; ALPR) จะทำการถ่ายภาพจำนวน 2 ภาพของทะเบียนรถทุกคันที่วิ่งสวนกับรถที่ติดตั้งโปรแกรมชนิดนี้ โดยรูปหนึ่งจะเป็นภาพถ่ายของพาหนะ ส่วนอีกภาพหนึ่งจะเป็นป้ายทะเบียน มากยิ่งกว่านั้นโปรแกรม ALPR ยังสามารถทำการบันทึกข้อมูลเกี่ยวกับเวลา วันที่ และสถานที่ได้ นอกจากนี้ข้อมูลที่ได้จากการเก็บบันทึกจากโปรแกรม ALPR (ALPR data) มีประโยชน์ในหลายด้าน เช่น เจ้าหน้าที่ตำรวจสามารถเปรียบเทียบตรวจหาพาหนะที่มีใบสำคัญแสดงสิทธิหรือพาหนะที่ถูกขโมยมา รวมถึงสามารถล้อม (fence) พื้นที่เป้าหมายให้แคบลงเพื่อให้เจ้าหน้าที่สามารถดำเนินการติดตามพาหนะของผู้ต้องสงสัยที่

[50] Michael Price. (2013, December). National Security and Local Police. Retrieved from brennancenter.org: https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf

ไปสถานที่ใดๆ อีกทั้งยังสามารถเก็บข้อมูลไว้เพื่อใช้ในงานสืบสวนอื่นๆ ที่เกี่ยวข้องต่อไปได้ โปรแกรมนี้ทำให้เจ้าหน้าที่บังคับใช้กฎหมายสามารถติดตามผู้ที่มีพฤติกรรมต้องสงสัยรายบุคคลได้

อนึ่ง ระบบโดเมนเพื่อการเตือนภัย (Domain Awareness Systems) เป็นอีกหนึ่งซอฟต์แวร์ที่ถูกใช้เป็นเครื่องมือการเฝ้าระวังแบบไม่เฉพาะเจาะจงผ่านเทคโนโลยี (Dragnet surveillance) โดยเครื่องมือชนิดนี้จะมาพร้อมอุปกรณ์กล้องจรปิด (Closed-circuit surveillance cameras) ที่มีความสามารถในตรวจจับการแผ่รังสีโดยใช้เซ็นเซอร์ต่างๆ (radiation sensors) และเซ็นเซอร์ชนิดอื่นๆ ที่ติดตั้งมาในกล้องวงจรปิดดังกล่าว สามารถช่วยตรวจจับคุณลักษณะรายบุคคลที่ตรงกับฐานข้อมูลของตำรวจ (Police Database) โดยเจ้าหน้าที่บังคับใช้กฎหมายในประเทศสหรัฐเมริกาใช้ประโยชน์จากการวิเคราะห์ขั้นสูง (advanced analytics) ของกล้องวงจรปิดระบบนี้ในด้านต่างๆ เช่น การใช้ประโยชน์จากการรู้จำแบบอัลกอริทึม (Pattern Recognition algorithms) เพื่อการตรวจจับภัยคุกคามจากภาพวิดีโอ อาทิ การตรวจจับภาพกระเป๋าสัมภาระที่ไม่มีเจ้าของ (unattended bags)[51] เป็นต้น

2. ประเทศแคนาดา

2.1 ความเป็นมา

ปัจจุบันหลายประเทศได้พัฒนาเทคโนโลยีเพื่อป้องกันและปราบปรามอาชญากรรมให้สามารถวิเคราะห์และตีความข้อมูลขนาดใหญ่ (big data) โดยใช้ปัญญาประดิษฐ์ (AI) ซึ่งเป็นเทคโนโลยีที่ใช้อัลกอริทึมและระบบที่สามารถเรียนรู้ได้จากตัวอย่างด้วยตนเองโดยปราศจากการป้อนคำสั่งของโปรแกรมเมอร์ (machine leaning) ในการปฏิบัติการ[52]

ประเทศแคนาดาใช้ประโยชน์จากข้อมูลขนาดใหญ่ผ่านนวัตกรรมเทคโนโลยีเป็นเครื่องมือในงานยุติธรรมเชิงป้องกัน โดยเครื่องมือทางเทคโนโลยีที่ประมวลผลข้อมูลขนาดใหญ่ด้วยระบบปฏิบัติการต่างๆ นั้นจะช่วยสนับสนุนงานยุติธรรมแก่เจ้าหน้าที่บังคับใช้กฎหมายในการปฏิบัติงานได้ 2 ด้านหลัก คือ 1) การให้ข้อมูลเชิงแนวทางการปฏิบัติงานที่ระบุข้อมูลแบบมีบุคคลเป็นฐาน (Person based) และแบบใช้สถานที่เป็น

---

[51] Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

[52] M. Purcell and M. Zaia. (2020). Prediction, prevention and proof: Artificial intelligence and peach bonds in Canada. The Canadian Bar Review. Vol. 98, pp. 515-542.

ฐาน (Place-based) อันสามารถนำไปสู่การจับกุมดำเนินคดีผู้ที่เกี่ยวข้องได้โดยเจ้าหน้าที่บังคับใช้กฎหมายเข้าไปแทรกแซงโอกาสในการประกอบอาชญากรรมของผู้ที่โอกาสสูงก่ออาชญากรรมในพื้นที่ต่างๆ (targeted intervention) และ 2) การให้หลักฐานเชิงความเสี่ยง (evidence of risk) ในกระบวนการดำเนินคดี (hearing stage)[53] ทั้งนี้การใช้ข้อมูลขนาดใหญ่ (big data) เพื่อการตีความหรือคาดการณ์ที่แม่นยำจำเป็นต้องมีการจัดหาหรือจัดเก็บข้อมูลขนาดใหญ่อยู่อย่างต่อเนื่อง เช่น ข้อมูลเกี่ยวกับบุคคล สถานที่ รวมถึงข้อมูลที่ถูกเก็บรวบรวมโดยเซ็นเซอร์และโทรศัพท์มือถือ เช่น รูปแบบการคลิกและการกดไลค์บนสื่อสังคมออนไลน์หรือโซเชียลมีเดีย[54] โดยในการประมวลผลนั้นปัญญาประดิษฐ์จะแปลงข้อมูลจำนวนมหาศาลให้เป็นผลลัพธ์เชิงสมติฐานเพื่อการคาดการณ์และการระบุตัวตนที่แม่นยำ[55] เช่น การระบุสถานที่เสี่ยงจะเกิดเหตุอาชญากรรม ประเภทของอาชญากรรมที่คาดการณ์ไว้ล่วงหน้า และบุคคลที่มีความเสี่ยงจะเป็นเหยื่ออาชญากรรม[56] ระบบปัญญาประดิษฐ์จะประมวลผลเพื่อให้เกิดการคาดการณ์เชิงสถิติซึ่งผลลัพธ์จากการวิเคราะห์นี้จะสามารถระบุเป้าหมายที่มีโอกาสจะก่ออาชญากรรมล่วงหน้า ทำให้เจ้าหน้าที่ตำรวจสามารถแทรกแซงโอกาสในการเกิดอาชญากรรมหรือยับยั้งเหตุก่อนเกิดได้ อันถือเป็นการป้องกันอาชญากรรมที่ทันต่อสถานการณ์[57]

การใช้ประโยชน์จากข้อมูลขนาดใหญ่ (big data) เพื่อการปรับปรุงความปลอดภัยสาธารณะถือเป็นโอกาสในการปฏิรูปวิธีคิดเกี่ยวกับการทำงานของตำรวจ ปัจจุบันมีแผนกนวัตกรรมจำนวนมากที่ถูกดำเนินการโดยใช้ข้อมูลขนาดใหญ่ (big data) เช่น หน่วยงานตำรวจในเมืองโตรอนโต และเมืองอื่นๆ ในประเทศแคนาดาได้พัฒนาเทคโนโลยีการวิเคราะห์ข้อมูลขนาดใหญ่ (big data) ไปสู่รูปแบบการปฏิบัติการเชิงพยากรณ์ด้วยแนวปฏิบัติการคาดการณ์ที่เรียกว่า ฮับ และ คอร์ (HUB and COR Model) ซึ่งแนวปฏิบัตินี้ช่วยอำนวยให้หน่วยงานตำรวจได้ปฏิบัติหน้าที่เปรียบดังสะพานเชื่อมในการเข้าถึงบริการสังคมอื่นๆ แทนที่จะ

---

[53] Sarah Brayne & Angèle Christin. (2020, March). Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts. Retrieved from Social Problems, spaa004,: https://doi.org/10.1093/socpro/spaa004

[54] N.M. Richards and J. King. Three Paradoxes of Big Data. Stan L Rev Online. 66, pp. 41-46, 2013.

[55] E.E. Joh. Increasing automation in policing," Communications of the ACM. 63, pp. 20-22, 2020.

[56] A.E. Waldman. Power, process, and automated decision-making. Fordham Law Review. 88(2), pp. 613-632, 2019.

[57] W.L. Perry, B. McInnis, C.C. Price, S.C. Smith, and J.S. Hollywood. “Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. Washington” RAND Corporation, 2013.

ให้หน่วยงานต่างๆ ตอบสนองต่อปัญหาสังคมมากมายด้วยเครื่องมือที่มีจำกัด การทำงานเชิงคาดการณ์สะท้อนให้เห็นถึงการให้บริการสังคมตามเป้าหมายซึ่งเป็นกลยุทธ์ที่มีประสิทธิภาพในการลดอาชญากรรม โดยเฉพาะอย่างยิ่งกับอาชญากรรมรุนแรงในกลุ่มเด็กและเยาวชน[58,59]

แนวปฏิบัติการคาดการณ์ ฮับ และ คอร์ (HUB and COR Model) เป็นเครื่องมือที่จำเป็นต้องจะใช้อาศัยข้อมูลที่ถูกเก็บรวบรวมจากหน่วยงานของรัฐหลายๆ แห่งเพื่อตั้งค่าสถานะบุคคลที่มีความเสี่ยงจะกลายเป็นเหยื่ออาชญากรรม ซึ่งโดยมากแล้วมักเป็นกลุ่มผู้เยาว์ ที่ต้องการการดูแลจากภาครัฐหรือมีเจ้าหน้าที่บังคับใช้กฎหมายเข้าคุ้มครองดูแลและแทรกแซงโอกาสการเกิดอาชญากรรมล่วงหน้าแก่กลุ่มเปราะบางเหล่านี้อย่างเร่งด่วน ภายหลังจากการตั้งค่าสถานะจากนั้นบุคคลที่ถูกระบุโดยแบบจำลองความเสี่ยงจะได้รับการตรวจสอบโดยตัวแทนจากหน่วยงานและกลุ่มชุมชนต่างๆ และจะมีแผนตอบสนองอย่างรวดเร็วต่อบุคคลที่ถูกระบุว่ามีความเสี่ยงสูงก่อนที่จะเกิดปัญหาร้ายแรงขึ้น ซึ่งแผนตอบสนองจะถูกปรับให้เหมาะกับความต้องการของแต่ละบุคคลหรือครอบครัว[60]

ขณะนี้มีการใช้ข้อมูลขนาดใหญ่ (big data) ร่วมกับอัลกอริทึมเพื่อการตัดสินใจอัตโนมัติในด้านการบริหาร[61] การตัดสินใจโดยอัตโนมัติถูกนำไปใช้ในหลายๆ ประเทศในบริบทต่างๆ เช่นการตัดสินของศาล และการย้ายถิ่นฐาน จากการเติบโตของอัลกอริทึมทำให้รัฐบาลแคนาดาออกคำสั่งให้นำระบบการตัดสินใจอัตโนมัติไปใช้ในหน่วยงานของรัฐและให้ดำเนินการพัฒนาระบบการตัดสินใจอัตโนมัติไปใช้ในลักษณะที่ช่วยลดความเสี่ยงต่อชาวแคนาดาและสถาบันของรัฐบาลกลางเพื่อให้นำไปสู่การตัดสินใจที่มีประสิทธิภาพ แม่นยำ สอดคล้อง และตีความตามกฎหมายของแคนาดาได้มากขึ้น[62]

---

[58] B.J. Bushman et al. Youth violence: what we know and what we need to know. Am Psychol. 71(1), pp. 17-39, 2016.

[59] W.S. Isaac. Hope, hype, and fear: the promise and potential pitfalls of the big data era in criminal justice. Ohio State Journal of Criminal Law. 15(2), pp. 543-558, 2018.

[60] W.S. Isaac. Hope, hype, and fear: the promise and potential pitfalls of the big data era in criminal justice. Ohio State Journal of Criminal Law. 15(2), pp. 543-558, 2018.

[61] C. Piovesan and V. Ntiri. Adjudication by algorithm: the risks and benefits of artificial intelligence in judicial decision-making. The Advocates' Journal. pp. 42-45, 2018.

[62] M. Purcell and M. Zaia. Prediction, prevention and proof: Artificial intelligence and peach bonds in Canada. The Canadian Bar Review. 98, pp. 515-542, 2020.

ตามการการแถลงการณ์ของรัฐบาลแคนาดานั้น ประแกรมประยุกต์หรือแอปพลิเคชันปัญญาประดิษฐ์ (AI) เชิงคาดการณ์ ซึ่งบางครั้งเรียกว่าระบบการตัดสินใจอัตโนมัติ (ADS) เหล่านี้ช่วยเสริมกระบวนการตัดสินใจของเจ้าหน้าที่โดยนวัตกรรมทางเทคโนโลยีเหล่านี้จะใช้เทคนิคทางสถิติหรือการคำนวณ[63] เนื่องจากระบบการตัดสินใจอัตโนมัติเกี่ยวข้องกับขอบเขตทางกฎหมายจึงได้ถูกแบ่งออกเป็น 2 ประเภท คือ ระบบผู้เชี่ยวชาญด้านกฎหมาย และ การวิเคราะห์เชิงคาดการณ์ ระบบผู้เชี่ยวชาญด้านกฎหมายช่วยให้กระบวนการตัดสินใจทางกฎหมายรวดเร็วและมีประสิทธิภาพ ระบบนี้มีชุดของกฎที่ออกแบบมาเพื่อทำการวิเคราะห์ทางกฎหมายเป็นกรณีๆ ไป ส่วนการวิเคราะห์เชิงคาดการณ์นั้นจะดำเนินการโดยใช้ข้อมูลขนาดใหญ่ (big data) เป็นข้อมูลที่ป้อนเข้าไปในระบบ รวมถึงระบบที่สามารถเรียนรู้ได้จากตัวอย่างด้วยตนเองโดยปราศจากการป้อนคำสั่งของโปรแกรมเมอร์ (machine leaning)[64]

2.2 แนวทางการใช้ข้อมูลขนาดใหญ่ (big data) ในการป้องกันและปราบปรามอาชญากรรม

ข้อมูลขนาดใหญ่ถูกนำไปใช้กับเทคโนโลยีเพื่อการป้องกันและปราบปรามอาชญากรรมของประเทศแคนาดาดังต่อไปนี้

2.2.1 เทคโนโลยีการคาดการณ์ (predictive technology)

เทคโนโลยีการคาดการณ์ถูกนำไปใช้ในกระบวนการยุติธรรมในหลายประเทศทั้งในด้านการรักษากฎหมายและการพิจารณาคดีในศาลอาญา[65] โดยมีหลักการเช่นเดียวกับกระบวนการคาดการณ์โดยมนุษย์ เช่น กระบวนการยุติธรรมเชิงป้องกันในประเทศแคนาดา ศาลอาญาจำเป็นต้องดำเนินการประเมินความเสี่ยงและกำหนดเงื่อนไขต่างๆ ลงในซอฟต์แวร์เพื่อการคาดการณ์อาชญากรรมเพื่อให้ซอฟต์แวร์แสดงมีผลด้านพฤติกรรมในอนาคตของผู้ถูกกล่าวหา (หรือผู้กระทำความผิด) ในการประกันตัว การผูกมัดเสรีภาพและขั้นตอนการพิจารณาคดี[66]

---

[63] W.S. Isaac. Hope, hype, and fear: the promise and potential pitfalls of the big data era in criminal justice. Ohio State Journal of Criminal Law. 15(2), pp. 543-558, 2018.

[64] M. Purcell and M. Zaia. Prediction, prevention and proof: Artificial intelligence and peach bonds in Canada. The Canadian Bar Review. 98, pp. 515-542, 2020.

[65] S.D. Konikoff and A. Owusu-Bemphah. "Big Data and Criminal Justice – What Canadians Should Know" (ND) at 4, online: Broadbent Institute <www.broadbentinstitute.ca> [Konikoff & Owusu-Bemphah].".

[66] M. Purcell and M. Zaia. Prediction, prevention and proof: Artificial intelligence and peach bonds in Canada. The Canadian Bar Review. 98, pp. 515-542, 2020.

ตั้งแต่ปี ค.ศ. 2513 เป็นต้นมานักสังคมศาสตร์ได้เริ่มศึกษาและสร้างเครื่องมือวิจัยเพื่อประเมินความเสี่ยงการกระทำผิดซ้ำ เครื่องมือเหล่านี้ได้ถูกนำมาประยุกต์ใช้อย่างเป็นรูปธรรมในประเทศแคนาดา[67] ซึ่งประเด็นหลักที่เพิ่มประสิทธิผลในการพยากรณ์หรือการคาดการณ์คือการนำปัจจัยเสี่ยงแบบไดนามิก (dynamic risk factor) เข้ามาปรับใช้ในการประกอบการสร้างแบบจำลอง ข้อมูลที่ใช้ในการสร้างแบบจำลองเชิงคณิตศาสตร์เพื่อประเมินความเสี่ยงการกระทำผิดซ้ำแบ่งออกได้เป็น 3 กลุ่ม คือ[68]

1) Static Factors เช่น ประเภทการกระทำผิด อายุปัจจุบัน อายุเมื่อถูกจับครั้งแรก ประวัติการมีงานทำ ประวัติการกระทำผิด ฯลฯ
2) Dynamic Factors เช่น ทัศนคติ กลุ่มเพื่อนที่คบหรือสมาคม สารเสพติดที่ใช้ บุคลิกในมิติด้านการต่อต้านสังคมฯลฯ ซึ่งเป็นข้อมูลที่ต้องดำเนินการเก็บเพิ่มเติมและประเมินคะแนนโดยผู้เชี่ยวชาญ
3) Real-time Data เช่น พฤติกรรม และสถานที่มั่วสุมในเวลาปัจจุบัน

ปัจจุบันตำรวจในประเทศแคนาดามีการใช้เทคโนโลยีการคาดการณ์โดยอาศัยปัญญาประดิษฐ์วิเคราะห์และตีความข้อมูลขนาดใหญ่เพื่อวัตถุประสงค์หลายประการ เช่น การตรวจจับและป้องกันอาชญากรรม[69] ตั้งแต่ปลายปี 2558 กรมตำรวจเมืองแวนคูเวอร์ ประเทศแคนาดาได้ใช้เทคโนโลยีที่เรียกว่าจีโอแดช (GeoDASH) ซึ่งเป็นเทคโนโลยีเพื่อการคาดการณ์เชิงป้องกันที่สามารถพยากรณ์หรือระบุตำแหน่งของอาชญากรรมประเภทอาชญากรรมประทุษร้ายต่อทรัพย์สิน (Property crime) ส่วนกรมตำรวจเมืองซัสแคตเชวัน (Saskatchewan) อยู่ระหว่างการสร้างเทคโนโลยีวิเคราะห์โพสต์บนโซเชียลมีเดียวิเคราะห์บันทึกของตำรวจ และวิเคราะห์ข้อมูลบริการสังคมเพื่อคาดการณ์ผู้ที่มีโอกาสหายตัวไป ในช่วงต้นปี 2563 กรมตำรวจเมืองเอ็ดมอนตัน (Edmonton; EPS) ได้เปิดตัวซอฟต์แวร์ Community Solutions Accelerator ร่วมกับพันธมิตรหลายองค์กร โดยซอฟต์แวร์ Community Solutions Accelerator นั้นใช้

---

[67] J. Bonta and D.A. Andrews. Risk-need-responsivity model for offender assessment and rehabilitation. Rehabilitation. 6, pp. 1-22, 01/01 2007.

[68] กรอบการวิเคราะห์ข้อมูลขนาดใหญ่ภาครัฐ, คณะอนุกรรมการออกแบบสถาปัตยกรรม (Architecture Design), “ระบบบูรณาการข้อมูลภาครัฐภายใต้คณะกรรมการขับเคลื่อนการดำเนินนโยบายเพื่อใช้ประโยชน์ข้อมูลขนาดใหญ่ (Big Data), ศูนย์ข้อมูล (Data Center) และคลาวด์คอมพิวติ้ง (Cloud Computing)”.

[69] Public Safety Canada, “The Hub - Centre of Responsibility (COR)” (14 Marc 2018), online: Government of Canada <www.publicsafety.gc.ca>; Nathan Munn, “Canada’s ‘Pre-Crime’ Model of Policing Is Sparking Privacy Concerns” (19 January 2017), online: Vice <www.vice.com>.".

ปัญญาประดิษฐ์ (AI) และระบบที่สามารถเรียนรู้ได้จากตัวอย่างด้วยตนเองโดยปราศจากการป้อนคำสั่งของโปรแกรมเมอร์ (machine leaning) เพื่อคาดการณ์อาชญากรรม ปรับปรุงความปลอดภัยสาธารณะ และระบุต้นตอพฤติกรรมของบุคคล (root causes of a person's actions) โดยมุ่งเน้นไปที่สหสัมพันธ์หรือความเชื่อมโยงกัน (interconnected) ของอาชญากรรม (crime) การเสพติด (addiction) การไร้ที่อยู่อาศัย (homeless) และสุขภาพจิต (Mental health)[70]

มีรายงานจากห้องปฏิบัติการพลเมืองของมหาวิยาลัยโตรอนโต[71] ซึ่งทำการตรวจสอบเทคโนโลยีอัลกอริทึมที่ออกแบบมาเพื่อใช้ในระบบบังคับใช้กฎหมายอาญา ในทางทฤษฎีนั้นการตรวจสอบอัลกอริทึมเป็นส่วนหนึ่งของการพัฒนาทางเทคโนโลยีที่ได้รับการออกแบบมาเพื่อช่วยให้หน่วยงานบังคับใช้กฎหมายสามารถตรวจตราโดยอัตโนมัติหรือเพื่อหาข้อสรุปผ่านการประมวลผลข้อมูลจำนวนมากโดยคาดหวังจะทำนายกิจกรรมทางอาญาที่อาจเกิดขึ้นได้ก่อนที่มันจะเกิด เทคโนโลยีดังกล่าวมักเรียกว่าการตรวจสอบแบบคาดการณ์ล่วงหน้า (predictive policing technology) วิธีการตรวจสอบอัลกอริทึมมักอาศัยการรวบรวมและวิเคราะห์ข้อมูลจำนวนมาก เช่น ข้อมูลส่วนบุคคล ข้อมูลการสื่อสาร ข้อมูลไบโอเมทริกซ์ ข้อมูลตำแหน่งทางภูมิศาสตร์ รูปภาพ เนื้อหาโซเชียลมีเดีย และข้อมูลสถิติจากการจับกุมของตำรวจหรือบันทึกอาชญากรรม วิธีการดังกล่าวอาจให้ความสำคัญกับคาดการณ์สถานที่ที่จะเกิดกิจกรรมทางอาญาและเกิดเมื่อใด หรือมุ่งเน้นไปที่บุคคลโดยคาดการณ์ความเป็นไปได้ของแต่ละบุคคลที่มีความเสี่ยงจะก่ออาชญากรรมหรืออาจมีแนวโน้มที่จะมีก่อคดีอาญาในอนาคต อนึ่งเทคโนโลยีการตรวจสอบแบบคาดการณ์ล่วงหน้าที่ให้ความสำคัญกับปัจจัยด้านสถานที่ตั้งนั้น เครื่องมือนี้มีจุดมุ่งหมายเพื่อพยากรณ์เกี่ยวกับแนวโน้มหรือโอกาสที่สถานที่ใดๆ (location) และเวลาไหน (Time) ที่อาจจะเกิดเหตุอาชญากรรมได้ เทคโนโลยีนี้จะใช้อัลกอริทึมเป็นระบบปฏิบัติการซึ่งอัลกอริทึมที่ได้ตั้งโปรแกรมไว้จะทำการค้นหาความสัมพันธ์จากฐานข้อมูลของตำรวจในอดีตเพื่อพยายามคาดการณ์เกี่ยวกับพื้นที่ทางภูมิศาสตร์ที่เสี่ยงต่อการเกิดอาชญากรรม ตัวอย่างเช่น การปฏิบัติงานของกรมตำรวจเมืองแวนคูเวอร์ (Vancouver Police Department; VPD) ที่ใช้ประโยชน์จากเทคโนโลยีจีโอแดช (GeoDASH)

---

[70] Michael Purcell, Mathew Zaia. (2020). "Prediction, Prevention and Proof: Artificial Intelligence and Peace Bonds in Canada". Retrieved from The Canadian Bar Review, Vol. 98 No.3 https://cbr.cba.org/index.php/cbr/article/view/4630

[71] K. Robertson, C. Khoo, and Y. Song. "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada", (University of Toronto Press, Canada). 2020.

มากยิ่งกว่านั้นกรมตำรวจเมืองแวนคูเวอร์ (Vancouver Police Department; VPD) ยังได้ใช้ประโยชน์จากเครื่องมือเทคโนโลยีการพยากรณ์อาชญากรรมในเมืองอย่างเป็นวงกว้าง (city-wide predictive policing tool) เพื่อป้องกันอาชญากรรมประทุษร้ายต่อทรัพย์สิน (property crime) โดยเทคโนโลยีประเภทนี้จะใช้ระบบที่สามารถเรียนรู้ได้จากตัวอย่างด้วยตนเองโดยปราศจากการป้อนคำสั่งของโปรแกรมเมอร์ (machine leaning) สำหรับวิเคราะห์ข้อมูลนาดใหญ่เพื่อคาดการณ์พื้นที่เสี่ยงที่อาชญากรอาจลงมือหรือบุกรุก (break-ins) เพื่อประกอบอาชญากรรม โดยเทคโนโลยีนี้จะส่งผลลัพธ์จากข้อมูลที่ผ่านการวิเคราะห์แล้วไปยังคอมพิวเตอร์ที่ติดตั้งไว้ในพาหนะสำหรับการตรวจตราหรือลาดตระเวน เจ้าหน้าที่ตำรวจสายตรวจจะได้รับข้อมูลการแจ้งเตือนพื้นที่เสี่ยงดังกล่าวภายในระยะเวลาประมาณ 2 ชั่วโมง ภายหลังได้รับข้อมูลเจ้าหน้าที่ตำรวจสายตรวจจะสามารถออกลาดตระเวนในพื้นที่คาดการณ์ซึ่งจะอยู่ในรัศมีระยะประมาณ 100-500 เมตร ดังนี้ถือเป็นการปฏิบัติงานเชิงการป้องกันเหตุอาชญากรรมเพื่อสังคม จากการทดลองนำเอาเครื่องมือทางเทคโนโลยีดังกล่าวมาปรับใช้ในการดำเนินงานของกรมตำรวจเมืองแวนคูเวอร์ในช่วงระยะเวลาทดลอง 6 เดือน ปีค.ศ. 2016 พบว่าหากเปรียบเทียบกับสถิติการเกิดอาชญากรรมใน 4 ปีที่ผ่านมา ภายหลังทดลองใช้เทคโนโลยีการพยากรณ์สถานที่อาชญากรรม ผลปรากฏว่าเหตุอาชญากรรมประทุษร้ายต่อทรัพย์สิน (property crime) ในเมืองแวนคูเวอร์ในเขตที่ทดลองปรับใช้เทคโนโลยีดังกล่าวลดลง 27% มากยิ่งกว่านั้นเทคโนโลยียังให้ข้อมูลที่แม่นยำ ตามทัศนะของเจ้าหน้าที่ผู้ปฏิบัติงาน อดัม พาล์มเมอร์ จากกรมตำรวจเมืองแวนคูเวอร์ สนับสนุนว่าเทคโนโลยีนี้สามารถให้ข้อมูลที่แมนยำถึง 80% ของแนวปฏิบัติ[72]

เทคโนโลยีการตรวจแบบคาดการณ์ล่วงหน้าที่เน้นบุคคลเป็นหลักอาศัยการวิเคราะห์ข้อมูลเพื่อพยายามระบุบุคคลที่มีแนวโน้มที่จะมีส่วนเกี่ยวข้องกับกิจกรรมทางอาญาที่อาจเกิดขึ้นหรือประเมินบุคคลที่ระบุว่ามีความเสี่ยงที่จะมีส่วนร่วมในกิจกรรมทางอาญาในอนาคต ตัวอย่างเช่น โครงการความร่วมมือของหน่วยงานตำรวจเมืองซัสคาทูน กับมหาวิทยาลัยซัสแคตเชวัน กระทรวงราชทัณฑ์ และกรมตำรวจซัสแคตเชวันเพื่อจัดตั้งห้องปฏิบัติการวิเคราะห์เชิงคาดการณ์ตำรวจซัสแคตเชวัน (Saskatchewan Police Predictive Analytics Lab, SPPAL) โครงการ SPPAL มีลักษณะพิเศษตรงที่มุ่งเน้นไปที่การระบุเหยื่อที่อาจเกิดขึ้นล่วงหน้า เช่น เยาวชนที่หายตัวไป โครงการ SPPAL ตั้งใจที่จะขยายขอบเขตของการทำงานแบบ

[72] Ian Kearns, Rick Muir. (2019, March). Data-driven policing and public value. Retrieved from The Police Foundation Kemp House: https://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/data_driven_policing_final.pdf

อัลกอริทึมในอนาคตเพื่อจัดการกับข้อกังวลด้านความปลอดภัยอื่นๆ และปัญหาของชุมชน เช่น ผู้กระทำความผิดซ้ำซาก ผู้กระทำกระทำความผิดรุนแรง ผู้กระทำรุนแรงต่อคู่ครอง และบุคคลที่มีความเจ็บป่วยทางจิตในกระบวนการยุติธรรมทางอาญา แนวทาง SPPAL อาจถือเป็นการขยายอัลกอริทึมในรูปแบบฮับ (Hub) ของความปลอดภัยในชุมชนซึ่งมีจุดมุ่งหมายเพื่อระบุบุคคลที่มีความเสี่ยงและเชื่อมโยงบุคคลดังกล่าวกับความต้องการช่วยเหลือทางสังคมที่จำเป็นก่อนที่กระบวนการยุติธรรมจะเข้ามาเกี่ยวข้อง

นอกจากนี้กรมตำรวจคาลการี (Calgary Police Service) ใช้ซอฟต์แวร์ Palantir Gotham ซึ่งเป็นผลิตภัณฑ์จากบริษัทเคโนโลยี Palantir Technology ในการรวบรวมข้อมูลบุคคลจากแหล่งต่างๆ เพื่อการวิเคราะห์ โดยข้อมูลบุคคลที่ถูกจัดเก็บจะเป็นข้อมูลเกี่ยวกับลักษณะทางกายภาพของบุคคล ความสัมพันธ์การมีปฏิสัมพันธ์กับตำรวจ การเข้าร่วมทางศาสนา และกิจกรรมที่เกี่ยวข้องที่เป็นไปได้ นอกเหนือจากนี้ยังมีการใช้ซอฟต์แวร์ Palantir เพื่อค้นหาสถานที่ที่มีรายงานอาชญากรรมและสถานที่ที่มีการร้องขอความช่วยเหลือ

2.2.2 เทคโนโลยีการเฝ้าระวังด้วยอัลกอริทึม (algorithmic surveillance technology)[73]

เทคโนโลยีการเฝ้าระวังด้วยอัลกอริทึมทำให้การรวบรวมและประมวลผลข้อมูลอย่างเป็นระบบเป็นไปโดยอัตโนมัติ (เช่นข้อมูลที่รวบรวมทางออนไลน์ หรือภาพทางกายภาพที่ถ่ายจากพื้นที่กลางแจ้ง) เทคโนโลยีการเฝ้าระวังด้วยอัลกอริทึมบางประเภทอาจประมวลผลจากข้อมูลที่ถูกจัดเก็บไว้แล้วในหน่วยงานบังคับใช้กฎหมายหรือแฟ้มงานดิจิทัลของตำรวจในรูปแบบใหม่ (เช่นการนำ mug-shot databases มาใช้เป็นฐานข้อมูลสำหรับเทคโนโลยีการจดจำใบหน้า) ตัวอย่างเทคโนโลยีการเฝ้าระวังด้วยอัลกอริทึม เช่น

1) เครื่องอ่านป้ายทะเบียนอัตโนมัติ (automated license plate reader, ALPR) ใช้ซอฟต์แวร์จดจำรูปแบบที่ฝังอยู่ในกล้องเพื่อสแกนและระบุหมายเลขป้ายทะเบียนของยานพาหนะที่จอดอยู่หรือเคลื่อนที่ เครื่องอ่านป้ายทะเบียนอัตโนมัติช่วยในการเฝ้าระวังได้โดยการรวบรวมข้อมูลจำนวนมากอย่างเป็นระบบ เช่น วันที่ เวลาและตำแหน่งทางภูมิศาสตร์ของยานพาหนะที่สแกนทั้งหมดและข้อมูลการลงทะเบียนที่เกี่ยวข้องกับยานพาหนะเหล่านั้น (เช่นข้อมูลประจำตัวของผู้ขับขี่) เทคโนโลยีนี้ถูกนำไปใช้โดย

[73] K. Robertson, C. Khoo, and Y. Song. “To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada”, (University of Toronto Press, Canada). 2020.

หน่วยงานบังคับใช้กฎหมายในจังหวัด ออนแทรีโอ บริติชโคลัมเบีย ซัสแคตเชวัน อัลเบอร์ตา โนวาสโกเชีย ควิเบกและเกาะปรินซ์เอ็ดเวิร์ด

2) ซอฟต์แวร์เฝ้าระวังโซเชียลมีเดีย (social media surveillance software) จะทำการสืบค้นเชิงลึกและวิเคราะห์ข้อมูลส่วนบุคคลและข้อมูลที่เกี่ยวข้องจากแพลตฟอร์มโซเชียลมีเดีย ข้อมูลดังกล่าวถูกใช้ในการอนุมานหรือทำนายรูปแบบพฤติกรรม กิจกรรมในอนาคต เหตุการณ์ในอนาคต หรือความสัมพันธ์และความเชื่อมโยงระหว่างผู้ใช้และบุคคลอื่น ซอฟต์แวร์ประเภทนี้นี้ได้ถูกนำไปใช้ในกรมตำรวจเมืองคาลการี กรมตำรวจเมืองโตรอนโต และกรมตำรวจเมืองออตตาวา

3) เทคโนโลยีจดจำใบหน้า (facial recognition technology, Clearview AI) เป็นเทคโนโลยีการระบุตัวตนแบบไบโอเมทริกซ์ที่ใช้อัลกอริทึมเพื่อตรวจจับรายละเอียดเฉพาะเกี่ยวกับใบหน้า เช่น รูปร่างใบหน้า และ ระยะห่างระหว่างคิ้ว จากนั้นใช้การแสดงรายละเอียดทางคณิตศาสตร์เพื่อระบุหรือจับคู่ใบหน้าที่เหมือนกันหรือคล้ายกันในฐานข้อมูลการจดจำใบหน้า เทคโนโลยีจดจำใบหน้าอาจใช้กับภาพถ่าย หรือ วิดีโอ เทคโนโลยีนี้ถูกนำไปปรับใช้ในกรมตำรวจเมืองคาลการี กรมตำรวจเมืองโตรอนโต นอกจากนี้เทคโนโลยีจดจำใบหน้ายังได้มีการนำไปทดสอบในกรมตำรวจเมืองออตตาวาและไนแอการา

4) การวิเคราะห์เครือข่ายโซเชียล (social network analysis) อาศัยสถิติและข้อมูลรูปภาพโดยมีจุดประสงค์เพื่อหาความสัมพันธ์ทางสังคมระหว่างผู้คนบนเครือข่ายโซเชียลมีเดียและวิธีที่พวกเขามีอิทธิพลต่อกัน เช่น ในบริบทของการเป็นสมาชิกแก๊งหรือองค์กรอาชญากรรม การวิเคราะห์อาชญากรรมบนเครือข่ายโซเชียลมีเดียถูกนำไปใช้ในกรมตำรวจเมืองคาลการี

2.3 สิทธิมนุษยชนและผลทางกฎหมายของการใช้เทคโนโลยีการเฝ้าระวังด้วยอัลกอริทึม[74]

จากรายงานที่จัดทำขึ้นโดยห้องปฏิบัติการพลเมืองมหาวิทยาลัยโตรอนโต ประเทศแคนาดา รายงานว่าการใช้เทคโนโลยีการเฝ้าระวังด้วยอัลกอริทึมโดยผู้บังคับใช้กฎหมายเพิ่มโอกาสการละเมิดรัฐธรรมนูญและสิทธิเสรีภาพภายใต้กฎบัตรสิทธิและเสรีภาพของแคนาดาและกฎหมายสิทธิมนุษยชนระหว่างประเทศ โดยเฉพาะอย่างยิ่งการรวบรวมข้อมูลส่วนบุคคลเพื่อวิเคราะห์และระบุประเด็นปัญหาที่เกี่ยวข้องกับ

[74] K. Robertson, C. Khoo, and Y. Song. “To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada”, (University of Toronto Press, Canada). 2020.

การเฝ้าระวังเกิดการรุกรานสิทธิส่วนบุคคลและระบบขาดความโปร่งใส ทำให้เกิดความกังวลในกระบวนการ เนื่องจากวิธีการใช้เทคโนโลยีการเฝ้าระวังด้วยอัลกอริทึมโดยพื้นฐานแล้วไม่สอดคล้องกับการคุ้มครองตามรัฐธรรมนูญและสิทธิมนุษยชนโดยเฉพาะอย่างยิ่งเกี่ยวกับสิทธิที่เกี่ยวข้องกับเสรีภาพ ความเสมอภาค และความเป็นส่วนตัว การใช้เทคโนโลยีการเฝ้าระวังด้วยอัลกอริทึมเป็นอันตรายต่อสิทธิมนุษยชนดังต่อไปนี้

1) สิทธิในความเป็นส่วนตัวผ่านประเด็นต่างๆ เช่น การเฝ้าระวังโดยไม่เลือกปฏิบัติ การทำลายความคาดหวังที่สมเหตุสมผลเกี่ยวกับความเป็นส่วนตัวในพื้นที่สาธารณะและออนไลน์ ความถูกต้องของการอนุมานข้อมูล และการแบ่งปันข้อมูลระหว่างหน่วยงานบังคับใช้กฎหมายและหน่วยงานอื่นๆ ของรัฐ

2) สิทธิในเสรีภาพในการแสดงออก การชุมนุมโดยสงบ และการรวมกลุ่มผ่านประเด็นต่างๆ เช่น การบ่อนทำลายการไม่เปิดเผยตัวตนของฝูงชน และการกำหนดเป้าหมายการเคลื่อนไหวทางสังคมและชุมชนชายขอบ

3) สิทธิในความเท่าเทียมกันผ่านประเด็นต่างๆ เช่น อคติของอัลกอริทึมที่ทำให้เกิดลูปข้อเสนอแนะที่เลือกปฏิบัติ การมองเห็นข้อมูลที่เพิ่มขึ้นของบุคคลที่ด้อยโอกาสทางเศรษฐกิจและสังคม และการเลือกปฏิบัติทางระบบคณิตศาสตร์ที่ลดความเป็นไปได้ของการปฏิรูปโครงสร้างเพื่อแก้ไขปัญหารากเหง้า

4) สิทธิในเสรีภาพและความเป็นอิสระจากการควบคุมตัวโดยพลจากการตีความแบบอัตโนมัติที่เข้ามาแทนที่การตีความด้วยบุคคล

5) สิทธิในกระบวนการออกข้อกำหนดและในการแก้ไขปัญหาต่างๆ เช่น การขาดความโปร่งใส การขาดความรับผิดชอบ ขาดกลไกการกำกับดูแล และขาดการเปิดเผยข้อมูล

3. สหราชอาณาจักร (UK)

3.1 ความเป็นมา

หน่วยงานบังคับใช้กฎหมาย (Law enforcement agencies; LEAs) และหน่วยงานความมั่นคงแห่งราชอาณาจักร (security agencies) ในสหราชอาณาจักร ได้นำข้อมูลขนาดใหญ่ (Bid data) ที่ได้จากการจัดเก็บข้อมูลประชากรจากการปฏิบัติหน้าที่ประจำวัน มาใช้ประโยชน์ในงานอาชญากรรมและการป้องกันประเทศใน 3 ด้านหลัก คือ 1) ด้านการป้องกันอาชญากรรม (crime prevention) 2) การตรวจจับอาชญากรรม (crime detection) และ 3) ด้านความมั่นคงแห่งราชอาณาจักร (national security) อีกทั้งการเข้ามาของเทคโนโลยีในยุคดิจิทัลส่งผลให้เกิดกระบวนการวิเคราะห์ข้อมูลขนาดใหญ่ที่มีความซับซ้อนได้ง่ายและรวดเร็วขึ้น เปิดโอกาสให้เจ้าหน้าที่หน่วยงานบังคับใช้กฎหมายและเจ้าหน้าที่หน่วยงานความมั่นคงได้

ใช้ประโยชน์จากข้อมูลเชิงลึกเกี่ยวกับอาชญากรรมทางอาญา อันเป็นผลลัพธ์ที่ได้จากการวิเคราะห์ข้อมูลขนาดใหญ่โดยนวัตกรรมแห่งยุคเทคโนโลยีไปใช้ในการปฏิบัติงานได้มีประสิทธิภาพมากขึ้น อนึ่งหน่วยงานบังคับใช้กฎหมาย (Law enforcement agencies; LEAs) และหน่วยงานความมั่นคงแห่งราชอาณาจักร (security agencies) ในสหราชอาณาจักร (UK) ที่นำข้อมูลขนาดใหญ่ไปใช้ประโยชน์ในการดำเนินงานประกอบด้วยดังนี้[75]

- หน่วยงานบังคับใช้กฎหมาย (Law enforcement agencies; LEAs)
    1. หน่วยอาชญากรรมท้องถิ่น (Local crime agencies) ประกอบด้วย สำนักงานตำรวจจำนวน 43 แห่งในเขตสหราชอาณาจักร (United Kingdom of Great Britain and Northern Ireland; UK) ซึ่งประกอบไปด้วย ประเทศอังกฤษ (England) เวลส์ (Wales) และหน่วยบริการตำรวจ (single Police Service) ในประเทศ สก๊อตแลนด์ (Scotland) และแคว้นไอร์แลนด์เหนือ(Northern Ireland)
    2. หน่วยบังคับใช้กฎหมายระดับชาติ (National bodies) และหน่วยตำรวจปฏิบัติการพิเศษ (special police forces) อาทิ ตำรวจขนส่งอังกฤษ (British Transport Police; BTP) และหน่วยงานปราบปรามอาชญากรรมแห่งชาติของสหราชอาณาจักร (National Crime Agency; NCA) ที่ดำเนินงานด้านการปราบปรามอาชญากรรมร้ายแรง (serious crime) และอาชญากรรมองค์กร (Organized Crime)
- หน่วยงานความมั่นคงแห่งราชอาณาจักร (security agencies)
    1. หน่วยความมั่นคง (Security Service; MI5) ซึ่งเป็นหน่วยข่าวกรองทหาร แผนก 5 (Military Intelligence, Section 5) ที่ดำเนินงานด้านการเก็บรวบรวมข้อมูลข่าวกรองเพื่อการต่อต้านการก่อการร้ายและการโจรกรรม ภายในสหราชอาณาจักร
    2. หน่วยข่าวกรองลับ (Secret Intelligence Service (MI6) เป็นหน่วยงานที่ดำเนินงานด้านการเก็บรวบรวมข้อมูลข่าวกรองนอกสหราชอาณาจักร หรือการสืบราชการลับนอกสหราชอาณาจักร

[75] The Parliamentary Office of Science and Technology. (2014, July). Big Data, Crime and Security. Retrieved from Houses of Parliament, The Parliamentary Office of Science and Technology. POSTnote Number 470: file:///D:/P%20Pim%20big%20data/UK/Big%20Data,%20Crime%20and%20Security%20-%20UK%20Parliament%20POST-PN-470.pdf

เพื่อสนับสนุนงานความมั่นคงภายในประเทศ และความมั่นคงทางเศรษฐกิจของสหราชอาณาจักร

3. กองบัญชาการสื่อสารของรัฐบาล (Government Communications Headquarters: GCHQ) เป็นหน่วยงานกำกับดูแลข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์เพื่อความมั่นคงภายในสหราชอาณาจักร การปฏิบัติการทางการทหาร งานบังคับใช้กฎหมายต่างๆ รวมถึงสนับสนุนงานด้านการให้คำปรึกษาและช่วยเหลืองานด้านป้องกันระบบสารสนเทศเพื่อการสื่อสารของรัฐบาล (Government's communication and information systems)

ปัจจุบันในสหราชอาณาจักรมีการใช้เทคโนโลยีวิเคราะห์ข้อมูลขนาดใหญ่เพื่อวัตถุประสงค์การใช้ในงานที่หลากหลาย สำหรับงานด้านการป้องกันและปราบปรามอาชญากรรม สหราชอาณาจักรได้ให้ความสำคัญกับการใช้ประโยชน์เทคโนโลยีวิเคราะห์ข้อมูลขนาดใหญ่เพื่อวัตถุประสงค์สำคัญใน 4 ด้านหลัก[76] ได้แก่

1) การพยากรณ์แผนที่อาชญากรรมล่วงหน้า (predictive crime mapping) ที่สามารถคาดการณ์พื้นที่เสี่ยง (identify areas) จะเกิดอาชญากรรมมากที่สุด ซึ่งจะช่วยให้เกิดการใช้ทรัพยากรที่มีอยู่อย่างจำกัดได้มีประสิทธิภาพมากที่สุด

2) การวิเคราะห์ข้อมูลอาชญากรรมล่วงหน้า (predictive analytics) อันสามารถช่วยระบุคุณลักษณะบุคคลที่มีโอกาสเสี่ยงสูงจะประกอบอาชญากรรมซ้ำ หรือคุณลักษณะที่สามารถนำไปสู่การก่ออาชญากรรมซ้ำของผู้กระทำความผิด ตลอดจนระบุคุณลักษณะของบุคคลที่มีโอกาสเสี่ยงสูงจะกลายเป็นเหยื่ออาชญากรรม เช่น การสูญหาย (missing)

3) การวิเคราะห์ข้อมูลอาชญากรรมขั้นสูง (advanced analytics) สามารถช่วยให้เจ้าหน้าที่ตำรวจควบคุมและใช้ประโยชน์ของข้อมูลได้อย่างเต็มประสิทธิภาพ ผ่านการเฝ้าระวังโดยใช้นวัตกรรมเทคโนโลยีต่างๆ เช่น ระบบการบันทึกภาพเคลื่อนไหวที่ถูกจับภาพโดยกล้องวงจรปิด (CCTV images) และระบบตรวจสอบป้ายทะเบียนอัตโนมัติ (automatic number plate recognition; ANPR)

---

[76] Alexander Babuta. (2017, September). Big Data and Policing An Assessment of Law Enforcement Requirements, Expectations and Priorities. Retrieved from Royal United Services Institute for Defence and Security Studies (RUSI),:
https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf

4) เทคโนโลยีข้อมูลขนาดใหญ่ (big data technology) มีรูปแบบที่สามารถปรับใช้ได้กับแหล่งข้อมูลเปิด อาทิ ข้อมูลที่ถูกจัดเก็บจากแหล่งสื่อสังคมออนไลน์ หรือโซเชียลมีเดีย เพื่อประโยชน์ด้านการระบุปัญหาอาชญากรรมอันจะส่งผลให้เกิดการพัฒนากลยุทธ์การบังคับใช้กฎหมายเชิงป้องกันได้ต่อไป

อย่างไรก็ดี แม้หน่วยงานภาครัฐสหราชอาณาจักรจะมีการใช้ประโยชน์จากนวัตกรรมวิเคราะห์ข้อมูลขนาดใหญ่อย่างกว้างขวาง อาทิ สำนักงานสรรพากรและศุลกากร (Her Majesty's Revenue and Customs: HMRC) ใช้เทคโนโลยีเพื่อช่วยงานสำคัญในการตรวจจับการหนีภาษี (detect tax fraud)[77] แต่สำนักงานตำรวจในสหราชอาณาจักรที่งานตรวจตราลาดตระเวนพื้นที่เสี่ยงต่อการเกิดอาชญากรรมถือเป็นงานสำคัญหลักงานหนึ่งกลับยังคงถือปฏิบัติงานด้านการป้องกันและปราบปรามอาชญากรรมโดยใช้แนวปฏิบัติหรือกลยุทธ์การด้านข่าวกรองมากกว่าการนำซอฟต์แวร์การพยากรณ์พื้นที่เสี่ยงต่อการเกิดอาชญากรรมล่วงหน้า เข้าไปบูรณาการปรับใช้ร่วมกับแนวแนวปฏิบัติการทำงานแบบเดิม ทั้งนี้พบว่ามีสำนักงานตำรวจในสหราชอาณาจักรจำนวนไม่มากที่ได้นำซอฟต์แวร์ดังกล่าวไปปรับใช้ในกลยุทธ์การปฏิบัติงานออกตรวจตราหรือลาดตระเวนพื้นที่ในปัจจุบัน [54]

จากการศึกษาวิจัยในปี ค.ศ. 2018 ด้านจำนวนหน่วยงานตำรวจในสหราชอาณาจักรที่ใช้โปรแกรมคาดการณ์อาชญากรรมในการปฏิบัติงาน พบว่ามีหน่วยงานตำรวจในสหราชอาณาจักรอย่างต่ำ จำนวน 14 แห่งกำลังปรับใช้โปรแกรมดังกล่าวในการปฏิบัติงาน ส่วนนอกเหนือจากนั้นบางหน่วยงานเคยปรับใช้มาก่อนแล้วหรืออยู่ระหว่างการศึกษาวิจัยเพื่อการปรับใช้โปรแกรม ดังมีรายละเอียดตามตารางที่ 1[78]

---

[77] The Parliamentary Office of Science and Technology. (2014, July). Big Data, Crime and Security. Retrieved from Houses of Parliament, The Parliamentary Office of Science and Technology. POSTnote Number 470: file:///D:/P%20Pim%20big%20data/UK/Big%20Data,%20Crime%20and%20Security%20-%20UK%20Parliament%20POST-PN-470.pdf

[78] Hannah Couchman, Alessandra Prezepiorski Lemos. (2019, January). Liberty report: Policing by Machine. Retrieved from libertyhumanrights.org.uk: https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/LIB-11-Predictive-Policing-Report-WEB.pdf

ตารางที่ 1 จำนวนหน่วยงานตำรวจในสหราชอาณาจักร (UK) (police forces) ที่ใช้โปรแกรมคาดการณ์อาชญากรรมในการปฏิบัติงาน

หน่วยงานตำรวจ (police forces)	กำลังปรับใช้โปรแกรมคาดการณ์แผนที่อาชญากรรม (predictive mapping programs) หรืออยู่ระหว่างพิจารณาปรับใช้	กำลังปรับใช้โปรแกรมประเมินความเสี่ยงรายบุคคลในการก่ออาชญากรรม (individual risk assessment programs)
Avon and Somerset	√	√
Cheshire	√	
Durham	–	√
Dyfed Powys	√ (อยู่ระหว่างการพัฒนา)	
Greater Manchester Police	√	
Kent	√	
Lancashire	√	
Merseyside	√	
The Met	√	
Norfolk	√	
Northamptonshire	√	
Warwickshire and West Mercia	√ (อยู่ระหว่างการพัฒนา)	
West Midlands	√	√
West Yorkshire	√	

3.2 แนวทางการใช้ข้อมูลขนาดใหญ่ (Big Data) ในการป้องกันและปราบปรามอาชญากรรม

ด้วยข้อมูลขนาดใหญ่สามารถถูกวิเคราะห์โดยใช้เทคโนโลยีเชิงวิเคราะห์ได้หลากหลายรูปแบบ หน่วยงานบังคับใช้กฎหมาย (Law enforcement agencies; LEAs) และหน่วยงานความมั่นคงแห่งราชอาณาจักร (security agencies) ในสหราชอาณาจักร (UK) เป็นหน่วยงานหลักที่ใช้ประโยชน์ข้อมูลขนาดใหญ่เพื่อการป้องกันและปราบปรามอาชญากรรมในด้านใน 3 ด้านหลัก คือ 1) ด้านการป้องกันอาชญากรรม (crime prevention) 2) การตรวจจับอาชญากรรม (crime detection) และ 3) ด้านความมั่นคงแห่ง

ราชอาณาจักร (national security) อนึ่ง เทคโนโลยีที่ใช้ในการเสริมประสิทธิภาพในการดำเนินงานด้านดังกล่าวของสหราชอาญาจักรที่น่าสนใจมีดังนี้

3.2.1 ระบบฐานข้อมูล (Database)

หน่วยงานบังคับใช้กฎหมาย (Law enforcement agencies; LEAs) และหน่วยงานความมั่นคงแห่งราชอาณาจักร (security agencies) ในสหราชอาณาจักร (UK) คือ

1) หน่วยงานบังคับใช้กฎหมาย (Law enforcement agencies; LEAs) ประกอบด้วย

1.1 หน่วยอาชญากรรมท้องถิ่น (Local crime agencies) ประกอบด้วย สำนักงานตำรวจจำนวน 43 แห่งในเขตสหราชอาณาจักร (United Kingdom of Great Britain and Northern Ireland; UK) ซึ่งประกอบไปด้วย ประเทศอังกฤษ (England) เวลส์ (Wales) และหน่วยบริการตำรวจ (single Police Service) ในประเทศ สก๊อตแลนด์ (Scotland) และแคว้นไอร์แลนด์เหนือ(Northern Ireland)

1.2 หน่วยบังคับใช้กฎหมายระดับชาติ (National bodies) และหน่วยตำรวจปฏิบัติการพิเศษ (special police forces) อาทิ ตำรวจขนส่งอังกฤษ (British Transport Police; BTP) และหน่วยงานปราบปรามอาชญากรรมแห่งชาติของสหราชอาณาจักร (National Crime Agency; NCA) ที่ดำเนินงานด้านการปราบปรามอาชญากรรมร้ายแรง (serious crime) และอาชญากรรมองค์กร (Organized Crime) และ

2) หน่วยงานความมั่นคงแห่งราชอาณาจักร (security agencies) ประกอบด้วย

2.1 หน่วยความมั่นคง (Security Service; MI5) ซึ่งเป็นหน่วยข่าวกรองทหารแผนก 5 (Military Intelligence, Section 5) ที่ดำเนินงานด้านการเก็บรวบรวมข้อมูลข่าวกรองเพื่อการต่อต้านการก่อการร้ายและการโจรกรรม (terrorism and espionage) ภายในสหราชอาณาจักร

2.2 หน่วยข่าวกรองลับ (Secret Intelligence Service (MI6) เป็นหน่วยงานที่ดำเนินงานด้านการเก็บรวบรวมข้อมูลข่าวกรองนอกสหราชอาณาจักร (secret information outside the UK) หรือการสืบราชการลับนอกสหราชอาณาจักรเพื่อสนับสนุนงานความมั่นคงภายในประเทศ (national security) และความมั่นคงทางเศรษฐกิจของสหราชอาณาจักร (economic well-being) และ 2.3 กองบัญชาการสื่อสารของรัฐบาล (Government Communications Headquarters: GCHQ) เป็นหน่วยงานกำกับดูแลข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์เพื่อความมั่นคงภายในสหราชอาณาจักร การ

ปฏิบัติการทางการทหาร งานบังคับใช้กฎหมายต่างๆ รวมถึงสนับสนุนงานด้านการให้คำปรึกษา และช่วยเหลืองานด้านป้องกันระบบสารสนเทศเพื่อการสื่อสารของรัฐบาล

หน่วยงานดังกล่าวมีการเก็บรวบรวมข้อมูลขนาดใหญ่ที่หลากหลาย ซึ่งสามารถแบ่งเป็น 2 ประเภทข้อมูล คือ 1) ข้อมูลแบบมีโครงสร้าง (Structured data) เช่น ชุดข้อมูลที่มีแบบแผน (set format) อาทิ สถานที่ ประเภทของอาชญากรรม รูปแบบสารพันธุกรรม (DNA profile) หรือข้อมูลส่วนบุคคลต่างๆ ของผู้ที่ถูกจับกุม (arrested) (charged) หรือตั้งข้อหา และ 2) ข้อมูลแบบไม่มีโครงสร้าง (Unstructured data) คือ ชุดข้อมูลที่ไม่มีแบบแผน อาทิ ถ้อยแถลงหรือคำกล่าวอ้างจากทั้งเจ้าหน้าที่ตำรวจและพยาน ข้อมูลเหล่านี้เก็บรวบรวมโดยหน่วยปฏิบัติการในระดับท้องถิ่น (local forces) และหน่วยปฏิบัติการระดับชาติ (national agencies) เพื่อใช้ประโยชน์ร่วมกันผ่านฐานข้อมูลข่าวกรองของสำนักงานตำรวจท้องถิ่นและหน่วยปฏิบัติการระดับชาติ อาทิ ตำรวจหน่วยปฏิบัติการในระดับท้องถิ่น (local police forces) และหน่วยปฏิบัติการระดับชาติ (national agencies) มีการใช้ฐานข้อมูลระดับชาติในระบบคอมพิวเตอร์ต่างๆ ร่วมกันดังนี้

1) ฐานข้อมูลตำรวจระดับชาติในระบบคอมพิวเตอร์ (Police National Computer; PNC) ซึ่งถูกสร้างขึ้นมาครั้งแรกตั้งแต่กลางปี ค.ศ. 1970 ฐานข้อมูลนี้จะประกอบไปด้วยข้อมูลประเภท ประวัติอาชญากรรม เช่นประวัติการถูกพิพากษาลงโทษ (convictions) การตักเตือน (cautions) การเตือนครั้งสุดท้าย (final warnings) และการตำหนิโทษ (reprimands)

2) ฐานข้อมูลพันธุกรรมและลายนิ้วมือ (National DNA Database and IDENT1 Fingerprint Database) โดยฐานข้อมูลนี้จะเก็บข้อมูลอิเล็กทรอนิกส์เกี่ยวกับรูปแบบสารพันธุกรรม (DNA profile) และลายนิ้วมือจากผู้ที่ถูกจับกุม (arrested individuals) และแหล่งที่เกิดอาชญากรรม (crime scenes) ในปี ค.ศ. 2013 มีรายงานว่าฐานข้อมูลพันธุกรรมและลายนิ้วมือ (National DNA Database and IDENT1 Fingerprint Database) มีบัญชีการบันทึกข้อมูลอิเล็กทรอนิกส์ลายนิ้วมือและรูปแบบสารพันธุกรรมจากผู้ที่ถูกจับกุมจำนวน 6,737,973 บัญชี และจากแหล่งที่เกิดอาชญากรรม (crime scenes) จำนวน 428,634 บัญชี (profiles)

3) ฐานข้อมูลตำรวจระดับชาติ (Police National Database; PND) ซอฟต์แวร์ฐานข้อมูลนี้ถูกสร้างขึ้นครั้งแรกเมื่อปี ค.ศ. 2011 โดยมีวัตถุประสงค์เพื่อแบ่งปันข้อมูลข่าวกรองร่วมกันในระดับชาติ ข้อมูลต่างๆ ที่ถูกบันทึกโดยสำนักงานตำรวจท้องถิ่นจะถูกอัพเดตขึ้นในฐานข้อมูลนี้โดยอัตโนมัติ

3.2.2 อินเทอร์เน็ตของสรรพสิ่ง (Internet of Things)

อินเทอร์เน็ตของสรรพสิ่ง (Internet of Things) คือเทคโนโลยีที่หมายรวมถึง วัตถุ อุปกรณ์ พาหนะ สิ่งของเครื่องใช้ และสิ่งอำนวยความสะดวกในชีวิตอื่นๆ ที่มนุษย์สร้างขึ้นโดยมีการฝังตัวของวงจรอิเล็กทรอนิกส์ ซอฟต์แวร์ เซ็นเซอร์ และการเชื่อมต่อกับเครือข่าย (network) ซึ่งวัตถุอุปกรณ์เหล่านี้ สามารถเก็บบันทึกและแลกเปลี่ยนข้อมูลกันได้ (exchange information) เพื่อบรรลุการใช้งานวัตถุประสงค์ด้านการจดจำอัจฉริยะ (smart recognitions) การระบุตำแหน่ง (positioning) การสืบติดตาม (tracing) การติดตาม (monitoring) และ การบริหารจัดการ (administration)[79]

สหราชอาณาจักรใช้อินเทอร์เน็ตของสรรพสิ่ง (Internet of Things) เป็นเครื่องมือในการป้องกันและปราบปรามอาชญากรรมหลายประเภท ตัวอย่างเช่น อาชญากรรมประเภทลักทรัพย์ โดยเจ้าหน้าที่ตำรวจในประเทศอังกฤษสามารถจับกุมผู้กระทำความผิดฐานลักขโมยได้โดยการตรวจสอบการเชื่อมต่ออุปกรณ์เร้าเตอร์ไวไฟ (wifi routers) ยี่ห้อ BT ของบ้านจำนวน 4 หลังติดกัน หนึ่งในนั้นคือบ้านของผู้เสียหายที่ถูกลักทรัพทย์ (burglary) ในตอนช่วงเวลากลางวัน ภายหลังการตรวจสอบพบว่าเร้าเตอร์ไวไฟ (wifi routers) ยี่ห้อ BT จากบ้านจำนวน 4 หลังดังกล่าวพบว่าเร้าเตอร์ได้แสดงผลข้อมูลอิเล็กทรอนิกส์ที่ระบบบันทึกไว้ว่ามีโทรศัพท์เคลื่อนที่เครื่องเดิมที่ทำการเชื่อมต่อกับสัญญาณไวไฟฟรีจากผู้ให้บริการอินเตอร์เน็ตเครือข่ายเดียวกันคือ BT (BT-FON service) ของวันที่เกิดเหตุอาชญากรรมขึ้น จึงทำให้เจ้าหน้าที่ตำรวจสามารถใช้ประโยชน์จากข้อมูลอุปกรณ์เทคโนโลยีดังกล่าวเพื่อการสืบติดตาม (track down) หาผู้กระทำความผิดได้ (perpetrato) ในที่สุด[80]

3.2.3 เทคโนโลยีเพื่อการคาดการณ์อาชญากรรม (Predictive Policing Technology)

เจ้าหน้าที่บังคับใช้กฎหมายแห่งสหราชอาณาจักรใช้เทคโนโลยีหลายรูปแบบในการบันทึกข้อมูลและวิเคราะห์ข้อมูลขนาดใหญ่เพื่อประโยชน์ด้านการป้องกันและปราบปรามอาชญากรรม ดังต่อไปนี้

---

[79] Keyur K Patel, Sunil M Patel. (2016, May). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. Retrieved from IJESC, Volume 6 Issue No. 5: https://www.researchgate.net/publication/330425585_Internet_of_Things-IOT_Definition_Characteristics_Architecture_Enabling_Technologies_Application_Future_Challenges

[80] Ian Kearns, Rick Muir. (2019, March). Data-driven policing and public value. Retrieved from The Police Foundation Kemp House: https://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/data_driven_policing_final.pdf

1) ซอฟต์แวร์คาดการณ์อาชญากรรม (Predictive Policing)[81]

ซอฟต์แวร์หรือโปรแกรมเพื่อการคาดการณ์อาชญากรรม (Predictive Policing) นี้ใช้อัลกอรึทึม (Algorithms) เป็นระบบปฏิบัติการประมวลผลข้อมูลเพื่อให้ข้อมูลเชิงการพยากรณ์ตำแหน่งที่ตั้งที่มีโอกาสเสี่ยงจะเกิดอาชญากรรมหรือแผนที่อาชญากรรม (Forecasting Crime Location) โดยเจ้าหน้าที่บังคับใช้กฎหมายในสหราชอาณาจักร (UK) ใช้ซอฟต์แวร์นี้เพื่อการตัดสินใจเลือกพื้นที่ออกตรวจตรา (patrolling decisions) โดยซอฟต์แวร์จะคาดคะเนสถานที่มีโอกาสเสี่ยงต่อการเกิดอาชญากรรม (Hotspots) ในการกระทำความผิดประเภทต่างๆ ในบริษัทของสหราชอาญาจักร คือ ลักทรัพย์ (burglary) ความรุนแรงบนท้องถนน (street violence) การโจรกรรมยานพาหนะ (vehicle theft) พฤติกรรมต่อต้านสังคม (anti-social behavior) ซึ่งเป็นคดีที่เกิดขึ้นอย่างสม่ำเสมอ (regularity) ในสหราชอาณาจักร หลักการทำงานของซอฟต์แวร์คาดการณ์อาชญากรรมคือใช้ข้อมูลสถานที่ที่เคยเกิดอาชญากรรมประเภทดังกล่าวในอดีต (historic location data) มาวิเคราะห์ตามแนวคิดที่เชื่อว่าสถานที่ที่เกิดอาชญากรรมในอดีตมีความเสี่ยงในการเกิดอาชญากรรมซ้ำได้อีกในสถานที่เดิม ดังนั้นเจ้าหน้าที่ตำรวจสายตรวจจะได้รับข้อมูลสถานที่เสี่ยงต่อการเกิดอาชญากรรมที่วิเคราะห์โดยซอฟต์แวร์ดังกล่าวและสามารถใช้เป็นข้อมูลในการตัดสินใจเพื่อกำหนดพื้นที่ที่จะออกเดินตรวจตรา (foot patrol) ได้ สำนักงานตำรวจภาคอีสต์มิดแลนส์ของอังกฤษ (East Midlands) ได้ทดลองปรับใช้ซอฟต์แวร์นี้ในการปฏิบัติงานเพื่อป้องกันและปราบปรามอาชญากรรมประเภทลักทรัพย์ พบว่าผลการคาดการณ์จากซอฟต์แวร์มีความแม่นยำถึง 78% ในแต่ละคดี ในขณะที่การปฏิบัติงานโดยใช้แนวปฏิบัติตามแบบแผนเดิม (traditional techniques) มีความแม่นยำในการคาดการณ์ข้อมูลด้านสถานที่อยู่ที่ 51% อนึ่งพบว่าในประเทศอังกฤษมีสำนักงานตำรวจจำนวน 2 แห่งที่ได้นำซอฟต์แวร์คาดการณ์อาชญากรรม (Predictive Policing) ไปปรับใช้ในการดำเนินงานในบริบทที่แตกต่างกัน คือ สำนักงานตำรวจแห่งเมืองเคนต์ (Kent) และ เวสต์ ยอร์กเชียร์ (West Yorkshire) อย่างไรก็ดี ด้วยหลักฐานด้านการรับรองประสิทธิภาพของผลการคาดการณ์อาชญากรรมเชิงภูมิศาสตร์ที่จำกัด (limited evidence) หรือยังไม่มีการรับรองผลอย่างเป็นทางการว่าการปรับใช้โปรแกรมนี้จะส่งผลต่ออัตราการเกิดอาชญากรรม มีรายงานว่ากรมตำรวจนครลอสแอนเจลิส ในประเทศสหรัฐอเมริกาปรับใช้ซอฟต์แวร์ดังกล่าวในการปฏิบัติหน้าที่และส่งผลให้

[81] The Parliamentary Office of Science and Technology. (2014, July). Big Data, Crime and Security. Retrieved from Houses of Parliament, The Parliamentary Office of Science and Technology. POSTnote Number 470: file:///D:/P%20Pim%20big%20data/UK/Big%20Data,%20Crime%20and%20Security%20-%20UK%20Parliament%20POST-PN-470.pdf

อาชญากรรมในพื้นที่ลดลง แต่ข้อมูลดังกล่าวยังไม่ได้รับการยืนยันอย่างความถูกต้อง และจากหลายๆ บทสังเคราะห์ที่เกี่ยวกับการศึกษาด้านการริเริ่มการบังคับใช้กฎหมายแบบมีภูมิศาสตร์เป็นฐานนั้น (geographically-focused policing initiatives)เสนอแนะว่าการใช้ซอฟต์แวร์พยากรณ์พื้นที่เสี่ยงเกิดอาชญากรรมล่วงหน้าไม่สามารถกำจัดอาชญากรรม (displace crime) ในพื้นที่ที่ถูกคาดการณ์ให้หายไปได้ แต่จะส่งผลกระทบในมิติอื่นคือสามารถลดโอกาสหรือยังยั้งการเกิดอาชญากรรมได้ ทั้งนี้การปฏิบัติงานด้านการออกตรวจตราหรือลาดตระเวนพื้นที่ของเจ้าหน้าที่ตำรวจระหว่างสหราชอาณาจักร (UK) และเจ้าหน้าที่ตำรวจในสหรัฐอเมริกา มีความแตกต่างกัน กล่าวคือเจ้าหน้าที่ตำรวจสายตรวจในสหรัฐอเมริกาใช้พาหนะในการลาดตระเวน (car patrols) แต่เจ้าหน้าที่ตำรวจสายตรวจในสหราชอาณาจักรใช้การเดินเท้าในการออกตรวจตราพื้นที่ (foot patrols) ดังนั้นประสิทธิผลของการใช้ซอฟต์แวร์คาดการณ์อาชญากรรมต่ออัตราการเกิดอาชญากรรมในสหราชอาณาจักรและสหรัฐอเมริกาจึงอาจจะแตกต่างกัน

1.1) ซอฟต์แวร์เพร็ดโพล (PredPol Software)[82]

ซอฟต์แวร์เพื่อการคาดการณ์อาชญากรรมเพร็ดโพล (PredPol's predictive policing software) เป็นหนึ่งในซอฟต์แวร์ที่มีหลักการทำงานเช่นเดียวกับการพยากรณ์แผนที่อาชญากรรม คือการคาดคะเนสถานที่มีโอกาสเสี่ยงเกิดอาชญากรรมโดยใช้อัลกอริทึม ในปี ค.ศ. 2013 สำนักงานตำรวจแห่งเมืองเคนต์ (Kent) ได้ทำลองปรับใช้ซอฟต์แวร์เพร็ดโพล (PredPol Software) เพื่อสนับสนุนงานด้านการป้องกันอาชญากรรม (Crime Prevention) พบว่าซอฟต์แวร์ทำการวิเคราะห์ข้อมูลอาชญากรรมที่ถูกบันทึกเข้ามาในระบบอย่างอัตโนมัติจำนวน 2 ครั้งต่อวัน โดยประเภทของข้อมูลที่เจ้าหน้าที่ตำรวจเมืองเคนต์บันทึกเข้าระบบและถูกซอฟต์แวร์วิเคราะห์อย่างทันต่อสถานการณ์ คือ ข้อมูลด้านสถานที่เกิดเหตุอาชญากรรมลักทรัพย์ (crime location data about burglar) ความรุนแรงบนท้องถนน (street violence) การโจรกรรมยานพาหนะ (vehicles theft) และพฤติกรรมต่อต้านสังคม (anti-social behavior) นอกจากนี้ซอฟต์แวร์เพร็ดโพลยังนำข้อมูลในด้านดังกล่าวมราถูกบันทึไว้ย้อนหลัง 5 ปีเข้ามาประมวลผลและวิเคราะห์หาความน่าจะเป็นของพื้นที่เสี่ยงเกิดอาชญากรรมล่วงหน้าในอีก 12 ชั่วโมงให้แก่เจ้าหน้าที่ตำรวจเมืองเคนต์ได้

[82] The Parliamentary Office of Science and Technology. (2014, July). Big Data, Crime and Security. Retrieved from Houses of Parliament, The Parliamentary Office of Science and Technology. POSTnote Number 470: file:///D:/P%20Pim%20big%20data/UK/Big%20Data,%20Crime%20and%20Security%20-%20UK%20Parliament%20POST-PN-470.pdf

รับทราบ รวมถึงแสดงแผนที่อาชญากรรมในรัศมี 500 ตารางฟุต (500 square foot) เพื่อให้เจ้าหน้าที่ตำรวจสามารถออกตรวจตราประจำวันในพื้นที่ได้อย่างมีเป้าหมาย อย่างไรก็ตาม ภายหลังจากการปรับใช้ซอฟต์แวร์เพร็ดโพลของเจ้าหน้าที่ตำรวจเมืองเคนต์ พบว่าซอฟต์แวร์เป็นประโยชน์ต่อการดำเนินงานและการเขียนรายงานการปฏิบัติงาน (reports) แต่ไม่สามารถสร้างความเปลี่ยนแปลงอย่างเป็นที่ประจักษ์ (small drops) ในมิติของการลดอัตราอาชญากรรมประเภทดังกล่าวและพฤติกรรมต่อต้านสังคมของผู้กระทำความผิดได้

1.2) ซอฟต์แวร์พยากรณ์แผนที่อาชญากรรมล่วงหน้า (Prospective Mapping)[83]

สำนักงานตำรวจแห่งเวสต์ ยอร์กเชียร์ (West Yorkshire) ได้พัฒนาซอฟต์แวร์พยากรณ์แผนที่อาชญากรรมล่วงหน้า (Prospective Mapping software) ขึ้นมาใช้เอง โดยมีการพัฒนาซอฟต์แวร์ร่วมกับนักวิจัยจากมหาวิทยาลัยคอลเลจลอนดอน (University College London) เพื่อใช้ในการคาดการณ์สถานที่เสี่ยงเกิดอาชญากรรมประเภทลักขโมย (forecast hotspots for burglary) และการโจรกรรมยานพาหนะ (vehicles theft) ซอฟต์แวร์ที่สำนักงานตำรวจแห่งเวสต์ ยอร์กเชียร์ (West Yorkshire) ได้พัฒนาขึ้นใช้เองนี้สามารถวิเคราะห์ข้อมูลได้ในทุกๆ 2 วัน โดยจะใช้ข้อมูลดิบด้านสถานที่ที่เกิดอาชญากรรมลักทรัพย์ขึ้นย้อนหลังไป 3 อาทิตย์ที่ผ่านมาพยากรณ์หาพื้นที่เสี่ยงเกิดอาชญากรรมล่วงหน้าในปัจจุบัน เจ้าหน้าที่ตำรวจสายตรวจออกปฏิบัติงานลาดตระเวนบ่อยขึ้นกว่าปกติในพื้นที่เสี่ยงที่ถูกซอฟต์แวร์คาดการณ์ไว้ ตลอดจนเข้าไปให้คำแนะนำเชิงป้องกันอาชญากรรมแก่ผู้อาศัยในละแวกใกล้เคียงพื้นที่เสี่ยงอย่างใกล้ชิด สถานีตำรวจเขตเกรเทอร์แมนเชสเตอร์ (Greater Manchester Police) นำแนวปฏิบัติและซอฟต์แวร์ดังกล่าวไปปรับใช้ ผลการประเมินจากผู้เชี่ยวชาญ (peer-reviewed evaluation) พบว่าอัตราการเกิดอาชญากรรมลดลงในพื้นที่ที่มีการปรับใช้แนวปฏิบัติ (technique) ดังกล่าวร่วมกับการใช้ซอฟต์แวร์คาดการณ์พื้นที่อาชญากรรมมากกว่าพื้นที่ที่ไม่มีการใช้แนวปฏิบัติดังกล่าวร่วมกับการใช้ประโยชน์จากซอฟต์แวร์ประเภทเดียวกัน

[83] The Parliamentary Office of Science and Technology. (2014, July). Big Data, Crime and Security. Retrieved from Houses of Parliament, The Parliamentary Office of Science and Technology. POSTnote Number 470: file:///D:/P%20Pim%20big%20data/UK/Big%20Data,%20Crime%20and%20Security%20-%20UK%20Parliament%20POST-PN-470.pdf

2) โปรแกรมประยุกต์หรือแอปพลิเคชั่น (App)[84]

สำนักงานตำรวจในสหราชอาณาจักรได้พยายามปรับเปลี่ยนรูปแบบการจัดการข้อมูลเพื่อการป้องกันอาชญากรรมให้เหมาะสมกับโลกยุคปัจจุบันที่เปลี่ยนแปลงไปอย่างรวดเร็วด้วยเทคโนโลยี รวมถึงพฤติกรรมของผู้ใช้ทั้งเจ้าหน้าที่ผู้บังคับใช้กฎหมายและประชาชนในการรับ-ส่งข้อมูลข่าวสาร โดยได้พัฒนาแอปพลิเคชั่นเพื่อการป้องกันและปราบปรามอาชญากรรมสำหรับมือถือไว้ในหลายรูปแบบ ดังนี้

2.1) แอปพลิเคชั่นพรอนโตไครม์ (Pronto Crime app)

สำนักงานตำรวจแห่งเวสต์ ยอร์กเชียร์ (West Yorkshire) ได้ปรับใช้แอปพลิเคชั่นพรอนโตไครม์ (Pronto Crime app) เพื่อบันทึกข้อมูลเกี่ยวกับเหตุอาชญากรรม (crime) และไม่เกี่ยวกับเหตุอาชญากรรม (non-crime)

2.2) แอปพลิเคชั่นเพื่อคนหาย (The Missing Person App)

ด้วยอัตราการเกิดคดีคนหายเกิดขึ้นบ่อยๆ ในเวสต์ ยอร์กเชียร์ (West Yorkshire) เจ้าหน้าที่ตำรวจแห่งเวสต์ ยอร์กเชียร์ (West Yorkshire) จึงมีศักยภาพและประสบการณ์ในการจัดการคดีดังกล่าวได้อย่างทันต่อสถานการณ์ โดยได้ใช้แอปพลิเคชั่นเพื่อคนหาย (The Missing Person App) เป็นเครื่องมือในการแบ่งปันข้อมูลของบุคคลที่สูญหายให้แก่ผู้ที่เกี่ยวข้องทันทีที่ได้รับการแจ้งเหตุ ซึ่งส่งผลดีต่อการติดตามหาบุคคลสูญหายได้อย่างทันท่วงที

2.3) อินเทลแอปพลิเคชั่น (Intel App)

โปรแกรมประยุกต์นี้ถูกสร้างขึ้นเพื่ออำนวยให้เจ้าหน้าที่ตำรวจที่ปฏิบัติงานส่วนหน้า (Front-line officer) สามารถบันทึก (Record) และแบ่งปันข้อมูลข่าวกรอง (Share intelligence) ร่วมกับหน่วยงานที่เกี่ยวข้องได้อย่างทันท่วงที ตลอดจนลดการกรอกเอกสารแบบดั้งเดิมลง

3) โปรแกรมเท็มโปรา (Tempora Program)

โปรแกรมเท็มโปรา (Tempora Program) เป็นเครื่องมือทางเทคโนโลยีที่ใช้จัดเก็บข้องมูลขนาดใหญ่ (Bulk Data Collection) ของประชาชนทั้งกลุ่มเสี่ยงที่จะก่ออาชญากรรมและกลุ่มประชาชนธรรมดาเพื่อวัตถุประสงค์ด้านความมั่นคงของประเทศ ตามเอกสารที่เผยแพร่โดยนายเอ็ดเวิร์ด สโนว์เดน

---

[84] Motorola Solutions. (2018, July). West Yorkshire Police Transforms Front-Line Policing. Retrieved from Motorola Solutions: https://www.motorolasolutions.com/content/dam/msi/docs/en-xu/public-safety/pronto_west_yorkshire_police_case_study.pdf

(Edward Snowden) ในปี ค.ศ. 2013 รายงานว่ากองบัญชาการสื่อสารของรัฐบาล (Government Communications Headquarters: GCHQ) ที่เป็นหน่วยงานกำกับดูแลข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์เพื่อความมั่นคงภายในสหราชอาณาจักร ได้ทำการเก็บข้อมูลการติดต่อสื่อสารบนโครงข่ายอินเตอร์เน็ตของประชาชนและสำรองข้อมูล (Storing) ไว้ 30 วันในโปรแกรมเท็มโปรา (Tempora Program) ต่อมาในเดือนมกราคม ปี ค.ศ. 2014 คณะกรรมาธิการแห่งสภายุโรปด้านสหเสรีภาพของพลเมือง (European Parliament Committee on Civil Liberties) และ หน่วยความยุติธรรมและกิจการภายใน (Justice and Home Affairs;LIBE) ได้สืบสวนหาข้อเท็จจริงและมีรายงานออกมาว่ามีหลักฐานที่สามารถยืนยันได้ว่าสหราชอาณาจักรและประเทศสหรัฐอเมริกาได้ดำเนินการจัดเก็บข้อมูล สำรองข้อมูล และวิเคราะห์ข้อมูลการติดต่อสื่อสาร และสถานที่ ของประชาชนไว้ในระดับที่ไม่สามารถคาดการณ์ได้ (unprecedented scale) ซึ่งถือเป็นการกระทำโดยวิสาสะ (indiscriminate)[85] อย่างไรก็ตาม หลายๆ รัฐบาลได้โต้แย้งว่าหน่วยงานด้านความมั่นคงแห่งราชอาณาจักรต่างๆ (security agencies) จำเป็นต้องดำเนินการเก็บและสำรองข้อมูลข่าวกรองที่ทันต่อสถานการณ์ (timely) และมีความถูกต้องแม่นยำ (accurate intelligence) เพื่อปกป้องความมั่นคงของประเทศ[86]

4) โปรแกรมประเมินความเสี่ยงอาชญากรรมรายบุคคล (Individual Risk Assessment programs)

ปัจจุบันมีโปรแกรมประเมินความเสี่ยงอาชญากรรมรายบุคคล (Individual Risk Assessment programs) ในสหราชอาณาจักรที่ถูกปรับใช้โดยหน่วยงานบังคับใช้กฎหมายอยู่อย่างหลากหลาย โดยใช้ชื่อที่แตกต่างกันไป หลักการทำงานของโปรแกรมในภาพรวมคือการวิเคราะห์ข้อมูลขนาดใหญ่เพื่อคาดคะเนความน่าจะเป็นระบุคุณลักษณะของบุคคลที่มีโอกาสสูงในการลงมือประกอบอาชญากรรม โดยใช้ระบบปฏิบัติการอัลกอริทึมหรือระบบที่สามารถเรียนรู้ได้จากตัวอย่างด้วยตนเองโดยปราศจากการป้อน

---

[85] Claude Moraes. (2014). Committee on Civil Liberties, Justice and Home Affairs, 2013/2188(INI). Retrieved from European Parliament: https://www.europarl.europa.eu/document/activities/cont/201403/20140306ATT80626/20140306ATT80626EN.pdf

[86] European Court of Human Rights (ECHR). (2018). Handbook on European data protection law 2018 Edition. Retrieved from European Union Agency for Fundamental Rights and Council of Europe: https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

คำสั่งของโปรแกรมเมอร์ (machine leaning) ซึ่งหน่วยงานตำรวจในสหราชอาณาจักรได้ปรับใช้โปรแกรมดังกล่าวในการดำเนินงานในบริบทที่หลากหลายและมีโปรแกรมที่ปรับใช้มีชื่อเรียกที่แตกต่างกันดังนี้

4.1) โปรแกรมคลิคเซ้นส์ (Qlik Sense)

สถานีตำรวจมณฑลเอวอนและซัมเมอร์เซต (Avon and Somerset Police Forces) ประเทศอังกฤษ ได้ปรับใช้โปรแกรมประเมินความเสี่ยงอาชญากรรมรายบุคคล (Individual Risk Assessment programs) ที่มีชื่อว่าโปรแกรมคลิคเซ้นส์ (Qlik Sense) ที่ให้ข้อมูลการพยากรณ์ผู้ที่มีลักษณะเสี่ยงอันอาจนำไปสู่การก่ออาชญากรรมล่วงหน้าจากการวิเคราะห์ข้อมูลขนาดใหญ่ที่ถูกจัดเก็บรวบรวมจากการปฏิบัติหน้าที่ประจำวันของเจ้าหน้าที่ผู้ปฏิบัติงาน(massive volumes of data collected on a daily basis) อย่างไรก็ดีการตัดสินใจคัดเลือกผู้ที่โปรแกรมวิเคราะห์ว่าอาจมีโอกาสเสี่ยงจะก่ออาชญากรรมนั้น เจ้าหน้าที่ผู้ปฏิบัติงานจะใช้การตัดสินในแบบมืออาชีพ (professional judgement) นอกจากนี้เจ้าหน้าที่ตำรวจสถานีตำรวจมณฑลเอวอนและซัมเมอร์เซต (Avon and Somerset Police Forces) ได้ใช้ประโยชน์จากโปรแกรมคลิคเซ้นส์ (Qlik Sense) ในการประเมินความเสี่ยงรายบุคคลในหลายๆ ด้าน อาทิ

- ความน่าจะเป็นด้านการกระทำความผิดซ้ำ (Likelihood of re-offending)
- ความน่าจะเป็นด้านการตกเป็นเหยื่อ (Likelihood of victimisation and vulnerability)
- ความน่าจะเป็นด้านโอกาสบุคคลสูญหาย (Likelihood of being reported missing)
- ความน่าจะเป็นด้านการกระทำความผิดเรื่องความรุนแรงในครอบครัว หรือความรุนแรงทางเพศ (Likelihood of perpetrating a “serious domestic violence or sexual violent offence”)
- ความน่าจะเป็นด้านการตกเป็นเหยื่อความรุนแรงในครอบครัว หรือความรุนแรงทางเพศ (Likelihood of being the victim of a “serious domestic violence or sexual violent offence”)
- ความน่าจะเป็นด้านการการกระทำความผิดฐานลักทรัพย์ (Likelihood of perpetrating a burglary offence)
- ความน่าจะเป็นด้านการกระทำความผิดฐานสะกดรอยตามผู้อื่นและการคุกคามหรือล่วงละเมิดผู้อื่น (Likelihood of perpetrating a stalking and harassment offence)

- ความน่าจะเป็นด้านการตกเป็นเหยื่อของอาชญากรรมความผิดฐานสะกดรอยตามผู้อื่นและการคุกคามหรือล่วงละเมิดผู้อื่น (Likelihood of being the victim of a stalking and harassment offence)
- ความน่าจะเป็นด้านการเจ็บไข้ได้ป่วยอันเนื่องมากจากความเครียดของเจ้าหน้าที่หรือพนักงาน (Likelihood of a staff member having a stress-related period of sickness)

4.2) โปรแกรมเครื่องมือประเมินความเสี่ยงภัยอันตราย (Harm Assessment Risk Tool; HART)[87]

เจ้าหน้าที่ตำรวจมณฑลเดอรัม (Durham Police) ได้ปรับใช้เครื่องมือเทคโนโลยีเพื่อการประเมินโอกาสเสี่ยงก่ออาชญากรรมในรายบุคคล (Individual risk assessment program) ที่เรียกว่าเครื่องมือประเมินความเสี่ยงภัยอันตราย (Harm Assessment Risk Tool; HART) โปรแกรมนี้ถูกสร้างขึ้นด้วยความร่วมมือระหว่างคณะอาชญาวิทยาแห่งมหาวิทยาลัยแคมบริดจ์ (Department of Criminology at the University of Cambridge) และกองกำลังตำรวจประจำมณฑลเดอรัม (Durham Constabulary) โดยมีการปรับใช้โปรแกรมในการทำงานครั้งแรกเมื่อในเดือนเมษายน ปี ค.ศ. 2016 จุดมุ่งหมายหลักในการใช้ประโยชน์จาดโปรแกรมหรือเครื่องมือประเมินความเสี่ยงภัยอันตราย (Harm Assessment Risk Tool; HART) คือเพื่อสนับสนุนงานเจ้าหน้าที่ผู้ปฏิบัติงานด้านคุมขัง (custody officers) ในการระบุลักษณะของผู้กระทำความผิดที่เข้าข่ายชะลอการดำเนินคดี (deferred prosecution) ทั้งนี้กองกำลังตำรวจประจำมณฑลเดอรัม (Durham Constabulary) มีการป้อนข้อมูลด้านงานคุมขังที่ถูกบันทึกไว้ในระบบของกองกำลังตำรวจประจำมณฑลเดอรัม (Durham Constabulary) ระหว่างปี ค.ศ. 2002 – 2012 เข้าสู่โปรแกรมดังกล่าวไปแล้วจำนวน 104,000 เหตุการณ์ (custody events) โดยในเหตุการณ์จำนวนนี้ โปรแกรมฯ ใช้ 34 ตัวพยากรณ์ (predictors) โดย 29 ตัวพยากรณ์มาจากลักษณะตัวแปรของผู้กระทำความผิดที่ถูกคุมขังด้านพฤติกรรม (behavior) อายุ (age) เพศ (gender) รหัสไปรษณีย์ใน 2 รูปแบบ (two forms of post code)

[87] Hannah Couchman, Alessandra Prezepiorski Lemos. (2019, January). Liberty report: Policing by Machine. Retrieved from libertyhumanrights.org.uk: https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/LIB-11-Predictive-Policing-Report-WEB.pdf

และการนับจำนวนรายงานข่าวกรองที่เกี่ยวข้องกับผู้ที่ถูกคุมขัง (a count of intelligence reports related to the detained person) อย่างไรก็ตามภายหลังจากการใช้ตัวพยากรณ์ด้านรหัสไปรษณีย์ กองกำลังตำรวจประจำมณฑลเดอรัม (Durham Constabulary) ถูกสังคมวิพากษ์วิจารณ์อย่างหนัก เนื่องจากรหัสไปรษณีย์และข้อมูลด้านสังคมประชากร (socio-demographic data) สามารถนำไปสู่การตัดสินใจโดยใช้อคติเป็นปัจจัยหนึ่งในระบบยุติธรรมทางอาญา

บทที่ 5

สรุป อภิปรายผลและข้อเสนอแนะ

1. สรุปและอภิปรายผลจากการเก็บรวบรวมข้อมูล

1.1 สรุปผลการเก็บรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึก

ผู้วิจัยได้ดำเนินการสัมภาษณ์เชิงลึก (In-depth Interview) โดยมีผู้ให้ข้อมูลสำคัญ (Key Informant) เป็นผู้ทรงคุณวุฒิ จำนวนทั้งสิ้น 10 ท่าน ทั้งนี้ หลักเกณฑ์ในการเลือกผู้ทรงคุณวุฒิเพื่อเป็นผู้ให้ข้อมูลสำคัญ ใช้การเลือกแบบเจาะจง (Purposive sampling) โดยพิจารณาถึงการได้ข้อมูลที่ครอบคลุมประเด็นสำคัญเกี่ยวกับแนวทางการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปรามอาชญากรรมในประเทศไทย เพื่อให้ได้มาซึ่งข้อมูลที่จะใช้ในการวิเคราะห์ร่วมกับวิธีการวิจัยวิธีอื่น มีผู้ให้ข้อมูลสำคัญจากผู้แทนหน่วยงานที่มีภารกิจเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมและการใช้นำข้อมูลขนาดใหญ่ภาครัฐ ได้แก่ ผู้แทนสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานกฎหมายและคดี กองพิสูจน์หลักฐาน สำนักงานตำรวจแห่งชาติ ผู้แทนจากสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) และผู้แทนสถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ โดยสามารถสรุปผลตามประเด็นสัมภาษณ์ได้ดังนี้

ประเด็นภารกิจของหน่วยงานที่เกี่ยวกับการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data)

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) : เนื่องจาก สพร. ไม่ได้เป็นหน่วยงานที่เป็นเจ้าของข้อมูลโดยตรง เป็นหน่วยงานขับเคลื่อนให้มีการนำข้อมูลมาใช้ประโยชน์ เป็นหน่วยงานสนับสนุนที่เข้าไปช่วยเหลือเวลาหน่วยงานรัฐมีปัญหาไม่ว่าจะเป็นในเชิงเทคนิค หรือการผลักดันให้มีการข้อมูลไปใช้ประโยชน์ มีระบบที่เกี่ยวข้องกับกระบวนการยุติธรรมที่เรียกว่า DXC ถือเป็นข้อมูลขนาดใหญ่ด้านงานยุติธรรม ปัจจุบันมีข้อมูลขนาดใหญ่อยู่ 2 ระบบที่มีการเชื่อมโยงกันในระบบของศูนย์แลกเปลี่ยนข้อมูลกลางตามพระราชบัญญัติการบริหารงานและให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 คือ ข้อมูลทะเบียนราษฎร์ของกรมการปกครอง กระทรวงมหาดไทย และข้อมูลทะเบียนนิติบุคคลของกรมธุรกิจการค้า กระทรวงพาณิชย์

สถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ (สวข.) : เป็นหน่วยงานภายในภายใต้สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (depa) จัดตั้งขึ้นเพื่อตอบสนองการดำเนินงานตามแนวทางการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) และรองรับการให้บริการด้านการพัฒนาบุคลากรและการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) ของภาครัฐ ตามยุทธศาสตร์ชาติยุทธศาสตร์ที่ 6 ด้านการปรับสมดุลและการพัฒนาระบบบริหารจัดการภาครัฐที่กำหนดให้มีระบบการบริหารจัดการข้อมูลที่มีความเชื่อมโยงระหว่างหน่วยงาน และแหล่งข้อมูลต่าง ๆ ไปสู่การวิเคราะห์การจัดการข้อมูลขนาดใหญ่ โดยมีวัตถุประสงค์เพื่อส่งเสริมให้เกิดวัฒนธรรมการวิเคราะห์และใช้ประโยชน์ข้อมูลขนาดใหญ่เพื่อประกอบการตัดสินใจ (Data-Driven Decision) สกัดข้อมูลเชิงลึกในการดำเนินงาน (Insight to Operation) และช่วยเหลือให้หน่วยงานภาครัฐสามารถให้บริการประชาชนได้อย่างเป็นรูปธรรม

ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานตำรวจแห่งชาติ : มีการนำข้อมูล Big Data มาจากสถานีตำรวจทั่วประเทศ และนำมารวมไว้เป็นฐานข้อมูลขนาดใหญ่ มีการจัดเก็บข้อมูลมาเป็นระยะเวลานาน แต่ข้อมูลดังกล่าวเป็นข้อมูลภายในใช้ในการบริหารจัดการคดี และส่วนใหญ่เป็นข้อมูลคดีอาญาเป็นหลัก เช่น ข้อมูลเกี่ยวข้องข้อหา รูปแบบการกระทำความผิดและมีการนำข้อมูลมาวิเคราะห์แนวโน้มโอกาสในการกระทำความผิดซ้ำ ความสัมพันธ์ของพฤติการณ์คดี การทำแผนที่อาชญากรรม

กองทะเบียนประวัติอาชญากร : มีหน้าที่ในการสนับสนุนงานป้องกันและปราบปรามอาชญากรรมให้แก่ทางสำนักงานตำรวจแห่งชาติ ข้อมูลที่กองทะเบียนประวัติอาชญากรมีเป็นข้อมูลประวัติอาชญากรรมของผู้ที่ถูกกล่าวหาว่ากระทำความผิด เป็นข้อมูลที่พนักงานสอบสวนส่งมาให้เพื่อจัดเก็บไว้ในระบบ ซึ่งข้อมูลประวัติอาชญากรจะใช้ทั้งในส่วนของงานราชการและงานเอกชน แต่งานหลักจะเป็นงานราชการ ทั้งงานสืบสวนและสอบสวน และตามกฎหมายข้อมูลข่าวสารของทางราชการจะเปิดให้อำนาจหน้าที่ของเจ้าหน้าที่รัฐที่มีอำนาจในการสอบสวนและปราบปรามอาชญากรรมสามารถขอเข้าถึงข้อมูลได้ และเป็นข้อยกเว้นของกฎหมายคุ้มครองข้อมูลส่วนบุคคล นอกจากนั้น ยังใช้ในการสนับสนุนงานของหน่วยงานภาครัฐเกี่ยวกับการตรวจสอบคุณสมบัติ และประวัติการกระทำความผิดของบุคคลที่เป็นข้าราชการ หรือผู้ที่สมัครเข้ารับราชการ หรือผู้เข้าดำรงตำแหน่งต่างๆ แต่สำหรับหน่วยงานภาคเอกชนที่นำข้อมูลไปใช้ ซึ่งไม่ใช่เป็นการใช้ในงานป้องกันและปราบปรามอาชญากรรม จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลทุกครั้ง และหน่วยงานที่นำข้อมูลทะเบียนประวัติอาชญากรไปใช้จะเป็นหน่วยงานในระดับสถานีตำรวจหรือกรมสอบสวนคดีพิเศษ หรือสำนักงานป้องกันและปราบปรามการฟอกเงิน โดยจะมีการประสานเพื่อขอข้อมูลโดยตรงกับสำนักงานตำรวจแห่งชาติ

ประเด็นแนวทางการนำข้อมูลขนาดใหญ่ (Big Data) มาวิเคราะห์เพื่อลดการเกิดอาชญากรรมและปรามปรามการกระทำความผิด

- การเชื่อมโยงข้อมูลของหน่วยงานในกระบวนการยุติธรรมมีปัญหามาก เนื่องจากมีกฎหมายหลายฉบับที่จะต้องปฏิบัติตาม อย่างในระบบ CRIME สามารถนำมาวิเคราะห์และประมวลผลได้ว่าในพื้นที่ใดมักจะมีอาญากรรมรูปแบบใดเกิดขึ้น เป็นข้อมูลที่ใช้ประโยชน์ในเชิงป้องกันเหมือนในต่างประเทศ รวมทั้งสามารถนำมาใช้ประโยชน์เป็นข้อมูลวิเคราะห์การกระทำความผิดซ้ำและการฟื้นฟูพฤตินิสัย ส่วนกล้อง CCTV นำมาวิเคราะห์และนำมาใช้ควบคู่กับระบบสแกนใบหน้าและเชื่อมโยงกับข้อมูลหมายจับ แต่การใช้ยังอยู่ในวงจำกัด

- ระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) ของสำนักงานกิจการยุติธรรมเพื่อดำเนินการแลกเปลี่ยนข้อมูลกับหน่วยงานต่างๆ เช่น สำนักงานอัยการสูงสุดสำนักงานตำรวจแห่งชาติ กรมการปกครอง กรมราชทัณฑ์ กรมการขนส่งทางบก เป็นต้น เป็นฐานข้อมูลสำคัญที่สามารถนำมาปรับใช้ในการนำข้อมูลมาใช้ในกระบวนงานยุติธรรม

- การนำข้อมูลขนาดใหญ่มาอยู่ในระบบฐานข้อมูลเดียวกันทำได้อยาก เนื่องจากหน่วยงานรัฐแต่ละหน่วยงาน โดยเฉพาะหน่วยงานในกระบวนการยุติธรรมจะเป็นหน่วยงานที่มีความเป็นอิสระ จะทำได้คือการเอาข้อมูลของแต่ละหน่วยงานมาเชื่อมโยงกัน เพราะข้อมูลสามารถที่จะไหลและเชื่อมโยงกันได้อยู่แล้ว ไม่จำเป็นต้องจัดเก็บในรูปแบบเดียวกัน แต่จะต้องสามารถเชื่อมโยงกันด้วยการค้นหาในระบบที่เป็นมาตรฐานกลาง เช่น การค้นข้อมูลและเชื่อมข้อมูลกันด้วยหมายเลขบัตรประชาชน เลขที่หมายจับ เลขที่สำนวน เป็นต้น

- ข้อมูลขนาดใหญ่ (Big Data) ของกระบวนการยุติธรรม จะมีหลายมติ ทั้งตัวบุคคล สถานที่ พื้นที่ ดังนั้น ต้องกำหนดให้ได้ว่าข้อมูลที่จะนำมาแลกเปลี่ยนกันจะยึดโยงที่ข้อมูลส่วนไหนเป็นหลัก เพราะการจัดเก็บข้อมูลของแต่ละหน่วยงานมีความแตกต่างกัน และจะนำมาเชื่อมกันอย่างไร ซึ่งสำนักงานตำรวจแห่งชาติก็กำลังดำเนินการเรื่องมาตรฐานการจัดเก็บข้อมูล

- ควรทำระบบฐานข้อมูลมีมาตรฐานกลางในการให้ทุกหน่วยงานสามารถเชื่อมข้อมูลเข้ามาในระบบได้ ควรมีเจ้าภาพในการดำเนินงาน เช่น การทำระบบสมุดหน้าเหลืองข้อมูล หรือ Data Catalog ให้มีชุดข้อมูลร่วมกันของกระบวนการยุติธรรม โดยแต่ละหน่วยงานต้องจำแนกรายละเอียดของข้อมูลที่จัดเก็บว่าจัดเก็บข้อมูลอะไรบ้าง มีกฎหมายข้อไหนที่ให้อำนาจในการเก็บข้อมูล ซึ่งเป็นเรื่องที่ดำเนินการยากมาก

- หน่วยงานรัฐไม่ควรมองว่าการบูรณาการข้อมูลจะต้องเป็นการดำเนินการให้ข้อมูลเป็นข้อมูลเดียวกัน ซึ่งเป็นไปไม่ได้ แต่ควรมองว่าหน่วยงานไหนมีการเก็บข้อมูล เก็บข้อมูลรูปแบบใด จะนำข้อมูลมาเชื่อมโยงอย่างไร และจะนำข้อมูลที่มีมาใช้วิเคราะห์และประมวลผลอย่างไร ควรเน้นเรื่องความร่วมมือ

- เจ้าหน้าที่รัฐควรจะมีอำนาจในการเข้าถึงข้อมูลและสามารถวิเคราะห์เบื้องต้นได้ด้วยตัวเองและนำข้อมูลมาใช้ในการวิเคราะห์เพื่อการป้องกันและปราบปรามอาชญากรรม

- การใช้ big data ในงานป้องกันอาชญากรรม อาจเป็นในรูปแบบของการใช้กล้อง CCTV การใช้เทคโนโลยีสแกนใบหน้าและเชื่อมโยงกับหมายจับ แต่อาจยังไม่ได้ใช้กับเป็นที่แพร่หลาย ยังจำกัดเฉพาะพื้นที่ เช่น พื้นที่เสี่ยง 3 จังหวัดชายแดนภายใต้

- ข้อมูลด้านอาชญากรรมที่สถานีตำรวจทั่วประเทศจัดเก็บมีความแตกต่างกันในแต่ละพื้นที่ ทำให้สามารถนำข้อมูลมาทำนายและคาดการณ์อาชญากรรมล่วงหน้าได้และกำหนดมาตรการป้องกันเหตุได้อย่างเฉพาะเจาะจง

- ข้อมูลขนาดใหญ่สามารถใช้คาดการณ์การเกิดอาชญากรรมล่วงหน้าได้ เช่น การทำแผนประทุษกรรมว่าคนร้ายใช้ช่องทางใดกระทำความผิด หรือกระทำความผิดในรูปแบบใด

- การนำข้อมูลขนาดใหญ่มาใช้เพื่อประโยชน์ด้านป้องกันอาชญากรรมจะต้องคำนึงถึงความสมดุลของประโยชน์สาธารณะกับสิทธิส่วนบุคคลของประชาชนภายใต้ขอบเขตของรัฐธรรมนูญแห่งราชอาณาจักรไทยและกฎหมายคุ้มครองข้อมูลส่วนบุคคล หน่วยงานภาครัฐจะต้องไม่นำข้อมูลไปใช้นอกขอบเขตตามที่มีกฎหมายบัญญัติรับรองให้กระทำได้ และจะมีเงื่อนไขและขั้นตอนของการเปิดเผยข้อมูลระหว่างหน่วยงานตามกฎหมายว่าด้วยข้อมูลข่าวสารของทางราชการที่จะต้องปฏิบัติให้ถูกต้องตามหลักเกณฑ์ของกฎหมาย

ประเด็นข้อจำกัดด้านกฎหมายในการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ในส่วนของการป้องกันและปราบปรามอาชญากรรม

- แม้จะมีกฎหมายให้อำนาจให้ดำเนินการตามกฎหมายการให้บริการและการบริหารงานภาครัฐผ่านระบบดิจิทัลที่กำหนดว่าหน่วยงานภาครัฐต้องสามารถนำข้อมูลมาแลกเปลี่ยนกันได้ แต่ทางปฏิบัติหน่วยงานเจ้าของข้อมูลจะมีกฎหมายที่ให้อำนาจในการจัดเก็บข้อมูลอยู่ และอำนาจในการให้อำนาจเชื่อมโยงข้อมูลยังเป็นอำนาจของหน่วยงานนั้นๆ และกฎหมายการบริหารงานและการให้บริหารภาครัฐผ่านระบบดิจิทัล ยังต้องอยู่ภายใต้กฎหมายอื่น ๆ เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กฎหมายว่าด้วยข้อมูลข่าวสารของทางราชการ

- กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้เปิดช่องให้ภาครัฐสามารถที่จะนำข้อมูลส่วนบุคคลมาใช้ในการวิเคราะห์เพื่อประโยชน์สาธารณะได้ แต่ในทางปฏิบัติเมื่อเกิดจากร้องขอเข้าถึงข้อมูลส่วนบุคคลที่อยู่ในอำนาจของหน่วยงานรัฐ หน่วยงานจะมีความกังวลเกี่ยวกับอนุญาตให้เข้าถึงข้อมูลและใช้ข้ออ้างด้านกฎหมายในการปฏิเสธการเชื่อมโยงข้อมูล ซึ่งหากพิจารณาแล้วเห็นว่า ส่วนใหญ่กฎหมายที่มีอยู่จะเปิดช่องให้สามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานรัฐได้อยู่แล้ว แต่ปัญหาที่เกิดขึ้นคือการเชื่อมโยงและใช้ประโยชน์จากข้อมูลและเจ้าหน้าที่ที่ปฏิบัติงานอาจมีความกังวลเกี่ยวกับความรับผิดที่อาจเกิดขึ้นจากข้อมูลรั่วไหล

- การใช้ข้อมูลเพื่อคาดการณ์อาชญากรรมจำเป็นต้องใช้ข้อมูลจากหน่วยงานอื่นที่ไม่ใช่เฉพาะหน่วยงานในกระบวนการยุติธรรมเท่านั้น จึงเป็นความยากในการบูรณาการความร่วมมือ เนื่องจากภารกิจมีความแตกต่างกัน

- การเชื่อมโยงข้อมูลข้อมูลในปัจจุบันจะมีกฎหมายที่เข้ามาเกี่ยวข้องหลายฉบับและหากจะเชื่อมโยงข้อมูลในระบบ ควรเชื่อมโยงกับฐานข้อมูลของกรมการปกครองผ่าน Data Linkgate เพราะเป็นหน่วยงานกลางที่สามารถเชื่อมโยงไปยังข้อมูลส่วนบุคคลของประชาชนได้

- ในทางปฏิบัติด้านเทคโนโลยี การจัดเก็บข้อมูลบนแพลตฟอร์มเดียวกันกระทำได้ยาก โดยเฉพาะหน่วยงานในกระบวนการยุติธรรม (ตำรวจ ศาล อัยการและราชทัณฑ์) เนื่องจากแต่ละหน่วยงานมีความเป็นอิสระต่อกัน การจะให้ทุกหน่วยงานนำข้อมูลมารวมไว้ในที่เดียวกันทำได้ยาก แต่การเชื่อมโยงข้อมูลสามารถทำได้โดยการใช้ index หรือรหัสตัวเดียวกัน หรือเลขอ้างอิงที่เป็นมาตรฐานเดียวกัน เช่น เลขบัตรประชาชน 13 หลัก หรือเลขคดีความ ที่สามารถเชื่อมโยงข้อมูลกันได้ โดยคำนึงถึงมิติของตัวบุคคล เวลา สถานที่ ฯลฯ ซึ่งในปัจจุบันของประเทศไทยข้อมูลส่วนใหญ่ที่เชื่อมโยงกันได้จะเป็นการเชื่อมโยงผ่านเลขบัตรประชาชน 13 หลัก

- การจัดเก็บข้อมูลของแต่ละหน่วยงานจะต้องจัดเก็บตามมาตรฐานสากลด้วย ซึ่งมาตรฐานสากลจะกำหนดรายละเอียดของฐานข้อมูลที่จัดเก็บ อาทิ การจัดเก็บข้อมูลอาชญากรรมจะมีมาตรฐานระหว่างประเทศว่าด้วยการจำแนกประเภทอาชญากรรมเพื่อประโยชน์ทางสถิติ (ICCS) เป็นแนวทางในการจัดเก็บ

- พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัลฯ แม้กฎหมายจะบัญญัติให้หน่วยงานรัฐกับหน่วยงานรัฐสามารถเชื่อมโยงข้อมูลกันได้ แต่ในทางปฏิบัติแต่ละหน่วยงานจะมีกฎหมายอื่นที่กำกับดูแลการใช้ข้อมูลอยู่ เช่น กฎหมายข้อมูลทะเบียนราษฎร์ กฎหมายสุขภาพแห่งชาติ กฎหมายข้อมูลข่าวสารราชการ กฎหมายคุ้มครองข้อมูลส่วนบุคคล ฯลฯ และกฎหมายแต่ละฉบับอาจมี

กำหนดหลักเกณฑ์ในการจะจัดเก็บแต่ไม่ได้บัญญัติการเชื่อมโยงหรือแลกเปลี่ยนข้อมูล จึงมีปัญหาในการตีความ ดังนั้น ควรมีหน่วยงานกลางที่เป็นตัวแทนร่วมกันตัดสินเรื่องการเชื่อมโยงข้อมูลระหว่างกัน

- สำหรับข้อมูลสถิติเป็นข้อมูลเปิด ไม่มีข้อจำกัดด้านกฎหมายไม่ว่าจะเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือระเบียบการรักษาความลับของทางราชการ เป็นข้อมูลที่ไม่มีปัญหาในการเข้าถึงหรือแลกเปลี่ยนข้อมูล แต่การที่หน่วยงานต้นทางไม่ให้ข้อมูล ส่วนใหญ่มาจากปัญหาในมิติเรื่องคุณภาพข้อมูล

- ในส่วนของสำนักงานตำรวจแห่งชาติ ไม่มีข้อจำกัดด้านกฎหมาย เนื่องจากในประมวลกฎหมายวิธีพิจารณาความอาญาให้อำนาจเจ้าหน้าที่ตำรวจในการสืบสวนสอบสวนและใช้ข้อมูลเพื่อประโยชน์ในการป้องกันอาชญากรรม แต่ทั้งนี้ต้องขึ้นอยู่กับข้อตกลงระหว่างหน่วยงาน เช่น กรมการปกครอง ว่าจะให้มีการเชื่อมโยงข้อมูลได้มากน้อยเพียงใด และเมื่อได้ข้อมูลมาแล้วจะต้องดูแลข้อมูลให้มีความปลอดภัยโดยการกำหนดคนที่มีสิทธิเข้าถึงข้อมูล ซึ่งถือเป็นเรื่องสำคัญอย่างยิ่ง สำนักงานตำรวจแห่งชาติจะมีการควบคุมสิทธิการใช้งานว่าต้องมีความถูกต้อง และข้อมูล log file สามารถตรวจสอบย้อนกลับได้เกือบร้อยเปอร์เซ็นต์

- มีปัญหาการเข้าถึงข้อมูลของภาคเอกชน เนื่องจากกฎหมายของประเทศไทยไม่ได้กำหนดให้สามารถเข้าถึงข้อมูลของเอกชนได้แบบกฎหมายต่างประเทศ ภาคเอกชนก็มีความกังวลเรื่องความปลอดภัยของข้อมูลของหน่วยงานภาครัฐ อีกทั้งข้อมูลของสำนักงานตำรวจแห่งชาติในระบบ Crime ก็เป็นข้อมูลที่เกี่ยวข้องกับคดีและบางคดียังไม่สิ้นสุด จึงไม่สามารถเปิดให้เอกชนเข้ามาเชื่อมโยงหรือใช้ประโยชน์ข้อมูลดังกล่าวได้ ส่วนข้อมูลที่เอกชนสามารถเข้าถึงและนำไปใช้ประโยชน์ได้นั้น จะต้องมีการหารือร่วมกันเกี่ยวกับขอบเขตการอนุญาตและการใช้ข้อมูลต่อไป

- ปกติเวลาสำนักงานตำรวจแห่งชาติมีการประสานเชื่อมโยงข้อมูลจากหน่วยงานใด จะไม่ได้นำข้อมูลมาเก็บไว้เอง ทั้งนี้เพื่อลดภาระในการเก็บข้อมูล และจะไม่ยอมให้หน่วยงานอื่นดึงข้อมูลไปเก็บไว้เช่นเดียวกัน เนื่องจากจะมีประเด็นเรื่องความปลอดภัยของข้อมูล

ประเด็นขอบเขตการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ของภาครัฐ

- ข้อมูลที่อยู่ในกระบวนการยุติธรรมส่วนมากเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว ดังนั้นหน่วยงานที่ไม่มีส่วนเกี่ยวข้องกับการดำเนินคดีอาจไม่มีอำนาจในการขอเชื่อมโยงข้อมูลได้ แต่ละหน่วยงานจะมีกรอบกฎหมายและอำนาจในการใช้ข้อมูล ก็ควรจะดำเนินการภายใต้กรอบกฎหมายของหน่วยงานตน

- หน่วยงานเจ้าของข้อมูลควรจะต้องทราบว่าข้อมูลถูกใช้ในภารกิจใด จึงเป็นหน้าที่ของหน่วยงานที่ร้องขอเข้าถึงข้อมูลจะต้องแสดงให้เห็นถึงกรอบกฎหมายและการนำข้อมูลไปใช้ โดยเฉพาะหาก

ข้อมูลที่ขอเข้าถึงเป็นข้อมูลส่วนบุคคล โดยในปัจจุบันการใช้ big data ที่เห็นผลอย่างมากคือการเชื่อมโยงข้อมูลภาคเกษตรเพื่อคำนวนผลผลิตทางการเกษตรและพื้นที่เพาะปลูก

- ภาครัฐควรกำหนดขอบเขตด้านเวลาในการใช้ข้อมูล เพื่อเป็นหลักประกันให้เจ้าของข้อมูล

- หน่วยงานรัฐอาจมีปัญหาการเชื่อมโยงข้อมูลในประเด็นกฎหมายการรักษาความลับของทางราชการ ปัญหาทางปฏิบัติที่เกิดขึ้นจึงอยู่ที่การตีความคำว่าความลับราชการ ที่แต่ละหน่วยงานตีความแตกต่างกัน

- การเชื่อมโยงข้อมูลจะต้องเป็นไปตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิตอล ซึ่งกำหนดมาตรฐานธรรมาภิบาลข้อมูล เป็นมาตฐานกลางเพื่อให้ทุกหน่วยงานของรัฐยึดถือปฏิบัติ ดังนั้น หน่วยงานของรัฐทุกหน่วยงานต้องทำตามมาตรฐานดังกล่าว ส่วนขอบเขตการใช้ข้อมูล ก็จะเป็นไปตามภารกิจของหน่วยงานที่อาจแตกต่างกัน การเอาข้อมูลของหน่วยงานมาแลกเปลี่ยนกันตามข้อกำหนดระหว่างหน่วยงานแตกต่างกันไปตามอำนาจหน้าที่

ประเด็นเรื่องหลักประกันเกี่ยวกับสิทธิของเจ้าของข้อมูล

- การคุ้มครองสิทธิของเจ้าของข้อมูลเป็นสิทธิตามกฎหมายที่เป็นหลักประกันให้กับเจ้าของข้อมูลส่วนบุคคล

- หน่วยงานรัฐที่นำข้อมูลไปใช้ควรมีความโปร่งใสและควรมีระบบการตรวจสอบจากหน่วยงานที่เกี่ยวข้องและประชาชนผู้มีส่วนได้เสีย

- หน่วยงานของรัฐนอกจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้วยังต้องคำนึงและปฏิบัติตามหลักเกณฑ์ของกฎหมายข้อมูลข่าวสารของทางราชการอีกด้วย และหน่วยงานควรเตรียมออกระเบียบหรือกฎหมายลูกที่เกี่ยวข้องเพื่อรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลด้วย

- จำเป็นต้องดำเนินการให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกฎหมายที่มีหลักประกันที่เพียงพอสำหรับเจ้าของข้อมูลส่วนบุคคล

- หน่วยงานภาครัฐในปัจจุบันมีข้อยกเว้นเกี่ยวกับการเก็บ ใช้และเปิดเผยข้อมูลส่วนบุคคลของประชาชนหลายประกา รโดยเฉพาะการกระทำเพื่อประโยชน์สาธารณะ รวมถึงการป้องกันและปราบปรามอาชญากรรมด้วย ทำให้ในบางครั้ง หน่วยงานรัฐจึงอาจยังไม่ได้ตระหนักถึงสิทธิความเป็นส่วนตัวของประชาชนที่มากเพียงพอ ซึ่งแตกต่างจากภาคเอกชนที่กฎหมายกำหนดโทษค่อนข้างรุนแรงหาก ไม่ปฏิบัติตามหลักเกณฑ์การคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล

ข้อเสนอแนะในการแก้ไขกฎหมายเพื่อนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ในระบบงานยุติธรรมด้านการป้องกันและปราบปรามอาชญากรรมและการบริหารจัดการข้อมูลขนาดใหญ่ของภาครัฐ

- ควรใช้ข้อมูลที่จัดเก็บบนมาตรฐานเดียวกันเพื่อลดปัญหาและเพิ่มประสิทธิภาพในการเชื่อมโยงข้อมูล ทั้งรายละเอียดข้อมูลที่จัดเก็บและข้อมูลอ้างอิงที่เป็นฐานข้อมูลเดียวกัน และหน่วยงานควรทำข้อมูลขององค์กรให้อยู่ในรูปแบบดิจิทัลทั้งหมด

- หน่วยงานในกระบวนการยุติธรรมที่มีการเชื่อมโยงข้อมูลจำเป็นต้องทำบัญชีข้อมูล (Data Catalog) คล้ายสมุดหน้าเหลือง เพื่อให้เห็นข้อมูลที่จัดเก็บทั้งระบบว่าเก็บข้อมูลอะไรบ้าง เก็บโดยใช้อำนาจตามกฎหมายใด เพื่อวัตถุประสงค์อย่างไร ใครเป็นเจ้าของข้อมูล และระบุคำอธิบายรายละเอียดของข้อมูลเอาไว้

- หน่วยงานทุกหน่วยงานควรทำตามมาตรฐานธรรมาภิบาลข้อมูลภาครัฐโดยทำผ่านระบบเทคโนโลยีสารสนเทศ เช่น การจัดชั้นความลับข้อมูล การอนุญาตให้เข้าถึงข้อมูล

- ควรพัฒนาศักยภาพของบุคลากร โครงสร้างพื้นฐานและสิ่งอำนวยความสะดวกของหน่วยงานภาครัฐ เพื่อรองรับการปฏิบัติงานด้านเทคโนโลยี

- กฎหมายในปัจจุบันเอื้อประโยชน์ต่อการทำงานและการเชื่อมโยงข้อมูลระหว่างหน่วยงานรัฐได้ในระดับหนึ่ง เพียงอาจจะติดขัดในเรื่องของการทำบันทึกความตกลงระหว่างหน่วยงาน

- เพิ่มเติมเรื่องงบประมาณทางด้านไอที เพื่อให้อุปกรณ์มีความทันสมัยและสามารถเชื่อมโยงข้อมูลได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น

- ปัญหาส่วนใหญ่จะไม่ใช่ปัญหาข้อกฎหมายแต่เป็นปัญหาในทางปฏิบัติของความร่วมมือระหว่างหน่วยงานรัฐที่เป็นเจ้าของข้อมูลและปัญหาจากกระบวนการนำข้อมูลมาเชื่อมโยงกัน เนื่องจากฐานข้อมูลแต่ละฐานมีคุณภาพของข้อมูลที่แตกต่างกัน ดังนั้น แนวทางแก้ไขควรจะแก้ไขที่คุณภาพของข้อมูลและรูปแบบการจัดเก็บและการเชื่อมโยงข้อมูล รวมทั้งการบูรณาการความร่วมมือระหว่างหน่วยงาน

1.2 สรุปผลการเก็บรวบรวมข้อมูลจากการประชุมกลุ่มย่อย

ผู้วิจัยได้ดำเนินการจัดประชุมกลุ่มย่อย (Focus Group) เพื่อรับฟังความเห็นเกี่ยวกับปัญหา อุปสรรค และแนวทางการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปรามอาชญากรรม โดยพื้นที่ในการเก็บรวบรวมข้อมูล ได้แก่ กรุงเทพมหานคร จังหวัดเชียงใหม่ จังหวัดชลบุรี ดังนี้

ครั้งที่ 1 จังหวัดเชียงใหม่ ในวันพฤหัสบดีที่ 17 กุมภาพันธ์ 2565 เวลา 13.30 -16.00 น.

ครั้งที่ 2 จังหวัดชลบุรี ในวันศุกร์ที่ 18 กุมภาพันธ์ 2565 เวลา 13.30 -16.00 น.

ครั้งที่ 3 กรุงเทพมหานคร ในวันจันทร์ที่ 7 มีนาคม 2565 เวลา 13.30 – 16.00 น.

กลุ่มประชากรเป้าหมาย ได้แก่ ผู้ที่มีส่วนได้เสีย (Stakeholders) ในการบังคับใช้กฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมและการบริหารข้อมูลขนาดใหญ่ภาครัฐ ดังนี้

กลุ่มที่ 1 กลุ่มหน่วยงานด้านเทคโนโลยีดิจิทัล ได้แก่ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมสำนักงานนวัตกรรมแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล

กลุ่มที่ 2 กลุ่มหน่วยงานในกระบวนการยุติธรรมทางอาญา ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม

กลุ่มที่ 3 กลุ่มภาคเอกชนและตัวแทนภาคประชาชน

มีสรุปผลการประชุมกลุ่มย่อยตามประเด็น ดังนี้

ประเด็นภารกิจของหน่วยงานที่เกี่ยวกับการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data)

ผู้แทนสำนักงานปลัดกระทรวงยุติธรรม - กระทรวงยุติธรรมมีการนำข้อมูล Big Data มาใช้ในการวิเคราะห์ในองค์กรประมาณ 3-4 ล้านข้อมูลจำนวนผู้กระทำความผิดที่เข้ามาสู่ระบบ แต่จะเน้นใช้ข้อมูลดังกล่าวกับงานของหน่วยงานที่มีภารกิจด้านพฤตินิสัยของผู้กระทำความผิด ได้แก่ กรมราชทัณฑ์ กรมคุมประพฤติ กรมพินิจและคุ้มครองเด็กและเยาวชน แต่ในงานวิจัยจำเป็นต้องกำหนดนิยามให้ชัดเจนว่าข้อมูล Big Data ต้องมีปริมาณข้อมูลขนาดไหน

กระทรวงยุติธรรมได้ดำเนินการเกี่ยวกับระบบ Big Data ตั้งแต่ปี 2562 และมีการบูรณาการข้อมูลจากหน่วยงานทั้ง 3 กรมและใช้ระบบ machine learning ในการวิเคราะห์ข้อมูลและการคาดเดาเหตุการณ์ในอนาคต กล่าวคือ มีการทำนายโอกาสในการกระทำความผิดซ้ำของผู้กระทำผิดที่เข้าสู่กระบวนการพัฒนาพฤตินิสัย มีการทำนายว่าผู้กระทำความผิดจะกลับมากระทำความผิดซ้ำหรือไม่ โดยมีการทำนาย 2 ครั้งคือครั้งแรกที่มีการเข้าสู่กระบวนการของหน่วยงานและครั้งที่ 2 คือเมื่อสิ้นสุดกระบวนการของ

หน่วยงาน โดยหน่วยงานต้องการใช้ประโยชน์ของข้อมูลว่าระดับความเสี่ยงในการกระทำความผิดซ้ำจะเป็นเท่าไหร่ มี 3 ระดับจากน้อยไปมากคือ เขียว เหลือง แดง และต้องการข้อมูลที่ทำให้ทราบถึงปัจจัยที่มีอิทธิพลต่อการกระทำความผิดซ้ำ เพื่อนำมาใช้ในการแก้ไขฟื้นฟูพัฒนานิสัยของผู้กระทำความผิดให้ตรงจุด และต้องการหาข้อมูลว่าถ้ามีการกระทำความผิด ผู้กระทำความผิดจะกลับมากระทำความผิดซ้ำในข้อหาใด

ผู้แทนกองบัญชาการตำรวจสอบสวนกลาง – ของสำนักงานตำรวจแห่งชาติมี 2 ระบบ คือ ระบบ Crime ซึ่งเป็นระบบการนำเข้าข้อมูล และระบบ Big Data ของกองบัญชาการตำรวจสอบสวนกลาง ซึ่งเป็นระบบการใช้ประโยชน์จากข้อมูล โดยปัจจุบันมีการพัฒนาระบบ Big Data ซึ่งในส่วนของการปราบปราม จะทำยังไงให้การบังคับใช้กฎหมายมีประสิทธิภาพ ปัญหาที่พบคือการเข้าถึงข้อมูลเพื่อให้ทราบข้อเท็จจริงและการกระทำความผิดและความไม่สมบูรณ์ครบถ้วนของข้อมูล ว่าจะทำยังไงให้สามารถนำข้อมูลหรือเบาะแสที่ได้รับมาขยายผลเพื่อนำไปสู่การพิสูจน์การกระทำความผิดได้ ในขณะเดียวกันข้อมูลที่เกี่ยวกับการแจ้งเตือนการกระทำความผิด เช่น พฤติกรรมที่สุ่มเสี่ยงต่าง ๆ ก็มีการนำมาวิเคราะห์และมำแผนประทุษกรรม ความคาดหวังของสำนักงานตำรวจแห่งชาติคือการคาดการณ์หรือพยากรณ์เหตุล่วงหน้า แต่ปัจจุบันภาครัฐมีปัญหาเรื่องข้อมูลของหน่วยงานภาครัฐไม่ได้มีมาตรฐานการจัดเก็บข้อมูลแบบเดียวกัน ชุดข้อมูลจึงเป็นคนละชุดกัน เช่น การเก็บชื่อ ที่อยู่ ถ้ามาจากต่างหน่วยงานก็จะเป็นข้อมูลคนละชุดกัน จะต้องใช้กระบวนกา รในการจัดการคัดแยกข้อมูลก่อนนำมาใช้ ซึ่งมีการใช้ Machine Learning มาช่วย และมีปัญหาเกี่ยวกับโครงสร้างของข้อมูล เช่น ข้อมูลคำพิพากษา หรือข้อมูลพฤติกรรมของบุคคล มีความท้าทายในการนำ ข้อมูลดังกล่าวมาใช้ และปัจจุบันสำนักงานตำรวจแห่งชาติกำลังศึกษาวิจัยเกี่ยวกับการจำแนกประเภทอาชญากรรมว่าจะทำอย่างไรให้การเก็บข้อมูล ณ จุดแรก เป็นมาตรฐานเดียวกัน เช่น การใช้มาตรฐาน ICCS มาเป็นแนวทาง เพื่อให้ข้อมูลดังกล่าวมาใช้ได้ เพราะปัจจุบันประเทศไทยเก็บข้อมูลแบบ Law Base โดยใช้ข้อหาเป็นตัวตั้ง แต่หลายประเทศจะมีมาตราฐานที่มุ่งเน้นการเก็บแบบเหตุการณ์เพื่อนำไปสู่การคัดแยกและใช้ประโยชน์จากข้อมูลต่อไป นอกจากนั้น ยังมีปัญหาความพร้อมข้อมูลในแต่ละพื้นที่ หากต้องการคาดการณ์พยากรณ์การเกิดเหตุก็ยังมีปัญหาเรื่องพิกัดของสถานที่เกิดเหตุ โมเดลที่น่าสนใจคือโมเดลของประเทศออสเตรเลีย

ผู้แทนสถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ (สวข.) - ปัจจุบันมีการดำเนินการเกี่ยวกับ big data ภาครัฐที่สำคัญได้แก่ โครงการ health link ที่มีการเชื่อมข้อมูลผู้ป่วย เป็นแพลตฟอร์มสำหรับเชื่อมโยงข้อมูลสุขภาพ เพื่อให้แพทย์สามารถเข้าดูข้อมูลสุขภาพของผู้ป่วยจากโรงพยาบาลอื่น ๆ ที่เข้าร่วมโครงการได้ และผู้ป่วยสามารถกำหนดสิทธิการเข้าถึงข้อมูลของตนเอง ซึ่ง

หมายความว่าไม่ใช่แพทย์ทุกคนที่จะเข้ามาดูข้อมูลสุขภาพของผู้ป่วยเมื่อไหร่ก็ได้ และยังเป็นประโยชน์สำหรับผู้ป่วยที่เข้ารับบริการฉุกเฉินเป็นอย่างมากในการให้สิทธิแพทย์ในห้องฉุกเฉินสืบค้นข้อมูลของผู้ป่วยที่หมดสติ ซึ่งข้อมูลที่ได้มานั้นอาจจะช่วยรักษาชีวิตของผู้ป่วยในห้องฉุกเฉินได้อย่างทันท่วงที การใช้ big data ส่วนมากจะใช้ในภาคสาธารณสุขที่มีการคาดการณ์เกี่ยวกับสถานการณ์ของโรคที่จะเกิดขึ้น เพื่อกำหนดนโยบายด้านสุขภาพ และทางสถาบันยังมีการดำเนินงานให้กับอีกหลายหน่วยงาน รวมทั้งการจัดอบรมเรื่องการวิเคราะห์ข้อมูล

ผู้แทนสำนักงานศาลยุติธรรม – สำนักงานศาลยุติธรรม (ในส่วนของสำนักงานอธิบดีผู้พิพากษาภาค 2) จะมีข้อมูลที่เกี่ยวกับคดี ข้อมูลคำพิพากษาและข้อมูลในส่วนของงานธุรการ มีการใช้ระบบ Microsoft Access เก็บข้อมูลที่มีโครงสร้าง และจะมีการส่งคำพิพากษามาจากศาล 21 ศาลในภูมิภาค เพื่อมาตรวจร่างก่อนที่จะอ่านคำพิพากษา การใช้ข้อมูล big data จะใช้ในส่วนข้อมูลที่เป็น information มากกว่าการนำข้อมูลมาใช้ในเชิงพยากรณ์ และมีการเชื่อมโยงข้อมูลในระบบของสำนักงานกิจการยุติธรรม หรือ DXC ที่เริ่มมาตั้งแต่ปี 2551 ซึ่งจะเชื่อมโยงเฉพาะในส่วนของคำพิพากษา แต่ในส่วนของข้อมูลทางคดีซึ่งเป็นข้อมูลลับจะไม่ได้มีการเชื่อมโยง โดยสามารถจำแนกข้อมูลได้เป็นสองประเภทคือ ข้อมูลที่สามารถเปิดเผยได้ อาทิ วันนัดพิจารณาคดี ข้อมูลคำพิพากษา (ซึ่งมีการปกปิดชื่อของโจทก์และจำเลย) และข้อมูลที่ไม่สามารถเปิดเผยได้ อาทิ ข้อมูลทางคดี

ผู้แทนสำนักงานตำรวจแห่งชาติ - ในสถานีตำรวจมีการใช้ข้อมูลการเกิดเหตุจากกล้องวงจรปิด CCTV มาลงไว้ในระบบ สำหรับการใช้ประโยชน์จากข้อมูลหน่วยงานตำรวจจะมีกองวิจัยและวางแผนดูแลเรื่องการวิเคราะห์ข้อมูลและสำนักงานยุทธศาสตร์ที่จะมีการนำข้อมูลมาวิเคราะห์ เพื่อใช้ประโยชน์ในการกำหนดกรอบอัตรากำลัง สถานีตำรวจจะมีหน้าที่ในการรวบรวม แต่ฐานของข้อมูลทั้งหมดจะอยู่ที่สำนักงานตำรวจแห่งชาติ และมีการกำหนดการเข้าถึงข้อมูลตามอำนาจหน้าที่ของหน่วยงาน

ผู้แทนกรมบัญชีกลาง – ข้อมูลขนาดใหญ่ของกรมบัญชีกลางจะเป็นข้อมูลในระบบ e-Government Procurement : e-GP ตามกฎหมายจัดซื้อจัดจ้างพัสดุภาครัฐ เป็นระบบที่เกี่ยวกับการเสนอราคา การประมูลงานของบริษัทผู้รับจ้าง ในปัจจุบันหน่วยงานภาครัฐก็ปรับวิถีการเสนอราคา จากการยื่นซองประมูลเป็นการประกวดราคาด้วยวิธีอิเล็กทรอนิกส์ผ่านระบบ e-GP ก็มีหน่วยงานเข้ามาใช้ระบบเป็นจำนวนมาก และในปัจจุบันมีการดึงข้อมูลในระบบ e-GP เพื่อคำนวณภาพรวมของเปอร์เซ็นต์ในการประหยัดงบประมาณภาครัฐ มีการดึงข้อมูลเกี่ยวกับราคากลางมาใช้ในการตรวจสอบ ซึ่งจะสัมพันธ์กับภารกิจของกรมบัญชีกลางในเรื่องการเบิกจ่ายงบประมาณ

ผู้แทนกรมสอบสวนคดีพิเศษ – กรมสอบสวนคดีพิเศษมีการเชื่อมโยงข้อมูลกับกรมการปกครอง สำนักงานตำรวจแห่งชาติ และกรมการขนส่งทางบก เพื่อนำข้อมูลมาใช้ในการสืบสวนสอบสวน มีการเก็บรวบรวมข้อมูลอาชญากรรมในพื้นที่และจัดเก็บไปที่ส่วนกลาง จากนั้นยังมีการเก็บข้อมูลจากแหล่งข่าว บนโปรแกรม iBase เป็นคลังข้อมูลและหน่วยงานส่วนกลางจะมีหน้าที่ในการวิเคราะห์และประมวลผล

ประเด็นแนวทางการนำข้อมูลขนาดใหญ่ (Big Data) มาวิเคราะห์เพื่อลดการเกิดอาชญากรรมและปรามปรามการกระทำความผิด

ผู้แทนกองบัญชาการตำรวจสอบสวนกลาง – แนวทางการนำข้อมูลขนาดใหญ่มาใช้จะมีด้วยกัน 3 ส่วนคือ 1) การใช้ข้อมูลในเชิงสถิติ 2) การใช้ข้อมูลในเชิงบริหาร และ 3) การใช้ข้อมูลในการคาดการณ์อาชญากรรม ส่วนปัญหาที่เจอคือ การเกิดอาชญากรรมแต่ละครั้งจะมีการนับสถิติอย่างไร ในกรณีที่เกี่ยวพันกับความผิดหลายข้อหา โดยโครงการที่มีการดำเนินการอยู่ ได้แก่ การจัดทำแผนประทุษกรรม ซึ่งจะเป็นส่วนหนึ่งที่จะเข้ามาช่วยทั้งในการปราบปรามและในเชิงป้องกัน เช่น การคาดการณ์ล่วงหน้าเกี่ยวกับแนวโน้มการกระทำความผิดของอาชญากรรมในภาพรวมของประเทศ โดยในปัจจุบันกลุ่มใหญ่ ๆ ได้แก่ อาชญากรรมแบบ Street Crime กับ Cyber Crime แผนประทุษกรรมจึงมีประโยชน์ในการแจ้งเตือนอาชญากรรม ส่วนการคาดการณ์การเกิดอาชญากรรม หรือ Crime Prediction อยู่ในระหว่างดำเนินการ แต่ปัญหาที่เกิดขึ้นขณะนี้อยู่ที่ความพร้อมของข้อมูล ทั้งนี้ มีการพัฒนาต่อยอดจากสถิติคดีอาญา 5 กลุ่มและข้อมูลจากการดำเนินงานของสายตรวจ โดยการออกตรวจของสายตรวจในแต่ละพื้นที่ จะต้องมีเหตุผลและความชัดเจนเพียงพอว่าทำไมจะต้องเป็นการตรวจในพื้นที่นั้น ๆ ส่วนการทำ Criminal Profiling จะเน้นใช้ประโยชน์ในงานด้านการสืบสวนมากกว่าการป้องกัน โดยเฉพาะในอาชญากรรมทางเพศเด็ก

ผู้แทนสถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ (สวข.) – การทำ Crime Prediction อย่างเช่น การคาดการณ์เหตุการณ์ในแต่ละช่วงเวลาว่าช่วงเวลาใดจะเกิดอาชญากรรมสูง ทำให้สามารถวางแนวทางการป้องกันอาชญากรรมล่วงหน้าได้ แต่มีประเด็นที่น่ากังวลคือ หากเป็นกรณีที่มีการคาดการณ์ว่ากลุ่มคน หรือตัวบุคคลลักษณะใดจะมีพฤติกรรมในการก่ออาชญากรรม จะเป็นประเด็นละเอียดอ่อนซึ่งกระทบต่อตัวบุคคล เป็นประเด็นผลกระทบต่อสิทธิมนุษยชน รวมทั้งการใช้ Face Recognition แล้วอาจมีข้อมูลผิดพลาด การตรวจจับผิด จะเป็นประเด็นขึ้นมา ดังนั้น ในแง่ของการนำข้อมูล

ขนาดใหญ่มาใช้ประโยชน์ ควรเน้นการคาดการณ์ในระดับพื้นที่ มากกว่าจะคาดการณ์เกี่ยวกับตัวบุคคล และอยากให้คำนึงถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย

ผู้แทนกระทรวงยุติธรรม – ควรมีการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเพื่อใช้ประโยชน์ร่วมกัน

ผู้แทนสำนักงานตำรวจแห่งชาติ - การนำข้อมูลมาใช้วิเคราะห์ในแต่ละพื้นที่ ในแต่ละสถานีตำรวจจะแตกต่างกันตามประเภทอาชญากรรมที่เกิดขึ้น ซึ่งเป็นอาชญากรรมพื้นฐาน (เพราะอาชญากรรมพิเศษจะอยู่ภายใต้หน่วยงานเฉพาะ) อาจใช้ข้อมูลมาวิเคราะห์ความถี่ของการเกิดอาชญากรรม ในพื้นที่นั้นๆ ทำให้ตำรวจสามารถจัดสายตรวจได้ตรงจุด สามารถวิเคราะห์ได้ว่าผู้กระทำความผิดมาจากพื้นที่ใด เป็นการใช้ข้อมูลเพื่อลดปัญหาอาชญากรรม

ผู้แทนสำนักงานศาลยุติธรรม – สำนักงานศาลยุติธรรมมีการบันทึกความตกลงร่วมกันในการเชื่อมโยงข้อมูลกับระบบ CRIME ของสำนักงานตำรวจแห่งชาติ เพื่อประโยชน์ในเรื่องของการออกหมายจับ ดูเหตุแห่งการออกหมายจับและสนับสนุนการปฏิบัติหน้าที่ของตำรวจศาล (Court Marshal) มีหน้าที่ในการออกหมายจับ ก็เป็นลักษณะของการใช้ประโยชน์จากตัวข้อมูลโดยตรง ไม่ใช่การใช้ในลักษณะของการพยากรณ์หรือการคาดการณ์แต่อย่างใด

ผู้แทนสำนักงานศาลยุติธรรม – สนับสนุนให้การนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ เพราะเป็นประโยชน์อย่างมากในการเตือนภัยเช่นเดียวกับต่างประเทศและมีประโยชน์ในด้านพยานหลักฐาน อาจจะต้องมีกฎหมายในเรื่องของพยานหลักฐานที่เพิ่มมากขึ้นให้รองรับการใช้ข้อมูล Big Data รวมทั้งควรมีกฎหมายในเรื่อง Big Data เป็นการเฉพาะ เพื่อให้การใช้ข้อมูลมีความโปร่งใสและเป็นไปตามหลักธรรมาภิบาล

ผู้แทนกรมสอบสวนคดีพิเศษ – ในมิติด้านการป้องกัน หากมีข้อมูลขนาดใหญ่ (big data) ที่เกี่ยวข้องกับการกระทำความผิด อาจนำมาใช้ในการวิเคราะห์สาเหตุของการกระทำความผิดซ้ำ ส่วนมิติของการปราบปราม หากภาครัฐสามารถเชื่อมโยงข้อมูลไม่ว่าจะเป็นหน่วยงานภาครัฐด้วยกันเองหรือกับภาคเอกชน จะเป็นประโยชน์ในการสืบสวนการกระทำความผิด

ประเด็นข้อจำกัดด้านกฎหมายในการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ในส่วนของการป้องกันและปราบปรามอาชญากรรม

ผู้แทนกองบัญชาการตำรวจสอบสวนกลาง – สภาพปัญหาของการทำโครงการ big data คือการเชื่อมโยงข้อมูล และนอกจากนั้นในส่วนของสำนักงานตำรวจแห่งชาติจะมีการศึกษาข้อกฎหมายเกี่ยวกับข้อมูลข่าวสารของทางราชการและกฎหมายการรักษาความลับของทางราชการเพิ่มเติมด้วย โดยในข้อเท็จริง

เรื่องการเชื่อมโยงข้อมูลของหน่วยงานรัฐ กฎหมายให้กระทำได้อยู่แล้ว ไม่ว่าจะเป็นกฎหมายว่าด้วยการบริหารงานและให้บริการภาครัฐผ่านระบบดิจิทัล หรือกฎหมายอื่น และยังได้รับการยกเว้นมิให้นำกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาบังคับใช้ นอกจากนั้น ปัญหาที่เกิดขึ้นคือ การใช้ข้อมูล Big Data ในงานป้องกันอาชญากรรม มีความจำเป็นต้องใช้ข้อมูลจำนวนมาก ซึ่งทางสำนักงานตำรวจแห่งชาติไม่ได้เป็นเจ้าของข้อมูลทั้งหมด ในส่วนข้อมูลที่อยู่กับภาคเอกชนนั้น หากจะนำมาเชื่อมโยงและใช้ประโยชน์ร่วมกันอาจมีข้อจำกัดด้านกฎหมาย เพราะปัจจุบันสามารถขอข้อมูลจากภาคเอกชนได้เฉพาะบางรายการที่มีเหตุตามที่กฎหมายอนุญาต เป็นการใช้ประโยชน์ในทางคดีซึ่งมีกฎหมายให้อำนาจไว้อยู่แล้ว แต่ลักษณะของการใช้ข้อมูลขนาดใหญ่ จำเป็นต้องมีข้อมูลปริมาณมาก ๆ มารวมกันและวิเคราะห์ เชิงลึกจากข้อมูลดังกล่าว ดังนั้น มีประเด็นข้อกฎหมายเกี่ยวกับการขอข้อมูลจากภาคเอกชน และในกรณีที่ทางสำนักงานตำรวจจะแชร์ข้อมูลที่มีให้หน่วยงานภาคเอกชน สามารถทำได้มากน้อยแค่ไหน รวมทั้งมาตรการรักษาความปลอดภัยข้อมูล นอกจากนั้นในปัจจุบันมีกฎหมายใหม่หลายฉบับที่บังคับใช้ ทำให้อาจเกิดการตีความข้อกฎหมายในประเด็นต่าง ๆ ของหน่วยงานในกระบวนการยุติธรรมและยังไม่มีความเห็นเป็นที่ยุติที่จะทำให้นำไปสู่การปฏิบัติได้จริงและเกิดความรวดเร็วในการดำเนินงาน

ผู้แทนสำนักงานตำรวจแห่งชาติ – ควรมีกฎหมายเอื้อประโยชน์ให้หน่วยงานภาครัฐสามารถขอเชื่อมโยงข้อมูลหรือขอข้อมูลจากภาคเอกชนได้ เนื่องจากข้อมูลขนาดใหญ่จะเกิดขึ้นในทุกภาคส่วนและภาครัฐจำเป็นต้องได้ข้อมูลในปริมาณที่มากมาเพื่อวิเคราะห์ต่อไป

ผู้แทนสำนักงานศาลยุติธรรม – ควรมีการร่างกฎหมายเกี่ยวกับการใช้ข้อมูลระหว่างหน่วยงานภาครัฐโดยเฉพาะ เช่นเดียวกับภาคเอกชนที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลและจะต้องมีการประชาสัมพันธ์ให้ทุกหน่วยงานทราบและปฏิบัติตามด้วย

ผู้แทนสำนักงานตำรวจแห่งชาติ – หากมีกฎหมายกำหนดเรื่องการแลกเปลี่ยนข้อมูล ขนาดใหญ่โดยเฉพาะก็จำเป็นต้องกำหนดโทษทางอาญา เช่น โทษจำคุก โทษปรับ สำหรับผู้ที่นำข้อมูลไปเผยแพร่และทำให้เกิดความเสียหายมากกว่าการใช้มาตรการทางปกครอง เพราะความเสียหายเกิดขึ้นโดยตรงกับเจ้าของข้อมูลส่วนบุคคล

ประเด็นขอบเขตการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ของภาครัฐ

ผู้แทนกองบัญชาการตำรวจสอบสวนกลาง – หน่วยงานภาครัฐจำเป็นต้องกำหนดมาตรฐานการบริหารจัดการข้อมูล (Data Governance) ซึ่งกฎหมายมีกำหนดไว้แล้วแต่ทางปฏิบัติจำเป็นต้องทำให้ชัดเจน

ว่าในแต่ละข้อมูลจะมีการกำหนดค่าในการรักษาความลับมากน้อยแค่ไหน รวมทั้งการแชร์ข้อมูลและการใช้ประโยชน์ ควรมีหน่วยงานต้นแบบให้หน่วยงานยึดถือเป็นแนวทาง และควรจัดทำคู่มือการปฏิบัติงาน

ประเด็นเรื่องหลักประกันเกี่ยวกับสิทธิของเจ้าของข้อมูล

ผู้แทนกองบัญชาการตำรวจสอบสวนกลาง – ในคดีบางประเภทกฎหมายให้ความคุ้มครองเหยื่อหรือผู้เสียหายในคดี เช่น คดีอาชญากรรมทางเพศ จึงต้องคำนึงด้วย โดยเฉพาะการทำ Criminal Profiling และในการใช้ข้อมูลขนาดใหญ่หน่วยงานของรัฐจะมีการคุ้มครองสิทธิของเจ้าของข้อมูลมากน้อยแค่ไหน

ผู้แทนสถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ (สวข.) – ควรระมัดระวังเรื่องการทำข้อมูลนิรนาม (data anonymous) เนื่องจากบางคนเข้าใจว่าการทำข้อมูลนิรานามคือการตัดชื่อและเลขบัตรประชาชนออก แต่ความจริงจะต้องทำให้ข้อมูลเหล่านั้นไม่สามารถระบุตัวตนได้อย่างสิ้นเชิง เพราะข้อมูลบางอย่างแม้ไม่มีข้อมูลชื่อหรือหมายเลขบัตรประชาชนเป็นยังเป็นข้อมูลที่ระบุตัวตนได้อยู่ เช่น ข้อมูลคนที่มีอายุมากที่สุดในกรุงเทพมหานคร ซึ่งสามารถระบุตัวตนได้ หรือข้อมูลตำแหน่งงาน ก็ยังเป็นข้อมูลที่ระบุตัวตนได้ เป็นต้น

กรมคุ้มครองสิทธิและเสรีภาพ – กรมคุ้มครองสิทธิอยู่ระหว่างการดำเนินการเพื่อเชื่อมข้อมูลกับระบบ Crime ของสำนักงานตำรวจแห่งชาติ อยู่ระหว่างการเจรจาเรื่องรูปแบบการเชื่อมโยงข้อมูล ซึ่งในส่วนของกรมจะเป็นการเชื่อมข้อมูลเกี่ยวกับตัวผู้เสียหาย เพื่อแจ้งให้มาขอรับเงินเยียวยาตามสิทธิของกฎหมาย สำหรับการให้หลักประกันสิทธิของเจ้าของข้อมูล กรมฯ ได้ดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และกรมคุ้มครองสิทธิและเสรีภาพได้มีการนำแนวทางปฏิบัติและแบบของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ DGA นำมาประยุกต์ใช้กับภารกิจของหน่วยงาน

ผู้แทนสำนักงานศาลยุติธรรม – การนำข้อมูลที่ได้มาจะต้องพิจารณาความถูกต้องของข้อมูลด้วย เนื่องจากอาจจะมีผลกระทบตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ข้อเสนอแนะในการแก้ไขกฎหมายเพื่อนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ประโยชน์ในระบบงานยุติธรรมด้านการป้องกันและปราบปรามอาชญากรรม

ผู้แทนกองบัญชาการตำรวจสอบสวนกลาง – มีความเห็นเป็น 3 ประเด็นดังนี้

1) ควรทำให้ข้อมูลภาครัฐเป็นข้อมูลเปิด (Open Data) ให้มากที่สุด และควรเปิดโอกาสให้ภาคเอกชนเข้ามามีส่วนร่วมในการบริหารจัดการด้วย เนื่องจากภาคเอกชนอาจมีความเชี่ยวชาญและมีมุงมองที่แตกต่างจากบุคลากรภาครัฐ ซึ่งอาจเป็นประโยชน์ต่อภาครัฐ และควรคำนึงเรื่องการเชื่อมต่อข้อมูล

2) มีความจำเป็นอย่างยิ่งในการพัฒนาบุคลกรให้มีทักษะความรู้ความเชี่ยวชาญในด้านเทคโนโลยี

3) การกำหนดมาตรการรักษาความปลอดภัยของข้อมูล ควรกำหนดทั้งมาตรการ Data Security และมาตรการ Cyber Security ทั้งในมุมของการเก็บข้อมูลให้ปลอดภัยทั้งจากกระบวนการประมวลผลข้อมูล และภัยคุกคามทางไซเบอร์

ผู้แทนกองบัญชาการศึกษา – สำนักงานตำรวจแห่งชาติ ในภารกิจด้านการศึกษา มีการใช้ประโยชน์จากข้อมูลขนาดใหญ่ในการถ่ายทอดความรู้ให้กับเจ้าหน้าที่ตำรวจในหลักสูตรต่าง ๆ ข้อเสนอแนะ คือ อยากให้มีการเชื่อมโยงข้อมูลกับภาคเอกชน ซึ่งงานของตำรวจจะมีทั้งมิติด้านการปราบปรามปละการป้องกัน ที่ทำได้ยากคือการใช้ข้อมูลในงานป้องกัน และจำเป็นต้องเชื่อมโยงข้อมูลกับภาคเอกชนที่ถือข้อมูลจำนวนมากและข้อมูลเหล่านั้นเป็นประโยชน์ต่องานป้องกันอาชญากรรม โดยควรศึกษาจากแนวทางการศึกษาของต่างประเทศแล้วนำมาปรับใช้กับประเทศไทย

ผู้แทนสำนักงานศาลยุติธรรม – ในปัจจุบันประเทศไทยมีปัญหาการขาดเจ้าภาพดูแลเรื่องข้อมูลขนาดใหญ่ (big data) ดังนั้น กฎหมายต้องกำหนดเจ้าภาพที่เป็นหน่วยงานกลางในการเชื่อมโยงข้อมูล ทำให้เกิดความชัดเจนของบุคคลที่มีสิทธิในการเข้าถึงข้อมูล เช่นเดียวกับในต่างประเทศ เช่น ประเทศสิงคโปร์ จีน สามารถนำข้อมูลมาเชื่อมโยงและใช้ประโยชน์ได้อย่างมีประสิทธิภาพ ทำให้การใช้ประโยชน์ในข้อมูลขนาดใหญ่ของประเทศไทยสมบูรณ์มากยิ่งขึ้น

ผู้แทนสำนักงานศาลยุติธรรม – ควรมีการเสนอร่างกฎหมายเกี่ยวกับพยานหลักฐานเพื่อรองรับการใช้ข้อมูลขนาดใหญ่

ข้อเสนอแนะเกี่ยวกับการบริหารจัดการข้อมูลขนาดใหญ่ของภาครัฐ

ผู้แทนกระทรวงยุติธรรม – มีความเป็นห่วงเกี่ยวกับปริมาณข้อมูลที่จัดเก็บ เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีหลักการคือให้เก็บและใช้ข้อมูลเท่าที่จำเป็น จากประสบการณ์เห็นว่า ภาครัฐมีการเก็บข้อมูลมากเกินไป ตัวอย่างเช่น การเก็บข้อมูลความพิการ ข้อมูลศาสนา ซึ่งเป็นข้อมูลอ่อนไหวและไม่มีความจำเป็นในการเก็บ ดังนั้น ภาครัฐควรตระหนักในเรื่องนี้อย่างมาก

ผู้แทนกองบัญชาการตำรวจสอบสวนกลาง – ปัญหาด้านการทำระบบคือปัญหาเรื่องของการปรับใช้กฎหมายกับการทำให้เป็นไปตามมาตรฐานด้านข้อมูล ซึ่งหน่วยงานภาครัฐควรมีคู่มือการปฏิบัติงานทั้งหมดที่เกี่ยวกับการจัดการข้อมูลขนาดใหญ่ ตั้งแต่กฎหมายต่าง ๆ ที่ต้องปฏิบัติตาม เช่น กฎหมายข้อมูลส่วนบุคคล กฎหมายข้อมูลข่าวสารของทางราชการ กฎหมายรักษาความมั่นคงปลอดภัยทางไซเบอร์ กฎหมาย

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายความรับผิดทางละเมิดของเจ้าหน้าที่ มติคณะรัฐมนตรีที่เกี่ยวข้อง ฯลฯ และมาตรฐานด้านต่าง ๆ ที่เกี่ยวข้อง เช่น มาตรฐานการรักษาความปลอดภัยของข้อมูล การทำตามหลักธรรมาภิบาลข้อมูลภาครัฐ ควรมีองค์กรเจ้าภาพในการจัดทำองค์ความรู้มาตรฐานในการปฏิบัติงาน

ผู้แทนสำนักงานศาลยุติธรรม – เพื่อสร้างความเชื่อมั่นในการใช้ข้อมูล ควรกำหนดขอบเขตของแต่ละหน่วยงานว่าจะสามารถใช้ข้อมูลได้มากน้อยแค่ไหนภายใต้ภารกิจของตน ควรมีนักวิทยาศาสตร์ข้อมูลประจำหน่วยงาน

2. ปัญหาและข้อจำกัดในการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปรามอาชญากรรมของประเทศไทย

2.1 ปัญหาด้านกฎหมาย

ฐานอำนาจตามกฎหมายที่สำนักงานตำรวจแห่งชาติในการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) ในการป้องกันและปราบปรามอาชญากรรม ได้แก่ พระราชบัญญัติตำรวจแห่งชาติ พ.ศ. 2547 บัญญัติให้สำนักงานตำรวจแห่งชาติมีอำนาจหน้าที่เกี่ยวกับการป้องกันและปราบปรามการกระทำความผิดทางอาญา รักษาความสงบเรียบร้อย ความปลอดภัยของประชาชนและความมั่นคงของราชอาณาจักร และปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของข้าราชการตำรวจ หรือสำนักงานตำรวจแห่งชาติ ตามความในมาตรา 6 (3) (4) และ (5) กับอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญาในการสืบสวน การสอบสวน การจับกุมผู้กระทำความผิด ฯลฯ โดยที่ในปัจจุบันสำนักงานตำรวจแห่งชาติได้มีการจัดทำระบบ Big Data ในงานป้องกันและปราบปรามอาชญากรรม โดยอยู่ระหว่างการดำเนินโครงการ

ข้อจำกัดด้านกฎหมายคือ ปัจจุบันพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ที่ตราขึ้นเพื่อหน่วยงานของรัฐจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพและตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งกำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการและการบูรณาการข้อมูล ภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล โดยวัตถุประสงค์ที่สำคัญประการหนึ่งคือเพื่อให้มีการบูรณาการฐานข้อมูลของหน่วยงานของ

รัฐทุกหน่วยงานเข้าด้วยกันเพื่อให้เป็นระบบข้อมูล เพื่อประโยชน์ในการบริหารราชการแผ่นดินและเพื่ออำนวยความสะดวกให้แก่ประชาชน และเพื่อยกระดับการบริหารงานและการให้บริการภาครัฐให้อยู่ในระบบดิจิทัล อันจะนำไปสู่การเป็นรัฐบาลดิจิทัลที่มีระบบการทำงานและข้อมูลเชื่อมโยงกันระหว่างหน่วยงานของรัฐอย่างมั่นคงปลอดภัย มีประสิทธิภาพ รวดเร็ว เปิดเผยและโปร่งใส ซึ่งในมาตรา 13 วางหลักว่า เพื่อประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชน ให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอที่จะเกิดการบูรณาการร่วมกัน โดยหน่วยงานของรัฐผู้รับข้อมูลดิจิทัลจะต้องใช้ข้อมูลตามวัตถุประสงค์ในหน้าที่และอำนาจของตนเท่านั้น และต้องดูแลรักษาข้อมูลให้มีความมั่นคงปลอดภัย ไม่มีการเปิดเผยหรือโอนข้อมูลไปยังบุคคลที่ไม่มีสิทธิเข้าถึงข้อมูล แต่กฎหมายดังกล่าวเป็นลักษณะการวางหลักเกณฑ์ทั่วไป เน้นเรื่องการให้บริการประชาชนกับและธรรมาภิบาลข้อมูลภาครัฐ ซึ่งในทางปฏิบัติอำนาจในการใช้ข้อมูลและการแบ่งปันข้อมูลก็จะเป็นอำนาจของหน่วยงานเจ้าของข้อมูล โดยเฉพาะการจัดเก็บข้อมูลของหน่วยงานในกระบวนการยุติธรรมที่จะเป็นการใช้ข้อมูลที่มีลักษณะพิเศษและเป็นข้อมูลที่มีผลกระทบสิทธิความเป็นส่วนตัวของประชาชน ซึ่งกฎหมายก็ไม่ได้มีการระบุชัดถึงการบริหารจัดการข้อมูลเพื่อใช้ในภารกิจด้านการป้องกันและปราบปรามอาชญากรรม อีกทั้ง การนำเทคโนโลยีการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) มาใช้จำเป็นต้องมีข้อมูลจำนวนมากที่มีความหลายหลายเพื่อนำมาใช้คาดการณ์สถานการณ์ของการกระทำความผิดในรูปแบบต่าง ๆ ของแต่ละพื้นที่และช่วงเวลา การดำเนินงานด้านเฝ้าระวังติดตาม การออกตรวจตรา การสืบสวน การบริหารความเสี่ยงในงานเฝ้าระวังติดตาม การใช้ข้อมูลจำนวนมากและหลายหลากดังกล่าว หน่วยงานภาครัฐมีความจำเป็นต้องเชื่อมโยงข้อมูลกับข้อมูลของภาคเอกชนและประชาชน และในส่วนของภาคเอกชนเองก็จำเป็นต้องขอเชื่อมโยงข้อมูลกับหน่วยงานรัฐในบางภารกิจที่เป็นประโยชน์สาธารณะ ดังนั้น จึงจำเป็นต้องให้อำนาจแก่หน่วยงานในการขอแบ่งปันข้อมูลจากภาคเอกชนและการใช้ข้อมูลร่วมกัน และกำหนดหลักเกณฑ์ต่าง ๆ ขึ้นมาเพื่อให้เกิดผลในทางปฏิบัติ ซึ่งประเด็นนี้ผู้วิจัยได้ศึกษาร่างกฎหมายธรรมาภิบาลข้อมูลของสหภาพยุโรป หรือ REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act) และกฎหมายว่าด้วยข้อมูลของสหภาพยุโรป (Data Act) เพื่อเป็นแนวทางในการปรับใช้สำหรับประเทศไทย

2.2 ประเด็นผลกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล

ปัจจุบันมีการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อคุ้มครองและป้องกันการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล โดยกำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและกำหนดกลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป รวมทั้งกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายไว้อย่างชัดเจน โดยการดำเนินงานด้านการป้องกันและปราบปรามอาชญากรรมจะเป็นกรณีมาตรา 4 (2) และ (5) ข้อยกเว้นของการไม่นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาใช้บังคับ กล่าวคือ ในมาตรา 4 กำหนดไว้ “พระราชบัญญัตินี้ไม่ใช้บังคับแก่ ...

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์ ...

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา”

บทบัญญัติดังกล่าวมีผลทำให้การประมวลผลข้อมูลส่วนบุคคลในกิจกรรมด้านงานป้องกันและปราบปรามอาชญากรรมทั้งกรณีงานด้านการป้องกันอาชญากรรม (การรักษาความปลอดภัยของประชาชน) และงานด้านการปราบปรามในการดำเนินกระบวนการยุติธรรมทางอาญา ทั้งงานสืบสวนแสวงหาข้อเท็จจริง งานสอบสวน การรวบรวมพยานหลักฐาน กระบวนการพิจารณาคดี ไม่ต้องอยู่ภายใต้การบังคับใช้ของกฎหมายดังกล่าว แต่อย่างไรดี ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับยกเว้นยังคงมีหน้าที่ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย เพื่อป้องกันไม่ให้ข้อมูลส่วนบุคคลรั่วไหลและป้องกันเหตุละเมิดข้อมูลส่วนบุคคลในรูปแบบต่าง ๆ โดยปัจจุบันให้เป็นไปตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 ที่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)

ประเด็นผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล จึงเป็นเรื่องกระบวนการในการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลของหน่วยงานที่จะนำไปใช้ในภารกิจในงานป้องกันและปราบปราม อาชญากรรมว่าจะต้องให้หลักประกันต่อประชาชนว่าข้อมูลที่เก็บรวบรวมไปนั้นจะนำไปใช้ตามภารกิจเท่านั้น และต้องมีมาตรการรักษาความปลอดภัยที่เหมาะสมด้วย รวมทั้งระดับของการคุ้มครองสิทธิของเจ้าของข้อมูล ส่วนบุคคลว่าหน่วยงานภาครัฐจะให้ความคุ้มครองในระดับใด เพราะกฎหมายมีข้อยกเว้นสำหรับหน่วงานรัฐ ดังนั้น จำเป็นจะต้องกำหนดขอบเขตการใช้ข้อมูลและการเชื่อมโยงข้อมูลกับหน่วยงานอื่นอย่างชัดเจนภายใต้ หลักเรื่องธรรมาภิบาลภาครัฐตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ประกอบกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้ เกิดผลในทางปฏิบัติและให้หน่วยงานรัฐมีความตระหนักในสิทธิของเจ้าของข้อมูลส่วนบุคคล

2.3 ข้อจำกัดด้านเทคโนโลยีและการใช้ประโยชน์จากข้อมูล

การนำเทคโนโลยีการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) มาใช้จำเป็นต้องมีข้อมูลจำนวน มากที่มีความหลายหลายเพื่อนำมาใช้คาดการณ์สถานการณ์ของการกระทำความผิดในรูปแบบต่าง ๆ ของแต่ ละพื้นที่และช่วงเวลา การดำเนินงานด้านเฝ้าระวังติดตาม การออกตรวจตรา การสืบสวน การบริหารความ เสี่ยงในงานเฝ้าระวังติดตาม การใช้ข้อมูลจำนวนมากและหลายหลากดังกล่าว หน่วยงานภาครัฐมีความ จำเป็นต้องเชื่อมโยงข้อมูลกับข้อมูลของภาคเอกชนและประชาชน ตัวอย่างการเชื่อมโยงข้อมูลขนาดใหญ่ (Big Data) ในปัจจุบันที่มีการพัฒนาระบบการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างของหน่วยงานภาครัฐ และพัฒนาเป็นคลังข้อมูลขนาดใหญ่ ได้แก่ “โครงการพัฒนาเพิ่มคุณภาพการบริการด้านการแพทย์และ สาธารณสุขผ่านเทคโนโลยีดิจิทัล” ภายใต้ความร่วมมือขององค์กรภาคีเครือข่ายด้านสุขภาพและเทคโนโลยี สารสนเทศ โดยความร่วมมือของหน่วยงานภาครัฐ 12 แห่งประกอบด้วย กระทรวงกลาโหม กระทรวง ดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงสาธารณสุข กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและ นวัตกรรม กรุงเทพมหานคร ราชวิทยาลัยจุฬาภรณ์ สภากาชาดไทยมหาวิทยาลัยนวมินทราธิราช สำนักงานหลักประกันสุขภาพแห่งชาติ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สถาบันการแพทย์ ฉุกเฉินแห่งชาติและสำนักงานตำรวจแห่งชาติ ภายใต้ข้อตกลงร่วมกันพัฒนาการเชื่อมโยงแลกเปลี่ยนข้อมูล สุขภาพ (Health Information Exchange : HIE) จากระเบียนข้อมูลสุขภาพส่วนบุคคลอิเล็กทรอนิกส์ (Electronic Personal Health Record :PHR) ของแต่ละฝ่ายระหว่างกัน ทำให้เกิดประโยชน์ของการ

บูรณาการข้อมูลเพื่อสนับสนุนนโยบายด้านสาธารณสุขของประเทศ และในการเชื่อมโยงแลกเปลี่ยนข้อมูลสุขภาพนี้จะเกิดประโยชน์หลายด้าน เช่น ประชาชนที่มีสิทธิเข้ารับบริการด้านสุขภาพได้ทุกหน่วยบริการ การบริการแพทย์ทางไกล การบริการสุขภาพรูปแบบใหม่ที่จะเกิดขึ้นจากการพัฒนาเทคโนโลยีดิจิทัล เพื่อระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ และการดำเนินการในระบบหลักประกันสุขภาพ เป็นต้น [88] รวมทั้งนำร่องในการเชื่อมโยงข้อมูลด้านสุขภาพผ่าน ระบบ Health Link ซึ่งเป็นแพลตฟอร์มสำหรับเชื่อมโยงข้อมูลสุขภาพ เพื่อให้แพทย์สามารถเข้าดูข้อมูลสุขภาพของคนไข้จากโรงพยาบาลที่เข้าร่วมโครงการโดยคนไข้จะสามารถกำหนดสิทธิการเข้าถึงข้อมูลของตนเองได้ ก่อให้เกิดประโยชน์สำหรับประชาชนที่จะได้รับความสะดวกสบายและประหยัดเวลา ไม่ต้องเดินทางไปขอข้อมูลจากโรงพยาบาลเอง และในกรณีเกิดเหตุฉุกเฉิน แพทย์จะทำการรักษาและวินิจฉัยได้รวดเร็วขึ้น

จะเห็นได้ว่า การใช้ประโยชน์ของข้อมูลขนาดใหญ่ จำเป็นต้องได้รับความร่วมมือจากภาคเอกชน เนื่องจากปัญหาที่เกิดขึ้นคือ การใช้ข้อมูลขนาดใหญ่งานป้องกันอาชญากรรม มีความจำเป็นต้องใช้ข้อมูลจำนวนมาก และข้อมูลดังกล่าวอยู่ในความครอบครองของหน่วยงานอื่น ในส่วนข้อมูลที่อยู่กับภาคเอกชน หากจะนำมาเชื่อมโยงและใช้ประโยชน์ร่วมกันอาจมีข้อจำกัดด้านกฎหมาย เพราะปัจจุบันสามารถขอข้อมูลจากภาคเอกชนได้เฉพาะบางรายการที่มีเหตุตามที่มีกฎหมายให้อำนาจให้เรียกข้อมูลจากภาคเอกชนได้ เช่น การสืบสวน สอบสวน รวบรวมพยานหลักฐานและกระบวนการพิจารณาคดี ซึ่งเป็นการใช้ประโยชน์ในทางคดี แต่ลักษณะของการใช้ข้อมูลขนาดใหญ่ (Big Data) มาวิเคราะห์และคาดการณ์สถานการณ์การเกิดอาชญากรรม ปัจจัยการกระทำความผิด ความถี่ในการกระทำความผิด พื้นที่และสถานที่เสี่ยง จำเป็นต้องมีข้อมูลที่มีความหลากหลายและมีปริมาณมาก ซึ่งเป็นข้อมูลที่ไม่มีกฎหมายให้อำนาจในการเชื่อมโยงกับข้อมูลของภาคเอกชน ดังนั้น จึงจำเป็นต้องให้อำนาจแก่หน่วยงานของรัฐในการขอแบ่งปันข้อมูลจากภาคเอกชนและการใช้ข้อมูลร่วมกันและกำหนดหลักเกณฑ์ต่าง ๆ ขึ้นมาเพื่อให้เกิดผลในทางปฏิบัติ การนำเทคโนโลยีการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) มาใช้จำเป็นต้องมีข้อมูลจำนวนมากที่มีความหลายหลายเพื่อนำมาใช้คาดการณ์สถานการณ์ของการกระทำความผิดในรูปแบบต่าง ๆ ของแต่ละพื้นที่และช่วงเวลา การดำเนินงานด้านเฝ้าระวังติดตาม การออกตรวจตรา การสืบสวน การบริหารความเสี่ยงในงานเฝ้า

---

[88] Health Link แพลตฟอร์มเชื่อมข้อมูลสุขภาพ สู่ "Big Data" ด้านสาธารณสุข, กรุงเทพธุรกิจ , เข้าถึงเมื่อ 15 เมษายน 2565 , https://www.bangkokbiznews.com/social/994209.

ระวังติดตาม การใช้ข้อมูลจำนวนมากและหลายหลากดังกล่าว หน่วยงานภาครัฐมีความจำเป็นต้องเชื่อมโยงข้อมูลกับข้อมูลของภาคเอกชนและประชาชน และในส่วนของภาคเอกชนเองก็จำเป็นต้องขอเชื่อมโยงข้อมูลกับหน่วยงานรัฐในบางภารกิจที่เป็นประโยชน์สาธารณะ ดังนั้น จึงจำเป็นต้องให้อำนาจแก่หน่วยงานในการขอแบ่งปันข้อมูลจากภาคเอกชนและการใช้ข้อมูลร่วมกันและกำหนดหลักเกณฑ์ต่าง ๆ ขึ้นมาเพื่อให้เกิดผลในทางปฏิบัติ

สำหรับกรณีศึกษาของต่างประเทศพบว่า ตัวอย่างที่น่าสนใจเป็นการใช้เทคโนโลยีและ Big data เพื่อการป้องกันและปราบปรามอาชญากรรมคดีทางเพศในเด็ก โดยในปี ค.ศ. 2008 มูลนิธิเพื่อยุติการแสวงหาประโยชน์ทางเพศจากเด็กหรือ ECPAT International ได้ดำเนินการศึกษาเกี่ยวกับการปฏิบัติงานเพื่อการต่อต้านการละเมิดทางเพศออนไลน์ในเด็กของผู้บังคับใช้กฎหมายพบว่า ในการดำเนินงานด้านการป้องกันและปราบปรามอาชญากรรมคดีเกี่ยวกับทางเพศในเด็กไม่สามารถดำเนินการให้สำเร็จลุล่วงได้ด้วยการปฏิบัติงานของหน่วยงานเดียวหรือ ปราศจากความร่วมมือจากหน่วยงานที่เกี่ยวข้องต่างๆ จากทั้งภายในประเทศและต่างประเทศ ดังนั้น เจ้าหน้าที่ระดับปฏิบัติการด้านงานสืบสวนในประเทศต่างๆ จึงมีความร่วมมืออย่างเป็นพหุภาคีในการอำนวยงาน เพื่อการต่อต้านอาชญากรรมเกี่ยวกับเพศในเด็กข้ามเขตอำนาจการสืบสวน และการแบ่งปันข้อมูลระหว่างกันอย่างเป็นรูปธรรมผ่านกลไกการบูรณาการทำงานร่วมกันระหว่างหลายภาคส่วน อาทิเช่น ศูนย์คุ้มครองการแสวงหาผลประโยชน์ออนไลน์ในเด็กแห่งสหราชอาณาจักร (UK Child Exploitation and Online Protection Centre (CEOP) ร่วมกับหน่วยงานเครือข่าย ภาคเอกชน องค์กรที่ไม่ใช่หน่วยงานของรัฐบาล นักวิชาการ และผู้มีส่วนได้ส่วนเสียอื่นๆ[89] เป็นต้น โดยเจ้าหน้าที่ผู้ปฏิบัติงานสืบสวนมีการใช้เทคโนโลยีระบบแบ่งปันฐานข้อมูลขนาดใหญ่ (Big data) ซึ่งมีชื่อเรียกแตกต่างกันออกไปอย่างหลากหลาย ทั้งนี้เทคโนโลยีดังกล่าวมีคุณสมบัติเป็นทั้งเครื่องมือการสืบสวนอัจฉริยะและฐานข้อมูลขนาดใหญ่ที่สามารถจัดเก็บไฟล์ภาพนิ่งและภาพเคลื่อนไหวอันมีเนื้อหาละเมิดทางเพศเด็กเพื่อวัตถุประสงค์ในการสืบค้น แลกเปลี่ยน แบ่งปันข้อมูล และการติดตามดำเนินคดีกับผู้ต้องหาที่ล่วงละเมิดทางเพศในเด็กร่วมกันของเจ้าหน้าที่บังคับใช้กฎหมายจากหลายประเทศทั่วโลก รวมถึงจากสหราชอาณาจักร และประเทศสหรัฐอเมริกา ดังจะได้กล่าวถึงรายละเอียดต่อไปนี้

---

[89] Victoria Baines. (2008, November). Online Child Sexual Abuse: The Law Enforcement Response. Retrieved from ECPAT International: https://www.ecpat.org/wp-content/uploads/legacy/Thematic_Paper_ICTLAW_ENG.pdf

1) ซอฟต์แวร์ระบบคุ้มครองเด็ก (Child Protection System - CPS)

สหราชอาณาจักร ซึ่งรวมถึงประเทศอังกฤษ เป็นหนึ่งในประเทศที่ใช้ประโยชน์จากซอฟต์แวร์ระบบคุ้มครองเด็ก (Child Protection System - CPS) หรือซอฟต์แวร์ CPS[90] ซึ่งปัจจุบันมีหน่วยงานบังคับใช้กฎหมายทั้งหมดจาก 96 ประเทศ และอีก 50 รัฐ กำลังใช้ประโยชน์จากซอฟต์แวร์ CPS เป็นเครื่องมือทางเทคโนโลยีในการป้องกันและปราบปรามการละเมิดทางเพศเด็กอยู่ ซอฟต์แวร์นี้เป็นเทคโนโลยีที่ใช้ในการระบุตัวตนผู้กระทำความผิดฐานละเมิดทางเพศเด็กและมุ่งช่วยเหลือเด็กจากการตกเป็นเหยื่ออาชญากรรมทางเพศ โดยมีวัตถุประสงค์หลักเพื่อ ติดตาม จับกุมและดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับเพศในเด็ก โดยซอฟต์แวร์ CPS ผลิตและพัฒนาโดยบริษัท TLO แต่ต่อมาถายหลังได้บริจาคซอฟต์แวร์ดังกล่าวให้แก่องค์กรไม่แสงหาผลกำไรที่ชื่อว่า องค์กร Child Rescue Coalition หรือ CRC ที่ตั้งอยู่ในประเทศสหรัฐอเมริกา องค์กรฯ ดังกล่าวได้ดำเนินบริหารหารการใช้ประโยชน์จากซอฟต์แวร์ CPS มาจนถึงปัจจุบัน[91]และเปิดให้เจ้าหน้าที่สืบสวนจากหน่วยงานบังคับใช้กฎหมายทั่วโลกเข้ามาใช้งานซอฟต์แวร์โดยไม่คิดค่าใช้จ่าย ในปัจจุบันองค์กร CRC ได้ใช้ประโยชน์จากซอฟต์แวร์ดังกล่าวป้องกันเด็กจากการตกเป็นเหยื่ออาชญากรรมทางเพศได้แล้วกว่า 600,000 คน มากยิ่งกว่านั้นยังนำไปสู่การจับกุมผู้กระทำความผิดได้แล้วมากกว่า 12,900 คน ตลอดจนได้จัดอบรมการใช้ซอฟต์แวร์ CPS แก่เจ้าหน้าที่จากหน่วยงานบังคับใช้กฎหมายจากทั่วโลกไปแล้วกว่า 12,900 คน[92]

<u>การทำงานของเทคโนโลยี CPS</u>

ซอฟต์แวร์ CPS มีหลักการทำงานเป็นระบบเดียวกันสำหรับผู้ใช้ทั่วโลก ในการใช้เทคโนโลยี (the use of technology) อัจฉริยะโดยมีซอฟต์แวร์ CPS เป็นเครื่องมือในการป้องกันและปราบปรามอาชญากรรมทางเพศในเด็กนั้น ซอฟต์แวร์ดังกล่าวมีการทำงานที่สามารถสั่งเก็บภาพหรือข้อมูลที่มีเนื้อหาหรือ

---

[90] Olivia Solon. (July, 2020 17). Inside the surveillance software tracking child porn offenders across the globe. Retrieved from NBC News: https://www.nbcnews.com/tech/internet/inside-surveillance-software-tracking-child-porn-offenders-across-globe-n1234019

[91] Claudia Peersman;Christian Schulze;Awais Rashid; Margaret Brennan;Carl Fischer. (2016, September). iCOP: Live forensics to reveal previously unknown criminal media on P2P networks. Retrieved from sciencedirect: https://www.sciencedirect.com/science/article/pii/S1742287616300779

[92] Child Rescue Coalition. (2020). Child Rescue Coalition Annual Report 2020. Retrieved from Child Rescue Coalition: https://childrescuecoalition.org/child-rescue-coalition-annual-report-2020.html

แสดงเกี่ยวกับกิจกรรมของผู้มีพฤติกรรมฝักใฝ่ทางเพศหรือล่วงละเมิดทางเพศในเด็ก และซอฟต์แวร์ CPS ยังสามารถระบุตัวตนของผู้ใช้งานอินเตอร์เน็ตแบบเชื่อมต่อข้ามโครงข่ายโดยตรงระหว่างเครื่องคอมพิวเตอร์ หรือ Peer to peer (P2P) ที่มีพฤติกรรมดาวน์โหลดเนื้อหาหรือรูปภาพที่ล่วงละเมิดทางเพศในเด็กได้ อย่างไรก็ตามการทำงานของซอฟต์แวร์ CPS นั้นยังมีข้อจำกัดในด้านการตรวจจับหรือระบุเนื้อหาหรือรูปภาพเกี่ยวกับการละเมิดทางเพศในเด็กใหม่ๆ ที่ถูกอัพโหลดเข้ามาในโครงข่ายอินเตอร์เน็ตอย่างเป็นปัจจุบัน กล่าวคือ ซอฟต์แวร์ CPS ที่อาศัยการทำงานแบบคำนวณหาค่าแฮช (hash value) หรืออัตลักษณ์หรือเอกลักษณ์ของข้อมูลโดยการจับคู่เนื้อหาบนแฟ้มเอกสารหรือภาพที่ส่งต่อกันบนโลกอินเตอร์เน็ตซึ่งข้อมูลของแต่ละภาพจะประกอบด้วยอัตลักษณ์อันแสดงถึงเนื้อหาที่มีการละเมิดทางเพศในเด็ก (CSA media) นั้น ซอฟต์แวร์ CPS ไม่สามารถแสดงผลการจับคู่เนื้อหาใหม่เกี่ยวกับการละเมิดทางเพศในเด็กที่เพิ่งถูกอัพโหลดลงบนระบบฐานข้อมูลอินเตอร์เน็ตอย่างทันต่อสถานการณ์ได้ แต่กลับเรียกข้อมูลที่ถูกเก็บไว้อยู่ในระบบอยู่แล้วนับหลายเดือนและหลายปีมาคำนวณจับคู่หาค่าอัตลักษณ์ของเนื้อหาแทนจึงส่งผลให้ผลลัพธ์ของการประมวลผลการจับคู่ของซอฟต์แวร์ CPS ไม่ทันต่อความเปลี่ยนแปลงอย่างรวดเร็วของพฤติกรรมผู้กระทำความผิดละเมิดทางเพศในเด็กบนโลกอินเตอร์เน็ต รวมถึงไม่สามารถตรวจจับหรือระบุภาพเนื้อหาละเมิดทางเพศในเด็กที่ไม่ได้บันทึกไว้ และถูกแก้ไขข้อมูล หรือฝังข้อมูลลงบนภาพปกติหรือวิดีโอปกติอื่นๆ ได้[93] อนึ่ง CPS ซอฟต์แวร์จะตรวจจับแค่ข้อมูลสาธารณะที่ส่งต่อกันบนโลกอินเตอร์เน็ต รวมถึงจะตรวจจับ IP address ประจำอุปกรณ์อิเล็กทรอนิกส์ของผู้ใช้งานอินเตอร์เน็ตที่มีส่วนเกี่ยวข้องกับเนื้อหาการแสวงหาผลประโยชน์ทางเพศในเด็ก จากนั้นเจ้าหน้าที่ผู้บังคับใช้กฎหมายจะขอหมายศาล ให้ผู้ให้บริการเครือข่ายอินเตอร์เน็ตแจ้งหมายเลข IP address ที่ชัดเจนเพื่อระบุตัวตนของผู้ใช้งานอินเตอร์เน็ตที่มีพฤติกรรมละเมิดทางเพศในเด็กและดำเนินการออกหมายค้นแก่ผู้ต้องหาต่อไป[94]

2) ระบบฐานข้อมูลการแสวงหาผลประโยชน์ทางเพศในเด็กระดับสากล (International Child Sexual Exploitation - ICSE) Database

---

[93] Claudia Peersman;Christian Schulze;Awais Rashid; Margaret Brennan;Carl Fischer. (2016, September). iCOP: Live forensics to reveal previously unknown criminal media on P2P networks. Retrieved from sciencedirect: https://www.sciencedirect.com/science/article/pii/S1742287616300779

[94] WALLIS, J. (2015, November 20). Justin FRAZIER, Appellant, v. STATE of Florida, Appellee. Case law, No. 5D14–171. Retrieved from Thomson Reuters: https://caselaw.findlaw.com/fl-district-court-of-appeal/1718791.html

แหล่งฐานข้อมูลที่ใช้แบ่งปันร่วมกันระหว่างเจ้าหน้าที่ผู้บังคับใช้กฎหมายทั่วโลกเพื่อป้องกันและปราบปรามอาชญากรรมทางเพศในเด็กที่สำคัญนั้นมีอยู่ด้วยกัน 3 แหล่งซึ่งแต่ละแหล่งข้อมูลมีผู้ดูแลฐานข้อมูลแตกต่างกันออกไป โดยผู้ดูแลแหล่งฐานข้อมูลที่สำคัญหลักมีจำนวน 3 หน่วยงาน ดังนี้ 1) ฐานข้อมูลของมูลนิธิเฝ้าระวังทางอินเตอร์เน็ต (Internet Watch Foundation-IWF) ตั้งอยู่ในสหราชอาณาจักร โดยระบบฐานข้อมูลของมูลนิธินี้มีเทคโนโลยีที่ทำหน้าที่เป็นเครื่องมืออัจฉริยะตรวจจับเว็บไซต์ที่มีเนื้อหาละเมิดทางเพศในเด็ก เพื่อปิดเว็บไซต์ที่แสดงเนื้อหาดังกล่าวลง 2) ฐานข้อมูลของศูนย์เพื่อเด็กหายและถูกฉวยผลประโยชน์แห่งชาติ (National Center for Missing and Exploited Children-NCMEC) แห่งประเทศสหรัฐอเมริกาและ 3) ฐานข้อมูลการแสวงหาผลประโยชน์ทางเพศในเด็กระหว่างประเทศ International Child Sexual Exploitation (ICSE) database ดำเนินการจัดการโดยองค์การตำรวจอาชญากรรมระหว่างประเทศ (Interpol)[95]

อนึ่ง ในที่นี่จะกล่าวถึงระบบฐานข้อมูลการแสวงหาผลประโยชน์ทางเพศในเด็กระดับสากล (International Child Sexual Exploitation - ICSE) Database หรือ ICSE database เป็นสำคัญ ระบบฐานข้อมูล ICSE ดำเนินการโดยองค์การตำรวจอาชญากรรมระหว่างประเทศ หรือ Interpol ได้รับการสนับสนุนโดยกลุ่มประเทศ G8 และกองทุนความมั่นคงภายในแห่งสหภาพยุโรป (the Internal Security Fund of the European Union)[96] ฐานข้อมูล ICSE นี้มีการเก็บรวบรวมและบันทึกภาพนิ่งและภาพเคลื่อนไหวไว้เป็นฐานข้อมูล ซึ่งถือเป็นเครื่องมือสืบสวนอัจฉริยะที่อำนวยให้เจ้าหน้าที่ด้านงานสืบสวนจากทั่วโลกได้แบ่งปันข้อมูลระหว่างกันเกี่ยวกับคดีละเมิดทางเพศในเด็ก ปัจจุบันมีเจ้าหน้าที่ผู้ปฏิบัติงานด้านงานสืบสวนจากกว่า 64 ประเทศทั่วโลกแบ่งปันแลกเปลี่ยนข้อมูลร่วมกันเพื่อลดความซ้ำซ้อนในการทำคดีที่มี

---

[95] May-Chahal, Corinne, Kelly, Emma. (2020). Online Child Sexual Victimisation. Retrieved from Bristol University Press: https://books.google.co.th/books?id=UGXXDwAAQBAJ&pg=PA94&lpg=PA94&dq=International+Child+Sexual+Exploitation+-+ICSE+USA+america&source=bl&ots=4JH_IT-E8h&sig=ACfU3U12dqCZ5d70O_ltgEL1Svlj7u0cmQ&hl=en&sa=X&ved=2ahUKEwj2h_2wyb70AhWESGwGHZ6ZA5EQ6AF6BAgMEAM#v=o

[96] INTERPOL and ECPAT International. (2018, February). Technical report: Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material. Retrieved from Interpol: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

ผู้เสียหายเป็นคนเดียวกัน และระบุสถานที่ ของเหยื่อเพื่อช่วยเหลือเหยื่อผู้เสียหายจากการละเมิดทางเพศในเด็ก[97] นอกจากนี้ประเทศสหรัฐอเมริกาเป็นหนึ่งใน 49 ประเทศที่มีการเชื่อมต่อฐานข้อมูลเกี่ยวกับการละเมิดทางเพศในเด็กร่วมกับฐานข้อมูล ICSE database ของ Interpol[98]

การทำงานของเทคโนโลยี ICSE Database[99]

ICSE Database เป็นเครื่องมือจำเพาะที่ให้ความสำคัญกับเหยื่อเป็นศูนย์กลาง เครื่องมือนี้ถูกออกแบบมาเพื่อช่วยอำนวยงานสืบสวนสำหรับสำหรับเจ้าหน้าที่บังคับใช้กฎหมาย โดยมีเพื่อวัตถุประสงค์หลักสำคัญ 3 ข้อ คือ 1) เพื่อลดความพยายามในการดำเนินงานที่ซ้ำซ้อนของเจ้าหน้าที่ในการระบุตัวเหยื่อผู้เสียหาย 2) เพื่อระบุตัวผู้กระทำความผิด และ 3) เพื่อระบุตัวเด็กที่เป็นผู้เสียหายจากการละเมิดทางเพศ โดยใช้เทคโนโลยีตรวจจับสื่อที่มีเนื้อหาการละเมิดทางเพศในเด็ก child sexual abuse material (CSAM) และสื่อที่มีเนื้อหาแสวงหาผลประโยชน์ทางเพศในเด็ก child sexual exploitation material (CSEM) ทั้งที่อยู่ในรูปแบบของภาพนิ่ง ภาพเคลื่อนไหว และข้อมูลอัตลักษณ์หรือเอกลักษณ์ต่างๆ หลักการทำงานของเครื่องมือจำเพาะชนิดนี้จะอาศัยการตรวจจับหาเนื้อหาที่มีข้อมูลอัตลักษณ์ต่างๆ ที่ถูกโพสบนอินเตอร์เน็ตโดยการเปรียบเทียบหาความเหมือนกับข้อมูลเอกลักษณ์ต่างๆ ที่ถูกตรวจยึด ได้หรือบันทึกไว้บนฐานข้อมูล ICSE โดยเจ้าหน้าที่บังคับใช้กฎหมายจากทั่วโลก ทั้งนี้ สำนักงานกลางแห่งชาติแห่งองค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL National Central Bureaus) จะเป็นผู้ทำหน้าที่ควบคุมหลักในการอนุญาตการเข้าถึงหรือการเข้าใช้ฐานข้อมูล ICSE ของผู้ใช้ (User) จากแต่ละชาติ ในฐานข้อมูล ICSE จะไม่มีการจำกัดควบคุมการเข้าถึงเนื้อหาที่ผิดกฎหมาย แต่จะแสดงเนื้อหาที่เกี่ยวข้องทั้งหมดที่ได้ถูกบันทึกไว้อยู่ในฐานข้อมูล

---

[97] Interpol. (2017, January). Interpol network identifies 10,000 child sexual abuse victims. Retrieved from Interpol: https://www.interpol.int/en/News-and-Events/News/2017/INTERPOL-network-identifies-10-000-child-sexual-abuse-victims

[98] Interpol. (2021, November 30). International Child Sexual Exploitation database. Retrieved from Interpol: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

[99] Interpol and ECPAT International. (2018, February). Technical report: Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material. Retrieved from Interpol: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

ซึ่งอาจเป็นเบาะแสไปสู่การระบุตัวตนของผู้กระทำความผิดและของเหยื่อผู้เสียหายเพื่อวัตถุประสงค์ด้านการเข้าให้ความช่วยเหลือเหยื่อและจับกุมผู้กระทำความผิดต่อไป

ด้วยฐานข้อมูล ICSE เป็นระบบที่เปิดให้สมาชิกผู้ใช้สามารถแบ่งปันหรืออัพโหลดข้อมูลการละเมิดทางเพศในเด็กลงบนฐานข้อมูลร่วมกันได้จากทั่วโลก เพื่อให้เกิดประสิทธิภาพในการแบ่งปันข้อมูลบนระบบฐานข้อมูล ICSE จึงมีการกำหนดให้ผู้ดูแลระบบของสำนักเลขาธิการแห่งองค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL’s General Secretariat) เป็นผู้ทำหน้าที่ความคุมกลั่นกรองคุณภาพของข้อมูลที่ถูกอัพโหลดลงไปในฐานข้อมูลดังกล่าวให้มีการจัดลำดับความสำคัญของข้อมูลที่เหมาะสมและเข้าเกณฑ์ความหมายการละเมิดทางเพศในเด็กตามนิยาม (Definition) ที่ได้บัญญัติไว้ในมาตราที่ 20 (2) แห่งอนุสัญญาการคุ้มครองเด็กเพื่อการต่อต้านการแสวงหาผลประโยชน์ทางเพศและการละเมิดทางเพศแห่งสภาสหภาพยุโรป ค.ศ. 2007 (the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) ที่มีใจความสำคัญว่าเนื้อหาที่เป็นการละเมิดทางเพศในเด็กคือเนื้อหาที่แสดงให้เห็นภาพทั้งภาพจริงหรือภาพเสมือนจริง รวมถึงอวัยวะทางเพศเพื่อวัตถุประสงค์ทางเพศของเด็กที่อายุต่ำกว่า 18 ปี ทั้งนี้หากมีผู้ใช้จากประเทศสมาชิกใดได้ทำการอัพโหลดรูปภาพหรือวิดีโอที่ซ้ำกันกับข้อมูลที่ถูกบันทึกไว้ในฐานข้อมูล ระบบจะแจ้งว่าผู้เสียหายหรือผู้กระทำความผิดที่เกี่ยวข้องกับภาพหรือวิดีโอนั้นถูก “ระบุตัวตนแล้ว” ในการนี้ Interpol ต้องอาศัยความร่วมมือของเจ้าหน้าที่เจ้าของคดีในการป้อนข้อมูลเกี่ยวกับสถานะของแต่ละเคสให้เป็นปัจจุบันในระบบฐานข้อมูล ICSE อนึ่งตามสถิติข้อมูลในเดือนสิงหาคมปี ค.ศ. 2017 มีภาพนิ่งและภาพเคลื่อนไหวที่ไม่ซ้ำกันอยู่ในระบบฐานข้อมูลของ ICSE กว่า 1 ล้านไฟล์

2.4 ข้อจำกัดด้านการจัดเก็บและการเชื่อมโยงข้อมูล

ปัญหาที่พบคือปัญหาการเข้าถึงข้อมูลเพื่อให้ทราบข้อเท็จจริงและการกระทำความผิดและความไม่สมบูรณ์ครบถ้วนของข้อมูลและปัญหาโครงสร้างของข้อมูล ว่าจะทำยังไงให้สามารถนำข้อมูลหรือเบาะแสที่ได้รับมาขยายผลเพื่อนำไปสู่การพิสูจน์การกระทำความผิด รวมทั้งการแจ้งเตือนการกระทำความผิดได้ เนื่องจากระบบการจัดเก็บข้อมูลอาชญากรรมการเงินของประเทศไทย เป็นการจัดเก็บข้อมูลโดยหน่วยงานในกระบวนการยุติธรรมที่มีลักษณะต่างคนต่างเก็บรวบรวมข้อมูลสถิติต่าง ๆ ที่ผ่านเข้าออกตามขั้นตอนของกระบวนงานในส่วนของตนเอง ตัวอย่างสถิติที่เป็นทางการได้แก่ สถิติอาชญากรรมของตำรวจ

สถิติคดีที่เข้าสู่การพิจารณาของศาลชั้นต้น สถิติผู้ต้องขังที่ราชทัณฑ์ดูแล สถิติคดีที่เกี่ยวข้องกับการที่ผู้กระทำความผิดเป็นการจัดเก็บข้อมูลตามภารกิจตามกฎหมายที่ให้อำนาจของแต่ละหน่วยงานจัดเก็บและเป็นการจัดเก็บตามความต้องการใช้ข้อมูลของหน่วยงานนั้น ขาดมาตรฐานกลางในการจัดเก็บรายละเอียดของข้อมูล นอกจากนั้น ยังพบปัญหาการเชื่อมโยงข้อมูลข้อมูลขนาดใหญ่ (Big Data) ชองแต่ละหน่วยงาน เพราะการอนุญาตให้ใช้หรือเชื่อมโยงข้อมูลจะเป็นอำนาจของแต่ละหน่วยงานผ่านรูปแบบข้อตกลงหรือบันทึกความตกลงร่วมกันระหว่างหน่วยงาน พิจารณาตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 16 บัญญัติว่า *“ภายใต้บทบัญญัติแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่หน่วยงานของรัฐได้มาซึ่งข้อมูลส่วนบุคคลหรือมีข้อมูลส่วนบุคคลอยู่ในความครอบครอง หากหน่วยงานของรัฐประสงค์จะใช้ข้อมูลส่วนบุคคลดังกล่าวในรูปแบบข้อมูลดิจิทัลเพื่อประโยชน์ในการบริหารราชการแผ่นดิน หน่วยงานของรัฐนั้นสามารถขอเชื่อมโยงและแลกเปลี่ยนข้อมูลส่วนบุคคลนั้นจากหน่วยงานของรัฐที่ครอบครองเพื่อนำมาวิเคราะห์หรือประมวลผลได้”* ซึ่งตามหนังสือตอบข้อหารือของสำนักงานปลัดนายกรัฐมนตรี เมื่อวันที่ 8 พฤษภาคม 2563 ได้ให้ข้อสังเกตว่าในกรณีที่เป็นข้อมูลข่าสารส่วนบุคคลไว้ 3 ประการคือ

1) การพิจารณาให้หน่วยงานของรัฐแห่งใดเชื่อมโยงข้อมูลที่เป็นข้อมูลข่าวสารส่วนบุคคลภายใต้บังคับพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 หน่วยงานที่ครอบครองหรือควบคุมดูแลข้อมูลข่าวสารส่วนบุคคลต้องพิจารณาว่าหน่วยงานที่จะขอเชื่อมโยงมีอำนาจหน้าที่ตามกฎหมายที่สามารถเข้าถึงหรือใช้ประโยชน์จากข้อมูลส่วนบุคคลได้หรือไม่และมีความจำเป็นอย่างต่อเนื่องที่จะ ต้องเข้าถึงข้อมูลข่าวสารส่วนบุคคลโดยผ่านระบบเครือข่ายคอมพิวเตอร์หรือไม่ หรือมีทางเลือกอื่นที่เหมาะสมกว่า

2) การเชื่อมโยงข้อมูลในระบบคอมพิวเตอร์ระหว่างหน่วยงานที่ครอบครองหรือควบคุมดูแลข้อมูลข่าวสารส่วนบุคคลกับหน่วยงานที่ขอเชื่อมโยงระบบคอมพิวเตอร์เพื่อประโยชน์ในการเข้าถึง ข้อมูลข่าวสารส่วนบุคคล ควรต้องดำเนินการภายใต้ข้อตกลงระหว่างหน่วยงาน ซึ่งจะต้องมีข้อกำหนดเกี่ยวกับวัตถุประสงค์ของการอนุญาตให้มีการเข้าถึงข้อมูลข่าวสารส่วนบุคคล ขอบเขตและข้อจำกัดในการเข้าถึงข้อมูล มาตรฐานในการรักษาความปลอดภัยของข้อมูล รวมทั้งรูปแบบของรายงานการใช้หรือเข้าถึงข้อมูลข่าวสารส่วนบุคคลดังกล่าวด้วย

3) ในกรณีที่จะอนุญาตให้มีการเชื่องโยงข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูแลให้กับหน่วยงานรัฐแห่งอื่นเพื่อประโยชน์ในการบริหารราชการแผ่นดิน ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 หน่วยงานที่ครอบครองหรือควบคุมดูแล

ข้อมูลข่าวสารส่วนบุคคลควรดำเนินการเชื่อมโยงข้อมูลข่าวสารส่วนบุคคลดังกล่าวผ่านระบบ สารสนเทศเชื่อมต่อฐานข้อมูลประชาชน (Linkage Center) ของกรมการปกครองและหน่วยงานของรัฐที่ประสงค์จะใช้ข้อมูลดังกล่าวจะต้องมีการจัดทำข้อตกลงเกี่ยวกับการใช้ข้อมูลข่าวสารส่วนบุคคลกับหน่วยงานของรัฐที่เป็นเจ้าของข้อมูลและต้องแจ้งข้อตกลงเกี่ยวกับการใช้ข้อมูลข่าวสารส่วนบุคคลกับหน่วยงานที่เป็นเจ้าของข้อมูลและต้องแจ้งข้อตกลงเกี่ยวกับการใช้ข้อมูลข่าวสารส่วนบุคคลดังกล่าวให้กรมการปกครองซึ่งเป็นหน่วยงานที่ดูแลระบบรับทราบเพื่อดำเนินการในส่วนที่เกี่ยวข้องต่อไป

จากประเด็นหารือข้างต้น กล่าวได้ว่า หากข้อมูลขนาดใหญ่ (Big data) ไม่ใช่ข้อมูลส่วนบุคคลตามความหมายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การเชื่อมโยงสามารถกระทำได้ผ่านระบบฐานข้อมูลหน่วยงานภาครัฐตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 แต่หากเป็นกรณีการใช้ข้อมูลและเชื่อมโยงข้อมูลที่เป็นข้อมูลส่วนบุคคล จำเป็นต้องควรต้องดำเนินการภายใต้ข้อตกลงระหว่างหน่วยงาน ซึ่งจะต้องมีข้อกำหนดเกี่ยวกับวัตถุประสงค์ของการอนุญาตให้มีการเข้าถึงข้อมูลข่าวสารส่วนบุคคล ขอบเขตและข้อจำกัดในการเข้าถึงข้อมูล มาตรฐานในการรักษาความปลอดภัยของข้อมูล รวมทั้งรูปแบบของรายงานการใช้หรือเข้าถึงข้อมูลข่าวสารส่วนบุคคลดังกล่าวด้วย และหน่วยงานที่ร้องขอและหน่วยงานเจ้าของข้อมูลต้องดำเนินการภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กล่าวคือ ต้องพิจารณาตามกิจกรรมที่ดำเนินการว่าเป็นกิจกรรมที่ได้รับการยกเว้นมิให้ต้องอยู่ในบังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ หากได้รับยกเว้นก็สามารถดำเนินการได้โดยไม่ต้องปฏิบัติตามหลักเกณฑ์การประมวลข้อมูลส่วนบุคคลตามกฎหมาย แต่ต้องมีมาตรการรักษาความปลอดภัยของข้อมูลที่เหมาะสม หากเป็นกิจกรรมที่ไม่เข้าข้อยกเว้นตามกฎหมาย หน่วยงานที่เกี่ยวข้องต้องดำเนินการแจ้งความเป็นส่วนตัว (Privacy Notice) ให้เจ้าของข้อมูลส่วนบุคคลทราบ โดยระบุวัตถุประสงค์ รวมทั้งกำหนดให้มีกระบวนการในการร้องรับสิทธิของเจ้าของข้อมูลตามกฎหมาย ดังนั้น หากต้องการลดข้อจำกัดด้านกฎหมายเกี่ยวกับการเชื่อมโยงฐานข้อมูลที่การทำบันทึกความตกลงหรือข้อตกลงความร่วมมือ (Memorandum of Understanding : MOU) เป็นเพียงหนังสือที่ฝ่ายหนึ่งแสดงความสมัครใจจะปฏิบัติอย่างหนึ่งอย่างใดตามเงื่อนไขที่ปรากฏในหนังสือกับอีกฝ่ายหนึ่ง โดยที่หนังสือนี้ไม่ถือว่าเป็นสัญญาผูกมัดและมีผลบังคับในทางกฎหมาย แต่แสดงถึงความต้องการของผู้ที่ลงนามว่าจะปฏิบัติดังที่ได้ระบุไว้เท่านั้น โดยกำหนดเป็นกรอบความร่วมมือด้านต่าง ๆ เช่น ความร่วมมือด้านวิชาการ การถ่ายทอดและแลกเปลี่ยนองค์ความรู้ การเชื่อมโยงข้อมูลทางระบบสารสนเทศ การสร้างเครือข่าย หรือความร่วมมือด้าน

อื่นๆ ซึ่งไม่มีความยั่งยืนและสามารถเปลี่ยนแปลงได้ตามนโยบายของผู้บริหารหน่วยงาน จึงควรต้องกำหนดหลักเกณฑ์ที่ชัดเจนไว้ในกฎหมายแม่บท เพื่อให้หน่วยงานของรัฐยึดถือเป็นแนวปฏิบัติ

3. ข้อเสนอแนะแนวทางและมาตรการด้านกฎหมายเพื่อรองรับการนำข้อมูลขนาดใหญ่มาใช้ประโยชน์ในการป้องกันและปราบปรามอาชญากรรมของภาครัฐ

ข้อมูลขนาดใหญ่หรือ Big Data มีประโยชน์ต่อใช้เป็นเครื่องมือในการป้องกันและปราบปรามอาชญากรรมหลายประการ ทั้งในด้านการสืบสวนและการสอบสวนในการแสวงหาข้อเท็จจริงและพยานหลักฐานต่าง ๆ ในคดี และมีประโยชน์ต่อการคาดการณ์เหตุการณ์การกระทำความผิดล่วงหน้า ซึ่งภาครัฐสามารถนำข้อมูล Big Data มาวิเคราะห์แนวโน้มและความถี่ของการเกิดอาชญากรรมในแต่ละพื้นที่ในแต่ละช่วงเวลา ตลอดจนวิเคราะห์กลุ่มเป้าหมายของอาชญากรรม ทำให้สามารถกำหนดแนวทางและวางมาตรการเชิงป้องกันการเกิดอาชญากรรมได้ สอดคล้องกับในปัจจุบันประเทศไทยมุ่งสู่ความเป็นรัฐบาลอิเล็กทรอนิกส์ (e-Government) โดยปรับรูปแบบการวิธีการในการบริหารจัดการภาครัฐสมัยใหม่ โดยการนำเอาเทคโนโลยีสารสนเทศและระบบเครือข่ายสื่อสาร เพื่อเป็นการเพิ่มประสิทธิภาพการดำเนินการของภาครัฐ รวมทั้งปรับปรุงการให้บริการแก่ประชาชน บริการงานทางด้านข้อมูลและสารสนเทศ เพื่อส่งเสริมการพัฒนาเศรษฐกิจและสังคม ทำให้ประชาชนได้รับบริการจากภาครัฐที่ดีขึ้น และมีนโยบายในการส่งเสริมการเชื่อมโยงแลกเปลี่ยนข้อมูลและการปฏิบัติการร่วมทางอิเล็กทรอนิกส์ หรือกระบวนงานระบบสารสนเทศระหว่างระบบสารสนเทศของหน่วยงานภาครัฐ เพื่ออำนวยความสะดวกในการให้บริการประชาชนและสนับสนุนการดำเนินงานของหน่วยงานภาครัฐ

ดังนั้น ผู้วิจัยจึงได้เสนอแนวทางแก้ไขเพิ่มเติมพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 โดยกำหนดเพิ่มส่วนที่เกี่ยวกับการบริหารจัดการข้อมูลเพื่อป้องกันและปราบปรามอาชญากรรม เพื่อเป็นกรอบในการกำกับดูแลข้อมูลภาครัฐ (Government Data Governance) ที่ใช้ในภารกิจด้านการป้องกันและปราบปรามอาชญากรรม เพื่อส่งเสริมให้หน่วยงานที่เกี่ยวข้องสามารถกำกับดูแลข้อมูลให้มีความถูกต้อง ตรงกัน สมบูรณ์และทันสมัย รวมทั้งอยู่ในสภาพที่พร้อมใช้งาน โดยมีการกำกับดูแลความปลอดภัยของข้อมูลให้ได้มาตรฐานตามชั้นความลับ เพื่อให้การใช้ประโยชน์และการบริการข้อมูลเกิดขึ้นได้อย่างเป็นรูปธรรม โดยมีสาระสำคัญ ดังนี้

1) กำหนดให้การเชื่อมโยงข้อมูลระหว่างหน่วยงานภาครัฐในภารกิจด้านการป้องกันและปราบปรามอาชญากรรมสามารถดำเนินการได้ตามพระราชบัญญัตินี้ โดยให้หน่วยงานที่ต้องการเชื่อมโยงเพื่อใช้ประโยชน์จากข้อมูลแจ้งความจำนงยังหน่วยงานเจ้าของข้อมูล โดยแจ้งรายละเอียดเกี่ยวกับอำนาจหน้าที่ในการใช้ข้อมูล วัตถุประสงค์ของการใช้ข้อมูล การอนุญาตให้มีการเข้าถึงข้อมูลข่าวสารส่วนบุคคล ขอบเขตและข้อจำกัดในการเข้าถึงข้อมูล มาตรฐานในการรักษาความปลอดภัยของข้อมูล และในส่วนที่เป็นข้อมูลส่วนบุคคลกำหนดให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

2) กำหนดหลักเกณฑ์การจัดทำบัญชีรายการข้อมูล (Data Catalog) ของหน่วยงานที่มีภารกิจด้านการป้องกันและปราบรามอาชญากรรม ได้แก่ สำนักงานตำรวจแห่งชาติ สำนักงานอัยการสูงสุด กรมสอบสวนคดีพิเศษ สำนักงานศาลยุติธรรม กรมราชทัณฑ์ กรมคุมประพฤติ กรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อสนับสนุนให้หน่วยงานภาครัฐที่เป็นเจ้าของข้อมูลจัดทำบัญชีข้อมูลสำคัญภายในหน่วยงานในรูปแบบที่เป็นมาตรฐานเดียวกัน ช่วยให้ผู้ใช้ประโยชน์ข้อมูลสามารถสืบค้น ร้องขอ เข้าถึง ทราบแหล่งที่มา ชั้นความลับ ประเภท รูปแบบและสามารถใช้ประโยชน์ของข้อมูลภาครัฐทั้งหมดได้ ซึ่งเป็นจุดเริ่มต้นสำคัญในการพัฒนาการใช้ประโยชน์ข้อมูลภาครัฐให้มีประสิทธิผล สามารถบูรณาการให้บริการและใช้ประโยชน์ข้อมูลข้ามหน่วยงานได้อย่างเป็นระบบ

3) กำหนดให้หน่วยงานเจ้าของข้อมูลจัดให้มีระบบบริการและแลกเปลี่ยนข้อมูลกลางเชื่อมต่อกับฐานข้อมูลภาครัฐ เพื่อกำกับดูแลชั้นความลับข้อมูล กระบวนการขอใช้สิทธิการเข้าถึงข้อมูล กลไกและระบบสารสนเทศที่สามารถตรวจสอบได้และเพื่อให้สามารถสรุปผลเชิงสถิติเรื่องการร้องขอใช้ข้อมูลของทั้งหน่วยงานภายในและภายนอก

4) กำหนดภารกิจของหน่วยงานในกระบวนการยุติธรรมในการวิเคราะห์และเผยแพร่ข้อมูลแนวโน้มอาชญากรรมอย่างเป็นระบบ เพื่อประโยชน์ในการกำหนดนโยบายทางอาญาทั้งการเพิ่มประสิทธิภาพบังคับใช้กฎหมาย การป้องกันปราบปรามอาชญากรรม และการแก้ไขพฤตินิสัยของผู้กระทำความผิด

5) กำหนดให้หน่วยงานภาครัฐสามารถเข้าถึงข้อมูลที่อยู่ในความครอบครองของภาคเอกชนเพื่อนำข้อมูลไปใช้ในการวิเคราะห์และประมวลผลและใช้ประโยนช์ในการป้องกันและปราบปรามอาชญากรรมได้ โดยต้องกำหนดรูปแบบการเข้าถึงและเชื่อมโยงข้อมูลที่ชัดเจน อาทิ เงื่อนไข ข้อกำหนดวิธีการเข้าถึง ช่องทางการในเข้าถึงและรับส่งข้อมูล ช่องทางการประสานงาน เป็นต้น

6) กำหนดกระบวนการในการปรับปรุงข้อมูลให้ทันสมัยอยู่เสมอ

ร่างการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล (ฉบับที่ ..) พ.ศ. ....

พระราชบัญญัติ
การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล (ฉบับที่ ...)
พ.ศ. ....

.....

.....

.....

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล

มาตรา 1 พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล (ฉบับที่ ..) พ.ศ. ... ”

มาตรา 2 พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา 3 ให้เพิ่มความต่อไปนี้เป็น หมวด 1 การบริหารจัดการข้อมูลขนาดใหญ่เพื่อป้องกันและปราบปรามอาชญากรรม มาตรา 18/1 ถึงมาตรา 18/7 แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

“หมวด 1
การบริหารจัดการข้อมูลเพื่อป้องกันและปราบปรามอาชญากรรม

มาตรา 18/1 ในหมวดนี้

“หน่วยงานที่มีภารกิจด้านการป้องกันและปราบปรามอาชญากรรม” หมายความว่า สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม กรมราชทัณฑ์ กรมคุมประพฤติ กรมพินิจและคุ้มครองเด็กและเยาวชน และหน่วยงานของรัฐอื่นที่เกี่ยวข้อง

“หน่วยงานผู้ร้องขอ” หมายความว่า หน่วยงานที่มีภารกิจด้านการป้องกันและปราบปรามอาชญากรรมที่ร้องขอเชื่อมโยงหรือแลกเปลี่ยนข้อมูล

“หน่วยงานเจ้าของข้อมูล” หมายความว่า หน่วยงานที่มีภารกิจด้านการป้องกันและปราบปรามอาชญากรรมที่ได้มาซึ่งข้อมูลส่วนบุคคลหรือมีข้อมูลส่วนบุคคลอยู่ในความครอบครอง

มาตรา 18/2 เพื่อเป็นหลักประกันและคุ้มครองสิทธิของประชาชน หน่วยงานที่มีภารกิจด้านการป้องกันและปราบปรามอาชญากรรมจะต้องดำเนินการตามกรอบธรรมาภิบาลข้อมูลภาครัฐอย่างเคร่งครัด

มาตรา 18/3 การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานที่มีภารกิจด้านการป้องกันและปราบปรามอาชญากรรมสามารถดำเนินการได้ตามพระราชบัญญัตินี้ โดยให้หน่วยงานผู้ร้องขอแจ้งความจำนงยังหน่วยงานเจ้าของข้อมูล โดยแจ้งรายละเอียดเกี่ยวกับอำนาจหน้าที่ในการใช้ข้อมูล วัตถุประสงค์ของการใช้ข้อมูล การอนุญาตให้มีการเข้าถึงข้อมูล ขอบเขตและข้อจำกัดในการเข้าถึงข้อมูล และมาตรฐานในการรักษาความปลอดภัยของข้อมูล

หากข้อมูลที่ต้องการเชื่อมโยงหรือแลกเปลี่ยนข้อมูลเป็นข้อมูลส่วนบุคคล ให้หน่วยงานผู้ร้องขอและหน่วยงานเจ้าของข้อมูลปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 18/4 เพื่อความสะดวกรวดเร็วในการเชื่อมโยงและแลกเปลี่ยนข้อมูล ให้หน่วยงานที่มีภารกิจด้านการป้องกันและปราบปรามอาชญากรรมจัดทำบัญชีรายการข้อมูล (Data Catalog) และใส่รายละเอียดชุดข้อมูล (Metadata) ภายในหน่วยงานในรูปแบบเดียวกันตามมาตรฐานที่สำนักงานกำหนด

มาตรา 18/5 ให้หน่วยงานเจ้าของข้อมูลจัดให้มีระบบบริการและแลกเปลี่ยนข้อมูลกลางเชื่อมต่อกับศูนย์แลกเปลี่ยนข้อมูลกลาง

มาตรา 18/6 ให้หน่วยงานที่มีภารกิจด้านการป้องกันและปราบปรามอาชญากรรมมีหน้าที่ในการวิเคราะห์และเผยแพร่ข้อมูลแนวโน้มอาชญากรรมอย่างเป็นระบบและนำข้อมูลมาใช้ประโยชน์ในการกำหนดนโยบายทางอาญาและมาตรการตามภารกิจของหน่วยงาน

มาตรา 18/7 ให้หน่วยงานที่มีภารกิจด้านการป้องกันและปราบปรามอาชญากรรมอาจขอเข้าถึงข้อมูลที่อยู่ในความครอบครองของภาคเอกชนเพื่อนำข้อมูลไปใช้ในการวิเคราะห์ ประมวลผลและใช้ประโยนช์ในงานป้องกันและปราบปรามอาชญากรรมได้

การขอเข้าถึงข้อมูลที่อยู่ในความครอบครองของภาคเอกชนให้เป็นไปตามข้อตกลงความร่วมมือระหว่างหน่วยงานที่มีภารกิจด้านการป้องกันและปราบปรามอาชญากรรมกับหน่วยงานกำกับดูแลภาคเอกชนหรือระหว่างหน่วยงานที่มีภารกิจด้านการป้องกันและปราบปรามอาชญากรรมกับหน่วยงานภาคเอกชนแล้วแต่กรณี

4. ข้อเสนอแนะแนวทางเตรียมความพร้อมของหน่วยงานบังคับใช้กฎหมายเพื่อสนับสนุนการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปรามอาชญากรรม

สำหรับแนวทางเตรียมความพร้อมของหน่วยงานบังคับใช้กฎหมายเพื่อสนับสนุนการนำข้อมูลขนาดใหญ่ (Big Data) มาใช้ในการป้องกันและปราบปรามอาชญากรรมนั้น มีข้อเสนอแนะดังนี้

1) พัฒนาระบบโครงสร้างพื้นฐานด้านเทคโนโลยี เพื่อบริหารจัดการข้อมูลระหว่างหน่วยงานรัฐเพื่อการวิเคราะห์ข้อมูลขนาดใหญ่ ให้ระบบสามารถรองรับการทำงานอย่างต่อเนื่อง รองรับการเชื่อมโยงข้อมูลอย่างเป็นระบบและมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

2) หน่วยงานรัฐที่มีหน้าที่ในการป้องกันและปราบปรามอาชญากรรมต้องเตรียมความพร้อมในการจัดเก็บข้อมูล Big data จะต้องมีการกำหนดภารกิจเกี่ยวกับการจัดทำบัญชีข้อมูล (Data Catalog) ให้สอดคล้องตามมาตรฐานที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) กำหนดลงใน Template มาตรฐานการจัดทำบัญชีข้อมูล ซึ่งหมายถึง เอกสารแสดงบรรดารายการของชุดข้อมูลที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงานของรัฐผ่านคำอธิบาย ข้อมูลหรือเมทาดาตา (Metadata) การรวบรวมข้อมูลนี้มาจากหลายแหล่งและนำข้อมูลมาจัดเป็นชุดให้ถูกต้องตามลักษณะโครงสร้างข้อมูลที่กำหนดไว้ เพื่อการวิเคราะห์ความสัมพันธ์ระหว่างข้อมูลกับการเชื่อมโยงกับข้อมูลหน่วยงานอื่น การทำบัญชีข้อมูล (Data Catalog) จะทำให้ผู้ใช้ข้อมูลทราบว่าข้อมูลมาจากแหล่งใด มีรูปแบบอย่างไร ช่วยอำนวยความสะดวกในการสืบค้นข้อมูล และใช้ประโยชน์ในการจัดทำบัญชีข้อมูล (Data Catalog) ของหน่วยงานและของประเทศและสนับสนุนในเกิดการเปิดเผยเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

3) พัฒนาฐานข้อมูลและระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการบริหารจัดการข้อมูล เพื่อเชื่อมโยงข้อมูลในกระบวนการยุติธรรมที่มีประสิทธิภาพ โดยการบูรณาการฐานข้อมูลที่สำคัญสอดคล้องกับความต้องการของหน่วยงานในกระบวนการยุติธรรม กำหนดมาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลตามมาตรฐานขั้นต่ำที่กฎหมายกำหนด เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบหรือโดยมิได้รับอนุญาต

4) พัฒนาระบบการรายงานข้อมูลภาครัฐ (Government Data Catalog) โดยการรวบรวมสรุปรายการโครงสร้างข้อมูลของหน่วยงานภาครัฐทั้งหมดเพื่อให้บริการแก่หน่วยงานต่าง ๆ ในการสืบค้นข้อมูล

5) การพัฒนาความรู้ความเข้าใจของเจ้าหน้าที่ผู้ปฏิบัติงานในการประยุกต์ใช้เทคโนโลยี Big Data กับภารกิจของหน่วยงาน รวมทั้งให้ความรู้เกี่ยวกับธรรมาภิบาลข้อมูล และมีการกระตุ้นให้บุคลากรทุกส่วนให้ความสำคัญและมีโอกาสได้นำความรู้ที่ได้ไปปรับใช้ในการทำงาน โดยจัดอบรมหลักสูตรอย่างต่อเนื่อง

6) จัดทำคู่มือแนวปฏิบัติในการดำเนินการกับข้อมูลขนาดใหญ่ (Big Data) โดยการอธิบายหลักและแนวปฏิบัติของกฎหมายที่เกี่ยวข้อง อาทิ กฎหมายว่าด้วยการให้บริการและการบริหารงานภาครัฐผ่านระบบดิจิทัล กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยข้อมูลข่าวสารของทางราชการ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่ ฯลฯ และคู่มือแนวปฏิบัติตามมาตรฐานด้านต่าง ๆ ที่เกี่ยวข้องกับการใช้ข้อมูลขนาดใหญ่ อาทิ มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

บรรณานุกรม

เอกสารภาษาไทย

กรอบการวิเคราะห์ข้อมูลขนาดใหญ่ภาครัฐ, คณะอนุกรรมการออกแบบสถาปัตยกรรม (Architecture Design), “ระบบบูรณาการข้อมูลภาครัฐภายใต้คณะกรรมการขับเคลื่อนการดำเนินนโยบายเพื่อใช้ประโยชน์ข้อมูลขนาดใหญ่ (Big Data), ศูนย์ข้อมูล (Data Center) และคลาวด์คอมพิวติ้ง (Cloud Computing)”.

จุฑารัตน์ เอื้ออำนวย . การสำรวจสถิติอาชญากรรมในประเทศไทยและข้อเสนอเพื่อพัฒนาการกระบวนการยุติธรรมยุคใหม่ . วารสารกระบวนการยุติธรรม เล่มที่ 2 ปีที่ 1.

ธันยวุฒิ อักขระสมชีพ. (2562). Big Data คืออะไร Data Science คืออะไร มีข้อมูลอยู่จะเริ่มอย่างไร ในทีมต้องมีใคร [ออนไลน์]. สืบค้นเมื่อวันที่ : 20 มกราคม 2563, จาก https://medium.com/@thanyavuth/bigdata-และ-data-science-คืออะไร-ทีมต้องมีใครบ้างมีข้อมูลอยู่จะเริ่มอย่างไร-2cb7fec385a3 อ้างถึงใน สมญัติ คำปาละ, การวิเคราะห์การใช้และประโยชน์ ระบบข้อมูลขนาดใหญ่ของ สำนักงานตำรวจแห่งชาติ, หน้า 114.

ภาสกร เจนประวิทย์, การจัดทำฐานข้อมูลและวิเคราะห์อาชญากรรมเบื้องต้นของศูนย์ปฏิบัติการคดีพิเศษภาค 4 , https://www.dsi.go.th/th/Detail/การจัดทำฐานข้อมูลและวิเคราะห์อาชญากรรมเบื้องต้นของศูนย์ปฏิบัติการคดีพิเศษภาค-4 , สืบค้นเมื่อ 15 เมษายน 2564.

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม . Bid Data . สืบค้นเมื่อ 15 ธันวาคม 2563, https://www.ops.go.th/main/index.php/knowledge-base/article-pr/657-big-data.

สถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ (GBDi) . กรอบการวิเคราะห์ข้อมูลขนาดใหญ่ภาครัฐ (Government Big Data Analytics Framework), 2563,

สภาความมั่นคงแห่งชาติ . แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ 1 (พ.ศ. 2563 – 2565), https://www.nsc.go.th/wp-content/uploads/2020/03/AcPlan-Data-Integration.pdf สืบค้นเมื่อ 16 พฤศจิกายน 2564.

สมญัติ คำปาละ . การวิเคราะห์การใช้และประโยชน์ ระบบข้อมูลขนาดใหญ่ของ สำนักงานตำรวจแห่งชาติ, วารสารสหวิทยาการ วิทยาลัยสหวิทยาการ มหาวิทยาลัยธรรมศาสตร์ . ปีที่ 17 ฉบับที่ 1 (มกราคม 2563 – มิถุนายน) , 2563.

สำนักงานเทคโนโลยีและการสื่อสาร สำนักงานตำรวจแห่งชาติ . คู่มืออบรมหลักสูตรพนักงานสอบสวน . “การใช้งานระบบสารสนเทศข้อมูลอาชญากรรมสำนักงานตำรวจแห่งชาติ, 2559.

สำนักงานกิจการยุติธรรม กระทรวงยุติธรรม . รายงานสถานการณ์อาชญากรรมและกระบวนยุติธรรม ประจำปี 2562.

สำนักงานคณะกรรมการกฤษฎีกา, บันทึกวิเคราะห์สรุปสาระสำคัญของร่างพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. .... , สืบค้นเมื่อ 6 กุมภาพันธ์ 2564 https://www.krisdika.go.th/data/comment/comment_lawdraft/2561/2065_2561_0126.htm

สำนักงานส่งเสริมเศรษฐกิจดิจิทัล . “รู้จักกับบิ๊กดาต้า Big Data Ecosystems” สืบค้นเมื่อ 3 พฤศจิกายน 2563, https://www.depa.or.th/th/article-view/big-data-ecosystems.

อุนิษา เลิศโตมรสกุล และ ผศ.ดร.ชาญคณิต กฤตยา สุริยะมณี . การศึกษาหาแนวทางในการป้องกันอาชญากรรมแบบไม่เป็นทางการ: กรณีศึกษาในเขตกรุงเทพมหานคร . กรุงเทพ : สำนักงานกิจการยุติธรรม , 2552.

Brantingham and Faust .(1976) A Conceptual Model of Crime Prevention . Crime Delinquency 22 , 1976 , pp 284-296 . อ้างถึงใน อุนิษา เลิศโตมรสกุล และ ผศ.ดร.ชาญคณิต กฤตยา สุริยะมณี, การศึกษาหาแนวทางในการป้องกันอาชญากรรมแบบไม่เป็นทางการ: กรณีศึกษาในเขตกรุงเทพมหานคร . กรุงเทพ : สำนักงานกิจการยุติธรรม , 2552.

Health Link แพลตฟอร์มเชื่อมข้อมูลสุขภาพ สู่ "Big Data" ด้านสาธารณสุข, กรุงเทพธุรกิจ , เข้าถึงเมื่อ 15 เมษายน 2565 , https://www.bangkokbiznews.com/social/994209.

เอกสารภาษาต่างประเทศ

A.E. Waldman. Power, process, and automated decision-making. Fordham Law Review. 88(2), pp. 613-632, 2019.

Alexander Babuta. (2017, September). Big Data and Policing An Assessment of Law Enforcement Requirements, Expectations and Priorities. Retrieved from Royal United

Services Institute for Defence and Security Studies (RUSI),: https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf

B.J. Bushman et al. Youth violence: what we know and what we need to know. Am Psychol. 71(1), pp. 17-39, 2016.

Barocas S, Rosenblat A, boyd d, Gangadharan SP, Yu C. (2014, October). Data & civil rights: technology primer. Retrieved from Data & Civil Rights: Why "Big Data" Is a Civil Rights Issue, Washington, DC: https://papers. ssrn.com/sol3/papers.cfm?abstract_id=2536579

Brayne, Rosenblat, & Boyd, (2015, October). Predictive Policing. Retrieved from datacivilrights.org: https://datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf

Brayne, S. (2017, August). Big Data Surveillance: The Case of Policing, Vol. 82(5) 977–1008. Retrieved from American Sociological Review: http://users.soc.umn.edu/~uggen/Brayne_ASR_17.pdf

C. Piovesan and V. Ntiri. Adjudication by algorithm: the risks and benefits of artificial intelligence in judicial decision-making. The Advocates' Journal. pp. 42-45, 2018.

Caplan, J. M. & Kennedy, L. W. (Eds.) 2011. Risk Terrain Modeling Compendium. Newark, NJ:

Child Rescue Coalition. (2020). Child Rescue Coalition Annual Report 2020. Retrieved from Child Rescue Coalition: https://childrescuecoalition.org/child-rescue-coalition-annual-report-2020.html

Claude Moraes. (2014). Committee on Civil Liberties, Justice and Home Affairs, 2013/2188(INI). Retrieved from European Parliament: https://www.europarl.europa.eu/document/activities/cont/201403/20140306ATT80626/20140306ATT80626EN.pdf

Claudia Peersman;Christian Schulze;Awais Rashid; Margaret Brennan;Carl Fischer. (2016, September). iCOP: Live forensics to reveal previously unknown criminal media on P2P networks. Retrieved from sciencedirect: https://www.sciencedirect.com/science/article/pii/S1742287616300779

E.E. Joh. Increasing automation in policing," Communications of the ACM. 63, pp. 20-22, 2020.

European Court of Human Rights (ECHR). (2018). Handbook on European data protection law 2018 Edition. Retrieved from European Union Agency for Fundamental Rights and Council of Europe: https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

G. O. Mohler, M. B. Short, Sean Malinowski, Mark Johnson, G. E. Tita, Andrea L. Bertozzi & P. J. Brantingham (2015) Randomized Controlled Field Trials of Predictive Policing, Journal of the American Statistical Association, 110:512, 1399-1411, DOI: 10.1080/01621459.2015.1077710

Haggerty KD, Ericson RV. 2006. The New Politics of Surveillance and Visibility. P.3. Toronto: Univ. Toronto Press

Hannah Couchman, Alessandra Prezepiorski Lemos. (2019, January). Liberty report: Policing by Machine. Retrieved from libertyhumanrights.org.uk: https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/LIB-11-Predictive-Policing-Report-WEB.pdf

Ian Kearns, Rick Muir. (2019, March). Data-driven policing and public value. Retrieved from The Police Foundation Kemp House: https://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/data_driven_policing_final.pdf

INTERPOL and ECPAT International. (2018, February). Technical report: Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material. Retrieved from Interpol: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

Interpol. (2017, January). Interpol network identifies 10,000 child sexual abuse victims. Retrieved from Interpol: https://www.interpol.int/en/News-and-Events/News/2017/INTERPOL-network-identifies-10-000-child-sexual-abuse-victims

Interpol. (2021, November 30). International Child Sexual Exploitation database. Retrieved from Interpol: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

J. Bonta and D.A. Andrews. Risk-need-responsivity model for offender assessment and rehabilitation. Rehabilitation. 6, pp. 1-22, 01/01 2007.

K. Robertson, C. Khoo, and Y. Song. “To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada”, (University of Toronto Press, Canada). 2020.

Keyur K Patel, Sunil M Patel. (2016, May). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. Retrieved from IJESC, Volume 6 Issue No. 5: https://www.researchgate.net/publication/330425585_Internet_of_Things-IOT_Definition_Characteristics_Architecture_Enabling_Technologies_Application_Future_Challenges

M. Purcell and M. Zaia. (2020). Prediction, prevention and proof: Artificial intelligence and peach bonds in Canada. The Canadian Bar Review. Vol. 98, pp. 515-542.

M. Purcell and M. Zaia. Prediction, prevention and proof: Artificial intelligence and peach bonds in Canada. The Canadian Bar Review. 98, pp. 515-542, 2020.

May-Chahal, Corinne, Kelly, Emma. (2020). Online Child Sexual Victimisation. Retrieved from Bristol University Press: https://books.google.co.th/books?id=UGXXDwAAQBAJ&pg=PA94&lpg=PA94&dq=International+Child+Sexual+Exploitation+-+ICSE+USA+america&source=bl&ots=4JH_IT-E8h&sig=ACfU3U12dqCZ5d70O_ltgEL1SvIj7u0cmQ&hl=en&sa=X&ved=2ahUKEwj2h_2wyb70AhWESGwGHZ6ZA5EQ6AF6BAgMEAM#v=o

Mehmood, Abid & Natgunanathan, Iynkaran & Xiang, Yong & Hua, Guang & Guo, Song. (2016). Protection of Big Data Privacy. Retrieved from researchgate: https://www.researchgate.net/publication/301716085_Protection_of_Big_Data_Privacy

Michael Price. (2013, December). National Security and Local Police. Retrieved from brennancenter.org: https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf

Michael Purcell, Mathew Zaia. (2020). “Prediction, Prevention and Proof: Artificial Intelligence and Peace Bonds in Canada”. Retrieved from The Canadian Bar Review, Vol. 98 No.3 https://cbr.cba.org/index.php/cbr/article/view/4630

Mohler, George & Short, M. & Malinowski, Sean & Johnson, Mark & Tita, George & Bertozzi, Andrea & Brantingham, P. (2015, October). Randomized Controlled Field Trials of Predictive Policing. Retrieved from Journal of the American Statistical Association: https://www.tandfonline.com/doi/abs/10.1080/01621459.2015.1077710?journalCode=uasa20

Motorola Solutions. (2018, July). West Yorkshire Police Transforms Front-Line Policing. Retrieved from Motorola Solutions: https://www.motorolasolutions.com/content/dam/msi/docs/en-xu/public-safety/pronto_west_yorkshire_police_case_study.pdf

N.M. Richards and J. King. Three Paradoxes of Big Data. Stan L Rev Online. 66, pp. 41-46, 2013.

Olivia Solon. (July, 2020 17). Inside the surveillance software tracking child porn offenders across the globe. Retrieved from NBC News: https://www.nbcnews.com/tech/internet/inside-surveillance-software-tracking-child-porn-offenders-across-globe-n1234019

Public Safety Canada, “The Hub - Centre of Responsibility (COR)” (14 Marc 2018), online: Government of Canada <www.publicsafety.gc.ca>; Nathan Munn, “Canada’s ‘Pre-Crime’ Model of Policing Is Sparking Privacy Concerns” (19 January 2017), online: Vice <www.vice.com>.".

Rutgers Center on Public Security. Retrieved from riskterrainmodeling.com: https://www.rutgerscps.org/uploads/2/7/3/7/27370595/riskterrainmodelingcompendium_caplankennedy2011.pdf

S.D. Konikoff and A. Owusu-Bemphah. "Big Data and Criminal Justice – What Canadians Should Know" (ND) at 4, online: Broadbent Institute <www.broadbentinstitute.ca> [Konikoff & Owusu-Bemphah].".

Sarah Brayne, Angèle Christin. (2020). Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts, Social Problems, spaa004, https://doi.org/10.1093/socpro/spaa004

Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from Annual Review of Law and Social Science, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

Shapiro, A. (2019, September). Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. Retrieved from Surveillance & Society. Vol 17 No 3/4 (2019): Visibilities and New Models of Policing : https://www.researchgate.net/publication/338419815_Predictive_Policing_for_Reform_Indeterminacy_and_Intervention_in_Big_Data_Policing

TaeHeon Moon, SunYoung Heo, SangHo Lee. (2014). Ubiquitous Crime Prevention System (UCPS) for a Safer City. Retrieved from ScienceDirect, Procedia Environmental Sciences, Volume 22, 2014: https://www.sciencedirect.com/science/article/pii/S1878029614001753?via%3Dihub

The Parliamentary Office of Science and Technology. (2014, July). Big Data, Crime and Security. Retrieved from Houses of Parliament, The Parliamentary Office of Science and Technology. POSTnote Number 470: file:///D:/P%20Pim%20big%20data/UK/Big%20Data,%20Crime%20and%20Security%20-%20UK%20Parliament%20POST-PN-470.pdf

Victoria Baines. (2008, November). Online Child Sexual Abuse: The Law Enforcement Response. Retrieved from ECPAT International: https://www.ecpat.org/wp-content/uploads/legacy/Thematic_Paper_ICTLAW_ENG.pdf

W.L. Perry, B. McInnis, C.C. Price, S.C. Smith, and J.S. Hollywood. “Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. Washington” RAND Corporation, 2013.

W.S. Isaac. Hope, hype, and fear: the promise and potential pitfalls of the big data era in criminal justice. Ohio State Journal of Criminal Law. 15(2), pp. 543-558, 2018.

WALLIS, J. (2015, November 20). Justin FRAZIER, Appellant, v. STATE of Florida, Appellee. Case law, No. 5D14–171. Retrieved from Thomson Reuters: https://caselaw.findlaw.com/fl-district-court-of-appeal/1718791.html