สิทธิของนักเรียนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และความท้าทายในการบังคับใช้ภายในสถานศึกษา

Students' Rights under the Personal Data Protection Act B.E. 2562 (2019) and the Challenges of Its Implementation in Educational Institutions

อภิภัสร์ ปาสานะเก[1], ณัฏฐ์ภัส ภาคะ[2], ชัยวัฒน์ ป้อมพิทักษ์[3],
สาลินี ลิขิตพัฒนะกุล[4] , รัชชานนท์ วิพัฒน์โสภากร[5]
นักศึกษาหลักสูตรนิติศาสตรดุษฎีบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม[1,3],
วิทยาลัยอาชีวศึกษาพิษณุโลก[2], มหาวิทยาลัยมหามกุฏราชวิทยาลัย[4], นักวิชาการอิสระ[5]
Apipat Pasanaga[1], Natthapat Phakha[2], Chaiwat Pomphithak[3] ,
Salinee Likitpattanakul[4] , Ratchanon Wiphatsopakorn[5]
Doctor of Laws (LL.D.) candidate, School of Law, Sripatum University[1,3],
Phitsanulok Vocational College[2],
Mahamakut Buddhist University[4] , Independent Scholar[5]
Corresponding Author E-mail: apipat.pasanaga@gmail.com[1],natthapat.phakha@gmail.com[2],
chaiwat0106@gmail.com, salinee.lik@gmail.com,ratchanon.wiphatsopakorn@gmail.com

(Received : November 24, 2025; Edit : December 5, 2025; accepted : December 7, 2025)

บทคัดย่อ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้เปลี่ยนกรอบคิดเกี่ยวกับการบริหารข้อมูลในสถานศึกษาไปอย่างมีนัยสำคัญ เนื่องจากโรงเรียนต้องจัดการข้อมูลของนักเรียนจำนวนมาก ทั้งข้อมูลทั่วไปและข้อมูลอ่อนไหว ซึ่งมีความเสี่ยงต่อการถูกละเมิดสิทธิ ความเป็นมาของปัญหานี้เกิดจากการที่สถานศึกษาขาดเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ที่มีความรู้ความเข้าใจโดยเฉพาะในการจัดการข้อมูลผู้เยาว์ ทั้งด้านนโยบาย และเทคโนโลยี การศึกษาครั้งนี้มีวัตถุประสงค์เพื่อวิเคราะห์สิทธิของนักเรียนตาม PDPA บทบาทและภาระหน้าที่ของสถานศึกษา ตลอดจนเปรียบเทียบกับกฎหมายต่างประเทศ โดยใช้วิธีการศึกษาวิเคราะห์กฎหมายและเอกสารเชิงทฤษฎี (documentary research) ภายใต้ขอบเขตโรงเรียนระดับขั้นพื้นฐานของไทย

ผลการศึกษาพบว่าสิทธิของนักเรียนตามมาตรา 30–34 ยังไม่ได้รับการคุ้มครองอย่างเพียงพอ เช่น สิทธิในการเพิกถอนความยินยอม หรือ สิทธิในการเข้าถึงและขอสำเนาข้อมูล แม้กฎหมายจะกำหนดกลไกสิทธิไว้อย่างชัดเจน แต่สถานศึกษาจำนวนมากยังขาดความเข้าใจและความพร้อมเชิงโครงสร้าง ทั้งด้านการกำหนดนโยบาย การจัดระบบความยินยอม การแจ้งวัตถุประสงค์ และการรักษาความมั่นคงปลอดภัยตามมาตรา 37 รวมถึงปัญหาเชิงปฏิบัติ เช่น การใช้แพลตฟอร์มออนไลน์ การเก็บข้อมูลเกินความจำเป็น และการรายงานเหตุข้อมูลรั่วไหลที่ไม่มีระบบ ขณะที่การเปรียบเทียบกับ GDPR, FERPA, COPPA และกฎหมายของสิงคโปร์ ญี่ปุ่น และเกาหลีใต้ ทำให้เห็นแนวปฏิบัติที่ส่งเสริมสิทธิของผู้เรียนอย่างเป็นระบบมากกว่า และ PDPA ยังขาดความชัดเจนในประเด็นสิทธิในการพกพาข้อมูล (Data Portability) และการกำหนดสิทธิของเด็กที่ชัดเจนตามแบบ GDPR ข้อเสนอแนะสำคัญ ได้แก่ การจัดทำ Privacy Notice ที่ครบถ้วน การแต่งตั้ง DPO การอบรมครูอย่างต่อเนื่อง การกำหนดมาตรฐานความปลอดภัยด้านไอที และการสร้างวัฒนธรรมการคุ้มครองข้อมูลส่วนบุคคลภายในสถานศึกษา เพื่อยกระดับการคุ้มครองสิทธิของนักเรียนในยุคดิจิทัลอย่างยั่งยืน

คำสำคัญ: สิทธิของนักเรียน, ข้อมูลส่วนบุคคล, ผู้ควบคุมข้อมูล, ความยินยอม, การคุ้มครองข้อมูลในสถานศึกษา

Abstract

The Personal Data Protection Act B.E. 2562 (2019) has significantly shifted the conceptual framework of data governance within educational institutions, as schools are required to manage large volumes of student data, including both general and sensitive information that carry substantial risks of rights violations. The root of this problem lies in the absence of adequately trained Data Protection Officers (DPOs) in schools, particularly regarding the management of minors' data in terms of policies and technological safeguards. This study aims to analyze students' rights under the PDPA, the roles and obligations of educational institutions, and relevant comparative legal frameworks. The research employs documentary analysis focusing on basic education schools in Thailand.

The findings reveal that students' rights under Sections 30–34 remain insufficiently protected, particularly the right to withdraw consent, and the right to access and obtain copies of personal data. Although the Act clearly defines these rights, many schools lack the structural readiness and understanding necessary for proper implementation, including policy formulation, consent management, notification of processing purposes, and security measures under Section 37. Practical issues also arise, such as the use of online platforms, excessive data collection, and the absence of systematic procedures for reporting data breaches. Comparisons with the GDPR, FERPA, COPPA, and the data-protection laws of Singapore, Japan, and South Korea reveal more robust and student-centered approaches, while the PDPA remains less explicit regarding data portability and the delineation of children's rights as articulated in the GDPR. Key recommendations include developing comprehensive Privacy Notices, appointing DPOs, providing continuous training for teachers, establishing IT security standards, and fostering a culture of personal data protection within schools to strengthen the long-term safeguarding of students' rights in the digital era.

Keywords: Students' Rights, Personal Data, Data Controller, Consent, Data Protection in Educational Institutions

บทนำ

การคุ้มครองข้อมูลส่วนบุคคลได้กลายเป็นประเด็นสำคัญในสังคมสมัยใหม่ ซึ่งโครงสร้างทางเศรษฐกิจและสังคมถูกกำหนดด้วยข้อมูลจำนวนมหาศาลที่ไหลเวียนในทุกระบบ โดยเฉพาะอย่างยิ่งในบริบทของสถานศึกษา ซึ่งนักเรียนในฐานะผู้เยาว์เป็นกลุ่มประชากรที่มีความเสี่ยงสูงต่อการละเมิดสิทธิส่วนบุคคล ซึ่งอาจก่อให้เกิดความเสี่ยงต่อโรงเรียนในด้านบทลงโทษทางปกครองและการฟ้องร้องทั้งทางแพ่งและอาญา ซึ่งเป็นปัจจัยสำคัญที่ทำให้ผู้บริหารต้องตระหนัก การจัดเก็บข้อมูลของสถานศึกษาไม่ได้จำกัดเพียงข้อมูลพื้นฐาน เช่น ชื่อ อายุ ชั้นเรียน หรือประวัติการศึกษา แต่ยังครอบคลุมข้อมูลที่มีความอ่อนไหวสูง เช่น ข้อมูลด้านสุขภาพ ประวัติพฤติกรรม ภาพจากระบบกล้องวงจรปิด ข้อมูลไบโอเมตริกซ์เกี่ยวกับร่างกายของบุคคล เช่น ลวดลายสีในดวงตา ซึ่งสามารถนำมาใช้เพื่อพิสูจน์ตัวตนของบุคคลนั้นได้ (Panurut Chuenpukdee, 2019: 10) ตลอดจนถึงข้อมูลครอบครัวที่อาจส่งผลกระทบต่อสวัสดิภาพของเด็กหากถูกนำไปใช้โดยมิชอบ การเติบโตของเทคโนโลยีดิจิทัลทำให้การเก็บ รวบรวม ใช้ และส่งต่อข้อมูลสามารถทำได้ง่ายขึ้น ขณะเดียวกันก็เพิ่มระดับความเสี่ยงที่สถานศึกษาจะนำข้อมูลไปใช้ผิดวัตถุประสงค์หรือขาดมาตรการป้องกันอย่างเพียงพอ สภาวะดังกล่าวนำไปสู่คำถามพื้นฐานเชิงนโยบายว่า สิทธิของนักเรียนในฐานะเจ้าของข้อมูลส่วนบุคคลควรถูกคุ้มครองอย่างไร และสถานศึกษาในฐานะผู้ควบคุมข้อมูลควรมีกรอบความรับผิดชอบแบบใดจึงจะสอดคล้องกับมาตรฐานกฎหมายสมัยใหม่

สถานศึกษาในระดับขั้นพื้นฐานต้องบริหารจัดการข้อมูลส่วนบุคคลของผู้เรียนในบริบทที่มีความละเอียดอ่อนเป็นพิเศษ เนื่องจากนักเรียนส่วนใหญ่ยังเป็นผู้เยาว์ซึ่งกฎหมายกำหนดให้การให้ความยินยอมต้องผ่านผู้ใช้อำนาจปกครองตามมาตรา 20 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (นพมาศ นิลแช่ม, 2568: 55) การขอความยินยอมผ่านบุคคลอื่นเช่นนี้ทำให้โรงเรียนต้องเผชิญความท้าทายทั้งด้านกฎหมายและกระบวนการปฏิบัติ ไม่เพียงต้องจัดทำเอกสารที่ระบุวัตถุประสงค์อย่างชัดเจนและเข้าใจง่าย แต่ยังต้องแยกแยะให้ได้ว่ากิจกรรมใดจำเป็นต้องใช้ความยินยอม และกิจกรรมใดอาศัยฐานทางกฎหมายอื่นตามมาตรา 24 การตีความผิดเพียงเล็กน้อยอาจนำไปสู่การละเมิดสิทธิของนักเรียนโดยไม่เจตนา โดยเฉพาะในยุคที่โรงเรียนพึ่งพาเทคโนโลยีดิจิทัลและแพลตฟอร์มออนไลน์ซึ่งเก็บข้อมูลจำนวนมากอย่างต่อเนื่อง ความซับซ้อนของการให้ความยินยอมของผู้เยาว์จึงกลายเป็นความเสี่ยงสำคัญที่สุดของสถานศึกษา ทั้งในด้านความรับผิดชอบต่อสิทธิของนักเรียน การบริหารจัดการข้อมูล และความเป็นไปได้ของข้อร้องเรียนหรือการกำกับตรวจสอบจากหน่วยงานรัฐ ส่งผลให้การขอความยินยอมที่ถูกต้องตามกฎหมายเป็นหัวใจของการคุ้มครองข้อมูลเด็กอย่างแท้จริงในระบบการศึกษาไทย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้รับการประกาศใช้เพื่อกำหนดมาตรฐานใหม่ในการรักษาความเป็นส่วนตัวของบุคคล โดยสร้างกลไกทางกฎหมายที่กำหนดให้ “ผู้ควบคุมข้อมูลส่วนบุคคล” ต้องเคารพสิทธิของเจ้าของข้อมูลในทุกขั้นตอนของการประมวลผลข้อมูล ไม่ว่าจะเป็นการเก็บรวบรวม ใช้ เปิดเผย โอน หรือจัดเก็บรักษา (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, 2562: 71-72) กฎหมายฉบับนี้ถือเป็นการยกระดับการคุ้มครองสิทธิส่วนบุคคลของประเทศไทยให้มีลักษณะสอดคล้องกับมาตรฐานสากล เช่น GDPR ของสหภาพยุโรป ซึ่งเน้นหลักการความโปร่งใส ความจำเป็น ความถูกต้อง ความมั่นคงปลอดภัย และความรับผิดรับชอบ โดยเฉพาะอย่างยิ่งเรื่อง “ความยินยอม” ที่ต้องนำเสนอในลักษณะที่แยกแยะได้ชัดเจนจากเรื่องอื่น ๆ สามารถเข้าถึงได้ โดยใช้ภาษาที่ชัดเจนและเข้าใจง่าย (Kuner, Christopher et al, 2021: 46) และเรื่อง “ข้อมูลส่วนบุคคลพิเศษ” ซึ่งจำเป็นต้องใช้มาตรการคุ้มครองที่เข้มงวดกว่า สำหรับสถานศึกษา การปฏิบัติตามกฎหมายดังกล่าวมีความซับซ้อนมากขึ้น เพราะนักเรียนจำนวนมากเป็นผู้เยาว์ ซึ่งต้องใช้กลไกการให้ความยินยอมของผู้ปกครองตามมาตรา 20 ขณะเดียวกันสถานศึกษายังมีบทบาทของ “ผู้ใช้อำนาจรัฐ” ในการดำเนินการตามหน้าที่ทางการศึกษา ทำให้ต้องตีความและปรับใช้ข้อยกเว้นของกฎหมายอย่างระมัดระวัง เช่น มาตรา 24 ที่กำหนดเงื่อนไขในการเก็บข้อมูลโดยไม่ต้องขอความยินยอม นำไปสู่ความจำเป็นในการแยกแยะระหว่างข้อมูลที่สถานศึกษาต้องใช้เพื่อการบริหารจัดการ กับข้อมูลที่ไม่ควรเก็บเกินความจำเป็น

ปัญหาเชิงปฏิบัติในสถานศึกษาปรากฏอย่างเด่นชัดเมื่อพิจารณาถึงรูปแบบการใช้งานข้อมูลจริง เช่น การถ่ายสำเนาบัตรประชาชนของนักเรียนและผู้ปกครอง การจัดทำทะเบียนสุขภาพ การติดตั้งระบบสแกนใบหน้าหรือการสแกนลายนิ้วมือ ระบบบันทึกพฤติกรรม การประมวลผลข้อมูลจากแพลตฟอร์มการเรียนออนไลน์ การไม่จำกัดระยะเวลาของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเด็กในสื่ออินเทอร์เน็ต (จิดาภา คีรีมาศทอง, 2568: 136-139) รวมถึงการถ่ายภาพนักเรียนเพื่อประชาสัมพันธ์ซึ่งมักกระทำโดยปราศจากการขอความยินยอมอย่างถูกต้องตามกฎหมาย แม้สถานศึกษาจะมีเจตนาดีในการบริหารจัดการหรือพัฒนาคุณภาพการเรียนรู้ แต่การขาดความรู้ทางกฎหมายเกี่ยวกับ PDPA ทำให้เกิดความคลาดเคลื่อนในการตีความบทบัญญัติต่าง ๆ เช่น มาตรา 19 ว่าด้วยการขอความยินยอม มาตรา 22–25 เกี่ยวกับการเก็บรวบรวมข้อมูล และมาตรา 26 ว่าด้วยข้อมูลส่วนบุคคลพิเศษ นอกจากนี้ ความท้าทายยังขยายไปถึงประเด็นโครงสร้างพื้นฐาน เช่น ความปลอดภัยของระบบสารสนเทศ การเข้าถึงข้อมูลโดยบุคลากรที่ไม่จำเป็น และการส่งต่อข้อมูลไปยังหน่วยงานภายนอก เช่น โรงพยาบาล บริษัทประกันภัย และผู้ให้บริการแพลตฟอร์มออนไลน์ ซึ่งทั้งหมดต้องอยู่ภายใต้กรอบของมาตรา 27–29 เกี่ยวกับการใช้ เปิดเผย และการโอนข้อมูลไปต่างประเทศ สถานศึกษาจึง

ต้องมีระบบการกำกับดูแลที่เข้มแข็งและมีมาตรการที่ชัดเจนเพื่อไม่ให้เกิดการละเมิดสิทธิซึ่งอาจส่งผลกระทบต่อเด็กอย่างไม่อาจกลับคืนได้

จากความซับซ้อนของกฎหมายและข้อท้าทายในการปฏิบัติในสถานศึกษา บทความนี้มีเป้าหมายเพื่อวิเคราะห์สิทธิของนักเรียนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมุ่งเน้นการอธิบายสิทธิขั้นพื้นฐานของนักเรียนตามหมวด 3 ของกฎหมาย ได้แก่ สิทธิขอเข้าถึงข้อมูล สิทธิขอรับข้อมูลในรูปแบบอิเล็กทรอนิกส์ สิทธิในการคัดค้าน สิทธิในการลบ สิทธิระงับการใช้ข้อมูล และสิทธิในการให้ข้อมูลถูกต้องครบถ้วน พร้อมทั้งวิเคราะห์สถานศึกษาว่ามีภาระหน้าที่ตามบทบัญญัติใดบ้าง ไม่ว่าจะเป็นมาตรการรักษาความมั่นคงปลอดภัย (มาตรา 37) การบันทึกกิจกรรมข้อมูล (มาตรา 39) การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 41–42) ตลอดจนการแจ้งเหตุละเมิดข้อมูล (data breach) ที่ต้องดำเนินการภายใน 72 ชั่วโมงตามที่กฎหมายกำหนด และยังเชื่อมโยงกรณีศึกษาจากต่างประเทศ เช่น มาตรการคุ้มครองข้อมูลของนักเรียนในสหภาพยุโรปและสหรัฐอเมริกา เพื่อสร้างความเข้าใจเชิงเปรียบเทียบ พร้อมเสนอแนวทางเชิงนโยบายสำหรับสถานศึกษาไทยในการปรับตัวด้วยมาตรฐานที่สูงขึ้น ทั้งในมิติของกฎหมาย เทคโนโลยี และธรรมาภิบาลข้อมูล (data governance) เพื่อทำให้การบริหารจัดการข้อมูลของนักเรียนเกิดความสมดุลระหว่างการคุ้มครองสิทธิส่วนบุคคลและประโยชน์สาธารณะด้านการศึกษาอย่างแท้จริง

สิทธิของนักเรียนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การคุ้มครองข้อมูลส่วนบุคคลของนักเรียนเป็นประเด็นที่มีความสำคัญอย่างยิ่งในบริบทของสถานศึกษา เนื่องจากนักเรียนจำนวนมากยังเป็นผู้เยาว์และมีสถานะที่กฎหมายให้ความคุ้มครองเป็นพิเศษ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลของนักเรียนในสถานศึกษาไม่เพียงต้องปฏิบัติตามหลักการทั่วไปเกี่ยวกับข้อมูลส่วนบุคคลเท่านั้น แต่ยังต้องพิจารณา “สถานะผู้เยาว์” ที่ทำให้ผู้ควบคุมข้อมูลจำเป็นต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองตามมาตรา 20 ด้วย การทำความเข้าใจสิทธิของนักเรียนตามหมวด 3 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงเป็นรากฐานสำคัญในการออกแบบมาตรการคุ้มครองข้อมูลภายในสถานศึกษา และเป็นเงื่อนไขจำเป็นเพื่อให้การจัดการข้อมูลสอดคล้องกับกรอบกฎหมายอย่างแท้จริง ซึ่งได้กำหนดเงื่อนไขในการใช้สิทธิ รวมถึงเหตุปฏิเสธสิทธิของเจ้าของข้อมูลไว้ในหลายกรณี (ชวิน อุ่นภัทร และ ปิยะบุตร บุญอร่ามเรือง, 2564: 55) หัวข้อนี้ผู้เขียนมุ่งอธิบายสิทธิสำคัญของนักเรียนที่ระบุไว้ในกฎหมาย พร้อมยกตัวอย่างการประยุกต์ใช้ในสถานศึกษา รวมถึงวิเคราะห์เงื่อนไขในการให้ความยินยอมของผู้เยาว์ตามมาตรา 19–25 ซึ่งมีผลต่อการตีความและการปฏิบัติอย่างเป็นรูปธรรมในบริบทจริงของโรงเรียนไทย

1. สิทธิขอเข้าถึงข้อมูลของนักเรียน (มาตรา 30)

มาตรา 30 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้สิทธิแก่นักเรียนในฐานะเจ้าของข้อมูลส่วนบุคคลในการ “ขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล” ที่สถานศึกษาจัดเก็บไว้ รวมถึงสิทธิขอให้โรงเรียนเปิดเผยวิธีการได้มาซึ่งข้อมูลในกรณีที่ข้อมูลนั้นไม่ได้มาจากการให้ความยินยอมโดยตรง (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, 2562: 68) สิทธินี้ถือเป็นหัวใจสำคัญของความโปร่งใสในการประมวลผลข้อมูล (transparency) และยังเป็นเครื่องมือป้องกันไม่ให้โรงเรียนเก็บข้อมูลมากเกินความจำเป็นหรือใช้ข้อมูลผิดวัตถุประสงค์

ในบริบทสถานศึกษา ข้อมูลที่นักเรียนสามารถใช้สิทธิขอเข้าถึง ได้แก่ ประวัติผลการเรียน ข้อมูลการลงโทษทางวินัย ข้อมูลสุขภาพที่โรงเรียนเก็บไว้ บันทึกการเข้า–ออกโรงเรียน รูปภาพหรือวิดีโอที่มีการจัดเก็บไว้ภายในระบบ ข้อมูลจากระบบ LMS เช่น Google Classroom หรือระบบเช็คชื่ออัตโนมัติ

การปฏิเสธคำขอทำได้เฉพาะกรณีที่มีเหตุอันชอบด้วยกฎหมาย เช่น การเปิดเผยข้อมูลอาจกระทบสิทธิของบุคคลอื่น หรือมีคำสั่งศาลห้ามเปิดเผย ในทุกกรณีที่โรงเรียนปฏิเสธคำขอ โรงเรียนต้อง “บันทึกเหตุผลการปฏิเสธ” ไว้ตามมาตรา 39 เพื่อให้สามารถตรวจสอบย้อนหลังได้

ในเชิงปฏิบัติ สถานศึกษาควรจัดทำ “ระบบคำร้องข้อมูลส่วนบุคคล” และกำหนดช่องทางให้ผู้ปกครองหรือนักเรียนยื่นคำขอได้โดยง่าย รวมทั้งต้องตอบคำขอภายใน 30 วัน ซึ่งเป็นระยะเวลาที่กฎหมายกำหนด เพื่อไม่ให้เกิดภาระเกินสมควรกับเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่นักเรียนสงสัยว่าข้อมูลของตนถูกนำไปใช้โดยมิชอบ สิทธินี้จึงมีบทบาทสำคัญในการคุ้มครองสวัสดิภาพของผู้เรียน

2. สิทธิขอรับข้อมูลและสิทธิในการโอนข้อมูล (มาตรา 31)

มาตรา 31 เป็นสิทธิที่สะท้อนมาตรฐานสากลด้าน data portability (Bárbara da Rosa Lazarotto, (2024: 3-4) โดยกำหนดให้เจ้าของข้อมูลมีสิทธิ “ขอรับข้อมูลส่วนบุคคลในรูปแบบที่สามารถอ่านโดยระบบอัตโนมัติได้” หรือขอให้โรงเรียนส่งต่อข้อมูลไปยังผู้ควบคุมข้อมูลรายอื่น เช่น โรงเรียนปลายทางในกรณีที่นักเรียนย้ายสถานศึกษา สิทธินี้ช่วยให้การเคลื่อนย้ายข้อมูลมี

ประสิทธิภาพ ลดความซ้ำซ้อน และลดความเสี่ยงจากการจัดทำข้อมูลใหม่

ตัวอย่างการใช้สิทธิในทางปฏิบัติ เช่น เมื่อผู้ปกครองต้องการย้ายบุตรหลานไปยังโรงเรียนใหม่ โรงเรียนเดิมต้องจัดส่งประวัติผลการเรียนในรูปแบบดิจิทัลตามคำขอ นักเรียนขอให้ย้ายไฟล์พอร์ตโฟลิโอที่จัดเก็บในระบบ LMS ไปยังแพลตฟอร์มอื่น หรือ ขอรับประวัติพฤติกรรมหรือประวัติการเข้าร่วมกิจกรรมในรูปแบบไฟล์อิเล็กทรอนิกส์ เป็นต้น

อย่างไรก็ตาม กฎหมายกำหนดข้อจำกัดสำคัญคือ สิทธินี้ไม่ใช้กับข้อมูลที่โรงเรียนประมวลผลเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ตามกฎหมาย เช่น ข้อมูลผลการสอบมาตรฐานระดับชาติ ข้อมูลดังกล่าวอาจต้องอยู่ภายใต้การควบคุมของรัฐและไม่สามารถโอนย้ายโดยอัตโนมัติได้

3. สิทธิคัดค้านการประมวลผลข้อมูล (มาตรา 32)

มาตรา 32 ให้นักเรียนมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตนในกรณีดังต่อไปนี้

(1) เมื่อข้อมูลถูกประมวลผลตามฐานประโยชน์สาธารณะ (มาตรา 24(4)) หรือฐานประโยชน์โดยชอบด้วยกฎหมายของโรงเรียน (มาตรา 24(5))

(2) การประมวลผลข้อมูลเพื่อ “การตลาดแบบตรง” ซึ่งแม้ตัวอย่างนี้อาจพบไม่มากในสถานศึกษา แต่มีความสำคัญในการป้องกันการใช้ข้อมูลนักเรียนในเชิงพาณิชย์

(3) การประมวลผลข้อมูลเพื่อวัตถุประสงค์ด้านการวิจัยหรือสถิติ หากเจ้าของข้อมูลเห็นว่าอาจมีผลกระทบต่อสิทธิของตน (สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม, 2567: ออนไลน์)

ตัวอย่างกรณีที่นักเรียนอาจใช้สิทธิคัดค้าน เช่น นักเรียนไม่ต้องการให้โรงเรียนใช้ภาพถ่ายของตนในสื่อประชาสัมพันธ์ ผู้ปกครองไม่ยินยอมให้โรงเรียนส่งข้อมูลไปยังบริษัทที่ให้บริการแอปพลิเคชันเสริมการเรียน หรือ นักเรียนไม่เห็นด้วยที่โรงเรียนใช้ข้อมูลพฤติกรรมเพื่อวิเคราะห์คะแนนพฤติกรรมด้วยระบบ AI เป็นต้น

เมื่อมีการคัดค้าน โรงเรียนต้องหยุดประมวลผลข้อมูลทันที เว้นแต่พิสูจน์ได้ว่ามีเหตุผลทางกฎหมายที่ “สำคัญยิ่งกว่า” ซึ่งเป็นเกณฑ์ที่ต้องตีความอย่างจำกัดเพื่อปกป้องสิทธิของนักเรียนอย่างแท้จริง

4. สิทธิขอลบหรือทำลายข้อมูล (มาตรา 33)

มาตรา 33 กำหนดสิทธิที่สำคัญอย่างยิ่งของนักเรียน คือ สิทธิขอให้โรงเรียนลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ (anonymization) ในกรณีต่อไปนี้

(1) ข้อมูลหมดความจำเป็นตามวัตถุประสงค์

(2) ผู้ปกครองหรือเจ้าของข้อมูลถอนความยินยอม

(3) นักเรียนคัดค้านการประมวลผลตามมาตรา 32 และโรงเรียนไม่อาจปฏิเสธ

(4) ข้อมูลถูกเก็บ รวบรวม หรือใช้โดยไม่ชอบด้วยกฎหมาย

กรณีในสถานศึกษา เช่น โรงเรียนยังคงเก็บข้อมูลนักเรียนที่จบการศึกษาไปนานหลายปีโดยไม่จำเป็น รูปภาพนักเรียนถูกใช้ในกิจกรรมประชาสัมพันธ์โดยไม่เคยได้รับความยินยอม หรือ ข้อมูลสุขภาพที่โรงเรียนเก็บไว้เกินระยะเวลาที่จำเป็นสำหรับการดูแล เป็นต้น

กฎหมายยังระบุว่า หากข้อมูลถูก “เปิดเผยต่อสาธารณะ” เช่น ลงเว็บไซต์ เฟซบุ๊ก หรือสื่อออนไลน์ โรงเรียนต้องรับผิดชอบดำเนินการให้สอดคล้องตามคำขอลบ “ทั้งในด้านเทคนิคและค่าใช้จ่าย” ซึ่งสะท้อนความรับผิดชอบสูงของสถานศึกษาในยุคดิจิทัล

5. สิทธิระงับการใช้ข้อมูล (มาตรา 34)

นอกจากสิทธิขอลบข้อมูลแล้ว มาตรา 34 ให้นักเรียนมีสิทธิ “ขอระงับการใช้ข้อมูล” ในสถานการณ์เฉพาะ เช่น ข้อมูลอยู่ระหว่างการตรวจสอบความถูกต้อง มีการขอลบข้อมูลแต่เจ้าของข้อมูลประสงค์ให้หยุดการใช้ก่อน ข้อมูลหมดความจำเป็นแต่เจ้าของข้อมูลต้องการเก็บไว้เพื่อใช้สิทธิตามกฎหมาย หรือ โรงเรียนอยู่ระหว่างการพิจารณาคัดค้านตามมาตรา 32

ตัวอย่างในโรงเรียน ได้แก่ ผู้ปกครองต้องการให้โรงเรียนระงับการใช้ข้อมูลสุขภาพของบุตรหลานระหว่างที่อยู่ระหว่างการแก้ไข นักเรียนร้องเรียนว่าข้อมูลพฤติกรรมถูกบันทึกผิดและต้องการให้หยุดใช้ก่อนแก้ไข หรือ โรงเรียนจะส่งข้อมูลนักเรียนให้บริษัทภายนอกแต่มีคำร้องขอให้ระงับก่อนตรวจสอบความเหมาะสมของสัญญา หากโรงเรียนไม่ดำเนินการตามคำร้อง เจ้าของข้อมูลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญทันที

6. ความยินยอมของผู้เยาว์และผลต่อการปฏิบัติในสถานศึกษา (มาตรา 19–25 และมาตรา 20)

การประมวลผลข้อมูลของนักเรียนในสถานศึกษาต้องตีความร่วมกับกฎเกณฑ์เกี่ยวกับ “การยินยอมของผู้เยาว์” ซึ่งมีลักษณะพิเศษกว่าการยินยอมของบุคคลทั่วไป

(1) ความยินยอมต้อง “ชัดแจ้ง” และ “แจ้งวัตถุประสงค์” (มาตรา 19) แบบฟอร์มต้องเข้าใจง่าย แยกจากเอกสารอื่น ไม่

บังคับให้ยินยอมในสิ่งที่ไม่จำเป็นต่อการศึกษา

(2) ผู้เยาว์ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครอง (มาตรา 20) หากผู้เยาว์ ไม่เกิน 10 ปี ต้องใช้ความยินยอมของผู้ปกครองเท่านั้น หากอายุเกิน 10 ปี แต่ยังไม่บรรลุนิติภาวะ ต้องได้รับความยินยอมจากทั้งผู้ปกครองและตัวเด็กในเรื่องที่กฎหมายกำหนด

(3) ข้อมูลที่สามารถเก็บโดยไม่ต้องยินยอม (มาตรา 24) ซึ่งมีผลอย่างมากต่อโรงเรียน เช่น ข้อมูลเพื่อประโยชน์สาธารณะด้านการศึกษา การปฏิบัติหน้าที่ตามกฎหมายของสถานศึกษา ข้อมูลเพื่อป้องกันอันตรายต่อชีวิตหรือสุขภาพนักเรียน

อย่างไรก็ตาม แม้เข้าข้อยกเว้น โรงเรียนต้องไม่เก็บเกินความจำเป็น และต้องแจ้งนักเรียนหรือผู้ปกครองตามมาตรา 23

7. ผลกระทบเชิงปฏิบัติในสถานศึกษา

เพื่อนำกฎหมายไปใช้ได้จริง สถานศึกษาต้องตีความสิทธิต่าง ๆ ของนักเรียนและออกแบบมาตรการที่เหมาะสม เช่น

(1) การให้ข้อมูลกับครูและบุคลากร ต้องจำกัดเฉพาะผู้มีหน้าที่ เช่น ครูประจำชั้น นักจิตวิทยา หรือฝ่ายวินัย มิใช่เผยแพร่ข้อมูลนักเรียนแก่ครูทุกคนโดยไม่จำเป็น

(2) การบันทึกภาพกิจกรรม ต้องได้รับความยินยอมก่อนถ่ายหรือใช้ภาพนักเรียน ห้ามใช้ภาพเพื่อประชาสัมพันธ์หากไม่แจ้งวัตถุประสงค์ชัดเจน หากเป็นภาพกิจกรรมสาธารณะ ต้องพิจารณาความเหมาะสมและไม่เปิดเผยข้อมูลที่อาจกระทบศักดิ์ศรีของนักเรียน

(3) การใช้งานระบบ LMS และแพลตฟอร์มออนไลน์ ต้องแจ้งนโยบายข้อมูลส่วนบุคคลของผู้ให้บริการให้ผู้ปกครองทราบ ห้ามส่งข้อมูลนักเรียนให้บริษัทภายนอกที่ไม่มีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอตามมาตรา 28 ควรมีมาตรการจำกัดการเข้าถึงข้อมูลในระบบ เช่น การกำหนดบัญชีผู้ใช้และสิทธิการเข้าถึงอย่างรัดกุม

(4) การรายงานผลการเรียนแก่ผู้ปกครอง แม้ถือเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ แต่ต้องส่งเฉพาะข้อมูลของบุตรหลาน ไม่เปิดเผยข้อมูลของนักเรียนคนอื่นร่วมด้วย เช่น ไม่ควรโพสต์ลำดับคะแนนรวมทั้งห้องลงกลุ่มไลน์ผู้ปกครอง

สรุปภาพรวมสิทธิของนักเรียนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ครอบคลุมทั้งมิติของความโปร่งใส การควบคุมข้อมูล และการได้รับความคุ้มครองจากการใช้ข้อมูลโดยไม่จำเป็น การใช้สิทธิอย่างมีประสิทธิภาพต้องอาศัยความเข้าใจของทั้งผู้ปกครอง นักเรียน และบุคลากรของโรงเรียน โดยมีสถานศึกษาเป็นผู้รับผิดชอบหลักในการวางระบบที่ทำให้สิทธิเหล่านี้เกิดผลอย่างแท้จริง บทบัญญัติแต่ละมาตราไม่ได้มีผลเฉพาะด้านเทคนิคของการจัดเก็บข้อมูล แต่ยังสะท้อนเจตนารมณ์ของกฎหมายที่ต้องการให้โรงเรียนเคารพศักดิ์ศรีและศักยภาพของผู้เรียนในฐานะปัจเจกบุคคลที่มีสิทธิพื้นฐานเหนือข้อมูลของตนเอง

บทบาทของสถานศึกษาในฐานะผู้ควบคุมข้อมูลส่วนบุคคล และความท้าทายด้านการบริหารจัดการข้อมูลนักเรียน

สถานศึกษาในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักกฎหมายอย่างรอบคอบ ทั้งการเก็บ การใช้ และการเปิดเผยข้อมูลนักเรียนภายใต้ PDPA กระบวนการดังกล่าวไม่เพียงก่อให้เกิดภาระหน้าที่เชิงนโยบายและเทคนิคเท่านั้น แต่ยังเผชิญความท้าทายหลายด้าน จึงจำเป็นต้องวิเคราะห์ทั้งบทบาทตามกฎหมายและปัญหาเชิงโครงสร้างอย่างเป็นระบบ

1. บทบาทของสถานศึกษาในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

สถานศึกษาเป็นหน่วยงานที่มีบทบาทสำคัญในการจัดการข้อมูลส่วนบุคคลของนักเรียน ทั้งในด้านการเก็บรวบรวม การใช้ การเปิดเผย การจัดเก็บรักษา และการลบหรือทำลายข้อมูลตามวัตถุประสงค์ทางการศึกษา ด้วยเหตุนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้สถานศึกษาทุกแห่งเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” โดยปริยาย เพราะโรงเรียนเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลของผู้เรียน บุคลากร และผู้ปกครอง บทบาทดังกล่าวก่อให้เกิดหน้าที่ตามกฎหมายหลายประการที่สถานศึกษาต้องดำเนินการอย่างเคร่งครัด มิฉะนั้นอาจก่อให้เกิดการละเมิดสิทธิของผู้เรียน และส่งผลกระทบทางกฎหมายและจริยธรรมอย่างร้ายแรง

(1) ภาระหน้าที่สำคัญที่สถานศึกษาต้องปฏิบัติตามคือ การแจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูล ตามมาตรา 23 ซึ่งกำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งรายละเอียดแก่นักเรียนหรือผู้ปกครองก่อนหรือขณะเก็บข้อมูล ไม่ว่าจะเป็นวัตถุประสงค์ของการใช้ข้อมูล ระยะเวลาเก็บรักษา หรือประเภทบุคคลที่ข้อมูลอาจถูกเปิดเผย การแจ้งวัตถุประสงค์อย่างโปร่งใสเป็นเงื่อนไขสำคัญที่ทำให้เจ้าของข้อมูลสามารถประเมินผลกระทบต่อสิทธิของตนได้ และเป็นกลไกที่สกัดกั้นไม่ให้โรงเรียนเก็บข้อมูลเกินความจำเป็นหรือใช้ข้อมูลนอกเหนือวัตถุประสงค์ที่กำหนดไว้ตามมาตรา 21

(2) หน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ตามมาตรา 37 ซึ่งกำหนดให้โรงเรียนต้องจัดระบบป้องกันการเข้าถึงข้อมูลโดยมิชอบ ทั้งในรูปแบบเอกสารและดิจิทัล รวมถึงต้องแจ้งเหตุละเมิดข้อมูลแก่สำนักงานภายใน 72 ชั่วโมงหากมี

ความเสี่ยงต่อสิทธิของเจ้าของข้อมูล (ปรีดา โชติมานนท์ และ สุขสมัย สุทธิบดี, 2566: 22) มาตราดังกล่าวเป็นความรับผิดชอบเชิงรุกที่สถานศึกษาต้องดำเนินการเพื่อป้องกันข้อมูลนักเรียนรั่วไหล โดยเฉพาะอย่างยิ่งในยุคที่ข้อมูลถูกจัดเก็บในระบบออนไลน์ และมีการส่งต่อผ่านแพลตฟอร์มเอกชนจำนวนมาก เช่น Google Workspace, Zoom หรือ Line ซึ่งมักมีนโยบายข้อมูลส่วนบุคคลที่ซับซ้อนและอาจตั้งอยู่ในต่างประเทศที่มีมาตรฐานคุ้มครองข้อมูลไม่เท่าเทียมตามเงื่อนไขของมาตรา 28

(3) สถานศึกษายังมีหน้าที่สำคัญในการให้ความเคารพสิทธิของนักเรียนในการใช้สิทธิตามกฎหมาย เช่น สิทธิขอเข้าถึงข้อมูล (มาตรา 30) สิทธิขอให้แก้ไขข้อมูล (มาตรา 35–36) สิทธิขอลบข้อมูล (มาตรา 33) หรือสิทธิระงับการใช้ข้อมูล (มาตรา 34) ในทางปฏิบัติ โรงเรียนต้องจัดทำระบบที่รองรับคำร้องเหล่านี้โดยตรงและกำหนดผู้รับผิดชอบที่ชัดเจน เพื่อให้การตอบสนองต่อคำร้องเป็นไปภายในระยะเวลาที่กฎหมายกำหนด มิฉะนั้นอาจเข้าข่ายละเมิดสิทธิ และนักเรียนหรือผู้ปกครองสามารถร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญได้ทันทีตามที่กฎหมายกำหนด

2. ความท้าทายด้านการบริหารจัดการข้อมูลนักเรียน

การปฏิบัติหน้าที่ของสถานศึกษามักต้องเผชิญกับความท้าทายหลายประการ ซึ่งส่วนใหญ่เกิดจากโครงสร้างการบริหารจัดการของโรงเรียนไทยและความไม่พร้อมด้านความรู้ของบุคลากร

(1) ความท้าทายด้านความไม่พร้อมของบุคลากรและความรู้ด้านกฎหมาย โดยเฉพาะในโรงเรียนขนาดเล็กที่เผชิญข้อจำกัดด้านงบประมาณ บุคลากร สื่อการสอน เทคโนโลยี และสถานที่ ทำให้การจัดการเรียนรู้และพัฒนาคุณภาพการศึกษาทำได้ไม่เต็มศักยภาพ (กัญจนา สัณฐาน และ ประกอบ คุณารักษ์, 2563: 98-99) อีกทั้งไม่มีผู้เชี่ยวชาญด้านการคุ้มครองข้อมูล อาจทำให้การตีความกฎหมาย เช่น มาตรา 19–26 เกี่ยวกับความยินยอมและการเก็บข้อมูลคลาดเคลื่อนหรือไม่ถูกต้อง นอกจากนี้ หลายโรงเรียนยังไม่มีความเข้าใจว่าการใช้แพลตฟอร์มออนไลน์ของเอกชน เช่น Google Classroom หรือ Zoom นับเป็นการ “โอนข้อมูลไปต่างประเทศ” ซึ่งอาจต้องอยู่ภายใต้มาตรา 28 ที่กำหนดให้ประเทศปลายทางต้องมีมาตรฐานคุ้มครองข้อมูลที่เพียงพอ

(2) ความท้าทายในการจัดการฐานข้อมูลที่กระจัดกระจาย (data fragmentation) โดยทั่วไปโรงเรียนมักมีข้อมูลที่ถูกเก็บไว้ในหลายระบบ เช่น ระบบงานทะเบียน ระบบกิจกรรมพัฒนาผู้เรียน ระบบสุขภาพ ระบบ LMS ระบบงานวินัย รวมถึงแฟ้มเอกสารของครูประจำชั้น การกระจัดกระจายเช่นนี้ทำให้โรงเรียนไม่สามารถควบคุมการเข้าถึงข้อมูลได้อย่างมีประสิทธิภาพ และทำให้การตอบสนองต่อคำร้องขอใช้สิทธิของนักเรียนเป็นไปอย่างยากลำบาก อีกทั้งยังเพิ่มความเสี่ยงของการใช้ข้อมูลผิดวัตถุประสงค์โดยบุคลากรที่ไม่เกี่ยวข้อง ซึ่งถือเป็นการละเมิดตามมาตรา 27

(3) ปัญหาการเก็บข้อมูลเกินความจำเป็น (over-collection) ก็ปรากฏอย่างกว้างขวางในสถานศึกษา เช่น การขอข้อมูลสุขภาพที่ละเอียดเกินควร การขอสำเนาบัตรประชาชนหลายครั้ง หรือการบันทึกข้อมูลพฤติกรรมรายวันโดยไม่จำเป็น การกระทำเช่นนี้ขัดต่อหลักการตามมาตรา 22 ที่กำหนดให้โรงเรียนเก็บข้อมูลเท่าที่จำเป็นต่อภารกิจทางการศึกษาเท่านั้น นอกจากนี้ ยังมีปัญหาความยากลำบากในการลบหรือระงับข้อมูล โดยเฉพาะเมื่อข้อมูลถูกจัดเก็บในระบบกลางของกระทรวงหรือระบบของบริษัทเอกชน โรงเรียนอาจไม่มีสิทธิ์ลบหรือแก้ไขข้อมูลได้ด้วยตนเอง แม้เป็นคำร้องของเจ้าของข้อมูลตามมาตรา 33 ซึ่งสร้างความท้าทายด้านความรับผิดชอบของโรงเรียนว่าใครเป็นผู้ควบคุมข้อมูลที่แท้จริงในระบบลักษณะดังกล่าว

(4) ปัญหาด้านจริยธรรมในการจัดการข้อมูลผู้เยาว์ การใช้ข้อมูลเด็กจำเป็นต้องอาศัยหลักการ “ผลประโยชน์สูงสุดของผู้เยาว์” และไม่ควรนำข้อมูลไปใช้ในลักษณะที่อาจสร้างตราบาปหรือจำกัดโอกาสในอนาคต เช่น การเก็บข้อมูลพฤติกรรมเชิงลบเป็นเวลานานเกินควร การเผยแพร่ภาพนักเรียนที่อาจกระทบต่อศักดิ์ศรีความเป็นมนุษย์ หรือการใช้ระบบวิเคราะห์ข้อมูลเพื่อประเมินความเสี่ยงของเด็กโดยไม่มีมาตรการกำกับอย่างเข้มงวด สถานศึกษาจึงต้องให้ความสำคัญกับความละเอียดอ่อนของข้อมูลเด็ก ไม่เพียงแต่ในเชิงกฎหมาย แต่รวมถึงในมิติของคุณธรรมและจริยธรรมทางการศึกษา

โดยสรุป บทบาทของสถานศึกษาในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีความซับซ้อนทั้งด้านกฎหมาย เทคโนโลยี การบริหารจัดการ และจริยธรรม การปฏิบัติตามกฎหมายอย่างมีประสิทธิภาพจำเป็นต้องอาศัยความเข้าใจเชิงลึกของบุคลากร การออกแบบระบบข้อมูลที่สอดคล้องกับหลักความจำเป็นและความปลอดภัย ตลอดจนการสร้างวัฒนธรรมภายในสถานศึกษาที่เคารพสิทธิของนักเรียนในฐานะเจ้าของข้อมูลส่วนบุคคลอย่างแท้จริง

การเปรียบเทียบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศกับบริบทสิทธิของนักเรียนในสถานศึกษา

การคุ้มครองข้อมูลส่วนบุคคลของผู้เรียนเป็นประเด็นระดับสากลที่ทุกประเทศต้องเผชิญอย่างจริงจัง โดยเฉพาะในยุคที่สถานศึกษาใช้ระบบดิจิทัล แพลตฟอร์มออนไลน์ และระบบจัดเก็บข้อมูลที่มีความซับซ้อนมากขึ้น ประเทศต่าง ๆ จึงพัฒนากฎหมายข้อมูลส่วนบุคคลเพื่อให้สอดรับกับสิทธิของผู้เรียนในฐานะกลุ่มเปราะบาง ซึ่งจำเป็นต้องได้รับความคุ้มครองมากกว่าบุคคลทั่วไป ใน

หัวข้อนี้ผู้เขียนมุ่งเปรียบเทียบกฎหมายสำคัญของต่างประเทศ ได้แก่ GDPR, FERPA, COPPA ตลอดจนกฎหมายข้อมูลส่วนบุคคลของสิงคโปร์ เกาหลีใต้ และญี่ปุ่น เพื่อวิเคราะห์บทเรียนที่ประเทศไทยสามารถนำมาปรับใช้เพื่อยกระดับการคุ้มครองข้อมูลของนักเรียนให้มีมาตรฐานสูงขึ้น

1. GDPR (สหภาพยุโรป): สิทธิของเด็กและความเข้มงวดด้านการยินยอม

GDPR หรือ General Data Protection Regulation ของสหภาพยุโรปถือเป็นกรอบกฎหมายที่ได้รับการยอมรับว่ามีความเข้มงวดที่สุดในโลก โดยได้กำหนดสิทธิของเด็กไว้อย่างชัดเจนว่าเป็น “กลุ่มผู้มีความเปราะบางสูง” (vulnerable data subjects) ซึ่งต้องได้รับมาตรการคุ้มครองพิเศษเมื่อมีการประมวลผลข้อมูลส่วนบุคคล เนื่องจากเด็กมักมีความตระหนักรู้เกี่ยวกับความเสี่ยง ผลกระทบที่อาจเกิดขึ้น และกลไกการคุ้มครองสิทธิของตนในบริบทของข้อมูลส่วนบุคคลน้อยกว่า จึงจำเป็นต้องมีมาตรการคุ้มครองที่เข้มงวดและเหมาะสมกับวัย (นคร เสรีรักษ์ และคณะ, 2562: 20) อีกทั้งกำหนดอายุขั้นต่ำในการให้ความยินยอมสำหรับบริการออนไลน์ที่มีลักษณะเป็น “information society services” ไว้ที่ 16 ปี แต่เปิดโอกาสให้ประเทศสมาชิกกำหนดอายุขั้นต่ำที่ 13 ปีได้ ซึ่งเรียกว่า age of digital consent (ปุญณิศา เข็มทอง, 2565: 427)

ในทางปฏิบัติ GDPR กำหนดให้การเก็บข้อมูลเด็กต้องอาศัยความยินยอมของผู้ปกครอง ผู้ควบคุมข้อมูลต้องสื่อสารกับเด็กและผู้ปกครองด้วยภาษาที่เหมาะสม เข้าใจง่าย ข้อมูลเกี่ยวกับเด็กมักถูกจัดอยู่ในข้อมูลที่ต้องมีมาตรการสูงสุด โดยเฉพาะข้อมูลสุขภาพ ข้อมูลชีวภาพ และข้อมูลพฤติกรรมในสภาพแวดล้อมการเรียนรู้

นอกจากนี้ GDPR ยังมีหลัก “data protection by design and by default” ตามมาตรา 25 แห่ง GDPR มุ่งให้ผู้ควบคุมข้อมูลคำนึงถึงความเป็นส่วนตัวตั้งแต่ขั้นออกแบบระบบและตั้งค่าการประมวลผลให้อยู่ในระดับต่ำสุดเท่าที่จำเป็น สอดคล้องหลักการจำกัดวัตถุประสงค์และการใช้ข้อมูลเท่าที่จำเป็น (European Union, 2025: online) สถานศึกษาจึงต้องออกแบบระบบเรียนออนไลน์ให้ปลอดภัยตั้งแต่ต้น เช่น การปิดระบบบันทึกภาพโดยอัตโนมัติ หรือจำกัดสิทธิผู้ใช้เฉพาะบุคลากรจำเป็นเท่านั้น บทเรียนที่สำคัญสำหรับไทยคือการกำหนดมาตรฐานการยินยอมของเด็กและระบบป้องกันข้อมูลตั้งแต่ขั้นตอนออกแบบระบบ ซึ่งปัจจุบันสถานศึกษาไทยยังไม่มีกลไกบังคับใช้ที่เข้มแข็งเช่นนี้

2. FERPA (สหรัฐอเมริกา): สิทธิของผู้เรียนในการควบคุมข้อมูลการศึกษา

FERPA หรือ Family Educational Rights and Privacy Act เป็นกฎหมายเฉพาะของสหรัฐอเมริกาเกี่ยวกับการคุ้มครองข้อมูลการศึกษา (education records) ซึ่งให้สิทธิสำคัญแก่ผู้เรียนและผู้ปกครอง (U.S. DEPARTMENT OF EDUCATION, 2025: online) ได้แก่ สิทธิขอเข้าถึงข้อมูลการศึกษา สิทธิขอแก้ไขข้อมูลที่ไม่ถูกต้อง สิทธิห้ามไม่ให้สถานศึกษาเปิดเผยข้อมูลต่อบุคคลอื่นโดยไม่ได้รับความยินยอม

FERPA กำหนดว่าสถานศึกษาไม่อาจเปิดเผยข้อมูลผู้เรียน แม้เพียงบางส่วน เช่น คะแนนสอบ หมายเลขประจำตัวนักเรียน หรือข้อมูลวินัย ยกเว้นในกรณีที่ผู้เรียนอายุเกิน 18 ปีและให้ความยินยอม หรือมีข้อยกเว้นเฉพาะที่กฎหมายกำหนด เช่น เพื่อความปลอดภัยเร่งด่วน

ลักษณะโดดเด่นของ FERPA คือการจำแนกข้อมูลการศึกษาอย่างเข้มงวด (education records) และกำหนดโทษทางปกครอง เช่น การตัดถอนเงินอุดหนุนหากสถานศึกษาละเมิด FERPA อย่างร้ายแรง ซึ่งเป็นกลไกบังคับใช้ที่มีประสิทธิผลมากกว่าการกำหนดโทษทางแพ่งอย่างเดียว บทเรียนสำคัญต่อไทยคือการสร้างระบบการกำกับดูแลที่มี “แรงจูงใจและแรงกดดัน” ให้สถานศึกษาปฏิบัติตามอย่างจริงจัง มิใช่อาศัยเพียงข้อกำหนดเชิงหลักการ

3. COPPA (สหรัฐอเมริกา): การเก็บข้อมูลเด็กอายุต่ำกว่า 13 ปีบนแพลตฟอร์มออนไลน์

COPPA หรือ Children’s Online Privacy Protection Act เป็นกฎหมายที่มุ่งคุ้มครองข้อมูลเด็กอายุต่ำกว่า 13 ปี ที่ใช้บริการออนไลน์ของผู้ประกอบการเว็บไซต์และผู้ให้บริการอินเทอร์เน็ต (ฉัตรฑริกา นภาธนาพงศ์ และ อัชราภรณ์ อริยสุนทร, 2566: 662) โดยกำหนดให้ผู้ให้บริการออนไลน์ต้องขอความยินยอมจาก “ผู้ปกครอง” ก่อนเก็บข้อมูลเด็ก (Topelson, D., et al, 2013: online) เปิดเผยนโยบายความเป็นส่วนตัวอย่างโปร่งใส เก็บข้อมูลเท่าที่จำเป็น ห้ามใช้ข้อมูลเด็กเพื่อการโฆษณาเชิงพฤติกรรม (behavioral advertising)

กฎหมายนี้สร้างผลกระทบอย่างมากต่อผู้ให้บริการแพลตฟอร์ม เช่น YouTube, Google, Roblox ซึ่งต้องเปลี่ยนแนวทางการเก็บข้อมูลเด็กอย่างมาก COPPA จึงเป็นกรอบสำคัญสำหรับสถานศึกษาไทย เมื่อใช้แพลตฟอร์มออนไลน์ของเอกชนในการจัดการเรียนการสอน เช่น Google Classroom หรือระบบประชุมออนไลน์ที่บันทึกภาพนักเรียน เพราะกฎหมายไทยยังไม่มีข้อกำหนดเฉพาะสำหรับแพลตฟอร์มดิจิทัลที่ใช้งานกับเด็กอย่างชัดเจน

4. กฎหมายของสิงคโปร์ เกาหลีใต้ และญี่ปุ่น

(1) สิงคโปร์ – PDPA และแนวปฏิบัติในสถานศึกษา

กฎหมาย PDPA 2012 ของสิงคโปร์ วางหลักคุ้มครองข้อมูลส่วนบุคคลที่เข้มงวดและครอบคลุมทุกองค์กรรวมถึง “สถานศึกษา” ซึ่งถูกจัดเป็น education institution ตามนิยามในมาตรา 2 (Personal Data Protection Act, 2012) โดยกำหนดให้สถานศึกษาต้องเก็บ ใช้ และเปิดเผยข้อมูลเฉพาะเท่าที่จำเป็นและเพื่อวัตถุประสงค์ที่แจ้งให้นักเรียนทราบล่วงหน้า (มาตรา 20) สิทธิสำคัญของนักเรียน เช่น สิทธิขอเข้าถึงข้อมูล (มาตรา 21) และสิทธิขอแก้ไขข้อมูล (มาตรา 22) ช่วยป้องกันการใช้ข้อมูลโดยพลการของโรงเรียน นอกจากนี้ PDPA กำหนดให้มี “การยินยอม” ก่อนการเก็บข้อมูล และต้องไม่เก็บเกินความจำเป็น (มาตรา 13–18) ซึ่งส่งผลโดยตรงต่อการคุ้มครองนักเรียนในยุคดิจิทัล เช่น แพลตฟอร์มการเรียนออนไลน์และระบบประเมินผล

เมื่อเทียบกับไทย ภายใต้ PDPA พ.ศ. 2562 แม้มีหลักการคล้ายคลึงกัน แต่ยังไม่มี “แนวปฏิบัติเฉพาะด้านสถานศึกษา” เช่นของสิงคโปร์ ทำให้โรงเรียนไทยมีความคลุมเครือในการตีความ โดยเฉพาะเรื่องการยินยอมแทนโดยผู้ปกครองและมาตรฐานความปลอดภัยข้อมูล ส่งผลให้การคุ้มครองสิทธิของนักเรียนยังไม่สม่ำเสมอในทางปฏิบัติ ต่างจากสิงคโปร์ที่มีระบบกำกับชัดเจนและเป็นรูปธรรมกว่า

(2) เกาหลีใต้ – PIPA และการคุ้มครองข้อมูลเด็กในระบบดิจิทัล

กฎหมาย PIPA ของเกาหลีใต้ ให้ความสำคัญอย่างยิ่งต่อสิทธิของเจ้าของข้อมูล โดยเฉพาะกรณี “ผู้เยาว์” และการใช้ข้อมูลในบริบทสถานศึกษา ซึ่งองค์กรทุกประเภทรวมทั้งโรงเรียน ต้องปฏิบัติตามมาตรการด้านความปลอดภัย การจำกัดวัตถุประสงค์ และการยินยอมอย่างเคร่งครัด หนึ่งในหลักสำคัญคือ การกำหนดให้ “ผู้แทนโดยชอบธรรม” มีสิทธิดำเนินการแทนผู้เยาว์อายุต่ำกว่า 14 ปีในการเข้าถึง แก้ไข หรือตรวจสอบข้อมูลตาม มาตรา 38(2) (Korean Personal Information Protection Act, 2011) ขณะเดียวกัน มาตรา 22(5) กำหนดว่าการเก็บและใช้ข้อมูลของผู้เยาว์ต้องได้รับความยินยอมจากผู้แทนโดยชอบธรรมก่อนเสมอ ซึ่งถือเป็นหลักที่สำคัญต่อบริบทโรงเรียน เนื่องจากข้อมูลนักเรียนถูกประมวลผลในระบบการเรียนการสอน การประเมินผล และกิจกรรมออนไลน์อย่างต่อเนื่อง

นอกจากนี้ PIPA ยังวางหลักด้าน “สิทธิในการเข้าถึง–แก้ไข–ลบ–จำกัดการประมวลผล” ซึ่งโรงเรียนต้องจัดช่องทางให้ผู้เยาว์หรือผู้แทนโดยชอบธรรมใช้สิทธิได้จริง พร้อมทั้งกำหนดให้ผู้ควบคุมข้อมูลต้องมีมาตรการด้านความปลอดภัยที่เพียงพอ เช่น การควบคุมผู้ประมวลผลข้อมูลและการอบรมบุคลากร

เมื่อเทียบกับไทย แม้ PDPA พ.ศ. 2562 จะมีหลักการคล้ายกัน แต่ยังขาด “ข้อกำหนดเฉพาะด้านการศึกษา” เหมือนที่เกาหลีใต้กำหนดไว้อย่างชัดเจน ส่งผลให้สถานศึกษาไทยยังตีความและปฏิบัติไม่เป็นเอกภาพ โดยเฉพาะประเด็นการยินยอมแทนและการจัดการข้อมูลดิจิทัลของนักเรียนในยุคแพลตฟอร์มออนไลน์

(3) ญี่ปุ่น – Act on Protection of Personal Information (APPI)

กฎหมาย APPI ของญี่ปุ่น มุ่งคุ้มครองสิทธิของบุคคลในยุคสังคมสารสนเทศขั้นสูง โดยวางหลักให้ผู้ควบคุมข้อมูลต้อง “ระบุวัตถุประสงค์การใช้ข้อมูลให้ชัดเจน” (Article 15) และห้ามใช้ข้อมูลเกินขอบเขตที่ระบุไว้โดยไม่ได้รับความยินยอม (Article 16) (Act on the Protection of Personal Information, 2003) หลักนี้มีความสำคัญต่อสถานศึกษา เนื่องจากโรงเรียนและมหาวิทยาลัยเป็น “business operators handling personal information” ตามนิยามมาตรา 2 และต้องปฏิบัติตามข้อกำหนดเรื่องการเก็บ การใช้ และการเปิดเผยข้อมูลของนักเรียนอย่างเคร่งครัด นอกจากนี้ APPI กำหนดให้ผู้ควบคุมข้อมูลต้องมี “มาตรการควบคุมความปลอดภัย” เพื่อป้องกันการรั่วไหลหรือความเสียหายของข้อมูล ซึ่งเป็นหัวใจต่อระบบบริหารจัดการข้อมูลนักเรียนในโรงเรียนดิจิทัล เช่น ระบบทะเบียนนักเรียน การประเมินออนไลน์ และฐานข้อมูลสุขภาพนักเรียน

เมื่อเปรียบเทียบกับไทย ภายใต้ PDPA พ.ศ. 2562 แม้มีหลักการคล้ายคลึงกัน เช่น การระบุวัตถุประสงค์ การยินยอม และการใช้ข้อมูลเท่าที่จำเป็น แต่ไทยยังไม่มี “แนวทางเฉพาะภาคการศึกษา” แบบของญี่ปุ่น ส่งผลให้โรงเรียนไทยขาดแนวปฏิบัติที่ชัดเจนเกี่ยวกับข้อมูลนักเรียน ขณะที่ญี่ปุ่นแม้ APPI ไม่ได้ระบุเรื่อง “ข้อมูลเด็ก” โดยเฉพาะ แต่มีระบบตีความและแนวทางจากหน่วยงานที่ทำให้สถาบันการศึกษาใช้ APPI ได้อย่างเป็นรูปธรรมและสม่ำเสมอกว่าไทย

5. บทเรียนที่ประเทศไทยควรนำมาปรับใช้

จากการเปรียบเทียบกฎหมายต่างประเทศ พบประเด็นสำคัญที่ไทยควรนำมาพิจารณาเพื่อยกระดับการคุ้มครองข้อมูลของผู้เรียน ได้แก่

(1) จัดทำ “กฎหมายลำดับรองเฉพาะภาคการศึกษา” เพื่อคุ้มครองข้อมูลเด็กอย่างเป็นรูปธรรม จากกรณี GDPR, FERPA, COPPA และ PDPA ของสิงคโปร์–เกาหลีใต้–ญี่ปุ่น ล้วนมี “แนวปฏิบัติเฉพาะสำหรับสถานศึกษา” หรือกฎหมายเฉพาะ (sector-specific rules) ทำให้ผู้บริหารโรงเรียนเข้าใจหน้าที่และวิธีปฏิบัติได้ชัดเจน ไทยจึงควรออกประกาศ/กฎกระทรวงเฉพาะด้านการศึกษา เพื่อกำหนดมาตรฐานการเก็บ ใช้ เปิดเผย และจัดเก็บข้อมูลของนักเรียนอย่างเป็นระบบ

(2) ยกระดับมาตรฐานการ “ยินยอมแทนโดยผู้ปกครอง” สำหรับผู้เยาว์ GDPR กำหนด age of digital consent อย่าง

ชัดเจน และ COPPA กำหนดให้ผู้ปกครองต้องให้ “verifiable parental consent” ก่อนเก็บข้อมูลเด็กอายุต่ำกว่า 13 ปี ขณะที่ PIPA เกาหลีใต้กำหนดให้ผู้แทนโดยชอบธรรมใช้สิทธิแทนเด็กอายุต่ำกว่า 14 ปี ไทยควรกำหนดอายุและรูปแบบ “การยินยอมแทนที่ตรวจสอบได้” ในกิจกรรมดิจิทัล เช่น การใช้แพลตฟอร์ม, แอปเรียนออนไลน์ และระบบบันทึกภาพ

(3) กำหนดมาตรฐาน “data protection by design/default” สำหรับระบบโรงเรียนดิจิทัล ตาม GDPR และแนวปฏิบัติของสิงคโปร์ โรงเรียนต้องออกแบบระบบให้ปลอดภัยตั้งแต่ต้น เช่น ปิดฟังก์ชันบันทึกภาพอัตโนมัติ จำกัดสิทธิ์เฉพาะบุคลากรจำเป็น และลดการเก็บข้อมูลเกินจำเป็น ไทยควรบังคับใช้หลักนี้อย่างเป็นทางการในทุกโรงเรียน ทั้งรัฐและเอกชน

(4) สร้างกลไกกำกับและลงโทษที่มีประสิทธิภาพ FERPA ใช้ระบบ “ตัดเงินอุดหนุน” เป็นแรงกดดัน ทำให้สถานศึกษาปฏิบัติตามกฎหมายอย่างจริงจัง ไทยควรมีมาตรการลงโทษที่เป็นรูปธรรม เช่น เงื่อนไขงบประมาณ การตรวจประเมิน หรือคะแนนมาตรฐานความปลอดภัยข้อมูลของโรงเรียน

(5) พัฒนาความรู้และระบบอบรมบุคลากรสถานศึกษา ทั้งสิงคโปร์ เกาหลีใต้ และญี่ปุ่นเน้นการอบรมเจ้าหน้าที่ การกำกับผู้ประมวลผลข้อมูล และการสื่อสารกับผู้ปกครอง–นักเรียนอย่างโปร่งใส ไทยควรจัดทำหลักสูตรอบรมบังคับสำหรับครูและผู้ดูแลระบบเพื่อเพิ่มความพร้อมด้านการคุ้มครองข้อมูลส่วนบุคคลในทุกระดับสถานศึกษา

ด้วยบทเรียนเหล่านี้ ประเทศไทยจะสามารถยกระดับการคุ้มครองข้อมูลของนักเรียนให้มีความสอดคล้องกับมาตรฐานสากล และสร้างระบบการศึกษาที่เคารพศักดิ์ศรีของผู้เรียนในฐานะเจ้าของข้อมูลส่วนบุคคลอย่างแท้จริง

การประยุกต์ใช้ PDPA ในสถานศึกษาไทย: ปัญหาเชิงโครงสร้างและแนวโน้มการปรับตัวในยุคดิจิทัล

การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ได้นำมาซึ่งความเปลี่ยนแปลงสำคัญต่อโครงสร้างการบริหารจัดการข้อมูลในสถานศึกษาไทย เนื่องจากโรงเรียนเป็นผู้ควบคุมข้อมูลส่วนบุคคล (data controller) ที่ต้องจัดเก็บข้อมูลของนักเรียนจำนวนมาก ครอบคลุมตั้งแต่ข้อมูลทั่วไปจนถึงข้อมูลอ่อนไหวตามมาตรา 26 เช่น ข้อมูลสุขภาพ ข้อมูลพฤติกรรม หรือข้อมูลชีวภาพที่เกิดจากระบบสแกนใบหน้า การประยุกต์ใช้ PDPA จึงเป็นภารกิจที่โรงเรียนต้องปรับระบบการจัดการทั้งด้านนโยบาย เทคโนโลยี และบุคลากร แต่การดำเนินการดังกล่าวกลับพบปัญหาเชิงโครงสร้างหลายประการที่สะท้อนถึงความพร้อมที่ยังไม่เพียงพอของระบบการศึกษาไทยในการเข้าสู่ยุคข้อมูลส่วนบุคคลเป็นศูนย์กลาง

(1) ปัญหาการกำหนดนโยบายข้อมูลส่วนบุคคลที่ไม่ชัดเจน โรงเรียนส่วนใหญ่ยังไม่มีการแจ้งนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice หรือ Privacy Policy) ในการจัดเก็บข้อมูลให้เจ้าของข้อมูลทราบ (ปพิชญา แจงจำรูญ, 2566: 58) รวมทั้งไม่มีประกาศนโยบายการประมวลผลข้อมูล (privacy notice) ที่ครอบคลุมตามข้อกำหนดของมาตรา 23 เช่น การแจ้งวัตถุประสงค์ ระยะเวลาการเก็บข้อมูล สิทธิของเจ้าของข้อมูล และข้อมูลผู้ควบคุมข้อมูลอย่างครบถ้วน แม้บางโรงเรียนจะมีแบบฟอร์มขอความยินยอมจากผู้ปกครอง แต่การร่างเอกสารมักใช้รูปแบบที่คัดลอกมาจากหน่วยงานอื่นโดยไม่ตรงกับกิจกรรมของโรงเรียนจริง เช่น การบันทึกภาพกิจกรรม การใช้แพลตฟอร์มออนไลน์ หรือการส่งข้อมูลให้บริษัทเทคโนโลยี ทำให้ความยินยอมไม่เป็น “ informed consent” ตามหลักกฎหมาย นอกจากนี้ โรงเรียนจำนวนมากยังเก็บข้อมูลเกินความจำเป็น (over-collection) ขัดกับหลักมาตรา 22 และไม่มีระบบกำหนดอายุข้อมูลตามมาตรา 33 ว่าข้อมูลใดต้องลบหรือทำให้ไม่สามารถระบุตัวบุคคลได้เมื่อหมดความจำเป็น

(2) ปัญหาการขาดเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ซึ่งเป็นข้อบังคับในกรณีที่โรงเรียนมีการประมวลผลข้อมูลจำนวนมากหรือข้อมูลอ่อนไหวตามมาตรา 41 แม้โรงเรียนจำนวนไม่น้อยจะเข้าเงื่อนไขต้องแต่งตั้ง DPO แต่กลับไม่มีบุคลากรที่มีความรู้เพียงพอหรือถูกแต่งตั้งอย่างเป็นทางการ ทำให้ไม่มีผู้ทำหน้าที่ตรวจสอบกระบวนการประมวลผล ให้คำปรึกษา และรายงานปัญหาการละเมิดข้อมูลตามหน้าที่ตามมาตรา 42 สถานศึกษาจำนวนมากยังเห็นว่า PDPA เป็นเพียง “กฎหมายไอที” ทั้งที่แท้จริงแล้วเป็นกฎหมายเชิงสิทธิมนุษยชนที่ครูและผู้บริหารต้องเข้าใจในระดับนโยบาย ไม่ใช่เพียงมอบให้ฝ่ายไอทีรับผิดชอบ

(3) ความไม่เข้าใจของครูและผู้บริหาร ซึ่งเป็นอุปสรรคหลักต่อการปฏิบัติตามกฎหมาย แม้ว่าครูต้องจัดการข้อมูลจำนวนมากในชีวิตประจำวัน เช่น การถ่ายรูปนักเรียน การส่งงานผ่านช่องทางออนไลน์ การจัดทำประวัติผลการเรียน หรือการใช้แพลตฟอร์มประชุมทางไกล แต่โรงเรียนส่วนใหญ่ไม่ได้ให้การอบรมเกี่ยวกับ PDPA อย่างเป็นระบบ ทำให้เกิดความเข้าใจผิด เช่น การสันนิษฐานว่าผู้ปกครองให้ความยินยอมโดยปริยาย หรือเชื่อว่าข้อมูลนักเรียนเป็น “ข้อมูลของโรงเรียน” สามารถใช้ได้ตามความเหมาะสม ทั้งที่ตามมาตรา 19 สิทธิในข้อมูลยังคงเป็นของเจ้าของข้อมูลเสมอ ปัญหานี้ทำให้เกิดความเสี่ยงต่อการละเมิดข้อมูลโดยไม่เจตนา เช่น การใช้ LINE ส่วนตัวติดต่อผู้เรียน การส่งข้อมูลผ่านโทรศัพท์มือถือส่วนบุคคล หรือการแชร์รูปนักเรียนลงสื่อสังคมออนไลน์โดยไม่ได้รับความยินยอม ซึ่งการมีความรู้พื้นฐานเกี่ยวกับกฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล จะช่วยลดผลกระทบที่อาจเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล (วรัชญ์ตะวันทร์ ชัยรัตน์ และคณะ, 2567: 446)

(4) ปัญหาการรายงานเหตุละเมิดข้อมูล (data breach) ที่ไม่เป็นระบบ ซึ่งขัดกับหน้าที่ตามมาตรา 37 (4) ที่กำหนดให้ต้อง

แจ้งสำนักงานภายใน 72 ชั่วโมง เมื่อเกิดเหตุรั่วไหลหรือเข้าถึงข้อมูลโดยมิชอบ ในทางปฏิบัติ โรงเรียนส่วนใหญ่ไม่รู้ว่ากรณีใดเข้าข่าย data breach หรือใครเป็นผู้มีอำนาจรายงาน ทำให้หลายเหตุการณ์ไม่ได้รับการแจ้ง เช่น โทรศัพท์ครูหาย ภาพนักเรียนถูกแชร์ต่อโดยไม่ได้เจตนา หรือฐานข้อมูลนักเรียนรั่วไหลจากระบบที่มีความปลอดภัยต่ำ ความไม่มีระบบรายงานทำให้ความเสียหายต่อผู้เรียนไม่ถูกบรรเทา และโรงเรียนเองก็ไม่พัฒนามาตรการป้องกันที่ดีขึ้น

(5) ความเสี่ยงจากอุปกรณ์ของครูและแพลตฟอร์มเอกชน (BYOD – Bring Your Own Device) ครูจำนวนมากใช้โทรศัพท์มือถือส่วนตัวถ่ายภาพ ส่งงาน หรือเก็บข้อมูลผู้เรียน ซึ่งนำไปสู่ความเสี่ยงต่อการสูญหาย การแฮ็ก หรือการเข้าถึงโดยบุคคลไม่เกี่ยวข้อง โรงเรียนจำนวนมากไม่มีแนวปฏิบัติด้าน “mobile device policy” หรือมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1) ทำให้เกิดช่องโหว่ด้านความปลอดภัยอย่างมาก นอกจากนี้ การใช้แพลตฟอร์มเช่น Google, Zoom, Microsoft Teams หรือแอปสื่อสารอย่าง LINE ยังไม่มีการตรวจสอบด้านความปลอดภัยหรือการส่งข้อมูลไปต่างประเทศตามมาตรา 28–29 ส่งผลให้สถานศึกษามีความเสี่ยงทางกฎหมายโดยไม่รู้ตัว

อย่างไรก็ตาม แนวโน้มในอนาคตสะท้อนการปรับตัวของสถานศึกษาอย่างค่อยเป็นค่อยไป โดยเริ่มมีการวางระบบที่ยั่งยืนมากขึ้น เช่น การพัฒนาระบบจัดเก็บข้อมูลกลาง ให้เป็นระบบศูนย์รวม (centralized data management) ลดปัญหาข้อมูลกระจัดกระจายและช่วยให้ควบคุมสิทธิการเข้าถึงได้ง่ายขึ้น อีกทั้งมีแนวโน้มเพิ่มการจัดอบรม PDPA ให้แก่ครูและผู้บริหารอย่างต่อเนื่อง เพื่อให้เข้าใจสิทธิของนักเรียนและภาระหน้าที่ของโรงเรียนตามกฎหมาย โรงเรียนจำนวนหนึ่งเริ่มกำหนด มาตรฐานด้านความปลอดภัยไอที เช่น การตั้งรหัสเข้มงวด การเก็บภาพนักเรียนในระบบกลางแทนมือถือครู และการจำกัดผู้เข้าถึงข้อมูล นอกจากนี้ ยังเริ่มมีการปลูกฝัง วัฒนธรรมการคุ้มครองข้อมูลส่วนบุคคลภายในโรงเรียน เช่น นโยบายไม่ถ่ายภาพนักเรียนโดยไม่จำเป็น นโยบายห้ามใช้ LINE ส่วนตัวกับผู้เรียน และการสร้างความตระหนักถึงสิทธิของผู้เรียนตามกฎหมาย ในภาพรวมแม้สถานศึกษาไทยยังเผชิญปัญหาการประยุกต์ใช้ PDPA อย่างกว้างขวาง แต่แนวโน้มการปรับตัวเชิงนโยบายและเชิงปฏิบัติที่เริ่มปรากฏชี้ให้เห็นว่า ระบบการศึกษาไทยกำลังพัฒนาไปสู่รูปแบบที่ให้ความสำคัญกับสิทธิของนักเรียนมากขึ้น การยกระดับโครงสร้างการบริหารข้อมูลจึงไม่ใช่เพียงข้อกฎหมาย แต่เป็นการเสริมสร้างความปลอดภัย ศักดิ์ศรี และความเป็นส่วนตัวของผู้เรียนในโลกยุคดิจิทัลอย่างแท้จริง

สรุป

การคุ้มครองข้อมูลส่วนบุคคลของนักเรียนภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นประเด็นที่สะท้อนการเปลี่ยนผ่านของสถานศึกษาไทยจากระบบบริหารที่เน้นเอกสารและการใช้อำนาจตามประเพณี มาสู่ระบบที่ให้ความสำคัญกับสิทธิของผู้เรียนในฐานะเจ้าของข้อมูลอย่างแท้จริง โดยบทบัญญัติตั้งแต่มาตรา 19–26 และมาตรา 30–39 ทำให้เห็นชัดว่าโรงเรียนมิใช่เพียงหน่วยบริการทางการศึกษา แต่เป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ที่ต้องดำเนินการอย่างรอบคอบ มีระบบแจ้งวัตถุประสงค์ การเก็บข้อมูลเท่าที่จำเป็น การจัดให้ใช้สิทธิตามกฎหมาย และการรักษาความมั่นคงปลอดภัยตามมาตรา 37 อย่างเคร่งครัด สิทธิของนักเรียน เช่น สิทธิขอเข้าถึงข้อมูล (มาตรา 30) สิทธิขอรับข้อมูลและโอนข้อมูล (มาตรา 31) สิทธิคัดค้าน (มาตรา 32) สิทธิขอลบข้อมูล (มาตรา 33) และสิทธิระงับการใช้ข้อมูล (มาตรา 34) เป็นกลไกสำคัญที่เปลี่ยนความสัมพันธ์เชิงอำนาจระหว่างโรงเรียนกับผู้เรียน ให้เกิดการใช้ข้อมูลอย่างโปร่งใสและตรวจสอบได้

อย่างไรก็ดี การปรับใช้ PDPA ภายในสถานศึกษาไทยยังเผชิญปัญหาเชิงโครงสร้างหลายด้าน ทั้งความไม่พร้อมของนโยบาย การขาดความเชี่ยวชาญความรู้เชิงลึกของบุคลากร ระบบรักษาความมั่นคงปลอดภัยของข้อมูล การใช้แพลตฟอร์มเอกชนที่มีความเสี่ยงด้านการส่งข้อมูลไปต่างประเทศ (มาตรา 28–29) และความเข้าใจคลาดเคลื่อนของครูผู้สอนซึ่งต้องจัดการข้อมูลในชีวิตประจำวัน นอกจากนี้ กลไกการแจ้งเหตุละเมิดข้อมูลตามมาตรา 37 (4) ยังไม่เป็นระบบ ทำให้โรงเรียนไม่สามารถตอบสนองต่อเหตุการณ์ที่กระทบต่อสิทธิของนักเรียนได้อย่างทันท่วงที การเปรียบเทียบกับกรอบกฎหมายต่างประเทศ เช่น GDPR, FERPA, COPPA และกฎหมายของสิงคโปร์หรือญี่ปุ่น ทำให้เห็นว่าประเทศไทยยังจำเป็นต้องพัฒนาแนวทางเชิงสถาบันและเชิงนโยบายอีกมากก่อนจะก้าวสู่มาตรฐานสากลในการคุ้มครองข้อมูลผู้เยาว์ในยุคดิจิทัล

ทิศทางการศึกษาในครั้งต่อไป ควรมีการดำเนินวิจัยเชิงสำรวจ (Survey Research) หรือ กรณีศึกษา (Case Study) เพื่อประเมินระดับความรู้ ความเข้าใจ และความพร้อมของครูและผู้บริหารสถานศึกษาไทยต่อการปฏิบัติตาม PDPA ในเชิงปริมาณและเชิงประจักษ์ การวิจัยดังกล่าวจะช่วยยืนยันประเด็นท้าทายที่ได้จากการวิเคราะห์บทความนี้ รวมถึงสะท้อนช่องว่างด้านความรู้ ความตระหนัก และการปฏิบัติจริงในสถานศึกษา อันจะนำไปสู่การพัฒนานโยบายและแนวทางสนับสนุนที่เหมาะสมยิ่งขึ้นในอนาคต

2. ข้อเสนอแนะ

สำหรับสถานศึกษา ควรกำหนดนโยบาย PDPA สำหรับนักเรียนโดยเฉพาะ เพื่อเป็นกรอบการจัดเก็บ ใช้ เปิดเผย และปกป้องข้อมูลของผู้เรียนอย่างเป็นระบบ พร้อมทั้งจัดตั้งคณะกรรมการผู้รับผิดชอบข้อมูลส่วนบุคคลของโรงเรียน เพื่อให้มีหน่วยงาน

กำกับดูแลอย่างเป็นรูปธรรม ขณะเดียวกันรัฐบาลควรออกแนวทางปฏิบัติ (Guidelines) เฉพาะสำหรับสถานศึกษาที่มีความชัดเจน โดยให้ความสำคัญเป็นพิเศษต่อการเก็บและใช้ข้อมูลภาพถ่าย–วิดีโอของนักเรียน ซึ่งเป็นข้อมูลที่สถานศึกษามักใช้ในกิจกรรมประชาสัมพันธ์และการสื่อสารสาธารณะ จึงมีความเสี่ยงต่อการละเมิดสิทธิ หากไม่มีหลักเกณฑ์ที่ชัดเจนรองรับ เมื่อพิจารณาควบคู่กับความจำเป็นในการมีนโยบายและแนวทางปฏิบัติที่ชัดเจนทั้งในระดับโรงเรียนและระดับภาครัฐแล้ว สถานศึกษาจึงควรดำเนินมาตรการเพิ่มเติมดังต่อไปนี้ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลของนักเรียนเป็นไปอย่างรอบด้านและสอดคล้องตามกฎหมาย

(1) จัดทำ Privacy Notice ของสถานศึกษาให้ครบถ้วนตามมาตรา 23 ควรจัดทำประกาศที่ระบุวัตถุประสงค์ของการเก็บข้อมูล ระยะเวลาเก็บรักษา สิทธิของนักเรียน และหน่วยงานผู้ควบคุมข้อมูลอย่างชัดเจน โดยจัดให้เข้าถึงง่ายและใช้ภาษาที่เข้าใจได้ตามหลักมาตรา 19

(2) แต่งตั้งและพัฒนาศักยภาพเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โรงเรียนที่มีข้อมูลจำนวนมากหรือข้อมูลอ่อนไหวควรแต่งตั้ง DPO ตามมาตรา 41 และจัดอบรมต่อเนื่องเพื่อให้สามารถให้คำปรึกษา ตรวจสอบ และรายงานเหตุละเมิดตามมาตรา 42 ได้อย่างมีประสิทธิภาพ

(3) กำหนดนโยบายภายในเกี่ยวกับการเก็บ ใช้ เปิดเผย และลบข้อมูลอย่างเป็นระบบ ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1) เช่น การกำหนดสิทธิการเข้าถึง การตั้งรหัสผ่าน การเข้ารหัสข้อมูล การทบทวนอุปกรณ์ที่ใช้ทำงาน ตลอดจนกำหนดอายุข้อมูลและกระบวนการลบตามมาตรา 33

(4) จัดการความเสี่ยงจากการใช้แพลตฟอร์มและอุปกรณ์ของครู (BYOD Policy) ควรกำหนดข้อปฏิบัติในการใช้โทรศัพท์มือถือส่วนตัว ระบบรับส่งงานออนไลน์ และแอปพลิเคชันสื่อสาร เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ชอบ รวมทั้งตรวจสอบประเด็นการส่งข้อมูลไปต่างประเทศตามมาตรา 28–29

(5) อบรมครูและผู้บริหารเกี่ยวกับสิทธิของผู้เรียนและหน้าที่ของสถานศึกษา ควรจัดทำหลักสูตรอบรม PDPA สำหรับครูทุกระดับ เพื่อให้มีความเข้าใจเกี่ยวกับสิทธิของนักเรียน เช่น สิทธิคัดค้าน (มาตรา 32) หรือสิทธิขอลบข้อมูล (มาตรา 33) และสามารถตอบสนองคำร้องขอได้อย่างถูกต้อง

(6) พัฒนาระบบฐานข้อมูลกลางของโรงเรียนหรือของกระทรวงศึกษา การจัดระบบข้อมูลแบบรวมศูนย์ช่วยลดความซ้ำซ้อน ลดความเสี่ยงจากการกระจายข้อมูลในหลายแพลตฟอร์ม และเอื้อต่อการควบคุมและตรวจสอบตามมาตรา 39

(7) สร้างวัฒนธรรมคุ้มครองข้อมูลส่วนบุคคลภายในโรงเรียน ควรปลูกฝังแนวคิดว่าข้อมูลของนักเรียนเป็นสิทธิพื้นฐานที่ต้องให้ความเคารพ ไม่ใช่เพียงข้อมูลที่โรงเรียนสามารถใช้ตามดุลพินิจ เช่น หลีกเลี่ยงการถ่ายรูปนักเรียนโดยไม่จำเป็น การแชร์ข้อมูลในกลุ่มสื่อสารส่วนตัว หรือการเผยแพร่ข้อมูลผลการเรียนโดยเปิดเผย

เอกสารอ้างอิง

กัญจนา สัณฐาน และ ประกอบ คุณารักษ์. (2563). **กลยุทธ์การบริหารโรงเรียนประถมศึกษาขนาดเล็กในเขตพื้นที่ชนบทเพื่อพัฒนาคุณภาพการศึกษาตามจุดเน้นของนักเรียน**. วารสารรัชต์ภาคย์, 14(32), 97-113.

จิดาภา คีรีมาศทอง. (2568). **มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของเด็กในยุคดิจิทัล.** วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต. มหาวิทยาลัยศรีปทุม

ฉัตรฑริกา นภาธนาพงศ์ และ อัชราภรณ์ อริยสุนทร. (2566). **ปัญหาการบังคับใช้ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562: ศึกษากรณีการคุ้มครองข้อมูลส่วนบุคคลของเด็ก**. วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. 52(3), 640-670.

ชวิน อุ่นภัทร และ ปิยะบุตร บุญอร่ามเรือง. (2564). **Thailand Data Protection Guidelines 3.2 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับการวิจัยและสถิติ**. พิมพ์ครั้งที่ 1. กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

นคร เสรีรักษ์, ณรงค์ ใจหาญ, ประสิทธิ์ ปิวาวัฒนพานิช, ศุภเกียรติ ศุภศักดิ์ศึกษากร และ นิชานันท์ นันทศิริ ศรณ์. (2562). **GDPR ฉบับภาษาไทย**. พิมพ์ครั้งที่ 1. กรุงเทพฯ: บริษัท พี.เพรส จำกัด.

นพมาศ นิลแช่ม. (2568). **ปัญหาการคุ้มครองข้อมูลส่วนบุคคลของเด็กในยุคดิจิทัลของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562.** วารสารกฎหมายนิติพัฒน์ นิด้า. 14(1), 45-71.

ปพิชญา แจงจำรูญ. (2566). **ปัญหาในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : ศึกษากรณีสถานศึกษาขั้นพื้นฐานระดับมัธยมศึกษา**. วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต. จุฬาลงกรณ์มหาวิทยาลัย.

ปรีดา โชติมานนท์ และ สุขสมัย สุทธิบดี. (2566). **รูปแบบการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับผู้ประกอบการขนาดกลางและขนาดเล็ก (SMEs)**. วารสารรามคำแหง ฉบับบัณฑิตวิทยาลัย. 6(1), 15-26.

ปุญณิศา เข็มทอง. (2565). **มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของเด็กจากการเผยแพร่ภาพถ่ายและวิดีโอบนสื่อโซเชียลมีเดีย**. วารสารวิชาการสถาบันวิทยาการจัดการแห่งแปซิฟิค สาขามนุษยศาสตร์และสังคมศาสตร์. 8(3), 422-431.

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. (2562, 27 พฤษภาคม). **ราชกิจจานุเบกษา**, 136(69 ก), 52-95.

วรัชญ์ตะวันทร์ ชัยรัตน์, สุพรรณา ภัทรเมธาวรกุล, และณัฐธิดา คำประเสริฐ. (2025). **ปัจจัยที่ส่งผลต่อการตระหนักรู้และความเข้าใจเกี่ยวกับกฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลของนักศึกษาปริญญาตรีในมหาวิทยาลัยกรุงเทพธนบุรี**. วารสาร Dhamma for Life, 31(1). 446-470.

สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม. (2567). **สิทธิในการคัดค้านการใช้ข้อมูลส่วนบุคคล (Right to Object) ตามมาตรา 32 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562**. เข้าถึงเมื่อ 10 พฤศจิกายน 2568 จาก https://www.ops.go.th/th/ content_page/ item/10975-right-to-object-32-2562

Act on the Protection of Personal Information, 2003.

Bárbara da Rosa Lazarotto. (2024). **The Right to Data Portability: A Holistic Analysis of GDPR, DMA and the Data Act**. European Journal of Law and Technology, 15(1), 1-15.

European Union. (2025). **The General Data Protection Regulation (GDPR)**. Retrieved October 12, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A3201 6 R0 6 79&qid=1763750310706

Korean Personal Information Protection Act, 2011.

Kuner, C., Bygrave, L., & Docksey, C. (eds.). (2021). **The EU General Data Protection Regulation (GDPR): A Commentary**. Oxford University Press.

Panurut Chuenpukdee. (2019). **Some legal issues of biometric data protection in Thailand. (Master's thesis)**. Master of Laws in Business Laws (English Program), Faculty of Law. Thammasat University.

Personal Data Protection Act 2012. (2020). **Personal Data Protection Act 2012 (2020 Revised Edition)**. Singapore Statutes Online. https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P11-#P11-

Topelson, D., Bavitz, C., Gupta, R., & Oberman, I. (2013). **Privacy and children's data – An overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act**. Retrieved October 13, 2025, from https://studentprivacycompass.org/wp-

content/uploads/2020/02/BERKMAN-Privacy-and-Child rens-Data-2013.pdf

U.S. DEPARTMENT OF EDUCATION. (2025). **FERPA 34 CFR PART 99—FAMILY EDUCATIONAL RIGHTSAND PRIVACY**. Retrieved October 13, 2025, from https://studentprivacy. ed.gov/ferpa