NITIPAT NIDA LAW JOURNAL

วารสารกฎหมาย นิติพัฒน์ นิด้า

NITIPAT NIDA LAW JOURNAL

ปีที่ 12 ฉบับที่ 1 มกราคม-มิถุนายน 2566
ISSN 2822-0560 (Print)
ISSN 2822-0609 (Online)

บทความ

คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์

วารสารกฎหมายนิติพัฒน์ นิด้า
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2566
คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์

Nitipat NIDA Law Journal
Volume 12 No. 1 January - June 2023
Graduate School of Law
National Institute of Development Administration
วารสารกฎหมายนิติพัฒน์ นิด้า
ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2566

บรรณาธิการ

อาจารย์ ดร. วิสาขา ภู่สำรวจ สถาบันบัณฑิตพัฒนบริหารศาสตร์

รองบรรณาธิการ

ประภัตรา ปักกัดตัง สถาบันบัณฑิตพัฒนบริหารศาสตร์

กองบรรณาธิการ

ศาสตราจารย์ ดร.ศักดา ธนิตกุล จุฬาลงกรณ์มหาวิทยาลัย
ศาสตราจารย์ ดร.บรรเจิด สิงคะเนติ สถาบันบัณฑิตพัฒนบริหารศาสตร์
รองศาสตราจารย์นเรศร์ เกษะประกร สถาบันบัณฑิตพัฒนบริหารศาสตร์
ศาสตราจารย์ ดร.พินัย ณ นคร มหาวิทยาลัยธรรมศาสตร์
ศาสตราจารย์ ดร.สราวุธ ปิติยาศักดิ์ มหาวิทยาลัยสุโขทัยธรรมาธิราช
รองศาสตราจารย์ ดร.ภูมิ โชคเหมาะ มหาวิทยาลัยธุรกิจบัณฑิตย์
รองศาสตราจารย์ ดร.สุปรียา แก้วละเอียด มหาวิทยาลัยธรรมศาสตร์
ผู้ช่วยศาสตราจารย์ ดร.เสถียรภาพ นาหลวง มหาวิทยาลัยอัสสัมชัญ
ผู้ช่วยศาสตราจารย์ ดร.วริยา ล้ำเลิศ สถาบันบัณฑิตพัฒนบริหารศาสตร์

ผู้อำนวยการโครงการ

ผู้ช่วยศาสตราจารย์ ดร.กฤษฎากร ว่องวุฒิกุล สถาบันบัณฑิตพัฒนบริหารศาสตร์

กองจัดการ

รองศาสตราจารย์ ดร.อมรรัตน์ กุลสุจริต สถาบันบัณฑิตพัฒนบริหารศาสตร์
อาจารย์ ดร.ธนัทเทพ เธียรประสิทธิ์ สถาบันบัณฑิตพัฒนบริหารศาสตร์

ผู้ประสานงานวารสาร

เขมจิรา คณนาธรรม สถาบันบัณฑิตพัฒนบริหารศาสตร์

นักศึกษาผู้ช่วยโครงการวารสาร

ถิรดา สุวรรณรัตน์ และปิ่นอนงค์ นุ้ยพิน
หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์

Nitipat NIDA Law Journal (Peer-reviewed Journal)

Volume 12 No. 1 January - June 2023

วัตถุประสงค์และขอบเขตการดำเนินงานของวารสาร

วารสารกฎหมายนิติพัฒน์ นิด้า (Nitipat NIDA Law Journal) จัดทำโดยคณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ เป็นวารสารที่ตีพิมพ์ปีละ 2 ฉบับ คือ ฉบับที่ 1: มกราคม - มิถุนายน และฉบับที่ 2: กรกฎาคม - ธันวาคม โดยมีวัตถุประสงค์เพื่อเป็นการสนับสนุนนักศึกษา อาจารย์ ข้าราชการ และนักวิชาการทั่วไปในการนำเสนอและเผยแพร่ผลงานวิชาการทางด้านนิติศาสตร์ รวมถึงศาสตร์อื่นที่เกี่ยวข้อง เช่น กฎหมายกับการพัฒนา สังคมวิทยากฎหมาย นิติเศรษฐศาสตร์ และนิติปรัชญา เป็นต้น

ประเภทของของผลงานวิชาการที่จะได้รับการตีพิมพ์ คือ บทความวิชาการ บทความวิจัย ปกิณกะกฎหมาย และแนะนำหนังสือ โดยบทความวิชาการและบทความวิจัย จะได้รับการประเมินจากกองบรรณาธิการและผู้ทรงคุณวุฒิอย่างน้อย 3 ท่านที่ตรงตามสาขาวิชา โดยเป็นการประเมินแบบลับในลักษณะ double-blinded ซึ่งบทความต้องไม่เคยได้รับการตีพิมพ์ที่ใดมาก่อน การเผยแพร่วารสารกฎหมายนิติพัฒน์ นิด้า มี 2 รูปแบบ กล่าวคือ เผยแพร่ในรูปแบบตัวเล่ม ซึ่งสามารถเข้าถึงได้ที่ห้องสมุด คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ หรือสั่งซื้อได้ที่ โครงการวารสารวิชาการ คณะนิติศาสตร์ “นิติพัฒน์ นิด้า” และเผยแพร่ในรูปแบบออนไลน์ ซึ่งสามารถเข้าถึงได้ที่เว็บไซต์ของ Thai Journal Online (ThaiJo)

เจ้าของ:	คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์
สถานที่ติดต่อ:	อาคารบุญชนะ อัตถากร ชั้น 5
	เลขที่ 148 ถนนเสรีไทย แขวงคลองจั่น เขตบางกะปิ กรุงเทพฯ 10240
โทรศัพท์:	0 2727 3662 โทรสาร: 0 2374 4731
E-mail:	nitipat_lawjournal@nida.ac.th

ออกแบบและพิมพ์ที่

บริษัท จรัลสนิทวงศ์การพิมพ์ จำกัด เลขที่ 219,221,223,225,227,229,231,233

แขวงบางแคเหนือ เขตบางแค กรุงเทพฯ 10160

โทรศัพท์ 0 280 2281-3 โทรสาร 0 2809 2284

http://www.fast-books.com E-mail: info@fast-books.com

ราคาจำหน่ายเล่มละ 150 บาท

บทบรรณาธิการ

วารสารกฎหมายนิติพัฒน์ นิด้า ปีที่ 12 ฉบับที่ 1 เดือนมกราคมถึงมิถุนายน ปี 2566 ได้รวบรวมบทความวิชาการและบทความวิจัยจากหลากหลายสาขา ในฉบับนี้ วารสารนำเสนอมุมมองและประเด็นทางกฎหมายที่เกิดจากการใช้เทคโนโลยีสมัยใหม่ซึ่งมีบทบาทอย่างสำคัญทางสังคมและเศรษฐกิจ

บทความแรก *"การเป็นพยานในพินัยกรรมแบบธรรมดาที่ทำขึ้นในช่วงการระบาดของโรคติดเชื้อไวรัสโคโรนา 2019"* โดยอาจารย์ ดร. ภาคภูมิ โลหวริตานนท์ นำเสนอประเด็นทางกฎหมายที่เกิดขึ้นจากการใช้วิธีเป็นพยานทางไกลผ่านการประชุมทางไกลด้วยวีดีทัศน์ (Video conference) ในการทำพินัยกรรมแบบธรรมดาแทนที่การมีตัวบุคคลเป็นพยานอยู่ต่อหน้ากันทางกายภาพในช่วงสถานการณ์การแพร่ระบาดของโรคโควิด-19 ผู้เขียนได้วิเคราะห์มาตรการทางกฎหมายในต่างประเทศและเสนอแนวทางปรับปรุงกฎหมายไทยเรื่องการเป็นพยานในพินัยกรรมแบบธรรมดา

บทความที่สอง *"การปฏิรูปกฎหมายเกี่ยวกับความรับผิดทางอาญาของผู้กระทำความผิดที่มีความผิดปกติทางจิตของประเทศไทย: กรณีมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตตามประมวลกฎหมายอาญา มาตรา 65"* โดยอาจารย์ ดร. ญาดา เดชชัย เธียรประสิทธิ์ เป็นบทความวิจัยในชุดบทความเรื่องการปฏิรูปกฎหมายเกี่ยวกับความรับผิดทางอาญาของผู้กระทำความผิดที่มีความผิดปกติทางจิตของประเทศไทย บทความนี้นำเสนอปัญหาข้อจำกัดตามมาตรา 48 ของประมวลกฎหมายอาญาซึ่งทำให้ศาลไม่สามารถเลือกใช้มาตรการจัดการผู้กระทำความผิดที่มีความผิดปกติทางจิตตามประมวลกฎหมายอาญามาตรา 65 ได้อย่างเหมาะสม ผู้เขียนศึกษาวิเคราะห์เปรียบเทียบมาตรการทางกฎหมายของสหราชอาณาจักร (อังกฤษและเวลส์ และสกอตแลนด์) และเสนอการแก้ไขมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตของประเทศไทยให้มีความหลากหลายและมีการเงื่อนไขการบังคับใช้ที่เหมาะสมมากขึ้น

บทความที่สาม *"The Challenges of Applying Competition Law to Online Platforms: The Case of Search Engines Market"* โดย Dr. Warut Songsujaritkul เป็นบทความวิชาการซึ่งนำเสนอข้อพิจารณาเกี่ยวกับการปรับใช้หลักกฎหมายแข่งขันทางการค้าในกรณีคดีข้อพิพาทที่เกิดขึ้นในสหภาพยุโรป กรณีกูเกิ้ล (Google) ปรับเปลี่ยนผลการค้นหา (search result) ในแพลตฟอร์มของตน ผู้เขียนนำเสนอข้อถกเถียงประเด็นสำคัญในคดีเกี่ยวกับการนำมาตรา 102 ในสนธิสัญญาว่าด้วยการดำเนินงานของสหภาพยุโรป (Treaty on the Functioning of the European Union) มาปรับใช้กับการกระทำของผู้ประกอบการซึ่งทำหน้าที่ให้บริการเป็นตัวกลางในการเข้าถึงข้อมูลออนไลน์ รวมถึงความไม่เหมาะสมในการใช้หลักการดังกล่าวเพื่อแก้ปัญหาสถานะผู้มีอำนาจเหนือตลาดในกรณีตลาดแพลตฟอร์มออนไลน์

บทความที่สี่ *"แนวทางการเปิดเผยข้อมูลข่าวสารของราชการตามพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 ที่มีข้อมูลส่วนบุคคลรวมอยู่ด้วย"* โดย ผู้ช่วยศาสตราจารย์ ดร.ปิติ เอี่ยมจำรูญลาภ เป็นบทความวิชาการซึ่งวิเคราะห์และนำเสนอแนวทางในการสร้างความสมดุลระหว่างการบังคับใช้พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 เพื่อให้เกิดความโปร่งใสและกลไกการตรวจสอบภาครัฐตามแนวคิด

ประชาธิปไตยกับการคุ้มครองบุคคลไม่ให้ถูกรุกล้ำความเป็นส่วนตัวจนเกินไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

บทความสุดท้ายของวารสารฉบับนี้ *“ความสัมพันธ์ระหว่างแนวคิดเรื่องความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล”* โดยอาจารย์ ดร. อัญธิกา ณ พิบูลย์ เป็นบทความวิจัยซึ่งศึกษาปัญหาการบริหารจัดการความสัมพันธ์ระหว่างแนวคิดเรื่องความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล และเสนอแนะแนวทางในการบริหารจัดการความสัมพันธ์ทั้งสองแนวคิดอย่างสมดุลภายในองค์กรด้วยการกำหนดนโยบายที่ชัดเจนและปรับใช้มาตรการอย่างเหมาะสมภายใต้บริบทของแต่ละองค์กร

กองบรรณาธิการยังคงมุ่งมั่นในการดำเนินภารกิจสำคัญของคณะนิติศาสตร์ในการเผยแพร่องค์ความรู้ทางวิชาการและงานวิจัยเกี่ยวกับการปรับใช้องค์ความรู้ด้านกฎหมายเพื่อพัฒนาสังคม รวมทั้งพัฒนาคุณภาพงานวารสารกฎหมายไทย กองบรรณาธิการวารสารขอขอบคุณทุกท่านที่ให้การสนับสนุนการทำงานของวารสารและหวังเป็นอย่างยิ่งว่าผู้อ่านจะติดตามและให้การสนับสนุนวารสารในฉบับต่อไป

บรรณาธิการวารสาร

สารบัญ

วารสารกฎหมายนิติพัฒน์ นิด้า ปีที่ 12 ฉบับที่ 1 มกราคม - มิถุนายน 2566

การเป็นพยานในพินัยกรรมแบบธรรมดาที่ทำขึ้นในช่วงการระบาดของโรคติดเชื้อไวรัสโคโรนา 2019

Witnessing an Ordinary Will made during the COVID-19 Pandemic

ภาคภูมิ โลหวริตานนท์[*]

คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

Pakpoom Lohavaritanond

Faculty of Law, Thammasat University

วันที่รับบทความ 30 สิงหาคม 2565; วันแก้ไขบทความ 11 มกราคม 2566; วันตอบรับบทความ 11 มกราคม 2566

บทคัดย่อ

การทำพินัยกรรมในประเทศไทย ผู้ทำพินัยกรรมสามารถเลือกแบบของพินัยกรรมที่ประสงค์จะทำได้ ซึ่งมีอยู่ด้วยกันหลายแบบ หนึ่งในแบบพินัยกรรมซึ่งเป็นที่นิยมก็คือ พินัยกรรมแบบธรรมดา อย่างไรก็ตาม ปัญหาสำคัญประการหนึ่งที่เกิดขึ้นหากมีการเลือกทำพินัยกรรมแบบธรรมดาในช่วงการระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 ก็คือการทำพินัยกรรมในรูปแบบนี้จำเป็นจะต้องมีพยานอย่างน้อยสองคน โดยผู้ทำพินัยกรรมต้องลงลายมือชื่อต่อหน้าพยาน และพยานก็ต้องลงลายมือชื่อรับรองลายมือชื่อของผู้ทำพินัยกรรม ซึ่งการรวมตัวกันระหว่างผู้ทำพินัยกรรมและพยานในที่เดียวกันย่อมก่อให้ความเสี่ยงในการติดเชื้อโควิด-19 รัฐบาลของประเทศต่างๆ จึงตัดสินใจในการแก้ปัญหาดังกล่าวด้วยการอนุญาตให้ใช้วิธีการเป็นพยานทางไกลมาใช้บังคับแก่การทำพินัยกรรมที่ทำขึ้นในช่วงที่มีการแพร่ระบาดของโรคโควิด-19 บทความนี้มุ่งศึกษาปัญหาทางกฎหมายที่เกิดขึ้นหากมีการนำวิธีการเป็นพยานทางไกล เช่น การเป็นพยานทางวิดีโอคอนเฟอเรนซ์มาใช้แทนที่การเป็นพยานในพินัยกรรมที่อยู่ต่อหน้ากันทางกายภาพ โดยจะได้ศึกษาตัวอย่างของกฎหมายของต่างประเทศเกี่ยวกับ

[*] อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

ที่อยู่: คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

เลขที่ 2 ถนนพระจันทร์ เขตพระนคร กรุงเทพฯ 10200

E-mail: pakpoom55@tu.ac.th

การเป็นพยานทางไกลในพินัยกรรมแบบธรรมดาที่ทำขึ้นในสถานการณ์การแพร่ระบาดของโรคโควิด-19 เพื่อนำมาใช้ในการวิเคราะห์และเสนอแนะแนวทางในการปรับปรุงกฎหมายของไทยที่เกี่ยวข้องกับการเป็นพยานในพินัยกรรมแบบธรรมดาเพื่อให้สอดรับกับสถานการณ์การแพร่ระบาดของโรคโควิด-19

คำสำคัญ: พินัยกรรมแบบธรรมดา, การเป็นพยานในพินัยกรรม, พยานทางไกล, โควิด-19

Abstract

To make a will in Thailand, a testator is free to choose the forms of will he wishes to do. One of the most popular forms of will chosen by the testator is an ordinary will. However, the critical problem that arises if the testator decides to make an ordinary will during the COVID-19 pandemic, is that it must be signed by the testator in the presence of at least two witnesses, and the witnesses are required to sign their names certifying the testator's signature. Thus, gathering the testator and witnesses in the same place poses a risk of contracting COVID-19. Therefore, the governments of various jurisdictions then decided to resolve this issue by allowing the adoption of remote witnessing to be applied to the wills made during COVID-19. This article focuses on the legal issues that may arise if remote witnessing measures, such as witnessing via video conference, are adopted instead of requiring witnesses to be physically present when witnessing the will. It will explore the examples of foreign law regarding remote witnessing in an ordinary will made during COVID-19. Lessons learned from them can be used to analyze and suggest a possible way to amend the Thai laws related to ordinary will witnessing will cope with the COVID-19 outbreak.

Keywords: Ordinary Will, Witnessing a Will, Remote Witnessing, COVID-19

1. บทนำ

เมื่อวันที่ 11 มีนาคม 2563 องค์การอนามัยโลกได้ประกาศให้โรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) หรือโรคโควิด-19 เป็นโรคระบาดใหญ่ที่ลุกลามไปทั่วโลก (pandemic) อันเนื่องมาจากการระบาดของโรคเป็นไปอย่างรวดเร็วและพบการระบาดในทุกภูมิภาคทั่วโลก[1] ซึ่งในระหว่างจัดทำบทความนี้การแพร่ระบาดของโรคดังกล่าวทั่วโลกรวมถึงในประเทศไทยก็ยังไม่สิ้นสุดลง ทำให้รัฐบาลของประเทศต่างๆ ได้กำหนดมาตรการให้ประชาชนของตนปฏิบัติเพื่อป้องกันการแพร่ระบาดของโรคโควิด-19 โดยมาตรการสำคัญที่มีการบังคับใช้ก็คือการเว้นระยะห่างทางสังคม (social distancing) และมาตรการล็อกดาวน์ (lockdown) อันส่งผลกระทบต่อการทำพินัยกรรมแบบธรรมดา เนื่องจากตามบทบัญญัติของประมวลกฎหมายแพ่งและพาณิชย์ได้กำหนดไว้ว่าในการทำพินัยกรรมแบบธรรมดา ผู้ทำพินัยกรรมจะต้องลงลายมือชื่อไว้ต่อหน้าพยานอย่างน้อยสองคนพร้อมกันซึ่งพยานสองคนนั้นจะต้องลงลายมือชื่อรับรองลายมือชื่อของผู้ทำพินัยกรรมไว้ในขณะนั้น[2] ด้วยเหตุดังกล่าวจึงมีความจำเป็นที่จะต้องมีบุคคลอื่นอย่างน้อยสองคนมาปรากฏตัวเป็นพยานต่อหน้าผู้ทำพินัยกรรมในเวลาที่ผู้ทำพินัยกรรมลงลายมือชื่อในพินัยกรรม ซึ่งการรวมตัวของบุคคลที่เป็นผู้ทำพินัยกรรมและพยานในพินัยกรรมนั้นอาจก่อให้เกิดความเสี่ยงในการติดเชื้อไวรัสโควิด-19 อีกทั้งอาจฝ่าฝืนมาตรการของรัฐเพื่อป้องกันการแพร่ระบาดของโรคโควิด-19 ดังนั้น ในสถานการณ์เช่นนี้ มีความจำเป็นอย่างยิ่งที่จะต้องลดการรวมกลุ่มหรือพบปะกัน และควรที่จะต้องนำวิธีการการเป็นพยานทางไกล (remote witnessing) เช่น การเป็นพยานในพินัยกรรมด้วยการประชุมทางไกลผ่านวิดีโอคอนเฟอเรนซ์ (video Conference) มาใช้ทดแทน อย่างไรก็ตาม การนำวิธีการดังกล่าวมาใช้ในการทำพินัยกรรม ก็อาจก่อให้เกิดปัญหาในการตีความกฎหมาย กล่าวคือ การนำวิธีการการเป็นพยานทางไกลมาใช้เพื่อมาทดแทนการปรากฏตัวทางกายภาพของพยานต่อหน้าผู้ทำพินัยกรรมจะทำได้หรือไม่[3] และจะส่งผลกระทบต่อความสมบูรณ์ของการทำพินัยกรรมแบบธรรมดาหรือไม่ ทั้งนี้ แม้ว่ากฎหมายของประเทศไทยอนุญาตให้มีการทำพินัยกรรมแบบเขียนเองทั้งฉบับ (Holographic will) ซึ่งไม่จำเป็นต้องมีพยานในการทำพินัยกรรม[4] ก็ตาม แต่บุคคลทั่วไปก็อาจจะประสงค์ที่จะ

---

[1] Tedros Adhanom Ghebreyesus, 'WHO Director-General's opening remarks at the Mission briefing on COVID-19 - 11 March 2020' (11 March 2020) <https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020> accessed 5 August 2022.

[2] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 1656.

[3] Brian Sloan, 'Witnessing Law Reform in the Coronavirus Era' (8 August 2020) <https://www.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2020/08/witnessing-law-reform-coronavirus-era > accessed 5 August 2022.

[4] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 1657.

ทำพินัยกรรมแบบธรรมดาอยู่ ไม่ว่าจะเป็นเพราะไม่ต้องการเขียนพินัยกรรมด้วยตนเอง แต่ต้องการให้ผู้อื่นที่เป็นผู้รู้กฎหมายช่วยจัดทำให้เพื่อให้แน่ใจว่าพินัยกรรมที่ทำขึ้นมีผลใช้บังคับได้ตามกฎหมาย หรืออาจจะต้องการพยานมารู้เห็นในการทำพินัยกรรมเพื่อประโยชน์ในการพิสูจน์ว่าได้มีการทำพินัยกรรมขึ้นจริง หากมีข้อพิพาทเกิดขึ้น เป็นต้น บทความนี้จะได้ศึกษาถึงความจำเป็นของการมีพยานในการทำพินัยกรรมหลักกฎหมายของไทยเกี่ยวกับการเป็นพยานในพินัยกรรมแบบธรรมดา จากนั้นจะได้ศึกษากฎหมายของต่างประเทศที่เกี่ยวกับการเป็นพยานในพินัยกรรมแบบธรรมดาในสถานการณ์การแพร่ระบาดของโรคโควิด-19 เพื่อนำมาใช้ในการวิเคราะห์และเสนอแนะแนวทางในการปรับปรุงกฎหมายของไทยที่เกี่ยวข้องกับการเป็นพยานในพินัยกรรมแบบธรรมดาเพื่อให้สอดรับกับสถานการณ์ของการแพร่ระบาดของโรคโควิด-19

2. เหตุผลความจำเป็นที่ต้องมีพยานในการทำพินัยกรรม

ในการทำพินัยกรรมนอกเหนือจากพินัยกรรมแบบเขียนเองทั้งฉบับ กฎหมายมักจะกำหนดให้มีบุคคลอื่นที่ไม่ใช่ผู้รับพินัยกรรมเป็นพยานในการทำพินัยกรรมของเจ้ามรดกและลงลายมือชื่อของบุคคลนั้นในพินัยกรรมในฐานะพยาน เหตุผลที่กฎหมายมรดกของประเทศต่างๆ กำหนดให้ต้องมีพยานในการทำพินัยกรรมก็เนื่องมาจากในการพิสูจน์ว่าพินัยกรรมได้ทำขึ้นโดยผู้ตายจริงหรือไม่จำเป็นต้องอาศัยการนำสืบจากบุคคลผู้เป็นพยานในพินัยกรรม[5] ซึ่งเป็นประโยชน์อย่างยิ่งในกรณีที่มีผู้ปฏิเสธว่าพินัยกรรมที่ทำขึ้นนั้นไม่ใช่พินัยกรรมที่ผู้ตายทำเอาไว้[6] ซึ่งอาจเป็นเพราะผู้ตายอาจจะไม่ได้เขียนหรือพิมพ์พินัยกรรมด้วยตนเองแต่ให้ผู้อื่นเขียนหรือพิมพ์ให้แทน พยานในพินัยกรรมจึงเข้ามามีบทบาทในการตรวจสอบว่าผู้ตายรู้หรือไม่ว่าเอกสารที่ตนเองลงลายมือชื่อไปนั้นเป็นพินัยกรรมของตนเอง และขณะที่ลงลายมือชื่อนั้นผู้ตายมีสติสัมปชัญญะสมบูรณ์หรือไม่[7] นอกจากนี้ยังช่วยในการพิสูจน์ด้วยว่าผู้ตายมิได้ลงลายมือชื่อในพินัยกรรมไปเพราะถูกข่มขู่[8] ทั้งนี้โดยทั่วไปกฎหมายมักจะกำหนดคุณสมบัติของผู้ที่จะมาเป็นพยานในพินัยกรรมว่าจะต้องไม่เป็นบุคคลซึ่งเป็นผู้รับพินัยกรรมเพื่อให้พินัยกรรมที่ถูกทำขึ้นนั้นเป็นไปตามเจตนาของผู้ทำพินัยกรรมอย่างแท้จริงโดย

---

[5] บวรศักดิ์ อุวรรณโณ, *คำอธิบายกฎหมายแพ่งและพาณิชย์ว่าด้วยมรดก* (พิมพ์ครั้งที่ 2 แก้ไขเพิ่มเติม, สำนักพิมพ์นิติธรรม 2548) 261.

[6] สอาด นาวีเจริญ, *คำบรรยายประมวลกฎหมายแพ่งและพาณิชย์ บรรพ 6 ว่าด้วยมรดก* (สำนักพิมพ์นิติบรรณการ 2517) 88.

[7] ไพโรจน์ กัมพูสิริ, *หลักกฎหมายมรดก* (พิมพ์ครั้งที่ 7 แก้ไขเพิ่มเติม, โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัย ธรรมศาสตร์ 2563) 130.

[8] Irwin Mitchell, 'Witnessing A Will' (2022) <https://www.irwinmitchell.com/personal/wills-trusts-estates/wills/guide/witnessing-a-will> accessed 8 August 2022.

ไม่ถูกครอบงำจากบุคคลดังกล่าวในการทำพินัยกรรม[9] และด้วยความสำคัญของการมีพยานในพินัยกรรมเพื่อพิสูจน์ข้อเท็จจริงเกี่ยวกับพินัยกรรมที่ถูกทำขึ้นนี้เอง ทำให้กฎหมายมรดกของแต่ละประเทศต้องกำหนดคุณสมบัติของผู้ที่สามารถมาเป็นพยานในพินัยกรรมได้ เช่น จะต้องเป็นผู้มีความสามารถบริบูรณ์ในทางกฎหมาย (full legal capacity) เป็นผู้จักษุไม่บอด ไม่เป็นใบ้ เป็นผู้รู้หนังสือ สามารถอ่านเขียนได้ เป็นต้น[10]

3. กฎหมายไทยเกี่ยวกับการเป็นพยานในพินัยกรรมแบบธรรมดา

ประมวลกฎหมายแพ่งและพาณิชย์ได้กำหนดหลักเกณฑ์เกี่ยวกับเรื่องพยานในพินัยกรรมแบบธรรมดาไว้ว่าผู้ทำพินัยกรรมจะต้องลงลายมือชื่อไว้ต่อหน้าพยานอย่างน้อยสองคนพร้อมกัน ซึ่งพยานสองคนนั้นจะต้องลงลายมือชื่อรับรองลายมือชื่อของผู้ทำพินัยกรรมไว้ในขณะนั้น[11] โดยพยานในพินัยกรรมจะต้องลงลายมือชื่อด้วยตนเองจะใช้วิธีอื่นแทนการลงลายมือชื่อ เช่น ลายพิมพ์นิ้วมือ แกงได ตราประทับ ไม่ได้[12] นอกจากนี้บุคคลที่จะเป็นพยานในพินัยกรรมจะต้องเป็นผู้บรรลุนิติภาวะแล้ว ไม่เป็นบุคคลวิกลจริตหรือบุคคลซึ่งศาลสั่งให้เป็นผู้เสมือนไร้ความสามารถ ไม่เป็นบุคคลที่หูหนวก เป็นใบ้ หรือจักษุบอดทั้งสองข้าง[13] อีกทั้งพยานและคู่สมรสของพยานจะเป็นผู้รับทรัพย์ตามพินัยกรรมไม่ได้[14] จากการพิจารณาหลักกฎหมายดังกล่าวจะเห็นได้ว่าประเด็นที่สำคัญที่สุดในเรื่องของการเป็นพยานในพินัยกรรมก็คือ ต้องมีพยานอย่างน้อยสองคนได้อยู่รู้เห็นในเวลาที่ผู้ทำพินัยกรรมลงลายมือชื่อในพินัยกรรม ดังนั้น หากมีพยานสองคน แต่พยานคนหนึ่งมิได้อยู่รู้เห็นด้วยตั้งแต่แรกในขณะที่ผู้ทำพินัยกรรมลงลายมือชื่อ พินัยกรรมนั้นก็ไม่สมบูรณ์เป็นพินัยกรรรมแบบธรรมดา[15] ดังเช่นตัวอย่างในคดีหนึ่งที่ศาลฎีกาเคยตัดสินไว้ว่าผู้ทำพินัยกรรมลงชื่อเป็นผู้ทำพินัยกรรมต่อหน้าพยานเพียงคนเดียว ส่วนพยานอีกคนหนึ่งมาถึงและลงชื่อเป็นพยานในพินัยกรรมภายหลังที่ผู้ทำพินัยกรรมลงชื่อแล้วประมาณ 5 นาที แม้ว่าขณะนั้นผู้ทำพินัยกรรมและพยานจะยังอยู่พร้อมหน้ากัน ก็ถือว่าพินัยกรรมนั้นเป็นพินัยกรรมที่ไม่ชอบด้วยประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 1656[16] อย่างไรก็ตาม ในส่วนของ

---

[9] Ibid.

[10] Mariusz Załucki, *Wills Formalities versus Testator's Intention: Functional model of effective testation for informal wills* (Nomos Verlagsgesellschaft mbH & Co. KG 2021) 150.

[11] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 1656.

[12] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 1666.

[13] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 1670.

[14] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 1653.

[15] พินัย ณ นคร, *กฎหมายลักษณะมรดก* (พิมพ์ครั้งที่ 4 แก้ไขเพิ่มเติม, สำนักพิมพ์วิญญูชน 2558) 330.

[16] คำพิพากษาศาลฎีกาที่ 1875/2517.

การลงลายมือชื่อของพยานในพินัยกรรม แม้ว่ามาตรา 1656 จะได้กำหนดให้พยานสองคนต้องลงลายมือชื่อเพื่อรับรองลายมือชื่อของผู้ทำพินัยกรรมในขณะนั้น ซึ่งทำให้เข้าใจได้ว่าพยานจะต้องลงลายมือชื่อในเวลาเดียวกับที่ผู้ทำพินัยกรรมลงลายมือชื่อและต้องกระทำต่อหน้าซึ่งกันและกัน แต่ศาลฎีกาก็มิได้ตีความเคร่งครัดถึงขนาดที่ว่าบุคคลที่เกี่ยวข้องกับพินัยกรรมทั้งผู้ทำพินัยกรรมและพยานจะต้องมาลงลายมือชื่อในเวลาเดียวกันทั้งหมด โดยแต่ละคนอาจจะลงลายมือชื่อไม่พร้อมกันก็ได้ เพียงแต่ว่าในขณะที่คนใดคนหนึ่งลงลายมือชื่อจะต้องมีคนอื่นๆ อยู่รู้เห็นด้วย[17] ดังเช่นในคดีหนึ่ง พยานลงชื่อในพินัยกรรมต่อหน้าผู้ทำพินัยกรรม ต่อมาภายหลัง 3 วันผู้ทำพินัยกรรมจึงได้ลงลายพิมพ์นิ้วมือของตนในพินัยกรรมต่อหน้าพยานชุดเดิมนั้นเอง ศาลฎีกาตัดสินว่าเป็นพินัยกรรมที่ถูกต้องเข้าเกณฑ์ครบถ้วนตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 1656[18] เหตุผลที่ศาลฎีกาวินิจฉัยในลักษณะนี้ก็อาจจะเป็นเพราะศาลได้พิจารณาว่าได้มีการดำเนินการไปตามเจตนารมณ์ของมาตรา 1656 ที่ต้องการให้ทั้งผู้ทำพินัยกรรมและพยานอยู่พร้อมกัน ในขณะอีกฝ่ายลงลายมือชื่อเพื่อยืนยันว่าได้มีการทำพินัยกรรมกันจริงหรือไม่เป็นสำคัญ เมื่อข้อเท็จจริงปรากฏว่าในตอนแรกพยานได้ลงลายมือชื่อต่อหน้าผู้ทำพินัยกรรมเรียบร้อยแล้ว และต่อมาผู้ทำพินัยกรรมซึ่งในตอนแรกมิได้ลงลายมือชื่อก็ได้มาลงลายมือชื่อต่อหน้าพยานในภายหลังในอีกสามวันต่อมา ซึ่งในเวลาที่ผู้ทำพินัยกรรมมาลงลายมือชื่อในตอนหลังนี้ พยานจะมาลงลายมือชื่อเดิมอีกรอบหรือไม่ย่อมไม่เป็นสาระสำคัญ เนื่องจากว่าขั้นตอนของการอยู่พร้อมหน้าสามคน (คือ ผู้ทำพินัยกรรมและพยานสองคน) และการลงลายมือชื่อต่อหน้ากันและกันได้สำเร็จลงตามความประสงค์ของกฎหมายแล้วนั่นเอง[19] ในทางตรงกันข้าม หากผู้ทำพินัยกรรมลงลายมือชื่อโดยไม่มีพยานรู้เห็นก็ดี หรือพยานคนใดคนหนึ่งลงลายมือชื่อในพินัยกรรม โดยมิได้รับรู้ถึงการลงลายมือชื่อของผู้ทำพินัยกรรมหรือของพยานคนอื่นก็ดี ย่อมถือว่าพินัยกรรมแบบธรรมดานั้นทำขึ้นไม่ถูกต้องตามแบบที่กฎหมายกำหนด[20]

อย่างไรก็ตาม การที่กฎหมายกำหนดให้พยานในพินัยกรรมต้องมาปรากฏตัวอยู่หน้าผู้ทำพินัยกรรมเพื่อมายืนยันว่าผู้ทำพินัยกรรมได้ทำพินัยกรรมขึ้นจริงอาจก่อให้เกิดปัญหาขึ้น เมื่อต้องนำมาปรับใช้ในสถานการณ์ของโรคระบาด โดยเฉพาะอย่างยิ่งโรคระบาดใหญ่ที่ลุกลามไปทั่วโลกดังเช่นโรคโควิด-19 ซึ่งโดยสภาพจะต้องมีการรักษาระยะห่างทางสังคม (social distancing) และงดการเดินทางไปมาหาสู่ระหว่างกันเพื่อลดโอกาสและความเสี่ยงในการติดเชื้อไวรัสโควิด-19 ดังนั้น การรวมกลุ่มของบุคคลซึ่งประกอบไปด้วยผู้ทำพินัยกรรมและพยานอย่างน้อยสองคนซึ่งอาจจะไม่ใช่คนในครอบครัว เนื่องจากกฎหมายห้ามมิให้

---

[17] พินัย ณ นคร (n 15) 331.

[18] คำพิพากษาศาลฎีกาที่ 1387/2500.

[19] ไพโรจน์ กัมพูสิริ (n 7) 131-132.

[20] พินัย ณ นคร (n 15) 331.

ผู้รับพินัยกรรมซึ่งโดยทั่วไปเป็นคนในครอบครัวมาเป็นพยานในพินัยกรรมก็อาจก่อให้เกิดความเสี่ยงในการติดเชื้อโควิด-19 ได้ โดยเฉพาะอย่างยิ่งผู้ทำพินัยกรรมที่เป็นผู้สูงอายุหรือมีโรคประจำตัว[21] ดังนั้น การติดต่อสื่อสารกันระหว่างบุคคลจึงควรทำผ่านสื่ออิเล็กทรอนิกส์ โดยไม่จำเป็นให้บุคคลหลายคนต้องมารวมตัวอยู่ในสถานที่เดียวกันทางกายภาพ เช่น การประชุมทางไกลผ่านวิดีโอคอนเฟอเรนซ์ (video conference) ซึ่งก็น่าจะรวมไปถึงการเป็นพยานในพินัยกรรมด้วย แต่การนำวิธีการดังกล่าวมาใช้กับการเป็นพยานในพินัยกรรมแบบธรรมดา ก่อให้เกิดปัญหาที่สำคัญด้วยกันสองประการ ดังนี้

ประการแรก กรณีที่พยานในพินัยกรรมนำวิธีการการเป็นพยานทางไกล (remote witnessing) มาใช้ เช่น เป็นพยานผ่านวิดีโอคอนเฟอเรนซ์ จะถือว่าเป็นกรณีที่พยานมาปรากฏตัวอยู่ “ต่อหน้า” ผู้ทำพินัยกรรมเช่นเดียวกับกรณีที่พยานมาปรากฏตัวทางกายภาพในสถานที่เดียวกันกับผู้ทำพินัยกรรมหรือไม่ ซึ่งย่อมส่งผลกระทบโดยตรงต่อความสมบูรณ์ของการทำพินัยกรรมแบบธรรมดา

ประการที่สอง เมื่อมีการนำวิธีการการเป็นพยานทางไกลมาใช้และพยานประสงค์จะลงลายมือชื่ออิเล็กทรอนิกส์ในพินัยกรรมที่ผู้พินัยกรรมลงลายมือชื่อ การลงลายมือชื่อดังกล่าวไม่อาจกระทำได้ เนื่องจากมีข้อยกเว้นมิให้นำพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาใช้กับธุรกรรมเกี่ยวกับมรดก[22] เช่น การทำพินัยกรรมโดยใช้ข้อมูลอิเล็กทรอนิกส์[23] ซึ่งก็รวมถึงการลงลายมือชื่ออิเล็กทรอนิกส์ในพินัยกรรมด้วย

4. กฎหมายของต่างประเทศเกี่ยวกับการเป็นพยานในพินัยกรรมแบบธรรมดาที่ทำขึ้นในสถานการณ์การระบาดของโรคติดเชื้อไวรัสโคโรนา 2019

สถานการณ์การแพร่ระบาดของไวรัสโคโรนา 2019 ที่เกิดขึ้นส่งผลต่อการดำเนินชีวิตของผู้คนทั่วโลกและย่อมส่งผลกระทบต่อการทำพินัยกรรมแบบธรรมดาซึ่งต้องมีพยานรู้เห็นในการพินัยกรรม เนื่องจากมีความจำเป็นที่บุคคลในสังคมจะต้องรักษาระยะห่างทางสังคมเพื่อป้องกันการแพร่ระบาดของโรค ส่งผลกระทบต่อการเคลื่อนย้ายโดยเสรีของบุคคล และทำให้การทำพินัยกรรมแบบที่ต้องมีพยานไม่อาจดำเนินการได้ดังเช่นในภาวะปกติ[24] ซึ่งสวนทางกับความต้องการในการทำพินัยกรรมของบุคคลที่มีมากขึ้นอย่างมีนัยสำคัญ

---

[21] ดู ข้อกำหนด ออกตามความในมาตรา 9 แห่งพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 (ฉบับที่ 1), ข้อ 8.

[22] พระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับ พ ศ 2549, มาตรา 3.

[23] พินัย ณ นคร, *กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ในยุคดิจิทัล* (สำนักพิมพ์วิญญูชน 2561) 141.

[24] Kelly Purser, Tina Cockburn and Bridget J Crawford, ‘Wills Formalities Beyond COVID-19: An Australian-United States Perspective’ (2020) 5 UNSW Law Journal Forum 1,2.

เนื่องจากมีความกังวลเกี่ยวกับเรื่องความไม่แน่นอนของสถานการณ์โรคระบาด[25] ด้วยเหตุดังกล่าวทำให้รัฐบาลในหลายประเทศตัดสินใจในการแก้ปัญหาดังกล่าวด้วยการอนุญาตให้นำวิธีการเป็นพยานทางไกล (remote witnessing) มาใช้ในการทำพินัยกรรมแบบธรรมดาได้ เพื่อที่จะให้พินัยกรรมที่ทำขึ้นในช่วงที่มีการระบาดของโควิด-19 มีผลใช้บังคับได้อย่างสมบูรณ์ โดยหากได้กระทำตามหลักเกณฑ์เกี่ยวกับการเป็นพยานทางไกลโดยครบถ้วนแล้ว ก็ย่อมมีผลในทางกฎหมายเช่นเดียวกับกรณีที่พยานมาปรากฏตัวต่อหน้าผู้ทำพินัยกรรม ('in the presence' of the testator)[26] ทั้งนี้ เนื่องมาจากกฎหมายเกี่ยวกับพินัยกรรมในหลายประเทศโดยเฉพาะอย่างยิ่งประเทศที่ใช้ระบบกฎหมายคอมมอนลอว์ (Common Law) มักไม่ยอมรับให้มีการทำพินัยกรรมแบบเขียนเองทั้งฉบับ แต่จะต้องทำพินัยกรรมประเภทที่ต้องมีพยาน (witnessed will)[27]เพื่อมารับรองว่าผู้ทำพินัยกรรมได้ลงลายมือชื่อในพินัยกรรมจริง[28] อีกทั้งยังช่วยรับรองว่าพินัยกรรมได้ทำขึ้นด้วยเจตนาของผู้ทำพินัยกรรมอย่างแท้จริง มิใช่เกิดจากการใช้อิทธิพลเกินสมควร (undue influence) ต่อตัวผู้ทำพินัยกรรม[29] จึงมีแนวโน้มที่จะตีความบทบัญญัติในเรื่องพยานในพินัยกรรมค่อนข้างเคร่งครัด และไม่ยอมให้มีการใช้พยานทางไกลเพื่อมาทดแทนพยานที่มาปรากฏตัวทางกายภาพต่อหน้าผู้ทำพินัยกรรม ตัวอย่างเช่น กฎหมายว่าด้วยพินัยกรรมของอังกฤษซึ่งกำหนดหลักการสำคัญเอาไว้ว่า พินัยกรรมย่อมไม่สมบูรณ์ เว้นแต่ผู้ทำพินัยกรรมจะได้ลงลายมือชื่อต่อหน้าพยานอย่างน้อยสองคนในเวลาเดียวกัน และพยานแต่ละคนได้ลงลายมือชื่อต่อหน้าผู้ทำพินัยกรรมเพื่อรับรองการทำพินัยกรรมนั้น[30] โดยในการตีความคำว่า "ต่อหน้า" นี้ ย่อมหมายถึง การอยู่ต่อหน้าทางกายภาพในห้องเดียวกัน[31] หรืออย่างน้อยต้องอยู่ในแนวสายตาที่ผู้ทำพินัยกรรมสามารถมองเห็นพยานได้อย่างชัดเจน (a line of sight)[32] เช่น มองผ่านช่องหน้าต่างของอาคารสำนักงาน[33]

---

[25] Mariusz Załucki, 'Preparation of Wills in Times of COVID-19 Pandemic – Selected observations' (2020) 2 Journal of Modern Science 143, 144.

[26] Purser, Cockburn and Crawford (n 24) 2.

[27] Jan Biemans, 'Will Requirements for Last Wills Remain as They Are?: The 'Physical Presence Requirement' of Witnesses and Notaries in the Light of the COVID-19 Interim Measures and the EU Freedom of (Notarial) Services' (2021) 3 Utrecht Law Review 51, 53.

[28] Purser, Cockburn and Crawford (n 24) 5.

[29] Ibid.

[30] Wills Act 1837, s 9 (1) (c) (d) (ก่อนแก้ไขเพิ่มเติมในปี 2563).
มีข้อสังเกตว่า บทบัญญัติในลักษณะเดียวกันนี้ยังปรากฏในกฎหมายมรดกของประเทศอื่นๆ ที่ใช้ระบบกฎหมายคอมมอนลลอว์ ตัวอย่างเช่น มาตรา 6 ของ Succession Act 2006 (รัฐนิวเซาท์เวลส์ ออสเตรเลีย), มาตรา 10 ของ Succession Act 1981 (รัฐควีนส์แลนด์ ออสเตรเลีย) หรือมาตรา 2-502 (a) ของ Uniform Probate Code (Uniform Law Commission 1969, rev 2019) (กฎหมายเอกรูปของสหรัฐอเมริกา) เป็นต้น

[31] Roger Kerriedge, *The Law of Succession* (10th edn, Sweet & Maxwell 1996) 83.

[32] Catherine Rendell, *Law of Succession* (Macmillan Press Ltd 1997) 43.

[33] *Casson v Dade* (1781) 28 ER 1010.

มองผ่านประตูบ้านหรือประตูรถที่เปิดอยู่ มองผ่านระเบียงหรือห้องข้างเคียงที่เปิดประตูเอาไว้[34] เป็นต้น จึงย่อมไม่อาจตีความขยายให้รวมไปถึงกรณีของการมองเห็นกันผ่านวิดีโอคอนเฟอเรนซ์ผ่านทางระบบออนไลน์ได้[35]

สำหรับแนวทางในการแก้ไขกฎหมายของประเทศต่างๆ เพื่ออนุญาตให้มีการนำพยานทางไกลมาใช้กับการทำพินัยกรรมแบบธรรมดาอาจแบ่งออกได้เป็น 2 แนวทาง ดังนี้

แนวทางแรก อนุญาตให้มีการนำวิธีการเป็นพยานทางไกล เช่น การเป็นพยานผ่านวิดีโอคอนเฟอเรนซ์หรือเทคโนโลยีการถ่ายทอดภาพและเสียง (audio-visual links) ในรูปแบบต่างๆ เช่น โปรแกรม Zoom, Skype ฯลฯ มาใช้บังคับกับการทำพินัยกรรมแบบธรรมดา แต่ไม่อนุญาตให้ผู้ทำพินัยกรรมและพยานลงลายมือชื่ออิเล็กทรอนิกส์ในพินัยกรรม[36] ดังนั้น แม้กฎหมายจะอนุญาตให้ใช้วิธีการเป็นพยานทางไกลในรูปแบบดังกล่าวได้ โดยให้ถือเสมือนว่าเป็นกรณีที่พยานอยู่ “ต่อหน้า” ผู้ทำพินัยกรรม แต่การลงลายมือชื่อของผู้ทำพินัยกรรมก็ดี หรือของพยานก็ดี ก็ต้องเป็นการลงลายมือชื่อกันจริงในทางกายภาพ (wet signature) อย่างไรก็ตาม ความเคร่งครัดในการลงลายมือชื่อในพินัยกรรมนี้อาจจะมีระดับที่แตกต่างกันออกไปบ้างในแต่ละประเทศ กล่าวคือ ในบางประเทศก็กำหนดไว้ค่อนข้างเคร่งครัดว่าจะต้องมีการส่งพินัยกรรมตัวจริงที่ผู้ทำพินัยกรรมลงลายมือชื่อในความรู้เห็นของพยานไปให้พยานทำการลงลายมือชื่อจริงๆ เพื่อให้เป็นพินัยกรรมที่สมบูรณ์โดยไม่อาจลงลายมือชื่อในสำเนาของตัวพินัยกรรมได้ เช่น ประเทศอังกฤษ หรือรัฐอัลเบอร์ตาของแคนาดา กำหนดไว้ค่อนข้างเคร่งครัดว่าจะต้องมีการส่งพินัยกรรมตัวจริงที่ผู้ทำพินัยกรรมลงลายมือชื่อในความรู้เห็นของพยานไปให้พยานทำการลงลายมือชื่อจริงๆ ในภายหลังโดยเร็วที่สุด เพื่อให้เป็นพินัยกรรมที่สมบูรณ์โดยพยานไม่สามารถลงลายมือชื่อในสำเนาของตัวพินัยกรรมได้[37] ในขณะที่บางประเทศ เช่น นิวซีแลนด์ หรือรัฐแคนซัส

---

[34] UK Government, ‘Guidance on making wills using video-conferencing (2020)’ <https://www.gov.uk/guidance/guidance-on-making-wills-using-video-conferencing> accessed 15 August 2022.

[35] UK Law Commission, Making a will- Consulting paper 231 (2017) 111.

[36] ตัวอย่างเช่น The Wills Act 1837 (Electronic Communications) (Amendment) (Coronavirus) Order 2020 (อังกฤษและเวลส์); Epidemic Preparedness (Wills Act 2007—Signing and Witnessing of Wills) Immediate Modification Order 2020 (นิวซีแลนด์); Alberta Ministerial Order 39/2020 [Justice and Solicitor General] (รัฐแอลเบอร์ตา แคนาดา); Electronic Transactions Amendment (COVID-19 Witnessing of Documents) Regulation 2020 (New South Wales) (รัฐนิวเซาท์เวลส์ ออสเตรเลีย), Justice Legislation (COVID-19 Emergency Response – Wills and Enduring Document) Regulation 2020 (Queensland) (รัฐควีนส์แลนด์ ออสเตรเลีย); New York Executive Order No.202.14 (Apr.7, 2020) (มลรัฐนิวยอร์ก สหรัฐอเมริกา), Kansas Executive Order No.20-20 (Apr.9, 2020) (มลรัฐแคนซัส สหรัฐอเมริกา) เป็นต้น

[37] Kimberley Martin, ‘Technology and wills – the dawn of a new era (COVID-19 special edition)’ (STEP 2020) 55.

ของสหรัฐอเมริกา ยอมรับให้พยานสามารถลงลายมือชื่อในสำเนาพินัยกรรมที่ผู้ทำพินัยกรรมส่งให้พยานด้วยวิธีการทางอิเล็กทรอนิกส์ได้ แต่ควรต้องจดแจ้งไว้ว่าการลงลายมือชื่อดังกล่าวเป็นการลงลายมือชื่อภายใต้วิธีการพยานทางไกลด้วยความจำเป็นอันเนื่องมาจากสถานการณ์โควิด[38]

แนวทางที่สอง อนุญาตให้มีการนำวิธีการเป็นพยานทางไกลมาใช้บังคับกับการทำพินัยกรรมแบบธรรมดา และอนุญาตให้ผู้ทำพินัยกรรมและพยานลงลายมือชื่ออิเล็กทรอนิกส์ในพินัยกรรม[39] อย่างไรก็ตาม แนวทางนี้ไม่ค่อยมีตัวอย่างปรากฏให้เห็นมากนัก เนื่องจากในหลายประเทศเห็นว่ายังไม่สมควรที่จะให้มีการใช้ลายมือชื่ออิเล็กทรอนิกส์ในพินัยกรรมรวมถึงการอนุญาตให้มีการทำพินัยกรรมอิเล็กทรอนิกส์ได้[40] ซึ่งอาจจะเป็นเพราะ มีการมองว่าพินัยกรรมเป็นธุรกรรมที่ต้องอาศัยความเป็นทางการหรือเคร่งครัดทางแบบพิธีเป็นพิเศษ[41] หรืออาจจะมีความกังวลเกี่ยวกับการฉ้อฉลในการลงลายมือชื่ออิเล็กทรอนิกส์ กล่าวคือ อาจจะมีผู้อื่นมาลงลายมือชื่อแทนโดยเจ้าของลายมือชื่อไม่มีส่วนรู้เห็น อีกทั้งการพิสูจน์ว่าลายมือชื่ออิเล็กทรอนิกส์เป็นของผู้ทำพินัยกรรมหรือพยานหรือไม่ก็มีความยุ่งยากหรือซับซ้อนกว่าการพิสูจน์ลายมือชื่อที่มีการลงกันทางกายภาพจริงๆ[42] อย่างไรก็ตาม ไม่ว่าประเทศต่างๆ จะเลือกใช้แนวทางไหนในการแก้ไขกฎหมาย แต่มีสิ่งสำคัญที่ตรงกันในทั้งสองแนวทางก็คือ การเป็นพยานทางไกลที่จะมาทดแทนการปรากฏตัวของพยานในทางกายภาพนั้นจะต้องอยู่ในลักษณะที่ผู้ทำพินัยกรรมและพยานต่างสามารถมองเห็นกันและกันได้อย่างชัดเจน (a clear line of sight) ในขณะที่แต่ละฝ่ายลงลายมือชื่อ[43] โดยอาศัยเทคโนโลยีที่สามารถช่วยให้เห็น ได้ยินและสื่อสารระหว่างกันได้ทันที (real time)[44] ในขณะที่มีการประชุมกันระหว่างผู้ทำพินัยกรรมและพยาน ทั้งนี้กฎหมายของบางประเทศก็ได้กำหนดข้อกำหนดเพิ่มเติมเกี่ยวกับคุณสมบัติของพยานเอาไว้ด้วย เช่น กฎหมายของรัฐออนแทรีโอ (Ontario) ของแคนาดาที่กำหนดให้พยานอย่างน้อยหนึ่งคนต้องเป็นทนายความที่ได้รับใบอนุญาต

---

[38] Martin (n 37) 54.

[39] ตัวอย่างเช่น COVID 19 Omnibus (Emergency Measures) (Electronic Signing and Witnessing) Regulations 2020 (Victoria) (รัฐวิคตอเรีย ออสเตรเลีย); Ministerial Order no. M161 (Electronic witnessing of wills (COVID-19) Order) (รัฐบริติชโคลัมเบีย แคนาดา).

[40] Martin (n 37) 11.

[41] พินัย ณ นคร (n 23) 140.

[42] UK Law Commission (n 35) 116.

[43] UK Government (n 34).

[44] Martin (n 37) 54.

จากรัฐ[45] หรือกฎหมายของมลรัฐนิวยอร์กของสหรัฐอเมริกา ที่กำหนดให้ต้องมีทนายความเข้าร่วมในการประชุมระหว่างผู้ทำพินัยกรรมและพยาน[46]

นอกจากนี้ยังมีข้อสังเกตว่า มาตรการทางกฎหมายของประเทศต่างๆ ที่อนุญาตให้มีการนำพยานทางไกลมาใช้ในการทำพินัยกรรมจะมีลักษณะเป็นมาตรการชั่วคราว (interim measures) กล่าวคือ จะใช้บังคับในช่วงเวลาใดเวลาหนึ่งตามที่กำหนดไว้ในกฎหมายเท่านั้น และเมื่อพ้นช่วงเวลาดังกล่าวไปแล้ว ก็จะต้องนำบทบัญญัติในเรื่องพินัยกรรมที่มีอยู่ก่อนสถานการณ์การแพร่ระบาดของโควิด-19 มาใช้บังคับ เช่น ตามกฎหมายอังกฤษ มาตรการนี้จะใช้บังคับแก่พินัยกรรมที่ทำขึ้นตั้งแต่วันที่ 31 มกราคม 2563 ถึงวันที่ 31 มกราคม 2567[47] ตามกฎหมายของนิวซีแลนด์กำหนดว่ามาตรการนี้ให้มีผลใช้บังคับจนกว่าประกาศมาตรการเตรียมพร้อมเพื่อรับมือกับโรคระบาดใหญ่ (โควิด-19) 2563 (The Epidemic Preparedness (COVID-19) Notice 2020) ซึ่งประกาศโดยรัฐบาลนิวซีแลนด์สิ้นผลไปหรือถูกยกเลิก[48] หรือตามกฎหมายของมลรัฐแคนซัสของสหรัฐอเมริกาที่กำหนดให้มาตรการนี้มีผลใช้บังคับในระหว่างที่ประกาศภาวะภัยพิบัติฉุกเฉินของมลรัฐเกี่ยวกับโรคระบาดโควิด-19 (The State of Disaster Emergency related to the Outbreak of COVID-19) มีผลใช้บังคับ เป็นต้น[49]

5. วิเคราะห์แนวทางในการปรับปรุงกฎหมายของไทยที่เกี่ยวข้องกับการเป็นพยานในพินัยกรรมแบบธรรมดาเพื่อให้สอดรับกับสถานการณ์ของการแพร่ระบาดของโรคโควิด-19

จากการพิจารณาถึงความจำเป็นของการมีพยานในการทำพินัยกรรม ปัญหาเกี่ยวกับการนำวิธีการในการเป็นพยานทางไกลมาใช้กับการทำพินัยกรรมแบบธรรมดาในประเทศไทย และแนวทางการบัญญัติกฎหมายของต่างประเทศที่อนุญาตให้นำวิธีการเป็นพยานทางไกลมาใช้กับการทำพินัยกรรมในช่วงสถานการณ์การแพร่ระบาดของโรคโควิด-19 มีประเด็นสำคัญที่ควรวิเคราะห์เพื่อพิจารณาแนวทางในการปรับปรุงกฎหมายของไทยเกี่ยวกับการเป็นพยานในพินัยกรรมแบบธรรมดาด้วยกันสองประเด็น ดังนี้

---

[45] Ontario Regulation 129/20 (Order under subsection 7.0.2 (4) of the Act – Signatures in wills and powers of attorney), Schedule 1, no.1.

[46] New York Executive Order no. 202.14 (Apr.7, 2020), para 7.

[47] Wills Act 1837, s 9 (2) ซึ่งแก้ไขเพิ่มเติมโดย The Wills Act 1837 (Electronic Communications) (Amendment) (Coronavirus) Order 2020 และ The Wills Act 1837 (Electronic Communications) (Amendment) Order 2022.

[48] Epidemic Preparedness (Wills Act 2007—Signing and Witnessing of Wills) Immediate Modification Order 2020, s 5.

[49] Kansas Executive Order No.20-20 (Apr.9, 2020), no.2.

ประเด็นแรก การตีความคำว่า “ต่อหน้า” พยานในมาตรา 1656[50] จะสามารถตีความให้รวมถึงการปรากฏอยู่ต่อหน้าผ่านวิดีโอคอนเฟอเรนซ์หรือเทคโนโลยีการถ่ายทอดภาพและเสียง (audio-visual links) ในรูปแบบต่างๆ ได้หรือไม่

เมื่อพิจารณาตามหลักการตีความกฎหมายโดยทั่วไป ผู้ตีความจะต้องทำการพิเคราะห์ตัวอักษรหรือถ้อยคำของบทบัญญัติแห่งกฎหมายเสียก่อนว่าสามารถให้ความหมายหลากหลายได้มากน้อยแค่ไหนเพียงใด จากนั้นจึงค้นหาเหตุผลหรือความมุ่งหมายของบทบัญญัติแห่งกฎหมายดังกล่าว เพื่อเอามาเป็นตัวกำหนดว่าจะเลือกเอาความหมายกว้างหรือแคบแค่ไหน[51] ซึ่งเมื่อพิจารณาถ้อยคำ “ต่อหน้า” แล้ว ย่อมมีความหมายเช่นเดียวกับคำว่า “เฉพาะหน้า”[52] และเมื่อพิจารณาบทบัญญัติต่างๆ ในประมวลกฎหมายแพ่งและพาณิชย์แล้ว ก็ปรากฏว่าคำว่า “เฉพาะหน้า”นั้น มีปรากฏอยู่ในบทบัญญัติเรื่องการแสดงเจตนาต่อบุคคลซึ่งอยู่เฉพาะหน้าในมาตรา 168[53] โดยในทางตำราได้มีการอธิบายเกี่ยวกับการแสดงเจตนาต่อบุคคลซึ่งอยู่เฉพาะหน้าเอาไว้ว่า หมายถึง การแสดงเจตนาที่บุคคลสามารถทราบหรือเข้าใจการแสดงเจตนาซึ่งกันและกันได้ทันที ไม่ว่าจะเป็นกรณีที่อยู่ต่อหน้ากันจริงๆ ทางกายภาพ หรือมิได้อยู่ต่อหน้ากันจริงๆ แต่ใช้วิธีอื่นซึ่งสามารถติดต่อสื่อสารถึงกันได้ทำนองเดียวกันก็อยู่ในความหมายของการแสดงเจตนาต่อบุคคลซึ่งอยู่เฉพาะหน้าได้[54] ดังนั้น จึงอาจเทียบเคียงลักษณะของการแสดงเจตนาต่อบุคคลซึ่งอยู่เฉพาะหน้ามาใช้ในการตีความเกี่ยวกับการลงลายมือชื่อของผู้ทำพินัยกรรม “ต่อหน้า” พยานได้ โดยควรแปลความการลงลายมือชื่อ “ต่อหน้า” พยานตามมาตรา 1656 ว่าหมายถึงกรณีที่มีการลงลายมือชื่อต่อหน้าพยานกันจริงๆ ในทางกายภาพ หรืออาจจะเป็นกรณีที่นำวิธีการการเป็นพยานทางไกลมาใช้ผ่านเทคโนโลยีการถ่ายทอดภาพและเสียงที่ทั้งผู้ทำพินัยกรรมและพยานสามารถติดต่อสื่อสารหรือเข้าใจการแสดงเจตนารวมไปถึงสามารถเห็นการลงลายมือชื่อของผู้ที่เกี่ยวข้องในพินัยกรรมได้ทันทีในลักษณะ real time เช่น Skype หรือ Facetime [55] นอกจากนี้ หากพิจารณาความมุ่งหมายของการมีพยานใน

---

[50] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 1656 วรรคแรก บัญญัติว่า “พินัยกรรมนั้น...ผู้ทำพินัยกรรมต้องลงลายมือชื่อไว้***ต่อหน้า***พยานอย่างน้อยสองคนพร้อมกัน ซึ่งพยานสองคนนั้นต้องลงลายมือชื่อของผู้ทำพินัยกรรมไว้ในขณะนั้น”

[51] สมยศ เชื้อไทย, *คำอธิบายวิชากฎหมายแพ่ง : หลักทั่วไป* (พิมพ์ครั้งที่ 23, สำนักพิมพ์วิญญูชน 2560) 177.

[52] พจนานุกรมฉบับราชบัณฑิตสถาน พ.ศ. 2554

[53] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 168 บัญญัติว่า “การแสดงเจตนาที่กระทำต่อบุคคลซึ่งอยู่***เฉพาะหน้า***ให้ถือว่ามีผลนับแต่ผู้รับการแสดงเจตนาได้ทราบการแสดงเจตนานั้น ความข้อนี้ให้ใช้ตลอดถึงการที่บุคคลหนึ่งแสดงเจตนาไปยังบุคคลอีกคนหนึ่งโดยทางโทรศัพท์ หรือโดยเครื่องมือสื่อสารอย่างอื่น หรือโดยวิธีอื่นซึ่งสามารถติดต่อถึงกันได้ทำนองเดียวกัน”

[54] จิ๊ด เศรษฐบุตร, *หลักกฎหมายแพ่งลักษณะนิติกรรมและสัญญา* (พิมพ์ครั้งที่ 5 แก้ไขเพิ่มเติม, โครงการตำราและเอกสารประกอบการสอนคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2552) 124; ศักดิ์ สนองชาติ, *คำอธิบายประมวลกฎหมายแพ่งและพาณิชย์ ว่าด้วยนิติกรรมและสัญญา* (พิมพ์ครั้งที่ 10 แก้ไขเพิ่มเติม, สำนักพิมพ์นิติบรรณการ 2551) 219; ศนันท์กรณ์ โสตถิพันธุ์, คำอธิบายนิติกรรม สัญญา (พิมพ์ครั้งที่ 16 แก้ไขเพิ่มเติม, สำนักพิมพ์วิญญูชน 2554) 142.

[55] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, *สัญญาต้องเป็นสัญญา* (2557) 23.

พินัยกรรมก็เพื่อให้มีบุคคลอื่นซึ่งไม่ใช่ผู้ที่รับพินัยกรรมมารับรู้ถึงการทำพินัยกรรมของผู้ทำพินัยกรรมและช่วยยืนยันว่าผู้ทำพินัยกรรมได้ทำพินัยกรรมไปด้วยเจตนาที่แท้จริง โดยปราศจากการถูกฉ้อฉลหรือข่มขู่ จึงได้ลงลายมือชื่อในพินัยกรรมของตน ดังนั้น การทำหน้าที่ของพยานดังกล่าวจึงไม่ควรถูกจำกัดว่าจะต้องเป็นการมารับรู้ถึงการลงลายมือชื่อของผู้ทำพินัยกรรมโดยมาปรากฏตัวอยู่ในสถานที่เดียวกันกับผู้ทำพินัยกรรมเท่านั้น แต่ควรตีความให้รวมไปถึงการเป็นพยานทางไกลผ่านการใช้เทคโนโลยีในรูปแบบอื่นๆ ที่ทำให้พยานสามารถเห็นถึงการลงลายมือชื่อของผู้ทำพินัยกรรม หรือในทางกลับกัน ผู้ทำพินัยกรรมก็สามารถเห็นพยานลงลายมือชื่อได้อย่างชัดเจนด้วย ทั้งนี้ อาจเทียบเคียงได้กับหลักในเรื่อง “a line of sight” ในกฎหมายของอังกฤษ

เหตุผลอีกประการหนึ่งที่ผู้เขียนตีความในลักษณะดังกล่าว ก็คือ ในการตีความกฎหมายแพ่ง ผู้ตีความควรตีความเพื่อให้สอดคล้องกับสภาวการณ์ที่เปลี่ยนแปลงไป เพื่อนำไปสู่ผลในทางกฎหมายที่เป็นธรรม ตราบเท่าที่ไม่เป็นการบิดเบือนกฎหมาย[56] ในกรณีนี้จึงสมควรตีความคำว่า “ต่อหน้า” อย่างกว้างเพื่อให้ครอบคลุมถึงการลงลายมือชื่อต่อหน้าพยานที่มิได้อยู่ในสถานที่เดียวกับผู้ทำพินัยกรรม แต่อยู่ต่อหน้าจอที่มีการประชุมพร้อมกันผ่านทางวีดีโอคอนเฟอเรนซ์หรือโปรแกรมประชุมออนไลน์อื่นๆ ที่สามารถเห็นถึงการลงลายมือชื่อได้เช่นเดียวกับการอยู่ต่อหน้ากันจริงๆ เพื่อให้การทำพินัยกรรมแบบธรรมดาสามารถทำได้จริงในสถานการณ์การระบาดของโรคโควิด-19 ซึ่งหากตีความคำว่า “ต่อหน้า” โดยเคร่งครัดแล้ว ย่อมส่งผลให้การทำพินัยกรรมที่ต้องมีพยาน ไม่อาจกระทำได้โดยสภาพ และเมื่อเราสามารถตีความคำว่า “ต่อหน้า” ในมาตรา 1656 ให้ครอบคลุมถึงกรณีการลงลายมือชื่อต่อหน้าพยานทางไกลแล้ว ก็ไม่มีความจำเป็นที่จะต้องแก้ไขเพิ่มเติมบทบัญญัติในมาตราดังกล่าวแต่อย่างใด

อย่างไรก็ดีเพื่อให้เกิดความชัดเจนและป้องกันข้อพิพาทที่อาจจะเกิดขึ้นในอนาคต ผู้เขียนเห็นว่าในระยะยาว รัฐอาจพิจารณาในการแก้ไขเพิ่มเติมบทบัญญัติเกี่ยวกับการเป็นพยานในพินัยกรรมให้ครอบคลุมถึงการเป็นพยานทางไกลด้วย โดยอาจกำหนดให้การลงลายมือชื่อของผู้ทำพินัยกรรมต่อหน้าพยานหรือกลับกันให้หมายความรวมถึง การลงลายมือชื่อต่อหน้ากันผ่านเทคโนโลยีถ่ายทอดภาพและเสียงที่สามารถเห็น ได้ยินและสื่อสารระหว่างกันได้ทันที นอกจากนี้ ผู้เขียนยังเห็นว่า การบัญญัติกฎหมายในลักษณะดังกล่าวสมควรที่จะบัญญัติขึ้นเพื่อรองรับเหตุการณ์ในลักษณะเดียวกันที่อาจเกิดขึ้นในอนาคตด้วย เช่น โรคระบาดหรือภัยพิบัติอื่นๆ ที่อาจเกิดขึ้นในอนาคต อีกทั้งยังเป็นการตอบสนองต่อการเปลี่ยนแปลงทางเทคโนโลยีที่เกิดขึ้นในสังคมที่เกิดขึ้นอย่างรวดเร็ว ดังนั้น จึงไม่ควรที่จะอนุญาตให้มีการใช้บังคับมาตรการดังกล่าวเฉพาะแต่ในสถานการณ์การแพร่ระบาดของโควิด-19 เท่านั้น

[56] สมยศ เชื้อไทย (n 51) 189.

ประเด็นที่สอง สมควรที่จะอนุญาตให้ผู้ทำพินัยกรรมและพยานลงลายมือชื่ออิเล็กทรอนิกส์ในพินัยกรรมในสถานการณ์โควิดได้หรือไม่

ประเด็นนี้เป็นประเด็นที่สืบเนื่องมาจากประเด็นแรก กล่าวคือ เมื่อมีการยอมรับให้นำวิธีการพยานทางไกลมาใช้ ก็จะต้องพิจารณาต่อไปว่า พยานในพินัยกรรมจะลงลายมือชื่อรับรองการลงลายมือชื่อของผู้ทำพินัยกรรมในพินัยกรรมได้อย่างไร ซึ่งแนวทางในการลงลายมือชื่อของพยานในพินัยกรรมก็อาจจะแบ่งออกได้เป็นสองวิธีด้วยกัน คือ วิธีแรก ให้พยานสามารถลงลายมือชื่ออิเล็กทรอนิกส์ในพินัยกรรมที่ผู้ทำพินัยกรรมส่งให้พยานแต่ละคน หรือวิธีที่สอง ให้ผู้ทำพินัยกรรมส่งพินัยกรรมตัวจริงให้พยานไปลงลายมือชื่อกันจริงๆ ภายหลังจากที่ผู้ทำพินัยกรรมได้ลงลายมือชื่อต่อหน้าพยานทางไกลแล้ว ซึ่งในความเห็นของผู้เขียนเห็นว่าควรที่จะดำเนินการตามกรณีหลัง เนื่องจากเป็นเรื่องที่สามารถดำเนินการได้ทันที โดยไม่ต้องรอให้มีการแก้ไขกฎหมาย เพราะหากเลือกที่จะดำเนินการตามวิธีการแรก ก็จำเป็นที่จะต้องแก้ไขพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เพื่ออนุญาตให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้กับธุรกรรมเกี่ยวกับมรดกได้ซึ่งรวมถึงการใช้ลายมือชื่ออิเล็กทรอนิกส์ในพินัยกรรม ซึ่งอาจใช้เวลาค่อนข้างมาก อีกทั้งยังจำเป็นต้องอาศัยการเปลี่ยนแปลงในเชิงนโยบายของรัฐเพื่อมาสนับสนุนการดำเนินการในเรื่องดังกล่าว[57] ในขณะที่หากดำเนินการตามวิธีที่สอง ผู้ทำพินัยกรรมและพยานสามารถลงลายมือชื่อในพินัยกรรมได้ตามกฎหมายที่ใช้บังคับอยู่ในปัจจุบัน อย่างไรก็ตาม การลงลายมือชื่อของพยานในภายหลังนี้จำเป็นอย่างยิ่งที่ทั้งผู้ทำพินัยกรรมและพยานจะต้องมาอยู่พร้อมหน้ากันอีกครั้ง ไม่ว่าจะเป็นการอยู่ต่อหน้าทางกายภาพก็ดี หรืออยู่พร้อมหน้ากันทางหน้าจอของวีดีโอคอนเฟอเรนซ์หรือโปรแกรมประชุมออนไลน์ต่างๆ เพื่อให้ผู้ทำพินัยกรรมได้รับรู้ถึงการลงลายมือชื่อของพยาน[58] ซึ่งวิธีการดังกล่าวนี้ ก็สอดคล้องกับแนวปฏิบัติของประเทศอังกฤษที่กำหนดว่าหากพยานไม่สามารถมาลงลายมือชื่อต่อหน้าผู้ทำพินัยกรรมได้ ก็จะต้องใช้

---

[57] ในปัจจุบันพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ยังไม่อนุญาตให้ใช้ข้อมูลอิเล็กทรอนิกส์แก่ธุรกรรมเกี่ยวกับมรดก รวมถึงการทำพินัยกรรมแบบธรรมดา เนื่องจาก เห็นว่าธุรกรรมเกี่ยวกับมรดกเป็นเรื่องที่มีความละเอียดอ่อนและเป็นประเด็นที่นำไปสู่ความขัดแย้งได้โดยง่ายจึงสมควรยกเว้นมิให้ดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

[58] กรณีนี้เทียบเคียงได้กับกรณีข้อเท็จจริงตามคำพิพากษาศาลฎีกาที่ 1378/2500 ซึ่งเป็นกรณีที่พยานลงลายมือชื่อในพินัยกรรมต่อหน้าผู้ทำพินัยกรรม อีกสามวันต่อมา ผู้ทำพินัยกรรมจึงได้ลงลายพิมพ์นิ้วมือต่อหน้าพยานชุดเดิม ศาลฎีกาวินิจฉัยว่า กรณีนี้เป็นพินัยกรรมที่ถูกต้องเข้าเกณฑ์ครบถ้วนตามมาตรา 1656 ดังนั้น จึงอาจจะอนุมานได้จากคำพิพากษาศาลฎีกานี้ว่าไม่จำเป็นที่บุคคลที่เกี่ยวข้องทั้งหมด (ผู้ทำพินัยกรรมและพยานสองคน) ต้องลงลายมือชื่อในเวลาเดียวกัน แต่ละคนอาจจะลงลายมือชื่อไม่พร้อมกันก็ได้ แต่ต้องปรากฏว่าในขณะที่แต่ละคนลงลายมือชื่อนั้น คนอื่นๆ จะต้องอยู่รู้เห็นด้วย เพื่อให้เป็นไปตามเจตนารมณ์ของกฎหมาย

วิธีการประชุมทางวีดีโอคอนเฟอเรนซ์หรือโปรแกรมประชุมออนไลน์ และใช้วิธีการเป็นพยานทางไกลอีกครั้งหนึ่ง โดยผู้ทำพินัยกรรมจะต้องเห็นพยานอย่างชัดเจนในขณะที่พยานลงลายมือชื่อในพินัยกรรม[59]

6. สรุป

การทำพินัยกรรมแบบธรรมดาในประเทศไทยมีความจำเป็นอย่างยิ่งที่จะต้องมีพยานเพื่อยืนยันว่าพินัยกรรมนั้นได้ทำขึ้นตามเจตนาที่แท้จริงของผู้ทำพินัยกรรม กฎหมายจึงได้กำหนดให้ผู้ทำพินัยกรรมต้องลงลายมือชื่อต่อหน้าพยานอย่างน้อยสองคน และพยานก็จะต้องลงลายมือชื่อเพื่อรับรองลายมือชื่อของผู้ทำพินัยกรรมในขณะนั้น อย่างไรก็ตาม เมื่อมีสถานการณ์การแพร่ระบาดของโรคโควิด-19 เกิดขึ้นในปี 2563 ก็ก่อให้เกิดปัญหาว่าในสถานการณ์เช่นนี้ การให้ผู้ทำพินัยกรรมและพยานอย่างน้อยสองคนมาอยู่ในที่เดียวกันเพื่อรับรองการทำพินัยกรรมย่อมก่อให้เกิดความเสี่ยงในการติดเชื้อโควิด-19 ซึ่งทำให้หลายประเทศ โดยเฉพาะอย่างยิ่งในประเทศที่ใช้ระบบกฎหมายคอมมอนลอว์ตัดสินใจในการแก้ไขกฎหมายของตนเพื่ออนุญาตให้มีการนำวิธีการเป็นพยานทางไกล (remote witnessing) มาใช้ทดแทนการรวมกลุ่มกันระหว่างผู้ทำพินัยกรรมและพยาน โดยถือว่ากรณีที่ผู้ทำพินัยกรรมได้ลงลายมือชื่อต่อหน้าพยานหรือพยานลงลายมือชื่อต่อหน้าผู้ทำพินัยกรรมผ่านทางวิดีโอคอนเฟอเรนซ์หรือเทคโนโลยีถ่ายทอดภาพและเสียงย่อมมีผลเช่นเดียวกับการลงลายมือชื่อต่อหน้ากันในทางกายภาพ ซึ่งเมื่อพิเคราะห์บทบัญญัติในประมวลกฎหมายแพ่งและพาณิชย์มาตรา 1656 แล้ว ก็อาจตีความว่าการลงลายมือชื่อต่อหน้าพยานโดยผู้ทำพินัยกรรมก็ดี หรือการลงลายมือชื่อต่อหน้าผู้ทำพินัยกรรมโดยพยานทั้งสองคนก็ดี ย่อมหมายความรวมถึงกรณีที่ลงลายมือชื่อในกรณีที่เป็นพยานทางไกลด้วย แต่อย่างไรก็ตาม เพื่อป้องกันข้อพิพาทที่อาจจะเกิดขึ้น ก็สมควรที่จะแก้ไขเพิ่มเติมหลักเกณฑ์เกี่ยวกับการเป็นพยานในพินัยกรรมแบบธรรมดาให้ครอบคลุมไปถึงการเป็นพยานต่อหน้ากันผ่านเทคโนโลยีถ่ายทอดภาพและเสียงที่สามารถเห็น ได้ยิน และสื่อสารระหว่างกันได้ทันที อีกทั้งยังสอดรับการเปลี่ยนแปลงทางเทคโนโลยีดิจิทัลอย่างรวดเร็วสืบเนื่องจากสถานการณ์การแพร่ระบาดของโรคโควิด-19 อีกด้วย

[59] UK Government (n 34).

การปฏิรูปกฎหมายเกี่ยวกับความรับผิดทางอาญาของผู้กระทำความผิดที่มีความผิดปกติทางจิตของประเทศไทย: กรณีมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตตามประมวลกฎหมายอาญา มาตรา 65*

Reforming Laws Regarding Criminal Responsibility of Mentally Disordered Offenders in Thailand: The Disposal of Mentally Disordered offenders under Section 65 of the Criminal Code of Thailand

*ญาดา เดชชัย เธียรประสิทธิ์***

คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

Yada Dejchai Tianprasit

Faculty of Law, Thammasat University

วันที่รับบทความ 4 เมษายน 2566; วันแก้ไขบทความ 2 มิถุนายน 2566; วันตอบรับบทความ 2 มิถุนายน 2566

บทคัดย่อ

มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตตามประมวลกฎหมายอาญา มาตรา 65 (ข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริต) ของประเทศไทยนั้นบัญญัติไว้ในมาตรา 48 ซึ่งประกอบได้ด้วยสองมาตรการ ได้แก่ การคุมตัวไว้ในสถานพยาบาลและการปล่อยตัว โดยมาตรการดังกล่าวเป็นส่วนหนึ่งของวิธีการเพื่อความปลอดภัยตามประมวลกฎหมายอาญา และจะกระทำได้โดยคำสั่งศาลเท่านั้น

---

*บทความวิจัยนี้คัดและแปลมาจากดุษฎีนิพนธ์ Yada Dejchai, 'Reforming the Insanity Defence in Thailand: A Comparative Study in the Light of Legal Developments in Scotland and England and Wales' (PhD Thesis, University of Aberdeen 2020) และเป็นบทความที่สองในชุดบทความเรื่องการปฏิรูปกฎหมายเกี่ยวกับความรับผิดทางอาญาของผู้กระทำความผิดที่มีความผิดปกติทางจิตของประเทศไทย สำหรับบทความแรก โปรดดู ญาดา เดชชัย เธียรประสิทธิ์, 'การปฏิรูปกฎหมายเกี่ยวกับความรับผิดทางอาญาของผู้กระทำความผิดที่มีความผิดปกติทางจิตของประเทศไทย: กรณีข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริตตามประมวลกฎหมายอาญา มาตรา 65' (2566) วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปี 52 ฉบับที่ 1 หน้า 1-25.

** อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, นิติศาสตรบัณฑิต มหาวิทยาลัยธรรมศาสตร์, Master of Laws with Merit, Oxford Brookes University, UK, Doctor of Philosophy, University of Aberdeen, UK.

ทั้งนี้ การที่ประมวลกฎหมายอาญากำหนดให้มีเพียงแค่สองมาตรการข้างต้นนั้นทำให้ศาลมีข้อจำกัดในเลือกใช้มาตรการ เพราะมีให้เลือกแค่หากปล่อยไปน่าจะเป็นอันตรายก็ให้คุมตัวไว้รักษาพยาบาล หรือหากเห็นว่าไม่เป็นอันตรายก็ให้ปล่อยตัวไป ดังนั้น หากเป็นกรณีที่อาจจะไม่ได้เป็นอันตรายถึงขนาด แต่ก็ควรได้รับการรักษาพยาบาลก็ทำให้ศาลต้องเลือกคุมตัวหรือปล่อยไปเท่านั้น ไม่สามารถสั่งให้บำบัดรักษาในรูปแบบอื่นได้ ทำให้อาจไม่ได้เป็นการบังคับใช้มาตรการที่เหมาะสมที่สุดในการจัดการผู้กระทำความผิดที่มีความผิดปกติทางจิต ซึ่งอาจส่งผลให้ผู้กระทำความผิดไม่ได้รับการบำบัดรักษาและมีความเสี่ยงที่จะก่ออันตรายต่อสังคมหรือกระทำผิดซ้ำต่อไป

ดังนั้น บทความวิจัยนี้จึงมุ่งนำเสนอการแก้ไขมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตของประเทศไทยให้มีความหลากหลายและมีการเงื่อนไขการบังคับใช้ที่เหมาะสมมากขึ้น โดยศึกษามาตรการปัจจุบันของประเทศไทยพร้อมทั้งวิเคราะห์ปัญหา และศึกษาเปรียบเทียบกับมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตของสหราชอาณาจักร (อังกฤษและเวลส์ และสกอตแลนด์)

คำสำคัญ: ผู้กระทำความผิดที่มีความผิดปกติทางจิต, มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิต, วิธีการเพื่อความปลอดภัย, การคุมตัวไว้ในสถานพยาบาล

Abstract

The disposal of mentally disordered offenders according to Section 65 (the insanity defence) of the Criminal Code of Thailand could be found under Section 48, which composites of a hospital order and an absolute discharge. These two measures are a part of measures of safety under the Criminal Code of Thailand and could only be imposed by the court order.

In this regard, the option of the court in Thailand to impose the disposal is very limited. Since it could only choose between if the offender is deemed to be dangerous, thus, the court should impose a hospital order, or if the offender seems not be dangerous, then, the court should make an absolute discharge. Therefore, in a case where the offender might not be that dangerous, but he should have received a treatment, the court will not have other options in between the above two measures. In this sense, sometimes the court might not have the best disposal available. Consequently, the offender might not receive treatment, thus, he might still pose risk to the society, or he might reoffend.

Therefore, this research article aims to propose the new disposal under Thai's law, in this regard, the reformed disposal should be more various and have more suitable options to be imposed. It will do so by analysing the current law relating to the disposal as well as its problems, and conduct a comparative analysis with the law relating to the disposal in United Kingdom (England and Wales, and Scotland)

Keywords: Mentally Disordered Offenders, Disposal, Measures of Safety, Hospital Order

1. บทนำ

ในปัจจุบัน กฎหมายหลักที่เกี่ยวข้องเกี่ยวข้องกับมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตตามประมวลกฎหมายอาญา มาตรา 65 ของประเทศไทย ได้แก่ ประมวลกฎหมายอาญา มาตรา 48 และ พระราชบัญญัติสุขภาพจิต พ.ศ.2551 ในส่วนที่เกี่ยวข้องกับผู้ป่วยคดี

โดยในส่วนของการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตตามประมวลกฎหมายอาญา มาตรา 65 จะขึ้นอยู่กับผลของการยกข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริต (ประมวลกฎหมายอาญา มาตรา 65)[1] ซึ่งหากยกข้อต่อสู้ฯ ได้สำเร็จจะมีผลเป็นสองกรณี ได้แก่ การยกเว้นโทษ หากเป็นกรณีผู้กระทำความผิดไม่รู้ผิดชอบหรือไม่สามารถบังคับตนได้ (มาตรา 65 วรรคแรก) และการลดโทษหากเป็นกรณีผู้กระทำความผิดยังรู้ผิดชอบหรือยังสามารถบังคับตนได้บ้าง (มาตรา 65 วรรคสอง) นอกเหนือไปจากนี้ หากศาลเห็นว่าการปล่อยตัวผู้กระทำความผิดไป เป็นการไม่ปลอดภัยแก่ประชาชน ศาลอาจสั่งให้คุมตัวบุคคลนั้นไว้ในสถานพยาบาลได้ตามมาตรา 48 อันเป็นส่วนหนึ่งของวิธีการเพื่อความปลอดภัยภายใต้ประมวลกฎหมายอาญา โดยหากมีคำสั่งคุมตัวไว้ในสถานพยาบาล พระราชบัญญัติสุขภาพจิต พ.ศ.2551 ในส่วนที่เกี่ยวข้องกับผู้ป่วยคดี ได้มีการกำหนดเงื่อนไขและรายละเอียดในการบำบัดรักษาและปล่อยตัวผู้ป่วยคดีเอาไว้ ซึ่งส่วนนี้เองคือมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิต (disposals) ตามประมวลกฎหมายอาญา มาตรา 65 ของประเทศไทย

สำหรับเหตุผลของการสั่งให้คุมตัวไว้ในสถานพยาบาลนั้น ก็เนื่องจากว่า ถึงแม้ผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตนั้นจะไม่ต้องรับโทษ (ตามวรรคแรก) หรือต้องรับโทษอยู่ (ตามวรรคสอง) แต่เนื่องจากผู้กระทำความผิดอันอาจมีภาวะที่เป็นอันตรายต่อสังคมและ/หรือตนเองอยู่ จึงมีมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตเพื่อความปลอดภัยของสาธารณะ เนื่องจากความเชื่อดั้งเดิมที่ว่า ความบ้า (insanity) มีแนวโน้มจะเป็นอันตรายและเกิดซ้ำได้[2] จึงใช้มาตรการคุมตัวในสถานพยาบาลเพื่อฟื้นฟูผู้กระทำความผิดฯ และการฟื้นฟูนี้ยังช่วยให้สาธารณะปลอดภัย เพราะโอกาสที่จะกระทำผิดซ้ำน้อยหรือไม่มีเลยเนื่องจากถูกคุมตัวไว้รักษาพยาบาลแล้ว อันสืบเนื่องมาจากแนวคิดที่ว่าผู้กระทำความผิดฯนั้นกระทำความผิดเพราะ ‘ความบ้า’ ดังนั้น เมื่อรักษาอาการแล้ว สาเหตุของการกระทำความผิดก็ไม่มีอีกต่อไป นอกจากนี้ การคุมตัวผู้กระทำความผิดที่มีความผิดปกติทางจิตไว้ในสถานพยาบาลเพื่อ

---

[1] สำหรับรายละเอียดเรื่องข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริต ตามประมวลกฎหมายอาญา มาตรา 65 โปรดดู ญาดา เดชชัย เธียรประสิทธิ์, ‘การปฏิรูปกฎหมายเกี่ยวกับความรับผิดทางอาญาของผู้กระทำความผิดที่มีความผิดปกติทางจิตของประเทศไทย: กรณีข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริตตามประมวลกฎหมายอาญา มาตรา 65’ (2566) วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปี 52 ฉบับที่ 1 หน้า 1-25.

[2] โปรดดู Lord Diplock in *R v Sullivan* [1984] AC 156 and Lord Denning in *Bratty v A-G for N. Ireland* [1963] AC 386.

บำบัดรักษานี้ยังเป็นเครื่องมือให้รัฐทำหน้าที่ผู้ปกครอง (paternal duty) โดยการผลักดันให้มีการบังคับบำบัดรักษา เพื่อประโยชน์แห่งผู้นั้นเอง[3]

ในแง่นี้ จึงมีความสำคัญที่ต้องแยกความแตกต่างระหว่างมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิต (disposals) และการลงโทษ เนื่องจากอาจมีข้อโต้แย้งได้ว่าจุดมุ่งหมายของทั้งมาตรการจัดการฯและการลงโทษนั้นคือเพื่อความสงบเรียบร้อยของสังคม โดยอนุญาตให้มีการจำกัดเสรีภาพของผู้กระทำความผิดนั้น เช่น การนำตัวไปไว้ในโรงพยาบาลจิตเวชหรือเรือนจำ เพื่อความปลอดภัยของสาธารณะ แต่อย่างไรก็ตาม ความแตกต่างหลักและที่สำคัญของทั้งสองคือมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตนั้นไม่เป็นการที่ผู้กระทำความผิดได้รับการประณาม (condemnation) จากสังคมโดยการถูกตราหน้าว่ามีความรับผิดทางอาญา (criminally responsible)[4] หรือสมควรถูกกล่าวโทษ (blameworthy) ดังนั้น จึงไม่ควรมีการลงโทษ ตามหลักการ ‘ผู้ที่มีความผิดปกติทางจิตไม่ควรต้องรับผิด’ ซึ่งต่างจากการลงโทษ เพราะการลงโทษนั้นจะประกอบไปด้วยทั้งสามสิ่งข้างต้น

จะเห็นได้ว่ามาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตนั้นมีความจำเป็น อย่างไรก็ดี เมื่อพิจารณาดูแล้ว มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตของประเทศไทยนั้นมีเพียงสองวิธีการ ได้แก่ การคุมตัวในสถานพยาบาลตามประมวลกฎหมายอาญา มาตรา 48 และการปล่อยตัว ทำให้ไม่มีความหลากหลายในการเลือกบังคับใช้มาตรการที่เหมาะสมที่สุดกับผู้กระทำความผิดแต่ละคนที่อาจจะมีอาการป่วยที่รุนแรงไม่เท่ากัน โดยเฉพาะอย่างยิ่งกรณีที่ผู้กระทำความผิดนั้นอาจมีภาวะเสี่ยงที่ควรได้รับการรักษา แต่ไม่มีอาการรุนแรงถึงขนาดต้องคุมตัวในสถานพยาบาลเพื่อรักษา แต่หากไม่คุมตัวไว้รักษาก็ต้องปล่อยตัวไป เช่นนี้ เพื่อเป็นการบำบัดรักษาผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตอย่างมีประสิทธิภาพ และไม่เป็นการลิดรอนสิทธิของผู้กระทำความผิดเกินสมควรกว่าเหตุ

---

[3] มีข้อโต้แย้งอยู่เช่นกันว่า มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ป่วยจิตเวชนั้นขัดแย้งกับอนุสัญญาว่าด้วยสิทธิคนพิการ (Convention of Rights of Persons with Disabilities) อย่างไรก็ดี หากพิจารณาดูตามความมุ่งหมายของอนุสัญญาฯ และเงื่อนไขการบังคับใช้มาตรการฯแล้วนั้นจะพบว่า แท้จริงแล้ว การใช้มาตรการฯนั้นไม่ขัดต่ออนุสัญญาฯแต่อย่างใด สำหรับรายละเอียด โปรดดู Yada Dejchai, ‘Balancing Rights of Mentally Disordered Offenders and Public’s Safety: The Compatibility of Conventions on The Rights of Persons With Disabilities’ (2564) The 10th ICADA 2021-SSIS. <http://icada2021.nida.ac.th/main/images/icada2021/the_proceedings_of_the10thICADA2021Compleat_N.pdf> สืบค้นวันที่ 2 เมษายน 2566.

[4] ในส่วนของประเทศไทย ผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตยังคงมีความรับผิดอยู่ แต่ไม่ต้องรับโทษหรือได้ลดโทษ ตามประมวลกฎหมายอาญา มาตรา 65

บทความวิจัยฉบับนี้จึงมุ่งนำเสนอการแก้ไขมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตของประเทศไทยให้มีความหลากหลายและยืดหยุ่นในการเลือกบังคับใช้ที่มากขึ้น โดยศึกษาเปรียบเทียบและวิเคราะห์มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตของประเทศไทย และสหราชอาณาจักร (อังกฤษและเวลส์และสกอตแลนด์) เพื่อจัดทำข้อเสนอในการแก้ไขกฎหมายที่เกี่ยวข้องกับมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตของประเทศไทยต่อไป

2. กฎหมายที่เกี่ยวข้องกับมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิต

2.1 ประเทศไทย

ในกรณีที่จำเลยสามารถยกข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริตตามประมวลกฎหมายอาญามาตรา 65 สำเร็จ ศาลมีทางเลือกสองทางในการบังคับใช้มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิต ได้แก่ คำสั่งให้คุมตัวในสถานพยาบาลหรือการปล่อยตัว โดยคำสั่งให้คุมตัวในสถานพยาบาลเป็นส่วนหนึ่งของวิธีการเพื่อความปลอดภัยตามมาตรา 48 แห่งประมวลกฎหมายอาญา ซึ่งบัญญัติว่า “ถ้าศาลเห็นว่า การปล่อยตัวผู้มีจิตบกพร่อง โรคจิตหรือจิตฟั่นเฟือน ซึ่งไม่ต้องรับโทษหรือได้รับการลดโทษตามมาตรา 65 จะเป็นการไม่ปลอดภัยแก่ประชาชน ศาลจะสั่งให้ส่งไปคุมตัวไว้ในสถานพยาบาลก็ได้ และคำสั่งนี้ศาลจะเพิกถอนเสียเมื่อใดก็ได้”[5]

โดยเงื่อนไขของการคุมตัวไว้ในสถานพยาบาลตามมาตรา 48 นั้น เป็นดังต่อไปนี้ ผู้กระทำความผิดที่มีความผิดปกติทางจิต ซึ่งยกข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริตตามมาตรา 65 วรรค 1 หรือวรรค 2 สำเร็จ อาจถูกสั่งให้ถูกคุมตัวไว้ในสถานพยาบาล หากศาลเห็นว่าการปล่อยตัวผู้กระทำผิดไปนั้นมีความเสี่ยงต่อความปลอดภัยสาธารณะ ทั้งนี้ การคุมตัวไว้ในสถานพยาบาลต้องกระทำโดยคำสั่งศาล และ ขึ้นกับดุลยพินิจของศาล เฉพาะกรณีที่หากเห็นว่าผู้กระทำความผิดนั้นเป็นบุคคลอันตรายและควรต้องรับการรักษาโดยศาลจะถอนคำสั่งเมื่อใดก็ได้[6]

ในการประเมินความเสี่ยงต่อสาธารณะ หรือกรณีการประเมินว่าผู้กระทำความผิดควรได้รับการรักษาในโรงพยาบาลหรือไม่ ศาลจะสั่งให้ผู้กระทำความผิด (ซึ่งยกข้อต่อสู้เรื่องวิกลจริต) ไปรับการประเมิน ‘ความอันตราย’ จากจิตแพทย์ที่สถาบันกัลยาณ์ราชนครินทร์ซึ่งเป็นสถาบันนิติจิตเวชแห่งเดียวในประเทศไทย[7]

---

[5] ประมวลกฎหมายอาญา มาตรา 48.

[6] Ibid.

[7] วนัทดา ถมค้าพาณิชย์ และดวงตา ไกรภัสสร์พงษ์, ‘ความเห็นของจิตแพทย์ในการดำเนินคดีอาญา’ (2552) 17(2) วารสารสุขภาพจิตแห่งประเทศไทย, 126.

ในที่นี้ แม้จะแพทย์จะมีความเห็นให้คุมตัวผู้กระทำความผิดไว้ในสถานพยาบาล แต่ศาลอาจไม่เห็นด้วยและไม่ทำตามก็ได้ เนื่องจากความเห็นของแพทย์นั้นไม่ได้ผูกพันต่อการออกคำสั่งศาล[8]

ในทางปฏิบัติ การคุมตัวไว้ในสถานพยาบาลนั้น สามารถใช้แก่ผู้กระทำความผิดที่มีความผิดปกติทางจิต ซึ่งยกข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริตตามมาตรา 65 วรรค 1 ได้เลย แต่ในทางตรงข้ามผู้กระทำความผิดที่ยังสามารถรู้ผิดชอบอยู่บ้างตามมาตรา 65 วรรค 2 ศาลต้องประวิงการลงโทษจำคุกไปเสียก่อนตาม ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 246 ก่อนที่จะสั่งให้คุมตัวไว้ในสถานพยาบาลได้[9] อย่างไรก็ดี ในทางปฏิบัติ มีความเป็นไปได้น้อยที่ผู้กระทำความผิดตามวรรค 2 จะถูกสั่งให้คุมตัวไว้ในสถานพยาบาลก่อนถูกลงโทษจำคุก เนื่องจากศาลอาจเห็นว่าระดับความวิกลจริตนั้นยังไม่มากพอที่จะสั่งให้เข้ารักษาในโรงพยาบาล โดยคำสั่งให้คุมตัวไว้ในสถานพยาบาลมักใช้บังคับกับผู้ที่เป็นโรคทางจิตเวชที่มี ‘ความวิกลจริตอย่างเห็นได้ชัด’ และก่อคดีอุกฉกรรจ์ เช่น ฆาตกรรม พยายามฆ่าและทำร้ายผู้อื่น[10]

ในส่วนของการจำหน่ายผู้กระทำความผิดฯหรือผู้ป่วยออกจากโรงพยาบาลนั้นต้องกระทำโดยคำสั่งศาล โดยมาตรา 37 แห่งพระราชบัญญัติสุขภาพจิต พ.ศ. 2551 วางหลักทั่วไปในการจำหน่ายผู้ป่วยว่าโรงพยาบาลต้องรายงานความคืบหน้าในการรักษาต่อศาลเมื่อครบ 180 วัน และหากการรักษายังไม่เสร็จสิ้นต้องรายงานทุกๆ 180 วัน[11] หากผู้ป่วยสามารถออกจากโรงพยาบาลได้ แพทย์ต้องรายงานต่อศาล[12] เพื่อให้ศาลถอนคำสั่งให้คุมตัวไว้ในสถาพยาบาล ในทางปฏิบัติ กระบวนการจำหน่ายผู้ป่วยจากโรงพยาบาลนั้นอาจใช้เวลานาน เพราะต้องส่งรายงานไปที่ศาลก่อน และต้องรอศาลพิจารณาก่อนที่ศาลจะออกคำสั่งให้ออกจากโรงพยาบาลได้ ทั้งนี้ การสั่งจำหน่ายออกจากโรงพยาบาลนั้นสามารถกระทำโดยจิตแพทย์ผู้รักษาเพียงผู้เดียวโดยไม่ผ่านคณะกรรมการทบทวนผลการรักษาหรือจำหน่ายแต่อย่างใด[13] ซึ่งกระบวนการนี้อาจก่อให้เกิด

---

[8] เนื่องจากประมวลกฎหมายอาญาและประมวลฎหมายวิธีพิจารณาความอาญาไม่ได้กำหนดให้ศาลต้องรับฟังและผูกพันกับคำให้การของแพทย์

[9] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 246 “เมื่อจำเลย สามี ภริยา ญาติของจำเลย พนักงานอัยการ ผู้บัญชาการเรือนจำ หรือเจ้าพนักงานผู้มีหน้าที่จัดการตามหมายจำคุกร้องขอ หรือเมื่อศาลเห็นสมควร ศาลมีอำนาจสั่งให้ทุเลาการบังคับให้จำคุกไว้ก่อนจนกว่าเหตุอันควรทุเลาจะหมดไปในกรณีต่อไปนี้ (1) เมื่อจำเลยวิกลจริต...”.

[10] ดวงตา ไกรภัสสร์พงษ์, ‘การบังคับรักษาผู้กระทำผิดอาญาที่มีความผิดปกติทางจิต’ (2551) 16(2) วารสารสุขภาพจิตแห่งประเทศไทย, 108.

[11] พระราชบัญญัติสุขภาพจิต พ.ศ. 2551 มาตรา 37.

[12] พระราชบัญญัติสุขภาพจิต พ.ศ. 2551 มาตรา 38.

[13] ระเบียบคณะกรรมการสุขภาพจิตแห่งชาติ.ว่าด้วยหลักเกณฑ์และวิธีการในการรายงานผลการตรวจวินิจฉัย การประเมินความสามารถในการต่อสู้คดีและผลการบำบัดรักษาของผู้ป่วย พ.ศ. 2551.

ข้อกังขาได้ และนอกจากนี้ยังเป็นการไม่มีระบบในการทวนสอบดุลยพินิจเพื่อเป็นมาตรการรับรอง (safeguard) ว่าผู้กระทำความผิดพร้อมออกมาจริงหรือไม่

2.2 สหราชอาณาจักร (อังกฤษและเวลส์)

มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตของอังกฤษและเวลส์นั้นอยู่ภายใต้กฎหมายที่ชื่อ Mental Health Act 1983 (as amended by the Mental Health Act 2007) and the Criminal Procedure (Insanity) Act 1964 (as amended by the Criminal Procedure (Insanity and Unfitness to Plead) Act 1991) โดยศาลจะมีตัวเลือกสามทางในส่วนของมาตรการในการจัดการผู้กระทำความผิด คือ คำสั่งคุมตัวไว้ในสถานพยาบาล (แบบมีข้อกำหนดหรือไม่มีข้อกำหนด) (a hospital order with or without restriction) คำสั่งควบคุมดูแล (a supervision order) และคำสั่งปล่อยตัว (an absolute discharge)[14]

ในการออกคำสั่งให้คุมตัวไว้ในสถานพยาบาลนั้น ศาลต้องแน่ใจว่าผู้กระทำความผิดมีความผิดปกติทางจิตจริงจึงต้องมีรายงานหรือคำให้การจากจิตแพทย์[15] สองคน[16] และศาลต้องแน่ใจว่าอาการเหล่านั้นต้องได้รับการรักษาในโรงพยาบาลเท่านั้น และมาตรการรักษาอื่นๆ นั้นไม่เพียงพอ[17] อย่างไรก็ตาม การสั่งให้คุมตัวไว้ในสถานพยาบาลจะเป็นมาตรการบังคับกรณีผู้กระทำความผิดนั้นถูกกล่าวหาว่าก่อคดีฆาตกรรม[18] โดยการคุมตัวในแต่ละครั้งนั้นจะมีระยะเวลาหกเดือนโดยสามารถขยายได้อีกครั้งละหกเดือน และหากจำเป็นต้องขยายต่ออีกจะเป็นครั้งละหนึ่งปี[19] โดยการออกคำสั่งให้คุมตัวไว้ในสถานพยาบาลนั้นอาจใช้ร่วมกับข้อกำหนด (restriction order) ได้หากศาลเห็นว่าจำเป็นเพื่อป้องกันสาธารณะจากอันตรายร้ายแรง เพราะจะทำให้แน่ใจได้ว่าผู้กระทำความผิดนั้นถูกควบคุมไว้ในโรงพยาบาลในช่วงเวลาตามคำสั่งศาล[20] โดยทั่วไปแล้ว ผู้กระทำความผิดจะถูกคุมตัวไว้ในโรงพยาบาลที่มีการรักษาความปลอดภัยสูงแห่งใดแห่งใดต่อไปนี้ Broadmoor, Rampton หรือ Ashworth หรือในโรงพยาบาลที่มีการรักษาความปลอดภัยปานกลาง[21]

โดยทั่วไป ผู้ที่สามารถสั่งจำหน่ายผู้ป่วยจากสถานพยาบาลได้แก่ แพทย์เจ้าของไข้ (responsible clinician) กรณีที่เห็นว่าไม่จำเป็นต้องได้รับการรักษาอีกต่อไปหรือ หรือ ผู้ป่วยสามารถร้องขอให้ผู้อำนวยการ

---

[14] Section 5(2) Criminal Procedure (Insanity) Act 1964.

[15] Law Commission, *Criminal Liability: Insanity and Automatism Scoping Paper* (London 2012) para 2.105.

[16] Section 37(2)(a) Mental Health Act 1983.

[17] ibid and 37(2)(b).

[18] Section 5 Criminal Procedure (Insanity) Act 1964.

[19] Section 20 Mental Health Act 1983.

[20] Section 41 Mental Health Act 1983.

[21] Ministry of Justice, *Mentally disordered offenders – the restricted patient system* (London 2017) 8.

โรงพยาบาล (hospital managers) หรือญาติผู้ป่วยสามารถร้องขอให้จำหน่ายผู้ป่วยออกจากสถานพยาบาลได้[22] หรือผู้ป่วยสามารถอุทธรณ์ต่อ the Mental Health Tribunal โดยตรงให้จำหน่ายตนเองจากสถานพยาบาลได้[23]

ทั้งนี้ ผู้กระทำความผิดอาจถูกจำหน่ายออกจากโรงพยาบาลโดยมีเงื่อนไข หรือ ถูกจำหน่ายออกโดยมีข้อกำหนด (restriction order) จาก Secretary of State[24] the Tribunal[25] หรือแพทย์เจ้าของไข้อย่างใดอย่างหนึ่ง โดยความยินยอมจาก Secretary of State ก็ได้[26] โดยผู้กระทำความผิดที่ถูกจำหน่ายออกจากโรงพยาบาลโดยมีเงื่อนไขนั้นจะต้องได้รับการดูแลจากจิตแพทย์และนักสังคมสงเคราะห์ในชุมชนโดยหน่วยงาน Mental Health Casework Section ซึ่งขึ้นกับกระทรวงยุติธรรมจะเป็นผู้รับรายงานจากผู้ดูแลอย่างสม่ำเสมอ อย่างไรก็ดี หากจำเป็น ผู้ป่วยเหล่านี้อาจถูก Secretary of State เรียกกลับเข้ารับการรักษาในโรงพยาบาลได้[27]

หากศาลเห็นว่าผู้กระทำความผิดไม่จำเป็นต้องได้รับการคุมตัวไว้ในสถานพยาบาล ศาลอาจสั่งให้มีคำสั่งควบคุมดูแล (supervision order) แทนได้ โดยผู้กระทำความผิดจะถูกควบคุมดูแลโดยนักสังคมสงเคราะห์จากคณะกรรมการคุมประพฤติในระดับท้องถิ่นหรือเจ้าหน้าที่จากหน่วยคุมประพฤติตามเวลาที่กำหนดแต่ต้องไม่เกินสองปี[28] และอาจมีคำสั่งควบคุมดูแลควบคู่กับเงื่อนไขให้รับการรักษาทางยาได้[29] ในที่นี้ การออกคำสั่งควบคุมดูแลนั้นจะกระทำได้โดยอาศัยคำให้การที่เป็นถ้อยคำหรือหนังสือจากจิตแพทย์สองคน[30] โดยคำสั่งควบคุมดูแลร่วมกับคำสั่งให้รักษานี้ ทำให้ผู้กระทำความผิดได้รับการรักษาแบบผู้ป่วยนอกซึ่งต่างจากคำสั่งให้คุมตัวไว้ในสถานพยาบาลซึ่งผู้กระทำความผิดจะได้รับการรักษาโดยเป็นผู้ป่วยใน[31]

ทั้งนี้ ผู้กระทำความผิดมีสิทธิที่จะอุทธรณ์คำสั่งให้คุมตัวไว้ในสถานพยาบาลและคำสั่งควบคุมดูแลได้ที่ศาลอุทธรณ์[32] และหากศาลอุทธรณ์พิจารณาเห็นว่าคำสั่งเดิมนั้นไม่เหมาะสม ศาลอุทธรณ์อาจสั่งให้ยกเลิก

---

[22] Section 23 Mental Health Act 1983.

[23] Section 69 และ 72(1)(c) Mental Health Act 1983.

[24] Section 42 Mental Health Act 1983.

[25] ibid Section 73.

[26] ibid Section 23.

[27] Ministry of Justice (n 21) 14.

[28] Criminal Procedure (Insanity) Act 1964 Schedule 1A.

[29] ibid Part 2.

[30] ibid.

[31] ibid.

[32] Section 16A Criminal Appeal Act 1968 (as amended by Domestic Violence, Crime and Victims Act 2004). โปรดดู The Criminal Procedure Rules Part 39.

หรือกำหนดมาตรการอื่นแทน หรือเปลี่ยนแปลง หรือเพิ่มเติม เงื่อนไขคำสั่งเดิมได้[33]

ในกรณีที่ศาลเห็นว่าอาการของผู้กระทำความผิดไม่ควรได้รับคำสั่งให้คุมตัวไว้ในสถานพยาบาลหรือคำสั่งควบคุมดูแล ศาลอาจออกคำสั่งปล่อยตัว (absolute discharge) ซึ่งในการนี้ ผู้กระทำความผิดจะถูกปล่อยให้เป็นอิสระโดยไม่มีมาตรการบังคับใดๆ

ทั้งนี้ ในการตัดสินว่าจะใช้มาตรการใดกับผู้กระทำความผิด นอกจากหลักฐานจากจิตแพทย์เกี่ยวกับโรคและผลของความผิดปกติทางจิตนั้นๆ แล้ว ศาลยังต้องพิจารณาองค์ประกอบอื่นๆ เพิ่มเติมรวมทั้งพฤติการณ์ของคดีและประวัติอาชญากรรมของผู้นั้นอีกด้วย[34]

Criminal Procedure (Insanity) Act 1964 (as amended by the Criminal Procedure (Insanity and Unfitness to Plead) Act 1991) ได้ยกเลิกคำสั่งคุมตัวไว้ในสถานพยาบาลโดยไม่มีกำหนด ในกรณีที่ผู้กระทำความผิดได้ยกข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริต และยังทำให้ศาลมีทางเลือกอื่นๆ เพิ่มเติมอีก อย่างไรก็ดี สำหรับ ผู้ถูกกล่าวหาว่ากระทำความผิดในคดีฆาตกรรมที่ถึงแม้จะได้ยกข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริตสำเร็จต้องถูกคุมตัวไว้ในสถานพยาบาลเพียงอย่างเดียวเท่านั้น ดังนั้น การยกข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริตอาจไม่เป็นที่ดึงดูดสำหรับผู้ถูกกล่าวหาว่ากระทำความผิดในคดีฆาตกรรมนัก ทั้งนี้ ผู้ถูกกล่าวหาในคดีดังกล่าวอาจยกข้อต่อสู้เรื่อง diminished responsibility[35] แทนได้ แต่เป็นการสุ่มเสี่ยงเพราะข้อต่อสู้เรื่อง diminished responsibility มีผลเป็นการลดโทษ จึงทำให้ผู้กระทำผิดยังต้องถูกลงโทษและยังต้องมีความรับผิด ซึ่งในทางกลับกัน ตามหลักการแล้ว ผู้กระทำความผิดไม่ควรต้องมีความรับผิดเนื่องจากความเจ็บป่วยทางจิตจึงไม่ควรถูกลงโทษ

นอกจากนี้ การออกคำสั่งควบคุมดูแลก็อาจจะยังไม่เหมาะสมในบางกรณี เพราะผู้กระทำความผิดต้องถูกควบคุมนานที่สุดถึงสองปี ดังนั้น ผู้กระทำความผิดบางคนอาจหลีกเลี่ยงโดยการยอมรับผิดและรับโทษดีกว่าจะยกข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริต เพราะยอมรับผิดและรับสารภาพในบางคดีอาจมีโทษจำคุกเล็กน้อยเท่านั้น[36]

---

[33] ibid Section 16B.

[34] Ministry of Justice (n 21) 4.

[35] เป็นข้อต่อสู้เรื่องความสามารถที่ลดลงในขณะที่กระทำความผิดของอังกฤษและเวลส์ใช้เฉพาะคดีฆ่าคนตายโดยเจตนาเท่านั้น โปรดดู Crown Prosecution Service, 'Diminished responsibility' (CPS, September 2022). <https://www.cps.gov.uk/legal-guidance/homicide-murder-and-manslaughter> สืบค้นวันที่ 2 เมษายน 2566.

[36] Law Commission (n 15) para 2.111.

2.3 สหราชอาณาจักร (สกอตแลนด์)

มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตของสกอตแลนด์ อยู่ภายใต้กฎหมาย The Criminal Procedure (Scotland) Act 1995 (as amended by the Mental Health (Care and Treatment) (Scotland) Act 2003) ซึ่งมาตรการฯ นั้นประกอบไปด้วยคำสั่งคุมตัวไว้ในสถานพยาบาลแบบมีข้อกำหนดหรือไม่มีข้อกำหนด (a compulsion order with restriction or no restriction) คำสั่งคุมตัวไว้ในสถานพยาบาลชั่วคราว (an interim compulsion order) คำสั่งผู้พิทักษ์ (a guardian order) คำสั่งควบคุมดูแลและบำบัดรักษา (a supervision and treatment order) หรือการไม่ออกคำสั่งใด (no order)[37]

ศาลอาจออกคำสั่งคุมตัวไว้ในสถานพยาบาลหากพิจารณาแล้วว่าผู้กระทำความผิดมีความผิดปกติทางจิตจากหลักฐานคำให้การหรือเอกสารจากจิตแพทย์สองคนและความผิดปกตินั้นต้องได้รับการรักษาเพราะหากไม่ให้มีการรักษาจะทำให้มีความเสี่ยงต่อสุขภาพ ความปลอดภัยและสวัสดิภาพของผู้กระทำความผิดและสาธารณะได้[38] โดยปกติแล้ว คำสั่งคุมตัวไว้ในสถานพยาบาลจะมีระยะเวลาหกเดือนและสามารถขอขยายได้อีกหกเดือน และหากจำเป็นต้องขยายต่อจะสามารถขยายต่อได้เป็นครั้งละ 12 เดือน[39]

ทั้งนี้ ศาลอาจสั่งให้มีคำสั่งคุมตัวไว้ในสถานพยาบาลโดยมีข้อกำหนดได้ หากเห็นว่าความผิดปกติทางจิตของผู้กระทำความผิดจะก่อให้เกิดความเสี่ยงต่อสาธารณะ[40] ซึ่งคำสั่งนี้จะให้ผู้กระทำความผิดถูกควบคุมตัวในสถานพยาบาลโดยไม่มีกำหนดเวลาขั้นต่ำ[41] และผู้กระทำความผิดจะถูกควบคุมตัวในโรงพยาบาลของรัฐที่มีการรักษาความปลอดภัยสูงที่มีชื่อว่า Carstairs State Hospital[42]

ในการจำหน่ายออกจากสถานพยาบาลนั้นจะกระทำโดย the Mental Health Tribunal ที่ถูกตั้งขึ้นตามอำนาจในมาตรา 21 แห่ง the Mental Health (Care and Treatment) (Scotland) Act 2003

---

[37] Section 57 Criminal Procedure (Scotland) Act 1995.

[38] Ibid.

[39] Scottish Government, 'Mental Health Act – compulsory treatment orders: guide' <https://www.gov.scot/publications/new-mental-health-act-guide-compulsory-treatment-orders/pages/10/> สืบค้นวันที่ 9 มิถุนายน 2566.

[40] Section 59 Criminal Procedure (Scotland) Act 1995.

[41] Ibid Section 57(a)(7).

[42] NHS Scotland, 'The State Hospital' (NHS Scotland, 2016). <https://www.tsh.scot.nhs.uk/Fact%20Sheets/About%20Us%20-%206%20Sep%2016.pdf> สืบค้นวันที่ 2 เมษายน 2566.

โดยแต่ละองค์คณะจะประกอบไปด้วยผู้ทรงคุณวุฒิทางด้านกฎหมาย (ซึ่งทำหน้าที่เป็นประธาน) ผู้ทรงคุณวุฒิทางการแพทย์และผู้ทรงคุณวุฒิทั่วไปจำนวนสามคน[43]

คำสั่งคุมตัวไว้ในสถานพยาบาลชั่วคราว หมายถึง การที่ผู้กระทำความผิดจะถูกควบคุมตัวในโรงพยาบาลเพื่อประเมินอาการและรักษาได้นานถึงสิบสองสัปดาห์ และต่อให้ได้นานที่สุดสิบสองเดือน[44] โดยการออกคำสั่งนี้ใช้เกณฑ์เดียวกับการออกคำสั่งคุมตัวไว้ในสถานพยาบาล

คำสั่งผู้พิทักษ์ คือคำสั่งให้อยู่ในชุมชนโดยมีผู้ดูแลสวัสดิภาพซึ่งจะถูกบังคับในกรณีที่ศาลเห็นว่าเป็นผลดีต่อสวัสดิภาพของผู้กระทำความผิด[45]

คำสั่งควบคุมดูแลและบำบัดรักษาเป็นคำสั่งให้อยู่ในชุมชนภายใต้การดูแลของนักสังคมสงเคราะห์ (ที่เรียกว่าเจ้าหน้าที่ควบคุมดูแล) โดยมีระยะเวลาไม่นานเกินกว่าสามปี ภายใต้ระยะเวลาดังกล่าว ผู้กระทำความผิดต้องปฏิบัติตามคำแนะนำของเจ้าหน้าที่และอาจต้องได้รับการรักษา[46] โดยการที่ศาลจะสั่งคำสั่งนี้ได้นั้น ศาลต้องได้รับหลักฐานคำให้การหรือเอกสารจากจิตแพทย์อย่างน้อยสองคน[47]

หากศาลไม่เห็นว่าผู้กระทำความผิดต้องได้รับการรักษาหรือการควบคุมดูแลใดๆ ศาลอาจไม่ออกคำสั่งใดเลยก็ได้ เช่นนี้ ผู้กระทำความผิดก็จะพ้นผิดทันที

ทั้งนี้ ผู้กระทำความผิดสามารถอุทธรณ์คำสั่งคุมตัวไว้สถานพยาบาลทั้งสองแบบได้ แต่ไม่อาจอุทธรณ์คำสั่งชนิดอื่นๆ ได้[48]

เพื่อให้สอดคล้องกับกฎหมายอังกฤษ The Criminal Procedure (Scotland) Act 1995 (as amended by the Mental Health (Care and Treatment) (Scotland) Act 2003) ได้ยกเลิกการคุมตัวไว้ในสถานพยาบาลอย่างไม่มีกำหนดเช่นกัน อย่างไรก็ดี กฎหมายของสกอตแลนด์มีความแตกต่างจากอังกฤษและเวลส์ เนื่องจากสกอตแลนด์ไม่ได้บังคับว่าจะต้องใช้คำสั่งคุมตัวไว้ในสถานพยาบาลกับผู้กระทำความผิดที่มีความผิดปกติทางจิตซึ่งถูกกล่าวหาว่าก่อคดีฆาตกรรม

---

[43] Mental Health Tribunal for Scotland, 'About the Tribunal' (Mental Health Tribunal for Scotland, 2023) <https://www.mhtscotland.gov.uk/mhts/About_Tribunal/About_Tribunal> accessed 9 June 2023.

[44] Section 53 Criminal Procedure (Scotland) Act 1995.

[45] ibid Section 57(2)(c).

[46] ibid Schedule 4.

[47] ibid Schedule 4 and Section 58 1(A).

[48] ibid Section 60. See also Criminal Appeal (Scotland) Act 1926.

ดังนั้น จะเห็นได้ว่ากฎหมายสกอตแลนด์กำหนดมาตรการจัดการผู้กระทำความผิดที่เป็นผู้มีความผิดปกติทางจิตไว้หลากหลายกว่ากฎหมายอังกฤษ เช่น การมีคำสั่งคุมตัวไว้ในสถานพยาบาลชั่วคราวเพื่อให้ศาลมีเวลาในการพิจารณาใช้มาตรการที่เหมาะสมที่สุดได้[49] ซึ่งแนวคิดนี้เป็นแนวคิดที่ดีที่ทำให้มั่นใจได้ว่าผู้กระทำผิดที่มีความผิดปกติทางจิตได้รับมาตรการที่เหมาะสมที่สุด นอกจากนี้ คำสั่งผู้พิทักษ์ก็มีผลดีต่อผู้กระทำความผิดที่ต้องการผู้ดูแลสวัสดิภาพในทันทีได้เช่นกัน เพราะสามารถออกคำสั่งได้หลังจากเสร็จสิ้นการดำเนินคดีทางอาญาโดยที่ไม่ต้องแยกไปฟ้องการบังคับทางแพ่งต่อไป

อย่างไรก็ตาม มาตรการจัดการผู้กระทำความผิดที่มีความผิดปกติทางจิตในสกอตแลนด์นั้นยังมีข้อด้อยกว่าในอังกฤษ กล่าวคือผู้กระทำความผิดยังจะอาจถูกคุมตัวในโรงพยาบาลและคำสั่งควบคุมดูแลทำให้ผู้กระทำความผิดอยู่ภายใต้การดูแลของเจ้าหน้าที่ได้นานถึงสามปี ซึ่งอาจจะส่งผลให้ผู้ถูกกล่าวหาไม่อยากยกข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริต และเลือกจะรับสารภาพเพื่อจะรับการลงโทษที่อาจเบากว่าแทนการถูกบังคับตามมาตรการจัดการผู้กระทำความผิดที่มีความผิดปกติทางจิต

3. วิเคราะห์เปรียบเทียบบทบัญญัติเรื่องมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตของไทยและสหราชอาณาจักร (อังกฤษและเวลส์และสกอตแลนด์)

จากการศึกษาพบว่า มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ป่วยจิตเวชภายใต้กฎหมายของอังกฤษและเวลส์ และสกอตแลนด์มีความคล้ายคลึงกัน โดยมีตั้งแต่คำสั่งให้คุมตัวไว้ในสถานพยาบาล หรือคำสั่งควบคุมดูแลไปจนถึงการปล่อยตัว โดยกฎหมายของสกอตแลนด์นั้นจะมีมาตรการที่ละเอียดกว่า เช่น การคุมตัวไว้ในสถานพยาบาลชั่วคราวเพื่อดูอาการหรือคำสั่งผู้พิทักษ์ โดยในเบื้องต้นคำสั่งคุมตัวไว้ในสถานพยาบาลของทั้งสองประเทศจะมีระยะเวลาหกเดือน โดยสามารถขยายได้ครั้งละหกเดือน และหากจำเป็นจะสามารถขยายต่อได้อีกครั้งละหนึ่งปี (อังกฤษและเวลส์) หรือสิบสองเดือน (สกอตแลนด์)

ในส่วนมาตรการของประเทศไทยมีเพียงคำสั่งให้คุมตัวไว้ในสถานพยาบาล หรือการปล่อยตัวเท่านั้น โดยคำสั่งให้คุมตัวไว้ในสถานพยาบาลจะถูกบังคับใช้ก็ต่อเมื่อศาลเห็นว่าหากการปล่อยตัวจำเลยไปนั้นจะเป็นอันตรายและสามารถคุมตัวไว้ได้ครั้งละ 180 วัน

ในส่วนของเงื่อนไขการบังคับใช้มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ป่วยจิตเวชในอังกฤษและเวลส์ และสกอตแลนด์ ก่อนที่ศาลจะบังคับใช้มาตรการใดมาตรการหนึ่งได้นั้นจำเป็นต้องมีความเห็น

---

[49] Scottish Executive, *Mental Health (Care and Treatment) (Scotland) 2003 Volume 3 compulsory power in relation to mentally disordered offenders* (Edinburgh 2005) 105.

ทางการแพทย์จากจิตแพทย์อย่างน้อย 2 คนเสียก่อนและมาตรการที่ศาลจะบังคับใช้นั้นจะเลือกใช้มาตรการที่จำเป็นและเหมาะสมกับผู้กระทำความผิดที่สุด ในขณะที่ในประเทศไทยไม่ได้มีข้อกำหนดใด

	อังกฤษและเวลส์	**สกอตแลนด์**	**ไทย**
มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ป่วยจิตเวช	- คำสั่งคุมตัวไว้ในสถานพยาบาล (มีข้อกำหนดหรือไม่มีข้อกำหนด) - คำสั่งควบคุมดูแล - คำสั่งปล่อยตัว	- คำสั่งคุมตัวไว้ในสถานพยาบาล (มีข้อกำหนดหรือไม่มีข้อกำหนด) - คำสั่งคุมตัวไว้ในสถานพยาบาลชั่วคราว - คำสั่งผู้พิทักษ์ - คำสั่งควบคุมดูแลและบำบัดรักษา - ไม่ออกคำสั่งใด	กรณีมาตรา 65 วรรคแรก: - คำสั่งคุมตัวไว้ในสถานพยาบาล (กรณีเป็นอันตราย) - คำสั่งปล่อยตัว กรณีมาตรา 65 วรรคสอง: - พิพากษาลดโทษ - คำสั่งคุมตัวไว้ในสถานพยาบาล (กรณีเป็นอันตราย)
พยานหลักฐานประกอบการกำหนดมาตรการ	จำเป็น สองชิ้นจากจิตแพทย์สองคน	จำเป็น สองชิ้นจากจิตแพทย์สองคน	ไม่จำเป็น

4. ปัญหาของมาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติของไทย

ในทางปฏิบัติ มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้ที่มีความผิดปกติทางจิตของประเทศไทยมีปัญหาต่างๆ ดังนี้

ประการแรก ในหลายคดีปรากฏว่าศาลเลือกจะไม่สั่งคุมตัวไว้ในสถานพยาบาลซึ่งแย้งกับความเห็นของจิตแพทย์ จากการศึกษาพบว่าจากจำนวน 274 คดี มีอัตราถึง 64.1% ของจำนวนคดีทั้งหมดที่ศาลไม่สั่งให้มีการรักษาในโรงพยาบาลหรือการรักษาตามคำแนะนำของจิตแพทย์[50] เพราะตามกฎหมายไทยแล้วศาลไม่จำเป็นต้องเห็นด้วยและผูกพันกับความเห็นของจิตแพทย์ ซึ่งก็เป็นประเด็นปัญหาเรื่องการใช้ดุลยพินิจของศาล แต่ข้อกระทบที่สำคัญที่สุดในที่นี้คือ กฎหมายไทยห้ามมิให้มีการอุทธรณ์คำสั่งคุมตัวไว้ใน

[50] วนัทดา ถมค้าพาณิชย์ และดวงตา ไกรภัสสร์พงษ์ (n 7) 125.

สถานพยาบาล[51] ดังนั้น หากศาลไม่สั่งให้มีการคุมตัวไว้ในสถานพยาบาลตามประมวลกฎหมายอาญา มาตรา 48 และศาลปล่อยตัวผู้กระทำผิดนั้น หากประสงค์จะให้ผู้กระทำความผิดที่มีความผิดปกติทางจิตได้รับการรักษาก็ต้องกระทำโดยวิธีการคุมตัวทางแพ่งผ่านทางพระราชบัญญัติสุขภาพจิต พ.ศ. 2551 ตามความในมาตรา 22 และมาตรา 29[52] ซึ่งระยะเวลาในการดำเนินการเพื่อขอคุมตัวทางแพ่งนั้นอาจกินระยะเวลานานและเป็นการปล่อยตัวผู้กระทำความผิดไปโดยไม่ได้รับการรักษาอย่างท่วงที นอกเหนือจากนี้ ไม่ใช่ทุกโรงพยาบาลจิตเวชที่มีสภาพพร้อมที่จะรับผู้กระทำความผิดที่มีความผิดปกติทางจิตไว้รักษาพยาบาล[53] ดังนั้นโรงพยาบาลจิตเวชอาจลังเลที่จะรับผู้ป่วยกลุ่มนี้ไว้[54] นั่นหมายความว่า หากศาลตัดสินใจไม่ใช้คำสั่งคุมตัวไว้ในสถานพยาบาล ผู้กระทำความผิดจะถูกปล่อยตัว (หากยกข้อต่อสู้ตามมาตรา 65 วรรค 1 สำเร็จ) หรือถูกจำคุก (หากยกข้อต่อสู้ตามมาตรา 65 วรรค 2 สำเร็จ) ในกรณีแรก (หากยกข้อต่อสู้ตามมาตรา 65 วรรค 1 สำเร็จ) กระบวนการยุติธรรมทางอาญาจะไม่มีอำนาจใดๆในการจัดการผู้กระทำความผิดนั้น ถึงแม้จะยังมีความเป็นไปได้ที่จะสามารถบังคับให้มีการรักษาโรคจิตเวชโดยการสั่งให้รับการรักษาในโรงพยาบาลภายใต้พระราชบัญญัติสุขภาพจิต พ.ศ. 2551 ตามที่ได้กล่าวไว้ข้างต้น แต่ก็มีความชักช้าและอาจไม่ทันการ เนื่องจาก

---

[51] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 219 ทวิ “ห้ามมิให้คู่ความฎีกาคัดค้านคำพิพากษาหรือคำสั่งในข้อ เท็จจริงในปัญหาเรื่องวิธีการเพื่อความปลอดภัยแต่อย่างเดียว แม้คดีนั้นจะไม่ต้องห้ามฎีกาก็ตาม...” เนื่องจากการคุมตัวไว้ในสถานพยาบาลเป็นวิธีการเพื่อความปลอดภัย ดังนั้นจึงต้องห้ามอุทธรณ์

[52] พระราชบัญญัติสุขภาพจิต พ.ศ. 2552 มาตรา 22 “บุคคลที่มีความผิดปกติทางจิตในกรณีใดกรณีหนึ่งดังต่อไปนี้เป็นบุคคลที่ต้องได้รับการบำบัดรักษา

(1) มีภาวะอันตราย

(2) มีความจำเป็นต้องได้รับการบำบัดรักษา

พระราชบัญญัติสุขภาพจิต พ.ศ. 2552 มาตรา 29 “เมื่อสถานบำบัดรักษารับบุคคลที่พนักงานเจ้าหน้าที่นำส่งตามมาตรา 27 วรรคสาม หรือแพทย์นำส่งตามมาตรา 28 แล้วแต่กรณี ให้คณะกรรมการสถานบำบัดรักษาตรวจวินิจฉัยและประเมินอาการบุคคลนั้นโดยละเอียดภายในสามสิบวันนับแต่วันที่รับตัวบุคคลนั้นไว้ในกรณีที่คณะกรรมการสถานบำบัดรักษาเห็นว่าบุคคลนั้นมีลักษณะตามมาตรา 22 ให้มีคำสั่งอย่างใดอย่างหนึ่ง ดังต่อไปนี้

(1) ให้บุคคลนั้นต้องเข้ารับการบำบัดรักษาในสถานบำบัดรักษา

(2) ให้บุคคลนั้นต้องรับการบำบัดรักษา ณ สถานที่อื่นนอกจากสถานบำบัดรักษาเมื่อบุคคลนั้นไม่มีภาวะอันตราย ทั้งนี้ จะกำหนดเงื่อนไขใดๆ ที่จำเป็นเกี่ยวกับการบำบัดรักษาให้บุคคลนั้นหรือผู้รับดูแลบุคคลนั้นต้องปฏิบัติด้วยก็ได้...”

[53] ปัจจุบันประเทศไทยมีโรงพยาบาลจิตเวชสังกัดกรมสุขภาพจิตทั้งหมด 20 แห่ง โปรดดู กรมสุขภาพจิต, ‘โรงพยาบาลจิตเวชสังกัดกรมสุขภาพจิต’ (กรมสุขภาพจิต, ตุลาคม 2019) < https://dmh.go.th/links/links-n.asp?catid=18> สืบค้นวันที่ 2 เมษายน 2566.

[54] วิสูตร ฟองศิริไพบูลย์ และสมบูรณ์ ธรรมเถกิงกิจ, ‘ความเสี่ยงในการจำหน่ายผู้ป่วยทางจิตเวช: หนึ่งอุทาหรณ์และมุมมองทางด้านนิติเวชศาสตร์’ (2552) ปีที่ 2 ฉบับที่ 2, เวชบันทึกศิริราช, 5.

พนักงานเจ้าหน้าที่ตามพระราชบัญญัติสุขภาพจิต พ.ศ. 2551 จะต้องนำตัวผู้ป่วยไปยังโรงพยาบาลเสียก่อน[55] และต้องมีการตั้งคณะกรรมการบำบัดรักษาขึ้นเสียก่อนเพื่อพิจารณาว่าจะรับตัวไว้รักษาหรือไม่[56] ในกรณีที่สอง (หากยกข้อต่อสู้ตามมาตรา 65 วรรค 2 สำเร็จ) เมื่อผู้กระทำความผิดถูกจำคุก ในกรณีนี้กรมราชทัณฑ์จะเป็นผู้รับผิดชอบในการบำบัดรักษาผู้ต้องขัง อย่างไรก็ดี เมื่อผู้ต้องขังเข้ามาอยู่ในระบบของราชทัณฑ์แล้ว กว่าที่ผู้ต้องขังจะได้รับการรักษาทางจิตเวชนั้นอาจผ่านกระบวนการที่ซับซ้อนและยืดเยื้อยาวนานเช่นกันโดยเฉพาะกรณีต้องนำตัวออกมาจากเรือนจำเพื่อรักษา[57] ดังนั้น เพื่อเป็นการป้องกันไม่ให้เกิดปัญหาดังกล่าวจึงอาจจำต้องมีการอนุญาตให้อุทธรณ์คำสั่งให้คุมตัวหรือไม่คุมตัวไว้ในสถานพยาบาลได้

ประการที่สอง คือการที่ประเทศไทยยังขาดแคลนหน่วยงานและสถานสำหรับการดูแลผู้ต้องขังหรือผู้กระทำความผิดที่มีความผิดปกติทางจิตโดยเฉพาะ ในปัจจุบัน สถาบันกัลป์ยาณ์ราชนครินทร์เป็นเพียงโรงพยาบาลจิตเวชเพียงแห่งเดียวที่มีความชำนาญในการดูแลผู้ต้องขังหรือผู้กระทำความผิดที่มีความผิดปกติทางจิต และสถาบันฯ ยังต้องรับหน้าที่ในการประเมินผู้กระทำความผิดที่มีความผิดปกติทางจิตอื่นๆ อีกด้วย เช่น การประเมินความสามารถในการสอบสวนหรือสู้คดี ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 14 และบำบัดรักษาผู้ที่ไม่สามารถสอบสวนหรือสู้คดีได้ เพื่อให้กลับมามีความสามารถเพียงพอและกลับเข้าสู่กระบวนการสอบสวนและพิจารณาคดีได้ ทั้งนี้ สถาบันฯเองก็รับผู้ป่วยจิตเวชทั่วไปเช่นเดียวกัน นอกจากภาระเหล่านี้แล้ว ข้อสังเกตอีกประการหนึ่งคือตัวสถาบันฯ เองก็ไม่ได้เป็นโรงพยาบาลที่มีการรักษาความปลอดภัยดีพอที่จะคุมตัวผู้กระทำความผิดที่มีความผิดปกติได้อย่างเพียงพอเพราะปัญหาการขาดแคลนเจ้าหน้าที่และตัวลักษณะของโรงพยาบาลเองก็ไม่ได้ถูกสร้างมาเพื่อวัตถุประสงค์ในการคุมตัวผู้กระทำความผิดที่มีความเสี่ยงสูง แต่สามารถรับผู้กระทำความผิดที่ถูกจัดไว้ในประเภท ‘ความเสี่ยงต่ำ’ ที่ไม่ใช่ผู้ที่กระทำความผิดในคดีอุฉกรรจ์หรือกระทำความผิดซ้ำ[58] ในทางปฏิบัติ ผู้กระทำความผิดที่มีความผิดปกติทางจิตที่ถูกส่งไปที่สถาบันฯ มักจะถูกรับตัวไว้ในสถาบันฯ เพื่อการรับการรักษาระยะสั้น ดังนั้น เมื่อเห็นว่ามีอาการคงที่แล้ว สถาบันฯ จะจำหน่ายตัวออกมาให้ครอบครัวดูแลหรือกลับเข้าเรือนจำเพื่อรับโทษต่อไป[59]

ประการที่สาม ประเทศไทยไม่มีมาตรการเฝ้าระวังหลังการจำหน่ายผู้ป่วยออกจากโรงพยาบาลเพราะจิตแพทย์สามารถจำหน่ายผู้กระทำความผิดออกจากโรงพยาบาลได้โดยไม่ต้องมีผู้ควบคุมดูแล จึงทำให้ผู้ป่วย

---

[55] พระราชบัญญัติสุขภาพจิต พ.ศ.2552 มาตรา 24.

[56] พระราชบัญญัติสุขภาพจิต พ.ศ.2552 มาตรา 27.

[57] โปรดดู พระราชบัญญัติราชทัณฑ์ พ.ศ. 2560.

[58] แสวง บุญเฉลิมวิภาส, ‘ผู้ป่วยจิตเวชกับปัญหา ในกระบวนการยุติธรรมทางอาญา’ (2550) ปีที่ 15 ฉบับที่ 2 วารสารสุขภาพจิตแห่งประเทศไทย, 75.

[59] Ibid.

บางคนที่ออกจากโรงพยาบาลแล้วสามารถกลับมาทำความผิดซ้ำได้ ตัวอย่างเช่นในกรณีของนางสาวจิตรลดา ซึ่งจะได้กล่าวต่อไป

ประการที่สี่ ในทางปฏิบัติ ระบบการจำหน่ายออกจากโรงพยาบาลใช้เวลานานเพราะต้องรายงานการจำหน่ายกลับไปที่ศาลและต้องรอให้ศาลออกคำสั่งถอนการคุมตัวซึ่งทำให้ผู้กระทำความผิดถูกจำกัดอิสรภาพโดยไม่จำเป็นเพราะต้องรอคำสั่งปล่อยที่นาน

ประการสุดท้าย ในทางปฏิบัติ ผู้ป่วยจะถูกจำหน่ายออกจากโรงพยาบาลกลับสู่การดูแลของครอบครัวโดยไม่มีผู้ควบคุม[60] จึงเป็นที่น่าสงสัยว่า ครอบครัวจะมีความตระหนักและความรู้เกี่ยวกับการเจ็บป่วยทางจิตและการดูแลผู้ป่วยมากน้อยเพียงใด (ซึ่งโดยปกติ การตระหนักรู้เรื่องโรคทางจิตเวชนั้นก็มีน้อยอยู่แล้วในสังคมไทย) นอกจากนี้ ผู้ป่วยบางคนก็ถูกจำหน่ายจากโรงพยาบาลทั้งที่ยังไม่ได้รับการรักษาจนหายดีอีกด้วย[61] จึงพบว่าหลังจากออกจากโรงพยาบาล ผู้ป่วยมักหยุดยาหรือครอบครัวเห็นว่าไม่ต้องรับยาต่อเพราะผู้ป่วยดู “ปกติดี” หรือเพียงเพราะไม่สะดวกในการไปโรงพยาบาลหรือมีความไม่สะดวกอื่นๆ [62] นอกจากนี้หลายครอบครัวไม่ยอมรับญาติพี่น้องที่มีความผิดปกติทางจิตกลับคืน[63] ในกรณีเช่นนี้แม้จะมีที่พักของรัฐที่สามารถรับผู้ป่วยไปดูแลได้[64] แต่ที่พักเหล่านี้ก็ไม่มีอุปกรณ์ที่เหมาะสมและไม่มีเจ้าหน้าที่ที่ได้รับการฝึกฝนมาในการดูแลผู้ป่วยที่อาจมีความรุนแรงซึ่งหากผู้ป่วยจิตเวชที่ถูกจำหน่ายออกจากโรงพยาบาลมีอาการสับสนหรือมีอาการทางจิตกลับมาอีกก็อาจจะต้องออกจากที่พักดังกล่าว

จากเหตุผลเหล่านี้ ในทางปฏิบัติจึงพบว่าผู้กระทำความผิดมักมีความผิดปกติทางจิตกลับมาอีกทำให้บางคนกระทำความผิดซ้ำและกลับเข้าสู่กระบวนการยุติธรรมอีกและปัญหาคงจะดำเนินต่อไปเช่นนี้จนกว่าประเทศไทยจะมีหน่วยงานที่สามารถคุมตัวและรักษาผู้ป่วยได้และปล่อยผู้ป่วยออกมาเมื่อรักษาหายดี

---

[60] ปัจจุบันไม่ได้มีการบังคับให้ต้องติดตามดูแลหลังปล่อยตัว แต่ในทางปฏิบัติ เจ้าหน้าที่จะตามเช็คผู้ป่วยหลังถูกปล่อยไป 2-3 เดือนแรก โปรดดู กรมสุขภาพจิต, ‘คู่มือระบบการดูแลผู้ป่วยจิตเวชที่มีความเสี่ยงสูงต่อความรุนแรง’ <https://mhso.dmh.go.th/fileupload/20201006161216739O.pdf> สืบค้นวันที่ 2 เมษายน 2566.

[61] ดังที่ได้กล่าวไว้ข้างต้นว่าเนื่องจากนโยบายโรงพยาบาลที่จำหน่ายผู้ป่วยออกเมื่ออาการคงที่

[62] ผลวิจัยชี้ว่า มีแค่ผู้กระทำความผิดจำนวนหนึ่งในสามสิบห้าคนเท่านั้น ที่กระทำผิดซ้ำ แต่เกินกว่าครึ่งของจำนวนดังกล่าวถูกส่งตัวกลับไปรักษาพยาบาล โปรดดู ไกรภัสสร์พงษ์ (n 10) 114.

[63] Prachathai, ‘คนบ้าหลังกำแพงคุก: การเดินทางกลับบ้านของชิต’ (Prachathai, กรกฎาคม 2561). <https://prachatai.com/journal/2018/07/77683> สืบค้นวันที่ 2 เมษายน 2566.

[64] ประกาศคณะกรรมการสุขภาพจิตแห่งชาติ เรื่อง กำหนดหน่วยงานด้านสงเคราะห์และสวัสดิการ พ.ศ. 2564.

และมีความปลอดภัยแทนที่จะปล่อยตัวเมื่อ ‘อาการคงที่เพียงชั่วคราว’ ดังที่ปฏิบัติกันในปัจจุบันซึ่งก็เป็นปัญหาที่สืบเนื่องมาจากภาวะมีคนไข้ล้นโรงพยาบาลด้วยเช่นกัน[65]

กรณีที่แสดงให้เห็นถึงความล้มเหลวของการจัดการผู้กระทำความผิดที่ความผิดปกติทางจิตในไทย คือ กรณีของนางสาวจิตรลดา ผู้กระทำความผิดที่เคยถูกตัดสินว่ามีความผิดฐานพยายามฆ่านักเรียนในปี พ.ศ. 2547[66] และถูกกล่าวหาว่ากระทำความผิดฐานฆ่าคนตายในเดือนมีนาคมปี พ.ศ. 2563[67]

ข่าวได้รายงานว่าเธอถูกจำหน่ายออกจากโรงพยาบาลเมื่อปี พ.ศ. 2555 และมีอาการดีมาตลอด[68] ประการที่น่าสนใจคือ ในการดำเนินคดีข้อหาพยายามฆ่าในปี พ.ศ. 2547 นั้น จิตรลดาไม่ประสบความสำเร็จในการยกข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริต แม้ว่าจะมีหลักฐานทางการแพทย์ว่าเธอเจ็บป่วยด้วยโรคจิตเภทตั้งแต่อายุ 20 ปี (ในขณะที่ก่อคดีแรกเธอมีอายุ 26 ปี) คำพิพากษาให้เหตุผลว่าผู้กระทำความผิดสามารถซื้อมีดเพื่อเตรียมการก่อนการกระทำผิด และภายหลังจากกระทำผิดเธอหลบหนีจากบริเวณที่ก่อเหตุ เปลี่ยนเสื้อผ้าและทรงผม และสามารถสื่อสารกับเจ้าหน้าที่ตำรวจและแพทย์ได้รู้เรื่องดี ดังนั้น เธอสามารถคุมตนเองได้[69] เธอถูกจำคุกสี่ปีและมีคำสั่งให้คุมตัวในสถานพยาบาลหลังพ้นโทษ[70] จากคำพิพากษาจะเห็นได้ว่าศาลเชื่อในจิตวิทยาแบบชาวบ้าน (folk psychology) และหลักฐานแวดล้อมในการที่จะตัดสินว่าจำเลยวิกลจริตหรือไม่ มากกว่าการให้น้ำหนักแก่หลักฐานทางการแพทย์และแรงกระตุ้นให้กระทำความผิด (จิตรลดาให้การว่าได้ยินเสียงจากสวรรค์สั่งให้จัดการกับคนรวย อย่างไรก็ดี อาจเป็นเพราะในคดีดังกล่าวเนื่องจากเป็นคดีร้ายแรงที่กระทำต่อเด็ก ศาลจึงเน้นการลงโทษมากกว่าเพื่อสนองความต้องการของสังคมในการแก้แค้นทดแทน เพราะในเวลานั้นสาธารณชนประณามผู้กระทำผิดโดยไม่สนใจว่าจะป่วยจิตหรือไม่ และสังคมต้องการเห็นว่ามีการลงโทษ อย่างไรก็ตาม ท้ายที่สุดแล้วจะเห็นได้ชัดว่าการลงโทษและการรักษาไม่เพียงพอที่จะช่วยฟื้นฟูผู้กระทำความผิดได้เพราะมีการกระทำผิดซ้ำ กรณีนี้ยังแสดงให้เห็นปัญหาของระบบการติดตามและ

---

[65] HFocus, ‘พ้อ สธ.ไม่สนใจงานจิตเวช สั่งลดบุคลากรใน รพ. ทั้งที่งานล้นมือ โอดถอดใจ-ไม่ไหวอีกต่อไปแล้ว’ (HFocus, 13 มกราคม 2561) <https://www.hfocus.org/content/2018/01/15223> สืบค้นวันที่ 4 เมษายน 2566.

[66] MGR Online, ‘คุก 4 ปี “จิตรลดา” มือแทงเด็กคอนแวนต์-พ้นโทษส่งบำบัดต่อ’ (MGR Online, 20 พฤศจิกายน 2551) <https://mgronline.com/crime/detail/9510000137416> สืบค้นวันที่ 23 สิงหาคม 2563.

[67] ไทยรัฐออนไลน์, ‘สลด "จิตรลดา" ก่อเหตุอีก แทงด.ญ.4 ขวบ ลูกแม่ค้าข้างบ้านเสียชีวิต’ (ไทยรัฐออนไลน์, 29 มีนาคม 2563)<https://www.thairath.co.th/news/local/central/1807424?fbclid=IwAR2djmwJp9811VnkhpBEn0csVaA2bPv85UCUr9yuJBxD-VGJ-1kYwIDnQRw> สืบค้นวันที่ 4 เมษายน 2566.

[68] Sanook, ‘ตื่น! "จิตรลดา"ผู้ป่วยจิตเวช ออกแล้ว ด้านสถาบันยันปลอดภัย วอนสังคมให้โอกาส’ (Sanook, 1 สิงหาคม 2556) <https://www.sanook.com/news/1200425/> สืบค้นวันที่ 4 เมษายน 2566.

[69] คำพิพากษาคดีหมายเลขดำที่ 6957/2549.

[70] เนื่องจากให้การรับสารภาพจึงได้ลดโทษ

การรักษาต่อเนื่องหลังจากจำหน่ายผู้กระทำความผิดหลังออกจากโรงพยาบาล เมื่อสถาบันกัลยาณ์ราชนครินทร์จะจำหน่ายผู้ป่วยออกทันทีที่เห็นว่าอาการคงที่และปล่อยภาระการดูแลต่อให้กับครอบครัว

กรณีดังกล่าวคงต้องจับตาดูกันต่อไปว่านางสาวจิตรลดาจะประสบความสำเร็จในการยกข้อต่อสู้เรื่องการกระทำความผิดในขณะวิกลจริตในคดีใหม่หรือไม่[71] แต่หากพิจารณาจากคดีก่อนก็น่าจะเป็นไปได้ยาก เพราะในคดีนี้เธอถูกกล่าวหาว่าฆ่าเด็กหญิงอายุสี่ปีและเป็นคดีฆ่าโดยเจตนาซึ่งมีอัตราโทษสูงสุดคือประหารชีวิตซึ่งในกรณีนี้ไม่อาจคาดการณ์ได้ว่าจะมีการลงโทษประหารชีวิตหรือไม่[72] หากไม่ลงโทษประหารชีวิตแล้วจำเลยอาจจะต้องโทษจำคุกตลอดชีวิตเพื่อความปลอดภัยของสาธารณะ เพราะประเทศไทยไม่มีโรงพยาบาลที่มีการรักษาความปลอดภัยพอที่จะกักขังผู้กระทำความผิดที่มีความผิดปกติทางจิตนั่นเอง

5. ข้อเสนอแนะ

คดีของนางสาวจิตรลดาที่ยกตัวอย่างมาข้างต้นคงไม่ใช่คดีสุดท้ายของประเทศไทยที่ผู้กระทำความผิดที่มีความผิดปกติทางจิตกระทำผิดซ้ำในคดีอุกฉกรรจ์ ดังนั้น เพื่อเป็นการป้องกันและแก้ไขปัญหาในการจัดการผู้กระทำความผิดที่มีความผิดปกติทางจิต บทความนี้จึงมีข้อเสนอแนะดังต่อไปนี้

ประการแรก ก่อนที่จะกำหนดมาตรการที่เหมาะสมในการจัดการผู้กระทำความผิดที่มีความผิดปกติทางจิตควรกำหนดให้ต้องมีหลักฐานจากแพทย์อย่างน้อยสองคน ซึ่งควรเป็นจิตแพทย์หรือนักจิตวิทยาคลินิคที่ได้รับการรับรอง[73] เพื่อวินิจฉัยอาการของจำเลยและทำข้อเสนอเรื่องการบำบัดรักษา ในการนี้ การที่ศาลจะสั่งใช้มาตรการใด ศาลควรที่จะผูกพันต่อคำแนะนำในการบำบัดรักษาของแพทย์นั้นด้วย นอกเหนือจากศาลจะมีเหตุอันควรอื่นที่ไม่ควรเชื่อถือหรือปฏิบัติตามคำสั่งนั้นเพื่อเป็นมาตรการป้องกัน (safeguard) ให้แน่ใจว่าศาลจะสั่งให้มีการคุมตัวไว้ในสถานพยาบาลในกรณีที่เหมาะสมและในขณะเดียวกันเป็นการลดแนวโน้มที่ศาลจะใช้ดุลยพินิจหลีกเลี่ยงไม่สั่งให้คุมตัวไว้ในสถานพยาบาลอันเป็นปัญหาในปัจจุบัน และเป็นการตอกย้ำว่าผู้กระทำผิดที่มีความผิดปกติทางจิตนั้น ‘เจ็บป่วย’ จึงไม่สมควรได้รับการลงโทษและควรได้รับการรักษาฟื้นฟู ดังนั้น แพทย์ (จิตแพทย์) จึงมีความสำคัญในการประเมินผู้กระทำผิดว่าควรได้รับการรักษาในโรงพยาบาลหรือไม่ หากสมควรจะมีการรักษาอย่างไร

---

[71] ในปัจจุบันเดือนเมษายน 2566 ยังไม่ปรากฏข่าวคืบหน้าคดีของนางสาวจิตรลดา

[72] เนื่องจากโทษประหารชีวิตถูกบังคับใช้ในทางปฏิบัติค่อนข้างน้อยภายในระยะเวลา 17 ปีย้อนหลัง โดยล่าสุดที่มีการบังคับโทษประหารชีวิตคือ เมื่อวันที่ 18 มิถุนายน 2561. Bangkok Post, ‘Debating the death penalty’ (Bangkok Post, 20 June 2018) <https://www.bangkokpost.com/opinion/opinion/1488770/debating-the-death-penalty> accessed 4 April 2566.

[73] เช่นกรณีอังกฤษและเวลส์

ประการที่สอง ควรมีมาตรการในการจัดการผู้กระทำความผิดที่มีความผิดปกติที่หลากหลายกว่านี้ ในแง่นี้ ประเทศไทยอาจใช้ต้นแบบจากประเทศสกอตแลนด์ที่ศาลมีทางเลือกใช้มาตรการฯ ถึงหกชนิด[74] เช่นนี้ ประเทศไทยจะมีมาตรการที่เพิ่มขึ้น ได้แก่ คำสั่งคุมตัวไว้ในสถานพยาบาลแบบมีข้อกำหนด คำสั่งคุมตัวไว้ในสถานพยาบาลชั่วคราว คำสั่งผู้พิทักษ์ และคำสั่งควบคุมดูแลและบำบัดรักษา ซึ่งมาตรการที่หลากหลายจะทำให้ศาลเลือกมาตรการที่เหมาะสมกับผู้กระทำความผิดแต่ละคนซึ่งมีผลดีต่อทั้งผู้กระทำความผิดเองและมีความปลอดภัยต่อสาธารณชน อย่างไรก็ดี อาจมีข้อโต้แย้งว่าคำสั่งคุมตัวไว้ในสถานพยาบาลแบบมีข้อกำหนดเป็นการจำกัดเสรีภาพของผู้กระทำความผิดเกินควร แต่ทั้งนี้ การดังกล่าวนั้นกระทำไปเพื่อความปลอดภัยของสาธารณะ ดังนี้ มาตรการนี้จึงเป็นสิ่งจำเป็นและสามารถกระทำได้เพื่อให้แน่ใจว่าจะไม่มีการก่ออาชญากรรมซ้ำอีก โดยเฉพาะในประเทศไทยที่ไม่มีระบบติดตามหลังจากที่ผู้กระทำความผิดหลังออกจากโรงพยาบาล นอกจากนี้ หากกฎหมายไทยมีการใช้คำสั่งผู้พิทักษ์และคำสั่งควบคุมดูแลและบำบัดรักษาจะก่อให้เกิดระบบที่สามารถติดตามผู้กระทำความผิดที่มีความผิดปกติทางจิตที่มีอันตรายน้อยไม่ถึงกับต้องถูกคุมตัวไว้ในสถานพยาบาล เพราะถึงแม้เขาจะไม่อันตรายหรืออันตรายน้อยแต่ก็มีระบบที่จะช่วยให้แน่ใจได้ว่าเขาได้รับการบำบัดรักษาฟื้นฟูอย่างเหมาะสมและไม่มีความเสี่ยงที่จะก่ออาชญากรรมซ้ำอีก

ประการที่สาม ดังที่ได้กล่าวไว้ข้างต้นแล้วว่าอังกฤษและเวลส์และสกอตแลนด์นั้นมีสถานที่เฉพาะในการคุมตัวและรักษาผู้กระทำความผิดที่มีความผิดปกติทางจิต ดังนั้น ประเทศไทยก็ควรมีเช่นเดียวกัน ในกรณีนี้ มีข้อเสนอว่าสถาบันกัลยาณ์ราชนครินทร์ซึ่งเป็นสถาบันที่มีความเชี่ยวชาญในการจัดการกับผู้กระทำความผิดที่มีความผิดปกติทางจิตในประเทศไทยอยู่แล้วควรได้รับการปรับโครงสร้างเพื่อรองรับการรักษาผู้กระทำความผิดที่มีความผิดปกติทางจิตทั้งในระยะสั้นและระยะยาวซึ่งจะช่วยแก้ปัญหาการขาดสถานที่ที่รับผิดชอบในการรักษาและคุมตัวผู้กระทำความผิดที่มีความผิดปกติทางจิตในประเทศไทย ยิ่งไปกว่านั้น หากมีการสร้างสถานที่เฉพาะขึ้นมาจะเป็นการช่วยแก้ปัญหาการที่ผู้ต้องขังที่มีความผิดปกติทางจิตอย่างรุนแรงที่ต้องอยู่ในเรือนจำร่วมกับผู้ต้องขังปกติ เพราะหากมีสถานที่เฉพาะ ผู้ต้องขังมีความผิดปกติทางจิตจะสามารถได้รับการรักษาอย่างเหมาะสมและมีความเสี่ยงน้อยกว่าการถูกจำคุกและรักษาตัวไว้ในเรือนจำปกติ

ประการที่สี่ การจำหน่ายผู้กระทำความผิดที่มีความผิดปกติทางจิตออกจากโรงพยาบาลจะทำได้ต่อเมื่อมีหลักฐานทางการแพทย์สนับสนุนเท่านั้น โดยหลักฐานทางการแพทย์จะต้องมาจากจิตแพทย์หรือแพทย์ผู้รักษาและจากจิตแพทย์หรือแพทย์อีกหนึ่งคน รวมเป็นสองคน โดยการจำหน่ายออกจากโรงพยาบาลต้องได้รับอนุญาตโดยคำสั่งศาล ซึ่งเป็น ‘ระบบควบคุมสองชั้น’ ที่ช่วยป้องกันคัดกรองผู้กระทำ

[74] Section 57 Criminal Procedure (Scotland) Act 1995.

ความผิดที่มีความผิดปกติทางจิตที่อาจมีความรุนแรงและเป็นอันตราย ก่อนถูกจำหน่ายออกจากโรงพยาบาล อย่างไรก็ตาม ข้อเสียของการที่กำหนดให้ศาลต้องออกคำสั่งจำหน่ายออกจากโรงพยาบาลคือความช้าในการจำหน่าย ดังนั้นเพื่อเป็นการแก้ปัญหานี้ จึงเสนอให้มีการแก้กฎหมาย[75] ให้อำนาจพนักงานอัยการในการอนุมัติคำสั่งจำหน่ายผู้กระทำความผิดที่มีความผิดปกติทางจิตออกจากโรงพยาบาลได้แทนศาล ซึ่งจะเป็นการลดระยะเวลาในการรอคอยลงได้มาก

6. บทสรุป

มาตรการในการจัดการผู้กระทำความผิดที่เป็นผู้มีความผิดปกติทางจิตของประเทศไทยที่บังคับใช้อยู่ในปัจจุบันนั้นมีเพียงการคุมตัวไว้ในสถานพยาบาลและการปล่อยตัวตามประมวลกฎหมายอาญามาตรา 48 ซึ่งไม่เพียงพอต่อการจัดการผู้กระทำความผิดที่มีความผิดปกติทางจิตอย่างมีประสิทธิภาพ เพราะสามารถเลือกได้แค่ว่าจะจำกัดอิสรภาพและบังคับรักษา หรือปล่อยตัวเป็นอิสระ ดังที่ได้กล่าวไว้ข้างต้นว่าผู้กระทำความผิดที่มีความผิดปกติทางจิตบางรายนั้นอาจไม่ได้มีภาวะอันตรายถึงกับขนาดต้องมีการคุมตัวไว้เพื่อรักษาแต่ก็ควรได้รับการบังคับรักษาหรือดูแลในรูปแบบอื่นๆ ซึ่งเนื่องจากข้อจำกัดข้างต้นศาลอาญาที่พิจารณาคดีนั้นจะไม่มีอำนาจในการสั่งให้ไปบำบัดรักษาโดยวิธีการอื่นๆ[76] ทำให้สุดท้ายแล้วผู้กระทำความผิดที่มีความผิดปกติทางจิตอาจไม่ได้รับการรักษาอาการหรือมีผู้ติดตามดูแล ส่งผลให้อาจมีอาการกำเริบและอาจเป็นอันตรายต่อสังคมหรือกระทั่งเกิดกระทำผิดซ้ำต่อไปได้

ดังนั้น บทความวิจัยนี้จึงเสนอให้มีการเพิ่มมาตรการในการจัดการผู้กระทำความผิดที่มีความผิดปกติทางจิตของประเทศไทยให้มีความหลากหลายขึ้น และเสนอให้มีการกำหนดให้มีสถานพยาบาลที่รับคุมตัวผู้กระทำความผิดที่มีความผิดปกติโดยเฉพาะ โดยบทความนี้เสนอให้มีมาตรการต่างๆ ดังนี้ การคุมตัวไว้ในสถานพยาบาล การคุมตัวไว้ในสถานพยาบาลโดยมีเงื่อนไข (เช่น ระยะเวลาขั้นต่ำ การขออนุญาตก่อนจำหน่ายออกจากโรงพยาบาล) การคุมตัวไว้ในสถานพยาบาลชั่วคราว การตั้งผู้พิทักษ์ การตั้งผู้ควบคุมดูแลและบำบัดรักษาและการปล่อยตัว ทั้งนี้ ในการพิจารณาว่าจะบังคับใช้มาตรการใด ศาลจำต้องพิจารณาพยานหลักฐานทางการแพทย์ประกอบด้วยซึ่งมาตรการเหล่านี้จะทำให้ศาลสามารถเลือกบังคับ

---

[75] ภายใต้ประมวลกฎหมายอาญาของประเทศไทย อำนาจในการสั่งปล่อยตัวออกจากสถานพยาบาลเป็นของศาลเพราะต้องกระทำเป็นคำสั่งศาล.

[76] ความจริงแล้ว หากเป็นกรณีที่ผู้กระทำความผิดที่มีความผิดปกติทางจิตได้รับการรอการลงโทษหรือรอการกำหนดโทษ (รอลงอาญา) ตามเงื่อนไขของประมวลกฎหมายอาญา มาตรา 56 หากศาลเห็นสมควรจะสั่งให้มีการไปบำบัดรักษาในฐานะเงื่อนไขของการคุมประพฤติก็ได้เช่นกัน แต่วิธีการนี้จะใช้ได้ต่อเมื่อผู้กระทำความผิดเข้าเงื่อนไขการรอลงอาญาตามกฎหมายเสียก่อนและศาลเห็นสมควรให้รอลงอาญาเท่านั้น

มาตรการที่เหมาะสมที่สุดสำหรับผู้กระทำความผิดแต่ละคนได้และเป็นการป้องกันสังคมจากการก่ออันตราย
จากผู้กระทำความผิดที่มีความผิดปกติทางจิตต่อไป

The Challenges of Applying Competition Law to Online Platforms: The Case of Search Engines Markets

ความท้าทายในการปรับใช้กฎหมายการแข่งขันทางการค้ากับแพลตฟอร์มออนไลน์: กรณีศึกษาตลาดเสิร์ชเอนจิน

Warut Songsujaritkul *

Faculty of Law, Chiang Mai University

วรุตม์ ทรงสุจริตกุล

คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่

Received 26 March 2023; Revised 15 June 2023; Accepted 16 June 2023

Abstract

The fast-emerging aspect of online platform economic structures cast into doubt whether antitrust enforcement in information technology industries can protect consumers without damaging businesses that are rapidly developing. Adapting the current competition law system to the high technology market and, more specifically, to the case of online platforms, will not be a simple task as the developments in these markets have been unforeseen or hardly considered. The application of established case law, legal tools, and economic theories may require some adjustments in the context of online platforms. The legal concepts and economic considerations in the context of competition law are still in the initial phase of development whereas the EU Commission and the national competition authorities try to discover how competition law should apply in the case of the online platform markets. This article analyzes the application of the EU competition law in a Google

* อาจารย์ประจำ คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่

ที่อยู่: 239 ถนนห้วยแก้ว ตำบลสุเทพ อำเภอเมือง จังหวัดเชียงใหม่ 50200

E-mail: songsujaritkul.w@gmail.com

manipulating search results case. The case of Google search engine represents the most high-profile competition investigation. This is because it raises questions about the effectiveness of Article 102 of the Treaty on the Functioning of the European Union in regulating online platform markets. Therefore, in this article, the allegations of the Google search engine case are crucial to examine to illustrate that competition law may not effectively be applied to control the abusive power in the online platform market and may require changes in application methodologies when concerning online platforms.

Keywords: Online Platform Market, Search Engine, Abuse of Dominant Position

บทคัดย่อ

เมื่อโครงสร้างทางเศรษฐกิจของแพลตฟอร์มออนไลน์พัฒนาไปอย่างรวดเร็ว ทำให้เกิดคำถามว่าจะสามารถปรับใช้หลักการแข่งขันทางการค้ากับอุตสาหกรรมเทคโนโลยีสารสนเทศเพื่อคุ้มครองผู้บริโภคโดยไม่ขัดขวางการพัฒนาทางธุรกิจและเทคโนโลยีได้หรือไม่ การปรับใช้กฎหมายการแข่งขันทางการค้ากับตลาดเทคโนโลยีขั้นสูงนั้นไม่ง่ายนัก โดยเฉพาะกับแพลตฟอร์มออนไลน์ เนื่องจากตลาดที่เกี่ยวข้องกับเทคโนโลยีเหล่านี้มีการพัฒนาอย่างต่อเนื่อง รวดเร็ว และคาดการณ์ได้ยาก การปรับใช้คำพิพากษาของศาลหรือคำวินิจฉัยขององค์กรที่เกี่ยวข้อง หลักกฎหมายและทฤษฎีทางเศรษฐศาสตร์อาจต้องมีการปรับเปลี่ยนเพื่อให้เหมาะสมและสอดคล้องกับบริบทของแพลตฟอร์มออนไลน์ ปัจจุบันคณะกรรมาธิการยุโรปและคณะกรรมการการแข่งขันทางการค้าของแต่ละประเทศกำลังเผชิญกับความท้าทายในการปรับใช้หลักการแข่งขันทางการค้ากับตลาดแพลตฟอร์มออนไลน์ บทความนี้วิเคราะห์ถึงการพิจารณาและการปรับใช้กฎหมายการแข่งขันทางการค้าของสหภาพยุโรปในคดีที่กูเกิ้ล (Google) ปรับเปลี่ยนผลการค้นหา (search result) ในแพลตฟอร์มของตน คดีนี้เป็นกรณีศึกษาสำคัญซึ่งเป็นคดีเกี่ยวกับการแข่งขันทางการค้าและเสิร์ชเอนจิน (search engine) ที่ได้รับความสนใจอย่างมากเนื่องจากมีประเด็นถกเถียงในทางวิชาการถึงการวินิจฉัยมาตรา 102 ในสนธิสัญญาว่าด้วยการดำเนินงานของสหภาพยุโรป (Treaty on the Functioning of the European Union) กับตลาดเสิร์ชเอนจินอย่างกูเกิ้ล บทความนี้จึงนำเสนอบทวิเคราะห์ว่ากฎหมายการแข่งขันทางการค้าอาจไม่เหมาะสมที่จะนำมาใช้แก้ปัญหาสถานะผู้มีอำนาจเหนือตลาดในตลาดแพลตฟอร์มออนไลน์ และอาจต้องปรับเปลี่ยนวิธีการในการวิเคราะห์การกระทำของผู้ให้บริการที่เป็นตัวกลางในการเข้าถึงข้อมูลออนไลน์

คำสำคัญ: ตลาดแพลตฟอร์มออนไลน์, เสิร์ชเอนจิน, การใช้อำนาจเหนือตลาดโดยมิชอบ

1. Introduction

Online platforms currently constitute a focal point of competition law developments. The growing attention to online platforms is due to the vast economic opportunities that they facilitate. Giant online platform companies such as Facebook and Google have achieved extravagant market valuations in a short period of time. The economic and societal potential lies in the fact that online platforms have succeeded in creating new markets and disrupting the well-established. Furthermore, online platforms are likely to become even more prominent with the recent increase in the use of smartphones and tablets to promptly access the Internet. With such a significant increase in use, there will undoubtedly be more occasions that need competition law scrutiny.

However, online platforms are part of a highly dynamic and competitive market, which raises consideration of whether intervention is even appropriate and whether it can be done adequately. A key challenge is the economic model that online platforms are based upon. The intensity of competition can be witnessed in the changes that have occurred in the online market since the early twentieth century. Online platforms that were considered dominant by competition authorities were heading toward failure and were eventually replaced by new, more innovative players.[1] The intensity of competition is constantly growing with the development of Internet technology which allows for lower launching costs for businesses and often in combination with low switching costs by consumers. Companies that were once unique in their market must now compete with multiple competitors. Such intense competition results not only from newcomers to the market, but also from established players that choose to expand their business operations.[2]

Additionally, in some cases, online platforms can be linked to one another in a new model to provide a new type of platform. These circumstances make the assessment of competition on the market difficult, compared to offline markets. Also, online platform businesses may often compete not only for an existing market but also for future markets that have yet to fully materialize. Such competition will only intensify with the development of internet technology which will allow more online platforms to gain increased access to consumers. Similarly, the provision of zero-priced goods or services and the way in which

[1] P.A. Geroski, 'Competition in Markets and Competition for Markets' (2003) 3(3), Journal of Industry, Competition and Trade, 151, 159.

[2] Ibid.

personal data has become an aspect of the trade will also be relevant for competitive assessments and are likely to increase complications. [3] Furthermore, market transparency, algorithmic trading, and online interaction between competitors participating in online platforms will challenge the discovery and prohibition of coordination between competitors.

With the abovementioned taken into account, there will be challenges when attempting to apply competition law to online platforms. There are concerns that even when enforcement correctly concludes anti-competitive conduct in online platform markets, it could cause more harm than good because the effects of such harmful conduct will be short-lived. Also, the authority's decisions to initiate an investigation are likely to become outdated and possibly cause detrimental effects on economic growth. [4] Consequently, specific platform characteristics and the dynamics of the online markets in which online platforms play a prominent role must also form part of the assessment concerning potential violations of competition law. Therefore, competition law should be applied cautiously when investigating big online platform companies such as Google and Facebook because a false positive would chill its innovation and competition that is currently providing immense benefits for consumers. [5]

This article discusses the application of competition law to regulate online intermediaries. It analyzes the situation where giant online intermediaries such as Google manipulates its result recommendations to favor its affiliated services. For instance, Google may promote content or sites of its business partnership over other sites. It may have a contract to present certain viewpoints of news or current affairs in its search results rather than the opposite opinions. Therefore, it is important to analyze how competition law can be applied to these actions. This article specifically examines an EU competition case in which Google manipulated its search engine results to favor its affiliated services. Part 2 of the article, therefore, provides the background of the EU Google Shopping case. An analysis of the EU Commission and the General Court decision will then be provided in Part 3.

---

[3] Howard A. Shelanski, 'Information, Innovation and Competition Policy for the Internet' (2013) 161 University of Pennsylvania Law Review, 1663, 1666.

[4] Ibid.

[5] Geoffrey A. Manne and Joshua D. Wright, 'Google and the Limits of Antitrust: The Case Against the Case Against Google' (2011) 34 Harvard Journal of Law & Public Policy, 171, 244.

2. Background of the Google Shopping Case

In November 2010, the European Commission announced the opening of the formal antitrust inquiry into the competitive violations performed by Google.[6] The complaints were initiated by three search service providers: Foundem, Ciao, and eJustice about the unfavorable treatment of their vertical search services in Google's organic search results. The complainants have claimed to the European Commission that Google placed its own affiliated vertical search services (i.e. Google Shopping) at a more preferential position in its organic search results (Google general search engine) and lowered the ranking of the competing vertical search services (i.e. comparison-shopping service) in Google organic search results.[7] Since users tend to click predominantly on the first few entries on the screen, advertisers will most likely prefer to advertise on a higher ranking in search results (which are Google's affiliated vertical search services in this case). Google thus exploited consumers' reliance on defaults with the effect that consumers stuck with Google Shopping rather than looking out for a competing comparison-shopping website. This would then lead to the consequence that Google Shopping would generate more and more traffic, putting itself in a better position to convince merchants to provide information about their products, generate more revenue, and collect more information on users. Consequently, the downgrading vertical search services of competitors of Google's affiliated services will be less attractive to advertisers and this practice eventually leads to the exclusion of Google's competitors in the affiliated vertical search services market. Therefore, Google allegedly abuses its dominant position under Article 102 of the Treaty on the Functioning of the European Union (TFEU).

The European Commission started the formal process of finding an infringement after rejecting Google's third package of remedies. After a 7-year-long period of investigations, on the 27th of June 2017, the European Commission ruled a controversial decision that Google had been abusing its market dominance as an organic search engine by promoting its own comparison-shopping service in its search results and demoting those of competitors.[8] In other words, The Commission found that Google abused its market dominance as a search engine:

---

[6] European Commission, *Antitrust: Commission Probes Allegations of Antitrust Violations by Google* (Press Release IP/10/1624, 30 November 2010).

[7] European Commission, *Commission Seeks Feedback on Commitments Offered by Google to Address Competition Concerns* (Memo/13/383, 25 April 2013).

[8] European Commission, *Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine* (Press Release IP/17/1784, 27 June 2017).

firstly, by systematically giving prominent placement to its own comparison-shopping service and, secondly, by demoting rival comparison-shopping services in its search results. In particular, the Commission found that most highly ranked rival firms appeared on average only on page four or further of Google's search results while Google Shopping would show up at the very top of the general search results page, displayed separately and in a particular rich format (e.g., including pictures) in the "Product Universal Box" or the "Google Shopping Unit" (which contained paid advertising) and were not subject to the general relevance-based ranking of the generic search results. This preferential treatment to own comparison-shopping services results in Google Shopping being much more visible to consumers in Google's organic search results, whilst rival comparison-shopping services were much less visible.

Since the Commission's Decision does not clearly address various arguable issues related to the case, there is a lot of criticism about this decision (which will be delineated in Part 3). The specific existing law upon which the case has been built is also unclear. Besides, this case has fallen under which existing case law or which existing type of abuse is uncertain. The Commission's decision was based on a theory of self-preferencing without relying on the essential facilities doctrine as abusive conduct. However, there is a debate on whether self-preferencing can fall under Article 102 of the TFEU since a prohibition of self-preferencing contradicts the strict requirements for access to a dominant undertaking's infrastructure that has been developed under the essential facilities doctrine.

However, this is not the end of the case. Google brought an action against the Commission's decision by appealing the decision to the General Court of the European Union which took several years before the matter was fully resolved in 2021. In November 2021, The General Court largely dismissed Google's action against the decision of the Commission and found that Google abused its dominant position by favoring its own comparison-shopping service over competing comparison-shopping services. The Google Shopping case is considered to be a landmark case setting a precedent which can be used as a framework to analyze the legality of similar conduct that online intermediary companies such as search engines (e.g. Google) and social media platforms (e.g. Facebook) may have engaged in regarding other actions in the online platform market.

This article will examine legal issues and controversial debates related to this case. Precisely, the concerns are based on the fact that the fast-emerging aspect of technological industries makes competition enforcement ineffective to protect consumers without damaging business development. In other words, competition law (i.e. Article 102 of the TFEU) has

limitations to regulating the action of Google. The following section will illustrate the application of competition law to regulate online intermediaries.

3. The Application of Article 102 of the TFEU

The action of online intermediaries in placing their own affiliated content at a preferential position in their result recommendations and lowering the ranking of other competing content can reduce the advertising revenue of content-generated websites. Since users tend to click on the first few entries on the search engine or social media screen, advertisers will most likely prefer to advertise on a higher ranking in result recommendations. Consequently, the downgraded content of other sites will be less attractive to advertisers and this practice eventually leads to the exclusion of these sites from online intermediaries' platforms. Therefore, the online intermediaries' manipulation of result recommendations can be considered a violation of the prohibition of abuse of a dominant position to exercise anti-competitive conduct.

The Google's manipulation of organic search engine results can be considered a violation of the prohibition of abuse of a dominant position to exercise anti-competitive conduct under Article 102 of the TFEU which states:

"Any abuse by one or more undertakings of a dominant position within the common market or in a substantial part of it shall be prohibited as incompatible with the common market insofar as it may affect trade within Member States".

To apply Article 102 of the TFEU, there are two elements to be concerned with. One is a dominant position in a relevant market and another element is the abusive manner which is harmful to competition.

3.1 Dominant Position in a Relevant Market

The finding of dominance entails a two-stage process: starting with the definition of the relevant market and followed by an assessment of the market power within the relevant market of the concerned undertaking.

3.1.1 Relevant Market

Before determining a dominant position of Google, the relevant market needs to be defined. In competition law, products which can reasonably be interchanged are counted as

the relevant market.[9] Defining the relevant market in the case of online platforms is not easy and straightforward. This is because the fact that the development of online platforms is fast-changing: online companies have expanded or invented a new way of their business to intersect and compete with other product markets. Consequently, the line drawing of interchangeable products is a blur and will make less sense to clarify over time.

For example, it is difficult to distinguish Facebook and other different types of social media to define the relevant market. Social media which have features or functions similar to Facebook such as Myspace, Google +, and Tumblr are included in the relevant market. However, Facebook can be considered to compete with microblogging such as Twitter, content communities such as Flickr and YouTube, and social curation such as BuzzFeed and Reddit. These sites are enabling the sharing of texts, pictures, videos, audio files, and applications which are overlapping and competing with Facebook. In practice, social media have many forms and some of them may overlap with each other; people can substitute these social media services with Facebook in some circumstances. Therefore, it causes practical problems if regulators try to differentiate the relevant market of each online platform. Due to the convergence of platforms and technology, many online platforms combine various services and can reasonably be interchanged.

For search engines such as Google, search engines now turn to Universal Search which displays results not only from Web sites but also from images, videos, news, maps, and products (replacing Ten Blue Links which displayed ten search results). Universal Search bridges many information search services to compete with each other by allowing a user to search for specific content such as books through a general search which negates the need to use specialized searches or online merchant search services. Therefore, it could be debatable that the relevant market of Google's organic search engine should not be as narrow as a general search engine market and should broadly encompass any virtual search activities for

[9] The European Commission's Notice on the definition of the relevant market explains that "a relevant product market comprises all those products and/or services which are regarded as interchangeable or substitutable by the consumer, by reason of the products' characteristics, their prices and their intended use." (European Commission, *Commission Notice on the Definition of the Relevant Market for the Purposes of Community Competition Law* (OJ C372, 9 December 1997) para.7.

information.[10] This is because, in competition law, products which can reasonably be interchanged are counted as the relevant market.

In this case, two markets are involved: first, the general search market across the entire internet for whatever one enters in the search engine, and the latter, the comparison-shopping service market that allows users to search for specific products and compare prices and characteristics across different online retailers. There is a vertical link between the two markets as general searches can be used to locate suppliers of comparison-shopping sites, and thus be considered upstream.[11] Google has argued that Google organic search engines face aggressive competition for the audience's attention with other finding information services such as specialized search engines, online merchant search services like Amazon, social media like Facebook and Twitter, and other tools. These services are overlapping and competing with each other to provide search navigation for people and people can substitute these services for Google search engines in some circumstances.

However, in the European Commission's assessment of the Google Shopping case, the general search market is separated from other aggregators such as online merchant platforms, social media, and specialized searches.[12] The decision does not provide a clear distinction of why other information search services should be separated from general searches. The high market share of Google is considered only from the narrow relevant market definition of general search engine market. Moreover, the Commission focuses on a very small number of comparison-shopping sites and constitute the relevant market for comparison-shopping service which excludes online merchant platforms, specialized searches focusing on one subject matter and online search advertising platforms.[13] In other words, the Commission assumes that there is a distinct market between comparison-shopping services (where consumers do not actually shop but only compare offers such as Google Shopping) and online merchant platforms (such as Amazon and eBay which offer products for sale).

---

[10] Andrew Langford, 'gMonopoly: Does Search Bias Warrant Antitrust or Regulatory Intervention?' (2013) Indiana Law Journal, 88(4) 1559, 1568; Google, 'The New Gründergeist' (*Google Europe Blog*, 13 October 2014) <http://googlepolicyeurope.blogspot.be/2014/10/the-new-grundergeist.html> accessed 17 January 2023; Amit Singhal, 'The Search for Harm' (*Google*, 15 April 2015) <http://googleblog.blogspot.be/2015/04/the-search-for-harm.html> accessed 17 January 2023.

[11] European Commission, Commission Decision Case AT.39740 - Google Search (Shopping), Recital 154-263.

[12] European Commission, Commission Decision Case AT.39740 - Google Search (Shopping), Recital 161-190.

[13] European Commission, Commission Decision Case AT.39740 - Google Search (Shopping), Recital 191-250.

In the author's point of view, this definition of comparison-shopping market is problematic and arguable. To put it simply, this also implies that the market definition would change easily only if Google Shopping provides 'One Click Shopping' for directly buying retailing products on its own as an online merchant service.[14] Furthermore, the Commission ignores the role of merchant platforms that also enable consumers to compare prices and assumes that consumers do not choose between Amazon and Google Shopping when they want to compare offers for products. People typically do not search for direct links to the product, but for information. For almost every specific question that Internet users have on product, there are more options than searching on comparison-shopping services: the user experience with these services is similar. The rationales of the Commission in the Google case ignore actual consumer behavior and online merchant platforms as competitors in comparison-shopping services.

Google appeals that the Commission has inappropriately excluded merchant platforms from the relevant market definition and the definition of the relevant markets is erroneous in that users compare products on merchant sites as they do on comparison-shopping sites. Thus, competition in the market for comparison-shopping services remains strong because of the presence of merchant platforms in that market. However, The General Court also rejects Google's argument and confirms the Commission's assessment that those platforms are not in the same market. Although both categories of websites offer product search functions, they do not do so under the same conditions, and users, whether internet users or online sellers, do not use them in the same way but do so on a complementary basis. Consequently, there is little competitive pressure on Google from merchant platforms.

3.1.2 Dominant Position

Even if the relevant market can be defined, a dominant position or market power itself still needs to be identified. Market share is one of the important factors to determine a dominant position. For instance, market share is a significant factor to differentiate the conclusions of the Google manipulating search results case in the US and the EU. As described by the European Commission, the fact that the market share of Google's competitors in the US is around 30 percent, while in Europe, Google has above 90 percent of market share is

[14] Justus Haucap, 'Why the European Commission's decision against Google is in many respects dubious, at best' (*D'KART*, 9 June 2017) <https://www.d-kart.de/the-google-case-first-comments/> accessed 17 January 2023.

the reason why the Commission continues investigating Google's actions, even though the US Federal Trade Commission has concluded that there was no competition issue.[15] It can also be implied that Yahoo! and Bing, whose combined market share are less than 5 percent in Europe and 30 percent in the US, can manipulate their search results without raising any competition investigations. Moreover, in circumstances where the search engines or social media market is an effective competitive market and there are no dominant companies in the market, any actions of online intermediaries do not have competition issues.

According to the Google Shopping case, the decision concludes that Google is dominant in general search markets: the assessment of dominance is based on the fact that Google's general search engine has held exceeding 90 percent of market shares in most EU countries.[16] Noteworthy, the fact that an online platform has a large market share does not always mean that it has a dominant position. Market share alone, though is an important factor, is not sufficient to determine a dominant position.[17] The assessment of market power is whether the constraint from the threat of rival competition exists. This needs to be considered in conjunction with many competitive factors.[18]

The assessment of a dominant position in a relevant market of an online platform is not straightforward even in the case where that platform has a large market share. The challenges posed by the new economy markets may make a big online platform such as Google and Facebook a leading competitor but not a dominant player with market power. [19] Particularly, the characteristics of online intermediaries and online services in the new economy market may address uncertainty and the problem of applying Article 102.[20]

---

[15] European Commission, *Commission Seeks Feedback on Commitments Offered by Google to Address Competition Concerns* (Memo/13/383, 25 April 2013) p.3.

[16] European Commission, Commission Decision Case AT.39740 - Google Search (Shopping), Recital 273-284.

[17] European Commission, 'Decision Case Microsoft/Skype COMP/M.6281' para.99; 'Decision Case Microsoft/Yahoo! Search Business COMP/M.5727' para.99; *Cisco Systems Inc v European Commission* (T-79/12) (2013) at [67].

[18] Andrew Langford, 'gMonopoly' (2013) 88(4) Indiana Law Journal 1559, 1573.

[19] Geoffrey Manne and Joshua Wright, 'Google and the Limits of Antitrust' (2011) 34(1) Harvard Journal of Law and Public Policy 194.

[20] Joyce Verhaert, 'The Challenges Involved with the Application of Article 102 of the TFEU to the New Economy' (2014) European Economics: Microeconomics & Industrial Organization eJournal < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2340958> accessed 17 January 2023.

Five characteristics of the digital sector and the difficulties they cause on EU competition law will be examined as follows:

(1) Intensive Competition and Innovation

The first characteristic of a new economy market to be considered is the intensive competition in innovation developments. Continuously investing in the improvement of existing applications and refining existing platforms are crucial for the input of production and cost reduction. Therefore, to survive in the online platform market, Google has to provide a certain level of innovation and needs to keep improving constantly to compete with other operators.[21] For instance, by considering that consumers use digital platforms and applications for their own advantage, the competitive product in search engine market is the quality of search results[22]; it is not difficult (compared to physical products) for competitors to produce better search results to suit the demand of users.[23] Consequently, although Google is now the leading search engine operator, it must preserve its higher innovation rates and have to provide a better quality of its search results than competitors to maintain its market leadership and keep users attracted to its service. The degree of dynamic and innovative competition can also be emphasized by the fact that numerous specialized search platforms have constantly emerged and the fact that the leadership in the search engine market has changed regularly.[24] This intensive degree of improvement can be the indicator that any of Google's decline in innovation or the quality of search results will lead to the loss of users to other search engine operators.[25] This characteristic of a new economy which is driven by strong innovative competition makes it difficult to define the dominant position of the online platform market.

(2) High Fixed Cost but Low Marginal Cost

The second characteristic of a new economy market is 'high fixed cost but low marginal cost'. Digital platforms usually have high sunk costs because the development of novel and original products requires enormous investments; but once the products are made, the

---

[21] OECD Competition Committee, 'Competition Policy and Policy and Knowledge-Based Capital: Key Findings' (OECD, 2013) 7.

[22] European Commission, 'Decision Case Microsoft Yahoo' (Comp/M.5727, 18 February 2010) para. 101.

[23] Mark Patterson, 'Google and Search Engine Market Power' (2013) Harv.J.L.Tech 1, 4.

[24] John Battelle, *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture* (Penguin Group 2005) 49-63.

[25] Christian Kersting and Sebastian Dworschak, 'Does Google Hold a Dominant Market Position? – Addressing the (Minor) Significance of High Online User Shares' (2014) Ifo Schnelldienst 6.

developing costs of production are often low marginal costs. This characteristic compensates companies for the large capital investment and business risk by allowing them to charge above the marginal costs. Therefore, for dynamic competition to exist in the digital market, it has a rational expectation for significant market power to persist for a reasonable amount of time.

For the issue of the high sunk cost but low marginal cost in search engine market, this characteristic of search engine markets tends to cause a barrier to entry into the market which supports the first movers to have the advantage and market power.[26] Therefore, Google may be considered to have a dominant position in the search engine market. However, by considering the factual evidence of the past and present states of the online platform market, it shows that the high sunk cost does not create a barrier which allows the leading firm operators to have a dominant position. For example, Altavista and Yahoo! were once the leading search engine operators at the time when Google entered the market. Google did not only succeed in entering the market but also displaced its competitors. Similarly, Yandex surpassed Rambler which is the former leading Russian search engine operator.[27] Even now Google does not only face pressure from Bing and Yahoo! but also from new potential competitors such as Baidu and ChatGPT. Therefore, this dynamic nature of the search engine market indicates that Google which is now the leading search engine operator in Europe is not insulated from the competitive threat by a barrier to entry into market.

(3) Network Effect and Two-side Market

The third and fourth characteristics of a new economy market are 'network effect' and 'two-sided market'. The major characteristics of the search engine market and social media market are the two-sided market which creates a network effect. Network effect arises when the value of a product to its customer grows with the number of other users of the product. In two-sided platforms, network effect can be seen where a rise in the number of consumers increases the attractiveness of the platform developers and vice-versa.[28] For example, the value of social media for users depends on an increase of other users using that social media. This so-called direct network effect relates to the number of users in certain services.

[26] Andrew Langford, 'gMonopoly: Does Search Bias Warrant Antitrust or Regulatory Intervention?' (2013) Indiana Law Journal, 88(4) 1559, 1574 - 1576.

[27] Justus Haucap and Ulrich Heimeshoff, 'Google, Facebook, Amazon, eBay: Is the Internet driving competition or market monopolization?' (2014) 11 International Economics & Economic Policy, 49, 56.

[28] OECD, 'Hearings: The Digital Economy' (DAF/COMP(2012)22, 7 February 2013), 8.

The more users, the greater utility those users receive directly.[29] They, therefore, create a barrier to entry and tend to reinforce leading companies to become dominant players. There is a distinction between the indirect network effect and the direct network effect. In the case of the indirect network effect, the number of users on one side of the market increases the number of customers (e.g. advertising companies) on the other side of the market: however, the increase of customers on the other side does not directly benefits users on the one side.[30] Therefore, market power will not always occur on both sides of the two-sided market.

Another characteristic of the search engine market is the two-sided market: the search advertising market and the unpaid search engine market. The Commission states that there is also a high barrier to entry into the organic search engine market because of network effects. However, the major characteristic of search engine's two-sided market is that it creates an indirect network effect. In particular, the indirect network effect in the search engine market appears in the market of search advertising. The number of users in the unpaid search engine market increases the value of the search advertising market. Besides, any unfair conduct of Google to advertisers does not affect the number of users in the unpaid search engine market side which is the key competition in search advertising market. Thus, Google has market power on the advertising market side. On the other hand, in the unpaid search engine market, users do not care about how many other users in Google or the number or the cost of advertising in search advertising market. They are primarily concerned about the quality of search results. Therefore, Google organic search does not have direct network effects as the Commission stated and the "revenue [from advertiser in search advertising market] which can be reinvested...and improvement...to attract more users"[31] is not directly in the definition of network effects. The indirect network effect does not provide market power to Google in the organic search engine market which is the market in the consideration of the case.

(4) Switching Cost

'Switching cost' is the final characteristic of the new economy market which is a factor to assess market power and identify a dominant position in the market. If people can easily switch from using one service to another without losing anything e.g. money and time to process, it tends to be that there is intense competition in the market. For example, in the

[29] Neal Finnegan, John Kwoka and Lawrence White, *The Antitrust Revolution* (OUP 2014) 520-527.

[30] Case T-201/04, *Microsoft Corp. v. Comm'n*, 2007 E.C.R. II-3601 (Ct. First Instance), para. 1061.

[31] European Commission, Commission Decision Case AT.39740 - Google Search (Shopping), Recital 296.

social media market, the switching cost is a near-zero cost. People are 'just one click away' from other social media without incurring any penalties if they are unhappy with the services or community from their current social media platform.[32] In particular, they just type in a URL and download or install any software or sign up for an account. Besides, in fact, users now utilize more than one social media in parallel (so-called 'multi-home'). Therefore, the ease to switch service providers constrains Facebook from exercising market power.[33] However, it can be argued that search engine market has a high information cost to click away because it is difficult for people to evaluate the quality of search results whether they receive better results than using other search engine providers. Thus, instead of switching to competitors when search result is defective; users simply modify search query. Nonetheless, it does not mean that leading search engine provider such as Google has a dominant position in search engine market since Google still cannot provide poor results than its competitors and the constraint from the threat of rival competition is exist.[34]

In my opinion, it can be academically debatable whether Google is the dominant undertaking in the search engine market. This is due to the complication of the various characteristics of the new economy market which needed to be considered. In order to determine market power, the factors which must take into account are such as the dynamic change in the digital platform market, the intensive competition of technological developments, the low switch cost, and the indirect network effect.

3.2 The Anti-competitive Conduct

Even if the relevant market can be defined and the market power of Google can be specified, a dominant position in the market in itself is not an offense under Article 102 which raises competitive concerns. To apply Article 102 to search engines' manipulation of search results, a dominant position in the market must be accompanied by the abuse of market power to prevent competition. The action of Google will be an abuse of market power on the condition that such bias "must be sufficient in magnitude to exclude rival search engines

[32] For search engines, see Joshua Hazan, 'Stop Being Evil: A Proposal for Unbiased Google Search' (2013) 111(5) Michigan Law Review 789, 813.

[33] Marina Lao, 'Neutral Search as a Basis for Antitrust Action?' (Harv.J.L.Tech Occasional Paper Series, 4 April 2013) 7.

[34] Eric Goldman, 'Search Engine Bias & the Demise of Search Engine Utopianism', in Berin Szoka and Adam Marcus, *Essays on the Future of the Internet* (TechFreedom 2010) 470-471.

[or social media] from achieving efficient scale".[35] It is uncertain whether the manipulation of result recommendations to favor their own content over other rival content can be regarded as anti-competitive conduct.

Not all forms of bias in content recommendations would be considered anti-competitive conduct under competition law.[36] Anti-competitive conduct under competition law is behavior that deviates from normal competitive manners and is regarded as an unfair or distortion of competition.[37] Actions which cannot be explained as having other incentives (such as serving consumers, improving innovation, or creating efficiency) than the purpose to destroy competition can be considered as an abuse of market power.[38] Therefore, for the operations of online intermediaries to plausibly raise competitive concerns, they have to cause significant impacts on anti-competitive foreclosure (not merely affecting a single competitor but must have a negative effect on the competitive process).[39] Merely the fact that online intermediaries manipulate their content recommendations and make some competitors (especially less efficient companies) hard to survive and consequently leave the market is not a concern of competition law at all.[40] From the aspect of competition law, manipulating content recommendations can be regarded as the action to differentiate between online intermediaries which is a natural by-product of competition, is desirable, and is beneficial to consumers.

3.2.1 Abusive Conduct

According to the Commission decision, Google abused its dominant position on the internet search market by systematically giving prominent placement to its own comparison-shopping service to be displayed at or near the top of the organic search results; while demoting rival comparison-shopping services in its search results (leading them to typically be

---

[35] Joshua Wright, 'Defining and Measuring Search Bias' (George Mason Law and Economics Research Paper No. 12-14, 3 November 2011) 8.

[36] Ioannis Lianos and Evgenia Motchenkova, 'Market Dominance and Quality of Search Results in the Search Engine Market' (2013) 9(2) Journal of Competition Law & Economics 419, 452.

[37] Richard Whish and David Bailey, *Competition Law* (7th edn, Oxford University Press 2012) 196-197.

[38] Marvin Ammori and Luke Pelican, 'Competitors' Proposed Remedies for Search Bias: Search "Neutrality" And Other Proposals' (2012) 15(11) Journal of Internet Law 1, 10.

[39] Richard Whish and David Bailey, *Competition Law* (7th edn, Oxford University Press 2012) 196-197.

[40] Joshua D. Wright, 'Defining and Measuring Search Bias: Some Preliminary Evidence' (2011) George Mason Law & Economics Research Paper No. 12-14, 7.

ranked very low and appear on the fourth page).[41] However, the relevant abusive conduct stated by the Commission remains unclear. While the Commission neither objects to Google's design of its display search results pages nor to Google's demotion of certain results, the Commission precisely lists these two practices when explaining how Google has abused its dominant position.[42] Also, US Federal Trade Commission found the same practices to be product improvement to the benefit of consumers.[43]

There are counter-arguments that the mere fact that search engines or social media favors their own content cannot be implied as anti-competitive conduct under Article 102. The discrimination of Google in favor of its own content will be an abuse of market power on the condition that such bias "must be sufficient in magnitude to exclude rival search engines from achieving efficient scale".[44] Nonetheless, Google's manipulation of search results to favor its own sites may lead to more consumer traffic to that sites but does not (and cannot) block competitors to enter or appear in the market. Besides, Google's manipulation of search results does not prevent consumers from visiting competitors' sites through various means such as using other search engines, using social media, or typing URLs.[45] Therefore, the Google's manipulation may not significantly exclude competitors from achieving efficient scale to compete with Google.

Based on the author's analysis, the conduct of search engines and social media in manipulating result recommendations can be considered an efficient competitive strategy of these online intermediaries in order to be different from their competitors; such conduct benefits consumers rather than an abuse of market power.[46] For example, Google may promote certain viewpoints of current affairs or content of its business partnership over others

---

[41] European Commission, Commission Decision Case AT.39740 - Google Search (Shopping), Recital 292-296.

[42] European Commission, *Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine* (Memo IP/17/1785, 27 June 2017) 1-2.

[43] Federal Trade Commission, 'Statement of the Federal Trade Commission Regarding Google's Search Practices: *In the Matter of Google Inc.*' (FTC File Number 111-0163, 3 January 2013).

[44] Joshua D. Wright, 'Defining and Measuring Search Bias: Some Preliminary Evidence' (2011) George Mason Law & Economics Research Paper No. 12-14, 8.

[45] Daniel A. Crane, 'Search Neutrality and Referral Dominance' (2012) 8(3) Journal Of Competition Law And Economics 459, 466.

[46] Federal Trade Commission, 'Statement of the Federal Trade Commission Regarding Google's Search Practices: *In the Matter of Google Inc.*' (FTC File Number 111-0163, 3 January 2013) 3.

in its search results. Facebook may conduct a policy of its platform which prefer certain content such as prioritizing content produced by its sponsorship and preventing content generated from other social media platforms to be shared on Facebook. To be noteworthy, these actions may very well end up being a bad strategy from the consumer's viewpoint and users may prefer a different platform. Consequently, an alternative search engine or social media can be a competitive product substituted for Google and Facebook. Punishing online intermediaries for favoring certain content may reject the competitive process where customers are free to choose from various search and social media platforms.

However, the General Court found that by favoring its own comparison-shopping service over competing services rather than a better result over another result, Google departed from competition on the merits. The General Court noted that even if the results from competing comparison-shopping services were more relevant, they could never receive the same treatment as results from Google's comparison-shopping service in terms of their positioning or their display. In other words, the discrimination did not lie in a different treatment based on the nature of the results, i.e., product-related, but on the differential treatment between the origin of the results (those coming from Google were treated better than those coming from competitors).[47]

It should be noted that while the Commission had found potential anticompetitive effects in both markets (comparison-shopping service market and general search service market), the Court only regards anticompetitive effects in the comparison-shopping services market. Traffic and market shares of competing comparison-shopping services declined after Google implemented its practices, potentially reducing their incentive to innovate and reducing the ability of consumers to access the best-performing comparison-shopping services. In contrast, in the market for general search, the Court does not consider the fact that Google's action in protecting the revenue generated by specialized search resulting in financing the general search service is an anti-competitive practice.[48]

---

[47] *Google and Alphabet v Commission (Google Shopping)*, Judgment of the General Court (Ninth Chamber, Extended Composition) of 10 November 2021, paras. 284 and 351.

[48] *Google and Alphabet v Commission (Google Shopping)*, Judgment of the General Court (Ninth Chamber, Extended Composition) of 10 November 2021, para. 451.

3.2.2 Theory of Harm

There are concerns that the action of search engines and social media in placing their own affiliated content at a more preferential position in their result recommendation and lowering the ranking of the other competing content will lead to the exclusion of competitors and have a significant effect on the competitive market.[49] These anti-competitive foreclosure arguments are premised on the notion that the disappearance from the top of the search results will exclude competitors from the market. Since users tend to click predominantly on the first few entries on the search engine or social media screen, advertisers will most likely prefer to advertise on a higher ranking in result recommendation. Consequently, the downgrading content of other content-generated sites will be reduced the revenue from the advertising and this practice eventually leads to the exclusion of these sites from online intermediaries' platforms.

In contrast, in my opinion, it is questionable whether these conducts are not abusive but instead a disruptive innovation resulting in the introduction of new products. One of the characteristics of a new economy market is disruptive innovation. Disruptive innovation refers to new technologies that displace existing markets: it is also referred to as 'dynamic competition' or 'competition for the market'.[50] While price has traditionally been the main competition for conventional competition, in dynamic competition such as in the online business, innovation becomes a relevant parameter for competition.[51] Especially where users get access with zero prices to online services such as search engines and social networks, their choice is based on quality and the level of innovation. Innovation can result in the improvement of existing products or in new business models that displace the earlier and create a new market.

The author agrees with some scholars that competition law focuses on the action of consumer harm and quality-related product degradation, not harm to only a group of competitors. In other words, competition law does not seek to protect inefficient competitors.

---

[49] Fairsearch, 'Can Search Discrimination by a Monopolist Violate U.S. Antitrust Law?' (*Fairsearch* 2011) 1 <http://www.fairsearch.org/wp-content/uploads/2011/07/Can-Search-Discrimination-by-a-Monopolist-Violate-U.S.-Antitrust-Laws1.pdf> accessed 17 January 2023; Fairsearch, 'Google's Transformation from Gateway to Gatekeeper' (*Fairsearch* 2011) 2 <http://www.fairsearch.org/wp-content/uploads/2011/10/Googles-Transformation-from-Gateway-to-Gatekeeper.pdf.> accessed 17 January 2023.

[50] See Clayton Christensen, *The Innovator's Dilemma* (HBSP 1997).

[51] J. Gregory Sidak and David Teece, 'Dynamic Competition in Antitrust Law' (2009) 5(4) J.C.L.E 581, 585.

Therefore, to impose any punishment under competition law, it must be clear that the harm caused to competitors is outweighed by the benefits gained by customers. The prevention of certain businesses and the punishment for introducing innovative products conflict with the key objectives of competition law. As Atkinson comments on the Google Shopping case:

"Today's ruling is bad for consumers and bad for innovation. … The EU's actions have created a cloud of uncertainty that will make large tech companies overly cautious about making changes to the user experience and service offerings that would benefit consumers."[52]

The Commission's explanation of the theory of harm for the abusive conduct in Google Search is also flawed. The decision appears to revolve around harm to a group of competitors and there is practically no discussion convincing how the users have been harmed. As Kucharczyk added[53]:

"It seems the Commission's case is mainly focused on competitors who disagree with Google competing on the merits. We fail to see the evidence for consumer harm and for quality-related product degradation."

Google appealed to the Court that the harm caused to competitors is outweighed by the benefits gained by customers. In contrast, the punishment imposed on Google causes limited benefits granted to Google Shopping's competitors but clearly diminishes benefits for society. Google's Shopping Unit reflects efficiency and is responsive to consumers, rather than exclusionary conduct. The categorization of the search result in the form of images, places, or news (not merely through the text-only links to Web sites) is more useful for consumers since they want to find the products quickly and easily. People usually prefer links that take them directly to the products they want, not to websites where they have to repeat their searches. Therefore, the way Google displays shopping advertisements saves consumers both time and frustration and benefits advertisers who want to promote those same products. In contrast, comparison-shopping services have likely been an outdated business as a result of the normal dynamics of competition as they could not innovate to catch up with the powerful online merchant services (e.g. Amazon).

---

[52] Robert Atkinson, 'Record EU Fine Against Google Risks Creating New "Too Big To Innovate" Standard' (*ITIF*, 27 June 2017) <https://itif.org/publications/2017/06/27/record-eu-fine-against-google-risks-creating-too-big-innovate-standard> accessed 17 January 2023.

[53] Jakob Kucharczyk, 'EC Issues Record Fine In Google Shopping Case; CCIA Concerned About Chilling Effect On Innovation' (*CCIA*, 27 June 2017) <http://www.ccianet.org/2017/06/ec-issues-record-fine-in-google-shopping-case-ccia-concerned-about-chilling-effect-on-innovation/> accessed 17 January 2023.

The General Court rejects Google's arguments and points out that Google's arguments take into account only the impact of the display of results from Google's comparison-shopping service, without considering the impact of the poor placement of results from competing comparison-shopping services in the generic results. By analyzing numerous factors such as specific traffic data generated by Google's general search engine for comparison-shopping services, the correlation between the significant increase in traffic for Google's own comparison-shopping service and the overall decrease in traffic from its general results pages to competing comparison-shopping services, the Court noted that there was a sufficient basis for showing the potential outcome was the disappearance of comparison shopping services, less innovation on their market and less choice for consumers, characteristic features of a weakening of competition.

Noteworthy, the Court emphasized that the demonstration of an infringement of Article 102 of the TFEU did not necessarily have to identify actual exclusionary since the Commission had sufficiently established potential effects by showing a correlation between the practices and the reduction in traffic.[54] In other words, abuse remains abuse even if it was unsuccessful by taking into account all the relevant circumstances. Furthermore, to reject Google's argument that the Commission had not established anticompetitive effects leading to higher prices, the Court held that the as-efficient-competitor test is warranted only in the case of pricing practices (e.g., predatory pricing or margin squeeze) and the test does not aim to assess actual market participants' efficiency.[55] Thus, the test was irrelevant in this case that does not involve pricing issues.

3.2.3 Essential Facility Doctrine

It can be considered that Google, which holds a large amount of market share in the general search engine market in Europe, has more responsibility than its competitors to refrain from doing some conduct concerning competition issues.[56] As the European Court of Justice

[54] *Google and Alphabet v Commission (Google Shopping)*, Judgment of the General Court (Ninth Chamber, Extended Composition) of 10 November 2021, para. 382.

[55] *Google and Alphabet v Commission (Google Shopping)*, Judgment of the General Court (Ninth Chamber, Extended Composition) of 10 November 2021, para. 538.

[56] Paul Craig and Grìnne de Búrca, *EU Law text, cases and materials* (5th edn, OUP 2011) 1025; Richard Whish and David Bailey, *Competition Law* (7th edn, OUP 2012) 192.

stated, a firm in a dominant position has a 'special responsibility' and this special duty becomes even greater if a firm is in a super-dominant position.[57]

The Court considered that general search engines have characteristics akin to those of an essential facility since there is currently no actual or potential substitute available to be replaced in an economically viable manner on the market and competing shopping services are generally dependent on traffic from Google.[58] Nevertheless, while the Commission accused Google of refusal to grant (equal) access, the Court considers that the practice at issue is based on a difference in treatment by Google for the sole benefit of its own comparison service. The Court confirms that not every practice relating to access to such a facility necessarily means that it must be assessed in the light of the conditions applicable to the refusal to supply. Unlike traditional infrastructures, whose value lies in the owner's ability to exclude others, Google's search engine's value lies in its capacity to be open to results from external sources.[59] A general search engine is an infrastructure that is, in principle, the value of which lies in its capacity to be open to results from external (third-party) sources and to display those sources, which enrich and enhance the credibility of the search engine. If it is Google's business model to show results from other parties and therefore use them in its infrastructure, it must be treated differently than companies whose business model it is to invest in their own infrastructure to use it exclusively. Google then cannot both claim to be a neutral search engine using results from diverse sources and then discriminate between them. Therefore, Google's preferential treatment towards its shopping service in the general search result was not a competition on the merits because it was "not consistent with the intended

---

[57] Opinion of AG Fenelly in Cases C-395/96 *Compagnie Maritime Belge NV and Dafra-Lines v. Commission*, 29.10.998, (2000) ECR I-1365; Court of Justice Case T-83/91, *Tetra Pak International v. Commission*, 6.10.1994, II (1994) ECR 755; Court of Justice Case T-228/97, *Irish Sugar v. Commission*, 7.10.1999, (1999) II ECR 2969.

[58] *Google and Alphabet v Commission (Google Shopping)*, Judgment of the General Court (Ninth Chamber, Extended Composition) of 10 November 2021, para. 224.

[59] *Google and Alphabet v Commission (Google Shopping)*, Judgment of the General Court (Ninth Chamber, Extended Composition) of 10 November 2021, para. 178.

purpose of a general search service".[60] In other words, the promotion of one type of specialized result involves a certain form of abnormality.[61]

However, there is a counter-argument that self-preferencing is widespread also in other industries with more competitive market structures, such as supermarkets. Also, the manipulation of search results can be regarded as an industry standard practice since other search engines such as Bing and Yahoo! also favor its own services to be on a higher ranking in the search results. It is common for search engines (including the dominant one) to link its affiliated businesses in search results which is similar to a publisher advertising its own products. Besides, if search results are regarded as free publicity for websites, these sites will have no right to demand the appearance in search results which is in the interest of search engines whether to provide it or not.[62] Therefore, this special responsibility to refrain from the 'methods different from those which condition normal competition'[63] (known as 'compete on the merit') does not prevent Google from favouring their services in search results.

In contrast, from my point of view, Google's business model is more directly aimed at providing consumers with choices which differ from supermarkets. Although consumers seem also to prefer supermarkets with a wide range of choices, it is at least theoretically possible to imagine a supermarket offering only one product per category coming from the same producer. On the other hand, Google's general search engine would completely collapse if it would show only results from the same source. Google's proximity to and influence over consumer choices are the delineating factors compared to the essential facilities cases. In this light, giving up neutrality completely for the most visible part of the search result page is hardly explainable by pro-competitive motives.[64] Therefore, even if the manipulation of search

---

[60] *Google and Alphabet v Commission (Google Shopping)*, Judgment of the General Court (Ninth Chamber, Extended Composition) of 10 November 2021, para. 184.

[61] *Google and Alphabet v Commission (Google Shopping)*, Judgment of the General Court (Ninth Chamber, Extended Composition) of 10 November 2021, para. 176.

[62] James D Ratliff and Daniel L Rubinfeld, 'Is There a Market for Organic Search Engine Results and Can Their Manipulation Give Rise to Antitrust Liability?' (2014) 10(3) Journal of Competition Law & Economics 517, 522-526.

[63] Court of Justice Case 85/76, *Hoffmann-La Roche & Co. AG v. Commission (Vitamins)*, 13.2.1979 ECR 461.

[64] Johannes Persch, 'Google Shopping: The General Court takes its position' (Kluwer Competition Law Blog, 15 November 2021) <https://competitionlawblog.kluwercompetitionlaw.com/2021/11/15/google-shopping-the-general-court-takes-its-position/> accessed 17 January 2023.

results can be considered as a competitive strategy to be different from others, online platforms (such as search engines and social media), by its nature and functionality, should have special responsibility to be neutral at certain level in order to refrain from doing some conduct concerning anti-competitive issues.

4. Conclusion

The analysis of the situation when big online intermediaries prioritize their own affiliated content illustrates that competition law may not effectively be applied to control the actions of online intermediaries. The overview provided in this article delineates that the application of EU competition law to online platforms will be a complex matter and will primarily require changes in application methodologies when concerning online platforms. This is particularly true in the qualification of practices under Article 102 of the TFEU as well as with regard to the justification possibilities that undertakings have under these provisions.

The Court decision in the Google Shopping case is surely not the end of the story. On the contrary, this case could also mark the beginning of the anti-competitive online intermediaries' case that there are other pending cases against online platform companies in deciding what consumers access in terms of information, choice, and prices; for instance, a court in Munich put an end to Google showing health-related information from only one source in an info box on top of the search results[65]; the German Federal Cartel Office is already investigating the Google News Showcase[66]; and the European Commission has opened a formal antitrust investigation on Facebook distorting competition in the markets for online classified ads by tying its online classified ads service (Facebook Marketplace) to its personal social network (Facebook)[67].

---

[65] Johannes Persch, Should Google Still be Allowed to Crown the Kings in Digital Markets? (*Promarket*, 13 July 2021) <https://www.promarket.org/2021/07/13/google-search-digital-markets-germany-antitrust/> accessed 17 January 2023.

[66] Bundeskartellamt, Bundeskartellamt examines Google News Showcase (Bundeskartellamt, 4 June 2021) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/04_06_2021_Google_Showcase.html?nn=3591568> accessed 17 January 2023.

[67] European Commission, 'Antitrust: Commission sends Statement of Objections to Meta over abusive practices benefiting Facebook Marketplace' (Press Release IP/22/7728, 19 December 2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7728?fbclid=IwAR3EoXFlpcMbha0jTF8nmcZI0TdGvkkEizlA5t6m4pdPaEjpkpN23XH3Iu8> accessed 17 January 2023.

My analysis suggests that the judgment in the Google Shopping case will certainly make it more difficult for an online platform to develop its algorithm operation by deciding what to show to the consumer. Every change that an online platform company makes will be very carefully looked at by competition authorities (and competitors for that matter). Also, it will be tough for online platform companies to justify any behavior which is considered anti-competitive on the basis of product improvements.

Antitrust enforcement seeks to achieve a fair balance between short-static efficiencies, which include reducing costs and maximizing consumer surplus. Equally, the regulations aim to preserve a stimulating innovative environment for competitors as they strive to produce new and better products for their customers. However, considering the characteristics of online platform markets and the variety of problems in applying competition law in a new economy market, the illustration arises that the current competition law may not be an appropriate tool to tackle abusive power in the online platform market.

In order to adapt competition law to be effective and appropriate in applying to online platforms markets, the author provides primary recommendations as follows:

1. In defining relevant markets for online platforms, regulators should not differentiate the relevant market from each online platform separately and should not consider only from a narrow scope of certain product or service. Since online platforms combine various services and can reasonably be interchanged, new model of business providing a new type of platform intersects and competes with other product markets. Therefore, regulators should regard actual consumer behavior and the role of online platforms in responding to the need of consumers for defining a wide relevant market.

2. To determine dominant position in online platforms market, a large market share is not a sufficient factor to determine a dominant position. The characteristics of new economy markets such as the dynamic change in the digital platform market, the intensive competition of technological developments, the low switch cost, and the indirect network effect are needed to be considered. Consequently, a big online platform may be regarded as only a leading competitor but not a dominant player. Also, with the fact that digital platforms usually have high sunk costs, thus it has a rational expectation for significant market power to persist for a reasonable amount of time for the large capital investment of innovation.

3. Competition law should adopt new notions or principles in applying to the online platforms market as the European Court of Justice considered that general search engines have characteristics akin to those of an essential facility. The author agrees with the European

Court of Justice that a firm which holds a large amount of market share (a leading competitor) should have a 'special responsibility' and this special duty becomes even greater if a firm is in a super-leading position. Therefore, even if a firm is not a dominant player in the market, it should have an accountability to refrain from doing some conduct which is different from normal competition known as 'compete on the merit'.

4. In analyzing anti-competitive conduct, regulators should focus on the action of consumer harm which can be determined by the intensive competition in innovation developments. While price has traditionally been the main competition in conventional competition, in the online platforms market, disruptive innovation becomes a relevant parameter for competition. Therefore, for the operations of online intermediaries to plausibly raise competitive concerns, they have to cause significant negative effect on innovative products, not merely harm to only a group of competitors. The intervention that would chill innovation and competition conflicts with the key objectives of competition law.

แนวทางการเปิดเผยข้อมูลข่าวสารของราชการตามพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 ที่มีข้อมูลส่วนบุคคลรวมอยู่ด้วย

An Approach for Disclosure of Official Information containing Personal Data

*ดร.ปิติ เอี่ยมจำรูญลาภ**

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

Dr. Piti Eiamchamroonlarp

Faculty of Law, Chulalongkorn University

วันที่รับบทความ 17 กุมภาพันธ์ 2566; วันแก้ไขบทความ 15 พฤษภาคม 2566; วันตอบรับบทความ 26 พฤษภาคม 2566

บทคัดย่อ

การเปิดเผยข้อมูลข่าวสารของราชการที่มีข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 นั้นสามารถดำเนินการโดยไม่เป็นการทำลายการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคลและสามารถเกิดขึ้นควบคู่ไปกับการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ อย่างไรก็ตาม การบังคับใช้กฎหมายดังกล่าวจะต้องคำนึงถึงปัจจัยต่างๆ เพื่อสร้างความสมดุลระหว่างความโปร่งใสภาครัฐและความเป็นส่วนตัวของปัจเจกบุคคล การดำเนินการดังกล่าวอาจดำเนินการได้โดยการแยกแยะองค์ประกอบของข้อมูลเพื่อแยกข้อมูลที่จำเป็นต่อการตรวจสอบการทำงานภาครัฐและข้อมูลที่กระทบต่อความเป็นส่วนตัวของปัจเจกบุคคล ข้อมูลข่าวสารของราชการมีส่วนที่แสดงให้เห็นถึงความถูกต้องโปร่งใสและตรวจสอบได้ของหน่วยงานของรัฐซึ่งสามารถแยกจากเนื้อหาของข้อมูลที่เผยถึงตัวตนของปัจเจกบุคคลได้ นอกจากนี้ โดยหลักแล้วหน่วยงานของรัฐที่มีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ยังมีหน้าที่ต้องรักษาความมั่นคงปลอดภัยทางของข้อมูลส่วนบุคคลตามมาตรฐานที่กำหนดขึ้นตามมาตรา 37(1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มีส่วนสนับสนุนให้หน่วยงานของรัฐที่ครอบครองข้อมูลส่วนบุคคลป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อีกด้วย

คำสำคัญ: ข้อมูลส่วนบุคคล, สิทธิในความเป็นส่วนตัว, ข้อมูลข่าวสารของราชการ, ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

---

*ผู้ช่วยศาสตราจารย์ ผู้อำนวยการหลักสูตร LL.M. (Business Law) International Program คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่อยู่: 254 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพมหานคร 10330

E-mail: piti.e@chula.ac.th

Abstract

Disclosure of official information which also contain personal data in accordance with the Official Information Act B.E. 2540 (1997) can be made without infringing a right to privacy of individuals. This disclosure can also be simultaneously deemed a lawful action under the Personal Data Protection Act B.E. 2562 (2019). However, this harmonization can only be achieved when a disclosing state agency strikes fair balance between transparency in the public sector and a right to privacy of individuals. This balancing activity can be conducted by analyzing and differentiating content of the information in question. Content of the information that appears necessary for public governance examination can be separated from the part that reveals identity of an individual. In addition, a state agency that is also a data controller under the Personal Data Protection Act B.E. 2562 (2019) owes a statutory duty to ensure security of personal data it possesses in accordance with Section 37(1) of the Personal Data Protection Act B.E. 2562 (2019). This implementation can contribute to a state agency's responsibilities to prevent, handle, and mitigate risks associated with cyber threats.

Keywords: personal data, right to privacy, official information, security of personal data

1. บทนำ

สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการอธิบายว่าพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (“พระราชบัญญัติข้อมูลข่าวสารของราชการฯ”) มีเจตนารมณ์ที่ต้องการให้ประชาชนมีโอกาสอย่างกว้างขวางในการรับข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่างๆ ของรัฐ เพื่อที่ประชาชนจะได้แสดงความคิดเห็นและใช้สิทธิทางการเมืองได้ถูกต้องตรงกับความจริง เป็นการพัฒนาระบอบประชาธิปไตยให้มั่นคง ประชาชนมีโอกาสรู้ถึงสิทธิและหน้าที่ของตนอย่างเต็มที่ ส่งเสริมให้การบริหารงานของรัฐเป็นไปอย่างมีความโปร่งใส[1] แนวคิดดังกล่าวสอดคล้องกับความสัมพันธ์ระหว่างประชาธิปไตยกับการเข้าถึงข้อมูลที่รัฐครอบครองในต่างประเทศ เช่น EU Directive 2019/1024 (on open data and the re-use of public sector information) ที่อธิบายว่าการทำให้เอกสารใดๆ ที่รัฐครอบครอง (ทั้งที่เกี่ยวกับกระบวนการทางการเมืองและขั้นตอนทางกฎหมายและทางปกครอง) กลายเป็นข้อมูลที่สาธารณชนสามารถเข้าถึงได้เป็นการทั่วไปเป็นองค์ประกอบขั้นพื้นฐานที่ส่งเสริมสิทธิที่จะรับรู้ (right to information) ซึ่งเป็นพื้นฐานของหลักประชาธิปไตย[2] นอกจากนี้ การที่สาธารณชนสามารถเข้าถึงข้อมูลที่รัฐครอบครองยังมีส่วนส่งเสริมความโปร่งใส (Transparency) ความรับผิดชอบ (Accountability) ซึ่งเป็นปัจจัยช่วยส่งเสริมให้เกิดการเปลี่ยนแปลงจากประเทศที่ปกครองโดยรัฐบาลเผด็จการไปเป็นรัฐบาลที่ปกครองโดยและเพื่อประชาชน[3]

อย่างไรก็ตาม การเข้าถึงข้อมูลที่รัฐครอบครองอาจเป็นการรุกล้ำความเป็นส่วนตัวของบุคคลได้ เช่น กรณีที่ข้อมูลนั้นสามารถเปิดเผยถึงตัวตนของปัจเจกบุคคล เช่น เจ้าหน้าที่รัฐหรือประชาชน เมื่อบุคคลเหล่านี้ได้รับความคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560[4] นอกจากนี้ ปัจเจกบุคคลยังมีสถานะเป็นเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ) อีกด้วย ด้วยเหตุนี้จึงเกิด “ความท้าทาย” ในการสร้างความสมดุลระหว่างการส่งเสริมความโปร่งใสผ่านการเปิดเผยข้อมูลที่รัฐครอบครองกับการคุ้มครองสิทธิในความเป็นส่วนตัวผ่านการบังคับใช้สิทธิในข้อมูลส่วนบุคคล โดยบทความนี้จะวิเคราะห์ความสัมพันธ์และการทำงานร่วมกันระหว่างสิทธิที่บุคคลสามารถร้องขอข้อมูลข่าวสารของราชการตามมาตรา 11 แห่ง พระราชบัญญัติข้อมูลข่าวสารของราชการฯ ซึ่งมีข้อยกเว้นตามมาตรา 15 วรรคหนึ่ง (6) พระราชบัญญัติข้อมูลข่าวสารของราชการฯ ในกรณีที่การเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร และการคุ้มครองสิทธิส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ การสร้างความสมดุลนี้เป็นการวิเคราะห์และเสนอ “โอกาส” ที่จะทำให้กฎหมายทั้งสองฉบับสามารถทำงานร่วมกันได้ และช่วยให้ความโปร่งใสในภาครัฐตลอดจนการ

---

[1] สำนักงานคณะกรรมการข้อมูลข่าวสารราชการ, *สิทธิรับรู้ข้อมูลข่าวสารของประชาชน* (พิมพ์ครั้งที่ 2, บริษัทสามเจริญพาณิชย์ (กรุงเทพ) จำกัด 2549) 7.

[2] EU Directive 2019/1024 (on open data and the re-use of public sector information), Preamble (43).

[3] Nurhan Kocaoglu and Andrea Figari, *Using the Right to Information as an Anti-Corruption Tool* (Berlin, Germany Transparency International 2006) 5.

[4] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 32 วรรคหนึ่ง.

พัฒนาประชาธิปไตยไม่รุกล้ำความเป็นส่วนตัวของปัจเจกบุคคลมากเกินสมควร และในขณะเดียวกันทำให้การคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคลไม่เป็นอุปสรรคต่อความโปร่งใสในภาครัฐตลอดจนการพัฒนาประชาธิปไตย

2. เนื้อหา

2.1 การคุ้มครองสิทธิส่วนบุคคลโดยหน่วยงานรัฐ

โดยทั่วไปแล้ว “หน่วยงานของรัฐ”[5] ตกอยู่ในบังคับของทั้ง พระราชบัญญัติข้อมูลข่าวสารของราชการฯ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ในส่วนของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ บัญญัติห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลหากมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยมีข้อยกเว้นคือเป็นกรณีที่ผู้ควบคุมดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นการปฏิบัติตามกฎหมาย[6] ในขณะที่ มาตรา 11 วรรคหนึ่งแห่ง พระราชบัญญัติข้อมูลข่าวสารของราชการฯ บัญญัติรับรองสิทธิของบุคคลให้มีสิทธิขอข้อมูลข่าวสารที่หน่วยงานรัฐครอบครอง ดังนั้น หากเจ้าหน้าที่ของหน่วยงานรัฐเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 11 วรรคหนึ่งแห่ง พระราชบัญญัติข้อมูลข่าวสารของราชการฯ ย่อมเป็นการกระทำที่ชอบด้วยกฎหมาย

2.1.1 ข้อมูลส่วนบุคคลในความครอบครองของหน่วยงานรัฐ

ตามมาตรา 4 แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ บัญญัติว่าพระราชบัญญัตินี้ไม่ใช้บังคับกับหน่วยงานรัฐบางประเภท ได้แก่ (ก) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์[7] (ข) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี[8] และ (ค) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการ

---

[5] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 4. บัญญัติว่า “หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ ส่วนราชการสังกัดรัฐสภา ศาลเฉพาะในส่วนที่ไม่เกี่ยวกับการพิจารณาพิพากษาคดี องค์กรควบคุมการประกอบวิชาชีพ หน่วยงานอิสระของรัฐและหน่วยงานอื่นตามที่กำหนดในกฎกระทรวง

[6] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (6) ประกอบ 27 วรรคหนึ่ง.

[7] เพิ่งอ้าง มาตรา 4 วรรคหนึ่ง (2).

[8] เพิ่งอ้าง มาตรา 4 วรรคหนึ่ง (4).

ยุติธรรมทางอาญา[9] ดังนั้น หน่วยงานรัฐและเจ้าหน้าที่รัฐที่ไม่ได้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามภารกิจข้างต้นจึงมีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ

จากข้อยกเว้นข้างต้นจึงมีหน่วยงานของรัฐที่ไม่ได้รับการยกเว้นและมีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ เช่น กรณีขององค์กรปกครองส่วนท้องถิ่นในการปฏิบัติภารกิจของตน เทศบาลตำบล (ราชการส่วนท้องถิ่น) มีหน้าที่ต้องทำในเขตเทศบาลเช่นรักษาความสะอาดของถนน หรือทางเดินและที่สาธารณะ รวมทั้งการกำจัดมูลฝอยและสิ่งปฏิกูล[10] ส่วนองค์การบริหารส่วนตำบลมีหน้าที่ต้องทำในเขตองค์การบริหารส่วนตำบลในการรักษาความสะอาดของถนน ทางน้ำ ทางเดิน และที่สาธารณะ รวมทั้งกำจัดมูลฝอยและสิ่งปฏิกูล[11] การปฏิบัติภารกิจของเทศบาลตำบลและองค์การบริหารส่วนตำบลนั้นไม่เข้าข้อยกเว้นตามมาตรา 4 แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ในการกำจัดมูลฝอยและสิ่งปฏิกูลนั้นเป็นบริการสาธารณะที่สามารถถูกส่งได้โดยระบบออนไลน์และฐานข้อมูลอิเล็กทรอนิกส์ เนื่องจากเทศบาลตำบลสามารถสร้างระบบการยื่นและรับคำร้องผ่านทางระบบออนไลน์ได้

องค์การบริหารส่วนตำบลบางปลา อำเภอบางพลี จังหวัดสมุทรปราการได้พัฒนาและใช้งานระบบการ “คำร้องขอถังขยะ” โดยระบุให้ผู้ร้องต้องกรอกข้อมูล (ซึ่งรวมไปถึงข้อมูลส่วนบุคคล) เช่น ชื่อ-สกุลของผู้ยื่นคำขอ ที่อยู่ของผู้ยื่นคำขอ เบอร์ติดต่อของผู้ยื่นคำขอ และจำนวนถังขยะที่ขอรับ[12] เมื่อผู้ยื่นคำขอกรอกข้อมูลดังกล่าวผ่านระบบออนไลน์ (เช่น พิมพ์ในหน้าเว็บไซต์) ข้อมูลจะถูกเก็บรวบรวมและใช้โดยเจ้าหน้าที่ขององค์การบริหารส่วนตำบลบางปลาเพื่อพิจารณาและตอบสนองต่อคำขอดังกล่าว

2.1.2 หน้าที่ของหน่วยงานรัฐตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ

ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเพื่อให้บริการข้างต้น องค์กรปกครองส่วนท้องถิ่นเป็นผู้มีอำนาจตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลประเภทใดและจะใช้เพื่อวัตถุประสงค์ใดเพื่อจัดหาถังขยะให้กับผู้ยื่นคำขอ ด้วยเหตุนี้ องค์กรปกครองส่วนท้องถิ่นจึงมีสถานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ[13] และมีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ บัญญัติโดยสามารถยกตัวอย่างหน้าที่ที่สำคัญได้ เช่น

---

[9] เพิ่งอ้าง มาตรา 4 วรรคหนึ่ง (5).

[10] พระราชบัญญัติเทศบาล พ.ศ. 2496 มาตรา 50 วรรคหนึ่ง (3).

[11] พระราชบัญญัติสภาตำบลและองค์การบริหารส่วนตำบล พ.ศ. 2537 มาตรา 67 (2).

[12] องค์การบริหารส่วนตำบลบางปลา, ‘คำร้องขอถังขยะ’ (Bangpla OSS, 27 ตุลาคม 2562) <https://bangpla.oss.in.th/public/ oss/data/formgeneral/id/61/menu/0> สืบค้นวันที่ 27 ตุลาคม 2565.

[13] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6. “ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

2.1.2.1 จัดเก็บข้อมูลเท่าที่จำเป็น (Data Minimization) และชี้แจงรายละเอียดการประมวลผล (Right to be informed/Transparency)

กล่าวคือจะต้องเก็บรวบรวมให้น้อยที่สุดเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย (data minimization)[14] ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดเกี่ยวกับวัตถุประสงค์ ฐานทางกฎหมาย ระยะเวลาการเก็บรักษาข้อมูล โอกาสที่ข้อมูลส่วนบุคคลจะถูกเปิดเผย ข้อมูลเกี่ยวกับตัวองค์กรปกครองส่วนท้องถิ่นในฐานะผู้ควบคุมข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคล[15]

2.1.2.2 อ้างอิงฐานทางกฎหมาย (Lawful basis for processing)

คำว่า “ฐานทางกฎหมาย (legal basis)” ในบริบทของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลนั้นหมายถึงเงื่อนไขที่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย เช่น การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ หรือการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 24 เช่น เป็นการจำเป็นเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคล[16] และเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล[17] ในกรณีนี้ องค์กรปกครองส่วนท้องถิ่นอาจระบุว่าการเก็บและใช้ข้อมูลตามตามแบบฟอร์มคำขอถังขยะนั้นมีความจำเป็นเพื่อดำเนินการตามคำขอของผู้ยื่นคำขอ

2.1.2.3 รักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

องค์กรปกครองส่วนท้องถิ่นในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด[18] นอกจากนี้ ยังต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษาหรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม[19]

---

[14] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22.

[15] เพิ่งอ้าง มาตรา 23.

[16] เพิ่งอ้าง มาตรา 24 (3).

[17] เพิ่งอ้าง มาตรา 24 (4).

[18] เพิ่งอ้าง มาตรา 37 (1).

[19] เพิ่งอ้าง มาตรา 37 (3).

ข้อมูลเกี่ยวกับการยื่นคำขอที่เผยให้เห็นถึงตัวตนของผู้ยื่นคำขอส่งผ่านระบบออนไลน์นั้นมีสถานะเป็นทั้ง “ข้อมูลส่วนบุคคล” ทั้งตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ และ พระราชบัญญัติข้อมูลข่าวสารของราชการฯ และขณะเดียวกันก็เป็นข้อมูลข่าวสารราชการเนื่องจากอยู่ในความครอบครองของหน่วยงานรัฐ หากปรากฏว่ามีบุคคลที่สามยื่นคำขอเพื่อขอรับข้อมูล

2.2 การสร้างสมดุลระหว่างการเปิดเผยข้อมูลข่าวสารของราชการกับการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคลในทางปฏิบัติ

โดยทั่วไปแล้ว “สิทธิในความเป็นอยู่ส่วนตัว (Right to Privacy)” หมายถึง สิทธิของบุคคลที่ไม่ถูกเปิดเผยต่อสาธารณชนโดยปราศจากความต้องการ และสิทธิที่จะไม่ถูกรัฐแทรกแซงโดยปราศจากเหตุผลอันสมควร (หรือในเรื่องที่รัฐไม่มีเหตุเกี่ยวข้อง)[20] สิทธิในความเป็นอยู่ส่วนตัวในเชิงของข้อมูล (informational privacy) จำกัดการเข้าถึงบุคคลอื่นในการเข้าถึง เผยแพร่ และใช้ข้อมูลเกี่ยวกับบุคคลอื่น (information about oneself)[21] ในมิติของความสัมพันธ์ระหว่างปัจเจกบุคคลกับรัฐนั้น สิทธิในความเป็นอยู่ส่วนตัวมุ่งที่จะจำกัดขอบเขตของอำนาจรัฐในการเข้าแทรกแซงความเป็นส่วนตัวของปัจเจกบุคคล[22] นอกเหนือจากความเป็นส่วนตัวในเชิงของข้อมูลแล้ว ความเป็นส่วนตัวยังหมายรวมถึงการไม่ถูกบุคคลอื่นและรัฐแทรกแซงทางกายภาพและในทางทรัพย์สินอีกด้วย[23]

เพื่อแสดงให้เห็นถึงตัวอย่างการสร้างสมดุลระหว่างการเปิดเผยข้อมูลข่าวสารของราชการกับการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคล บทความนี้จะยกตัวอย่างถึงการวินิจฉัยอุทธรณ์คำสั่งมิให้เปิดเผยข้อมูลข่าวสารของเทศบาลตำบลด่านเกวียนเกี่ยวกับค่าตอบแทน (คำวินิจฉัยคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย (ที่ สค 200/2565)) และคำพิพากษาของศาลสหรัฐอเมริกาที่ศาลมีคำสั่งมิให้มีการเปิดเผยข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในกระบวนยุติธรรมทางอาญา (คดี U.S. Department of Justice v. Reporters Committee)

2.2.1 คำวินิจฉัยคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย (ที่ สค 200/2565)

คำวินิจฉัยนี้เป็นการวินิจฉัยถึงคำอุทธรณ์คำสั่งมิให้เปิดเผยข้อมูลข่าวสารของเทศบาลตำบลด่านเกวียนเกี่ยวกับค่าตอบแทน โดยผู้อุทธรณ์ได้ยื่นคำขอข้อมูลข่าวสารของเทศบาลตำบลด่านเกวียนเกี่ยวกับค่าตอบแทน 3 รายการ ได้แก่

---

[20] ปิติ เอี่ยมจำรูญลาภ,*การให้รัฐเข้าถึงและได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันในสหรัฐอเมริกา* (สถาบันพระปกเกล้า 2562) 6-7.

[21] Jed Rubemfeld, ‘The Right of Privacy’ (1989) 102 Harvard Law Review 737, 740.

[22] เพิ่งอ้าง 737.

[23] Anita L. Allen, ‘Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm’ (2000) 32 Connecticut Law Review 861, 866.

(1) <u>รายการที่ 1</u> สำเนาคำสั่งการจ่ายเงินประโยชน์ตอบแทนอื่นเป็นกรณีพิเศษ อันมีลักษณะเป็นเงินรางวัลประจำปีสำหรับพนักงานเทศบาล ลูกจ้างประจำ และพนักงานจ้าง ของเทศบาลด่านเกวียน ประจำปีงบประมาณ พ.ศ. 2563 จำนวน 1 ชุด

(2) <u>รายการที่ 2</u> สำเนารายการประชุมคณะกรรมการพิจารณาจ่ายเงินประโยชน์ตอบแทนอื่นเป็นกรณีพิเศษ อันมีลักษณะเป็นเงินรางวัลประจำปีสำหรับพนักงานเทศบาล ลูกจ้างประจำ และพนักงานจ้างของเทศบาลด่านเกวียน ประจำปีงบประมาณ พ.ศ. 2563 จำนวน 1 ชุด

(3) <u>รายงานที่ 3</u> สำเนาหลักฐานการลงรับหนังสือขอรับประโยชน์ตอบแทนอื่นเป็นกรณีพิเศษของผู้รับมอบอำนาจ[24]

คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย พิจารณาแล้วเห็นว่า ข้อมูลทั้งสามรายการ *“ไม่มีข้อความใดเข้าลักษณะที่หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยได้ตามมาตรา 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการฯ”*[25] โดยคณะกรรมการยังได้วินิจฉัยต่อไปว่า

> *“...การเปิดเผยข้อมูลข่าวสารจะแสดงให้เห็นถึงความถูกต้องโปร่งใส และตรวจสอบได้ของหน่วยงานของรัฐ เมื่อไม่ปรากฏว่าการเปิดเผยข่าวสารจะก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยของบุคคลคนหนึ่งบุคคลใด ดังนั้น เมื่อพิจารณาถึงการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานของรัฐ ประโยชน์สาธารณะ และประโยชน์ของเอกชนที่เกี่ยวข้องประกอบกันแล้ว จึงเห็นควรเปิดเผยข้อมูลข่าวสารรายการที่ 1 ถึงรายการที่ 3...”*[26]

อย่างไรก็ตาม คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารได้กำหนดให้ลบ ตัดทอน หรือกระทำด้วยประการใดๆ ที่ไม่เป็นการเปิดเผยข้อมูลข่าวสารส่วนบุคคลบุคคลหรือข้อมูลข่าวสารในขอบเขตสิทธิส่วนบุคคล ได้แก่ อัตราเงินเดือน อัตราค่าตอบแทน และจำนวนเงินที่จ่ายโบนัส ของผู้รับประโยชน์ตอบแทนอื่นเป็นกรณีพิเศษ ซึ่งการเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควรตามมาตรา 15 วรรคหนึ่ง (5) แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการฯ”[27]

2.2.2 คดี *U.S. Department of Justice v. Reporters Committee*

ข้อมูลส่วนบุคคลอาจถูกเก็บรวบรวมในฐานข้อมูลของรัฐ เช่น ข้อมูลเกี่ยวกับพฤติกรรมที่ถูกกล่าวหาว่าไม่ชอบด้วยกฎหมายอาจถูกเก็บรวบรวมโดยเจ้าหน้าที่ของรัฐในกระบวนยุติธรรมทางอาญา โดยมีกรณีศึกษาได้แก่คดี *U.S. Department of Justice v. Reporters Committee* ซึ่งถูกพิพากษาโดยศาลฎีกาของสหรัฐอเมริกาในปี ค.ศ. 1989 ในคดีดังกล่าว นักข่าวได้ยื่นคำร้องข้อมูลเกี่ยวกับพี่น้องสี่คนซึ่งถูกกล่าวหาว่าได้รับข้อมูลจากเจ้าหน้าที่รัฐสภาที่มีพฤติกรรมทุจริตตามกฎหมายว่าด้วยเสรีภาพในข้อมูลข่าวสาร

---

[24] คำวินิจฉัยคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย ที่ สค 200/2565.

[25] เพิ่งอ้าง 3.

[26] เพิ่งอ้าง 4.

[27] เพิ่งอ้าง.

(Freedom of Information Act หรือ “FOIA”) เมื่อคำขอถูกปฏิเสธ นักข่าวจึงได้ฟ้องคดีต่อศาลโดยอาศัยฐานที่ว่าการปฏิเสธนั้นจำกัดสิทธิในการเข้าถึงข้อมูลที่เข้าถึงได้โดยสาธารณะ (publicly available information)

กรณีมีข้อสังเกตว่า FOIA ของสหรัฐอเมริกานั้นมีเจตนารมณ์และสาระสำคัญที่สามารถเทียบเคียงได้กับพระราชบัญญัติข้อมูลข่าวสารราชการฯ[28] ของประเทศไทยซึ่งสามารถแสดงได้ตาม ตารางที่ 1 ดังนี้

ตารางที่ 1 : เปรียบเทียบเจตนารมณ์และสาระสำคัญของ FOIA (สหรัฐอเมริกา) และ พระราชบัญญัติข้อมูลข่าวสารราชการฯ

กฎหมาย	FOIA (สหรัฐอเมริกา)	พระราชบัญญัติข้อมูลข่าวสารราชการฯ
เจตนารมณ์	ให้ประชาชนมีสิทธิรับรู้ถึงข้อมูลเกี่ยวกับรัฐบาลของตน[29] เพื่อการตรวจสอบ (inspection) และการขอสำเนา (copying)[30]	ให้ประชาชนมีโอกาสอย่างกว้างขวางในการรับข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่างๆ ของรัฐ เพื่อที่ประชาชนจะได้แสดงความคิดเห็นและใช้สิทธิทางการเมืองได้ถูกต้องตรงกับความจริง
หลักการสำคัญ	ให้สิทธิแก่สารธารณชนให้สามารถเรียกร้องการเข้าถึง (request access) ข้อมูลใดๆ จากหน่วยงานรัฐในสหพันธรัฐ	หน่วยงานรัฐมีหน้าที่ตามมาตรา 9 ต้องจัดให้มีข้อมูลข่าวสารของราชการให้ประชาชนได้เข้าตรวจดู และรับรองสิทธิของประชาชนในการยื่นคำขอข้อมูลข่าวสารราชการตามมาตรา 11
ข้อยกเว้น (ตัวอย่าง)	ไม่เปิดเผยในกรณีมีความจำเป็นเพื่อรักษาความเป็นส่วนตัวของบุคคล ความมั่นคงของรัฐ และการบังคับใช้กฎหมาย	ไม่เปิดเผยในกรณีมีความจำเป็นเพื่อรักษาความเป็นส่วนตัวของบุคคล ความมั่นคงของรัฐ และการบังคับใช้กฎหมายตามมาตรา 15
การดำเนินการ	หากปรากฏความจำเป็นอย่างชัดเจนที่จะต้องป้องกันการรุกล้ำความเป็น	ถ้ามีส่วนที่ต้องห้ามมิให้เปิดเผยตามมาตรา 14 หรือมาตรา 15 อยู่ด้วย ให้ลบหรือตัดทอนหรือ

[28] รองศาสตราจารย์ คณาธิป ทองรวีวงศ์ ได้ตั้งข้อสังเกตเอาไว้ว่า “สำหรับการใช้ดุลพินิจในการเปิดเผยข้อมูลนั้น กฎหมาย FOIA มีหลักการคล้ายคลึงกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ของไทย ดังที่ได้วิเคราะห์มาแล้ว แต่พบว่ามีข้อแตกต่างที่สำคัญในส่วนของการใช้ดุลพินิจไม่เปิดเผยข้อมูล ซึ่งตามกฎหมายไทยนั้น มิได้มีการกำหนดโทษสำหรับกรณีเจ้าพนักงานใช้ดุลพินิจไม่เปิดเผย แต่มีการกำหนดโทษในกรณีการเปิดเผยข้อมูลที่ไม่ชอบด้วยกฎหมาย อย่างไรก็ตาม เมื่อเปรียบเทียบกับ กฎหมาย FOIA พบว่า มีการกำหนดโทษทางวินัยสำหรับเจ้าหน้าที่ซึ่งไม่อนุญาต (Withholding) ให้เปิดเผยข้อมูลหากเป็นการกระทำตามอำเภอใจหรือตามอารมณ์ (Arbitrarily or capriciously) จึงเห็นได้ว่า กฎหมาย FOIA มุ่งเน้นหลักการสนับสนุนสิทธิได้รู้ (Right to know) โดยให้หน่วยงานของรัฐเปิดเผยข้อมูลข่าวสารมากกว่ากรณีของกฎหมายไทย โปรดดู คณาธิป ทองรวีวงศ์, ‘ข้อยกเว้นของการเปิดเผยข้อมูลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 : ศึกษากรณีข้อมูลส่วนบุคคล’ (2560) 1(1) วารสารนิติศาสตร์และสังคมท้องถิ่น 47, 62.

[29] FOIA, ‘What is the FOIA?’ (United States Department of Justice, 2022) <https://www.foia.gov/faq.html> accessed 31 October 2022.

[30] US Code § 552 (Public information; agency rules, opinions, orders, records, and proceedings), (a)(2).

ตารางที่ 1 : เปรียบเทียบเจตนารมณ์และสาระสำคัญของ FOIA (สหรัฐอเมริกา) และ พระราชบัญญัติข้อมูลข่าวสารราชการฯ		
กฎหมาย	FOIA (สหรัฐอเมริกา)	พระราชบัญญัติข้อมูลข่าวสารราชการฯ
(กรณีจำเป็นเพื่อคุ้มครองความเป็นส่วนตัว)	ส่วนตัวเกินสมควร (unwarranted invasion of personal privacy) หน่วยงานของรัฐสามารถลบรายละเอียดออกได้[31]	ทำโดยประการอื่นใดที่ไม่เป็นการเปิดเผยข้อมูลข่าวสารนั้น (มาตรา 9 วรรคสอง)

ศาลฎีกาของสหรัฐอเมริกาวินิจฉัยว่าข้อมูลที่ถูกร้องขอนั้นแม้จะเคยเป็นข้อมูลสาธารณะอยู่ ณ เวลาหนึ่ง แต่เมื่อคำนึงถึงต้นทุนในการระบุถึงข้อมูล ตำแหน่งที่เก็บ และการเข้าถึง ทำให้เกิดความความคาดหวังอย่างสมเหตุสมผลในความเป็นส่วนตัว (reasonable expectation of privacy)[32] ข้อมูลเกี่ยวกับตัวพี่น้องทั้งสี่นั้นไม่ได้เป็นข้อมูลสาธารณะเพียงเพราะครั้งหนึ่งเคยเป็นข้อมูลสาธารณะ แต่ความคาดหวังอย่างสมเหตุสมผลในความเป็นส่วนตัวนั้นมีอยู่เนื่องจากความยุ่งยากในการเข้าถึงข้อมูลนั้น (practical obscurity)[33] คดี *U.S. Department of Justice v. Reporters Committee* ได้แสดงให้เห็นว่าข้อมูลที่ถูกเก็บรวบรวมโดยรัฐนั้นอาจก่อให้เกิดสถานการณ์ที่จะต้องมีการใช้สิทธิที่จะถูกลืม[34]ได้ เช่น เป็นกรณีที่ข้อมูลส่วนบุคคลของปัจเจกบุคคลถูกเก็บรวบรวมโดยเจ้าหน้าที่รัฐในกระบวนยุติธรรม[35]

2.2.3 แนวทางในการสร้างสมดุลระหว่างความโปร่งใสภาครัฐกับสิทธิในความเป็นส่วนตัวของปัจเจกบุคคล

คำวินิจฉัยคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย (ที่ สค 200/2565) และคดี *U.S. Department of Justice v. Reporters Committee* แสดงให้เห็นว่าการเปิดเผยข้อมูลที่หน่วยงานรัฐครอบครองนั้นสามารถเกิดขึ้นโดยไม่เป็นการทำลายการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคล

---

[31] Ibid.

[32] Christopher Kotfila, 'This Message Will Self-Destruct: The Growing Role of Obscurity and Self-Destructing Data in Digital Communication' (2014) Bulletin of the Association for Information Science and Technology 40(2) 12, 13.

[33] Ibid.

[34] สิทธิที่จะถูกลืม (Right to be Forgotten) หมายถึง สิทธิของเจ้าของข้อมูลส่วนบุคคลที่ข้อมูลส่วนบุคคลของตนจะถูกลบทำลาย หรือทำให้ไม่สามารถระบุตัวตนได้เมื่อหมดความจำเป็นที่ข้อมูลนั้นจะต้องถูกประมวลผลหรือเข้าถึงได้อีกต่อไป ไม่ว่าจะโดยการที่เจ้าของข้อมูลส่วนบุคคลร้องขอหรือผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการโดยปราศจากการร้องขอของเจ้าของข้อมูลส่วนบุคคล

[35] ปิติ เอี่ยมจำรูญลาภ, *บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) และแนวทางแก้ไขกฎหมายที่เกี่ยวข้อง* (สถาบันพระปกเกล้า 2565) 58.

ข้อมูลข่าวสารของเทศบาลตำบลด่านเกวียนเกี่ยวกับค่าตอบแทนนั้นเป็นข้อมูลที่ช่วยให้ข่าวสารจะแสดงให้เห็นถึงความถูกต้องโปร่งใส และตรวจสอบได้ของหน่วยงานของรัฐ โดยการเปิดเผยเพื่อสร้างความโปร่งใสดังกล่าวไม่จำเป็นต้องมีการเปิดเผยถึงตัวตนของปัจเจกบุคคล ด้วยเหตุนี้ จึงมีการไม่เปิดเผยข้อมูลส่วนที่จะกระทบต่อสิทธิส่วนบุคคลได้ ในขณะที่ คดี *U.S. Department of Justice v. Reporters Committee* ก็แสดงให้เห็นว่าข้อมูลส่วนบุคคลที่เคยมีประโยชน์จากการให้สารณชนเข้าถึง ณ เวลาหนึ่ง อาจหมดความจำเป็นที่จะต้องถูกเข้าถึงได้เมื่อเวลาผ่านพ้นไป โดยสามารถแสดงแนวทางการวิเคราะห์ได้ตามตารางที่ 2 ดังนี้

ตารางที่ 2 : แนวทางการวิเคราะห์เพื่อสร้างความสมดุลระหว่าง ความโปร่งใสภาครัฐและความเป็นส่วนตัวของปัจจเจกบุคคล		
ข้อมูล	ค่าตอบแทนการจ่ายเงินประโยชน์ตอบแทนอื่นเป็นกรณีพิเศษ รายการประชุมคณะกรรมการพิจารณาจ่ายเงินประโยชน์ตอบแทนอื่น สำเนาหลักฐานการลงรับหนังสือขอรับประโยชน์ตอบแทนอื่นขององค์กรปกครองส่วนท้องถิ่น	
การแยกแยะองค์ประกอบ	ส่วนที่แสดงถึงเฉพาะการปฏิบัติงานของหน่วยงานรัฐเท่านั้น	ส่วนที่ระบุถึงตัวตนของผู้รับเงินได้ (เป็นข้อมูลส่วนบุคคล)
ประโยชน์ที่ถูกคุ้มครอง	ประโยชน์สาธารณะ (ความถูกต้องโปร่งใส และตรวจสอบได้ของหน่วยงานของรัฐ)	สิทธิในความเป็นส่วนตัว
มิติด้านเวลา	เป็นข้อมูลข่าวสารราชการซึ่งอาจมีการลบทำลายเมื่อถึงเวลาที่กฎหมายกำหนด	เมื่อเวลาพ้นผ่านไปอาจไม่ความจำเป็นที่สาธารณชนจะต้องเข้าถึงข้อมูลนี้
การเปิดเผยข้อมูล	✓	✗

ตารางที่ 2 แสดงให้เห็นว่าการเปิดเผยข้อมูลข่าวสารของราชการเพื่อสร้างความโปร่งใสภาครัฐนั้นสามารถดำเนินการโดยไม่เป็นการทำลายการคุ้มครองข้อมูลส่วนบุคคลจนเกินสมควรและสามารถเกิดขึ้นควบคู่ไปกับการคุ้มครองข้อมูลส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้

2.3 ความท้าทายในการรักษาความมั่นคงปลอดภัยของข้อมูล

ความท้าทายในโลกยุคดิจิทัลอาจเกิดขึ้นจากปัญหาความปลอดภัยทางไซเบอร์ “ข้อมูลข่าวสารของราชการ” ที่หน่วยงานรัฐครอบครองอาจถูกเก็บรวบรวมและเก็บรักษาโดยระบบอิเล็กทรอนิกส์ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 กำหนดให้ยกเลิกความในข้อ 29 แห่งระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. 2526 ซึ่งแก้ไขเพิ่มเติมโดยระเบียบสำนักนาย กรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ 2) พ.ศ. 2548 และให้ใช้ความต่อไปนี้แทน

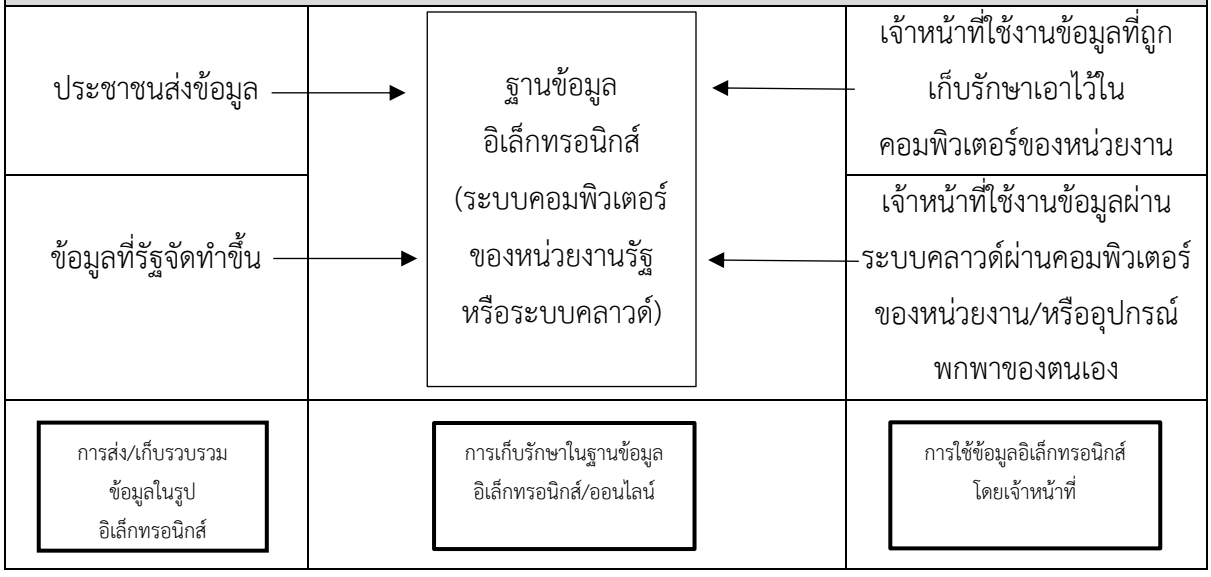
"การติดต่อราชการให้ดำเนินการด้วยระบบสารบรรณอิเล็กทรอนิกส์เป็นหลักเว้นแต่กรณีที่เป็นข้อมูลข่าวสารลับชั้นลับที่สุดตามระเบียบว่าด้วยการรักษาความลับของทางราชการหรือเป็นสิ่งที่เป็นความลับของทางราชการชั้นลับที่สุดตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ หรือมีเหตุจำเป็นอื่นใดที่ไม่สามารถรถดำเนินการด้วยระบบสารบรรณอิเล็กทรอนิกส์ได้"[36]

นอกจากนี้ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 ยังให้ยกเลิกความในวรรคสองของข้อ 27 แห่งระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. 2526 ซึ่งแก้ไขเพิ่มเติมโดยระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ 2) พ.ศ. 2548 ซึ่งให้นิยามของ "หนังสืออื่น"[37] เอาไว้ และให้ใช้ข้อความต่อไปนี้แทน

"สื่อกลางบันทึกข้อมูลตามวรรคหนึ่ง หมายความว่า สื่อใดๆ ที่อาจใช้บันทึกข้อมูลได้ด้วยอุปกรณ์ทางอิเล็กทรอนิกส์ รวมตลอดทั้งพื้นที่ที่ส่วนราชการใช้ในการจัดเก็บข้อมูลอิเล็กทรอนิกส์ด้วย เช่น บริการคลาวด์ (cloud computing)"[38]

เมื่อพิจารณาระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณซึ่งถูกแก้ไขเพิ่มเติมข้างต้นแล้ว กล่าวได้ว่าหน่วยงานรัฐสามารถเก็บรวบรวมและใช้ข้อมูลข่าวสารราชการซึ่งถูกเก็บในรูปอิเล็กทรอนิกส์และอาจถูกเก็บรักษาในระบบคลาวด์ได้โดยสามารถแสดงให้เห็นตัวอย่างตามแผนภาพที่ 1 ดังนี้

แผนภาพที่ 1 : การเก็บรวบรวม เก็บรักษา และใช้ข้อมูลข่าวสารราชการในรูปแบบอิเล็กทรอนิกส์



[36] ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 ข้อ 7.

[37] "หนังสืออื่น" คือ หนังสือหรือเอกสารอื่นใดที่เกิดขึ้นเนื่องจากการปฏิบัติงานของเจ้าหน้าที่เพื่อเป็นหลักฐานในราชการ ซึ่งรวมถึงภาพถ่าย ฟิลม์ แถบบันทึกเสียง แถบบันทึกภาพ และสื่อกลางบันทึกด้วย หรือหนังสือของบุคคลภายนอก ที่ยื่นต่อเจ้าหน้าที่และเจ้าหน้าที่ได้รับเข้าทะเบียนของทางราชการแล้ว มีรูปแบบตามที่กระทรวง ทบวง กรม จะกำหนดขึ้นตามความเหมาะสม เว้นแต่มีแบบตามกฎหมายเฉพาะเรื่องให้ทำตามแบบ เช่น โฉนด แผนที่ แบบ แผนผัง สัญญา หลักฐานการสืบสวนและคำร้อง เป็นต้น

[38] ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 ข้อ 6.

การส่งหรือเก็บรวบรวมข้อมูลในรูปอิเล็กทรอนิกส์ การเก็บรักษาในฐานข้อมูลอิเล็กทรอนิกส์หรือออนไลน์ การใช้ข้อมูลอิเล็กทรอนิกส์โดยเจ้าหน้าที่นั้นอาจภัยคุกคามทางไซเบอร์[39] จากการกระทำของอาชญากรไซเบอร์และอาจรั่วไหลอันเกิดจากการประมาทของเจ้าหน้าที่ของหน่วยรัฐ

2.3.1 การรักษาความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ”) ให้นิยามของ “การรักษาความมั่นคงปลอดภัยไซเบอร์” เอาไว้ว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ[40] ส่วน “ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง[41]

หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีหน้าที่ตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฯต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว[42]

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ[43]
นอกจากนี้ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้ออกประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการ

---

[39] “ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

[40] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 3.

[41] เพิ่งอ้าง.

[42] เพิ่งอ้าง มาตรา 44 วรรคหนึ่ง.

[43] เพิ่งอ้าง มาตรา 44 วรรคสาม.

รักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 เพื่อเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากลเพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[44]

2.3.2 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

การมีมาตรการความมั่นคงปลอดภัยที่เหมาะสมมีวัตถุประสงค์เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยผู้ที่ไม่ได้รับอนุญาตทั้งเจตนาและไม่ได้เจตนา ซึ่งในบางกรณีความมั่นคงปลอดภัยของข้อมูลอาจถือเป็นความมั่นคงปลอดภัยทางไซเบอร์ประเภทหนึ่ง เนื่องจากเป็นการป้องกันเครือข่ายและระบบข้อมูลขององค์กรจากการโจมตีทางไซเบอร์ และยังครอบคลุมถึงเรื่องมาตรการความมั่นคงปลอดภัยทางกายภาพและทางองค์กร (physical and organisational security measures) อีกด้วย[45]

มาตรา 37(1) แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ เป็นส่วนหนึ่งที่แสดงให้เห็นว่ากฎหมายสามารถสร้างแนวทางการดำเนินการเพื่อสร้างความมั่นคงปลอดภัยแก่ข้อมูลส่วนบุคคล โดยกฎหมายบัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่

“จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด”

ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 มาตรการรักษาความความมั่นคงปลอดภัย หมายความว่า “การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของ

---

[44] ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564, บทนำ.

[45] ปิติ เอี่ยมจำรูญลาภ และ ปรีชา เลิศอัศววิวัฒน์, ‘โครงการศึกษาและพัฒนามาตรฐานความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Samsung Knox Solutions)’ (รายงานผลการวิจัยเสนอต่อบริษัท ไทยซัมซุง อิเลคโทรนิคส์ จำกัด), คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย 2564.

ข้อมูลส่วนบุคคล ทั้งนี้เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ[46]

มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม[47] นอกจากนี้ มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล[48]

2.3.3 แนวทางในการรักษาความมั่นคงปลอดภัยของข้อมูอิเล็กทรอนิกส์และการใช้งานข้อมูลในฐานข้อมูลอิเล็กทรอนิกส์

การที่หน่วยงานของรัฐ (ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ) มีหน้าที่ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ และมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ซึ่งมีหน้าที่ต้องรักษาความมั่นคงปลอดภัยทางของข้อมูลส่วนบุคคลตามมาตรฐานที่กำหนดขึ้นตามมาตรา 37(1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ย่อมนับได้ว่าเป็น “โอกาส” ที่หน่วยงานของรัฐจะสามารถบริหารจัดการความเสี่ยงอันเกิดจากภัยคุกคามทางไซเบอร์หรือการรั่วไหลของข้อมูลส่วนบุคคลโดยความประมาทเลินเล่อ ซึ่งสามารถแสดงตัวอย่างได้ตามตารางที่ 3 ด้านล่างนี้

---

[46] ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 3.

[47] เพิ่งอ้าง ข้อ 4(1).

[48] เพิ่งอ้าง ข้อ 4(2).

ตารางที่ 3 : ตัวอย่างแนวทางในการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์และการใช้งานข้อมูลในฐานข้อมูลอิเล็กทรอนิกส์		
กฎหมาย	พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ฯ	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ
สถานะของหน่วยงาน	หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	ผู้ควบคุมข้อมูลส่วนบุคคล
ความท้าทาย	ถูกอาชญากรไซเบอร์ใช้โปรแกรมไม่พึงประสงค์โดยมุ่งประทุษร้ายต่อข้อมูลคอมพิวเตอร์ของหน่วยงานของรัฐ	เจ้าหน้าที่ทำอุปกรณ์พกพาส่วนตัวซึ่งสามารถเข้าถึงข้อมูลส่วนบุคคลในฐานะข้อมูลออนไลน์ได้หาย
มาตรการ (ตัวอย่าง)	- จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ[49] - จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์[50]	- นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลภายในองค์กร โดยกำหนดข้อปฏิบัติแก่เจ้าหน้าที่ และ จำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น - จัดหาอุปกรณ์มือถือที่ได้รับการออกแบบมาด้วยความปลอดภัยซึ่งมีเทคโนโลยีการพิสูจน์ตัวตน มีนวัตกรรมการจดจำใบหน้าและลายนิ้วมือ เสียง การเข้าถึงข้อมูลแม้ว่าอุปกรณ์จะสูญหายหรือถูกขโมย

3. บทสรุป

เมื่อพิจารณาแล้วว่ารัฐต้องเก็บรวบรวมข้อมูลเท่าที่จำเป็นและชี้แจงรายละเอียดการประมวลผลข้อมูลที่ถูกเก็บรวบรวม การดำเนินการเพื่อเก็บรวบรวมและเก็บรักษาข้อมูลต้องระบุว่าการเก็บและใช้ข้อมูลนั้นมีความจำเป็นเพื่อดำเนินการอย่างไร และในกรณีการเปิดเผยข้อมูลข่าวสารของราชการตามพระราชบัญญัติข้อมูลข่าวสารราชการฯ นั้นสามารถดำเนินการโดยไม่เป็นการทำลายการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคลและสามารถเกิดขึ้นควบคู่ไปกับการคุ้มครองข้อมูลส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้ อย่างไรก็ตาม การบังคับใช้กฎหมายดังกล่าวจะต้องคำนึงถึงปัจจัยต่างๆ เพื่อสร้างความสมดุล

[49] ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564, 17.

[50] เพิ่งอ้าง 5.

ระหว่างความโปร่งใสภาครัฐและความเป็นส่วนตัวของปัจเจกบุคคล การดำเนินการดังกล่าวอาจดำเนินการได้โดยการแยกแยะองค์ประกอบของข้อมูลเพื่อแยกข้อมูลที่จำเป็นต่อการตรวจสอบการทำงานภาครัฐและข้อมูลที่กระทบต่อความเป็นส่วนตัวของปัจเจกบุคคล เมื่อได้แยกแยะข้อมูลดังกล่าวแล้วก็จะเห็นถึงประโยชน์ของการเปิดเผยข้อมูลในแต่ละส่วนกล่าวคือส่วนที่เป็นประโยชน์สาธารณะและส่วนที่เป็นข้อมูลส่วนบุคคล การเปิดเผยสามารถเลือกเฉพาะส่วนที่ไม่เป็นการรุกล้ำความเป็นส่วนตัวเกินสมควรหรือส่วนที่ไม่จำเป็นต่อการตรวจสอบการทำงานของหน่วยงานรัฐได้ซึ่งเป็นแนวทางการปฏิบัติที่สอดคล้องกับการดำเนินการในต่างประเทศ เช่น กฎหมาย FOIA ของสหรัฐอเมริกา โดยเมื่อพิจารณาร่วมกับแนวทางตามกฎหมายไทยดังปรากฏในคำวินิจฉัยคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย (ที่ สค 200/2565) แล้วจะเห็นว่ารัฐจะต้องเปิดเผยข้อมูลข่าวสารของราชการที่จะแสดงให้เห็นถึงความถูกต้องโปร่งใส และตรวจสอบได้ของหน่วยงานของรัฐ อย่างไรก็ตามเป็นหน้าที่ของรัฐที่การเปิดเผยเพื่อสร้างความโปร่งใสดังกล่าวจะต้องไม่กระทบต่อข้อมูลที่การเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร และต้องพิจารณาถึงสถานการณ์ที่จะต้องมีการใช้สิทธิที่จะถูกลืมได้ เช่น เป็นกรณีที่ข้อมูลส่วนบุคคลของปัจเจกบุคคลถูกเก็บรวบรวมโดยเจ้าหน้าที่รัฐในกระบวนยุติธรรม ดังนั้นการร้องขอให้เปิดเผยข้อมูลข่าวสารของทางราชการเพื่อตรวจสอบความโปร่งใสในอนาคต หน่วยงานของรัฐจึงต้องมีความระวัดระวังทั้งในเรื่องของการจัดเก็บข้อมูลส่วนบุคคลและการเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการฯและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ อันเป็นสร้างสมดุลระหว่างการเปิดเผยข้อมูลข่าวสารของราชการกับการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคลในทางปฏิบัติให้เหมาะสม

เนื่องจากติดต่อราชการได้กลายเป็นการดำเนินการด้วยระบบสารบรรณอิเล็กทรอนิกส์เป็นหลัก การส่งหรือเก็บรวบรวมข้อมูลในรูปอิเล็กทรอนิกส์ การเก็บรักษาในฐานข้อมูลอิเล็กทรอนิกส์หรือออนไลน์ การใช้ข้อมูลอิเล็กทรอนิกส์โดยเจ้าหน้าที่ย่อมกลายเป็นสิ่งที่หลีกเลี่ยงไม่ได้ ซึ่งหน่วยงานของรัฐครอบครองอยู่ตามพระราชบัญญัติข้อมูลข่าวสารของราชการฯ และรวมถึงการที่ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ อยู่ในรูปข้อมูลอิเล็กทรอนิกส์หรือออนไลน์ ซึ่งสิ่งเหล่านี้ก่อให้เกิด “ความท้าทาย” เช่นภัยคุกคามทางไซเบอร์อันเป็นกระทำโดยจงใจของอาชญากรไซเบอร์ หรือการรั่วไหลของข้อมูลอันอาจเกิดจากการประมาทของเจ้าหน้าที่ของหน่วยรัฐ ซึ่งหน่วยงานของรัฐมีหน้าที่ทั้งตามพระราชบัญญัติ ความมั่นคงทางไซเบอร์ ในฐานะเป็นหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการรักษาความมั่นคงปลอดภัยของข้อมูอิเล็กทรอนิกส์และการใช้งานข้อมูลในฐานข้อมูลอิเล็กทรอนิกส์ และหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

การที่หน่วยงานของรัฐมีหน้าที่ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ และขณะเดียวกันก็มีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ซึ่งมีหน้าที่ต้องรักษาความมั่นคงปลอดภัยทางของข้อมูล

ส่วนบุคคลตามมาตรฐานที่กำหนดขึ้นตามมาตรา 37(1) แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2565 ย่อมนับได้ว่าเป็น “โอกาส” ที่หน่วยงานของรัฐจะสามารถบริหารจัดการความเสี่ยงอันเกิดจากภัยคุกคามทางไซเบอร์หรือการรั่วไหลของข้อมูลส่วนบุคคลโดยความประมาทเลินเล่อได้ โดยเป็นการรักษาและคุ้มครองข้อมูลส่วนบุคคลโดยอาศัยอำนาจหน้าที่ที่กฎหมายทั้งสองฉบับส่งเสริมซึ่งกันและกันในการคุ้มครองข้อมูลส่วนบุคคล เช่น การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์เพื่อเป็นแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ร่วมกับการจัดหาอุปกรณ์ที่ได้รับการออกแบบมาด้วยความปลอดภัยให้กับเจ้าหน้าที่ เป็นต้น ขั้นตอนการรักษาข้อมูลส่วนบุคคลในแง่นี้จำเป็นต้องคำนึงถึงทั้งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ และพระราชบัญญัติความมั่นคงทางไซเบอร์ฯ

ความสัมพันธ์ระหว่างแนวคิดเรื่องความปลอดภัยไซเบอร์ และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล

The Correlations between the Concept of Cybersecurity and The Personal Data Protection Law*

*ดร. อัญธิกา ณ พิบูลย์***

คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์

Dr. Auntika Na Pibul

Graduate School of Law, National Institute of Development Administration

วันที่รับบทความ 15 พฤษภาคม 2566; วันแก้ไขบทความ 1 มิถุนายน 2566; วันตอบรับบทความ 6 มิถุนายน 2566

บทคัดย่อ

ในปัจจุบัน เทคโนโลยีเข้ามามีบทบาทอย่างมากต่อการดำรงชีวิตและการดำเนินกิจกรรมต่างๆ ของทั้งภาครัฐ ภาครัฐวิสาหกิจ และภาคเอกชน และเนื่องจากกระบวนการทำงานของเทคโนโลยีดังกล่าวจะต้องมีการประมวลผลข้อมูลส่วนบุคคลเพื่อนำเสนอบริการประเด็นในเรื่องความปลอดภัยไซเบอร์จึงได้รับความสนใจอย่างมากจากสังคม เพราะเป็นปัจจัยสำคัญที่ส่งผลกระทบโดยตรงต่อการคุ้มครองข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล แนวคิดในเรื่องความปลอดภัยไซเบอร์เป็นหลักการสำคัญที่ปรากฏอยู่ในหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เป็นหน้าที่ของผู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลซึ่งจำเป็นต้องจัดให้มีมาตรการทางเทคโนโลยีและมาตรการขององค์กรที่เหมาะสมในการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคล อย่างไรก็ตาม การเชื่อมโยงความสัมพันธ์ระหว่างแนวคิดในเรื่องความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องที่ค่อนข้างท้าทาย เนื่องจากเครื่องมือที่ใช้ในการสร้างความปลอดภัยไซเบอร์อาจไม่มีประสิทธิภาพในการคุ้มครองข้อมูลตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนั้น การบริหารจัดการความสัมพันธ์ระหว่างแนวคิดเรื่องความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลจึงเป็นสิ่งสำคัญสำหรับทุกองค์กร การสร้างความสมดุลระหว่างผลประโยชน์ด้านความปลอดภัยไซเบอร์และการคุ้มครองสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลจึงอาจเป็น

---

*บทความวิจัยนี้เป็นส่วนหนึ่งของโครงการวิจัยเรื่องความสัมพันธ์ระหว่างความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล

** อาจารย์ประจำคณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์

ที่อยู่: คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ 148 ถนนเสรีไทย แขวงคลองจั่น เขตบางกะปิ กทม 10240.

E-mail: auntika.n@nida.ac.th

แนวทางที่เหมาะสมในการบริหารจัดการความสัมพันธ์ระหว่างแนวความคิดทั้งสอง ซึ่งในการดำเนินการดังกล่าวจะต้องมีการกำหนดนโยบายที่ชัดเจนและปรับใช้มาตรการที่เหมาะสมกับบริบทขององค์กร

คำสำคัญ: ความปลอดภัยไซเบอร์, หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล, ความสัมพันธ์

Abstract

Nowadays, technology plays a crucial role in various aspects of life and business operations for both the public sector, state-owned enterprises, and private sector. This is because the workflow of such technologies often involves processing personal data for providing services. Cybersecurity has therefore gained significant attention from society, as it is a vital factor directly impacting the protection of personal data and the right to privacy of data subjects. The concept of cybersecurity is an important principle reflected in personal data protection law, as it is the responsibility of those who involved in processing personal data to implement appropriate technological and organizational measures in order to ensure security of personal data. However, aligning cybersecurity concepts with personal data protection laws can be challenging. This is because the tools used to enhance cybersecurity may not necessarily be effective in protecting data according to personal data protection law. Therefore, managing the correlations between the concept of cybersecurity and the protection of personal data is crucial for every organization. Striking a balance between the interests of the cybersecurity and the right to privacy of data subjects may be a suitable approach in managing the correlations between these two concepts. By combining the ideas and ensuring a balance, organization should set out a clear policy and implement measures that are suitable for the organization's context.

Keywords: Cybersecurity, Personal Data Protection Law, Correlations

1. บทนำ

เทคโนโลยีมีบทบาทสำคัญต่อการดำเนินกิจกรรมของมนุษย์ในฐานะเป็นปัจจัยหลักในการขับเคลื่อนภารกิจต่างๆ ของทั้งภาครัฐ ภาครัฐวิสาหกิจ และภาคเอกชน เนื่องจากเทคโนโลยีต่างๆ มักจะถูกนำมาใช้ในการอำนวยความสะดวก ทำให้เกิดความรวดเร็ว และป้องกันความผิดพลาดต่างๆ ที่อาจเกิดขึ้นจากการกระทำความของมนุษย์ และด้วยเหตุดังกล่าวจึงทำให้ทุกคนในสังคมตัดสินใจใช้เทคโนโลยีรูปแบบต่างๆ ทั้งในการดำรงชีวิตประจำวันและการทำงาน จึงอาจกล่าวได้ว่า เทคโนโลยีเป็นปัจจัยสำคัญสำหรับการดำรงชีวิตของมนุษย์และความเจริญก้าวหน้าของสังคมและประเทศชาติ

อย่างไรก็ตาม ในขณะที่เทคโนโลยีถูกนำไปใช้เพื่อให้เกิดประโยชน์และการพัฒนา อาชญากรก็นำเอาเทคโนโลยีดังกล่าวไปใช้เป็นเครื่องมือในการกระทำความผิดในหลากหลายรูปแบบ ซึ่งการกระทำความผิดดังกล่าวจะถูกเรียกว่า “อาชญากรรมไซเบอร์”หรือ “Cybercrime” หากพิจารณาจากสถิติของอาชญากรรมไซเบอร์ที่เกิดขึ้นในช่วงทศวรรษที่ผ่านมาก็จะพบว่ามีแนวโน้มเพิ่มสูงขึ้นทุกปี[2] นอกจากนั้น ปรากฏการณ์การระบาดของโรคติดเชื้อไวรัสโคโรนาก็ถือเป็นปัจจัยสำคัญประการหนึ่งที่ทำให้ประชาชนจะต้องอยู่ในระบบออนไลน์มากขึ้น จึงส่งผลโดยตรงต่ออัตราการเกิดขึ้นของอาชญากรรมไซเบอร์ที่เพิ่มสูงขึ้นไปด้วย รวมทั้งทำให้เกิดอาชญากรรมไซเบอร์ในรูปแบบใหม่ๆ และมีความหลากหลายมากยิ่งขึ้น[3] ซึ่งสถานการณ์เหล่านี้ก่อให้เกิดความเสียหาย ส่งผลกระทบต่อความปลอดภัยของประชาชนที่ตกเป็นเหยื่อทั้งในส่วนของร่างกาย ชีวิตและทรัพย์สิน รวมทั้งส่งผลกระทบต่อองค์กรและความเจริญก้าวหน้าทางเศรษฐกิจของประเทศในภาพรวมอีกด้วย และด้วยลักษณะของเทคโนโลยีที่มีความซับซ้อน จึงก่อให้เกิดปัญหาและอุปสรรคในการดำเนินกระบวนการยุติธรรมทางอาญาเพื่อป้องกันและปราบปรามอาชญากรรมไซเบอร์ในหลากหลายประเด็น เช่น ในกรณีที่ผู้กระทำความผิดสวมรอยเป็นบุคคลอื่น หรือผู้กระทำความผิดอยู่ต่างประเทศ ปัจจัยเหล่านี้ส่งผลให้เกิดความยากลำบากในการบ่งชี้ตัวผู้กระทำความผิดและอาจต้องใช้ระยะเวลาค่อนข้างนานในการค้นหาและจับกุมตัวผู้กระทำความผิดมาลงโทษ ดังนั้น การปรับใช้มาตรการต่างๆ เพื่อเป็นการสนับสนุนให้เกิดความปลอดภัยไซเบอร์จึงเป็นประเด็นที่ทุกหน่วยงานให้ความสำคัญเป็นอย่างมากในฐานะที่เป็นเครื่องมือในการป้องกันมิให้เกิดอาชญากรรมไซเบอร์

---

[2] Eduard Kovacs ‘Cybercrime Losses Exceeded $10 Billion in 2022: FBI’ (SecurityWeek, 13 March 2023). <https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi/> accessed 1 March 2023.

[3] Rejest Kumar, Siddharth Sharma, Chirag Vachhani and Nitish Yadav, ‘What Changed in the Cyber-Security After COVID-19?’ (2022) 120 Computer & Security 1, 1-2 And Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple and Xavier Bellekens, ‘Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic’ (2021) 105(1) Computers & Security 1; Statista, ‘Where Do IT Professionals See an Increase in Cyber Attacks and Attack Attempts Following the COVID-19 Pandemic?’ (Statista, July 2021). <https://www.statista.com/statistics/1258261/covid-19-increase-in-cyber-attacks> accessed 1 March 2023.

ในขณะเดียวกัน หากพิจารณาถึงลักษณะของอาชญากรรมไซเบอร์ที่เกิดขึ้น ก็จะพบว่ามีการใช้เทคโนโลยีในการประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมากและก่อให้เกิดความเสียหายทั้งต่อประชาชนและสังคม กล่าวคือ มีการกระทำความผิดในลักษณะของการเข้าถึงโดยมิชอบหรือการเปิดเผยโดยทุจริตซึ่งข้อมูลส่วนบุคคลของประชาชนเป็นจำนวนมาก ดังนั้น ประเด็นในเรื่องการคุ้มครองข้อมูลส่วนบุคคลซึ่งมีความเชื่อมโยงกับสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลจึงได้รับความสนใจอย่างมากจากสังคมในช่วงที่ผ่านมา

ตัวอย่างสถานการณ์ที่เกิดขึ้นในประเทศไทย เช่น ในเดือนกันยายน พ.ศ. 2564 กรณีที่แฮกเกอร์อ้างว่าสามารถเข้าถึงข้อมูลผู้ป่วยของกระทรวงสาธารณสุขจำนวนประมาณ 16 ล้านรายการ และนำเอาข้อมูลดังกล่าวไปจำหน่ายผ่านเว็บบอร์ด ที่ชื่อว่า Raidforums โดยใช้ชื่อบัญชีว่า Inanimate ในการลงขายข้อมูล โดยอ้างว่านำมาจากระบบของกระทรวงสาธารณสุขประเทศไทย ซึ่งข้อมูลดังกล่าวประกอบด้วยข้อมูลเลขทะเบียนผู้ป่วย ชื่อ นามสกุล ที่อยู่ วันเดือนปีเกิด เบอร์โทรศัพท์ รวมถึงชื่อแพทย์เจ้าของไข้ รหัสเข้าใช้ระบบโรงพยาบาล และข้อมูลอื่นๆ[4]

ตัวอย่างสถานการณ์ที่เกิดขึ้นในต่างประเทศ เช่น ในเดือนกุมภาพันธ์ พ.ศ. 2564 บริษัท Dedalus Biologie ซึ่งเป็นบริษัทขายโปรแกรมสำหรับห้องปฏิบัติการวิเคราะห์ผลทางการแพทย์ ทำข้อมูลของคนไข้จำนวนประมาณ 500,000 รายการรั่วไหลสู่สาธารณชน ซึ่งข้อมูลดังกล่าวประกอบด้วย ชื่อ นามสกุล หมายเลขประกันสังคม ชื่อของแพทย์เจ้าของไข้ วันที่คนไข้เข้ารับการตรวจ และข้อมูลสุขภาพประวัติการเจ็บป่วยของคนไข้ ในกรณีนี้บริษัทดังกล่าวถูกปรับเป็นจำนวน 1.5 ล้านยูโร โดยสำนักงานกำกับดูแลเรื่องการคุ้มครองข้อมูลของฝรั่งเศส เนื่องจากมีการโอนย้ายข้อมูลในระบบนอกเหนือไปจากคำสั่งของผู้ว่าจ้างซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล ถือเป็นการดำเนินการเกินขอบเขตวัตถุประสงค์ที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล รวมทั้งไม่มีการใช้มาตรการทางเทคนิคที่เหมาะสมในกระบวนการโอนย้ายข้อมูลส่วนบุคคลในระบบจึงทำให้ข้อมูลเกิดการรั่วไหล ในกรณีนี้เนื่องจากบริษัทดังกล่าวอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปหรือที่เรียกกันว่า “กฎข้อบังคับการคุ้มครองข้อมูลทั่วไป” (General Data Protection Regulation (GDPR)) บริษัท Dedalus Biologie จึงมีความรับผิดฐานไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล[5]

จากสถานการณ์ที่กล่าวมาข้างต้น จึงสะท้อนให้เห็นถึงความสัมพันธ์ระหว่างความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ผู้เขียนจึงมุ่งศึกษาแนวคิดของความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อวิเคราะห์ความสัมพันธ์และผลกระทบของความปลอดภัยไซเบอร์ที่มีต่อ

---

[4] ‘พบประกาศขายข้อมูลคนไข้ของ สธ. ล่าสุดลิงค์หายไปแล้ว’ (ไทยโพสต์, 7 กันยายน 2564) <https://www.thaipost.net/main/detail/115865> สืบค้นวันที่ 1 มีนาคม 2566.

[5] European Data Protection Board ‘Health Data Breach: Dedalus Biologie Fined 1.5 Million Euros’ (EDPB, 4 May 2022) <https://edpb.europa.eu/news/national-news/2022/health-data-breach-dedalus-biologie-fined-15-million-euros_en> accessed 1 March 2023.

การคุ้มครองข้อมูลส่วนบุคคล นอกจากนั้นจะมุ่งศึกษาเพื่อค้นหาแนวทางที่เหมาะสมในการสร้างความสมดุลระหว่างการสร้างความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

บทความนี้มีวัตถุประสงค์ในการนำเสนอผลการศึกษาวิจัยเพื่อค้นหาคำตอบของโจทย์วิจัยที่ว่า “ความปลอดภัยทางไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีความสัมพันธ์กันหรือไม่ อย่างไร” ซึ่งในการตอบคำถามดังกล่าว ผู้เขียนได้กำหนดขอบเขตของการศึกษาวิจัยเป็น 4 หัวข้อ ดังต่อไปนี้

1. แนวคิดและทฤษฎีที่เกี่ยวข้องกับความปลอดภัยไซเบอร์
2. แนวคิดของการคุ้มครองข้อมูลส่วนบุคคลและหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล
3. วิเคราะห์ความสัมพันธ์ระหว่างแนวคิดในเรื่องความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล
4. บทสรุปและข้อเสนอแนะ

งานวิจัยนี้ใช้วิธีการวิจัยเชิงเอกสาร (Documentary Research) โดยมุ่งศึกษา

1) เอกสารขั้นปฐมภูมิ (primary document) ได้แก่ กฎหมายของสหภาพยุโรปที่เกี่ยวข้องกับความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

2) เอกสารชั้นทุติยภูมิ (secondary document) ได้แก่ หนังสือ บทความในวารสารวิชาการทั้งภาษาไทยและต่างประเทศ รวมทั้งข้อมูลจากหน่วยงานที่เกี่ยวข้องในการกำหนดแนวทางในการปฏิบัติตามหลักกฎหมายที่เกี่ยวข้องกับความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป เช่น Article 29 Data Protection Working Party (A29WP), European Data Protection Board (EDPB) รวมทั้งข้อมูลจากเว็บไซต์ของหน่วยงานต่างๆ ที่เกี่ยวข้อง

2. แนวคิดและทฤษฎีที่เกี่ยวข้องกับความปลอดภัยไซเบอร์

คำว่า “ความปลอดภัยไซเบอร์ หรือ Cybersecurity” ถูกใช้เป็นการทั่วไปแทนคำว่า “ความปลอดภัยของคอมพิวเตอร์และความปลอดภัยของข้อมูลข่าวสาร” (Information Security and Computer Security) เป็นแนวคิดที่เน้นเรื่องความปลอดภัยของระบบเครือข่าย ข้อมูล โปรแกรม และคอมพิวเตอร์ จากการกระทำที่ไม่มีอำนาจหรือการเปลี่ยนแปลงที่เกิดขึ้นโดยไม่ตั้งใจ การสูญหาย การแก้ไขหรือการเข้าถึงโดยมิชอบ และด้วยเหตุผลหน่วยงานต่างๆ เช่น ภาครัฐ องค์กรธุรกิจ สถานพยาบาล สถาบันทางด้านการเงิน ฯลฯ มีการเก็บรวบรวมข้อมูลไว้ในระบบคอมพิวเตอร์และส่งต่อกันผ่านระบบเครือข่าย จึงทำให้อัตราของการโจมตีทางไซเบอร์มีจำนวนเพิ่มมากขึ้น ดังนั้น แนวคิดในเรื่องความปลอดภัยไซเบอร์จึงไม่ใช่แค่เพียงความปลอดภัยของข้อมูลและความลับทางการค้าเท่านั้น แต่ยังหมายถึงความปลอดภัยของโครงสร้างพื้นฐานของประเทศอีกด้วย แนวคิดในเรื่องความปลอดภัยไซเบอร์ (Cyber Security) คือแนวคิดเดียวกันกับเรื่องความปลอดภัยทาง

เทคโนโลยี (IT Security) ซึ่งหมายถึงการสงวนรักษาไว้ซึ่งข้อมูลข่าวสารให้ปลอดภัยจากความเสียหายต่างๆที่อาจเกิดขึ้นจากการกระทำโดยไม่มีอำนาจ[6]

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union (ITU)) ได้กำหนดคำนิยามของคำว่า “ความปลอดภัยไซเบอร์ (Cyber Security)” ว่าหมายถึง “การรวบรวมเครื่องมือ นโยบาย แนวคิดเรื่องความปลอดภัย แนวคิดเรื่องการรักษาความปลอดภัย แนวทาง วิธีการจัดการกับความเสี่ยง การดำเนินการ การฝึกอบรม แนวปฏิบัติที่ดี และเทคโนโลยีที่สามารถใช้ในการคุ้มครองสภาพแวดล้อมทางไซเบอร์ รวมทั้งทรัพย์สินขององค์กรและของผู้ใช้งานซึ่งหมายความรวมถึงอุปกรณ์คอมพิวเตอร์ โครงสร้างพื้นฐาน แอปพลิเคชัน บริการ ระบบการสื่อสาร รวมทั้งข้อมูลข่าวสารทั้งหมดที่มีการโอนและ/หรือเก็บรักษาในสภาพแวดล้อมทางไซเบอร์[7]

แนวคิดพื้นฐานในการสร้างความปลอดภัยไซเบอร์ประกอบด้วย 3 หลักการดังนี้

1) Confidentiality (การรักษาความลับ) กล่าวคือ การมีมาตรการในการควบคุมและป้องกันมิให้มีการเข้าถึงข้อมูลโดยผู้ที่ไม่มีอำนาจ

2) Integrity (ความสมบูรณ์) กล่าวคือ การมีมาตรการในการรักษาไว้ซึ่งความถูกต้องและความสมบูรณ์ของข้อมูล โดยการป้องกันมิให้มีการแก้ไขข้อมูลโดยไม่มีอำนาจ

3) Availability (ความพร้อมใช้งาน) คือ การมีมาตรการที่ทำให้สามารถเข้าถึงข้อมูลและสามารถใช้งานข้อมูลได้ตลอดเวลา[8]

รูปแบบภัยคุกคามที่ส่งผลกระทบต่อความปลอดภัยไซเบอร์มีหลายรูปแบบ โดยมีตัวอย่างดังต่อไปนี้

1) Malware เป็นคำที่มาจากคำว่า Malicious และ Software หมายถึง โปรแกรมที่ประสงค์ร้ายซึ่งถูกสร้างขึ้นเพื่อนำไปใช้ในการโจรกรรมข้อมูล ทำให้เสียหาย ทำลายคอมพิวเตอร์และระบบคอมพิวเตอร์ ตัวอย่าง Malware ที่รู้จักกันทั่วไป เช่น Viruses, Worms, Ransomware, Adware, Spyware

2) Phishing หมายถึง รูปแบบการโจมตีเหยื่อผ่านทางอีเมล, ข้อความ, เว็บไซต์ หรือสื่อสังคมออนไลน์ต่างๆ โดยใช้วิธีการหลอกให้ผู้ใช้งานหลงเชื่อและส่งมอบข้อมูลส่วนตัวให้ เช่น เลขประจำตัวประชาชน หมายเลขบัตรเครดิต หรือข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวไปใช้ซึ่งจะก่อให้เกิดความเสียหายต่อเจ้าของข้อมูล

---

[6] Cynthia Brumfield, *Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework* (1st edn, Wiley 2021).

[7] International Telecommunication Union, ‘Definition of Cybersecurity’ <https://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20strives%20to%20ensure%20the,risks%20in%20the%20cyber%20environment.> accessed 1 March 2023.

[8] Manju Khari, Gulshan Shrivastava, Sana Gupta and Rashmi Gupta, ‘Role of Cyber Security in Today’s Scenario’ in Information Resources Management Associations (ed), *Cyber Security and Threads: Concepts, Methodologies, Tools and Applications* (1st edn, IGILOBAL: USA 2018) 1-15.

3) Spam หมายถึง รูปแบบการส่งข้อมูล, ข้อความที่ไม่พึงประสงค์ให้กับผู้รับผ่านช่องทางต่างๆ เช่น อีเมล, ข้อความ, เว็บไซต์ หรือสื่อสังคมออนไลน์ต่างๆ โดยเป็นการส่งจำนวนมาก ซึ่งโดยส่วนมากจะทำไปเพื่อวัตถุประสงค์ในการโฆษณาเชิงพาณิชย์

4) DDoS (Distributed Denial of Service) Attack หมายถึง รูปแบบการโจมตี โดยการส่งชุดคำสั่งเป็นจำนวนมากไปรบกวนการทำงานโดยปกติของระบบการให้บริการ ระบบเครือข่าย หรือเซิร์ฟเวอร์ ส่งผลให้เกิดการชะลอหรือขัดขวางการทำงานจนเพื่อไม่สามารถใช้งานได้[9]

การกำหนดแนวทางในการสร้างความปลอดภัยไซเบอร์นั้น จะต้องพิจารณาทั้งในส่วนของภัยคุกคามภายนอกและภัยคุกคามภายในซึ่งอาจเกิดขึ้นจากความตั้งใจหรือไม่ตั้งใจของบุคลากรภายในด้วย ควรมีการกำหนดนโยบายเพื่อรักษาความปลอดภัยของระบบเครือข่ายและควบคุมการเข้าถึงระบบเครือข่าย เช่น การจำกัดประเภทของอุปกรณ์ที่สามารถเข้าถึงเครือข่าย หรือ ใช้ไฟร์วอลล์ (Firewall) เพื่อรักษาความปลอดภัยของเครือข่าย[10] นอกจากนั้น การบริหารจัดการความเสี่ยง (Risk Management) ถือเป็นเรื่องสำคัญที่ต้องพิจารณาดำเนินการโดยผู้เชี่ยวชาญ การบริหารจัดการความเสี่ยงที่ดีนั้นจะเกิดขึ้นจากกำหนดนโยบายและแนวทางที่ชัดเจนในการรับมือกับเหตุการณ์ภัยคุกคามไซเบอร์ประเภทต่างๆ และในขณะเดียวกันแนวทางดังกล่าวจะต้องมีความเหมาะสมกับบริบทขององค์กร การบริหารจัดการความเสี่ยงที่ดีจะช่วยป้องกันความเสียหายที่อาจจะเกิดขึ้น รวมทั้งสร้างความเชื่อมั่นให้กับลูกค้าซึ่งจะส่งผลดีต่อชื่อเสียงขององค์กรด้วย[11]

หลักกฎหมายของสหภาพยุโรปที่เกี่ยวข้องกับมาตรการในการสร้างความปลอดภัยไซเบอร์ที่สำคัญถูกกำหนดขึ้นในปี ค.ศ. 2016 ภายใต้ชื่อว่า “ระเบียบเกี่ยวกับมาตรการในการรักษาความปลอดภัยของเครือข่ายและระบบข้อมูลข่าวสารระดับสูงทั่วไปที่ใช้ทั่วทั้งสหภาพ” (*Directive* (EU) 2016/1148 on Measures for a High Common Level of Security of Network and Information Systems Across the Union)[12] โดยมีสาระสำคัญคือ การกำหนดให้ประเทศสมาชิกปรับใช้มาตรการและกลยุทธ์ที่เกี่ยวกับการรักษาความปลอดภัยของเครือข่ายและระบบข้อมูลข่าวสาร การแต่งตั้งเจ้าหน้าที่ที่มีความสามารถเพื่อตอบสนองต่อภัยคุกคามไซเบอร์ที่เกิดขึ้น รวมทั้งจัดตั้งคณะทำงานเพื่อให้เกิดความสะดวกในการร่วมกันทำงานและแลกเปลี่ยนข้อมูลกันระหว่างประเทศสมาชิก

ต่อมาระเบียบฉบับนี้ได้รับการปรับปรุงเพื่อให้มีความทันสมัยเหมาะสมกับสถานการณ์ความเจริญก้าวหน้าทางเทคโนโลยีในปัจจุบันมากขึ้น ภายใต้ชื่อว่า “ระเบียบเกี่ยวกับมาตรการในการรักษาความปลอดภัยไซเบอร์ระดับสูงทั่วไปที่ใช้ทั่วทั้งสหภาพ” (Directive (EU) 2022/2555 on Measures for a High

---

[9] Jonathan Clough, *Principles of Cybercrime* (2nd edn, CUP 2015) 3-21.

[10] National Institute of Standards and Technology (NIST), ‘ Framework for Improving Critical Infrastructure Cybersecurity’ (12 February 2014, Version 1.0).

[11] Peter Sommer and Ian Brown, ‘Reducing Systemic Cybersecurity Risks’ (OECD/IFP Project on Future Global Shocks, 2011).

[12] *Directive* (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on Measures for a High Common Level of Network and Information Systems Across the Union (NIS Directive).

Common Level of Cybersecurity Across the Union)[13] โดยมีวัตถุประสงค์เพื่อขยายขอบเขตของการบังคับใช้ของกฎเกณฑ์ที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ให้ครอบคลุมไปยังหน่วยงานทุกภาคส่วนของสังคม รวมทั้งมีการพัฒนาความยืดหยุ่นของระบบของภาครัฐและภาคเอกชนในการตอบสนองต่อภัยคุกคามที่เกิดขึ้น และพัฒนาความสามารถของพนักงานเจ้าหน้าที่ที่เกี่ยวข้อง

สาระสำคัญของระเบียบฉบับนี้ คือ การกำหนดมาตรการทางกฎหมายเพื่อเพิ่มระดับความปลอดภัยไซเบอร์ในสหภาพยุโรป ยกตัวอย่างเช่น การกำหนดภาระหน้าที่ให้หน่วยงานต่างๆ จะต้องจัดให้มีมาตรการในการรักษาความปลอดภัยที่เหมาะสม และหากมีภัยคุกคามที่ร้ายแรงเกิดขึ้น จะต้องมีการแจ้งไปยังพนักงานเจ้าหน้าที่ที่เกี่ยวข้อง โดยประเทศสมาชิกจะต้องจัดตั้งทีมสำหรับการตอบสนองต่อเหตุการณ์คุกคามความปลอดภัยทางคอมพิวเตอร์ (Computer Security Incident Response Team (CSIRT)) และ เจ้าหน้าที่ที่มีความสามารถเกี่ยวกับเครือข่ายระดับชาติและระบบข้อมูลข่าวสาร (A Competent National Network and Information Systems (NIS) Authority) นอกจากนั้น ยังมีการกำหนดให้ผู้ให้บริการดิจิทัลประเภทต่างๆ เช่น ผู้ให้บริการ Cloud Computing ผู้ให้บริการ Online Marketplaces และผู้ให้บริการ Search Engine จะต้องอยู่ภายใต้ระเบียบฉบับนี้ด้วย

3. แนวคิดของการคุ้มครองข้อมูลส่วนบุคคลและหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล

แนวคิดของการคุ้มครองข้อมูลส่วนบุคคลได้รับการพัฒนาขึ้นอย่างเป็นรูปธรรมอย่างชัดเจนในประเทศแถบภาคพื้นยุโรป ปัจจัยสำคัญที่ทำให้มีการพัฒนาและนำหลักเกณฑ์ในเรื่องการคุ้มครองข้อมูลส่วนบุคคลมาใช้อย่างจริงจังนั้นเริ่มมาจากแนวคิดที่ว่า การคุ้มครองข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัวซึ่งเป็นสิทธิมนุษยชนขั้นพื้นฐานของประชาชนที่ได้การรับรองตามกฎหมาย บุคคลจึงได้ควรรับการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวอย่างเสมอกัน ไม่จำกัดแต่เฉพาะบุคคลที่เป็นสมาชิกรัฐใดรัฐหนึ่งเท่านั้น ทั้งนี้เนื่องจากในเรื่องของความเป็นส่วนตัวในข้อมูลส่วนบุคคลของแต่ละคนนั้นเป็นสิ่งที่ติดตัวมากับความเป็นมนุษย์ กฎหมายจึงเป็นเพียงเครื่องมือในการรับรองการมีอยู่หรือดำรงอยู่ตามธรรมชาติของสิทธินั้นเท่านั้น[14]

แต่อย่างไรก็ตาม สิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคลนั้นมิใช่สิทธิเด็ดขาด อาจมีบางกรณีที่รัฐสามารถกำหนดมาตรการหรือกระทำการบางอย่างอันมีผลเป็นการแทรกแซงสิทธิในข้อมูลส่วนบุคคลได้เช่นกัน โดยรัฐจะแทรกแซงสิทธิของบุคคลได้ก็ต่อเมื่อมีการปฏิบัติตามเงื่อนไขที่กำหนดไว้ในกฎหมายหรือกฎเกณฑ์ระหว่างประเทศด้านสิทธิมนุษยชนอย่างเคร่งครัด ซึ่งตั้งอยู่บนหลักการพื้นฐานสำคัญ 3 ประการคือ หลักความ

---

[13] *Directive* (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive).

[14] Orla Lynskey, *The Foundations of EU Data Protection Law (Oxford Studies in European Law)* (1st edn, OUP 2016) 14-44.

จำเป็นและความได้สัดส่วน (Necessity and Proportionality) หลักความโปร่งใส (Transparency) และหลักประโยชน์สาธารณะ (Public Interest)[15]

เนื่องจากข้อมูลส่วนบุคคลถือเป็นปัจจัยสำคัญในการขับเคลื่อนและพัฒนาทั้งทางด้านเศรษฐกิจและสังคม ประเทศต่าง ๆ จึงให้ความสำคัญกับการกำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคลโดยนำแนวคิดและหลักการทั่วไปสำหรับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งแนวทางในระดับระหว่างประเทศที่กำหนดขึ้นโดยองค์กรต่างๆ เช่น องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organisation for Economic Co-Operation and Development หรือ OECD) มาใช้เป็นแนวทางในการกำหนดกฎเกณฑ์และบัญญัติกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

แนวทางในการคุ้มครองความเป็นส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ (Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data) ขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD)[16] มีสาระสำคัญ คือ การกำหนดแนวทางทั่วไปที่เกี่ยวข้องกับการเก็บรวบรวม การบริหารจัดการข้อมูลส่วนบุคคลในระดับระหว่างประเทศ เพื่อทำหน้าที่ในการช่วยเหลือรัฐบาล ภาคธุรกิจ และผู้บริโภคในการคุ้มครองสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และในขณะเดียวกันก็เป็นการลดข้อจำกัดของการโอนข้อมูลระหว่างประเทศซึ่งอยู่ในรูปแบบ Online และ Offline โดยแนวทางดังกล่าวอยู่ภายใต้หลักการสำคัญ 8 ประการ ดังนี้

1) ข้อ 7 “หลักข้อจำกัดในการเก็บรวบรวมข้อมูล” (Collection Limitation Principle) : ควรมีการจำกัดการเก็บรวบรวมข้อมูลส่วนบุคคล โดยการเก็บรวบรวมข้อมูลนั้นต้องชอบด้วยกฎหมายและต้องใช้วิธีการที่เป็นธรรมและเหมาะสม ซึ่งในการเก็บรวบรวมข้อมูลนั้นจะต้องให้เจ้าของข้อมูลรู้เห็น รับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูล

2) ข้อ 8 “หลักคุณภาพของข้อมูล” (Data Quality Principle) : ข้อมูลที่เก็บรวบรวมจะต้องเกี่ยวข้องกับวัตถุประสงค์ของการใช้ข้อมูล และภายในขอบเขตเท่าที่จำเป็นสำหรับวัตถุประสงค์ดังกล่าว และจำเป็นต้องถูกต้อง สมบูรณ์ หรือทำให้เป็นปัจจุบันอยู่เสมอ

3) ข้อ 9 “หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ” (Purpose Specification Principle): ควรกำหนดวัตถุประสงค์ของการเก็บรวบรวมข้อมูลให้ชัดเจนก่อนการดำเนินการ และต้องใช้ข้อมูลนั้นอย่างจำกัดเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวหรือวัตถุประสงค์อื่นๆ ที่ไม่ขัดแย้งกัน

---

[15] Peter Carey, ‘Data Protection Principles’ in Peter Carey (edn), *Data Protection : A Practical Guide to UK and EU Law* (5 th, OUP 2018) 32-41.

[16] Organisation for Economic Co-Operation and Development (OECD), ‘Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data’ (Adopted on 23 September 1980).

4) ข้อ 10 “หลักข้อจำกัดในการนำไปใช้” (Use Limitation Principle) : ข้อมูลส่วนบุคคลจะต้องไม่ถูกเปิดเผย ทำให้ปรากฏเป็นการทั่วไป และไม่ถูกใช้เพื่อวัตถุประสงค์อื่นใดที่นอกเหนือไปจากที่กำหนดไว้ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

5) ข้อ 11 หลักการรักษาความปลอดภัยข้อมูล (Security Safeguards Principle) : ข้อมูลส่วนบุคคลควรได้รับการคุ้มครองโดยการมาตรการในการรักษาความปลอดภัยที่เป็นเหตุเป็นผล เพื่อป้องกันความเสี่ยงภัยใดๆ ที่อาจจะทำให้ข้อมูลนั้นสูญหาย หรือมีการเข้าถึง ทำลาย ใช้ ดัดแปลงแก้ไข หรือเปิดเผยโดยมิชอบ

6) ข้อ 12 หลักการเปิดเผยข้อมูล (Openness Principle) : ควรมีการประกาศนโยบายทั่วไปให้ทราบโดยทั่วกัน หากมีการปรับปรุงแก้ไขหรือพัฒนาแนวนโยบายหรือแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคล ก็ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้ข้อมูลใดๆ ที่สามารถระบุเกี่ยวกับหน่วยงานของรัฐผู้ให้บริการที่อยู่ผู้ควบคุมข้อมูลส่วนบุคคลด้วย

7) ข้อ 13 หลักการมีส่วนร่วมของบุคคล (Individual Participation Principle) : เจ้าของข้อมูลควรมีสิทธิได้รับแจ้งหรือยืนยันจากผู้ควบคุมข้อมูลว่ามีการเก็บรวบรวมข้อมูลที่เกี่ยวกับตนไว้ โดยควรแจ้งภายในระยะเวลาที่เหมาะสม ในลักษณะที่เหมาะสม ในรูปแบบที่เจ้าของข้อมูลสามารถเข้าใจได้ง่าย

8) ข้อ 14 หลักความรับผิดชอบ (Accountability Principle) : ผู้ควบคุมข้อมูลควรมีความรับผิดชอบในการปฏิบัติตามมาตรการต่างๆ เพื่อให้เป็นไปตามหลักการข้อ 1- 7 ข้างต้น[17]

ในสหภาพยุโรป ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลเป็นสิทธิขั้นพื้นฐานที่สำคัญของพลเมืองทุกคนซึ่งได้รับการรับรองและคุ้มครองโดยกฎหมาย ดังจะเห็นได้จาก มาตรา 8 ของอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention on Human Rights)[18] ซึ่งกำหนดไว้ว่า

“1. ทุกคนมีสิทธิที่จะได้รับการเคารพในสิทธิความเป็นส่วนตัวและชีวิตครอบครัว ที่อยู่อาศัยและสถานที่ที่ติดต่อได้

2. การเข้าแทรกแซงสิทธิดังกล่าวโดยการใช้อำนาจของพนักงานเจ้าหน้าที่นั้น ไม่สามารถกระทำได้ เว้นแต่จะเป็นไปตามที่กฎหมายกำหนดไว้ หรือมีความจำเป็นสำคัญต่อสังคมแบบประชาธิปไตย ต่อผลประโยชน์ของความมั่งคงของประเทศ ความปลอดภัยของสังคมและระบบเศรษฐกิจของประเทศ หรือเพื่อเป็นการป้องกันอาชญากรรม คุ้มครองสุขภาพหรือศีลธรรม หรือสำหรับการคุ้มครองสิทธิและความเป็นอิสระของผู้อื่น”

---

[17] Ibid Part Two: Basic Principles of National Application.

[18] European Convention on Human Rights (came into force on 3 September 1953).

นอกจากนั้น สิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคล (the right to the protection of personal data) ยังได้รับการรับรองและคุ้มครองตามกฎบัตรว่าด้วยสิทธิขั้นพื้นฐานของสหภาพยุโรป (The Charter on Fundamental Rights of the European Union)[19] ซึ่งมาตรา 8 กำหนดไว้ ดังต่อไปนี้

"1. บุคคลมีสิทธิได้รับความคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับตนเอง

2. ข้อมูลดังกล่าวจะต้องถูกประมวลผลอย่างเป็นธรรม สำหรับวัตถุประสงค์ที่เฉพาะเจาะจงและอยู่บนพื้นฐานความยินยอมของบุคคลที่เกี่ยวข้องและอยู่บนหลักการของความชอบด้วยกฎหมายตามที่กฎหมายได้กำหนดไว้ และทุกคนมีสิทธิที่จะเข้าถึงข้อมูลที่ถูกจัดเก็บไว้ซึ่งมีความเกี่ยวข้องกับตนเอง และมีสิทธิที่จะขอแก้ไขข้อมูลดังกล่าวให้ถูกต้อง

3. การปฏิบัติตามหลักเกณฑ์ทั้งหลายเหล่านี้อยู่ภายใต้การควบคุมของเจ้าหน้าที่ที่มีความเป็นอิสระ"

ทั้งนี้ เพื่อเป็นการปฏิบัติตามหลักเกณฑ์ดังกล่าวข้างต้น สหภาพยุโรปจึงได้มีการบัญญัติกฎหมายที่กำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล ซึ่งกฎหมายที่บังคับใช้อยู่ในปัจจุบัน คือ ข้อบังคับทั่วไปเกี่ยวกับการคุ้มครองข้อมูล หรือที่เรียกว่า General Data Protection Regulation (GDPR) ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 25 พฤษภาคม 2561 เป็นต้นมา[20]

วัตถุประสงค์ของ GDPR คือ เพื่อกำหนดกฎที่เกี่ยวข้องกับการคุ้มครองบุคคลธรรมดาในประเด็นที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลและกฎที่เกี่ยวข้องกับการเคลื่อนไหวอย่างเป็นอิสระของข้อมูล ทั้งนี้ เพื่อคุ้มครองสิทธิเสรีภาพขั้นพื้นฐานของบุคคลธรรมดาและโดยเฉพาะอย่างยิ่งสิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งเพื่อสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกในสหภาพยุโรปให้มีมาตรฐานเดียวกัน และในขณะเดียวกันก็เพื่อลดอุปสรรคในการดำเนินธุรกิจ โดยกฎหมายฉบับนี้จะเป็นเครื่องมือในการสนับสนุนให้เกิดการเคลื่อนไหวของข้อมูลส่วนบุคคลได้อย่างอิสระในสหภาพยุโรป[21]

สาระสำคัญของ GPDR คือ กำหนดหลักเกณฑ์และเงื่อนไขในการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย รวมทั้งกำหนดภาระหน้าที่ของผู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ทั้งนี้ เพื่อให้บรรลุวัตถุประสงค์ในการคุ้มครองสิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคลซึ่งมีความเชื่อมโยงกันอย่างใกล้ชิดกับสิทธิความเป็นส่วนตัวในฐานะเป็นสิทธิขั้นพื้นฐานของพลเมืองทุกคนที่ได้รับการรับรองโดยอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention on Human Rights)

GDPR ให้ความคุ้มครองข้อมูลส่วนบุคคล 2 ประเภทดังนี้

---

[19] Charter on Fundamental Rights of the European Union (came into force in December 2009).

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)).

[21] GDPR, Article 1.

1) “ข้อมูลส่วนบุคคล” หมายถึง “ข้อมูลที่สามารถระบุตัวบุคคลได้ไม่ว่าโดยทางตรงหรือทางอ้อม ยกตัวอย่างเช่น ชื่อ นามสกุล เลขประจำตัวประชาชน ข้อมูลที่แสดงถึงสถานที่ตั้ง หรือข้อมูลใดๆ ที่แสดงถึงลักษณะทางกายภาพ ทางชีวภาพ ทางกรรมพันธุ์ ทางจิตใจ ทางเศรษฐกิจ ทางวัฒนธรรม หรืออัตลักษณ์ทางสังคมของบุคคลดังกล่าว”[22]

2) “ข้อมูลส่วนบุคคลชนิดพิเศษ” หมายถึง “ข้อมูลส่วนบุคคลที่เปิดเผยต้นกำเนิดทางเชื้อชาติและชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา หรือปรัชญา หรือการเป็นสมาชิกสหภาพวิชาชีพ และการประมวลผลข้อมูลพันธุกรรม ข้อมูลชีวมาตราเพื่อวัตถุประสงค์ในการระบุอัตลักษณ์ของบุคคลธรรมดาอย่างเฉพาะเจาะจง ข้อมูลเกี่ยวข้องกับสุขภาพ ข้อมูลเกี่ยวกับชีวิตทางเพศหรือวิถีทางเพศของบุคคลธรรมดา”[23]

GDPR กำหนดสถานะของผู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ไว้ 2 สถานะ ดังนี้

1) ผู้ควบคุมข้อมูล (data controller) หมายถึง “บุคคลธรรมดาหรือนิติบุคคล หน่วยงานสาธารณะ หน่วยงาน หรือองค์กรอื่นใดที่กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล ไม่ว่าโดยลำพังหรือร่วมกัน”[24]

2) ผู้ประมวลผลข้อมูล (data processor) หมายถึง “บุคคลธรรมดาหรือนิติบุคคล หน่วยงานสาธารณะ หน่วยงาน หรือองค์กรอื่นใดที่ประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูล”[25]

ทั้งนี้ เพื่อเป็นการทำให้แน่ใจว่าจะมีการปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้อย่างถูกต้องและครบถ้วน GDPR กำหนดภาระหน้าที่ให้ผู้ควบคุมและผู้ประมวลผลที่จะต้องปฏิบัติตามหลักเกณฑ์ของกฎหมายในเรื่องของการหลักการในการประมวลผลข้อมูลส่วนบุคคล และจะต้องเป็นการประมวลผลข้อมูลบุคคลภายใต้เงื่อนไขที่กฎหมายกำหนดไว้ รวมทั้งจะต้องสามารถแสดงให้เห็นได้ว่ามีการปฏิบัติตามกฎหมายแล้ว

สำหรับแนวคิดพื้นฐานของหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งอยู่เบื้องหลังหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่ GDPR กำหนดไว้ให้เป็นหน้าที่ของผู้ควบคุมและผู้ประมวลผลข้อมูลจะต้องปฏิบัติตามนั้น ปรากฏอยู่ใน GDPR มาตรา 5 เรื่องหลักการที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล อันเป็นพื้นฐานสำคัญสำหรับแนวทางปฏิบัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่ดี ซึ่งมีรายละเอียดดังนี้

1) หลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (Lawfulness, Fairness and Transparency) กล่าวคือ ข้อมูลส่วนบุคคลต้องถูกประมวลผลโดยชอบด้วยกฎหมาย เป็นธรรม และในรูปแบบที่โปร่งใสต่อเจ้าของข้อมูลส่วนบุคคล[26]

---

[22] GDPR, Article 4 (1).

[23] GDPR, Article 9.

[24] GDPR, Article 4(7).

[25] GDPR, Article 4(8).

[26] GDPR, Article 5(1)(a).

2) หลักการจำกัดวัตถุประสงค์ (Purpose Limitation) กล่าวคือ ข้อมูลส่วนบุคคลต้องถูกเก็บรวบรวมสำหรับวัตถุประสงค์ที่ระบุไว้โดยเฉพาะเจาะจงอย่างชัดเจนและชอบด้วยกฎหมายและไม่ได้ถูกประมวลผลในลักษณะที่ขัดกับวัตถุประสงค์ในการเก็บรวบรวม โดยที่การประมวลผลข้อมูลส่วนบุคคลที่มีวัตถุประสงค์ในการเก็บรวบรวมเพื่อประโยชน์สาธารณะ เพื่อการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติตามมาตรา 89 (1) ไม่ถือว่าขัดกับวัตถุประสงค์ในการเก็บรวบรวมแต่แรก[27]

3) หลักน้อยที่สุดเท่าที่จำเป็น (Data Minimization) กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลจะต้องทำเท่าที่เพียงพอ เท่าที่เกี่ยวข้องและจำกัดเฉพาะเท่าที่จำเป็นภายในกรอบวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลเท่านั้น[28]

4) หลักความถูกต้องของข้อมูล (Accuracy) กล่าวคือ จะต้องประมวลผลข้อมูลส่วนบุคคลที่มีความถูกต้องและในกรณีที่จำเป็นจะได้รับการแก้ไขให้เป็นปัจจุบันอยู่เสมอ และในทุกขั้นตอนของการประมวลผลจะต้องทำให้มั่นใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้อง (เมื่อพิจารณาจากวัตถุประสงค์ของการประมวลผลข้อมูลดังกล่าวแล้ว) จะถูกลบหรือแก้ไขโดยไม่ชักช้า[29]

5) หลักการจำกัดการจัดเก็บข้อมูล (Storage Limitation) กล่าวคือ ข้อมูลส่วนบุคคลจะต้องถูกเก็บไว้ในรูปแบบที่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลในเวลาไม่เกินความจำเป็นสำหรับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลอาจถูกเก็บไว้เป็นระยะเวลานานกว่านั้นเฉพาะกรณีที่ข้อมูลส่วนบุคคลถูกประมวลผลสำหรับวัตถุประสงค์ในการเก็บรวบรวมเพื่อประโยชน์สาธารณะ การวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ หรือทางสถิติตามมาตรา 89 (1) ภายใต้การดำเนินงานตามความเหมาะสมทางเทคนิคและมาตรการเกี่ยวกับองค์กรที่จำเป็นตามกฎข้อบังคับนี้เพื่อปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล[30]

6) หลักความสมบูรณ์และการรักษาความลับ (Integrity and Confidentiality (Security)) กล่าวคือ การประมวลผลข้อมูลจะต้องดำเนินการในลักษณะของการสร้างความมั่นใจในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม รวมทั้งการป้องกันการประมวลผลข้อมูลส่วนบุคคลที่ไม่ได้รับอนุญาตหรือผิดกฎหมาย และการป้องกันความสูญเสียจากอุบัติเหตุ การถูกทำให้เสียหายหรือถูกทำลาย โดยการใช้มาตรการด้านเทคนิคหรือมาตรการขององค์กรที่เหมาะสม[31]

---

[27] GDPR, Article 5(1)(b).

[28] GDPR, Article 5(1)(c).

[29] GDPR, Article 5(1)(d).

[30] GDPR, Article 5(1)(e).

[31] GDPR, Article 5(1)(f).

7) หลักความรับผิดชอบ (Accountability) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีความรับผิดชอบในการปฏิบัติตามหลักเกณฑ์ของกฎหมาย และสามารถแสดงให้เห็นได้ว่ามีการปฏิบัติตามหลักเกณฑ์ทั้ง 6 ประการข้างต้นแล้ว[32]

นอกจากนั้น เนื่องจาก GDPR มีผลใช้บังคับแก่การประมวลผลข้อมูลส่วนบุคคลโดยใช้ระบบอัตโนมัติ ซึ่งก็คือการใช้เทคโนโลยีในการช่วยเหลือให้เกิดการประมวลผลข้อมูลส่วนบุคคล ดังนั้น มาตรการทางด้านเทคโนโลยีจึงถือเป็นเครื่องมือสำคัญที่ GDPR ให้ความสำคัญในฐานะเป็นเครื่องมือที่สามารถนำมาใช้ในการรักษาความมั่นคงความปลอดภัยของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันมิให้เกิดการละเมิดข้อมูลส่วนบุคคลในรูปแบบต่างๆ ได้ เช่น การทำให้เสียหาย การทำลาย การเข้าถึงโดยมิชอบ ฯลฯ ในกรณีนี้ ในส่วนที่ 2 ของ GDPR กำหนดหลักเกณฑ์เรื่องความปลอดภัยของข้อมูลไว้ โดยมาตรา 32 กำหนดเรื่องความปลอดภัยในการประมวลผลข้อมูลไว้ว่า

“1. ผู้ควบคุมและผู้ประมวลผลจะต้องกำหนดให้มีมาตรการทางเทคนิคและมาตรการขององค์กรตามสมควรเพื่อรับประกันถึงระดับของความปลอดภัยที่เหมาะสมกับความเสี่ยง โดยพิจารณาโดยละเอียดร่วมกับระดับเทคโนโลยีล่าสุด ค่าใช้จ่ายในการนำไปปฏิบัติและธรรมชาติ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผลเช่นเดียวกับแนวโน้มที่จะเกิดและความรุนแรงในระดับต่างๆ ของความเสี่ยงต่อสิทธิเสรีภาพของบุคคลธรรมดาโดยถือว่ามาตราการดังต่อไปนี้นั้นเป็นไปตามสมควร

(a) การปกปิดอัตลักษณ์และการเข้ารหัสข้อมูลส่วนบุคคล

(b) ความสามารถในการรับประกันถึงการเป็นความลับ ความสมบูรณ์ การเข้าถึงได้ และความสามารถในการรับมือต่อเหตุต่างๆ ดังที่เป็นอยู่ของระบบและการบริการ

(c) ความสามารถในการกู้คืนการเข้าถึงได้ และการเข้าถึงข้อมูลส่วนบุคคล ด้วยวิธีการทันท่วงทีในกรณีที่เกิดเหตุ ไม่ว่าจะเป็นทางเทคนิคหรือทางกายภาพ

(d) กระบวนการสำหรับทดสอบ ประเมินสถานการณ์และประเมินประสิทธิภาพของมาตรการทางเทคนิค และการจัดการองค์กรอย่างสม่ำเสมอเพื่อรับประกันความปลอดภัยของการประมวลผล

2. ในการประเมินสถานการณ์เกี่ยวกับระดับความปลอดภัยที่เหมาะสมควรพิจารณาร่วมโดยรายละเอียดกับความเสี่ยงบางประการโดยเฉพาะที่ปรากฏขึ้นจากการประมวลผล โดยเฉพาะอย่างยิ่งจากการทำลายโดยอุบัติเหตุหรือที่ไม่ชอบด้วยกฎหมาย ความเสียหาย การเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึงข้อมูลส่วนบุคคลที่ถูกถ่ายทอด เก็บรักษา หรือด้วยวิธีอื่นใด โดยไม่มีอำนาจ”[33]

ทั้งนี้ เพื่อให้การบังคับใช้กฎหมายมีประสิทธิภาพ GDPR จึงกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่ฝ่าฝืนไม่ปฏิบัติตามภาระหน้าที่ตามหลักเกณฑ์ที่ GDPR กำหนดไว้ จะต้องรับผิด

---

[32] GDPR, Article 5(2).

[33] GDPR, Article 32.

โดยการถูกปรับตามจำนวนที่พนักงานเจ้าหน้าที่กำหนด และหากการไม่ปฏิบัติตามกฎหมายดังกล่าวก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ก็จะมีความรับผิดต้องชดใช้ค่าเสียหายตามมูลค่าที่เสียหายจริงให้กับเจ้าของข้อมูลส่วนบุคคล[34]

4. บทวิเคราะห์ความสัมพันธ์ระหว่างความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ในขณะที่เทคโนโลยีได้รับการพัฒนาให้เจริญก้าวหน้าขึ้นในทุกๆปี อัตราของประชาชนที่ใช้งานเทคโนโลยีก็มีจำนวนที่เพิ่มมากขึ้น และด้วยเหตุที่เทคโนโลยีได้รับการพัฒนาเพื่ออำนวยความสะดวกสำหรับการดำเนินกิจกรรมในชีวิตประจำวันของประชาชนในหลากหลายกิจกรรม เช่น การทำธุรกรรมทางการเงินผ่านธนาคารด้วยระบบ mobile banking การจองตั๋วเครื่องบินโดยสารผ่าน website การสั่งอาหารผ่าน online application ซึ่งในขั้นตอนของการเริ่มใช้งาน ระบบจะบังคับให้ต้องมีการลงทะเบียน โดยการกรอกข้อมูลส่วนบุคคลของผู้ใช้บริการเพื่อเป็นการยืนยันตัวตนก่อนการใช้บริการ และหากจะต้องมีการชำระค่าบริการ ก็จะต้องมีการกรอกข้อมูลที่ใช้สำหรับการธุรกรรมทางการเงิน เช่น เลขบัตรเครดิต บัตร เดบิต ฯลฯ จากข้อเท็จจริงเหล่านี้จึงทำให้ข้อมูลส่วนบุคคลของประชาชนอยู่ในความครอบครองของผู้ให้บริการเทคโนโลยีเป็นจำนวนมาก

จากสถานการณ์ข้างต้นจึงทำให้อาชญากรให้ความสนใจและมองเห็นช่องทางในการกระทำความผิดในรูปแบบที่หลากหลาย เช่น การเจาะระบบคอมพิวเตอร์เพื่อนำข้อมูลไปขาย หรือการทำให้เสียหาย การแก้ไขเปลี่ยนแปลงข้อมูลในระบบคอมพิวเตอร์ เหล่านี้จึงส่งผลให้ในหลายปีที่ผ่านมา อัตราการเกิดขึ้นของการโจมตีทางไซเบอร์มีจำนวนเพิ่มมากขึ้นรวมทั้งลักษณะและรูปแบบของการโจมตีมีความหลากหลายและซับซ้อนมากยิ่งขึ้น ซึ่งส่งผลกระทบในลักษณะที่ก่อให้เกิดความเสียหายต่อทั้งภาครัฐ ภาครัฐวิสาหกิจ ภาคเอกชน และประชาชนทั่วไป ดังนั้น ความปลอดภัยไซเบอร์จึงเป็นประเด็นสำคัญที่ได้รับความสนใจจากสังคมเพิ่มมากขึ้นเรื่อยๆ ทั้งจากผู้กำหนดนโยบายขององค์กรภาครัฐและภาครัฐวิสาหกิจ เจ้าของกิจการในองค์กรภาคเอกชน นักวิชาการ และประชาชนทั่วไป[35]

ตัวอย่างสถานการณ์การโจมตีทางไซเบอร์ในประเทศไทย เช่น ในเดือนมีนาคม พ.ศ. 2566 ตำรวจสอบสวนกลาง ได้รับเรื่องร้องทุกข์กรณีบริษัทพาวเวอร์ไทเทเนียม ร่วมกับบริษัททรูมันนี่จัดแคมเปญนำรหัสใต้ฝาเครื่องดื่มพาวเวอร์ไทเทเนียมวิตามินมาแลกรับเงินสดผ่านระบบทรูมันนี่วอเลท โดย 1 รหัสใต้ฝา สามารถนำมาแลกเป็นเงินในระบบทรูมันนี่ได้ 10 บาท ต่อมา บริษัททรูมันนี่ได้ตรวจพบแล้วว่ามีการใช้งานระบบ

---

[34] GDPR, Article 77-84.

[35] Tims Rains and Timothy Youngblood CISSP, *Cybersecurity Threats, Malware Trends, and Strategies: Discover Risk Mitigation Strategies for Modern Threats to your Organization* (2nd edn, Packt Publishing 2023) 23-42.

แม่ข่ายหรือเซิร์ฟเวอร์ของบริษัทมากจนทำให้ระบบการประมวลผลทำงานได้ช้าลงอย่างมาก และไม่สามารถเข้าใช้งานได้ตามปกติ และเมื่อเจ้าหน้าที่ของบริษัทฯ ได้ตรวจสอบโดยละเอียด จึงพบว่าในช่วงวันที่ 11-13 ธันวาคม พ.ศ. 2565 มีคนร้ายโจมตีระบบข้อมูลมากกว่า 300,000 ครั้ง อย่างต่อเนื่อง จึงเป็นเหตุให้ระบบทำงานช้าลง นอกจากนั้น คนร้ายยังสามารถ hack code รหัสแลกรางวัลได้มากกว่า 6,000 code เพื่อนำไปแลกเป็นเงินสด สรุปเป็นเงินจำนวนประมาณ 60,000 บาทได้อีกด้วย [36]

จากสถานการณ์การโจมตีทางไซเบอร์ที่เกิดขึ้น จึงสามารถพิจารณาได้ว่าแนวคิดเรื่องความปลอดภัยไซเบอร์นั้นมีความเกี่ยวข้องโดยตรงต่อหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งมุ่งคุ้มครองสิทธิความเป็นตัวและสิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นสิทธิขั้นพื้นฐานของประชาชนทุกคนในสังคม แต่อย่างไรก็ตามความสัมพันธ์ระหว่างแนวคิดเรื่องความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลค่อนข้างมีความซับซ้อน การสร้างความปลอดภัยไซเบอร์อาจก่อให้เกิดประเด็นความท้าทายในการคุ้มครองข้อมูลส่วนบุคคล[37] ดังนั้น ผู้เขียนจึงมุ่งศึกษาวิเคราะห์ความสัมพันธ์ระหว่างแนวคิดในเรื่องความความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยแบ่งเป็น 2 กรณี ดังต่อไปนี้

1. ความสัมพันธ์ในกรณีส่งผลกระทบทางบวก

หากพิจารณาแนวคิดเรื่องความปลอดภัยไซเบอร์กับแนวคิดตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามที่ได้กล่าวมาในหัวข้อที่ 2 และ 3 แล้วจะพบว่ามีสาระสำคัญของแนวคิดที่ค่อนข้างคล้ายคลึงเชื่อมโยงไปในทิศทางเดียวกัน กล่าวคือ การที่องค์กรสามารถกำหนดนโยบายและมาตรการในการป้องกันเหตุการณ์ภัยคุกคามไซเบอร์เพื่อสร้างความปลอดภัยไซเบอร์ได้มีประสิทธิภาพมากเท่าใด ก็จะส่งผลดีต่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและการคุ้มครองสิทธิที่จะได้รับการคุ้มครองข้อมูลของเจ้าของข้อมูลส่วนบุคคลมากเท่านั้น

แนวคิดของการคุ้มครองข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล ถือเป็นหลักการสำคัญประการหนึ่งในการสร้างความปลอดภัยไซเบอร์ โดยแนวคิดดังกล่าวจะเป็นตัวช่วยในการพิจารณาเพื่อกำหนดนโยบายและจัดหามาตรการที่เหมาะสมที่จะนำมาใช้ในการป้องกันและปราบปรามภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ ที่ส่งผลกระทบต่อความปลอดภัยไซเบอร์และก่อให้เกิดความเสียหายต่อข้อมูลส่วนบุคคลที่อยู่ในระบบต่อไป รวมทั้งพิจารณาจัดทำกลยุทธ์ในแผนการบริหารความเสี่ยงเกี่ยวกับความปลอดภัยไซเบอร์ และพัฒนาทักษะของพนักงานให้สามารถปรับใช้

---

[36] ‘จับ 2 แฮกเกอร์หนุ่ม เจาะระบบขโมยข้อมูล’ (สำนักข่าวไทย, 23 มีนาคม 2566) <https://tna.mcot.net/crime-1140181> สืบค้นวันที่ 1 มีนาคม 2566.

[37] Muharman Lubis and Dini Oktarina D. Handayani, ‘The Relationship of Personal Data Protection Towards Internet Addiction : Cyber Crimes, Pornography and Reduced Physical Activity’ (2022) 197 Procedia Computer Science 151, 151-160.

มาตรการต่างๆ ในการสร้างความปลอดภัยไซเบอร์ในลักษณะที่เหมาะสมและไม่เป็นการละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล[38]

ในขณะเดียวกันหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลก็ให้ความสำคัญกับแนวคิดในเรื่องการสร้างความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในฐานะที่เป็นมาตรการหนึ่งในการคุ้มครองสิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ซึ่งจะเห็นได้อย่างชัดเจนว่า GDPR มาตรา 24 กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลมีหน้าที่ในการจัดหามาตรการทางเทคนิคและมาตรการขององค์กรที่เหมาะสมเพื่อที่จะทำให้แน่ใจได้ว่ามีการปฏิบัติตามกฎหมายอย่างถูกต้องและครบถ้วน มาตรการในการสร้างความปลอดภัยไซเบอร์จึงถือว่าเป็นเครื่องมือที่ดีในการรักษาความปลอดภัยของข้อมูลและคุ้มครองสิทธิของเจ้าของของข้อมูลส่วนบุคคล[39]

ดังนั้นจึงอาจกล่าวได้ว่า แนวคิดในเรื่องความปลอดภัยไซเบอร์มีความสัมพันธ์อย่างใกล้ชิดและส่งผลกระทบโดยตรงต่อหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล มาตรการที่ใช้ในการรักษาความปลอดภัยไซเบอร์ที่ดีก็สามารถส่งผลดีต่อการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลด้วย ในขณะเดียวกันหากไม่มีความปลอดภัยไซเบอร์ การคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวเนื่องกับการประมวลผลข้อมูลผ่านระบบเทคโนโลยีสารสนเทศต่างๆ ก็อาจเป็นไปได้ยากหรือเป็นไปไม่ได้เลย

2. ความสัมพันธ์ในกรณีส่งผลกระทบทางลบ

หากพิจารณาตามความเข้าใจโดยทั่วไปแล้ว ทุกคนต่างยอมรับว่าระดับของความปลอดภัยไซเบอร์ส่งผลต่อระดับของความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และระดับความเข้มแข็งในการให้ความคุ้มครองสิทธิที่จะได้รับการคุ้มครองข้อมูลของเจ้าของข้อมูลส่วนบุคคล ซึ่งเหล่านี้ถือเป็นความสัมพันธ์ระหว่างแนวคิดในเรื่องความความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลในลักษณะที่ส่งผลกระทบทางบวก

อย่างไรก็ตาม หากพิจารณาทฤษฎีอันเป็นรากฐานสำคัญของแนวคิดในเรื่องความความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว ก็จะพบว่ามีความแตกต่างในเชิงหลักการบางประการ กล่าวคือ หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลถูกบัญญัติขึ้นมาเพื่อวัตถุประสงค์ในการรับรองและคุ้มครองของสิทธิความเป็นตัวและสิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิที่ติดตัวมนุษย์มาตั้งแต่กำเนิดจึงถือเป็นสิทธิมนุษยชนขั้นพื้นฐานที่กฎหมายระดับระหว่างประเทศให้

---

[38] Sylvia Kierkegaard, 'Cybercrime Convention: Narrowing the Cultural and Privacy Gap?' (2007) 1(1) International Journal of Intercultural: Information Management 17, 18-30.

[39] Derek E. Bambauer, 'Privacy versus Security' (2013) 103(3) *Journal of Criminal Law and Criminology* 667, 683.

ความสำคัญในการรับรองสิทธิดังกล่าว แต่ในเรื่องความปลอดภัยไซเบอร์นั้นเกิดขึ้นจากการที่รัฐกำหนดกฎหมายขึ้นมาเพื่อป้องกันและปรามปรามภัยคุกคามต่างๆ ที่ส่งผลกระทบต่อความปลอดภัยไซเบอร์ ซึ่งเป็นเรื่องที่กระทบต่อความสงบสุขของสังคม

ดังนั้นแม้ทั้งสองแนวคิดจะให้ความสำคัญในสิ่งที่ดูเหมือนจะคล้ายกันและมีความเชื่อมโยงกันก็ตาม แต่หากพิจารณาในรายละเอียดแล้ว ก็จะพบว่ามีความแตกต่างกันในส่วนของวัตถุประสงค์พื้นฐานในเชิงทฤษฎีเหล่านี้จึงส่งผลให้องค์กรจะต้องมีความระมัดระวังในการกำหนดมาตรการที่ใช้ในการสร้างความปลอดภัยไซเบอร์และการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งรวมถึงสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล เนื่องจากการเลือกใช้มาตรการทั้งทางด้านเทคนิคและมาตรการขององค์กรบางประการอาจจะเป็นการขัดหรือแย้งหรือส่งผลกระทบทางลบต่อวัตถุประสงค์หลักของแนวคิดอีกเรื่องหนึ่งได้[40]

ตัวอย่างเช่น กรณีข้อเสนอในการเพิ่มความเข้มแข็งในเรื่องความปลอดภัยไซเบอร์ภายใต้แนวคิดของการยืนยันตัวตนโดยการกำหนดให้ผู้ใช้งานเทคโนโลยีประเภทต่างๆ ใส่ข้อมูลส่วนบุคคลเป็นจำนวนมากทั้งในส่วนของข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ข้อมูลม่านตา ข้อมูลลายนิ้วมือ ข้อมูลภาพสแกนใบหน้าประกอบกับการกรอกข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล เลขบัตรประจำตัวประชาชนเป็นประจำทุกครั้งที่มีการเข้าสู่ระบบการให้บริการทุกประเภท ทั้งนี้ เพื่อเป็นการลดความไม่มีตัวตนในระบบออนไลน์ (reducing online anonymity) หรือกรณีข้อเสนอในการกำหนดนโยบายให้มีการเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่น่าจะมีความเกี่ยวข้องกับการก่อให้เกิดความเสี่ยงต่อความปลอดภัยไซเบอร์ต่อสาธารณชน เพื่อเป็นการแจ้งเตือนหรือป้องปรามมิให้เกิดการกระทำความผิดซึ่งอาจส่งผลให้เกิดความเสียหายได้

จากตัวอย่างข้างต้น แม้มาตรการดังกล่าวจะส่งผลดีต่อความปลอดภัยไซเบอร์ แต่อาจไม่ส่งผลดีต่อแนวคิดและหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งกำหนดหลักเกณฑ์ของการเก็บรวบรวมและการประมวลผลข้อมูลส่วนบุคคลไว้ว่าจะต้องเก็บรวบรวม ใช้ และเปิดเผยเท่าที่จำเป็น โดยการดำเนินการดังกล่าวจะต้องมีความเกี่ยวข้องกับวัตถุประสงค์ที่จะต้องมีการประมวลผลข้อมูลส่วนบุคคลดังกล่าวเท่านั้น หลักเกณฑ์เหล่านี้เป็นไปตามหลักทฤษฎีในเรื่องความได้สัดส่วน (proportionate) และความจำเป็น (necessary) ซึ่งเป็นแนวความคิดตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ดังนั้น การดำเนินการตามข้อเสนอแนะเพื่อสร้างความเข้มแข็งในเรื่องความปลอดภัยไซเบอร์ข้างต้นจึงอาจดูขัดแย้งกับแนวคิดตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล เนื่องจากการเก็บข้อมูลส่วนบุคคลในกิจกรรมดังกล่าวมีลักษณะที่ค่อนข้างเกินไปกว่าความจำเป็นภายใต้ขอบเขตของวัตถุประสงค์ที่จะต้องประมวลผลข้อมูลส่วนบุคคลดังกล่าวนั้น นอกจากนั้น ข้อมูลที่จัดเก็บบางส่วนเป็นข้อมูลส่วนบุคคลชนิดพิเศษหรือข้อมูลอ่อนไหวซึ่งกฎหมายให้ความสำคัญกับความมั่นคงปลอดภัยของข้อมูลประเภทนี้ค่อนข้างมาก

---

[40] Christopher Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey and Christopher Millard, 'The Rise of Cybersecurity and Its Impact on Data Protection' (2017) 7(2) International Data Privacy Law 73, 73-75.

การเก็บรวบรวมข้อมูลส่วนบุคคลในลักษณะดังกล่าวนอกจากเป็นการสร้างภาระทางด้านค่าใช้จ่ายให้กับผู้ควบคุมข้อมูลแลผู้ประมวลผลข้อมูลในการที่จะต้องจัดหามาตรการด้านเทคนิคและมาตรการขององค์กรในการรักษาความมั่นคงปลอดภัยให้กับข้อมูลส่วนบุคคลประเภทดังกล่าวแล้ว ก็ยังเป็นการเพิ่มอัตราความเสี่ยงในส่วนของความรับผิดชอบของผู้ควบคุมข้อมูลและผู้ประมวลข้อมูลที่จะต้องมีความรับผิดและต้องรับโทษตามกฎหมาย ในกรณีที่ข้อมูลดังกล่าวถูกทำละเมิดในรูปแบบต่างๆ เช่น การเข้าถึงโดยมิชอบ การทำให้เสียหาย การทำลาย ฯลฯ [41]

จึงอาจกล่าวได้ว่า มาตรการทั้งทางด้านเทคนิคและมาตรการขององค์กรที่ได้รับการพิจารณาแล้วว่าส่งผลดีและเหมาะสมต่อการสร้างความปลอดภัยไซเบอร์นั้น อาจจะไม่ใช่มาตรการที่ส่งผลดีและเหมาะสมในบริบทของการคุ้มครองข้อมูลส่วนบุคคลตามหลักกฎหมายคุ้มครองข้อมูลส่วนเสมอไป ประเด็นนี้ถือว่ามีความสำคัญที่ทุกองค์กรควรจะต้องตระหนักถึงและควรนำไปใช้ในการพิจารณาเพื่อกำหนดนโยบาย กำหนดมาตรการและวิธีการในการสร้างความปลอดภัยไซเบอร์ในลักษณะที่ไม่ขัดหรือแย้งต่อหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล ต้องพึงตระหนักไว้เสมอว่า การกำหนดมาตรการใดๆ เพื่อประโยชน์ในการรักษาความปลอดภัยไซเบอร์แต่หากมีลักษณะที่ขัดต่อหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล การกระทำดังกล่าวก็อาจจะส่งผลให้องค์กรมีความรับผิดและต้องรับโทษตามกฎหมาย ซึ่งจะส่งผลเสียต่อชื่อเสียงและภาพลักษณ์ขององค์กรต่อไป

5. บทสรุปและข้อเสนอแนะ

ในขณะที่เทคโนโลยีเข้ามามีบทบาทอย่างมากต่อการพัฒนาและอำนวยความสะดวกให้กับทุกภาคส่วนในสังคม ในอีกด้านหนึ่งอาชญากรก็นำเอาเทคโนโลยีไปใช้ในการกระทำความผิดซึ่งสร้างความเสียหายให้กับประชาชน สังคมและประเทศชาติเป็นจำนวนมาก หากพิจารณาจากลักษณะของอาชญากรรมไซเบอร์ที่เกิดขึ้นในคดีต่างๆ ก็จะพบว่าก่อให้เกิดประเด็นพิจารณาทางด้านการคุ้มครองข้อมูลส่วนบุคคลซึ่งส่งผลกระทบต่อสิทธิในการได้รับการคุ้มครองข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัว ซึ่งเป็นเป็นสิทธิมนุษยชนขั้นพื้นฐานของประชาชนทั้งสิ้น

ดังนั้น จึงอาจกล่าวได้ว่า แนวคิดในเรื่องความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีความสัมพันธ์อย่างใกล้ชิดและค่อนข้างมีความซับซ้อนในฐานะที่ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลจะได้รับการคุ้มครองตามกฎหมายหรือไม่ก็จะขึ้นอยู่กับปัจจัยในเรื่องความปลอดภัยไซเบอร์ด้วยเช่นกัน สิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคลจะไม่สามารถได้รับการคุ้มครองได้หากไม่มีมาตรการทางเทคนิคในการรักษาความมั่งคงปลอดภัยไซเบอร์

---

[41] Roslyn Layton and Silvia Elaluf-Calderwood, 'A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices' (12th CMI Conference on Cybersecurity and Privacy, 28-29 November 2019).

ที่เหมาะสม เพียงพอและมีประสิทธิภาพ ซึ่งความสัมพันธ์ดังกล่าวสะท้อนให้เห็นอย่างชัดเจนในแนวคิด ทฤษฎี รวมทั้งหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งกำหนดภาระหน้าที่ของผู้ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลส่วนบุคคลไม่ว่าจะอยู่ในสถานะผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล ให้ต้องกำหนดมาตรการทางเทคนิคและมาตรการขององค์กรที่เหมาะสมในการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อทำให้แน่ใจว่ามีการปฏิบัติตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้อย่างถูกต้องและครบถ้วนแล้ว

นอกจากนั้นแนวคิดในเรื่องความปลอดภัยไซเบอร์ยังส่งผลกระทบโดยตรงต่อการคุ้มครองข้อมูลส่วนบุคคลในแทบจะทุกกรณี เนื่องจากในปัจจุบันการทำงานของเทคโนโลยีประเภทต่างๆ เพื่ออำนวยความสะดวกให้กับประชาชนในสังคมก็จำเป็นที่จะต้องมีการใส่ข้อมูลส่วนบุคคลเข้าสู่ระบบคอมพิวเตอร์ โดยระบบฯ จะดำเนินการประมวลผลข้อมูลเพื่อนำเสนอบริการให้กับผู้ใช้บริการแต่ละคน จึงปฏิเสธไม่ได้ว่าข้อมูลส่วนบุคคลของประชาชนกระจายอยู่ในความครอบครองของผู้ให้บริการเทคโนโลยีต่างๆ มากมาย ดังนั้นในยุคปัจจุบัน การค้นหาแนวทางในการบริหารจัดการความสัมพันธ์ระหว่างแนวคิดในเรื่องของความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงเป็นสิ่งสำคัญและจำเป็นอย่างยิ่งที่จะต้องดำเนินการ ทั้งนี้ เพื่อเป็นการสร้างความปลอดภัยไซเบอร์ และในขณะเดียวกันก็เป็นการให้ความคุ้มครองสิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลด้วย นอกจากนั้นยังส่งผลเป็นการลดความเสี่ยงในกรณีที่องค์กรจะต้องมีความรับผิดตามหลักกฎหมายที่เกี่ยวข้องในฐานะที่ไม่มีการกำหนดมาตรการที่เหมาะสมในสร้างความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

ข้อควรพิจารณาในการกำหนดแนวทางในการบริหารจัดการความสัมพันธ์ระหว่างแนวคิดในเรื่องของความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ แม้ทั้งสองเรื่องจะสามารถเชื่อมโยงกันและส่งผลกระทบในด้านบวกในหลายแง่มุม ตัวอย่างเช่น ในหลายกรณีที่การสร้างความปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลสามารถดำเนินการได้โดยใช้เครื่องมือประเภทเดียวกัน เช่น การเข้ารหัสลับ (encryption) หรือการจำกัดสิทธิการเข้าถึง (access control) ทำให้มองได้ว่ามาตรการที่ดีสำหรับการคุ้มครองความปลอดภัยไซเบอร์ก็จะส่งผลดีต่อการคุ้มครองข้อมูลส่วนบุคคลด้วย

อย่างไรก็ดี จากการศึกษาวิเคราะห์แนวคิดและทฤษฎีเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว พบว่าแนวคิดพื้นฐานในบางส่วนของทั้งสองเรื่องอาจจะไม่ได้สอดคล้องกันทั้งหมด จึงทำให้ทั้งสองเรื่องมีความสัมพันธ์ในกรณีที่สามารถส่งผลกระทบด้านลบต่อกันได้เช่นกัน ตัวอย่างเช่น การใช้มาตรการทางด้านเทคนิคในการสร้างความรัดกุมและเข้มงวดในการเข้าถึงระบบ โดยการบังคับให้ผู้ใช้บริการต้องกรอกข้อมูลส่วนบุคคลเป็นจำนวนมากเพื่อยืนยันตัวตนก่อนเข้าใช้งานระบบ แม้จะเป็นการทำเพื่อวัตถุประสงค์ในการสร้างความปลอดภัยไซเบอร์ แต่อาจไม่ใช่แนวทางที่ดีตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งยึดหลักการในเรื่องของการเก็บรวบรวมข้อมูลเท่าที่เพียงพอและเท่าที่จำเป็นภายใต้วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลนั้นเท่านั้น กล่าวคือ มาตรการทางเทคโนโลยีในการคุ้มครอง

ความปลอดภัยไซเบอร์อาจก่อให้เกิดความเสี่ยงภัยต่อสิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นสิทธิมนุษยชนขั้นพื้นฐานที่ได้รับการคุ้มครองตามกฎหมายได้

จากข้อมูลข้างต้น จึงสามารถสรุปได้ว่า หลักการสำคัญของแนวทางในบริหารจัดการความสัมพันธ์ระหว่างแนวคิดเรื่องความปลอดภัยไซเบอร์ และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล ก็คือ การหาจุดสมดุลและกำหนดมาตรการเพื่อให้เกิดความสมดุลระหว่างความปลอดภัยไซเบอร์และการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อทำให้สามารถผสมผสานแนวคิดของทั้งสองเรื่องในลักษณะที่สามารถนำไปใช้ได้อย่างมีประสิทธิภาพมากที่สุด[42] โดยมีประเด็นที่ต้องพิจารณาเพื่อหาจุดสมดุลดังกล่าวดังนี้

1. ประเด็นพิจารณาในส่วนของการสร้างความปลอดภัยไซเบอร์ในแง่ของความปลอดภัยของข้อมูลนั้นจะประกอบด้วยแนวคิดในเรื่องดังนี้ 1) การรักษาความลับ (Confidentiality) คือ แนวคิดในการรักษาความเป็นส่วนตัวของข้อมูล 2) ความสมบูรณ์ (Integrity) เป็นแนวคิดที่มีความเชื่อมโยงกับความมีอยู่ของการรักษาความลับของข้อมูล ข้อมูลจะต้องได้รับความคุ้มครองต่อการถูกแก้ไขเปลี่ยนแปลงโดยไม่มีอำนาจซึ่งอาจเกิดขึ้นโดยตั้งใจหรือโดยอุบัติเหตุ 3) ความพร้อมใช้งาน (Availability) กล่าวคือ ข้อมูลจะต้องอยู่ในสถานะที่สามารถใช้งานได้ตลอดเมื่อต้องการ[43]

2. ประเด็นพิจารณาในส่วนของหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลจะประกอบด้วยแนวคิดในเรื่องของ 1) หลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (Lawfulness, Fairness and Transparency) 2) หลักการจำกัดวัตถุประสงค์ (Purpose Limitation) 3) หลักน้อยที่สุดเท่าที่จำเป็น (Data Minimization) 4) หลักความถูกต้องของข้อมูล (Accuracy) 5) หลักการจำกัดการจัดเก็บข้อมูล (Storage Limitation) 6) หลักความซื่อสัตย์สุจริตและการรักษาความลับ (Integrity and Confidentiality (Security)) 7) หลักความรับผิดชอบ (Accountability)[44]

ดังนั้น แนวทางในบริหารจัดการความสัมพันธ์ระหว่างแนวคิดเรื่องความปลอดภัยไซเบอร์และหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ดีและเหมาะสมที่สุดนั้นจะต้องเกิดขึ้นจากการพิจารณารายละเอียดในแต่ละบริบทของแต่ละองค์กร เนื่องจากแต่ละองค์กรจะต้องพิจารณาหาความสมดุลโดยคำนึงถึงรายละเ อียดของการประมวลผลข้อมูลส่วนบุคคลและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลที่เกิดขึ้นในแต่ละกิจกรรมในองค์กร เพื่อกำหนดนโยบายที่เหมาะสมกับองค์กรในสร้างความปลอดภัยไซเบอร์และคุ้มครองสิทธิที่ได้รับการคุ้มครองข้อมูลของเจ้าของข้อมูลส่วนบุคคล ในกรณีที่องค์กรใดเห็นว่าควรกำหนดนโยบายในการจัดการกับข้อมูลโดยเน้นไปในทางความปลอดภัยไซเบอร์มากกว่าการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล องค์กรนั้นก็จะต้องจัดเตรียมมาตรการต่างๆ ไว้ให้พร้อมสำหรับการรับมือกับภาระหน้าที่ในการดูแลความมั่งคงปลอดภัยของข้อมูลจำนวนมหาศาลที่อยู่ในความครอบครอง เช่น การใช้มาตรการทางเทคนิคในการจำกัดสิทธิ

---

[42] Maria Grazia Porcedda, 'Data Protection and the Prevention of Cybercrime: The EU as an Area OF Security?' (Working Papers LAW 2012/25, European University Institute, Department of Law, 2012) 67-70.

[43] Anderson Ross, *Security Engineering. A Guide to Building Dependable Distributed Systems*. (Wiley:Indianapolis 2008).

[44] GDPR, Article 24.

การเข้าถึงมาสนับสนุน แต่ในทางตรงกันข้าม หากองค์กรใดเห็นว่าควรกำหนดนโยบายที่เน้นไปในทางของการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล องค์กรดังกล่าวก็จะต้องมีการจัดเตรียมมาตรการสำหรับการรับมือกับช่องโหว่ในระบบที่อาจเกิดขึ้นซึ่งจะนำไปสู่การโจมตีทางไซเบอร์และก่อให้เกิดความเสียหายได้

ในประเด็นของการกำหนดนโยบายที่เหมาะสมเพื่อจะสร้างความปลอดภัยไซเบอร์และคุ้มครองข้อมูลส่วนบุคคลนั้น นักวิชาการหลายท่านพยายามเสนอแนะหลักการพิจารณาเพื่อกำหนดนโยบายดังกล่าว โดยเสนอแนะให้พิจารณาแนวความคิดในเชิงทฤษฎีซึ่งสามารถแยกพิจารณาออกเป็น 2 แนวคิด ดังนี้

1. พิจารณากำหนดนโยบายโดยเน้นการกำหนดบทลงโทษต่อการกระทำที่ก่อให้เกิดหรือส่งผลต่อการเกิดขึ้นของอาชญากรรมทางไซเบอร์และการโจมตีความปลอดภัยไซเบอร์ หรือ

2. พิจารณากำหนดนโยบายโดยเน้นการกำหนดภาระหน้าที่ให้กับผู้เกี่ยวข้องเพื่อป้องกันอาชญากรรมทางคอมพิวเตอร์และสร้างความปลอดภัยไซเบอร์[45]

องค์กรสามารถเลือกกำหนดนโยบายตามแนวคิดใดแนวคิดหนึ่งหรืออาจจะเป็นการผสมผสานระหว่างสองแนวความคิดข้างต้นก็ได้ ภายหลังเมื่อมีการกำหนดนโยบายขององค์กรในการสร้างความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลเรียบร้อยแล้ว การกำหนดมาตรการด้านเทคนิคเพื่อนำมาใช้เป็นเครื่องมือในการปฏิบัติตามนโยบายดังกล่าวก็เป็นเรื่องที่มีความสำคัญที่จะต้องพิจารณา เนื่องจากจะมีความเชื่อมโยงไปยังประเด็นในเรื่องของค่าใช้จ่ายที่องค์กรจะต้องรับภาระและประเด็นเรื่องความเหมาะสมของมาตรการทางด้านเทคนิคกับบริบทการทำงานขององค์กร ซึ่งมีมาตรการหลายอย่างที่องค์กรต่างๆ มักนิยมนำมาใช้ เช่น การยืนยันตัวบุคคล (Authentication) การกำหนดสิทธิ/จำกัดสิทธิในการเข้าถึง (Access Control) การทำข้อมูลให้เป็นนิรนาม (Data Anonymisation) การปกปิดข้อมูลโดยทำให้ข้อมูลนั้นแสดงเป็นข้อมูลหลอกหรือนามแฝงเพื่อปกปิดข้อมูลจริง (Data Masking) การระบุแทนค่าข้อมูลด้วยนามแฝง (Data Pseudonymisation) การแปลงค่าข้อมูล (Encoding) การแปลงค่าข้อมูลโดยมีการกำหนดรหัสในการเข้าถึง (Encryption) การแปลงค่าข้อมูลไปเป็นอีกรูปแบบหนึ่งโดยไม่สามารถแปลงกลับมาเป็นข้อมูลต้นฉบับได้ (Hashing)

ในท้ายสุด สิ่งที่ควรต้องคำนึงถึงคือ เรื่องความรับรู้ (awareness) ของเจ้าของข้อมูลส่วนบุคคล แม้องค์กรจะกำหนดนโยบายและมาตรการต่างๆ ที่ประเมินแล้วว่า เป็นแนวทางที่เหมาะสมกับบริบทขององค์กรในการบริหารจัดการเพื่อสร้างความสมดุลระหว่างแนวคิดเรื่องความปลอดภัยไซเบอร์กับแนวคิดตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้วก็ตาม สิ่งสำคัญที่พึงต้องดำเนินการก่อนการนำเอานโยบายดังกล่าวไปใช้งานคือ การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบและยอมรับก่อน การดำเนินการดังกล่าวถือเป็นเรื่องที่มีความสำคัญและเป็นหน้าที่ตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งกำหนดให้องค์กรในฐานะผู้ควบคุมข้อมูลจะต้องปฏิบัติ โดยองค์กรสามารถแจ้งรายละเอียดของนโยบายดังกล่าวโดยระบุไว้เป็นส่วนหนึ่งของ

---

[45] Cynthia Brumfield and Brain Haugli, *Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework* (1st edition Wiley 2021).

นโยบายความเป็นส่วนตัว (Privacy Notice) ขององค์กรที่จะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่าองค์กรจะใช้มาตรการใดในการรักษาความมั่นคงปลอดภัยของข้อมูลและคุ้มครองสิทธิที่จะได้รับการคุ้มครองข้อมูลของเจ้าของข้อมูลส่วนบุคคล ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่เห็นด้วยหรือไม่ยอมรับ องค์กรจะต้องจัดเตรียมช่องทางที่สะดวกให้กับเจ้าของข้อมูลส่วนบุคคลได้ใช้สิทธิในการยกเลิกความยินยอมที่จะให้องค์กรเก็บรวบรวมหรือประมวลผลข้อมูล รวมทั้งให้ลบข้อมูลหรือระงับการดำเนินการใดๆ กับข้อมูลของตนเองได้ด้วย[46]

[46] Seung-Hun Hong and Mamoun Alazab, 'Cybercrime and Data Breach: Privacy Protection through the Regulation of Voluntary Notification' (Prepared for the Korea Legislation Research Institute (KLRI), Legal Scholar Roundtable, How Law Operates in the Wired Society, Seoul, Korea, 2017).

คำแนะนำในการส่งบทความเพื่อพิจารณาตีพิมพ์ในวารสารกฎหมายนิติพัฒน์ นิด้า

คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์

1. วัตถุประสงค์

วารสารกฎหมายนิติพัฒน์ นิด้า (Nitipat NIDA Law Journal) มีวัตถุประสงค์เพื่อเผยแพร่องค์ความรู้ ผลงานทางวิชาการและผลงานวิจัยทางด้านนิติศาสตร์ รวมถึงกฎหมายเพื่อการพัฒนา สังคมวิทยากฎหมาย นิติเศรษฐศาสตร์ นิติปรัชญาและสาขาอื่นที่เกี่ยวข้องกับกฎหมาย และเพื่อพัฒนาคุณภาพงานตีพิมพ์วารสารให้เป็นไปตามมาตรฐานซึ่งเป็นที่ยอมรับในระดับประเทศและระดับสากล

2. กำหนดการตีพิมพ์

วารสารกฎหมายนิติพัฒน์ นิด้า เป็นวารสารวิชาการซึ่งตีพิมพ์ผลงานวิชาการ ที่เขียนขึ้นโดยบุคลากรทั้งภายในและภายนอกมหาวิทยาลัย โดยจัดพิมพ์ปีละ 2 ฉบับ ทุก 6 เดือน ดังนี้

ฉบับที่ 1/.... เดือนมกราคม - มิถุนายน

ฉบับที่ 2/.... เดือนกรกฎาคม – ธันวาคม

3. คำแนะนำสำหรับผู้เขียน

3.1 ใช้รูปแบบการเขียนและภาษาที่เหมาะสมกับลักษณะของบทความทางวิชาการอันเป็นที่ยอมรับโดยทั่วไป ไม่มีการคัดลอกผลงานของผู้อื่น และมีการตรวจทานต้นฉบับทั้งในส่วนของรูปแบบการเขียน รูปแบบการอ้างอิง การสะกดคำ และไวยากรณ์แล้วเป็นอย่างดี

3.2 จัดพิมพ์บทความด้วยโปรแกรม Microsoft Word โดยใช้ขนาดกระดาษ A4 แบบหน้าเดียว ความยาวไม่เกิน 25 หน้า เว้นระยะห่างจากขอบบน 1 นิ้ว ขอบซ้าย 1 นิ้ว ขอบขวา 1 นิ้ว และขอบล่าง 1 นิ้ว ใช้ตัวอักษร TH SarabunPSK เว้นวรรคบรรทัดเดียว (Single-line spacing) โดยผู้เขียนสามารถใช้แบบฟอร์มของวารสารกฎหมายนิติพัฒน์ นิด้า ซึ่งสามารถดาวน์โหลดได้ที่ law.nida.ac.th/journal

3.3 องค์ประกอบของบทความต้องมีรายละเอียด ดังต่อไปนี้

3.3.1 ชื่อเรื่อง (Title)

ทั้งภาษาไทยและภาษาอังกฤษ ใช้ตัวอักษร TH SarabunPSK ขนาดตัวอักษร 18 พอยต์ ตัวหนา

3.3.2 บทคัดย่อ (Abstract)

ภาษาไทยและภาษาอังกฤษ โดยอธิบายเป็นเรียงความย่อหน้าเดียวที่มีใจความครบถ้วน

อันประกอบด้วย วัตถุประสงค์ ความสำคัญของบทความ และบทสรุป

ชื่อหัวข้อของบทคัดย่อ ใช้ตัวอักษร TH SarabunPSK ขนาดตัวอักษร 16 พอยต์ ตัวหนา

โดยภาษาไทยใช้คำว่า “บทคัดย่อ” และภาษาอังกฤษใช้คำว่า “Abstract”

3.3.3 คำสำคัญ (Keyword)

จำนวน 3-5 คำ ทั้งภาษาไทยและภาษาอังกฤษ

ชื่อหัวข้อของคำสำคัญ ใช้ตัวอักษร TH SarabunPSK ขนาดตัวอักษร 16 พอยต์ ตัวหนา

โดยภาษาไทยใช้คำว่า “คำสำคัญ” และภาษาอังกฤษใช้คำว่า “Keywords”

3.3.4 บทนำ (Introduction)

ชื่อหัวข้อของบทนำ ใช้ตัวอักษร TH SarabunPSK ขนาดตัวอักษร 16 พอยต์ ตัวหนา

โดยภาษาไทยใช้คำว่า “บทนำ” และภาษาอังกฤษใช้คำว่า “Introduction”

3.3.5 เนื้อหา ใช้ตัวอักษร TH SarabunPSK ขนาดตัวอักษร 16 พอยต์

3.3.6 บทสรุป ใช้ตัวอักษร TH SarabunPSK ขนาดตัวอักษร 16 พอยต์

4. รูปแบบการอ้างอิง (เชิงอรรถ)

วิธีการอ้างอิงประยุกต์จากแบบ The Oxford Standard for Citation of Legal Authorities (OSCOLA) (ที่มา: https://www.law.ox.ac.uk/sites/files/oxlaw/oscola_4th_edn_hart_2012.pdf) ใช้ตัวอักษร TH SarabunPSK ขนาดตัวอักษร 14 พอยต์ ยกตัวอย่างดังต่อไปนี้

<u>หนังสือ</u>

ภาษาไทย

ชื่อผู้แต่ง,*ชื่อหนังสือ* (พิมพ์ครั้งที่, สำนักพิมพ์ ปีที่พิมพ์) เลขหน้าที่อ้างถึง.

บรรเจิด สิงคะเนติ, *หลักกฎหมายเกี่ยวกับการควบคุมฝ่ายปกครอง* (พิมพ์ครั้งที่ 5, สำนักพิมพ์วิญญูชน 2560) 123.

ภาษาอังกฤษ

author, *title* (additional information, edition, publisher year) page number.

Andrew Burrows, *Remedies for Torts and Breach of Contract* (3rd edn, OUP 2004) 317.

<u>บทความ</u>

ภาษาไทย

ชื่อผู้แต่งบทความ, ‘ชื่อบทความ’ (ปีที่พิมพ์) ฉบับที่ ชื่อวารสาร หน้าแรกของบทความ, เลขหน้าที่อ้างถึง.

มนตรี เกิดมีมูล, ‘ความพร้อมของข้าราชการไทยในการเข้าสู่ประชาคมอาเซียน’ (2560) 57 วารสารพัฒนบริหารศาสตร์ 152, 158-159.

ภาษาอังกฤษ

author, ‘title’(year) Volume No. Journal’s Name or Abbreviation first page, referred page(s).

Alison L Young, ‘In Defence of Due Deference’ (2009) 72 MLR 554, 556-557.

<u>บทความจากหนังสือรวบรวมบทความ</u>

ภาษาไทย

ชื่อผู้แต่งบทความ,‘ชื่อบทความ’ ใน ชื่อผู้รวบรวมบทความ, *ชื่อหนังสือ* (พิมพ์ครั้งที่, สำนักพิมพ์ ปีที่พิมพ์) เลขหน้าที่อ้างถึง.

สุจิตต์ วงษ์เทศ, ‘ประวัติศาสตร์ไทยเป็นส่วนหนึ่งที่แยกไม่ได้ของประวัติศาสตร์สุวรรณภูมิในอาเซียน’ ใน พิพัฒน์ กระแจะจันทร์, *ยุคมืดของประวัติศาสตร์ไทย หลังบายน พุทธเถรวาท การเข้ามาของคนไท* (สำนักพิมพ์มติชน 2559) 123.

ภาษาอังกฤษ

author, 'title' in editor (ed) book title (additional information, publisher year)/ referred page(s).

Justine Pila, 'The Value of Authorship in the Digital Environment' in William H Dutton and Paul W Jeffreys (eds), *World Wide Research: Reshaping the Sciences and Humanities in the Century of Information* (MIT Press 2010) 23.

<u>วิทยานิพนธ์</u>

ภาษาไทย

ชื่อผู้แต่งวิทยานิพนธ์, 'ชื่อวิทยานิพนธ์'(วิทยานิพนธ์ปริญญาโท-เอก, ชื่อมหาวิทยาลัย ปีที่สำเร็จการศึกษา).

นัทมน คงเจริญ, 'การใช้กฎหมายเพื่อการอนุรักษ์ช้างในประเทศไทย' (วิทยานิพนธ์ปริญญาโท, จุฬาลงกรณ์มหาวิทยาลัย 2538).

ภาษาอังกฤษ

Author, 'title' (type of thesis, university year of completion).

Javan Herberg, 'Injunctive Relief for Wrongful Termination of Employment' (DPhil thesis, University of Oxford 1989).

<u>เว็บไซต์</u>

ภาษาไทย

ชื่อผู้แต่ง, 'ชื่อข้อความที่อ้าง' (แหล่งที่มา, วันเดือนปี ที่ลงบทความ) <ชื่อเว็บไซต์> สืบค้นวันที่ วัน เดือน ปี.

ปรีชา สุวรรณทัต, 'Government Shutdown /การเมืองเรื่องการงบประมาณของสหรัฐ' (แนวหน้า, 9 กุมภาพันธ์ 2561) <http://www.naewna.com/politic/columnist/33994> สืบค้นวันที่ 18 มิถุนายน 2561.

ภาษาอังกฤษ

Author, 'title' (source, date of publication on the website) <web address> accessed Day Month Year.

Sarah Cole, 'Virtual Friend Fires Employee' (Naked Law, 1 May 2009) <www.nakedlaw.com/2009/05/index.html> accessed 19 November 2009.

<u>หนังสือพิมพ์</u>

ภาษาไทย

ชื่อผู้แต่ง, 'ชื่อบทความในหนังสือพิมพ์' ชื่อหนังสือพิมพ์ (เมืองที่พิมพ์, วันที่เผยแพร่) <ชื่อเว็บไซต์> สืบค้นวันที่.

สุจิตต์ วงษ์เทศ, 'พลังสร้างสรรค์ ถูกทำให้ฝ่อ ด้วยพลังของความเป็นไทย' หนังสือพิมพ์มติชน, (กรุงเทพมหานคร, 21 พฤษภาคม 2561) <https://www.matichon.co.th/article/news_969609> สืบค้นวันที่ 18 มิถุนายน 2561.

ภาษาอังกฤษ

Author,/‘title’/(the name of the newspaper/date of publication on the website) <web address> the date of most recent access

Jane Croft, ‘Supreme Court Warns on Quality’ Financial Times (London, 1 July 2010) accessed 3 July 2019.

<u>การอ้างซ้ำ</u>

1. ในกรณีที่ไม่มีเชิงอรรถอื่นมาคั่น

1.1 สำหรับเอกสารภาษาไทยให้ใช้ เพิ่งอ้าง

(ก) กรณีอ้างหน้าเดียวกัน

เพิ่งอ้าง

(ข) กรณีหน้าที่อ้างถึงต่างกัน ให้ระบุเลขหน้าไปด้วย

เพิ่งอ้าง 33-35.

1.2 สำหรับเอกสารภาษาอังกฤษให้ใช้ ibid.

(ก) กรณีอ้างหน้าเดียวกัน

Ibid.

(ข) กรณีหน้าที่อ้างถึงต่างกัน ให้ระบุเลขหน้าไปด้วย

ibid 33-35.

2. กรณีการอ้างอิงที่มีมาก่อนและมีเชิงอรรถมาคั่น

2.1 สำหรับเอกสารภาษาไทยให้ใช้

ชื่อผู้แต่ง (‘เชิงอรรถ’ เชิงอรรถที่อ้างอิงถึง) เลขหน้าที่อ้างถึง.

มนตรี เกิดมีมูล (เชิงอรรถ 19) 155.

2.2 สำหรับเอกสารภาษาอังกฤษให้ใช้

Author’ surname, ‘work title’ (n first cited footnote) page number.

Ashworth, ‘Testing Fidelity to Legal Values’ (n 27) 635-37.

5. วิธีการส่งบทความเพื่อตีพิมพ์

ผู้เขียนสามารถส่งบทความผ่านระบบ ThaiJO (Thai Journal Online) https://so04.tci-thaijo.org/index.php/nitipat/about/submissions ในรูปแบบของไฟล์ Word โดยทำตามคำแนะนำก่อนส่งบทความเกี่ยวกับการไม่ระบุตัวตนของผู้เขียนตามระบบ Thaijo

6. เงื่อนไขการตีพิมพ์

บทความหรือผลงานวิชาการจะต้องไม่เคยได้รับการตีพิมพ์และไม่เคยเผยแพร่ที่ใดมาก่อน และไม่อยู่ระหว่างการเสนอเพื่อพิจารณาตีพิมพ์ในวารสารฉบับอื่น บทความที่จะได้รับการตีพิมพ์ต้องได้รับการประเมินจากผู้ทรงคุณวุฒิอย่างน้อย 3 ท่านที่ตรงตามสาขาวิชา โดยเป็นการประเมินแบบลับในลักษณะ double-blinded การพิจารณารับตีพิมพ์บทความขึ้นอยู่กับดุลยพินิจของบรรณาธิการและกองบรรณาธิการ โดยผลการพิจารณาจากกองบรรณาธิการถือเป็นที่สุด

บทความ

GSL NIDA
คณะนิติศาสตร์

กองบรรณาธิการวารสารกฎหมายนิติพัฒน์ นิด้า
คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์
148 ถนนเสรีไทย แขวงคลองจั่น เขตบางกะปิ กรุงเทพฯ 10240
Tel: 0 2727 3662
Fax: 0 2374 4731
E-mail: nitipat_lawjournal@nida.ac.th
Website: law.nida.ac.th/journal