

Criminal Liability under the Personal Data Protection Act B.E. 2562: A Critical Analysis of Sections 79 and 80 as Mechanisms for Fundamental Rights Protection and Implications for Legal Enforcement in Thailand

Nara Bunlikitkul

Faculty of Social Sciences,
Mahachulalongkornrajavidyalaya University,
Chanthaburi Campus, Thailand

Lakkana Doungtatip

Central Administrative Court, Thailand

Abstract

This academic article aims to critically analyze the structure of criminal liability under the Personal Data Protection Act B.E. 2562 (PDPA), focusing specifically on Sections 79 and 80, which establish criminal sanctions for data controllers and for persons who acquire personal data of others through the performance of duties under the Act, respectively. This article proposes that while the PDPA carries significant legislative intent to protect personal data rights as a fundamental right under Section 32 of the Constitution of the Kingdom of Thailand B.E. 2560, the criminal liability framework under Sections 79 and 80 contains several jurisprudential weaknesses that undermine effective enforcement. Although the focus is criminal liability, the article also examines administrative fines and civil liability insofar as they shape how the criminal provisions operate in practice.

The article analyzes the issue across four principal dimensions: (1) an analysis of the elements of offences under Sections 79 and 80 in comparison with general principles of criminal law, particularly issues of strict liability and burden of proof; (2) a comparative analysis of the liability structures applicable to data controllers versus persons who acquire personal data through the performance of duties under the Act; (3) an examination of selected publicly reported cases and enforcement practices of the Personal Data Protection Committee Office (PDPC) during B.E. 2565–2568; and (4) a critical examination of PDPA's implications in the context of modern digital technology, including instances where PDPA has been invoked in cases involving publicly accessible personal data.

CORRESPONDING AUTHOR

Nara Bunlikitkul, Faculty of Social Sciences, Mahachulalongkornrajavidyalaya University, Chanthaburi Campus
Chanthaburi Buddhist College, Mahachulalongkornrajavidyalaya University, Bang Kacha Sub-district,
Mueang Chanthaburi District, Chanthaburi 22000, Thailand E-mail: blc.kulnara@gmail.com
© College of Local Administration, Khon Kaen University. All rights reserved.

The analysis concludes that Sections 79 and 80 establish differentiated forms of liability for data controllers and persons who acquire personal data through duties performed under the Act, but possess significant weaknesses in two areas: first, the standard of proof for “damage” remains insufficiently defined in practice, and second, the prescribed penalties may be inadequate to deter violations by large organizations. This article proposes a reform framework termed the “Multi-tiered Organizational Accountability Model” (MOAM) to strengthen the effectiveness of PDPA enforcement in Thailand.

Keywords

personal data protection act, criminal liability, section 79, section 80, data controller, right to personal data privacy

โทษทางอาญาภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562: วิพากษ์มาตรา 79 และมาตรา 80 ในฐานะกลไกคุ้มครองสิทธิขั้นพื้นฐานและนัยต่อการบังคับใช้กฎหมายในประเทศไทย

นรา บรรลิตกุล

คณะสังคมศาสตร์ มหาวิทยาลัยมหาจุฬาลงกรณ
ราชวิทยาลัย วิทยาเขตจันทบุรี

ลักขณา ดวงตาทิพย์

ศาลปกครองกลาง

บทคัดย่อ

บทความวิชาการนี้มีวัตถุประสงค์เพื่อวิพากษ์โครงสร้างความรับผิดทางอาญาภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) โดยเฉพาะมาตรา 79 และมาตรา 80 ซึ่งเป็นบทบัญญัติหลักที่กำหนดโทษทางอาญาสำหรับผู้ควบคุมข้อมูลส่วนบุคคลและผู้ที่เกี่ยวข้องข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ตามลำดับ บทความนี้เสนอว่าแม้ PDPA จะมีเจตนารมณ์สำคัญในการคุ้มครองสิทธิในข้อมูลส่วนบุคคลอันเป็นสิทธิขั้นพื้นฐานของประชาชนตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 32 แต่โครงสร้างโทษทางอาญาภายใต้มาตรา 79 และมาตรา 80 ยังมีปัญหาเชิงนิติศาสตร์หลายประการที่ส่งผลกระทบต่อประสิทธิภาพของการบังคับใช้กฎหมาย แม้บทความนี้มุ่งวิเคราะห์ความรับผิดทางอาญาเป็นหลัก แต่ได้พิจารณาความรับผิดทางปกครองและทางแพ่งควบคู่ไปด้วยในขอบเขตที่เกี่ยวข้องกับการทำงานของบทบัญญัติทางอาญาในทางปฏิบัติ บทความนี้วิเคราะห์ใน 4 มิติหลัก ได้แก่ (1) การวิเคราะห์องค์ประกอบความผิดของมาตรา 79 และมาตรา 80 เปรียบเทียบกับหลักทั่วไปของกฎหมายอาญา โดยเฉพาะประเด็น strict liability และภาระการพิสูจน์ (2) การวิเคราะห์เปรียบเทียบโครงสร้างความรับผิดของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ที่เกี่ยวข้องข้อมูลส่วนบุคคลเนื่องจากการปฏิบัติหน้าที่ (3) การศึกษากรณีที่เคยเผยแพร่ต่อสาธารณะซึ่งคัดเลือกมาและแนวปฏิบัติของสำนักงานคณะกรรมการ

คุ้มครองข้อมูลส่วนบุคคล (สคส.) ในช่วง พ.ศ. 2565–2568 และ (4) การวิพากษ์นัยของ PDPA ในบริบทของเทคโนโลยีดิจิทัลสมัยใหม่ รวมถึงกรณีที่มีการอ้างถึง PDPA ในคดีที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่มีลักษณะสาธารณะ

ผลการวิเคราะห์ชี้ว่า มาตรา 79 และมาตรา 80 มีจุดแข็งในการกำหนดรูปแบบความรับผิดชอบที่แตกต่างกันระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ที่เกี่ยวข้องข้อมูลส่วนบุคคลเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แต่มีจุดอ่อนสำคัญในสองด้าน ด้านแรกคือเกณฑ์การพิสูจน์ “ความเสียหาย” ที่ยังขาดความชัดเจนในทางปฏิบัติ และด้านที่สองคือโทษที่กำหนดไว้อาจไม่เพียงพอต่อการยับยั้งการละเมิดในองค์กรขนาดใหญ่ บทความนี้เสนอกรอบแนวทางการปฏิรูปที่เรียกว่า “แบบจำลองความรับผิดชอบเชิงองค์กรแบบหลายชั้น” (Multi-tiered Organizational Accountability Model — MOAM) เพื่อเสริมสร้างประสิทธิภาพการบังคับใช้ PDPA ในประเทศไทย

คำสำคัญ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, โทษทางอาญา, มาตรา 79, มาตรา 80, ผู้ควบคุมข้อมูล, สิทธิในข้อมูลส่วนบุคคล

บทนำ

ในยุคที่ข้อมูลดิจิทัลกลายเป็นทรัพยากรที่มีมูลค่าสูงสุดในระบบเศรษฐกิจสมัยใหม่ สิทธิในการควบคุมข้อมูลส่วนบุคคลของตนเองจึงกลายเป็นสิทธิขั้นพื้นฐานที่ต้องได้รับความคุ้มครองจากกฎหมาย ประเทศไทยได้ตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในรูปของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งมีผลบังคับใช้อย่างเต็มรูปแบบเมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 โดยได้รับแรงบันดาลใจอย่างมีนัยสำคัญจาก General Data Protection Regulation (GDPR) ของสหภาพยุโรป แม้จะมีการปรับเปลี่ยนให้สอดคล้องกับบริบทกฎหมายไทย (European Union, 2016; Personal Data Protection Act, 2019)

ในเชิงความเป็นมา PDPA ตราขึ้นในรัฐบาลพลเอกประยุทธ์ จันทร์โอชา โดยผ่านความเห็นชอบของสภานิติบัญญัติแห่งชาติซึ่งทำหน้าที่รัฐสภาในขณะนั้น และประกาศในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 (Personal Data Protection Act, 2019) โดยเป็นส่วนหนึ่งของชุดกฎหมายด้านเศรษฐกิจดิจิทัลที่รัฐบาลผลักดัน ด้วยเหตุผลสำคัญสามประการ คือ การอุดช่องว่างจากการคุ้มครองข้อมูลที่เดิมกระจัดกระจายอยู่ในกฎหมายเฉพาะรายสาขา การรองรับความเสี่ยงจากการนำข้อมูลส่วนบุคคลไปใช้โดยไม่ชอบในยุคดิจิทัล และการยกระดับมาตรฐานของไทยให้สอดคล้องกับ GDPR เพื่อประโยชน์ด้านการค้าและการถ่ายโอนข้อมูลระหว่างประเทศ

อย่างไรก็ตาม นับแต่มีผลบังคับใช้จนถึง พ.ศ. 2568 การบังคับใช้บทบัญญัติทางอาญาของ PDPA โดยเฉพาะมาตรา 79 และมาตรา 80 ยังมีข้อจำกัดอย่างมีนัยสำคัญ ในทางปฏิบัติการบังคับใช้ดำเนินผ่านการปรับทางปกครองเป็นหลัก โดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) มีคำสั่งปรับทางปกครองรายแรกเมื่อเดือนกรกฎาคม พ.ศ. 2567 ในขณะที่คดีอาญาที่ถึงคำพิพากษาตาม มาตรา 79 และมาตรา 80 ยังปรากฏจำนวนน้อยและกระจุกตัวอยู่ในกรณีการซื้อขายข้อมูลโดยมิชอบ (Somwaiya et al., 2024; Suwanmatajarn, 2024) ปรากฏการณ์นี้สะท้อนให้เห็นถึงปัญหาเชิงโครงสร้างในการบังคับใช้กฎหมายที่ต้องได้รับการวิเคราะห์อย่างเป็นระบบ

นอกจากนี้ ความก้าวหน้าของเทคโนโลยีดิจิทัลยังก่อให้เกิดกรณีใหม่ที่ PDPA อาจถูกนำมาอ้างอิงในบริบทที่ซับซ้อนยิ่งขึ้น เช่น กรณีสมมติเชิงวิเคราะห์ที่มีการอ้างมาตรา 26 ต่อการพิมพ์รหัสหรือบาร์โค้ดที่อาจสืบย้อนถึงตัวผู้ลงคะแนนบนบัตรเลือกตั้ง โดยให้เหตุผลว่าเข้าข่ายการเก็บรวบรวมข้อมูลความเห็นทางการเมืองโดยไม่ได้รับความยินยอม กรณีเช่นนี้แสดงให้เห็นว่าขอบเขตการบังคับใช้ PDPA อาจขยายออกไปสู่มิติใหม่ที่เกี่ยวข้องกับสิทธิทางการเมืองและรัฐธรรมนูญ (การอภิปรายในบทความนี้ใช้เป็นกรณีสมมติเพื่อการวิเคราะห์เชิงหลักการ มิใช่คดีที่มีคำวินิจฉัยแล้ว)

บทความนี้มุ่งตอบคำถามวิจัยสี่ข้อ ได้แก่ (1) โครงสร้างองค์ประกอบความผิดของมาตรา 79 และมาตรา 80 มีความสอดคล้องกับหลักทั่วไปของกฎหมายอาญาไทยมากน้อยเพียงใด (2) ความแตกต่างระหว่างความรับผิดของผู้ควบคุมข้อมูลตามมาตรา 79 และผู้ที่ล่วงรู้ข้อมูลส่วนบุคคลเนื่องจากการปฏิบัติหน้าที่ตามมาตรา 80 มีนัยสำคัญต่อประสิทธิภาพการบังคับใช้กฎหมายอย่างไร (3) แนวปฏิบัติของ สคส. ในช่วง พ.ศ. 2565–2568 สะท้อนถึงจุดแข็งและจุดอ่อนของโครงสร้างโทษทางอาญาอย่างไร และ (4) ควรปฏิรูปโครงสร้างโทษทางอาญาของ PDPA ในทิศทางใดเพื่อเสริมสร้างประสิทธิภาพการคุ้มครองสิทธิของประชาชน วิธีวิทยาที่ใช้ในการวิจัยเชิงคุณภาพทางนิติศาสตร์ โดยอาศัยการวิเคราะห์ด้วยทฤษฎีหมาย คำพิพากษา แนวปฏิบัติของ สคส. และการเปรียบเทียบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและประเทศอื่น ทั้งนี้ กรณีศึกษาที่นำมาวิเคราะห์คัดเลือกจากคำสั่งของ สคส. และคำพิพากษาที่เผยแพร่ต่อสาธารณะและตรวจสอบได้ ซึ่งเกี่ยวข้องโดยตรงกับการเปิดเผยหรือการรักษาความมั่นคงปลอดภัยของข้อมูล และสะท้อนประเด็นเชิงโครงสร้างของความรับผิด แล้วสังเคราะห์ข้อค้นพบเชื่อมโยงกับการวิเคราะห์องค์ประกอบความผิดและการเปรียบเทียบเชิงกฎหมาย ทั้งนี้ แม้จุดเน้นของบทความอยู่ที่ความรับผิดทางอาญา แต่บทความได้วิเคราะห์มาตรการปรับทางปกครองและความรับผิดทางแพ่งควบคู่ไปด้วย เนื่องจากกลไกดังกล่าวมีผลโดยตรงต่อการทำงานของบทบัญญัติทางอาญาในทางปฏิบัติ และเนื่องจากกรณีศึกษาที่ใช้ยังมีจำนวนจำกัด ข้อค้นพบของบทความจึงมีลักษณะเป็นการวิเคราะห์เชิงหลักการ มิใช่การสรุปแนวคำพิพากษาที่เป็นที่ยุติแล้ว

หัวข้อที่ 1: กรอบทฤษฎีและการทบทวนวรรณกรรม

กรอบทฤษฎีนิติศาสตร์ที่ใช้ในการวิเคราะห์

บทความนี้อาศัยกรอบทฤษฎีนิติศาสตร์สองสำนักหลักในการวิเคราะห์โครงสร้างความรับผิดทางอาญาภายใต้ PDPA สำนักแรกคือทฤษฎีกฎหมายอาญาเชิงวิพากษ์ (Critical Criminal Law Theory) ซึ่งเสนอว่ากฎหมายอาญามีได้เป็นระบบที่เป็นกลางและสอดคล้องกันในตัวเอง หากแต่ถูกกำหนดรูปโดยเงื่อนไขทางสังคมและประวัติศาสตร์ จึงต้องถูกประเมินอย่างวิพากษ์ (Norrie, 2014) โดยเกณฑ์การประเมินสำคัญประกอบด้วย ความชอบธรรมของโทษ (legitimacy of punishment) ที่ตั้งคำถามถึงความสมเหตุสมผลในการลงโทษของรัฐ (Hart, 1968) ความได้สัดส่วนระหว่างโทษกับความผิด (proportionality) ซึ่งมีรากฐานมาตั้งแต่แนวคิดคลาสสิกของ Beccaria (1764/1872) และได้รับการพัฒนาในเชิงทฤษฎีการลงโทษสมัยใหม่ (von Hirsch, 1993) และประสิทธิภาพในการยับยั้ง (deterrence) ตามแนวคิดอรรถประโยชน์นิยม (Bentham, 1789) และการวิเคราะห์เชิงเศรษฐศาสตร์ว่าด้วยระดับโทษที่เหมาะสมต่อการยับยั้งผู้กระทำที่คำนวณต้นทุน–ผลได้ (Becker, 1968) ในการวิเคราะห์ PDPA มาตรา

79 และมาตรา 80 จึงต้องตั้งคำถามว่าโทษที่กำหนดไว้นั้นได้สัดส่วนกับความเสียหายที่เกิดขึ้นหรือไม่ และมีพลัยยับยั้งเพียงพอต่อองค์กรขนาดใหญ่ที่มีกำลังทรัพย์สูงหรือไม่

สำนักที่สองคือทฤษฎีสติธิในความเป็นส่วนตัว (Right to Privacy Theory) ที่พัฒนาโดย Warren และ Brandeis (1890) และต่อมาโดย Westin (1967) ซึ่งอธิบายว่าสิทธิในความเป็นส่วนตัวเป็นรากฐานของเสรีภาพส่วนบุคคลในระบอบประชาธิปไตย และต้องได้รับการคุ้มครองจากการล่วงละเมิดทั้งโดยเอกชนและโดยรัฐ ในบริบทของ PDPA สิทธิในข้อมูลส่วนบุคคลจึงเป็นส่วนหนึ่งของสิทธิในความเป็นส่วนตัวที่รัฐธรรมนูญ มาตรา 32 รับรองไว้ (Constitution of the Kingdom of Thailand, 2017) และ PDPA เป็นกลไกทางกฎหมายที่รัฐสร้างขึ้นเพื่อคุ้มครองสิทธินี้ในโลกดิจิทัล

การทบทวนวรรณกรรม

งานวิชาการที่เกี่ยวข้องแบ่งออกเป็นสามกลุ่มหลัก กลุ่มแรกคืองานวิชาการด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับสากล Voigt และ von dem Bussche (2017) วิเคราะห์โครงสร้าง GDPR อย่างละเอียด โดยชี้ว่าความสำเร็จของ GDPR อยู่ที่การกำหนดโทษปรับที่สูงมากถึงร้อยละ 4 ของรายได้ทั่วโลก ซึ่งสร้างแรงจูงใจที่แท้จริงให้องค์กรขนาดใหญ่ปฏิบัติตามกฎหมาย ในขณะที่โทษปรับของ PDPA มาตรา 79 ที่กำหนดไว้เพียงไม่เกินห้าแสนบาทอาจไม่มีพลัยยับยั้งเพียงพอสำหรับองค์กรขนาดใหญ่

กลุ่มที่สองคืองานวิชาการด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย Ubon และ Niyomrungrueangchai (2023) อธิบายเหตุผลความจำเป็นในการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ว่าเกิดจากความก้าวหน้าทางเทคโนโลยีและแนวโน้มการละเมิดสิทธิในข้อมูลส่วนบุคคลที่เพิ่มขึ้น โดยเฉพาะการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์หรือเปิดเผยโดยมิชอบ รวมถึงการนำไปใช้ในการกระทำความผิด เช่น การฉ้อโกง จึงจำเป็นต้องมีกลไกคุ้มครองข้อมูลส่วนบุคคลที่เป็นมาตรฐานเดียวกันและสอดคล้องกับมาตรฐานสากล ส่วน Chantarane (2023) วิเคราะห์ความสัมพันธ์ระหว่างฐานความยินยอมกับฐานความจำเป็นเพื่อการปฏิบัติตามสัญญา โดยเสนอว่าผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณาฐานทางกฎหมายอื่นนอกเหนือจากฐานความยินยอมก่อน และจะอาศัยฐานความจำเป็นเพื่อการปฏิบัติตามสัญญาได้เฉพาะเมื่อการประมวลผลนั้นจำเป็นต่อการปฏิบัติหน้าที่ตามสัญญาที่สมบูรณ์ตามกฎหมาย งานวิชาการกลุ่มนี้ช่วยอธิบายบริบทการตรากฎหมายและหลักเกณฑ์ฐานทางกฎหมายของ PDPA แต่ยังไม่ได้มุ่งวิเคราะห์โครงสร้างความรับผิดชอบทางอาญาตามมาตรา 79 และมาตรา 80 โดยตรง

กลุ่มที่สามคืองานวิชาการว่าด้วยความรับผิดชอบขององค์กรในทางอาญา Wells (2001) วิเคราะห์ทฤษฎีความรับผิดชอบขององค์กร (corporate criminal liability) โดยให้ความสำคัญกับการจัดสรรความรับผิดชอบระหว่างนิติบุคคลกับบุคคลที่มีอำนาจสั่งการหรือรับผิดชอบการดำเนินงานขององค์กร แนวคิดดังกล่าวอาจนำมาเชื่อมโยงกับมาตรา 81 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งกำหนดความรับผิดของกรรมการ ผู้จัดการ หรือบุคคลผู้รับผิดชอบการดำเนินงานของนิติบุคคล เมื่อความผิดของนิติบุคคลเกิดจากการสั่งการ การกระทำ หรือการละเว้นการสั่งการหรือการกระทำของบุคคลดังกล่าวภายใต้เงื่อนไขที่กฎหมายกำหนด

สรุปได้ว่า ช่องว่างสำคัญในวรรณกรรมที่มีอยู่คือการขาดการวิเคราะห์เชิงเปรียบเทียบที่เป็นระบบระหว่างมาตรา 79 และมาตรา 80 ในแง่ประสิทธิภาพการบังคับใช้จริง และการขาดกรอบแนวทางการปฏิรูปที่มีฐานทางทฤษฎีที่ชัดเจน บทความนี้มุ่งเติมเต็มช่องว่างดังกล่าว

หัวข้อที่ 2: วิเคราะห์องค์ประกอบความผิดมาตรา 79 และมาตรา 80

องค์ประกอบความผิดและโทษตามมาตรา 79

มาตรา 79 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดโทษทางอาญาสำหรับผู้ควบคุมข้อมูลส่วนบุคคลที่ฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย โดยมีโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ และในกรณีที่กระทำเพื่อแสวงหาประโยชน์ที่มีควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น มีโทษสูงขึ้นเป็นจำคุกไม่เกินหนึ่งปีหรือปรับไม่เกินหนึ่งล้านบาทหรือทั้งจำทั้งปรับ ทั้งนี้ มาตรา 79 วรรคสาม บัญญัติให้ความผิดตามมาตรา 79 เป็นความผิดอันยอมความได้ (Personal Data Protection Act, 2019)

เมื่อวิเคราะห์องค์ประกอบความผิดของมาตรา 79 ตามหลักทั่วไปของกฎหมายอาญา พบว่าประกอบด้วยองค์ประกอบสี่ประการ ประการแรก ผู้กระทำความผิดต้องเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ตามนิยามในมาตรา 6 แห่ง PDPA กล่าวคือต้องเป็นบุคคลธรรมดาหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ประการที่สอง การกระทำความผิดต้องเป็นการฝ่าฝืนมาตรา 27 หรือไม่ปฏิบัติตามมาตรา 28 โดยเกี่ยวกับข้อมูลประเภทพิเศษตามมาตรา 26 ซึ่งได้แก่ข้อมูลอ่อนไหว เช่น ข้อมูลสุขภาพ ข้อมูลเชื้อชาติ ข้อมูลความเห็นทางการเมือง และข้อมูลอื่นตามที่กำหนด ประการที่สาม การกระทำความผิดต้องเป็นไปโดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ซึ่งตัวบทมิได้กำหนดให้ต้องพิสูจน์ความเสียหายที่เกิดขึ้นจริงในทุกกรณี และประการที่สี่ ผู้กระทำความผิดต้องกระทำโดยเจตนาตามหลักทั่วไปในมาตรา 59 แห่งประมวลกฎหมายอาญา เนื่องจากมาตรา 79 มิได้บัญญัติให้ต้องรับผิดเมื่อกระทำโดยประมาท (Act Promulgating the Criminal Code, 1956)

ในทางนิติศาสตร์ ประเด็นที่สำคัญและยังเป็นที่ถกเถียงคือเรื่องของ “ความเสียหาย” ตามองค์ประกอบประการที่สาม กล่าวคือ PDPA มิได้นิยามคำว่าความเสียหายไว้อย่างชัดเจน ทำให้เกิดคำถามว่าความเสียหายดังกล่าวต้องเป็นความเสียหายทางทรัพย์สินที่วัดได้เป็นตัวเงินเท่านั้น หรือรวมถึงความเสียหายที่ไม่อาจวัดเป็นตัวเงินได้ เช่น ความเสียหายด้านชื่อเสียง การได้รับความอับอาย หรือความเครียดและความกังวลใจ แนวปฏิบัติของ สศส. แสดงให้เห็นว่าองค์กรนี้ตีความคำว่าความเสียหายอย่างกว้าง โดยรวมถึงความเสียหายที่ไม่ใช่ทรัพย์สินด้วย แต่ยังไม่มีความพิพากษาศาลที่ยืนยันแนวทางนี้อย่างชัดเจน

อีกประเด็นหนึ่งที่มีความสำคัญเชิงทฤษฎีคือคำถามว่ามาตรา 79 เป็นความผิดที่ต้องพิสูจน์เจตนา (mens rea) หรือเป็น strict liability ที่ต้องพิสูจน์แต่เพียงการกระทำ (actus reus) และผลที่เกิดขึ้นเท่านั้น จากการวิเคราะห์ตัวบท บทความนี้เสนอว่าโครงสร้างความรับผิดตามมาตรา 79 มีลักษณะที่ลดทอนเงื่อนไขการพิสูจน์ความเสียหายที่เกิดขึ้นจริง โดยตัวบทใช้เกณฑ์ว่าการกระทำนั้น “น่าจะทำให้” ผู้อื่นได้รับความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย อย่างไรก็ตาม การจัดประเภทความผิดดังกล่าวว่าเป็น semi-strict liability จำเป็นต้องพิจารณาหลักเจตนาและหลักความรับผิดทางอาญาตามกฎหมายไทยเพิ่มเติม

องค์ประกอบความผิดและโทษตามมาตรา 80

มาตรา 80 แห่ง PDPA กำหนดโทษทางอาญาสำหรับผู้ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่น เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วนำไปเปิดเผยแก่ผู้อื่น โดยมีโทษจำคุกไม่เกินหกเดือนหรือปรับไม่เกินห้าแสนบาทหรือทั้งจำทั้งปรับ ทั้งนี้ มาตรา 80 วรรคสอง กำหนดข้อยกเว้นไว้ เช่น การเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์แก่การสอบสวนหรือการพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐที่มีอำนาจหน้าที่ตามกฎหมาย และการเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล โครงสร้างของมาตรา 80 แตกต่างจากมาตรา 79 ในสาระสำคัญสองประการ ประการแรก ผู้กระทำความผิดตามมาตรา 80 ไม่จำเป็นต้องเป็นผู้ควบคุมข้อมูล แต่ต้องเป็นผู้ล่วงรู้ข้อมูลส่วนบุคคลเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO) หรือบุคคลอื่นที่มีหน้าที่เกี่ยวข้องโดยตรง ทั้งนี้ การปรับใช้มาตราดังกล่าวต้องพิจารณาขอบเขตหน้าที่และข้อเท็จจริงเป็นรายกรณี และไม่อาจสรุปได้ว่าผู้ปฏิบัติงานทุกคนที่เข้าถึงข้อมูลส่วนบุคคลในองค์กรอยู่ภายใต้มาตรา 80 โดยอัตโนมัติ ประการที่สอง องค์ประกอบของความผิดตามมาตรา 80 ไม่ได้กำหนดเงื่อนไขเรื่อง “ความเสียหาย” ไว้อย่างชัดเจนเท่ากับมาตรา 79 กล่าวคือ ตัวบทมิได้กำหนดให้ต้องพิสูจน์ความเสียหายเป็นองค์ประกอบความผิดโดยชัดแจ้ง แต่ต้องพิจารณาข้อยกเว้นตามวรรคสองประกอบด้วย อย่างไรก็ตาม การจะจัดประเภทบทบัญญัตินี้เป็น strict liability ยังต้องวิเคราะห์เพิ่มเติมตามหลักกฎหมายอาญาไทย การตีความตัวบท และแนวปฏิบัติของศาล อนึ่ง มีรายงานว่าศาลชั้นต้นบางคดีได้ปรับใช้มาตรา 80 กับผู้กระทำที่มีใช้ผู้ปฏิบัติหน้าที่ตามพระราชบัญญัตินี้โดยตรง ซึ่งจุดประเด็นถกเถียงเรื่องขอบเขตการลงโทษทางอาญา (Suwanmatajarn, 2024) นอกจากนี้ มาตรา 80 มิได้มีบทบัญญัติให้เป็นความผิดอันยอมความได้ดังเช่นมาตรา 79 วรรคสาม

การเปรียบเทียบมาตรา 79 และมาตรา 80 เชิงนิติศาสตร์

เมื่อเปรียบเทียบทั้งสองมาตราตาม Table 1 จะเห็นได้ว่าทั้งสองมาตรามีแนวคิดพื้นฐานที่แตกต่างกัน มาตรา 79 มุ่งกำกับ “อำนาจ” ในฐานะผู้ควบคุมข้อมูลที่ใช้อำนาจโดยมิชอบ ในขณะที่มาตรา 80 มุ่งกำกับ “ความไว้วางใจ” ในฐานะผู้ที่ได้รับมอบหมายให้เข้าถึงข้อมูลแล้วทรยศต่อความไว้วางใจนั้น ความแตกต่างเชิงแนวคิดนี้มีนัยสำคัญต่อการกำหนดนโยบายการบังคับใช้กฎหมาย เพราะกลยุทธ์การป้องกันและการตรวจสอบที่เหมาะสมสำหรับทั้งสองกรณีย่อมแตกต่างกัน

Table 1. Comparative Analysis of Statutory Elements: Section 79 vs Section 80

Comparative Issues	Section 79	Section 80
Subject of Liability	Data Controller	Any person who acquires another person’s personal data through the performance of duties under the PDPA (e.g., a DPO or others with directly related duties; determined case by case)

Table 1. Comparative Analysis of Statutory Elements: Section 79 vs Section 80

Comparative Issues	Section 79	Section 80
Actus Reus (Material Elements)	Violation of Sections 27 or 28 concerning personal data under Section 26	Unauthorized disclosure of personal data acquired through the performance of duties
Damage Requirement	The conduct must be likely to cause damage, impair reputation, or expose the data subject to scorn, hatred, or humiliation, as specified in Section 79.	No express damage element; disclosure is subject to the exceptions in Section 80, paragraph two.
Nature of Liability	Likelihood-of-harm standard; classification as semi-strict liability requires further analysis under Thai criminal-law principles.	Not necessarily strict liability; the classification requires further analysis under Thai criminal-law principles.
Underlying Legal Theory	Regulation of the “Abuse of Power”	Regulation of the “Breach of Trust/Confidence”
Maximum Penalty	Imprisonment not exceeding 1 year and/or a fine not exceeding THB 1 million (in cases of unlawful gain)	Imprisonment not exceeding 6 months and/or a fine not exceeding THB 500,000
Compoundable Offense	Yes (Section 79, paragraph three)	No express provision (non-compoundable under the general rule)

จาก Table 1. มีข้อสังเกตประการแรกว่า มาตรา 80 มิได้กำหนดให้ต้องพิสูจน์ความเสียหายเป็นองค์ประกอบความผิดโดยชัดแจ้ง อย่างไรก็ตาม การจะจัดประเภทบทบัญญัติดังกล่าวว่าเป็น strict liability ยังต้องวิเคราะห์เพิ่มเติมตามหลักกฎหมายอาญาไทย การตีความตัวบท และแนวปฏิบัติของศาล ประการที่สอง แม้ทั้งสองมาตรามีโทษในระดับใกล้เคียงกัน แต่มาตรา 79 มีโทษสูงสุดที่รุนแรงกว่าในกรณีที่มีการแสวงหาประโยชน์ ซึ่งสะท้อนให้เห็นว่าผู้บัญญัติกฎหมายมองว่าการที่ผู้มีอำนาจควบคุมข้อมูลใช้อำนาจนั้นเพื่อประโยชน์ส่วนตนมีความร้ายแรงกว่าการที่ผู้ล่วงรู้ข้อมูลเนื่องจากการปฏิบัติหน้าที่นำข้อมูลนั้นไปเปิดเผย สรุปได้ว่าโครงสร้างโทษทางอาญาใน PDPA สะท้อนการแยกรูปแบบความรับผิดชอบระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ล่วงรู้ข้อมูลเนื่องจากการปฏิบัติหน้าที่ แต่ยังมีช่องโหว่ในเรื่องการกำหนดเกณฑ์ “ความเสียหาย” ที่ต้องได้รับการพัฒนาต่อไป

หัวข้อที่ 3: กรณีศึกษาและแนวปฏิบัติของ สคส. พ.ศ. 2565–2568

ภาพรวมสถิติและแนวโน้มการบังคับใช้

ในช่วง พ.ศ. 2565–2568 การบังคับใช้ PDPA ในทางปฏิบัติดำเนินผ่านอำนาจปรับทางปกครองของ สคส. เป็นหลัก มากกว่าการดำเนินคดีอาญาตามมาตรา 79 และมาตรา 80 เมื่อวันที่ 31 กรกฎาคม พ.ศ. 2567 มีการออกคำสั่งปรับทางปกครองต่อผู้ควบคุมข้อมูลเป็นครั้งแรก และมีการเผยแพร่

หรือรายงานต่อสาธารณะในเดือนสิงหาคม พ.ศ. 2567 โดยยอดค่าปรับรวมอยู่ที่ 7 ล้านบาท (Chitranukroh et al., 2024; Somwaiya et al., 2024) และจนถึงเดือนตุลาคม พ.ศ. 2568 มีรายงานว่าคดีสำคัญที่ได้ข้อยุติแล้วห้าคดี ซึ่งรวมถึงคดีข้างต้น มียอดค่าปรับทางปกครองรวมกันกว่า 14 ล้านบาท ทั้งต่อหน่วยงานภาครัฐและภาคเอกชน (Panyasereeporn & Marsh, 2025) ในขณะที่คดีอาญาที่ถึงคำพิพากษายังปรากฏจำนวนน้อยและกระจุกตัวอยู่ในกรณีการซื้อขายข้อมูลโดยมิชอบ (Suwanmatajarn, 2024) ข้อมูลเชิงประจักษ์นี้สะท้อนว่าการบังคับใช้โทษทางอาญามาตรา 79 และมาตรา 80 ยังอยู่ในระดับต่ำเมื่อเทียบกับขนาดของปัญหา และเครื่องมือที่ถูกใช้จริงในทางปฏิบัติคือมาตรการทางปกครองมากกว่าโทษอาญา

การวิเคราะห์กรณีศึกษาสำคัญ

กรณีที่หนึ่ง: ความบกพร่องเชิงระบบของผู้ควบคุมข้อมูล เมื่อวันที่ 31 กรกฎาคม พ.ศ. 2567 คณะกรรมการผู้เชี่ยวชาญซึ่งแต่งตั้งตาม PDPA ได้ออกคำสั่งปรับทางปกครองต่อบริษัทจำหน่ายสินค้าออนไลน์รายใหญ่ และมีการเผยแพร่หรือรายงานต่อสาธารณะในเดือนสิงหาคม พ.ศ. 2567 โดยยอดค่าปรับรวมอยู่ที่ 7 ล้านบาท ภายหลังข้อมูลส่วนบุคคลของลูกค้ารั่วไหลไปสู่กลุ่มมิจฉาชีพคอลเซ็นเตอร์ โดยคณะกรรมการวินิจฉัยว่าบริษัทฝ่าฝืนมาตรา 41 (ไม่แต่งตั้ง DPO) มาตรา 37(1) (ไม่จัดให้มีมาตรการความมั่นคงปลอดภัยที่เหมาะสม) และมาตรา 37(4) (ไม่แจ้งเหตุละเมิดภายในกำหนด) (Chitranukroh et al., 2024; Somwaiya et al., 2024) กรณีนี้สะท้อนว่าความเสียหายที่ร้ายแรงที่สุดในทางปฏิบัติมักมีต้นเหตุจากความบกพร่องเชิงระบบขององค์กร ซึ่ง PDPA จัดการด้วยโทษปรับทางปกครองมากกว่าโทษอาญามาตรา 79 อันเป็นข้อสังเกตสำคัญต่อการออกแบบโครงสร้างความรับผิดชอบ

กรณีที่สอง: การปรับใช้มาตรา 80 กับผู้กระทำที่มีใช้ปฏิบัติหน้าที่ตามพระราชบัญญัตินี้มีรายงานเกี่ยวกับคำพิพากษาของศาลจังหวัดภูเก็ตใน พ.ศ. 2567 ว่า ศาลลงโทษผู้กระทำซึ่งนำข้อมูลส่วนบุคคล เช่น ชื่อ หมายเลขโทรศัพท์ อีเมล และเลขบัญชี จากแพลตฟอร์มการพนันออนไลน์ไปประกาศขายบนสื่อสังคมออนไลน์ โดยมีการกล่าวถึงการปรับใช้มาตรา 80 ของ PDPA ร่วมกับความผิดฐานอื่น (Suwanmatajarn, 2024) หากข้อเท็จจริงเป็นไปตามที่มีการรายงาน คดีนี้อาจเป็นตัวอย่างของการปรับใช้มาตรา 80 กับผู้กระทำที่มีใช้ปฏิบัติหน้าที่ตามพระราชบัญญัติโดยตรง ซึ่งสัมพันธ์กับข้อสังเกตในหัวข้อที่ 2 เรื่องขอบเขตของผู้กระทำตามมาตรา 80 และข้อกังวลเรื่องการขยายขอบเขตการลงโทษทางอาญา อย่างไรก็ตาม ข้อมูลคดีดังกล่าวมาจากบทความวิเคราะห์ข่าวกฎหมาย มิใช่คำพิพากษาดั้งเดิม จึงควรตรวจสอบคำพิพากษาดั้งเดิมก่อนสรุปขอบเขตการใช้มาตรา 80

กรณีที่สาม: ข้อมูลอ่อนไหวและฐานการประมวลผลโดยชอบด้วยกฎหมาย ในเดือนมีนาคม พ.ศ. 2567 ศาลชั้นต้นได้พิจารณาคดีที่โจทก์ฟ้องบริษัทประกันภัยในฐานะผู้ควบคุมข้อมูล กรณีเปิดเผยผลตรวจระดับแอลกอฮอล์ในเลือดของโจทก์ ซึ่งเป็นข้อมูลอ่อนไหวตามมาตรา 26 โดยไม่ได้รับความยินยอมโดยชัดแจ้ง ศาลวินิจฉัยว่าการประมวลผลดังกล่าวมีความจำเป็นเพื่อการต่อสู้คดีของบริษัทตามมาตรา 26(4) จึงไม่ต้องอาศัยความยินยอม และพิพากษายกฟ้อง (Tilleke & Gibbins, 2024) กรณีนี้แสดงให้เห็นถึงบทบาทขององค์กรประกอบเรื่องฐานการประมวลผลโดยชอบด้วยกฎหมายและการพิสูจน์ “ความเสียหาย” ในการจำกัดขอบเขตความรับผิดชอบตามมาตรา 79

จุดแข็งและจุดอ่อนของกลไกการบังคับใช้

จากการวิเคราะห์กรณีศึกษาข้างต้น พบจุดแข็งของกลไกการบังคับใช้ PDPA สามประการ ประการแรก การกำหนดความรับผิดชอบของกรรมการ ผู้จัดการ หรือบุคคลผู้รับผิดชอบการดำเนินงานของนิติบุคคลตามมาตรา 81 ภายใต้งบเงื่อนไขที่กฎหมายกำหนด อาจช่วยสร้างแรงจูงใจให้ผู้บริหารระดับสูงให้ความสำคัญกับการปฏิบัติตามกฎหมายมากขึ้น ประการที่สอง การให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจลงโทษปรับทางปกครองสูงถึงห้าล้านบาทตามมาตรา 84 นอกเหนือจากโทษทางอาญา ทำให้มีเครื่องมือบังคับใช้ที่หลากหลาย ดังปรากฏในกรณี พ.ศ. 2567 ที่ยอดค่าปรับรวมจากการฝ่าฝืนหลายประการอยู่ที่ 7 ล้านบาท (Panyasereeporn & Marsh, 2025) และประการที่สาม การเปิดให้ฟ้องคดีแพ่งเพื่อเรียกค่าเสียหายได้ตามมาตรา 77 สร้างกลไกการเยียวยาที่ครบถ้วน

ขณะเดียวกัน พบจุดอ่อนที่สำคัญสามประการ ประการแรก แม้ สคส. จะเริ่มใช้อำนาจปรับทางปกครองในระดับสูง แต่โทษ “ทางอาญา” ตามมาตรา 79 ที่กำหนดโทษปรับไว้เพียงไม่เกินห้าแสนบาท (หรือหนึ่งล้านบาทกรณีแสวงหาประโยชน์) ยังต่ำเกินไปสำหรับองค์กรขนาดใหญ่ที่มีรายได้หลายพันล้านบาท เพราะไม่มีพลังยับยั้งเพียงพอ ประการที่สอง การที่มาตรา 79 วรรคสาม บัญญัติให้ความผิดตามมาตรานี้เป็นความผิดอันยอมความได้ ทำให้เจ้าของข้อมูลอ่อนแอหรือขาดข้อมูลอาจถูกกดดันให้ถอนคำร้อง และประการที่สาม การขาดแนวปฏิบัติที่ชัดเจนจากศาลในการตีความ “ความเสียหาย” ทำให้เกิดความไม่แน่นอนในการบังคับใช้กฎหมาย

สรุปได้ว่า แม้ PDPA จะวางโครงสร้างความรับผิดทางอาญาไว้อย่างมีแนวคิดที่ดี แต่การบังคับใช้จริงในช่วงสามปีแรกยังมีข้อจำกัดอยู่มาก ทั้งในเรื่องระดับโทษอาญาที่ไม่เพียงพอและความไม่ชัดเจนในการตีความองค์ประกอบความผิด

หัวข้อที่ 4: วิพากษ์เชิงนิติศาสตร์และข้อเสนอการปฏิรูป

ปัญหาเชิงโครงสร้างของโทษทางอาญาใน PDPA

เมื่อวิเคราะห์โครงสร้างโทษทางอาญาของ PDPA เปรียบเทียบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและประเทศอื่น พบปัญหาเชิงโครงสร้างสำคัญสี่ประการ ประการแรก ปัญหาความไม่ได้สัดส่วนของโทษ GDPR ของสหภาพยุโรปกำหนดโทษปรับสูงสุดถึงสี่สิบล้านยูโรหรือร้อยละสี่ของรายได้ทั่วโลกขององค์กร แล้วแต่จำนวนใดจะสูงกว่า ในขณะที่ PDPA กำหนดโทษปรับทางอาญาสูงสุดเพียงห้าแสนบาทตามมาตรา 79 วรรคหนึ่ง (หรือหนึ่งล้านบาทตามวรรคสอง) และโทษปรับทางปกครองสูงสุดห้าล้านบาทตามมาตรา 84 (European Union, 2016; Voigt & von dem Bussche, 2017) ความแตกต่างนี้มีนัยสำคัญมากสำหรับองค์กรข้ามชาติที่ดำเนินธุรกิจในประเทศไทย เพราะโทษตาม PDPA อาจถือเป็น “ต้นทุนทางธุรกิจ” ที่รับได้ มากกว่าจะเป็นแรงจูงใจที่แท้จริงในการปฏิบัติตามกฎหมาย ยิ่งไปกว่านั้น GDPR ยังวางฐานคิดเชิงกำกับดูแลที่ลงโทษการไม่จัดให้มีระบบคุ้มครองที่เพียงพอตั้งแต่ก่อนเกิดความเสียหาย อันมุ่งสร้างวัฒนธรรมการกำกับดูแลข้อมูลเชิงป้องกัน ต่างจาก PDPA ที่เน้นความรับผิดภายหลังการละเมิดเป็นหลัก

ประการที่สอง ปัญหาการตีความ “ความเสียหาย” ที่ไม่ชัดเจน ดังที่ได้วิเคราะห์ไว้แล้วว่า PDPA ไม่ได้นิยามคำว่าความเสียหายไว้อย่างชัดเจน ทำให้เกิดความไม่แน่นอนในทางปฏิบัติ ปัญหานี้รุนแรงขึ้นเมื่อพิจารณาว่าข้อมูลส่วนบุคคลในยุคดิจิทัลมักก่อให้เกิดความเสียหายในรูปแบบที่ยากต่อการวัดค่าเป็น

ตัวเงิน เช่น ความเสียหายจากการถูกเลือกปฏิบัติโดยอาศัยข้อมูล หรือความเสียหายจากการสูญเสียอำนาจควบคุมข้อมูลของตนเอง

ประการที่สาม ปัญหาของการเป็นความผิดอันยอมความได้ตามมาตรา 79 วรรคสาม แม้จะมีประโยชน์ในแง่ของการลดภาระของกระบวนการยุติธรรม แต่ยังมีความเสี่ยงที่สำคัญ เพราะเจ้าของข้อมูลที่เป็นผู้บริโภคทั่วไปมักไม่มีความรู้ทางกฎหมายและมีอำนาจต่อรองต่ำกว่าองค์กรขนาดใหญ่ที่ครอบครองข้อมูล ทำให้มีความเสี่ยงที่การยอมความจะเกิดขึ้นภายใต้ความกดดันที่ไม่เป็นธรรม

ประการที่สี่ ปัญหาการขาดกลไกการตรวจสอบเชิงป้องกัน ปัจจุบัน PDPA เน้นการลงโทษภายหลังเกิดการละเมิด แต่ขาดกลไกที่กระตุ้นให้องค์กรสร้างระบบป้องกันตั้งแต่ต้น เช่น การตรวจสอบผลกระทบด้านการคุ้มครองข้อมูล (Data Protection Impact Assessment — DPIA) ยังไม่ได้ถูกกำหนดให้เป็นข้อบังคับสำหรับกิจกรรมที่มีความเสี่ยงสูงในบริบทไทย

ข้อเสนอการปฏิรูป: แบบจำลอง MOAM

จากการวิเคราะห์ข้างต้น บทความนี้เสนอ “แบบจำลองความรับผิดชอบเชิงองค์กรแบบหลายชั้น” (Multi-tiered Organizational Accountability Model - MOAM) ซึ่งประกอบด้วยสี่ชั้นการปฏิรูปที่สัมพันธ์กันเป็นระบบเดียว ดังนี้

ชั้นที่หนึ่งคือการปฏิรูปโครงสร้างโทษ โดยเสนอให้แก้ไขมาตรา 79 เพื่อกำหนดโทษปรับในลักษณะที่สัมพันธ์กับรายได้หรือขนาดขององค์กร เช่น กำหนดขั้นต่ำที่ร้อยละ 2 ของรายได้ต่อปีสำหรับองค์กรขนาดใหญ่ ซึ่งจะสร้างพลังยับยั้งที่แท้จริงในทุกระดับขนาดองค์กร

ชั้นที่สองคือการกำหนดนิยาม “ความเสียหาย” ที่ชัดเจน โดยเสนอให้ออกกฎกระทรวงหรือแนวปฏิบัติที่กำหนดประเภทความเสียหายตามลำดับความร้ายแรง ตั้งแต่ความเสียหายทางทรัพย์สินที่วัดได้ ความเสียหายด้านชื่อเสียง ความเสียหายด้านโอกาส และความเสียหายทางจิตใจ เพื่อให้ศาลและ สศส. มีแนวทางที่ชัดเจนในการประเมิน

ชั้นที่สามคือการเสริมสร้างกลไกการตรวจสอบเชิงป้องกัน โดยเสนอให้กำหนดให้ DPIA เป็นข้อบังคับสำหรับกิจกรรมที่มีความเสี่ยงสูงที่กำหนดไว้ชัดเจน และให้การดำเนินการ DPIA ที่ถูกต้องสามารถใช้เป็นเหตุบรรเทาโทษในกรณีที่เกิดการละเมิดได้ ซึ่งจะสร้างแรงจูงใจให้องค์กรลงทุนในระบบป้องกันตั้งแต่ต้น

ชั้นที่สี่คือการแก้ไขลักษณะของความผิดอันยอมความได้ โดยเสนอให้แบ่งความผิดออกเป็นสองระดับ ระดับแรกสำหรับการละเมิดที่กระทบต่อเจ้าของข้อมูลรายบุคคลที่อาจยอมความได้ และระดับที่สองสำหรับการละเมิดที่กระทบต่อสาธารณะในวงกว้างหรือเกี่ยวกับข้อมูลอ่อนไหวตามมาตรา 26 ที่ไม่อาจยอมความได้ เพื่อปิดช่องว่างที่อาจถูกใช้กดดันเจ้าของข้อมูลที่อ่อนแอ

ความสัมพันธ์ระหว่างสี่ชั้นเป็นไปตามหลักความได้สัดส่วน กล่าวคือชั้นที่หนึ่งและชั้นที่สามทำหน้าที่เป็นกลไกป้องกันและจูงใจการปฏิบัติตามล่วงหน้า ในขณะที่ชั้นที่สองและชั้นที่สี่กำกับความรุนแรงและขอบเขตของการลงโทษให้สอดคล้องกับระดับความผิด จุดที่ทำให้ MOAM แตกต่างจากกรอบแนวคิดเดิม คือ ต่างจากแบบจำลองความรับผิดชอบเชิงกำกับดูแลของ GDPR ที่อาศัยมาตรการทางปกครองเป็นหลัก (Voigt & von dem Bussche, 2017) และต่างจากทฤษฎีความรับผิดชอบขององค์กรทั่วไป (Wells, 2001) ตรงที่ MOAM บูรณาการมิติการป้องกันเชิงระบบ การนิยามความเสียหาย และการจัดระดับความผิดอันยอมความได้เข้ากับโครงสร้างโทษอาญาเฉพาะของมาตรา 79–80 อย่างเป็นระบบเดียว การปฏิรูปทั้งสี่ชั้น

จึงต้องดำเนินการพร้อมกัน เพราะการแก้ไขเพียงชั้นเดียวไม่เพียงพอที่จะแก้ปัญหาเชิงโครงสร้างที่มีความซับซ้อนหลายมิติ

องค์ความรู้ใหม่

จากการศึกษาวิเคราะห์โทษทางอาญาภายใต้ PDPA มาตรา 79 และมาตรา 80 บทความนี้ นำเสนอองค์ความรู้ใหม่สองประการ ประการแรกคือ “แบบจำลองความรับผิดชอบเชิงองค์กรแบบหลายชั้น” (MOAM) ที่เสนอกรอบการปฏิรูปโครงสร้างโทษทางอาญาของ PDPA อย่างเป็นระบบ โดยบูรณาการหลักทฤษฎีกฎหมายอาญา ทฤษฎีสติปัญญาในความเป็นส่วนตัว และบทเรียนจากกฎหมายเปรียบเทียบเข้าด้วยกัน ประการที่สองคือการพัฒนา “เกณฑ์การทดสอบสามชั้นสำหรับการพิสูจน์ความเสียหายตาม PDPA” ซึ่งประกอบด้วย ชั้นที่หนึ่ง ทดสอบความเสียหายทางทรัพย์สินที่วัดได้เป็นตัวเงิน ชั้นที่สอง ทดสอบความเสียหายทางสังคมที่วัดได้จากการเปลี่ยนแปลงในความสัมพันธ์ทางสังคมหรือโอกาสในชีวิต และชั้นที่สาม ทดสอบความเสียหายทางอำนาจการควบคุมข้อมูลตนเองที่เป็นนามธรรมแต่มิใช่นัยสำคัญต่อสิทธิขั้นพื้นฐาน

สรุป

บทความวิชาการนี้ได้วิพากษ์โครงสร้างความรับผิดชอบทางอาญาภายใต้ PDPA มาตรา 79 และมาตรา 80 และได้ข้อสรุปสำคัญสี่ประการ ประการแรก คือ มาตรา 79 และมาตรา 80 มีแนวคิดพื้นฐานที่แตกต่างกันอย่างมีนัยสำคัญ โดยมาตรา 79 มุ่งกำกับการใช้อำนาจโดยมิชอบของผู้ควบคุมข้อมูล ในขณะที่มาตรา 80 มุ่งกำกับการทรยศต่อความไว้วางใจของผู้ที่ล่วงรู้ข้อมูลเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ความแตกต่างนี้มีนัยสำคัญต่อการกำหนดกลยุทธ์การบังคับใช้กฎหมายที่เหมาะสม ประการที่สอง คือ โครงสร้างโทษทางอาญาของทั้งสองมาตรายังมีจุดอ่อนสำคัญในสองด้าน ได้แก่ ระดับโทษที่ต่ำเกินไปสำหรับองค์กรขนาดใหญ่ และความไม่ชัดเจนในการนิยาม “ความเสียหาย” ที่เป็นองค์ประกอบสำคัญของความผิด ประการที่สาม กรณีศึกษาที่คัดเลือกจากแนวปฏิบัติของ สคส. และคำพิพากษาที่มีการรายงานในช่วง พ.ศ. 2565–2568 บ่งชี้ว่าการบังคับใช้โทษทางอาญายังอยู่ในระดับต่ำเมื่อเทียบกับขนาดของปัญหาที่เกิดขึ้นจริง และประการที่สี่ คือ บริบทใหม่ของเทคโนโลยีดิจิทัลกำลังทำให้ขอบเขตการบังคับใช้ PDPA ขยายออกไปสู่มิติที่ซับซ้อนยิ่งขึ้น โดยเฉพาะในกรณีที่ข้อมูลส่วนบุคคลเกี่ยวข้องกับสิทธิทางการเมืองและสิทธิตามรัฐธรรมนูญ

บทความนี้เสนอแบบจำลอง MOAM เป็นกรอบการปฏิรูปที่บูรณาการสี่มิติพร้อมกัน ได้แก่ การปรับโครงสร้างโทษให้สัมพันธ์กับขนาดองค์กร การนิยาม “ความเสียหาย” ที่ชัดเจน การเสริมสร้างกลไกเชิงป้องกัน และการทบทวนลักษณะของความผิดอันยอมความได้ การปฏิรูปตาม MOAM จะช่วยให้ PDPA บรรลุเจตนารมณ์หลักในการคุ้มครองสิทธิในข้อมูลส่วนบุคคลของประชาชนในฐานะสิทธิขั้นพื้นฐานตามรัฐธรรมนูญได้อย่างมีประสิทธิภาพและยั่งยืนมากยิ่งขึ้น

เอกสารอ้างอิง

Act Promulgating the Criminal Code, B.E. 2499 (1956). *Royal Thai Government Gazette*, Vol. 73, Part 95 Special Issue, pp. 1–171 (November 15, 1956). (In Thai)

- Beccaria, C. (1872). *An essay on crimes and punishments: By the Marquis Beccaria of Milan, with a commentary by M. de Voltaire: A new edition corrected.* (Original work published 1764). W. C. Little & Co.
- Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, 76(2), 169–217. <https://doi.org/10.1086/259394>.
- Bentham, J. (1789). *An introduction to the principles of morals and legislation.* T. Payne and Son.
- Chantarane, C. (2023). Issues concerning interplay between consent and necessity for the performance of a contract under the Personal Data Protection Act B.E. 2562. *Thammasat Law Journal*, 52(1), 92–122. (In Thai)
- Chitranukroh, N., Lalitkamon, N., & Mahakunkitchareon, G. (2024, November 14). *First fine imposed under Thailand's Personal Data Protection Act.* IAPP. <https://iapp.org/news/a/first-fine-imposed-under-thailand-s-personal-data-protection-act> (In Thai)
- Constitution of the Kingdom of Thailand, B.E. 2560 (2017). Royal Thai Government Gazette, Vol. 134, Part 40 A (April 6, 2017). (In Thai)
- European Union. (2016). 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 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.
- Hart, H. L. A. (1968). *Punishment and responsibility: Essays in the philosophy of law.* Clarendon Press.
- Norrie, A. (2014). *Crime, reason and history: A critical introduction to criminal law* (3rd ed.). Cambridge University Press.
- Panyasereeporn, P., & Marsh, M. (2025, October 24). *Thailand: Legal update: PDPA enforcement intensifies: Key cases, risks, and compliance insights.* One Asia Lawyers. <https://oneasia.legal/en/6627> (In Thai)
- Personal Data Protection Act, B.E. 2562 (2019). *Royal Thai Government Gazette*, Vol. 136, Part 69 A (May 27, 2019). (In Thai)
- Somwaiya, K., Ua-areetham, P., & Aroonpakmongkol, W. (2024, September 30). *Thailand first administrative fine for data breach: An analysis of law and practice.* LawPlus Ltd. <https://www.lawplusltd.com/2024/09/thailand-first-administrative-fine-for-data-breach-an-analysis-of-law-and-practice/>
- Suwanmatajarn, P. (2024, December 18). *Data privacy: Criminal penalties imposed by the court raise concerns of practice.* Lexology. <https://www.lexology.com/library/detail.aspx?g=e0a16940-c04e-4314-a2cc-321dfc8ca1f3> (In Thai)
- Tilleke & Gibbins. (2024, June 24). *Thailand: Ruling clarifies “lawful basis” for processing certain personal data.* <https://www.tilleke.com/insights/thailand-ruling-clarifies-lawful-basis-for-processing-certain-personal-data/>
- Ubon, W., & Niyomrungrueangchai, N. (2023). The necessity for have a Personal Data Protection Act, B.E. 2562. *Rangsit Journal of Law and Society*, 5(1), 41–56. (In Thai)

- Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer. <https://doi.org/10.1007/978-3-319-57959-7>
- Von, Hirsch, A. (1993). *Censure and sanctions*. Clarendon Press.
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220. <https://doi.org/10.2307/1321160>
- Wells, C. (2001). *Corporations and criminal responsibility* (2nd ed.). Oxford University Press.
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum.