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).

ผู้สนับสนุนหลักในการจัดพิมพ์วารสาร

บทความแต่ละบทความเป็นความคิดเห็นอิสระของผู้เขียน