การคุ้มครองสิทธิมนุษยชนจากมาตรการความร่วมมือระหว่างประเทศในกรอบของสหประชาชาติว่าด้วยการเข้าถึงข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ เพื่อการป้องกันและปราบปรามอาชญากรรมไซเบอร์

The protection of human right from international cooperation in accessing personal data for prevention of cybercrime under draft treaty of the United Nations.

คณาธิป ทองรวีวงศ์[1*]

Kanathip Thongrawewong[1*]

[1] รองศาสตราจารย์ คณะนิติศาสตร์ มหาวิทยาลัยเกษมบัณฑิต

[1] Associate Professor, Faculty of law, Kasembundit University.

[*]**Corresponding author, E-mail:** kanathip.tho@kbu.ac.th

บทคัดย่อ

อาชญากรรมไซเบอร์เกิดขึ้นโดยไม่จำกัดเขตแดน แต่มาตรการเข้าถึงข้อมูลคอมพิวเตอร์เพื่อการสืบสวนสอบสวนอาชญากรรมดังกล่าวอาจส่งผลกระทบต่อสิทธิมนุษยชน การวิจัยนี้มีวัตถุประสงค์เพื่อ 1. วิเคราะห์มาตรการความร่วมมือระหว่างประเทศในปัจจุบันเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์เพื่อการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ 2. วิเคราะห์มาตรการเข้าถึงและได้มาซึ่งข้อมูลในกรอบร่างสนธิสัญญาสหประชาชาติ โดยเปรียบเทียบกับมาตรการความร่วมมือที่ประเทศต่าง ๆ ใช้ในปัจจุบัน ในแง่ประสิทธิภาพและผลกระทบต่อสิทธิมนุษยชน สำหรับกรอบแนวคิดที่ใช้ในการวิจัยคือแนวคิดเกี่ยวกับสิทธิในความเป็นอยู่ส่วนตัว ข้อมูลส่วนบุคคล และการจำกัดสิทธิดังกล่าวภายใต้หลักความจำเป็นและได้สัดส่วน

ผลการศึกษาพบว่า 1. มาตรการความร่วมมือระหว่างประเทศที่ประเทศต่าง ๆ ใช้ในปัจจุบันเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์ ได้แก่ มาตรการ MLA ซึ่งมีข้อจำกัดในเชิงประสิทธิภาพ และมาตรการฝ่ายเดียวซึ่งมีผลกระทบต่อสิทธิมนุษยชน 2. ผลการศึกษาร่างสนธิสัญญาเพื่อความร่วมมือระหว่างประเทศในการแสวงหาพยานหลักฐานของสหประชาชาติ พบว่ามีบทบัญญัติสำหรับการได้มาซึ่งข้อมูลคอมพิวเตอร์โดยเฉพาะ แต่ในส่วนมาตรการเข้าถึงข้อมูลคอมพิวเตอร์ข้ามพรมแดนโดยตรง ให้น้ำหนักกับการสืบสวนสอบสวนมากกว่าการคุ้มครองสิทธิมนุษยชน (3) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลวางหลักการห้ามเปิดเผยหรือส่งข้อมูลไปต่างประเทศตามมาตรา 28 แต่ไม่ได้กำหนดเรื่องการเปิดเผยข้อมูลส่วนบุคคลตามความร่วมมือระหว่างประเทศในการแสวงหาพยานหลักฐานไว้อย่างชัดเจน

ผู้วิจัยจึงมีข้อเสนอแนะเชิงนโยบายต่อรัฐในการดำเนินการมาตรการร่วมมือเพื่อแสวงหาหลักฐานของอาชญากรรมไซเบอร์อย่างสมดุลกับการคุ้มครองสิทธิมนุษยชน

คำสำคัญ: อาชญากรรมไซเบอร์, ข้อมูลส่วนบุคคล, สิทธิมนุษยชน, สหประชาชาติ

Abstract

Cybercrime could be committed without borders. However, legal measures of access to computer data for the investigation of such crimes could have impact on human rights. The purposes of this study were: 1) to analyze existing international cooperation measures on access to computer data for the prevention and suppression of computer crime 2) to analyze data acquisition and access measures stipulated in the United Nations draft treaty framework of cybercrime by making comparative analysis with the existing international cooperation measures in terms of efficiency and impact on human rights. The conceptual framework used in the research is the right to privacy, the protection of personal data and the restriction of such right under the principle of proportionality.

This qualitative research used content analysis of related international, foreign and domestic laws. It was found that 1.) Existing international cooperation measures regarding access to computer data consist of two main measures, i.e., MLAs which are limited in their effectiveness and unilateral measures which affect human rights. 2) Certain provisions of the UN's Draft Treaty for International cooperation could impact human rights such as measures of direct access to computer data across borders. Consequently, the researcher, therefore, proposed recommendations for the Thai government to implement cooperative measures to obtain evidence of cybercrime in balance with human rights protection.

Keywords: Cybercrime, personal data, human rights, United Nations.

บทนำ

อาชญากรรมคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ ประกอบด้วยรูปแบบพฤติกรรมหลากหลาย ทั้งในส่วนของอาชญากรรมที่กระทบต่อความปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์ที่เรียกว่าอาชญากรรมไซเบอร์โดยแท้ (Pure cybercrime) และอาชญากรรมรูปแบบดั้งเดิมแต่เปลี่ยนวิธีการมากระทำทางระบบคอมพิวเตอร์ เช่น การใช้เนื้อหาข้อมูลเท็จหลอกลวงหรือที่เรียกว่า การฉ้อโกงหลอกลวงทางคอมพิวเตอร์ (Yvonne, 2010) อาชญากรรมดังกล่าวส่งผลกระทบในหลายแง่มุม เช่น ผลกระทบในด้านการเงิน ซึ่งประเมินได้อย่างเป็นรูปธรรม ดังจะเห็นได้จากความผิดเกี่ยวกับบัญชีธนาคาร ทั้งใน

ลักษณะของการหลอกลวงให้เหยื่อโอนเงิน การเจาะเข้าระบบบัญชีธนาคารออนไลน์ของผู้อื่นและใช้บัญชีของบุคคลนั้นทำธุรกรรม (Hoofnagle, 2007) นอกจากผลโดยตรงด้านการเงินที่เสียไปแล้ว ยังมีผลกระทบด้านอื่นเช่น เวลาที่เสียไปในการจัดการกับปัญหาที่เกิดขึ้น เวลาและค่าใช้จ่ายเกี่ยวกับการดำเนินคดีของผู้เสียหาย (Listerman and Romesberg,2009) ในบางกรณีอาชญากรรมคอมพิวเตอร์ใช้ข้อมูลส่วนบุคคลผู้อื่นกระทำผิดเพื่อปกปิดตัวตน ส่งผลให้เจ้าของข้อมูลตกเป็นผู้ต้องหากระทำความผิด (Biegelman, 2009) นอกจากในระดับของบุคคลผู้ได้รับผลกระทบโดยตรง ยังส่งผลกระทบในระดับมหภาคต่อสถาบันการเงิน ภาคธุรกิจอื่น (Conkey 2007) รวมทั้งส่งผลกระทบต่อทัศนคติ และความเชื่อมั่นของผู้บริโภคต่อการพาณิชย์อิเล็กทรอนิกส์ (Jonker, 2007) รวมทั้งความกังวลต่อการใช้บริการธนาคารทางอินเทอร์เน็ต (Sproule & Archer, 2010) ดังนั้น การบังคับใช้กฎหมายเพื่อป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์จึงมีความสำคัญ แต่เนื่องจากอาชญากรรมคอมพิวเตอร์มีลักษณะข้ามพรมแดน (Cross border) ทั้งในแง่ของการกระทำที่ไม่จำกัดเขตแดนรัฐ และในแง่พยานหลักฐานที่อยู่ในรูปแบบข้อมูลคอมพิวเตอร์ อาจถูกเก็บรักษาไว้โดยผู้ให้บริการ (Service provider) หรือในอุปกรณ์เก็บข้อมูลที่ตั้งอยู่ในประเทศอื่น ประกอบกับสภาพของอาชญากรรมไซเบอร์ที่พยานหลักฐานในรูปข้อมูลคอมพิวเตอร์อาจถูกแก้ไขเปลี่ยนแปลงหรือลบได้โดยง่าย ทำให้เกิดอุปสรรคต่อการบังคับใช้กฎหมายและการแสวงหาพยานหลักฐาน นำไปสู่ความจำเป็นของความร่วมมือระหว่างประเทศ

ในปัจจุบันประเทศต่างๆ ดำเนินการความร่วมมือโดยอาศัยสนธิสัญญา (Mutual Legal Assistance Treaty ซึ่งต่อไปในบทความนี้จะเรียกว่า MLAT) แต่มีข้อจำกัดเนื่องตัวบทและหลักการของสนธิสัญญาวางหลักเกี่ยวกับการดำเนินการทางกายภาพ เช่น การส่งประเด็นไปสอบสวนสืบพยานบุคคล พยานเอกสาร พยานวัตถุ ในต่างประเทศ การส่งคำฟ้อง หมายเรียก ฯลฯ ไม่ได้ระบุถึงการเข้าถึงข้อมูล คอมพิวเตอร์ไว้โดยตรง อีกทั้งขึ้นอยู่กับการตกลงทวิภาคีระหว่างรัฐเป็นกรณีไป สำหรับประเทศไทยมีความตกลง MLAT กับบางประเทศ เช่น สหรัฐอเมริกา สหราชอาณาจักร สาธารณรัฐประชาชนจีน ฯลฯ และดำเนินการภายใต้กรอบกฎหมายภายในคือพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 ซึ่งไม่ได้ระบุเรื่องความร่วมมือในการเข้าถึงหรือได้มาซึ่งข้อมูลคอมพิวเตอร์ระหว่างประเทศ ในระดับเดือนธันวาคม ค.ศ. 2019 ที่ประชุมสมัชชาใหญ่สหประชาชาติได้รับรองมติว่าด้วย “การต่อต้านการใช้เทคโนโลยีสารสนเทศเพื่อประกอบอาชญากรรม” และจัดตั้งคณะทำงานเฉพาะกิจ (Ad Hoc Committee) เพื่อดำเนินการเกี่ยวกับการร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยี (Draft of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes ซึ่งในที่นี้จะเรียกว่า “ร่างสนธิสัญญา”) ประกอบด้วยหลายหมวด เช่น การกำหนดต้นแบบฐานความผิด (Model offence) สำหรับงานวิจัยนี้จะศึกษาหมวด 4 ว่าด้วย “ความร่วมมือระหว่างประเทศ” (International cooperation) ซึ่งวางหลักการเกี่ยวกับความร่วมมือเข้าถึงข้อมูลคอมพิวเตอร์หลายมาตรา ปัจจุบันร่างดังกล่าวอยู่ระหว่างการจัดทำโดย

ผู้แทนประเทศสมาชิก ในส่วนของประเทศไทยไม่ปรากฏการเป็นผู้แทนหรือคณะทำงาน (Ad hoc committee) ในการร่างสนธิสัญญา แม้ว่ามาตรการตามร่างสนธิสัญญานี้วางหลักเกณฑ์เจาะจงถึงการเข้าถึงข้อมูลคอมพิวเตอร์ ซึ่งไม่ปรากฏชัดเจนในแนวทางความร่วมมือแบบ MLAT แต่ในอีกแง่หนึ่งมาตรการได้มาหรือเข้าถึงข้อมูลคอมพิวเตอร์ส่งผลกระทบต่อสิทธิมนุษยชนของประชาชนหรือเจ้าของข้อมูล จึงนำไปสู่ประเด็นการชั่งน้ำหนักเพื่อความสมดุลระหว่างมาตรการแสวงหาหลักฐานเพื่อปราบปรามอาชญากรรมไซเบอร์กับการคุ้มครองสิทธิมนุษยชนในแง่สิทธิในความเป็นอยู่ส่วนตัวและข้อมูลส่วนบุคคล ซึ่งการศึกษาวิจัยครั้งนี้มีประเด็นคำถามสำคัญว่า 1. มาตรการร่วมมือระหว่างประเทศที่มีผลใช้บังคับในปัจจุบันเกี่ยวกับการได้มาหรือเข้าถึงข้อมูลคอมพิวเตอร์เพื่อป้องกันปราบปรามอาชญากรรมไซเบอร์ มีหลักและข้อจำกัดหรืออุปสรรคอย่างไรอันนำไปสู่การร่างหลักความร่วมมือของสหประชาชาติ รวมทั้งคำถามว่ามาตรการดังกล่าวส่งผลกระทบต่อสิทธิมนุษยชนอย่างไร 2. มาตรการความร่วมมือตามร่างสนธิสัญญาสหประชาชาติมีข้อดีและข้อจำกัดอย่างไร และผลกระทบต่อสิทธิมนุษยชนอย่างไรเมื่อเปรียบเทียบกับมาตรการที่มีผลบังคับใช้อยู่ โดยนำเกณฑ์หรือองค์ประกอบตามหลักสิทธิมนุษยชนมาวิเคราะห์ชั่งน้ำหนักมาตรการเข้าถึงข้อมูลเพื่อสืบสวนสอบสวนอาชญากรรมไซเบอร์กับการคุ้มครองสิทธิเสรีภาพ การศึกษาตามประเด็นดังกล่าวนอกจากมีประโยชน์ทางวิชาการในการสร้างแนวทางการนำเกณฑ์สิทธิมนุษยชนมาวิเคราะห์ประเมินมาตรการของรัฐที่อ้างเหตุผลอย่างกว้างเกี่ยวกับการปราบปรามอาชญากรรมแล้วยังสามารถนำไปประยุกต์ใช้เพื่อจัดทำข้อเสนอแนะเชิงนโยบายเพื่อการดำเนินการของประเทศไทยเพื่อสร้างความสมดุลระหว่างการป้องกันปราบปรามอาชญากรรมกับการคุ้มครองสิทธิมนุษยชนด้วย

วัตถุประสงค์ของการวิจัย

1. วิเคราะห์มาตรการความร่วมมือระหว่างประเทศที่ประเทศต่างๆใช้ในปัจจุบันเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์เพื่อการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ในแง่ประสิทธิภาพและผลกระทบต่อสิทธิมนุษยชน

2. วิเคราะห์ประสิทธิภาพและผลกระทบต่อสิทธิมนุษยชนของมาตรการเข้าถึงและได้มาซึ่งข้อมูลในกรอบร่างสนธิสัญญาสหประชาชาติ โดยวิเคราะห์เนื้อหาเปรียบเทียบกับมาตรการความร่วมมือที่ประเทศต่าง ๆ ใช้ในปัจจุบัน ในแง่ประสิทธิภาพและผลกระทบต่อสิทธิมนุษยชน

แนวคิด ทฤษฎี กรอบแนวคิด

มาตรการของรัฐในการแสวงหาข้อมูลคอมพิวเตอร์เพื่อดำเนินคดีหรือสืบสวนสอบสวน ส่งผลกระทบต่อข้อมูลส่วนบุคคล เช่น ข้อมูลผู้ใช้บริการที่จัดเก็บในระบบของผู้ให้บริการ ในแง่สิทธิมนุษยชนการกระทำที่กระทบต่อข้อมูลนั้นเกี่ยวข้องกับ “สิทธิในความเป็นอยู่ส่วนตัว” (Right to privacy) ซึ่งจัดเป็นสิทธิขั้นพื้นฐานของมนุษย์ (Hannah, 1973) กล่าวคือ เป็นสิทธิที่ติดตัวคนมาตั้งแต่กำเนิด จึงอยู่ใน

กลุ่มของสิทธิมนุษยชน (Donnelly ,1982) บางตำราเรียกว่า สิทธิที่จะอยู่ตามลำพัง (Right to be let alone) กล่าวคือ ปราศจากการแทรกแซงจากบุคคลภายนอก (Samuel and Brandies,1890) แต่การพิจารณาในแง่ปราศจากการแทรกแซงหรือความลับอาจทำให้สิทธินี้กว้างเกินไป โดยเฉพาะในสภาพสังคมที่มีการติดต่อระหว่างบุคคล ทำให้การไม่ถูกแทรกแซงเป็นไปได้ยาก (Alan F. Westin, 1967) ต่อมามีการพัฒนาแนวคิดว่าหมายถึง การจำกัดการเข้าถึงปัจเจกชนโดยบุคคลอื่น (Rubenfield, 1989) ในทางวิชาการ สิทธิดังกล่าวยังคงมีความหมายและขอบเขตกว้าง (Schoeman, 1984) โดยจำแนกได้หลายมิติ รวมถึงการคุ้มครองข้อมูลส่วนบุคคล (Solove,2006) ตามกฎหมายสหรัฐอเมริกา สิทธิในความเป็นอยู่ส่วนตัวปรากฏในกฎหมายคอมมอนลอว์และกฎหมายอื่น เช่น กฎหมายลักษณะละเมิด (Bloustein, 1984) เมื่อพิจารณาในระดับกฎหมายระหว่างประเทศ พบว่า กติกาสากลว่าด้วยสิทธิทางแพ่งและการเมืองของสหประชาชาติ (International Covenant on Civil and Political Rights ค.ศ.1966 หรือ ICCPR) รับรองสิทธินี้ไว้ในข้อ 17 แต่มีข้อยกเว้นว่า การจำกัดหรือแทรกแซงสิทธิดังอาจชอบด้วยกฎหมายหากมีกฎหมายบัญญัติไว้ แต่ทั้งนี้มิใช่รัฐจะสามารถตรากฎหมายจำกัดสิทธิเสรีภาพได้อย่างกว้าง โดยข้อวินิจฉัยทั่วไปที่ 16 (General comment No. 16) อธิบายข้อ 17 ของ ICCPR ว่า กฎหมายที่จำกัดสิทธิจะต้องมีข้อจำกัดและเงื่อนไขเพื่อมิให้เกิดการใช้อำนาจแทรกแซงความเป็นส่วนตัวโดยอำเภอใจ (Arbitrary interference) (Office of the High commissioner for human rights,1988) กล่าวคือ กฎหมายที่จำกัดเสรีภาพต้องสอดคล้องกับหลักความจำเป็นและได้สัดส่วน ซึ่งแยกพิจารณาตามองค์ประกอบหลายประการ แช่น

(1) องค์ประกอบในแง่การตรวจสอบถ่วงดุล กล่าวคือ มาตรการตามกฎหมายที่จำกัดสิทธิเสรีภาพต้องมีกระบวนการตรวจสอบจากองค์กรอิสระจากหน่วยงานที่ใช้อำนาจ เช่น เจ้าหน้าที่บังคับใช้กฎหมายต้องขอหมายศาล หรือ การตรวจสอบโดยองค์กรอิสระอื่น (2) องค์ประกอบในแง่ความแคบและเจาะจงของกฎหมายที่จำกัดสิทธิ กล่าวคือ กฎหมายที่ให้อำนาจเข้าถึงข้อมูล ต้องระบุรายละเอียดเกี่ยวกับเงื่อนไขปัจจัย และองค์ประกอบอันนำไปสู่การจำกัดเสรีภาพอย่างชัดเจนและเจาะจง (Office of the High commissioner for human rights, 1988) รวมทั้งมีขอบเขตจำกัดในแง่เป้าหมายของข้อมูล เพื่อมิให้เกิดการเข้าถึงข้อมูลที่ไม่เกี่ยวข้อง และมีขอบเขตจำกัดในแง่วิธีการในการเข้าถึงหรือได้มาซึ่งข้อมูล เพื่อมิให้มีการใช้วิธีการทางเทคนิคที่กระทบสิทธิเกินจำเป็น (United Nations Special Rapporteur on freedom of opinion and expression, 2015) จะเห็นได้ว่า มาตรการของรัฐในการแสวงหาพยานหลักฐานโดยการเข้าถึงข้อมูล แม้ว่าจะเป็นการดำเนินตามกฎหมายแต่ก็ยังคงต้องพิจารณาชั่งน้ำหนักตามหลักความจำเป็นและได้สัดส่วน (Cate, 1995) ซึ่งแยกเป็นองค์ประกอบหลายประการ

สำหรับกฎหมายต่างประเทศที่กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลที่ส่งผลกระทบต่อหลายประเทศ ได้แก่กฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป (Directive 95/46/EC) ซึ่งมีผลผูกพันตามกฎหมายต่อประเทศสมาชิกสหภาพยุโรป โดยหลักสำคัญประการหนึ่งของกฎหมายนี้คือ การวางเงื่อนไขการใช้การเปิดเผย การโอนข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อจำกัดด้านการโอนข้อมูลออกนอกประเทศ ต่อมา

ค.ศ. 2018 กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ของสหภาพยุโรป (General Data Protection Regulation หรือ GDPA) มีผลใช้บังคับแทนกฎหมายเดิม (Directive 95/46/EC) โดยมีหลักการสำคัญเช่นเดิมคือ การเก็บรวบรวมใช้เปิดเผยข้อมูลส่วนบุคคลของผู้อื่นต้องอ้างอิงฐานทางกฎหมาย ซึ่งโดยหลักต้องอาศัยฐานความยินยอม เว้นแต่เข้าข้อยกเว้นเช่นการปฏิบัติตามกฎหมาย อย่างไรก็ตามในบริบทของกฎหมายสหภาพยุโรป การดำเนินการของรัฐหรือการบังคับใช้กฎหมายที่กระทบข้อมูลส่วนบุคคลยังต้องอยู่ภายใต้สนธิสัญญาสิทธิมนุษยชนยุโรปอีกฉบับด้วย ซึ่งรับรองสิทธิในความเป็นส่วนตัวและข้อมูลในมาตรา 8 ซึ่งมีข้อยกเว้นหรือข้อจำกัดสิทธิคือ กรณีที่มีกฎหมายบัญญัติไว้ แต่ทั้งนี้ กฎหมายดังกล่าวต้องอยู่ภายใต้เงื่อนไขการคุ้มครองสิทธิ (Safeguard) ซึ่งเมื่อพิจารณาจากคำพิพากษาศาลสิทธิมนุษยชนยุโรปจะพบว่าศาลวางหลักเกณฑ์หรือองค์ประกอบในการชั่งน้ำหนักกฎหมายที่เป็นข้อยกเว้นหรือจำกัดสิทธิไว้หลายประการ (Council of Europe, 2016) เช่น กฎหมายที่จำกัดสิทธิต้องมีขอบเขตเจาะจง แคบและจำกัด การตรวจสอบถ่วงดุลโดยองค์กรอิสระ ซึ่งจะเห็นได้ว่าเป็นองค์ประกอบการชั่งน้ำหนักกฎหมายอันเป็นข้อยกเว้นของสิทธิในความเป็นส่วนตัว ในแนวทางคล้ายคลึงกับแนวทางของสหประชาชาติ

จากกรอบแนวคิดสรุปได้ว่า ความร่วมมือในการเข้าถึงข้อมูลคอมพิวเตอร์เพื่อป้องกันและปราบปรามอาชญากรรม ส่งผลจำกัดหรือแทรกแซงสิทธิมนุษยชน แม้ว่ากฎหมายระหว่างประเทศเกี่ยวกับสิทธิมนุษยชนกำหนดให้รัฐทำได้โดยการบัญญัติกฎหมาย แต่กฎหมายดังกล่าวต้องสอดคล้องกับหลักความจำเป็นและได้สัดส่วน (Fromholz, 2000) ซึ่งจำแนกเป็นองค์ประกอบย่อยหลายประการ เช่น การตรวจสอบถ่วงดุลการบัญญัติกฎหมายจำกัดสิทธิที่แคบและจำกัด ซึ่งงานวิจัยนี้จะนำองค์ประกอบดังกล่าวมาวิเคราะห์มาตรการความร่วมมือในการเข้าถึงข้อมูลต่อไป

วิธีดำเนินการวิจัย

งานวิจัยนี้ใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ศึกษาข้อมูลเอกสาร (Documentary Research) โดย มีขั้นตอนดังนี้

1. ข้อมูลที่นำมาวิเคราะห์ ประกอบด้วยเอกสาร 3 กลุ่มคือ (1) ร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมอิเล็กทรอนิกส์ (2) วรรณกรรมทางกฎหมายที่เกี่ยวข้องจากงานวิจัย บทความวิชาการเกี่ยวกับกฎหมายในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ การคุ้มครองข้อมูลส่วนบุคคล

2. การเก็บรวบรวมข้อมูลมาจากแหล่งเอกสาร ห้องสมุด ในส่วนของแหล่งข้อมูลอิเล็กทรอนิกส์เก็บรวบรวมจากเว็บไซต์ของหน่วยงานที่เกี่ยวข้องกับการบัญญัติและตีความกฎหมาย เช่น เว็บไซต์องค์การสหประชาชาติ เว็บไซต์ของสถาบันการศึกษา ฐานข้อมูลวิจัยออนไลน์ต่างประเทศ เช่น SpingerLink , EBSCO, ProQuest เป็นต้น

3. การวิเคราะห์ข้อมูล ใช้วิธีการวิเคราะห์เชิงเนื้อหา (Content analysis) นำหลักการเกี่ยวกับความร่วมมือระหว่างประเทศที่มีผลใช้บังคับอยู่ และร่างสนธิสัญญาของสหประชาชาติมาวิเคราะห์เนื้อหาเชิงเปรียบเทียบกับในประเด็นเกี่ยวกับประสิทธิภาพและผลกระทบต่อสิทธิมนุษยชน

การศึกษาวิจัยนี้มุ่งเน้นการวิเคราะห์ตีความเนื้อหาตัวบทกฎหมายและร่างตัวบทของสนธิสัญญาเพื่อทราบข้อจำกัด อุปสรรค และผลกระทบต่อสิทธิมนุษยชน ซึ่งจะนำไปสู่การสร้างองค์ความรู้ทางวิชาการและข้อเสนอแนะเชิงนโยบาย โดยไม่ได้ใช้วิธีเชิงปริมาณและสถิติ

ผลการวิจัย

1. ผลการศึกษา มาตรการความร่วมมือระหว่างประเทศที่ประเทศต่างๆใช้ในปัจจุบันเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์เพื่อการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ พบว่า ประกอบด้วยสองมาตรการคือ MLA และมาตรการฝ่ายเดียว (Unilateral measure) พบว่า ในแง่ประสิทธิภาพของการแสวงหาหลักฐาน มาตรการความร่วมมือ MLA มีข้อจำกัดและอุปสรรคหลายประการ ไม่สอดคล้องกับการป้องกันปราบปรามอาชญากรรมในสภาพแวดล้อมการสื่อสารสารสนเทศ อย่างไรก็ตามมาตรการดังกล่าวเป็นที่ยอมรับในทางกฎหมายระหว่างประเทศและเป็นการขอให้ประเทศปลายทางที่ข้อมูลจัดเก็บอยู่ดำเนินการซึ่งเป็นไปภายใต้กฎหมายภายในของประเทศผู้รับคำขอ แม้เป็นข้อจำกัดของสิทธิมนุษยชนแต่ก็สอดคล้องกับหลักความจำเป็นและได้สัดส่วน เมื่อเปรียบเทียบกับมาตรการฝ่ายเดียว พบว่ามีประสิทธิภาพมากกว่าเนื่องจากลดขั้นตอนและกระบวนการในการติดต่อกับหน่วยงานประเทศที่ผู้ให้บริการตั้งอยู่ แต่ไม่มีหลักการและขั้นตอนที่ชัดเจน ไม่ผ่านกระบวนการตามกฎหมายภายในของประเทศปลายทางหรือที่จัดเก็บข้อมูล จึงส่งผลกระทบต่อสิทธิมนุษยชนในแง่ความเป็นส่วนตัวและข้อมูลส่วนบุคคล

2. ผลการศึกษากรอบความร่วมมือของสหประชาชาติพบวาปัจจุบันมีการร่างสนธิสัญญาเพื่อความร่วมมือระหว่างประเทศในการแสวงหาพยานหลักฐานในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ ซึ่งมีบทบัญญัติเฉพาะเกี่ยวกับความร่วมมือในการเข้าถึงหรือได้มาซึ่งข้อมูลคอมพิวเตอร์เพื่อการสืบสวนสอบสวนอาชญากรรม แบ่งเป็น 3 มาตรา คือ มาตรา 68 มาตรา 70 และมาตรา 72 ผลการวิเคราะห์เนื้อหาพบว่า มาตรา 68 และ 70 พัฒนาขึ้นเพื่อแก้ไขข้อจำกัดของมาตรการร่วมมือระหว่างประเทศรูปแบบเดิมที่ใช้ในปัจจุบัน เช่น MLA เพราะออกแบบเพื่อตอบสนองรูปแบบอาชญากรรมในยุคสารสนเทศ แต่ในอีกแง่หนึ่งพบว่า หลักการบางส่วนของมาตรการนี้ โดยเฉพาะมาตรา 72 ให้น้ำหนักกับการสืบสวนสอบสวนมากกว่าการคุ้มครองสิทธิมนุษยชน โดยเฉพาะอย่างยิ่งมาตรการให้สิทธิสมาชิกสนธิสัญญาในการเข้าถึงข้อมูลคอมพิวเตอร์ข้ามพรมแดนโดยตรง (Cross border data access)

ในส่วนของกฎหมายไทย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายที่เกี่ยวข้องกับการเปิดเผยข้อมูลส่วนบุคคลให้หน่วยงานต่างประเทศ แม้ว่ามีหลักการห้ามเปิดเผยตามมาตรา 28 แต่ไม่ได้กำหนดเรื่องการเปิดเผยตามความร่วมมือระหว่างประเทศชัดเจน รวมทั้งให้คณะกรรมการไว้อย่างกว้าง จึงอาจทำให้สามารถเปิดเผยข้อมูลตามความร่วมมือแบบต่าง ๆ ที่ศึกษาในงานวิจัยนี้ ซึ่งการเปิดเผยตามความร่วมมือบางประการส่งผลกระทบต่อสิทธิมนุษยชน

สรุปและอภิปรายผล

การอภิปรายผลจะจำแนกตามวัตถุประสงค์ของการวิจัยดังนี้

1. จากวัตถุประสงค์การศึกษาข้อ 1 พบว่า มาตรการความร่วมมือระหว่างประเทศเกี่ยวกับการเข้าถึงข้อมูลข้ามพรมแดน มี 2 มาตรการ คือ มาตรการความร่วมมือทางอาญาในการดำเนินมาตรการช่วยเหลือระหว่างประเทศ (Mutual legal assistance (MLA) และมาตรการฝ่ายเดียว (Unilateral measure) ซึ่งจะวิเคราะห์เปรียบเทียบในแง่ประสิทธิภาพและผลกระทบต่อสิทธิมนุษยชน ดังนี้

1.1 ความร่วมมือทางอาญาในการดำเนินมาตรการช่วยเหลือระหว่างประเทศ (Mutual legal assistance (MLA) ซึ่งเมื่อทำเป็นความตกลงระหว่างประเทศในรูปสนธิสัญญาทวิภาคีหรือพหุภาคีจะเรียกว่า สนธิสัญญาความร่วมมือทางอาญาระหว่างประเทศ “Mutual legal assistance treaty” (MLAT) โดยจะมีขอบเขตในเรื่อง การให้ความร่วมมือในการสืบสวนสอบสวน พยานหลักฐาน หรือร่วมมือตามมาตรการย่อยอื่น เช่น

- สนธิสัญญาสหภาพยุโรปว่าด้วยความร่วมมือในทางอาญา (The European Convention on Mutual Assistance in Criminal Matters) กำหนดกรอบความร่วมมือในการให้ความช่วยเหลือทางกฎหมายร่วมกันระหว่างประเทศสมาชิก ซึ่งมีพันธกรณีจะให้ความร่วมมืออย่างโดยกำหนดมาตรการในระดับกว้างที่สุดที่เป็นไปได้ (Widest measure) เพื่อการสืบสวนสอบสวน ดำเนินคดีกับออาชญากรรม โดยมีเงื่อนไขสำคัญคือ ประเทศผู้ร้องขอ (Requesting state) และประเทศผู้รับการร้องขอ (Requested state) ต้องมีความตกลงร่วมกัน ด้วยการส่งคำร้องขอและพิจารณาคำร้อง ตามหลักต่างตอบแทนและตามความตกลงระกว่างกัน สนธิสัญญานี้เปิดให้ประเทศนอกสหภาพยุโรปให้สัตยาบันด้วย ซึ่งมีประเทศนอกสหภาพยุโรปที่เข้าร่วมเช่น รัสเซีย อิสราเอล เกาหลีใต้ สำหรับไทยไม่ได้ให้สัตยาบันสนธิสัญญานี้

- สนธิสัญญาความร่วมมือในการดำเนินกระบวนการทางอาญาของอาเซียน (Treaty on Mutual Legal Assistance in Criminal Matters (MLAT) เป็นความตกลงของประเทศสมาชิกอาเซียน โดยไทยเข้าร่วมลงนามในปี ค.ศ. 2006 ขอบเขตความร่วมมือ ระบุในมาตรา 1 ว่า ประเทศสมาชิกจะดำเนินการให้ความร่วมมือในมาตรการช่วยเหลือกันทางด้านคดีอาญาอย่างกว้างเท่าที่สุดที่เป็นไปได้ รวมถึงความร่วมมือด้านสืบสวนสอบสวน การเก็บรวบรวมพยานหลักฐานหรือเอกสารจากบุคคล การจัดให้ซึ่งเอกสารต้นฉบับหรือสำเนา บันทึก และหลักฐานการสืบสวนและบ่งระบุตัวพยานและผู้ต้องสงสัย

เมื่อวิเคราะห์เนื้อหาของมาตรการ พบว่า MLAT เป็นความร่วมมือระหว่างประเทศเกี่ยวกับเรื่องทางอาญาแบบดั้งเดิม ที่ประเทศต่างๆยังคงใช้เป็นวิธีการหรือช่องทางหลักของการแสวงหาพยานหลักฐาน (UNODC, 2013) แต่มีข้อจำกัดหลายประการ เช่น

- ไม่ได้กำหนดหลักเกณฑ์เกี่ยวกับความร่วมมือในด้านการเข้าถึงข้อมูลคอมพิวเตอร์ข้ามพรมแดน (Cross border data access) (Swire and Hemmings, 2017) จะเห็นได้จากสนธิสัญญา MLAT สหภาพยุโรปและอาเซียน ไม่ได้ระบุถึงความร่วมมือในการเข้าถึงข้อมูลคอมพิวเตอร์ที่ตั้งอยู่ใน

ประเทศสมาชิกอื่น หรือเข้าถึงข้อมูลข้ามพรมแดนไว้โดยตรง แม้ว่ามีบทบัญญัติความร่วมมือในแง่ของพยานหลักฐาน แต่ถ้อยคำตามตัวบทยังคงมุ่งเน้นการส่งเอกสารทางกายภาพ การสอบถามหรือส่งตัวบุคคล ฯลฯ ไม่ได้บ่งระบุมาตรการที่มีลักษณะเจาะจงทางเทคโนโลยีสารสนเทศหรือข้อมูลคอมพิวเตอร์ (Woods, 2015) เนื่องจากมาตรการ MLA มีโครงสร้างและหลักการที่เกิดขึ้นตั้งแต่ก่อนการแพร่หลายของการสื่อสารทางอินเทอร์เน็ต จึงไม่รองรับการร้องขอข้อมูลทางคอมพิวเตอร์จากรัฐที่มีจำนวนมากทั้งในแง่ความถี่และปริมาณ (Hill and Noyes, 2018)

- มาตรการ MLA อยู่บนพื้นฐานหลักการที่ว่าประเทศที่ร้องขอข้อมูลทราบว่าข้อมูลนั้นจัดเก็บที่ใดในประเทศผู้รับการร้องขอ เช่น เก็บไว้ที่ผู้ให้บริการรายใด อย่างไรก็ตามในสภาพแวดล้อมการใช้ข้อมูลคอมพิวเตอร์ซึ่งมีการเก็บข้อมูลในระบบคลาวด์เป็นการยากที่จะบ่งระบุที่ตั้งข้อมูลชัดเจน (Schwerha, 2010)

- กำหนดหลักการกว้างในลักษณะกรอบความร่วมมือ โดยให้ประเทศภาคีตกลงร่วมกันในการร่วมมือเป็นรายกรณีด้วยกระบวนการส่งคำร้องขอและพิจารณาคำร้องขอ การศึกษาในสหรัฐอเมริกาชี้ให้เห็นข้อจำกัดของ MLA ในแง่ที่อยู่บนหลักการต่างตอบแทน (Reciprocal) กล่าวคือ หากสหรัฐอเมริกาไม่ให้ความร่วมมือประเทศอื่นที่ขอเข้าถึงข้อมูลคอมพิวเตอร์ที่เก็บรักษาไว้โดยผู้ให้บริการสหรัฐอเมริกา รัฐบาลสหรัฐก็จะไม่ได้รับความร่วมมือในกรณีที่ประสงค์จะขอเข้าถึงข้อมูลที่เก็บรักษาไว้นอกประเทศ (Halefom, 2021)

- การแสวงหาหลักฐานเพื่อดำเนินคดีกับอาชญากรรมคอมพิวเตอร์ ในกรณีที่ข้อมูลหลักฐานอยู่ในความครอบครองของผู้ให้บริการที่อยู่นอกประเทศ หากใช้กระบวนการ MLA ซึ่งใช้เวลาและขั้นตอนอาจทำให้ไม่สามารถได้มาซึ่งหลักฐานอิเล็กทรอนิกส์เนื่องจากเกิดการแก้ไขเปลี่ยนแปลงหรือสูญหายของข้อมูลนั้น (Nojeim, 2015)

1.2 มาตรการฝ่ายเดียว (Unilateral measure) ในการเข้าถึงหรือได้มาซึ่งข้อมูลคอมพิวเตอร์ในวิชาการหมายความถึง การดำเนินมาตรการต่าง ๆ ของหน่วยงานรัฐประเทศหนึ่งที่ต้องการข้อมูลคอมพิวเตอร์ที่จัดเก็บในอีกประเทศหนึ่งเพื่อใช้ดำเนินคดี ในกรณีที่ไม่มีความตกลงระหว่างประเทศระดับทวิภาคีหรือพหุภาคี หรือในกรณีที่มีความตกลง MLAT แต่มีข้อจำกัดในด้านเวลาและกระบวนการทำให้ต้องดำเนินมาตรการฝ่ายเดียว (Tahraoui, 2016) ดังนั้น มาตรการฝ่ายเดียวจึงเป็นคำที่มีความหมายกว้างครอบคลุมการดำเนินการหลายอย่างของรัฐ ตัวอย่างเช่น การขอความร่วมมือไปยังผู้ให้บริการที่จัดเก็บข้อมูลในประเทศอื่นส่งข้อมูลให้หรือขอให้ถอดรหัสในกรณีที่ข้อมูลนั้นถูกเข้ารหัส (Encryption) การใช้กฎหมายภายในบังคับกับทรัพย์สินของผู้ให้บริการต่างประเทศในส่วนทรัพย์สินที่อยู่ในเขตแดนของประเทศที่ใช้มาตรการฝ่ายเดียว การฟ้องร้องหรือจับกุมลูกจ้างของผู้ให้บริการข้อมูลต่างประเทศ ซึ่งทำงานหรืออาศัยในประเทศที่ดำเนินมาตรการฝ่ายเดียว (Swire, 2012)

การวิเคราะห์เนื้อหาเปรียบเทียบมาตรการดังกล่าวในสองประเด็น พบว่า

(1) ในแง่ประสิทธิภาพของมาตรการ พบว่า มาตรการฝ่ายเดียว แก้ไขข้อจำกัดและอุปสรรคของมาตรการ MLA ดังกล่าวในผลการศึกษาข้อ 1.3 โดยเฉพาะอย่างยิ่ง การขาดความรวดเร็วในการเข้าถึงข้อมูลคอมพิวเตอร์ (Timely access) ซึ่งจัดเก็บโดยผู้ให้บริการที่อยู่นอกประเทศ เพราะเป็นมาตรการที่มุ่งเน้นความรวดเร็วเชิงกระบวนการและลดขั้นตอนการประสานงานขอให้ประเทศปลายทางดำเนินการทำให้สามารถเข้าถึงข้อมูลหลักฐานทางคอมพิวเตอร์ได้ก่อนมีการเปลี่ยนแปลงหรือลบ จึงเป็นการให้น้ำหนักกับการปราบปรามอาชญากรรมและมีประสิทธิภาพมากกว่ามาตรการ MLA

(2) ในแง่ของผลกระทบต่อสิทธิมนุษยชน เมื่อนำองค์ประกอบการชั่งน้ำหนักกฎหมายที่จำกัดสิทธิเสรีภาพจากกรอบแนวคิดมาทำการวิเคราะห์ประกอบกับวรรณกรรมที่เกี่ยวข้อง แยกพิจารณาได้ดังนี้

- การเข้าถึงข้อมูลตามมาตรการฝ่ายเดียวขึ้นอยู่กับการตกลงระหว่างหน่วยงานของประเทศผู้ขอข้อมูลกับผู้ให้บริการในอีกประเทศที่เก็บข้อมูลไว้ เป็นการดำเนินการระหว่างฝ่ายบริหารไม่มีการตรวจสอบโดยศาลหรือองค์กรอิสระ และเนื่องจากกระบวนการนี้ไม่มีกระบวนการที่ชัดเจน อาจดำเนินการโดยไม่เปิดเผย เจ้าของข้อมูลที่เป็นผู้ใช้บริการและภาคประชาสังคมอาจไม่สามารถทราบว่ามีการเข้าถึงข้อมูลโดยหน่วยงานต่างประเทศ เป็นอุปสรรคต่อการตรวจสอบโดยเอกชนที่ได้รับผลกระทบหรือภาคประชาสังคม ลักษณะดังกล่าวไม่สอดคล้องกับหลักการตรวจสอบถ่วงดุล (Council of Europe, 2016)

- มาตรการฝ่ายเดียวมีขอบเขตกว้างในแง่เป้าหมายข้อมูลที่อาจเข้าถึง อาจนำไปสู่การเข้าถึงข้อมูลที่กว้างเกินจำเป็นกับการสืบสวนอาชญากรรมอันเป็นเหตุให้ดำเนินมาตรการแต่ละครั้ง และ มีความกว้างในแง่วิธีการซึ่งอาจรวมถึงการใช้เทคนิคต่างๆ เช่น การถอดรหัส ฯลฯ จึงไม่สอดคล้องกับหลักการจำกัดสิทธิที่จะต้องมีขอบเขตแคบและจำกัด

- เนื่องจากความไม่ชัดเจนเจาะจงของมาตรการฝ่ายเดียว ส่งผลทางลบต่อผู้ให้บริการที่อาจไม่สามารถประเมินความเสี่ยงในการปฏิบัติตามหรือไม่ปฏิบัติตามมาตรการ เพราะหากยินยอมเปิดเผยหรือให้เจ้าหน้าที่รัฐประเทศอื่นเข้าถึงข้อมูล อาจฝ่าฝืนกฎหมายภายในของประเทศที่ผู้ให้บริการนั้นตั้งอยู่ แต่หากไม่ปฏิบัติตามคำขอฝ่ายเดียวก็มีความเสี่ยงฝ่าฝืนกฎหมายของประเทศที่ร้องขอเข้าถึงข้อมูล ดังตัวอย่างหน่วยงานรัฐบราซิลร้องขอเข้าถึงข้อมูลที่จัดเก็บโดยผู้ให้บริการในสหรัฐอเมริกา ซึ่งไม่ตกลงยอมตามคำขอเพราะเกรงจะฝ่าฝืนกฎหมายสหรัฐอเมริกา ส่งผลให้เกิดการดำเนินคดีตามกฎหมายบราซิล (Smith and Browne, 2019)

- ความร่วมมือตามมาตรการฝ่ายเดียวที่อาจเกิดขึ้นโดยการเจรจาระหว่างฝ่ายบริหารหรือเจ้าหน้าที่ของสองประเทศ โดยไม่มีกฎหมายระบุชัด ซึ่งไม่สอดคล้องกับหลักการจำกัดสิทธิมนุษยชนต้องเป็นไปโดยกฎหมายบัญญัติ

เมื่อนำมาตรการฝ่ายเดียวมาเปรียบเทียบกับมาตรการ MLA พบว่า เป็นที่ยอมรับทางกฎหมายระหว่างประเทศและเป็นแนวทางหลักของความร่วมมือในปัจจุบัน โดยเป็นการขอให้ประเทศปลายทางที่

ข้อมูลจัดเก็บอยู่ดำเนินการซึ่งเป็นไปภายใต้กฎหมายภายในของประเทศผู้รับคำขอ มีกระบวนการขั้นตอนชัดเจน สามารถตรวจสอบได้ จึงสอดคล้องกับหลักการจำกัดสิทธิโดยกฎหมายบัญญัติ หลักความชัดเจนของกระบวนการขั้นตอน

2. จากวัตถุประสงค์การศึกษาข้อ 2 พบว่า ในกรอบการดำเนินการของสหประชาชาติเกี่ยวกับอาชญากรรมไซเบอร์ ได้มีการจัดทำร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยี (Draft of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes) หมวด 4 ว่าด้วย “ความร่วมมือระหว่างประเทศ” (International cooperation) ซึ่งผลการศึกษาในส่วนมาตรการร่วมมือด้านการเข้าถึงข้อมูลทางระบบคอมพิวเตอร์ พบร่างมาตราที่เกี่ยวข้องคือ หลักทั่วไปมาตรา 56 หลักการเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 68 มาตรา 70 และมาตรา 72 โดยจำแนกวิเคราะห์ดังนี้

(1) หลักการทั่วไปของความร่วมมือ ปรากฏใน ร่างมาตรา 56 ของสนธิสัญญาสหประชาชาติกำหนดหลักการเกี่ยวกับความร่วมมือระหว่างประเทศทั่วไปในการป้องกันและปราบปรามอาชญากรรมเทคโนโลยี มีหลักการสำคัญว่า ประเทศสมาชิกจะดำเนินการให้ความร่วมมือระหว่างกัน ในการดำเนินมาตรการป้องกันปราบปรามอาชญากรรรมอิเล็กทรอนิกส์ในด้านสืบสวนสอบสวน การบังคับใช้กฎหมาย การรวบรวม แลกเปลี่ยน พยานหลักฐาน การดำเนินคดีกับอาชญากรรม...”

จากเนื้อหาตัวบทมาตรา 56 พบว่าไม่ได้ระบุถึงการเข้าถึงข้อมูลคอมพิวเตอร์ แต่เป็นหลักทั่วไประบุขอบเขตความร่วมมือเกี่ยวกับพยานหลักฐานทางอิเล็กทรอนิกส์ซึ่งรวมถึงการเข้าถึงข้อมูลคอมพิวเตอร์ สำหรับประเด็นที่ว่าอาชญากรรมไซเบอร์อันเป็นเหตุแห่งการขอความร่วมมือนั้น ร่างยังไม่เป็นที่สุด จากความเห็นผู้แทนประเทศที่เข้าร่วมการร่างแบ่งเป็นสองฝ่าย (United Nations, 2022) ฝ่ายหนึ่งเห็นว่าอาชญากรรมในขอบเขตความร่วมมือจำกัดเฉพาะฐานความผิดที่ระบุในสนธิสัญญานี้ ซึ่งเป็นอาชญากรรมที่กระทบต่อความปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์ เช่น การโจรกรรมข้อมูลคอมพิวเตอร์ โดยไม่รวมถึงความผิดเกี่ยวกับเนื้อหาเช่น การโพสต์แชร์ข้อมูลหรือหมิ่นประมาทออนไลน์ แต่อีกฝ่ายเห็นว่ามาตรการความร่วมมือนี้ควรเป็นไปอย่างกว้างเพื่อป้องกันและปราบปรามอาชญากรรมใดก็ตามที่กระทำผ่านระบบคอมพิวเตอร์ แม้ว่าไม่ระบุในสนธิสัญญานี้ ในแง่สิทธิมนุษยชน ความร่วมมือตามสนธิสัญญานี้ประกอบด้วยมาตรการหลากหลายรวมถึงการเข้าถึงข้อมูลคอมพิวเตอร์ การขยายขอบเขตความร่วมมือไปครอบคลุมอาชญากรรมที่ไม่ระบุเจาะจงอาจทำให้ประเทศสมาชิกบางแห่งใช้มาตรการนี้โดยมิชอบ (Abuse) ซึ่งอาจส่งผลต่อการสื่อสารของสื่อมวลชน ข้อมูลส่วนบุคคลของผู้ใช้บริการ การสื่อสารที่เป็นความผิดอื่นนอกเหนือจากความผิดต่อความมั่นคงของระบบหรือข้อมูลคอมพิวเตอร์

(2) หลักการเกี่ยวกับการขอข้อมูลหรือเข้าถึงข้อมูลแบ่งเป็น 4 มาตราดังนี้ 1. ร่างมาตรา 68 มีหลักว่า ประเทศสมาชิกอาจร้องขอให้ประเทศสมาชิกดำเนินการออกคำสั่งหรือดำเนินการตามกฎหมายภายในของประเทศผู้รับคำร้อง เพื่อให้มีการเก็บรักษาไว้ซึ่งข้อมูลคอมพิวเตอร์ในระบบหรืออุปกรณ์ที่ตั้งอยู่

ในเขตอำนาจของประเทศผู้รับคำร้องขอ 2. ร่างมาตรา 69 ในการดำเนินการความร่วมมือตามมาตรา 68 ประเทศผู้รับการร้องขอต้องเปิดเผยข้อมูลจราจรคอมพิวเตอร์ที่เกี่ยวกับข้อมูลการสื่อสารนั้น 2. ร่างมาตรา 70 มีหลักว่า ประเทศสมาชิกอาจร้องขอให้ประเทศสมาชิก ทำการค้น (Search) หรือเข้าถึง (Access) หรือยึด (Seize) หรือการกระทำอื่นในลักษณะเดียวกัน และ เปิดเผย (Disclose) ข้อมูลคอมพิวเตอร์ที่เก็บไว้ในระบบหรืออุปกรณ์คอมพิวเตอร์ในเขตอำนาจประเทศสมาชิกนั้น 3. ร่างมาตรา 73 มีหลักว่า ประเทศสมาชิกมีพันธกรณีในการให้ช่วยเหลือประเทศสมาชิกอื่นเกี่ยวกับการเก็บรวบรวมข้อมูลจราจรคอมพิวเตอร์แบบตามเวลาจริง (Real time traffic data collection) 4. ร่างมาตรา 72 มีหลักว่า ประเทศสมาชิกมีสิทธิเข้าถึงข้อมูลคอมพิวเตอร์ที่เก็บไว้ในระบบคอมพิวเตอร์ใด ๆ ซึ่งเปิดเผยหรือเข้าถึงได้โดยสาธารณะโดยไม่ต้องดำเนินการร้องขอต่อประเทศสมาชิกอื่น และมีสิทธิเข้าถึงข้อมูลคอมพิวเตอร์ผ่านระบบการสื่อสารใดๆ ที่จัดเก็บไว้อุปกรณ์ที่ตั้งอยู่ในประเทศสมาชิกอื่น ต่อเมื่อได้รับความยินยอมจากผู้มีสิทธิตามกฎหมายของระบบคอมพิวเตอร์นั้น หลักการเกี่ยวกับการเข้าถึงข้อมูลจำแนกวิเคราะห์ได้เป็นสองกลุ่มคือ

กลุ่มที่ 1 มาตรการเข้าถึงหรือขอข้อมูลผ่านกระบวนการของประเทศผู้รับคำขอพบได้จาก ร่างมาตรา 68 จัดเป็นความร่วมมือในการขอให้เก็บรักษาข้อมูล (Preservation of computer data) โดยการขอให้ให้ประเทศผู้รับคำขอระงับการแก้ไขเปลี่ยนแปลงหรือให้เก็บรักษาข้อมูลไว้ แต่ยังไม่มีการเข้าถึงหรือขอให้ส่งข้อมูล ซึ่งอาจดำเนินการต่อไปในการขอความร่วมมือค้นหรือเข้าถึงข้อมูลดังกล่าวตามร่างมาตรา 70 นอกจากนี้ ยังอาจมีการขอความร่วมมือให้ส่งข้อมูลจราจรคอมพิวเตอร์แบบเรียลไทม์ตามมาตรา 73 เมื่อเปรียบเทียบเนื้อหากับมาตรการ MLA พบข้อแตกต่างคือ ร่างสหประชาชาติระบุเจาะจง ถึงข้อมูลคอมพิวเตอร์ และ มาตรการร่วมมือด้านการขอให้เก็บรักษาและเข้าถึงข้อมูลไว้โดยเฉพาะซึ่งหลักการนี้ไม่ปรากฏในสนธิสัญญา MLAT สหภาพยุโรปและอาเซียน ในแง่หนึ่งจึงเป็นมาตรการที่ปรับปรุงให้มีประสิทธิภาพขึ้นกว่ามาตรการ MLA แต่หากวิเคราะห์การชั่งน้ำหนักระหว่างการสืบสวนอาชญากรรมกับการคุ้มครองสิทธิบุคคล ตามหลักสิทธิมนุษยชนในแง่ความได้สัดส่วน พบว่า ร่างมาตรา 68 และ 70 ไม่ได้เปิดทางให้เจ้าหน้าที่ของประเทศที่ร้องขอ ทำการเข้าถึงข้อมูลคอมพิวเตอร์ได้เอง แต่เป็นการขอให้หน่วยงานตามกฎหมายของประเทศผู้รับคำขอในการดำเนินการ โดยในกรณีที่ข้อมูลเก็บอยู่ในความครอบครองของผู้ให้บริการในประเทศผู้รับคำร้องขอ ร่างมาตราดังกล่าวไม่ได้กำหนดว่าประเทศผู้ร้องขอสามารถดำเนินการขอข้อมูลจากผู้ให้บริการโดยตรง แต่ยังคงต้องผ่านกระบวนการและการดำเนินการของประเทศที่รับคำขอ นอกจากนั้น ความร่วมมือตามร่างมาตรา 68 70 และ 73 ยังปรากฏในกรอบความร่วมมือระหว่างประเทศอื่น เช่น ความร่วมมือในกรอบสนธิสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป อย่างไรก็ตาม ในส่วนของการขอข้อมูลจราจรคอมพิวเตอร์แบบเรียลไทม์ ซึ่งแม้ว่าเป็นข้อมูลเมทาดาทา (Metadata) ซึ่งไม่ใช่เนื้อหาการสื่อสาร (Content) แต่ในแง่สิทธิมนุษยชน การได้มาซึ่งข้อมูลดังกล่าวอาจส่งผลกระทบต่อสิทธิเสรีภาพในหลายมิติ ดังจะเห็นได้จากข้อมติสมัชชาใหญ่แห่งสหประชาชาติ เกี่ยวกับความเป็นส่วนตัวในยุคดิจิทัล (United Nations,2020) วางแนวทางว่า ข้อมูลเมทาดาทา (Metadata)

บางชนิดเมื่อนำมาประมวลรวมกัน อาจบ่งชี้หรือทำให้เห็นถึงข้อมูลส่วนบุคคลที่มีความ “อ่อนไหว” (Sensitive) ไม่น้อยไปกว่าเนื้อหาการสื่อสาร (content data) เช่น ข้อมูลจราจรคอมพิวเตอร์ ที่นำมาวิเคราะห์บ่งชี้ พฤติกรรมทางสังคม ความชื่นชอบของบุคคล สำหรับคณะมนตรีสิทธิมนุษยชนสหประชาชาติมีความเห็นทำนองเดียวกัน ว่าข้อมูลเมทาดาทา อาจมีลักษณะ “อ่อนไหว” โดยเฉพาะเมื่อนำไปบ่งชี้พฤติกรรม ความเคลื่อนไหวของบุคคล กิจกรรมทางการเมือง ความชื่นชอบส่วนบุคคล และ เอกลักษณ์ของบุคคล (United Nations, 2021) ดังนั้น มาตรการเข้าถึงหรือได้มาซึ่งข้อมูลจราจรคอมพิวเตอร์จึงทำให้ทราบถึงข้อมูลในมิติชีวิตของบุคคลอย่างกว้างกว่าเนื้อหาการสื่อสารเรื่องใดเรื่องหนึ่ง

กลุ่มที่ 2 มาตรการเข้าถึงหรือขอข้อมูลข้ามพรมแดนโดยตรง ร่างมาตรา 72 ซึ่งให้สิทธิประเทศสมาชิกทำการเข้าถึงหรือได้มาซึ่งข้อมูลคอมพิวเตอร์ที่จัดเก็บในประเทศสมาชิกอื่น (Cross-border access to stored computer data) โดยอาจดำเนินการทางเทคนิคจากระยะไกล (Remote access) และไม่ต้องขอให้หน่วยงานของประเทศปลายทางดำเนินการ แต่มีเงื่อนไขจำแนกตามประเภทข้อมูลได้สองกรณีคือ 1 กรณีข้อมูลที่เปิดเผยต่อสาธารณะ กำหนดให้สิทธิเข้าถึงได้โดยไม่ต้องขออนุญาตหรือขอให้หน่วยงานประเทศปลายทางดำเนินการ 2. กรณีข้อมูลที่จัดเก็บหรืออยู่ในอุปกรณ์ของบุคคลใดในประเทศปลายทาง เช่น ผู้ให้บริการหรือผู้ประกอบการเอกชน ประเทศสมาชิกสามารถเข้าถึงได้เองภายใต้เงื่อนไขขอความยินยอมจากผู้มีสิทธิ

จากหลักการเข้าถึงข้อมูลตามมาตราในกลุ่มที่ 2 ในแง่ประสิทธิภาพของมาตรการ มาตรา 72 แก้ไขข้อจำกัดและอุปสรรคของมาตรการ MLA เนื่องจากเป็นการร้องขอโดยตรงระหว่างประเทศที่ร้องขอกับผู้ให้บริการในต่างประเทศ โดยไม่ผ่านกระบวนการและขั้นตอนของประเทศปลายทาง จึงมีความรวดเร็วในการเข้าถึงข้อมูลคอมพิวเตอร์ (Timely access) จัดเป็นมาตรการที่ให้น้ำหนักกับประสิทธิภาพในการปราบปรามอาชญากรรม ในแง่ผลกระทบต่อสิทธิมนุษยชน ร่างมาตรา 72 กำหนดหลักการใหม่ที่ไม่ปรากฏใน MLA และมีลักษณะเทียบเคียงได้กับมาตรการฝ่ายเดียว (Unilateral measure) โดยในกรณีที่รัฐผู้ประสงค์ได้ข้อมูลจะเข้าถึงข้อมูลซึ่งอยู่ในความครอบครองของผู้ให้บริการในอีกประเทศ จะดำเนินการร้องขอความยินยอมไปยังผู้ให้บริการโดยไม่ต้องผ่านหรืออาศัยการดำเนินการของหน่วยงานรัฐประเทศปลายทางที่ผู้ให้บริการนั้น จึงมีหลักการที่ส่งผลกระทบต่อสิทธิมนุษยชนมากกว่ามาตรการ MLA ในหลายแง่มุม เมื่อนำองค์ประกอบการชั่งน้ำหนักกฎหมายที่จำกัดสิทธิเสรีภาพจากกรอบแนวคิดมาทำการวิเคราะห์ประกอบกับวรรณกรรมที่เกี่ยวข้องจะแยกพิจารณาได้ดังนี้

- การเข้าถึงข้อมูลโดยตรงในกรณีที่จัดเก็บในระบบของผู้ให้บริการเอกชน รัฐผู้ขอมีสิทธิเข้าถึงได้เองโดยขอความยินยอมจากผู้มีสิทธิ ซึ่งกระบวนการนี้ไม่มีการขอหมายศาล จึงไม่สอดคล้องกับหลักเกณฑ์ตรวจสอบถ่วงดุลโดยศาล (Judicial review) หรือองค์กรอิสระ (Independent review) (Council of Europe, 2016)

- องค์กรสิทธิมนุษยชนระหว่างประเทศ เช่น “Article19” แสดงความไม่เห็นด้วยกับร่างสนธิ

สัญญาในหลายประเด็น เช่น การเปิดทางให้เจ้าหน้าที่แสวงหาพยานหลักฐานในลักษณะสอดแนม (Surveillance) โดยไม่ได้กำหนดกระบวนการตรวจสอบที่เหมาะสม (Article19, 2022)

- องค์กรสิทธิมนุษยชนระหว่างประเทศ หลายองค์กร (เช่น Privacy International (PI) และ Electronic Frontier Foundation) ร่วมกันจัดทำรายงานความเห็นต่อร่างสนธิสัญญาอาชญากรรมไซเบอร์สหประชาชาติ โดยมีความเห็นและข้อกังวลในส่วนร่างมาตรการเข้าถึงข้อมูลว่า จากตัวบทที่กว้างอาจเปิดทางให้รัฐที่ประสงค์เข้าถึงข้อมูลใช้วิธีการและมีเป้าหมายอย่างกว้าง เปรียบเหมือนการแฮกโดยภาครัฐ (Government hacking) (Privacy International, 2022).

- การกำหนดองค์ประกอบของการเข้าถึงข้อมูลที่อยู่ในความครอบครองของผู้ประกอบการเอกชนเป็นถ้อยคำที่กว้าง ไม่ระบุวิธีการที่รัฐต่างประเทศจะนำมาใช้เพื่อเข้าถึง ไม่ได้ระบุข้อจำกัดการใช้วิธีการทางเทคนิคบางประการ หากข้อมูลเข้ารหัสอาจใช้วิธีการถอดรหัส (Decrypt) หรือการใช้รหัสที่ทำให้เกิดช่องโหว่ในระบบที่ต้องการเข้าถึง (Article 19, 2023)

- ตามหลักการชั่งน้ำหนักด้านสิทธิมนุษยชน มาตรการเข้าถึงข้อมูลเพื่อสืบสวนสอบสวนต้องเป็นไปอย่างจำกัดและเจาะจง หากให้อำนาจเข้าถึงได้กว้าง นอกจากส่งผลในแง่สิทธิในความเป็นอยู่ส่วนตัวยังส่งผลกระทบต่อสิทธิมนุษยชนในการแสดงความคิดเห็น (United Nations Special Rapporteur on freedom of opinion and expression ,2015) เมื่อพิจารณาหลักการเข้าถึงข้อมูลโดยตรง พบว่าไม่ระบุขอบเขตอย่างจำกัด ในแง่เป้าหมายและขอบเขตข้อมูลที่จะเข้าถึง และไม่ได้จำกัดวิธีการเข้าถึง ดังนั้น รัฐที่เข้าถึงอาจเข้าถึงข้อมูลเป้าหมายโดยอ้างความจำเป็นหรือความเกี่ยวข้องกับเรื่องที่จะสืบสวนอย่างกว้างทำให้ได้มาหรือเข้าถึงข้อมูลส่วนบุคคลอื่น

- แม้ว่าความร่วมมือในการเข้าถึงข้อมูลที่อ้างอิงเหตุผลด้านความรวดเร็วในการสืบสวนสอบสวนอาชญากรรม แต่มาตรการดังกล่าวยังคงต้องอยู่ภายใต้หลักความได้สัดส่วน ซึ่งคณะกรรมมาธิการต่อต้านการก่อการร้ายสหประชาชาติ เห็นว่าการให้อำนาจหน่วยงานบังคับใช้กฎหมายเข้าถึงข้อมูลได้อย่างรวดเร็วอาจส่งผลกระทบในอีกหลายแง่มุม เช่น กระทบต่อกฎหมายสารบัญญัติ (United Nations Security Council Counter-Terrorism Committee Executive Directorate, 2022)

- ในทางวิชาการมีความเห็นเกี่ยวกับการให้อำนาจเข้าถึงโดยไม่ผ่านกระบวนการหรือขั้นตอนตามกฎหมายภายในว่าเป็นกรณีที่ไม่สอดคล้องกับหลักการตรวจสอบถ่วงดุลตามหลักสิทธิ มีข้อเสนอให้ความร่วมมือในกรอบสหประชาชาติควรต้องทบทวนหลักการส่วนนี้ (Albader, 2022)

- คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป มีข้อแนะนำ โดยสนับสนุนหลักการความร่วมมือแสวงหาพยานหลักฐานข้ามพรมแดน แต่เห็นว่าในส่วนมาตรการเข้าถึงข้อมูลโดยตรง ไม่ได้สัดส่วนกับผลกระทบต่อสิทธิในข้อมูลส่วนบุคคล เนื่องจากมีขอบเขตที่กว้างไม่เจาะจงและขาดการตรวจสอบถ่วงดุล (European Data Protection Supervisor, 2022)

นอกจากนี้ ในแง่ของผู้ให้บริการที่ได้รับคำร้องขอจากหน่วยงานรัฐประเทศอื่น หากมาตรา 72 มี

ผลบังคับและประเทศที่ผู้ให้บริการตั้งอยู่ได้ให้สัตยาบันจะส่งผลว่าประเทศนั้นมีพันธกรณีที่จะต้องปรับปรุงกฎหมายภายในเพื่อให้การส่งข้อมูลของผู้ให้บริการชอบด้วยกฎหมาย ซึ่งจะส่งผลกระทบต่อผู้ใช้บริการเจ้าของข้อมูลที่ได้รับผลกระทบอาจไม่สามารถใช้กลไกทางกฎหมายภายในต่อผู้ให้บริการที่เปิดเผยข้อมูลตามคำร้องขอนั้นได้อีกด้วย

จากการวิเคราะห์ดังกล่าวจึงเห็นได้ว่า หลักการความร่วมมือตามร่างมาตรากลุ่มที่ 2 ไม่สอดคล้องกับองค์ประกอบการชั่งน้ำหนักตามหลักสิทธิมนุษยชนหลายประการ เช่น หลักการตรวจสอบถ่วงดุลโดยศาลหรือองค์กรอิสระ หลักความเจาะจงและจำกัดในแง่ขอบเขตเป้าหมาย (Target) และวิธีการของการเข้าถึงหรือได้มาซึ่งข้อมูล จึงเป็นการให้น้ำหนักกับการสืบสวนสอบสวนโดยไม่ได้สัดส่วนกับการคุ้มครองสิทธิมนุษยชน

สำหรับ กฎหมายไทยที่มีผลบังคับในปัจจุบันเกี่ยวกับการเข้าถึงข้อมูลส่วนบุคคล ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีความเกี่ยวข้องเมื่อหน่วยงานรัฐต่างประเทศขอข้อมูลหรือเข้าถึงข้อมูลในความครอบครองของผู้ให้บริการในประเทศไทย โดยหากผู้ให้บริการทำตามคำขอจะเป็นการเปิดเผยข้อมูลและเป็นการส่งข้อมูลไปต่างประเทศ ซึ่งพระราชบัญญัตินี้ วางหลักห้ามผู้ให้บริการเปิดเผยหรือโอนข้อมูลไปต่างประเทศ ตามมาตรา 28 ภายใต้เงื่อนไขว่าประเทศปลายทางต้องมีมาตรฐานคุ้มครองข้อมูลที่เหมาะสม ตามหลักเกณฑ์ที่คณะกรรมการกำหนดในมาตรา 16 (5) ทั้งนี้มาตรการคุ้มครองที่เหมาะสมมีความหมายมุ่งเน้นแง่ความปลอดภัย (Security) (คณาธิป ทองรวีวงศ์, 2564) โดยไม่ได้มุ่งเน้นถึงมาตรการคุ้มครองในมิติสิทธิมนุษยชนเช่นหลักความได้สัดส่วน จึงทำให้คณะกรรมการฯ สามารถกำหนดเกณฑ์การโอนหรือส่งข้อมูลให้รัฐบาลต่างประเทศที่มีคำร้องขอได้ หากกำหนดมาตรการรักษาความปลอดภัย ส่งผลให้โครงสร้างกฎหมายไทยเกี่ยวกับข้อมูลส่วนบุคคลที่เป็นอยู่เอื้ออำนวยให้สามารถเปิดเผยข้อมูลส่วนบุคคลในประเทศหรือที่อยู่ในครอบครองของผู้ให้บริการในประเทศ แก่รัฐบาลต่างประเทศตามความร่วมมือระหว่างประเทศแบบต่างๆ ที่ศึกษาในงานวิจัยนี้คือ (1) รัฐต่างประเทศเข้าถึงข้อมูลโดยมีคำขอบนพื้นฐานความตกลง MLAT (2) รัฐต่างประเทศเข้าถึงข้อมูลโดยการดำเนินการฝ่ายเดียว (Unilateral) (3) การเข้าถึงข้อมูลตามหลักการของร่างสนธิสัญญาสหประชาชาติ รวมถึงการเข้าถึงโดยตรงตามมาตรา 72 จากเงื่อนไขกฎหมายไทยในปัจจุบันดังกล่าว ในแง่หนึ่งอาจพิจารณาได้ว่ากฎหมายมีเงื่อนไขที่ยืดหยุ่นและเปิดทางให้เกิดความร่วมมือแสวงหาหลักฐานซึ่งเป็นการให้น้ำหนักกับการบังคับใช้กฎหมายแต่ในอีกแง่หนึ่งอาจพิจารณาได้ว่าเป็นการเปิดทางให้เข้าถึงข้อมูลส่วนบุคคลโดยมีข้อจำกัดและเงื่อนไขการคุ้มครองสิทธิที่เข้มงวดน้อยกว่ากฎหมายสหภาพยุโรป ซึ่งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรปให้ความเห็นแย้งมาตรการเข้าถึงโดยตรงดังที่วิเคราะห์มาแล้ว

ข้อเสนอแนะ

เมื่อพิจารณาถึงความสำคัญในการป้องกันปราบปรามอาชญากรรมไซเบอร์ในการแสวงหาหลักฐาน ประกอบกับการสร้างความสมดุลกับสิทธิมนุษยชนแล้วเห็นว่า ความร่วมมือระดับพหุภาคีตาม

กรอบองค์กรระหว่างประเทศเช่นสหประชาชาติมีความจำเป็นต่อประเทศไทย ซึ่งแม้ไม่ปรากฏว่ามีส่วนร่วมในการร่างสนธิสัญญาดังกล่าวแต่เมื่อสหประชาชาติเปิดให้ประเทศต่าง ๆ ให้สัตยาบันแล้วจะมีข้อเสนอแนะเชิงนโยบายต่อภาครัฐ ดังนี้

- เสนอให้ดำเนินการให้สัตยาบันในส่วนหลักการความร่วมมือในการเข้าถึงข้อมูลตามมาตรา 68 และ 70 ซึ่งเป็นมาตรการที่พัฒนาขึ้นจาก MLA โดยไม่มีลักษณะที่กระทบต่อสิทธิมนุษยชนจนเกินความจำเป็นและได้สัดส่วน แต่ควรตั้งข้อสงวน (Reservation) ในส่วนของมาตรการเข้าถึงข้อมูลข้ามพรมแดนโดยตรง ตามมาตรา 72 ซึ่งผลการศึกษาประเมินว่ามีความไม่สอดคล้องกับหลักความจำเป็นและได้สัดส่วนในหลายองค์ประกอบ เช่น ความกว้างและไม่เจาะจงในแง่ขอบเขตเป้าหมาย วิธีการ ขาดการตรวจสอบถ่วงดุลโดยศาลหรือองค์กรอิสระ

- เมื่อให้สัตยาบันและมีความผูกพันตามมาตรการแสวงหาข้อมูลโดยกระบวนการร้องขอตามกรอบสหประชาชาติมาตรา 68 และ 70 แล้ว เสนอให้กำหนดนโยบายและกฎหมายให้มีความชัดเจนในการที่จะไม่ให้หน่วยงานรัฐใช้มาตรการฝ่ายเดียว (Unilateral measure) ซึ่งผลการศึกษาประเมินว่ามาตราฝ่ายเดียวมีความไม่สอดคล้องกับหลักความจำเป็นและได้สัดส่วนในหลายองค์ประกอบ เช่น การจำกัดสิทธิโดยไม่มีกฎหมายบัญญัติชัดเจน ความกว้างและไม่เจาะจงในแง่ขอบเขตเป้าหมาย วิธีการ ขาดการตรวจสอบถ่วงดุลโดยศาลหรือองค์กรอิสระ โดยมีข้อเสนอสองแนวทางคือ (1) กำหนดเป็นกฎหมายเฉพาะ ที่วางหลักการเรื่องการเปิดเผยข้อมูลส่วนบุคคลตามคำร้องขอจากหน่วยงานต่างประเทศ (2) แก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลให้ชัดเจนว่าการเปิดเผยข้อมูลส่วนบุคคลตามคำขอรัฐบาลต่างประเทศจะทำได้ต่อเมื่อเป็นไปตามหลักการและแนวทางของความร่วมมือตามแนวทางมาตรา 68 และ 70 และกำหนดในตัวบทให้ชัดเจนว่าไม่รวมถึงการเปิดเผยข้อมูลตามมาตรการฝ่ายเดียวและการเข้าถึงโดยตรงของหน่วยงานรัฐต่างประเทศ

เอกสารอ้างอิง

คณาธิป ทองรวีวงศ์. (2564). หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล. กรุงเทพฯ : สำนักพิมพ์นิติธรรม.

Albader, F. (2022). The Pivotal Role of International Human Rights Law in Defeating Cybercrime. Vanderbilt Transnational Law, 55(5), 1115-1128.

Article19. (2022). UN: Cybercrime treaty must enhance human rights protections. Retrieved from https://www.article19.org/resources/

Article 19. (2023). Article 19’s comments on the consolidated negotiating document on the elaboration of a comprehensive international convention on countering the use of information communications technologies for criminal purposes.

Bloustein, E. (1984). Privacy as an Aspect of Human Dignity. “Philosophical Dimensions of privacy: An Anthology”, Schoeman, Ferdinand (ed.), UK: Cambridge University Press.

Cate, F. H. (1995). “The EU Data Protection Directive, Information Privacy, and the Public Interest”. Iowa Law Review, 80 (1), 431 - 443.

Council of Europe. (2016). Mass surveillance - Who is watching the watchers?. Council of Europe.

Fromholz, J. M. (2000). The European Union data privacy directive. Berkeley technology law journal, 15(1), 460 - 484.

Hannah, A. (1973). The Human Condition. Chicago : University of Chicago Press.

Donnelly, J. (1982). Human Rights and Human Dignity. The American Law Review, 76(2), 303-316.

Tahraoui, M. (2016). Unilateralism Ahead? Human Rights, Digital Surveillance and the “Extraterritorial Question” in International Law. Retrieved from https://voelkerrechtsblog.org/unilateralism-ahead

European Data Protection Supervisor. (2022). Opinion 9/2022. Retrieved from http://edps.europa.eu

Biegelman, T. (2009). Identity theft Handbook Detection, Prevention and Security. New Jersey : John Wiley & Sons, Inc.

Conkey, C. (2007). Assessing Identity-Theft Costs. Retrieved from https://www.wsj.com/articles/SB119621922590906207

European Data Protection Supervisor. (2022). Opinion 9/2022. Retrieved from http://edps.europa.eu

Hoofnagle, J.(2007). Identity theft: Making the Known Unknowns Known. Harvard Journal of Law & Technology, 21(1), 98-112.

Halefom H. A.(2021). Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives, International Journal of Law and Information Technology, 29(2), 118–153.

Jonker, N. (2007) Payment instruments as perceived by consumers - Results from a household survey. De Economist, 155(3), 271-303.

Listerman, R & Romesberg, J. (2009). Are we safe yet? Creating a culture of security is key to stopping a data breach. Strategic Finance, 91(1), 27-38.

Nojeim,G. (2015). MLAT Reform: A Straw Man Proposal. Retrieved from. https://cdt.org/insights/mlat -reform-a-straw-man-proposal/a (UN-Backed) Global Treaty on Cybercrime. Vanderbilt Journal of Transnational Law, 55, 1117.

Hill, J. and Noyes, M. (2018). Rethinking Data, Geography, and Jurisdiction: Towards A Common Framework for Harmonizing Global Data Flow Controls. Washington D.C. : New America and Cybersecurity Initiative.

Office of the High commissioner for human rights,1988). CCPR General comment No.16: Article 17 (Right to privacy). Retrieved from https://www.ohchr.org/en/treaty-bodies/general-comments.

Privacy International (2022). Privacy International and Electronic Frontier Foundation's comments on the consolidated negotiating document of the UN Cybercrime Treaty. Retrieved from https://privacyinternational.org/sites/default/files/

Rubenfield, J. (1989). The Right of Privacy. Harvard Law Review, 102(4), 737-807.

Schwerha, J. (2010) Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from Cloud Computing Providers. Strasbourg : Council of Europe.

Smith, B. and Browne, C. (2019). Tools and Weapons: The Promise and the Peril of the Digital Age. Hodder & Stoughton.

Swire, P. (2012). From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud. International Data Privacy Law, 2(4), 200-206.

Swire, P., and Hemmings, J. (2017). Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program. NYU Annual Survey of American Law, 71(1), 688-738.

Sproule S & Archer, N. (2010) Measuring identity theft and identity fraud. International Journal of Business Governance and Ethics, 5(1), 51-63.

Schoeman, F. (1984). Philosophical Dimensions of privacy: An Anthology. UK : Cambridge University Press.

Solove, D. (2006). A Taxonomy of Privacy. The University of Pennsylvania Law Review, 154(3), 477 - 560.

UNODC. (2013). Comprehensive study of the problem of cybercrime and responses to it by Member States. Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013

United Nations. (2022). Compilation of Draft provisions submitted by Member States on Criminalization. Retrieved from https://www.unodc.org/documents/Cybercrime /AdHocCommittee

United Nations. (2020). UN General Assembly Resolution on the Right to Privacy in the Digital Age. Retrieved from https://digitallibrary.un.org/record/3896430?ln=en

United Nations. (2021). UN Human Rights Council Resolution on the Right to Privacy in the Digital Age. UN Doc A/HRC/RES/48/4. Retrieved from https://www.ohchr.org /en/calls-for-input/2021/right-privacy-digital-age-report.

United Nations Special Rapporteur on freedom of opinion and expression. (2015). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Retrieved from https://www.ohchr.org /en/special-procedures/

United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED). (2022). The state of international cooperation for lawful access to digital evidence: Research Perspectives. Retrieved from https://www.un.org/security council/ctc/sites/www.un.org.securitycouncil.ctc/files.

Woods, A. (2015). Data Beyond Borders: Mutual Legal Assistance in the Internet Era. Global Network Initiative. Retrieved from https://globalnetworkinitiative.org/wp-content/uploads/2016/12/GNI-MLAT-Report.pdf

Warren D Samuel, Brandies D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193 - 220.

Westin, A. (1967). Privacy and Freedom. New York : Atheneum.

Yvonne, J. (2010). Media and Crimes, Second Edition. London : Sage Publications.