กฎหมายคุ้มครองข้อมูลส่วนบุคคล : จากสิทธิในความเป็นส่วนตัว สู่มาตรฐานทางธุรกิจ

กฤตานน อวยพรรุ่งรัตน์

นิวตรอน อภิวงศ์สุวรรณ

ภัทรกิจ สัญชยานุกูล[1]

1. บทนำ

กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กลายเป็นหนึ่งในกฎหมายที่สำคัญที่สุดในโลกยุคปัจจุบัน ยุโรปได้ประกาศใช้บังคับกฎหมายคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรป (General Data Protection Regulation : GDPR) ในปี พ.ศ. 2561 ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สมบูรณ์และคลอบคลุมมากที่สุดฉบับหนึ่งในโลก กฎหมายฉบับนี้ยังเป็นแม่บทให้กับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย (Personal Data Protection Act : PDPA) ที่ประกาศใช้บังคับในปี พ.ศ. 2565 ภายหลังการประกาศใช้บังคับสังคมไทยได้มีการตื่นตัวต่อการเกิดขึ้นของกฎหมายฉบับนี้ นอกจากภาคประชาชนแล้วภาคองค์กรธุรกิจก็เป็นอีกฝ่ายหนึ่งที่ตื่นตัวกับการบังคับใช้กฎหมายฉบับดังกล่าว บุคคลที่ให้ความสนใจกฎหมายฉบับนี้อาจเข้าใจไปว่ามันมีขึ้นเพราะต้องการตอบสนองต่อความเปลี่ยนแปลงของสังคม อาทิการพัฒนาของเทคโนโลยีจัดเก็บข้อมูล การใช้ข้อมูลส่วนบุคคลของภาคเอกชนและธุรกิจในการประมวลผลเพื่อจุดประสงค์ทางธุรกิจ ซึ่งเป็นความเข้าใจที่ถูกต้องแต่เป็นเพียงบางส่วนเท่านั้น เนื่องจากแนวคิดที่เป็นรากฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ถือกำเนิดขึ้นอย่างยาวนาน โดยบทความนี้คณะผู้เขียนนำเสนอเริ่มจากแนวคิดพื้นฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลอันมีจุดเริ่มต้นมาจากแนวคิดในการคุ้มครองความเป็นส่วนตัว (Privacy) ต่อมาคณะผู้เขียนจะชี้ให้เห็นว่าจากกฎหมายที่มุ่งคุ้มครองสิทธิในความเป็นส่วนตัวได้พัฒนากลายเป็นมาตรฐานทางธุรกิจได้อย่างไรและเหตุใดถึงต้องเป็นเช่นนั้น และการเปลี่ยนแปลงนั้นจะเป็นผลดีต่อการคุ้มครองสิทธิของบุคคลอย่างไร

---

[1] นิสิตชั้นปีที่ 4 คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

*คณะผู้เขียนขอขอบพระคุณ รองศาสตราจารย์ ดร.ปิยะบุตร บุญอร่ามเรือง ที่ได้กรุณารับเป็นที่ปรึกษาให้แก่บทความฉบับนี้

2. สิทธิในความเป็นส่วนตัวบนฐานของกฎหมายละเมิด

2.1. สิทธิขั้นพื้นฐานของบุคคลก่อนสิทธิในความเป็นส่วนตัว

(1) สิทธิในชีวิตอาจกล่าวได้ว่าเป็นสิทธิที่สำคัญที่สุดที่กฎหมายมุ่งจะคุ้มครอง เพราะถ้าหากปราศจากการรับรองและคุ้มครองชีวิตของบุคคลแล้ว การพิจารณาถึงสิทธิอื่น ๆ ก็ย่อมไร้ความหมาย สังคมมนุษย์ในอดีตไม่มีกฎหมายคุ้มครองทำให้การดำรงอยู่ของมนุษย์ขึ้นอยู่กับว่าใครคือผู้ที่แข่งแกร่งที่สุดและผู้นั้นจะเป็นผู้ที่อยู่รอด เมื่อสังคมพัฒนามาสู่ยุคที่มีกฎหมายจึงเกิดแนวคิดในการคุ้มครองชีวิต ซึ่งแนวคิดของสิทธิในชีวิตมีมาตั้งแต่สมัยโบราณ เช่น ในประมวลกฎหมายฮัมมูราบีก็ปรากฏบทบัญญัติที่เกี่ยวข้องกับกฎหมายอาญา โดยประมวลกฎหมายนี้มีความมุ่งหมายที่จะยกระดับความเป็นอยู่ของประชาชนเพื่อคุ้มครองไม่ให้ผู้ที่แข่งแกร่งทำร้ายผู้ที่อ่อนแอ[2] นอกจากนี้ยังมีหลักฐานในอดีตที่แสดงให้เห็นถึงความสำคัญของสิทธิในชีวิต เอกสารทางกฎหมายชิ้นแรกที่ได้กล่าวถึงสิทธิในชีวิต ได้แก่ The Virginia Declaration of Right 1776 ซึ่งกล่าวถึงสิทธิในชีวิตอย่างชัดแจ้ง (the enjoyment of life)[3] โดยต่อมาสิทธิดังกล่าวก็ได้ถูกยืนยันอีกครั้งในคำประกาศอิสรภาพของประเทศสหรัฐอเมริกา[4] ดังนั้นแนวคิดทางกฎหมายในการคุ้มครองชีวิตมนุษย์จึงเป็นแนวคิดที่ได้ถูกพัฒนามาเป็นเวลานานแล้วโดยแสดงออกผ่านการบัญญัติกฎหมาย เช่น กฎหมายอาญาความผิดฐานฆ่าผู้อื่น เป็นต้น

(2) สิทธิที่สำคัญอีกชนิดหนึ่งที่กฎหมายคุ้มครอง ได้แก่ สิทธิในทรัพย์สิน ในยุคโบราณทรัพย์สินทั้งหมดเป็นของราชาหรือกษัตริย์ แม้ว่าโลกจะก้าวเข้าสู่ยุคสมัยใหม่แต่แนวคิดที่มองว่ารัฐควรเป็นเจ้าของทรัพย์สินก็ยังคงปรากฏ เช่น แนวคิดแบบสังคมนิยม เป็นต้น ในขณะที่ฝ่ายเสรีนิยมสนับสนุนการให้เอกชนเป็นเจ้าของทรัพย์สินโดยเชื่อว่าการให้กรรมสิทธิ์แก่ปัจเจกบุคคลจะสร้างแรงจูงใจในการสร้างงานและผลผลิตมากกว่า อย่างไรก็ตามระบบกฎหมายของประเทศที่ปกครองโดยระบอบเสรีนิยมประชาธิปไตยเกือบทุกประเทศในปัจจุบันรับรองสิทธิในทรัพย์สินแก่บุคคล กล่าวคือ กฎหมายรับรองว่าบุคคลสามารถมีกรรมสิทธิ์เหนือวัตถุต่าง ๆ และถ้าหากว่ามีคนเข้ามารบกวนการใช้ประโยชน์จากทรัพย์สินนั้น กฎหมายก็จะคุ้มครองผู้ที่เป็นเจ้าของ เช่น

---

[2] P.G.Lauren, “The Foundations of Justice and Human Rights in Early Legal Texts and Thought,” chap.7 in D. Shelton (ed.), The Oxford Handbook of International Human Rights Law, (Oxford,Oxford University Press, October 2013), pp. 163-93, at 164-5.

[3] Casey-Maslen, S., & Heyns, C.. “An Historical Introduction to the Right to Life’” In The Right to Life under International Law: An Interpretative Manual, (Cambridge: Cambridge University, 2021), pp. 1-6.

[4] Christian Tomuschat, “The Right to Life – Legal and Political Foundations,” chap.1 in The Right to Life (Leiden: Brill | Nijhoff, 2010), p.4.

การให้ผู้เป็นเจ้าของมีสิทธิเรียกร้องค่าเสียหายจากผู้ที่เข้ามาทำความเสียหายผ่านกฎหมายละเมิด หรือแม้แต่การลงโทษผู้กระทำความผิดหากการกระทำนั้นเป็นความผิดตามกฎหมายอาญา

(3) กฎหมายคุ้มครองทรัพย์สินที่ไม่มีรูปร่าง เช่น ความนึกคิดของคนที่มีมูลค่า การทำซ้ำหรือลอกเลียนงานศิลปะหรือสิ่งประดิษฐ์ สิ่งเหล่านี้ถือเป็นทรัพย์สินทางปัญญาที่กฎหมายให้ความคุ้มครอง กฎหมายที่เข้ามาคุ้มครองสิทธิเหล่านี้ เช่น กฎหมายลิขสิทธิ์ กฎหมายเครื่องหมายการค้า กฎหมายสิทธิบัตร เป็นต้น แนวคิดเกี่ยวกับทรัพย์สินทางปัญญาถือกำเนิดตั้งแต่ยุคโบราณเช่นเดียวกันแม้ว่าในยุคดังกล่าวยังไม่ได้มีกฎหมายคุ้มครองทรัพย์สินทางปัญญาอย่างในยุคปัจจุบัน ตัวอย่างกรณีศึกษาที่ถูกอ้างถึงใน *The Genesis of American Patent and Copyright Law* (Bugbee 1967) เป็นตัวอย่างคดีที่เกิดขึ้นในยุคโบราณ เช่น วิตรูวิอุส (Vitruvius) ได้จับผู้ขโมยความคิดของผู้อื่นในการประกวดงานเขียน ซึ่งในขณะที่ทำหน้าที่เป็นกรรมการ วิตูวิอุสจับกวีคนหนึ่งที่กระทำความผิดได้ต่อมากวีผู้นั้นถูกพิพากษาว่ามีความผิดจากการที่ไปขโมยคำศัพท์จากงานของผู้อื่นมาใส่ในงานของตน[5]

2.2 พัฒนาการสิทธิในความเป็นส่วนตัว

สิทธิในความเป็นส่วนตัวได้รับการอธิบายว่าเป็น “สิทธิที่จะไม่ถูกรบกวน” (right to be let alone)[6] ไว้ในบทความ “The right to privacy”[7] ที่เขียนโดยซามูเอล ดี วอเร็นและโลอิส แบรนไดซ์ (Samuel D. Warren and Louis Brandeis) บทความฉบับนี้เป็นบทความฉบับแรก ๆ ที่กล่าวถึงสิทธิในความเป็นส่วนตัวและมีอิทธิพลต่อพัฒนาการของแนวคิดของสิทธิในความเป็นส่วนตัวเป็นอย่างมาก โดยในบทความนี้จุดประกายให้สังคมตระหนักถึงความสำคัญและการมีอยู่ของสิทธิในความเป็นส่วนตัว และเป็นจุดเริ่มต้นที่สำคัญที่นำไปสู่การศึกษาค้นคว้าโดยนักกฎหมายยุคต่อมารอสโก พาว (Roscoe Pound) กล่าวยกย่องบทความของวอเร็นและแบรนไดซ์ว่าคือการเพิ่มเนื้อหาบทใหม่ให้กับระบบกฎหมาย[8]

บทความของวอเร็นและแบรนไดซ์ให้สิทธิในความเป็นส่วนตัวได้รับความสนใจและมีชื่อเสียงขึ้นมาในระบบกฎหมายของประเทศอเมริกา แต่บทความดังกล่าวไม่ได้ให้รายละเอียด

---

[5]Moore, Adam and Ken Himma. "Intellectual Property", *The Stanford Encyclopedia of Philosophy* (Fall 2022 Edition), Edward N. Zalta & Uri Nodelman (eds.). Accessed December 14, 2022, Available from: https://plato.stanford.edu/archives/fall2022/entries/intellectual-property

[6] คำนี้เคยถูกกล่าวมาก่อนโดยผู้พิพากษา Thomas M. Cooley

[7] Warren, Samuel D., and Louis D. Brandeis. “The Right to Privacy,” Harvard Law Review 4, no. 5 (1890): 193–220.

[8] Letter from Roscoe Pound to William Chilton (1916), quoted in A. Mason, *Brandeis: A Free Man's Life*, p. 70 (1956), cited by Glancy 1979, p. 1.

ของสิทธิในความเป็นส่วนตัวว่ามีลักษณะเช่นไร และจะได้รับการปกป้องคุ้มครองอย่างไร ในยุคต่อมาจึงมีนักกฎหมายและนักวิชาการอีกหลายคนที่ได้พัฒนาแนวคิดของสิทธิในความเป็นส่วนตัวต่อไป เช่น วิลเลียม พรอสเซอร์ (William Prosser) ได้ทำให้สิทธิในความเป็นส่วนตัวของวอร์เร็นและแบนรไดซ์เป็นระบบมากขึ้นด้วยการจำแนกสิทธิในความเป็นส่วนตัวออกเป็นการละเมิด 4 ประเภท ได้แก่ 1). การรุกล้ำพื้นที่หรือการก้าวก่ายเรื่องราวส่วนตัว 2). การเปิดเผยข้อเท็จจริงที่หน้าอับอายของโจทก์ 3). การทำให้สาธารณชนเข้าใจโจทก์ผิด 4). การหาผลประโยชน์จากข้อมูลส่วนตัวของผู้อื่น[9]

อลัน เวสติน (Alan Westin) ได้เขียนหนังสือชื่อ “Privacy and freedom” ซึ่งนำแนวคิดของวอร์เร็นและแบรนไดซ์ก้าวเข้ามาสู่ศตวรรษที่ 21 โดยกล่าวว่าความเป็นส่วนตัวคือเหตุผลที่ปัจเจกบุคคล กลุ่มบุคคล หรือสถาบันใช้ยกขึ้นอ้างเพื่อที่จะกำหนดว่าข้อมูลส่วนตัวของพวกเขาจะถูกถ่ายทอดหรือสื่อสารออกไปสู่ผู้อื่นเมื่อใด อย่างไร และภายใต้ขอบเขตเพียงใด[10] ในหนังสือเวสตินกล่าวว่าความเป็นส่วนตัวนำไปสู่อิสรภาพ และเป็นสิทธิของปัจเจกบุคคลที่จะกำหนดว่าจะเปิดเผยข้อมูลส่วนบุคคลแค่ไหนและเปิดเผยต่อใคร นอกจากนี้ยังรวมไปถึงวิธีที่จะเก็บรักษาข้อมูลและวิธีเผยแพร่อีกด้วย แนวคิดของเวสติน ต่อมาได้พัฒนาไปเป็นรากฐานของกฎหมายที่เกี่ยวกับความเป็นส่วนตัวในโลกออนไลน์ [11]

แดเนียล เจ โซลอฟ (Daniel J. Solove) กล่าวว่าความเป็นส่วนตัวคือแนวคิดที่ยังคงมีความสับสนอยู่ นักวิจารณ์กล่าวว่าแนวคิดในเรื่องความเป็นส่วนตัวมีความคลุมเครือเกินไปจนไม่เกิดประโยชน์มากนักในทางปฏิบัติ เพราะเมื่อเราพูดถึงการรุกล้ำความเป็นส่วนตัว เรามักไม่สามารถอธิบายได้ว่าทำไมการรุกล้ำนั้นจึงถือเป็นการคุกคามที่เป็นอันตราย บ่อยครั้งที่การให้เหตุผลของฝ่ายที่ไม่สนับสนุนสิทธิในความเป็นส่วนตัว เช่น เพื่อเสรีภาพในการแสดงความคิดเห็น (free speech) การเพิ่มประสิทธิภาพในการทำธุรกรรมของลูกค้า หรือความมั่นคงปลอดภัย เป็นต้น เป็นเหตุผลที่ฟังขึ้นมากกว่า ดังนั้นการพยายามจะให้คำจำกัดความที่เป็นหนึ่งเดียวและอธิบายทุกสิ่งที่เกี่ยวกับความเป็นส่วนตัวจะนำไปสู่สภาวะกลืนไม่เข้าคายไม่ออก (dilemma)

---

[9] Daniel J. Solove and Neil M. Richards, “Prosser’s Privacy Law: A Mixed Legacy,” California law review 98 1887 (December 2010): 1889-1890.

[10] Maria Tzanou, “Data Protection as a Fundamental Right,” in The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance, (Oxford, Hart Publishing, 2017), p.11.

[11] Jubin Gorji, Olivia Graham, Michele Wang. “Overview of Privacy and Privacy Legislation” [online]. 2021. Accessed 14 December, 2022, Available from: https://projects.iq.harvard.edu/privacyproject/overview-privacy-legislation.

กล่าวคือถ้าให้ความหมายกว้างเกินไปกฎหมายก็จะมีความคลุมเครือไม่แน่นอน แต่ถ้าหากให้ความหมายอย่างแคบก็จะทำให้การคุ้มครองที่กฎหมายจะบังคับให้ถูกจำกัดลง[12] อย่างไรก็ตาม แม้ว่าจะยังไม่มีข้อยุติเรื่องความหมายของสิทธิในความเป็นส่วนตัว แต่ความสำคัญของสิทธิในความเป็นส่วนตัวก็ไม่ได้ลดน้อยลงแต่อย่างใด กลับยิ่งทวีความสำคัญมากขึ้นเรื่อย ๆ ในโลกยุคปัจจุบัน

2.3. สิทธิในความเป็นส่วนตัวกับกฎหมายละเมิด

ก่อนที่จะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัวถูกคุ้มครองภายใต้กฎหมายละเมิดลักษณะของกฎหมายละเมิดตั้งอยู่บนนโยบายการจัดการความเสียหายที่เกิดขึ้นแล้ว (Ex-post) กฎหมายประเภทนี้เป็นการกำหนดบทลงโทษที่ไม่อาจควบคุมหรือป้องกันความเสียหายในอนาคตได้ โดยกฎหมายละเมิดตั้งอยู่บนพื้นฐานของทฤษฎีที่ว่าบุคคลจะมีความรับผิดต่อเมื่อเขาก่อความเสียหายให้กับผู้อื่น[13] ดังนั้นกฎหมายละเมิดจะถูกบังคับใช้ต่อเมื่อมีการกระทำความผิดและมีความเสียหายเกิดขึ้น ซึ่งโจทก์มีภาระในการพิสูจน์ว่าได้รับความเสียหายจากการกระทำของจำเลย หลักเกณฑ์ว่าการกระทำใดบ้างจะเป็นความผิดกฎหมายไม่ได้เขียนไว้อย่างชัดเจนเพราะการคุ้มครองผู้เสียหายจะถูกจำกัด แต่จะเปิดช่องให้ผู้พิพากษาใช้ดุลพินิจ เช่น การพิจารณาว่าการกระทำของจำเลยประมาทหรือไม่ก็จะต้องพิจารณาเป็นรายกรณีไป บุคคลจึงไม่สามารถคาดเดาผลกระทบจากการกระทำของตนได้อย่างแน่นอนว่าการกระทำดังกล่าวเป็นความผิดหรือไม่[14] โดยผลที่ตามมาได้แก่ความเสี่ยงที่การกระทำจะเป็นความผิดตามกฎหมายและความเสี่ยงจากการถูกฟ้องร้องจะทำให้บุคคลเพิ่มความระมัดระวังในการกระทำของตนมากที่สุด[15] ซึ่งแนวคิดที่ได้กล่าวมานี้แตกต่างจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลในยุคปัจจุบันที่ใช้แนวคิดเชิงป้องกัน (Ex ante) อันเป็นแนวคิดที่ต้องการสร้างมาตรฐานให้บุคคลปฏิบัติตามเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในอนาคต

---

[12] Daniel J. Solove, “The meaning and value pf privacy,” in Social Dimensions of Privacy: Interdisciplinary Perspectives, eds. B. Roessler & D. Mokrosinska (Cambridge, Cambridge University Press, 2015), PP. 73-74.

[13] Christopher H. Schroeder, “Corrective Justice and Liability for Increasing Risks,” *UCLA Law Review* 37 (1990): 439.

[14] Aiken, Jane H., "Ex Post Facto in the Civil Context: Unbridled Punishment,” *Georgetown Law Faculty Publications and Other Works* 37 (1992): 439.

[15] Kolstad, C. D., Ulen, T. S., and Johnson, G. V, “Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements?,” The American Economic Review 80(4) (September 1990): 888.

กฎหมายละเมิดจะพิจารณาหน้าที่ซึ่งในระบบกฎหมายละเมิดของคอมมอนลอว์จะมีสิ่งที่เรียกว่า หน้าที่ต้องระมัดระวัง (Duty of care) โดยหน้าที่คือองค์ประกอบหนึ่งที่สำคัญของละเมิดอันเกิดจากความประมาท เพราะการที่จำเลยจะมีความรับผิดฐานละเมิดต้องปรากฏว่าจำเลยมีหน้าที่บางประการต่อโจทย์ในอันจะต้องระมัดระวังตามสมควร และจำเลยล้มเหลวในการปฏิบัติตามมาตรฐานที่กฎหมายกำหนดและการกระทำนั้นนำไปสู่ความเสียหาย ซึ่งความเสียหายเป็นผลโดยตรงจากการกระทำโดยประมาท[16]

นอกจากนี้กฎหมายละเมิดยังมีหลักความยินยอมไม่เป็นละเมิด (Volenti non fit injuria)[17] กล่าวคือถ้าหากผู้เสียหายได้ให้ความยินยอมไว้ก่อนแล้ว แม้ว่าจะมีความเสียหายเกิดขึ้น ก็จะไม่สามารถเรียกร้องค่าเสียหายได้ ยกตัวอย่างเช่น การที่บุคคลสมัครใจเข้าชกมวยกัน ถึงแม้ว่าจะได้รับบาดเจ็บก็ไม่สามารถเรียกร้องค่าเสียหายจากอีกฝ่ายได้เพราะเป็นเรื่องปกติธรรมดาที่ผู้ชกมวยต้องได้รับความเสียหายจากการกระทำ โดยขอบเขตในการให้ความยินยอมค่อนข้างจะกว้างขวางและไม่ได้มีกฎหมายกำหนดมาตรฐานไว้ว่าความยินยอมแบบใดหรือลักษณะใดจะมีผลหรือไม่มีผลบังคับ เพียงแต่มีหลักการว่าความยินยอมนั้นจะต้องไม่ขัดต่อกฎหมายหรือศีลธรรมอันดีของประชาชน เป็นต้น หลักการให้ความยินยอมดังที่กล่าวมานี้ถือได้ว่าทำได้โดยสะดวกและมีมาตรฐานไม่เข้มงวดซึ่งจะแตกต่างจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลในปัจจุบันที่เพียงแต่เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมก็ยังไม่ถือว่าเพียงพอ แต่จะมีหลักเกณฑ์อื่นๆ ที่เข้ามาชี้อีกว่าความยินยอมจะมีผลหรือไม่ ซึ่งได้กล่าวถึงรายละเอียดในส่วนต่อไป

3. กฎหมายคุ้มครองข้อมูลส่วนบุคคลในฐานะที่เป็นมาตรการป้องกัน

3.1 พัฒนาการกฎหมายคุ้มครองข้อมูลส่วนบุคคล

หากไม่เป็นการนับตั้งแต่ความเป็นมาของสิทธิส่วนบุคคล นับตั้งแต่ปี ค.ศ. 1974 ได้มีการพัฒนาและกำหนดออกมาเป็นลายลักษณ์อักษรที่สื่อถึงการคุ้มครองข้อมูลส่วนบุคคลอย่างจริงจังเพื่อใช้บังคับ ซึ่งจะเห็นได้จากความพยายามในการออกกฎหมายไม่ว่าจากทางสหรัฐฯ และทางสหภาพยุโรป ในการคุ้มครองข้อมูลในเรื่องต่าง ๆ

---

[16] Kidner, Richard, “Negligence: The Basic Principles of Duty of Care,” In Casebook on Torts, (Oxford: OUP Oxford, 2012), P.10.

[17] สุพัชรินทร์ อัศวธิตานนท์, “พัฒนาการของหลักกฎหมาย VOLENTI NON FIT INJURIA : ศึกษาการปรับใช้กับประเทศไทย,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2551).

ลำดับปี	เนื้อหา
FERPA (Family Educational Right and Privacy Act 1974) [18] And COPPA (Children's Online Privacy Protection Act 1998) [19]	กฎหมายเฉพาะ: FERPA เป็นกฎหมายที่เกี่ยวกับสาธารณสุขเพื่อที่จะคุ้มครองข้อมูลบันทึกส่วนตัวที่เกี่ยวกับการศึกษาของนักเรียน[20] ส่วน COPPA เป็นกฎหมายที่เกี่ยวกับการคุ้มครองผู้บริโภคในการคุ้มครองเด็กที่มีอายุต่ำกว่า 13 ปี
	มาตรการป้องกัน: FERPA กำหนดกำกับดูแลทุกโรงเรียนที่ได้รับทุนภายใต้โครงการที่เกี่ยวข้องของกระทรวงศึกษาธิการของสหรัฐฯให้ปฏิบัติตาม FERPA และให้สิทธิแก่ผู้ปกครองและนักเรียนที่ได้รับโอนสิทธิเมื่ออายุครบ 18 ปีหรือได้เข้าศึกษาในระดับสูงกว่ามัธยมมีสิทธิตาม FERPA ต่อข้อมูลบันทึกของตนเอง ส่วน COPPA กำหนดกำกับดูแล Operator หรือผู้ให้บริการบนเว็บไซต์หรือออนไลน์ที่มีความเกี่ยวข้องกับเด็กโดยตรงหรือได้ทราบถึงการดำเนินการเก็บข้อมูลเด็กจะต้องปฏิบัติตาม COPPA เพื่อป้องกันการกระทำความผิดต่อข้อมูลเด็ก
	กฎหมายเฉพาะ: กฎหมายที่เกี่ยวข้องกับหน่วยงานรัฐเพื่อที่จะคุ้มครองข้อมูลข่าวสารส่วนบุคคลของประชาชนที่ถูกจัดเก็บโดยหน่วยงานต่างๆ ของรัฐที่จัดเก็บข้อมูล

[18] 1.Centers for Disease Control and Prevention. Family Educational Rights and Privacy Act (FERPA). Page last reviewed: June 27, 2022. Accessed 8 November, 2022, available from: https://www.cdc.gov/phlp/publications/topic/ferpa.html.

2. U.S. Department of Education. Family Educational Rights and Privacy Act (FERPA). Accessed 8 November , 2022, Available from: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[19] 1. Education Framework. Student Privacy Laws: What District & School Administrators Need to Know. Accessed 8 November, 2022, Available from: https://educationframework.com/resources/student-privacy-laws/federal-laws.

กฎหมายทั้ง FERPA และ COPPA เป็นการตอบโจทย์ในการคุ้มครองข้อมูลส่วนบุคคล (Best Practice recommendation) ในการคุ้มครองข้อมูลที่อ่อนไหวของนักเรียน ซึ่งรายละเอียดล้วนเป็นกำหนดในเชิงกำกับดูแลเพื่อไม่ให้เกิดปัญหาภายหลัง ไม่ใช่เพื่อแก้ไขเมื่อปัญหาเกิดขึ้น

2. Ferderal Trade Commission. Children's Online Privacy Protection Rule "COPPA". Accessed 8 November, 2022, Available from: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

[20] มี 2 วัตถุประสงค์ในการคุ้มครองข้อมูลบันทึกส่วนตัวที่เกี่ยวกับการศึกษาของนัก เรียน:

(1) กำหนดให้"ผู้ปกครอง" (Parents) หรือ "นักเรียน" ซึ่งมีอายุถึง 18 ปี หรือได้เข้าไปศึกษาในสถานบันการศึกษาที่สูงกว่าระดับมัธยมปลาย (eligible students) สามารถควบคุมข้อมูลการศึกษาได้มากขึ้น

(2) กำหนดห้ามสถาบันศึกษาที่อยู่ภายใต้ FERPA เปิดเผยข้อมูลที่ระบุตัวตนจากข้อมูลบันทึกส่วนตัวที่เกี่ยวกับการศึกษา โดยปราศจากความยินยอมเป็นลายลักษณ์อักษรของนักเรียน หรือหากนักเรียนเป็นผู้เยาว์จะต้องได้รับความยินยอมจากผู้ปกครอง

กฎหมายฉบับนี้มีความต้องการที่จะให้เข้าใจในเนื้อหาและให้ปฏิบัติตามกฎหมาย ถือว่าเป็นเจตนารณ์ที่สำคัญในการคุ้มครองข้อมูลส่วนบุคคลทางด้านการศึกษาของนักเรียน

The Privacy Act 1974[21]	มาตรการป้องกัน: กำหนดให้หน่วยงานของรัฐจะต้องจัดหามาตรการอย่างเหมาะสมเพียงพอเพื่อวัตถุประสงค์ของกฎหมายคือ เพื่อมุ่งคุ้มครองและรับรองการบันทึกข้อมูล (record) ไม่ให้เกิดการทุจริตดังที่เคยเกิดขึ้นจากคดีวอร์เตอร์เกต (Watergate scandal)
TCPA (Telephone Consumer Protection Act 1986) and “National Do not call”[22 23] ข้อสังเกต คำนิยาม 1. FCC (US Federal Communications Commission) 2. FTC คือ (Federal Trade Commission)	กฎหมายเฉพาะ: กฎหมายที่เกี่ยวกับการตลาดผ่านทางโทรศัพท์ที่คุ้มครองข้อมูลของเจ้าของเบอร์โทรศัพท์
	มาตรการป้องกัน: การจำกัดการทำการตลาดผ่านทางโทรศัพท์และการใช้ระบบโทรออกอัตโนมัติและข้อความเสียงเทียมหรือที่บันทึกไว้ล่วงหน้า ซึ่งเป็นการกำหนดหน้าที่ต่อ ผู้ให้บริการที่เป็นบริการโทรคมนาคมสาธารณะ (common carriers) และนักการตลาดอื่นๆ เช่น นักการตลาดหรือ telemarketers โดย FCC และ FTC เป็นหน่วยงานรัฐที่ได้รับอำนาจการสร้างระบบทะเบียน “National Do not call Registry” ซึ่งเป็นมาตรการการจัดให้ผู้บริโภคลงทะเบียนห้ามโทรแต่ยังไม่มีผลบังคับจนกระทั้ง กฎหมายการลงทะเบียน (registry) มีผลบังคับใช้ในปี 2003 และบริหารจัดการโดย FTC
HIPPA (the Health Insurance Portability and Accountability Act 1996) [24]	กฎหมายเฉพาะ: กฎหมายที่เกี่ยวกับสาธารณสุขที่คุ้มครองข้อมูลสุขภาพของบุคคล

[21] 1.สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ. กฎหมายเฉพาะว่าด้วยการคุ้มครองส่วนบุคคล. สืบค้นเมื่อ 8 พฤศจิกายน 2256, จาก http://www.oic.go.th/FILEROOM/CABOICFORM02/DRAWER05/GENERAL/DATA0000/00000332.PDF.

2.สำนักงานคณะกรรมการข้อมูลข่าสารของราชการ. สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 12. สืบค้นเมื่อ 8 พฤศจิกายน 2256, จาก http://www.oic.go.th/FILEWEB/CABIWEBSITE/DRAWER01/GENERAL/DATA0007/00007545.PDF.

3. Office of the Privacy and Civil Liberties. Overview of the Privacy Act: 2020 Edition. Accessed 8 November, 2022, Available from: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction.

[22] ในปี 1986 เมื่อเทคโนโลยีโทรศัพท์เข้าถึงง่ายมากขึ้นซึ่งมาพร้อมกับการทำการตลาดผ่านทางโทรศัพท์โดยการโทรที่มาขึ้น ดังนั้นสภาจึงได้ออกกฎหมาย “Telephone Consumer Protection Act” (TCPA) โดยสภาคอนแกรส

[23] 1. Federal Communications Commission. FCC Actions on Robocalls, Telemarketing. Accessed 8 November, 2022, Available from: https://www.fcc.gov/general/telemarketing-and-robocalls.

2. techtarget, Wesley Chai. DEFINITION Telephone Consumer Protection Act (TCPA). Accessed 8 November, 2022, Available from: https://www.techtarget.com/whatis/definition/Telephone-Consumer-Protection-Act-TCPA#:~:text=The%20Telephone%20Consumer%20Protection%20Act%20(TCPA)%20of%201991%20is%20a,consumers%20from%20invasive%20telemarketing%20practices.

[24] HHS.gov. Summary of the HIPAA Privacy Rule. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

	มาตรการป้องกัน: กำหนดมาตรฐานความเป็นส่วนตัวของข้อมูลสุขภาพที่ระบุตัวบุคคลได้ หรือ “Privacy Rule” โดยกำหนดมาตรฐานการใช้และการเปิดเผยข้อมูลสุขภาพส่วนบุคคลที่จัดเก็บโดยองค์กรที่เกี่ยวข้องกับสาธารณสุข หรือ “covered entities” ต่อข้อมูลสุขภาพส่วนบุคคล หรือ “protected health information” โดยมีหน่วยงาน OCR (The Office for Civil Rights) เข้ามากำกับดูแลภายใต้กฎหมายฉบับนี้
EU Data Protection Directive (Directive 95/46/EC 1995)	กฎหมายแม่บท: กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป
	มาตรการป้องกัน: แม้ว่าจะเป็นบทบัญญัติที่มีผลบังคับระหว่างประเทศฉบับแรก[25]แต่ไม่ถือว่าประสบความสำเร็จในการบังคับใช้[26]
FCRC (Fair Credit Reporting Act 1971)	กฎหมายเฉพาะ: กฎหมายที่เกี่ยวกับการกำกับดูแลการประกอบธุรกิจข้อมูลเครดิต
	มาตรการป้องกัน: การเข้าไปควบคุมการประกอบธุรกิจด้านการจัดเก็บข้อมูล โดยสร้างข้อกำหนดและกฎเพื่อสอดคล้องกับระบบข้อมูลเครดิต ซึ่งระบบข้อมูลเครดิต จะดำเนินการไปได้ก็ต่อเมื่อได้มีการจัดเก็บข้อมูลที่ถูกต้องเหมาะสมและเป็นประโยชน์ต่อการนำไปใช้งาน เรียกข้อมูลเหล่านี้ว่า Consumer Report ซึ่งถูกรวบรวมหรือจัดให้มีขึ้นโดยองค์กรที่จัดเก็บข้อมูลอย่าง Consumer Reporting Agency[27]
	กฎหมายเฉพาะ: กฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลทางด้านการเงิน

[25] นคร เสรีรักษ์. (5 เมษายน 2561). GDPR คืออะไร สำคัญอย่างไร? ทำไมจึงต้องเข้าใจ GDPR? : โดย นคร เสรีรักษ์. Matichon Online. จาก https://www.matichon.co.th/article/news_902461.

[26] Paul Voigt, *The EU General Data Protection Regulation (GDPR),* p.2 ; เจตนารณ์ของบทบัญญัติฉบับนี้เพื่อที่จะกำหนดการคุ้มครองสิทธิส่วนบุคคลขั้นพื้นฐานกับการประมวลผลข้อมูลผ่านกิจกรรมและเป็นการให้ความมั่นใจในการโอนข้อมูลอิสระระหว่างประเทศสมาชิกของสหภาพยุโรป แต่ไม่ประสบผลสำเร็จเนื่องจากบทบัญญัตินี้จะต้องได้รับการภาคยานุวัติในแต่ละประเทศทำให้การกำหนดมาตรการที่ไม่เหมือนกันและมีขั้นตอนในการดำเนินการหลายขั้นตอนทำให้ไม่ได้เป็นไปตามวัตถุประสงค์ของบทบัญญัตินี้

[27] ยอดวรุณ วิไลรัตน์,“ปัญหาข้อมูลเครดิตตามกฎหมายว่าด้วย การประกอบธุรกิจข้อมูลเครดิต,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขากฎหมายธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2560).

GLBA (Gramm Leach Billey Act 1999)[28]	มาตรการป้องกัน: การกำหนดให้สถาบันทางการเงินต่างๆ (financial institutions) เช่นธุรกิจที่ให้บริการทางการเงิน อธิบายข้อมูลของผู้ใช้บริการรวม การปฏิบัติต่อผู้ใช้บริการและมาตรการความปลอดภัยต่อข้อมูลที่อ่อนไหว[29]
GDPR (General Data Protection Regulation 2018)	กฎหมายแม่บท: กฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป โดย GDPR เป็นกฎหมายที่เข้ามาแทนที่ EU Data Protection Directive เพื่อพัฒนาให้เกิดความชัดเจนของกฎหมายและขจัดอุปสรรคในการไหลเวียนอย่างอิสระของข้อมูลส่วนตัวจากปัญหาที่เกิดขึ้นจาก EU Data Protection Directive
	มาตรการป้องกัน: กำหนดให้ผู้ใดก็ตามที่ประมวลผลข้อมูลส่วนบุคคลไม่ว่าจะเป็นข้อมูลพลเมืองของสหภาพยุโรป หรือผู้พำนักในสหภาพยุโรปแม้กระทั้งกรณีที่ขายสินค้าหรือบริการแก่บุคคลดังกล่าว ไม่ว่าบุคคลนั้นจะอยู่ในสหภาพยุโรปหรือไม่จะต้องปฏิบัติตามกฎหมาย GDPR[30]
PDPA (Privacy Data Protection Act 2019)	กฎหมายแม่บท: กฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย
	มาตรการป้องกัน: กำหนดให้มีกฎหมายที่คุ้มครองสิทธิความเป็นส่วนตัวซึ่งเป็นสิทธิขั้นพื้นฐานคือข้อมูลส่วนบุคคลเป็นการทั่วไป โดยกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป[31]

โดยสรุปพัฒนาการที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในระยะเวลาที่ผ่านมาก่อนที่จะถึงปี 2018 ได้มีการกำหนดกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลแต่เป็นเพียงเฉพาะเรื่องที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เว้นแต่กรณีเช่น EU Data Protection Directive (1995) ของสหภาพยุโรปแต่ไม่ได้ประสบผลสำเร็จ จนกระทั้งก่อให้เกิด GDPR ในปี 2018 ซึ่งเป็นการวางมาตรการที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปเป็นการทั่วไป ไม่ใช่การกำหนดคุ้มครองข้อมูลเฉพาะเรื่อง เช่นที่ผ่านมา ดังนั้น**มาตรการป้องกันก่อน GDPR จึงยังไม่เป็นมาตรฐานทางธุรกิจ**

[28]คีกฤทธิ์ สิงหพ, “พัฒนาการของการประกอบธุรกิจธนาคารพาณิชย์ในลักษณะของ Universal Banking และกลไกในทางกฎหมายในการคุ้มครองผู้บริโภคทางการเงิน: บทเรียนจากความล้มเหลวของการคุ้มครองผู้บริโภคที่ใช้บริการทางการเงินในช่วงวิกฤติเศรษฐกิจการเงินในประเทศสหรัฐอเมริกา ปี ค.ศ. 2008,” วารสารพัฒนบริหารศาสตร์.

[29] Federal Trade Commission, “Gramm-Leach-Bliley Act”.

[30] GDPR.EU. What is GDPR, the EU’s new data protection law?. Available from: https://gdpr.eu/what-is-gdpr/ .

[31] หมายเหตุ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในฐานะที่เป็นกฎหมายแม่บทเชิงป้องกัน

การศึกษากระบวนการการทำงานของกฎหมายข้อมูลส่วนบุคคลนั้นทำให้เกิดความเข้าใจในเรื่องหลักการการทำงานและวัตถุประสงค์ของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล นำไปสู่การเข้าใจกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยในฐานะกฎหมายแม่บทเชิงป้องกัน โดยจะศึกษาผ่าน GDPR หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป เนื่องจากเป็นกฎหมายแม่บท ที่กำหนดหลักเกณฑ์มาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป และเป็นมาตรฐานสากลอันถือเป็นแบบอย่างของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกิดขึ้นภายหลัง รวมถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของไทยซึ่งมีเนื้อหาสาระโดยได้รับอิทธิพลมาจาก GDPR[32]

3.2.1 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในฐานะมาตรการป้องกัน (Preventive measures)

การตรากฎระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคลลในยุโรป[33] เป็นยกตัวอย่างที่ดีในการอธิบายกฎหมายคุ้มครองข้อมูลส่วนบุคคลว่า “ทำไม” ถึงต้องคุ้มครองข้อมูลส่วนบุคคล และจะคุ้มครองข้อมูลส่วนบุคคล “อย่างไร” โดยขอแบ่งเพื่อสร้างความเข้าใจออกเป็น (1) *การคุ้มครองความเป็นส่วนตัว* และ (2) *การคุ้มครองข้อมูล*

การคุ้มครองความเป็นส่วนตัว (Privacy Protection) สหประชาชาติได้รับรองหลักการเรื่องสิทธิความเป็นส่วนตัวซึ่งบัญญัติในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (ICCPR)[34] ซึ่งให้หลักการในสิทธิความเป็นส่วนตัวว่าจะต้องไม่มีใครถูกแทรกแซงความเป็นส่วนตัว และมีสิทธิในการได้รับความคุ้มครองตามกฎหมาย[35] จะเห็นได้ว่าเป็นการอธิบายกรอบของสิทธิความเป็นส่วนตัวทั้งในภาคมหาชนและเอกชน ในส่วนสหภาพยุโรปได้บัญญัติ อนุสัญญาด้านสิทธิมนุษยชน

---

[32] นพดล นิ่มหนู, “หลักการคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเปรียบเทียบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับพระราชบัญญัติข้อมูลข่าวสารของราชการพ.ศ. 2540,” วารสารมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยมหาสารคาม, 41(3).

[33] Aurelia Tamo-Larrieux, *Designing for privacy and its legal framework,* p.73

[34] ศูนย์เฝ้าระวังสถานการณ์ภาคใต้ deep south watch. กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง. จาก https://deepsouthwatch.org/sites/default/files/archives/docs/iccpr_th.pdf, ICCPR ข้อ 17, ซึ่งแปลได้ว่า

“1. บุคคลจะถูกแทรกแซงความเป็นส่วนตัว ครอบครัว เคหสถาน หรือการติดต่อสื่อสารโดยพลการหรือไม่ชอบด้วยกฎหมายมิได้ และจะถูกลบหลู่เกียรติและชื่อเสียงโดยไม่ชอบด้วยกฎหมายมิได้

2. บุคคลทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายมิให้ถูกแทรกแซงหรือลบหลู่เช่นว่านั้น”.

[35] Aurelia Tamo-Larrieux, p.74

(EUCHR) ในเวลาต่อมา โดยอนุสัญญานี้กำหนดเงื่อนไขในการแทรกแซงสิทธิส่วนตัวว่าจะต้อง[36] (1) สอดคล้องกับกฎหมายหรือเป็นไปตามที่กฎหมายกำหนด (in accordance with the law or prescribed by law) และ (2) จำเป็นต่อสังคมประชาธิปไตย (necessary in a democratic society) จึงอาจสรุปได้ว่าการแทรกแซงสิทธิความเป็นส่วนตัวจะต้องเป็นไปตามกฎหมายซึ่งอยู่ภายใต้ความจำเป็น ได้สัดส่วนตามระบอบประชาธิปไตย และต้องเป็นไปตามวัตถุประสงค์โดยชอบด้วยกฎหมาย

ทั้ง 2 หลักการข้างต้นเป็นรากฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในยุโรป[37] แม้ว่ากฎหมายในประเทศเช่น กฎหมายที่มาจากฝ่ายนิติบัญญัติหรือมาจากคำพิพากษาที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล จะตีความเกี่ยวกับกรอบความคุ้มครองที่แตกต่างกันในแต่ละประเทศ แต่หลักการยังคงเหมือนกับ 2 หลักการข้างต้นคือ การที่พลเมืองไม่ควรถูกแทรกแซงโดยอำนาจรัฐ ซึ่งจะพบว่าแต่ละประเทศในยุโรปต่างมองว่าการคุ้มครองข้อมูลส่วนบุคคลเป็นสิ่งที่จำเป็นอย่างยิ่ง และเป็นการป้องกันเชิงห้ามปราม (เชิงแก้ไข) อย่างไรก็ดีการเพิ่มขึ้นของเทคโนโลยีดิจิทัลทำให้การเข้าถึงสิทธิความเป็นส่วนตัวที่ง่ายมากขึ้น แต่ละประเทศจำเป็นต้องสร้างมาตรการความปลอดภัย (เชิงป้องกัน) ซึ่งทำให้เกิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศนั้น ๆ

การคุ้มครองข้อมูล (Data Protection)[38] เกี่ยวข้องกับกฎหมายเรื่องอื่น ๆ ซึ่งหากดูตามตัวอย่างตารางข้างต้น จะเห็นได้ว่ามีการเกิดขึ้นของการคุ้มครองข้อมูลซึ่งนอกเหนือจากสิทธิความเป็นส่วนตัว (the right to privacy or personality) ซึ่งเป็นส่วนหนึ่งในการพัฒนากฎหมายที่เกี่ยวกับคุ้มครองข้อมูล แต่ก็ปฏิเสธไม่ได้ว่ากฎหมายที่เกี่ยวข้องกับการคุ้มครองสิทธิ

---

[36] European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights, The Scope of Article 8, p.7, 31 Aug 2022

Art. 8 “1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in

accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

[37] Bygrave, Data Privacy, p. 86, ได้กล่าว ICCPR ข้อ 17 กำหนดกรอบอย่างจำเป็นเรื่องการห้ามในการแทรกแซงความเป็นส่วนตัว ขณะ ECHR ข้อ 8 กำหนดกรอบเงื่อนไขการใช้สิทธิ “เคารพชีวิตส่วนตัว” โดยกำหนดเงื่อนไขในการอนุญาตให้แทรกสิทธิสิทธิดังกล่าวได้.

[38] Aurelia Tamo-Larrieux, p.75

ความเป็นส่วนตัว บุคลิกภาพ การหมิ่นประมาท ก็เป็นรากฐานของกฎหมายว่าด้วยการคุ้มครองข้อมูลเช่นเดียวกัน การคุ้มครองข้อมูลไม่ได้มีจุดประสงค์เพื่อคุ้มครองตัวข้อมูล แต่เป็นการคุ้มครองเจ้าของข้อมูลที่ถูกประมวลผล แนวคิดดังกล่าวได้รับการพัฒนาเพื่อที่จะทำให้การคุ้มครองข้อมูลกลายเป็นหลักการทั่วไป ทั้งนี้ไม่ได้มีเพียง EUCFR[39] เท่านั้นอแต่กฎหมายอื่น ๆ[40]ก็มีการพูดถึงเรื่องนี้ก่อนที่จะมี GDPR เช่นกัน จะเห็นได้ว่ากฎหมายต่าง ๆ ที่พูดถึงการคุ้มครองข้อมูลมีลักษณะเป็นชุดหรือคู่มือการแนะนำหลักการประมวลผลข้อมูลที่ระบุเงื่อนไขการดำเนินประมวลผลข้อมูลมากกว่า

เมื่อเทียบระหว่างทั้งสองหลักการจะพบว่า 1). สิทธิความเป็นส่วนตัวไม่ได้เป็นสิทธิโดยสมบูรณ์แต่จะต้องเป็นไปตามหลักการทำงานในสังคมนั้น ๆ การประมวลผลข้อมูลจะชอบธรรมก็ต่อเมื่อเป็นไปตามอรรถประโยชน์ของสังคมที่มองว่าเป็นเรื่องที่เหนือกว่าประโยชน์ส่วนตัว 2). การคุ้มครองข้อมูลจะเป็นข้อกำหนดที่เตือนให้กระทำตามกฎหมาย มากกว่าเป็นการสั่ง โดยถ้าไม่ได้อยู่ภายใต้หลักการประมวลผล ก็อาจเป็นการรุกล้ำสิทธิส่วนบุคคล

3.2.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในฐานะกฎหมายแม่บท (General Rule)

กฎหมายคุ้มครองข้อมูลส่วนบุคคลสามารถวางภาพรวมได้ว่า เรื่องใดบ้างที่จำเป็นจะต้องมีสำหรับการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยเป็นการสรุปหน้าที่ทางกฎหมายที่ผูกพันกับบุคคลองค์กรหรือหน่วยงาน[41]

1. ข้อบังคับสำหรับหน่วยงานหรือองค์กรจะต้องมี[42]

---

[39] Charter of Fundamental Rights of The European Union, Article 8, Protection of personal data

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority"

[40] Convention 108, Directive 95/46/EC (so-called e-Privacy Directive) and later adopted in the GDPR, OECD Privacy Guidance 1980

[41] Paul Voigt, *The EU General Data Protection Regulation (GDPR),* p.3

[42] (1) โดยผู้ควบคุมและผู้ประมวลผลจะต้องทำการบันทึกของการประมวลผลกิจกรรมนั้นโดยพิสูจน์ว่าปฏิบัติตาม GDPR ต่อหน่วยงานกำกับดูแล และให้ข้อมูลเรื่องข้อผูกพันต่อเจ้าข้อมูลส่วนบุคคล, (2) ถ้าเป็นกรณีที่ข้อมูลถูกใช้ในกิจกรรมหลักสำหรับกลยุทธ์ทางธุรกิจซึ่งประกอบไปด้วยการตรวจสอบเจ้าของข้อมูลอย่างสม่ำเสมอและเป็นระบบ หรือเป็นการประมวลผลข้อมูลที่เป็นข้อมูลอ่อนไหวเป็นจำนวนมาก, (3) จะต้องจัดให้มีการระบุการใช้มาตรการความปลอดภัยที่เหมาะสมในกรณีที่มีความเสี่ยงที่การประมวลผลข้อมูลจะทำให้ข้อมูลเกิดความเสี่ยงที่อาจเป็นการละเมิดสิทธิและเสรีภาพของเจ้าของข้อมูล, (4) เพื่อให้บังคับใช้ตามแนวคิด GDPR ได้ จะต้องระบุถึงแนวคิดของความเป็นส่วนตัว (the concepts of Privacy by Design and Privacy by

1). การบันทึกกิจกรรมการประมวลผลขององค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (Records of Processing) Activities), 2). การแต่งตั้งเจ้าหน้าที่ข้อมูลส่วนบุคคล (Designation of a Data Protection Officer), 3). การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment), 4). การคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบและค่าเริ่มต้น (Data Protection by Design and by Default), 5). มาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการ (Technical and Organizational Measures, 6). Data Subject Rights), 7). หนังสือแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Data Breach Notification), 8). การพัฒนาระบบป้องกันและจัดการข้อมูลส่วนบุคคล (Data Protection Management), 9). การแต่งตั้งตัวแทนมาจากนิติบุคคลที่ไม่ได้มาจากสหภาพยุโรป (Appointment of a Representative by Non-EU Entities) และ 10). จรรยาบรรณและการรับรอง (Codes of Conduct and Certifications)

2. ทำให้แน่ใจว่าได้ปฏิบัติตามตามกฎหมายของการประมวลผลซึ่งจะต้องมี[43] 1).

Default) ด้วยเพื่อเป็นไปตามวัตถุประสงค์ของการป้องกันข้อมูลของ GPDR, (5) เพื่อรับประกันความปลอดภัยของข้อมูลส่วนบุคคล จะต้องมีการระบุระดับมาตรการการคุ้มครองข้อมูลส่วนบุคคลตามความเสี่ยงของของการประมวลผลข้อมูลแต่ละเรื่องๆ ไป, (6) จะต้องได้รับการแจ้งสิทธิของผู้เป็นเจ้าของข้อมูลส่วนบุคคลแก่คนๆ นั้น, (7) จะต้องแจ้งต่อผู้เป็นเจ้าของข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง และกรณีที่เกิดความเสี่ยงดังกล่าว เจ้าหน้าที่ที่เกี่ยวข้องกับการตรวจสอบเจ้าเข้ามาช่วยเหลือผู้ควบคุมข้อมูล, (8) เป็นระบบการปฏิบัติตาม GDPR ภายในองค์กรเพื่อที่จะตรวจสอบ the data-protection-related และ safety-related requirement, (9) กรณีที่ไม่ได้อยู่ในขอบเขตการใช้กฎหมาย GDPR จะมีกำหนดตำแหน่ง an EU-Located representative ประสานงานสำหรับเจ้าของข้อมูลและหน่วยงานกำกับดูแล, (10) เป็นเครื่องพิสูจน์ว่าได้ปฏิบัติตาม GDPR และลดอุปสรรคในการพิสูจน์ต่อหน่วยงานกำกับดูแล

[43] (1) ห้ามให้มีการประมวลข้อมูลทุกกิจกรรมเว้นแต่กฎหมายกำหนด ซึ่งฐานกฎหมาย (Legal bases) ในการประมวลผลภายใน GDPR ได้มีการบัญญัติใน the Data Protection Direction มาก่อนแล้ว ยกตัวอย่างเช่น ฐานการความยินยอม (Valid Consent), ฐานกฎหมายอื่น ๆ ในการประมวลผลเช่น ฐานความจำเป็นทางสัญญา (Contractual necessity) หรือ ฐานโดยชอบด้วยกฎหมาย (legitimate interests of controller) รวมถึง วัตถุประสงค์ในการเปลี่ยนการประมวลผลข้อมูล ซึ่งต่างมีวิธีการใช้ฐานไม่เหมือนกัน, (2) การประมวลผลข้อมูลที่เป็นกิจกรรมระหว่างภายในองค์กร (Intra-Group) ควรจะมีมาตรฐานการคุ้มครองข้อมูลของตนเองภายในองค์กร และในกรณีการโอนข้อมูลจะต้องเป็นไปตามที่กฎหมายกำหนดซึ่งเทียบเท่าระดับการโอนข้อมูลให้กับบุคคลที่สาม (third Party), (3) ประเภทข้อมูลพิเศษซึ่งจะต้องได้รับการปกป้องและการประมวลผลข้อมูลเฉพาะจะต้องมีมาตรการในการคุ้มครองข้อมูลที่เหมาะสมซึ่งเป็นไปตามความเสี่ยงสูงของตัวข้อมูลดังกล่าว ซึ่งอาจกล่าวได้ว่าการประมวลผลข้อมูลที่เป็นข้อมูลประเภทพิเศษตามหลักถูกห้ามไม่ให้ประมวลผล ถ้าไม่ได้เป็นการยินยอม หรือความจำเป็นหรือ บริบทที่มีจะต้องมีการประมวลผลข้อมูลดังกล่าว, (4) ผู้ประมวลผลนั้นไม่ได้เป็นบุคคลที่สาม แต่อยู่ภายใต้ความต้องการของผู้ควบคุมข้อมูลและไม่ได้ต้องการฐานทางกฎหมาย ซึ่งรวมถึงผู้ประมวลผลที่อยู่ในประเทศที่สาม อย่างไรก็ตาม ผู้ควบคุมข้อมูลจะต้องเลือกผู้ประมวลผลข้อมูลที่เหมาะสมสามารถรับประกันการคุ้มครองข้อมูลในระดับของข้อมูลที่เหมาะสม และจะถูกบังคับอยู่ภายใต้ข้อผูกพันขององค์กรซึ่งอยู่ภายใต้ GDPR, (5) ข้อบังคับในการโอนข้อมูลออกจาก EU จะต้องมีมาตรการเฉพาะในการคุ้มครองข้อมูลตามความเหมาะสม หน่วยงานหรือองค์กรจะต้องยืนยันได้ว่า (1) การประมวลผลข้อมูลจะต้องให้เหตุผลทางกฎหมายได้ (2) มาตรการความปลอดภัยที่เหมาะสมจะต้องใช้ได้, (6) กรณีที่ผู้ส่งออกข้อมูลอยู่ใน EU และผู้นำเข้าข้อมูลอยู่นอก EU จะต้องจัดให้มีสัญญาที่เกี่ยวข้องกับการโอนข้อมูลคือ “The EU Standard Contractual Clauses” ซึ่งมาจาก the European

พื้นฐานทางกฎหมายสำหรับการประมวลผล (Legal Bases for Processing), 2). กิจการการประมวลผลภายในกลุ่ม (Intra-Group Processing Activities), 3). ข้อมูลส่วนบุคคลประเภทพิเศษ (Special categories of Personal Data), 4). ความเกี่ยวข้องของผู้ประมวลผล (Involvement of a Processor), 5). หลักเกณฑ์การโอนทั่วไปสำหรับประเทศที่สาม (General Requirements for Third Country Data Transfers, others), 6). ข้อสัญญามาตรฐานของสหภาพยุโรป (EU Standard Contractual Clauses), 7). การคุ้มครองความเป็นส่วนตัวระหว่างสหภาพยุโรปและสหรัฐอเมริกา (EU – U.S. Privacy Shield) และ 8). กฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (Binding Corporate Rules)

จากที่กล่าวถึงภาพรวมทำให้เกิดคำถามที่ว่าผู้ควบคุม (Controller) ผู้ประมวลผล (Process) เจ้าของข้อมูล (Data Subject) และฝ่ายที่สาม (Third party) คืออะไร จะต้องเข้าใจในเรื่องของ “ความเป็นส่วนตัว” ในเอกสารของ โซลอฟเรื่อง Taxonomy ซึ่งระบุถึงกิจกรรมที่กระทบสิทธิส่วนบุคคลว่าจะทำให้เกิดปัญหาหรือเกิดความเสียหายหรือไม่[44] โดยกิจกรรมนั้นเป็นปัญหาหรือไม่จะต้องพิจารณาผ่าน 1). การกำหนดนิยามกิจกรรมหรือการกระทำ 2). การอธิบายว่าเหตุใดจึงก่อให้เกิดปัญหาหรือเกิดความเสียหาย โดยกำหนดให้ชัดว่า “อะไรคือปัญหา” ในบริบทที่เกิดขึ้น การที่กำหนดได้ว่ากิจกรรมใดเกิดปัญหานั้นในทางกลับกันเท่ากับได้รู้ว่าสิ่งใดคือความเป็นส่วนตัว ซึ่งสามารถกำหนดได้อย่างง่ายมากขึ้นในบริบทที่ความเป็นส่วนตัวนั้นมีความหมายกำกวม นอกจากนี้ Taxonomy ได้แยกออกเป็น “ความเสียหาย” และ “ปัญหา”[45] กรณีคำว่า “ความเสียหาย” อาจเป็นได้ทั้งทางกายภาพและความเสียหายในเชิงนามธรรมซึ่งจะต้องเป็นความเสียหายที่กฎหมายได้ระบุไว้ สำหรับกรณีคำว่า “ปัญหา” ปัจจุบันปรากฏในลักษณะที่เป็นโครงสร้าง อาจเรียกได้ว่าเป็น “architectural problems” ซึ่งได้แยกออกมาเป็น 1). กรณีการเพิ่มความเสี่ยงที่ความเสียหายอาจจะเกิดขึ้น ได้แก่กิจกรรมการที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และ 2). กิจกรรมบางกิจกรรมที่อาจเป็นการเสียสมดุลของสังคมและอำนาจเชิงสถาบันในทางที่ไม่พึงประสงค์ แม้ว่าจะไม่เป็นการก่อให้เกิดความเสียหายโดยตรงแต่สามารถส่งกระทบต่อชีวิต

Commission หรือ National Supervisory Authorities โดยสัญญาฉบับนี้จะสอดคล้องกับมาตรการความปลอดภัยการโอนข้อมูลระหว่างประเทศอย่างเหมาะสม, (7) เป็นโครงสร้างทางกฎหมาย (legal framework) จาก the European Commission ซึ่งอนุญาตให้ หน่วยงานหรือองค์กรในสหรัฐฯรับรองลักษนะการแถลงตนเองว่าเป็นไปตามมาตรฐานหรือ a (self-)certification สำหรับเรื่องมาตรการคุ้มครองข้อมูลตามระดับข้อมูลที่เหมาะสม และ (8) กลุ่ม หน่วยงานหรือองค์กรที่รับผิดชอบซึ่งเกี่ยวข้องกับกิจกรรมทางเศรษฐกิจร่วมกันอาจจะต้องจัดให้มี Binding Corporate Rules เพื่อที่จะกำหนด (1) นโยบายคุ้มครองข้อมูลในภาพรวม(global privacy policy) ของกลุ่มสมาชิก และ (2) การโอนข้อมูลระหว่างประเทศไปยังกลุ่มสมาชิกที่อยู่ในประเทศสามที่ยังไม่ได้มีการคุ้มครองข้อมูลอย่างเพียงพอ.

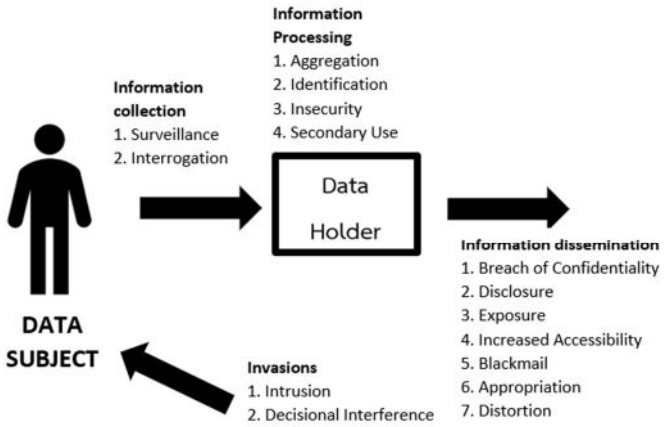
[44] Daniel J. Solove, A TAXONOMY OF PRIVACY, p.484 – 489.

[45] “harms” and “problems” privacy

ของบุคคลได้ เช่น อำนาจของเจ้าหน้าที่รัฐที่มีมากเกินไป การตรวจตรา (Surveillance) เป็นหนึ่งในผลกระทบดังกล่าว ความเสียหายชนิดนี้ก่อให้เกิดผลกระทบที่ทำให้บุคคลเกิดความไม่แน่ใจว่าอะไรที่เขาจทำได้หรือทำไม่ได้ (chilling effect) นอกจากนี้ในเวลาต่อมา จูลี่ โคเฮ็น และ พอล ชวอร์ท (Julie Cohen and Paul Schwart พัฒนา “ความเป็นส่วนตัว” โดยกำหนดความหมายว่า ความเป็นส่วนตัวเป็นองค์ประกอบหนึ่งของสังคมพลเรือน

โซลอฟได้แตกกลุ่มในการระบุกิจกรรมที่ก่อให้เกิดความเสียหายต่อความเป็นส่วนตัวดังนี้ 1). การเก็บรวบรวมข้อมูล (information collection), 2). การประมวลผลข้อมูล (information processing), 3). การเผยแพร่ข้อมูล (information dissemination) และ 4). การรุกล้ำข้อมูล (invasion) ซึ่งการแบ่งดังกล่าวนั้นจะวิเคราะห์คู่กับเจ้าของข้อมูล (Data Subject)[46] โดยความสัมพันธ์อาจแสดงเป็นภาพตัวอย่างได้ดังนี้

(ภาพตัวอย่างที่ 1 ความสัมพันธ์ของแต่ละประเภท)[47]



จากภาพตัวอย่างที่ 1 ข้างต้น สรุปได้ว่ากิจกรรมใดที่กระทบต่อสิทธิความเป็นส่วนตัวจะต้องสามารถระบุได้ว่าเป็น 1). กิจกรรมอะไร 2). อะไรคือปัญหาและเกิดความเสียหายอย่างไร จึงจะถือว่ากิจกรรมนั้นได้ละเมิดสิทธิแล้ว อาจกล่าวได้ว่า ถ้าข้อมูลนั้นประกอบไปด้วยสิทธิความเป็นส่วนตัวและสามารถระบุได้ว่าได้รับผลกระทบจากกิจกรรมใดกิจกรรมนึง ก็ถือว่าเป็นการละเมิด

[46] The individual whose life is most directly affected by activities classified in the taxonomy

[47] Daniel J. Solove, A TAXONOMY OF PRIVACY, p.490.

สิทธิของบุคคลนั้นแล้ว ซึ่งข้อมูลดังกล่าวเรียกได้ว่า “Personal Data”[48]เจ้าของข้อมูลของคนนั้นได้ว่า “Data Subject” ส่วนกรณี “Controller” หากพิจารณาตาม GDPR[49] ประกอบไปด้วยคำว่า “Processing” จะมีความหมายทำนองว่า ปฏิบัติการใด ๆ หรือชุดของปฏิบัติการใดๆ ที่ดำเนินการกับข้อมูลส่วนบุคคลหรือชุดของข้อมูลส่วนบุคคล ไม่ว่าจะด้วยวิธีการอัตโนมัติหรือไม่ก็ตาม[50] ดังนั้นข้อมูลที่เกี่ยวข้องหรืออยู่ในกระบวนการประมวลผลข้อมูลนั้นเรียกได้ว่าเป็น Controller หรือ Data Controller ซึ่งสมัยก่อนเรียกผู้ควบคุมข้อมูลว่า Data holder ส่วนคำว่า “Processor”[51] เป็นผู้ประมวลผลแทนผู้ควบคุมหรือเรียกได้ว่าประมวลคำสั่งตามผู้ควบคุม ส่วน “Third Party” คือสิ่งที่นอกเหนือจาก Data Subject, Data Controller, Data Processor, หรือผู้ที่ได้รับอำนาจจากผู้ควบคุมข้อมูลหรือผู้ประมวลได้รับอำนาจในการประมวลผลข้อมูลส่วนบุคคล

GDPR อาจแบ่งขอบเขตในการบังคับใช้เป็น 3 ประการ ได้แก่ 1). กรณีใดที่บทบัญญัติให้บังคับใช้[52] ซึ่งอาจแบ่งการพิจารณาออกเป็น (1) Processing กำหนดว่าอะไรเป็นการประมวลผลข้อมูล (2) Personal Data การประมวลผลข้อมูลจะต้องสอดคล้องกับสิ่งที่ประมวลซึ่งจะต้องเป็นข้อมูลส่วนบุคคล และจะต้องระบุว่าข้อมูลดังกล่าวเป็นข้อมูลประเภทอะไร เช่นเป็นการระบุว่าอะไรคือ Data Subject, Anonymization หรือ Pseudonymization โดยแต่ละข้อมูลนั้นมีผลต่อการปฏิบัติตามกฎหมายของผู้ที่ประมวลผล และอะไรเป็นข้อยกเว้นในการบังคับใช้บทบัญญัตินี้ และ 2). จะกำกับกับใคร บุคคล องค์กรหรือหน่วยงานใด เป็นที่เข้าใจว่าหากเป็นหน่วยงานหรือเป็นบุคคลที่จะต้องปฏิบัติตามภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ก็ต้องใช้ทรัพยากรเพื่อปฏิบัติตามกฎหมาย สิ่งที่สำคัญที่ควรจะต้องตระหนักก็คือ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้กำกับดูแลใคร นี่เป็นเรื่องที่สำคัญ เพราะหากไม่ได้เป็นบุคคลหรือหน่วยงานตามที่กฎหมายกำหนด ก็จะไม่ถูกบังคับให้ปฏิบัติตามกฎหมายฉบับนี้ โดยจะต้องเข้าใจว่าใครคือ “Controller” ใครคือ “Processor” และผู้ใดที่ได้ประโยชน์จากการคุ้มครองภายใต้ GDPR อีกทั้งบทบัญญัตินี้สามารถใช้ได้ที่ไหนบ้าง[53] ซึ่งแบ่งการพิจารณาออกเป็น (1) การ

---

[48] An identified or identifiable individual., Art.4 No.1 GDPR.

[49] Art.4 No.2 and 7 GDPR.

[50] GDPR ฉบับภาษาไทย, นคร เสรีรักษ์ ณรงค์ ใจหาญ ประสิทธิ์ ปิวาวัฒนพาณิช ศุภเกียรติ ศุภศักดิ์ศึกษากร นิชานันท์ นันทศิริศรณ์ แปลและเรียบเรียง; ได้ยกตัวอย่างการประมวลผลเช่น การเก็บรวบรวม, การบันทึก, การจัดระบบ, การวางโครงสร้าง การเก็บรักษา การปรับใช้หรือการแปรสภาพ การค้นคืน การสืบค้นข้อมูลเพิ่มเติม การใช้ประโยชน์การเปิดเผยโดยการส่งต่อ เผยแพร่หรือวิธีอื่นใดอันทำให้เข้าถึงได้ การจัดเรียงหรือรวมเข้าด้วยกัน การจำกัดการเข้าถึงการลบหรือทำลาย

[51] Art.4 No.8 GDPR

[52] Art.2 – Material Scope

[53] Art. 3 -Territorial scope

ประมวลผลข้อมูลในบริบทของกิจกรรม (Data Processing in the context of the Activities) และ (2) การประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล (Processing of Personal Data of Data Subject)

ตารางเปรียบเทียบระหว่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) กับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)

	GDPR	PDPA
Scope	Art. 3, 4 (1) Recital 2,14, 22 – 25	Section 4-6, 37(2)
1. Personal scope	- มีผลบังคับใช้กับหน่วยงานของรัฐ - มีการใช้กับบุคคลธรรมดาไม่ว่าจะมีสัญชาติใดหรือพำนักที่ไหน ซึ่งเกี่ยวข้องการประมวลผลข้อมูลของท่าน	- ไม่มีผลบังคับใช้กับหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐตามมาตรา 4 (3) - มีการใช้กับ Data subjects ในประเทศไทยและไม่ได้ระบุชัดเจนถึงสัญชาติและแหล่งที่พำนัก ซึ่งเกี่ยวข้องการประมวลผลข้อมูลของท่าน
2. Territorial scope	Art. 3, 4, 11 Recital 2, 14, 22-25 - สอดคล้องกัน	Section 5 - สอดคล้องกัน
3. Material scope	Art.2, 3, 4, 9, 26 Recitals 15-21, 26 - กำหนดถึงวิธีการประมวลผลข้อมูลว่าเป็น automated means or non-automated means ถ้าเป็นการจัดระเบียบข้อมูลเป็นการจัดเก็บเอกสาร (filling system) - ไม่รวมกับ “ข้อมูลนิรนาม” (anonymized) จากการใช้ GDPR - ไม่รวมกับองค์กรนิติบัญญัติ - ไม่ได้พูดถึงบริษัทข้อมูลเครดิตและการดำเนินการของบริษัทดังกล่าว	Sections 4, 5, 26 - ไม่ได้กำหนดความแตกต่างในเรื่องการประมวลผลข้อมูล - แม้ว่าจะ PDPA จะให้สิทธิในการขอให้ข้อมูลเป็นข้อมูลนิรนาม แต่ไม่ได้กำหนดชัดเจนว่าไม่บังคับใช้กับข้อมูลนิรนามด้วย - ไม่รวมกับภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี - ไม่รวมการดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วย การประกอบธุรกิจข้อมูลเครดิต

Key definitions	Art.4(1), 9 Recitals 26-30	Section 6, 22, 23, 26, 33
Personal data	- GDPR ระบุว่าข้อมูลที่ระบุตัวตนบนโลกออนไลน์อาจได้รับการพิจารณาว่าเป็นข้อมูลส่วนบุคคล เช่น IP addresses, cookie identifiers, และ radio frequency identification tags. - GDPR ไม่บังคับใช้กับข้อมูลนิรนาม anonymized กล่าวคือข้อมูลประเภทที่ไม่สามารถระบุไปถึงเจ้าของข้อมูลได้	- The PDPA ไม่ได้กล่าวถึง IP addressed, cookie identifiers และ radio frequency identification tags ไว้เป็นการเฉพาะ - แม้ว่า PDPA จะให้สิทธิร้องขอว่าให้ข้อมูลส่วนบุคคลถูกทำให้เป็นข้อมูลนิรนาม แต่ไม่ได้ยกเว้นอย่างชัดเจนในส่วนข้อมูลนิรนามจากการบังคับใช้ในกฎหมายฉบับนี้
Pseudonymization	Art. 4(5), 11 Recitals 26, 28 - มีการกำหนดนิยาม	Section 33 - ไม่มีการกำหนดนิยาม
Controllers and processors	Art. 4, 17, 28, 30, 32, 33, 35, 37, 38 Recitals 64, 90, 93 - สอดคล้องกัน	Sections 5, 6, 30-41 - สอดคล้องกัน
Children	Art. 6, 8, 12, 40, 57 Recitals 38, 58, 75 - GDPR พิจารณาเด็กในฐานะบุคคลธรรมดาในฐานะบุคคลที่มีความอ่อนไหวพิเศษ “vulnerable natural persons” ซึ่งสมควรได้รับการคุ้มครองข้อมูลส่วนบุคคลเป็นกรณีพิเศษ ยกตัวอย่างเช่นการคุ้มครองข้อมูลส่วนบุคคลของเด็กในกรณีที่ข้อมูลถูกนำไปใช้ในการทำการตลาดหรือการเก็บรวบรวมข้อมูลที่นำไปใช้เพื่อจัดทำบริการที่มุ่งต่อเด็กโดยตรง - เมื่อข้อมูลส่วนบุคคลของเด็กถูกกล่าวอ้างถึง ผู้ควบคุมข้อมูลต้องใช้มาตรการที่เหมาะสมในขั้นตอนการการส่งต่อข้อมูลไปเพื่อการประมวลในรูปแบบที่แม่นยำ โปร่งใส เข้าใจและเข้าถึงได้ง่าย ใช้ภาษาที่เข้าใจง่ายและชัดเจนเพื่อที่เด็กจะสามารถเข้าใจได้ - GDPR บัญญัติว่าผู้ควบคุมข้อมูลมีหน้าที่ต้องใช้ความพยายามอย่างเหมาะสมตามสมควรในการยืนยันว่าได้มีการให้ความยินยอมหรือได้รับอนุญาตโดยผู้แทนโดยชอบธรรมหรือผู้ปกครองแล้ว - GDPR บังคับใช้กับบริการสารสนเทศ (information services)	Sections 19, 20(1), 20(2) - PDPA ไม่ได้ระบุมาตราการคุ้มครองไว้โดยเฉพาะในกรณีที่ข้อมูลส่วนบุคคลของเด็กที่ถูกนำไปใช้ในการทำการตลาดหรือการเก็บรวบรวมข้อมูลเพื่อจัดทำบริการที่มุ่งต่อเด็กโดยตรง - PDPA ไม่ได้กำหนดแนวทางที่ต้องทำไว้ให้กับผู้ควบคุมข้อมูลเมื่อกล่าวถึงข้อมูลส่วนบุคคลของเด็กหรือเมื่อนำเสนอข้อมูลต่อเด็ก - PDPA ไม่ได้ระบุว่าผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นที่จะต้องใช้ความพยายามอันมีเหตุผลตามสมควรในการยืนยันว่าได้รับความยินยอมหรือได้รับอนุญาตโดยผู้แทนโดยชอบธรรมหรือผู้ปกครองของเด็กแล้ว - PDPA มีขอบเขตกว้างกว่า
Research	Art. 5(1)(b), 9(2)(j), 14(5), 17(3), 21(6), 89 Recitals 33, 159-61	Sections 24, 26, 32

	- GDPR อธิบายว่าการประมวลผลข้อมูลส่วนบุคคลเพื่อจุดประสงค์ในการวิจัยทางวิทยาศาสตร์ควรถูกตีความอย่างกว้าง ยกตัวอย่างเช่นให้รวมถึง การสาธิตหรือการพัฒนาทางด้านเทคโนโลยี การวิจัยพื้นฐาน การวิจัยประยุกต์ และการวิจัยโดยทุนส่วนตัว - ภายใต้ GDPR เมื่อข้อมูลส่วนบุคคลได้รับการประมวลผลเพื่อจุดประสงค์ด้านการวิจัย สมาชิกรัฐภาคีอาจจะเพิกถอนสิทธิบางอย่างของเจ้าของข้อมูลส่วนบุคคล เช่น สิทธิเข้าถึงข้อมูลส่วนบุคคล สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สิทธิในการคัดค้านและสิทธิในการจำกัดการประมวลผล เมื่อสิทธิเช่นว่านั้นจะทำให้การบรรลุวัตถุประสงค์หนึ่งใดไม่อาจเกิดขึ้นได้หรือเกิดความเสียหายอย่างร้ายแรง โดยการเพิกถอนสิทธิต้องเป็นสาระสำคัญต่อการบรรลุวัตถุประสงค์	- PDPA ไม่ได้ให้คำจำกัดความของการวิจัยทางวิทยาศาสตร์ - PDPA ไม่มีเนื้อหาเรื่องการเพิกถอนสิทธิของเจ้าของข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ด้านการวิจัย
Legal basis	Art 5-10 Recitals 39-48 - สอดคล้องกัน	Sections 19, 24, 26 - สอดคล้องกัน
Controller and processor obligations **Data transfers**	Art 44-50 Recitals 101, 112 - จะต้องเป็นการโอนข้ามพรมแดนที่ได้รับการอนุมัติโดย ข้อตกลงระหว่างประเทศสำหรับความร่วมมือทางศาล - จะต้องเป็นการโอนที่มาจากการลงทะเบียนซึ่งสอดคล้องกับกฎหมายของแต่ละประเทศนั้นหรือกฎหมายในสหภาพหรือโดยอ้างประโยชน์โดยชอบธรรม	Section 28, 29 - ไม่ได้ระบุเป็นการเฉพาะในการปฏิบัติตามคำตัดสินของศาลหรือคำตัดสินของประเทศที่สามที่มีอำนาจ - ไม่ได้กล่าวถึง
Data processing records	Art. 30 Recital 82 - มีการกำหนดรายชื่อข้อมูลที่ Data processor จะต้องบันทึก - มีการกำหนดรายชื่อข้อมูลที่ Data controller จะต้องบันทึก การโอนข้อมูลส่วนบุคคลระหว่างประเทศ กับการระบุของประเทศที่ 3 หรือ องค์กรระหว่างประเทศ หรือเอกสารที่เกี่ยวกับมาตรการความปลอดภัยที่เหมาะสม	Sections 39, 40 - ไม่ได้ระบุที่จะต้องบันทึก - ไม่ได้ระบุไว้ชัดเจน
Data protection impact assessment (DPIA)	Art. 35-36 Recitals 75, 84, 89-93 - มีการกำหนดให้ ทำ DPIA หากเป็นไปตามสถานการณ์ที่กำหนดไว้ - มีการกำหนดการประเมินจะต้อง	Sections 37, 40 - ใช้เฉพาะกรณีที่จำเป็นมีการเปลี่ยนเทคโนโลยี ให้ปฏิบัติตามมาตราฐานขั้นต่ำที่กำหนดเฉพาะโดย สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือ สคส. (PDPC)

	ประกอบไปด้วยสิ่งที่กฎหมายกำหนด - Data controller จะต้องมีการขอคำปรึกษากับ ผู้มีอำนาจกำกับดูแลก่อนการประมวลผลที่อาจจะมีความเสี่ยงที่จะไม่มีมาตรการเยียวยาตามที่ระบุไว้ใน DPIA	- ไม่มีการกำหนดขอบเขตไว้ - ไม่มีการกำหนดว่าจะต้องขอคำปรึกษาของผู้มีอำนาจก่อนการประมวลผล
Data protection officer appointment	Articles 13-14, 37-39 Recital 97 - สอดคล้องกัน - เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะได้รับแต่งตั้งในกรณีที่ดำเนินการประมวลผลโดยหน่วยงานของรัฐหรือหน่วยงานอื่นๆ - เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตอบรับความเป็นอิสระของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	Sections 29, 41, 42 - สอดคล้องกัน - ผู้ที่มีอำนาจหรือหน่วยงานอื่นๆ ที่ต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องได้รับประกาศจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล - PDPA ไม่ได้กล่าวถึงความเป็นอิสระของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างชัดเจน
Data security and data breaches	Art. 5, 24, 32-34 Recitals 74-77, 83-88 - ภายใต้ GDPR ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้กับเจ้าของข้อมูลส่วนบุคคลในกรณีที่มีแนวโน้มความเสี่ยงสูงที่จะมีการละเมิดข้อมูลอันมีผลกระทบต่อสิทธิและเสรีภาพของข้อมูลส่วนตัว เว้นแต่ • ได้มีการจัดมาตรการการคุ้มครองต่อตัวองค์กรและทางเทคนิคอย่างเหมาะสมแล้ว • มีมาตรการภายหลังเพื่อทำให้แน่ใจว่าจะไม่เกิดการละเมิดอีกอย่างเป็นรูปธรรม; หรือ • เกี่ยวข้องกับความพยายามที่ไม่ได้สัดส่วน - GDPR จะต้องมีการแจ้งการละเมิดข้อมูลส่วนบุคคลเป็นอย่างน้อยตาม GDPR ที่กำหนดมาเป็นรายชื่อ เช่น การแจ้งที่จะต้องอธิบายถึงลักษณะของการละเมิด จำนวนเจ้าข้อมูลข้อมูลที่มีความเสี่ยงที่จะถูกละเมิด และผลจากการละเมิดข้อมูล - GDPR จัดให้มีมาตรการขององค์กรและทางเทคนิคอย่างเหมาะสมตามที่ GDPR กำหนดเป็นรายชื่อในกรณีผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลดำเนินการจัดทำข้อมูลแฝง (pseudonymization), การเข้ารหัสข้อมูล (Encryption) และความสามารถในการเข้าถึงข้อมูลส่วนบุคคลในกรณีที่เกิดเหตุการณ์ทาง	Sections 24-26, 37, 40 - ปัจจุบัน PDPA ไม่ได้ให้ข้อยกเว้นที่เจ้าของข้อมูลส่วนบุคคลจะต้องแจ้งกรณีมีการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลอย่างรุนแรง อย่างไรก็ตาม ข้อยกเว้นเฉพาะอาจมีการบัญญัติภายหลังในอนาคตในรูปแบบเป็นมาตรการเพิ่มเติมของ PDPC - ปัจจุบัน PDPA จะไม่ได้กำหนดให้แจ้งกรณีที่มีการละเมิดข้อมูลส่วนบุคคลซึ่งในอนาคตอาจมีการบัญญัติเป็นมาตรการเพิ่มเติมของ PDPC - PDPA ไม่ได้ให้รายชื่อมาตรการขององค์กรและทางเทคนิค อย่างไรก็ตาม กฎหมายคุ้มครองข้อมูลส่วนบุคคลจะกำหนดรายชื่อมาตรการความปลอดภัยเป็นมาตรการเพิ่มเติมของ PDPC - PDPA กำหนดให้ผู้ประมวลผลข้อมูลจะต้องแจ้งต่อผู้ควบคุมโดยทันที แต่ไม่ได้ระบุระยะเวลาเป็นการเฉพาะ

	กายภาพหรือทางเทคนิคเพื่อทำให้แน่ใจว่าเป็นความลับและสมบูรณ์ - ผู้ประมวลผลข้อมูลจะต้องแจ้งผู้ควบคุมข้อมูลอย่างทันทีภายหลังที่ทราบถึงการละเมิดข้อมูลส่วนบุคคลไม่ล่วงเวลา (undue delay)	
Accountability	Art. 5, 24-25, 35, 37 Recital 39 - ค่อนข้างสอดคล้องกัน - N/A	Sections 37, 39 - ค่อนข้างสอดคล้องกัน - N/A
Individuals' Rights	Art.12, 17 Recital 59, 65 – 66	Section 23(6), 33
Right to erasure		
Right to be informed	Art. 5-13, 14, 47 Recitals 58-63	Sections 19, 21, 23-25, 27, 28, 31, 41, 73
Right to object	Art. 7, 12, 18, 21	Sections 19, 23, 32
Right to access	Art. 15 Recitals 59-64	Section 30
Right not to be subject to discrimination in the exercise of rights	- GDPR ไม่ได้ระบุถึงสิทธิที่จะไม่ถูกเลือกปฏิบัติไว้อย่างชัดแจ้ง ดังนั้นขอบเขตของการบังคับใช้จึงไม่ได้ถูกจำกัดความ	- PDPA ไม่ได้ระบุถึงสิทธิที่จะไม่ถูกเลือกปฏิบัติไว้อย่างชัดแจ้ง ดังนั้นขอบเขตของการบังคับใช้จึงไม่ได้ถูกจำกัดความ
Right to data portability	Art. 12, 20, 28 Recital 68, 73	Section 24, 31
Enforcement	Art. 83-84 Recitals 148-152	Sections 79-90
Monetary penalties		
Supervisory Authority	Art. 51-84 Recitals 117-140	Sections 8, 16, 71-76, 90
Civil remedies for individuals	Art. 79-80, 82 Recitals 131, 146-147, 149	Sections 73, 77-78

9.กฎหมายคุ้มครองข้อมูลส่วนบุคคลในฐานะมาตรฐานทางธุรกิจ

กฎหมายคุ้มครองข้อมูลส่วนบุคคลในฐานะกฎหมายแม่บทเชิงป้องกัน สิ่งที่จะต้องคำนึงในกฎหมายฉบับดังกล่าวไม่ได้คำนึงถึงบทลงโทษที่ปรากฏในกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งใน GDPR บทที่เกี่ยวกับการเยียวยา ความรับผิด และโทษนั้นมีเพียง 7 มาตราเท่านั้น อย่างไรก็ตามเกือบทั้งหมดของ GDPR เป็นการพูดถึงมาตราการป้องกันก่อนเกิดความเสียหายหรือปัญหา สิ่งที่จะต้องคำนึงจากกฎหมายฉบับดังกล่าวคือ (1) ข้อบังคับที่หน่วยงานหรือองค์กรต้องปฏิบัติตาม

(2) มีการประมวลผลข้อมูลส่วนบุคคลตามกฎหมายหรือไม่ กิจกรรมอะไรที่กระทบต่อข้อมูลส่วนบุคคล กฎหมายข้อมูลส่วนบุคคลไม่ว่าจะเป็น GDPR หรือ PDPA ในฐานะกฎหมายแม่บทอาจจะจัดให้มีกฎหมายเฉพาะหรือมาตรการเฉพาะเพื่อสำหรับเฉพาะเรื่องหรือขยายรายละเอียดจากเดิมเพื่อให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในฐานะกฎหมายแม่บท จากที่ได้อธิบายไปก่อนหน้า กฎหมายคุ้มครองข้อมูลส่วนบุคคลในปัจจุบันนั้นได้พัฒนาขึ้นโดยมีพื้นฐานมาจากหลักกฎหมายละเมิด กระทั่งกลายเป็นมาตรฐานทางธุรกิจ ที่เป็นการวางกฎเกณฑ์เพื่อกำกับดูแลองค์กร ซึ่งการเปลี่ยนแปลงนี้มีผลกระทบต่อองค์กรต่าง ๆ ดังต่อไปนี้

9.1 มาตรการป้องกันในฐานะที่เป็นมาตรฐานทางธุรกิจของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

PDPA และ GDPR เป็นกฎหมายที่ได้วางมาตรการป้องกันไว้เพื่อให้องค์กรปฏิบัติตาม ทุกองค์กรมีหน้าที่ในการวางระบบโครงสร้างและดำเนินการให้สอดคล้องกับ PDPA อันเปรียบเสมือนมาตรฐานขั้นต่ำของกฎหมาย เพื่อให้มั่นใจว่าการเก็บรวบรวม ใช้ เปิดเผย และการรักษาข้อมูลมีความปลอดภัยในระดับเกณฑ์ที่กำหนด ทั้งนี้ หากเกิดกรณีที่ข้อมูลส่วนบุคคลถูกเข้าถึงโดยไม่ชอบด้วยกฎหมาย แต่หากบริษัทได้ปฏิบัติตามมาตรฐาน PDPA แล้ว กล่าวคือ มีการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานแล้ว บริษัทก็ไม่มีความรับผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

ในตัวบท PDPA มีการกำหนดให้องค์กรต่างๆ ปฏิบัติให้ได้ตามมาตรฐาน[54] ทั้งนี้ มาตรฐานนี้เป็นไปตามข้อปฏิบัติที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด แต่ในปัจจุบันนี้การร่างแนวปฏิบัติจากคณะกรรมการนั้นยังไม่เสร็จสมบูรณ์ และอาจใช้เวลานานหลายปี ภาคประชาสังคมจึงมีการสร้างมาตรฐานและแนวปฏิบัติขึ้นเพื่อใช้ในกลุ่มวิชาชีพของตน หรือเพื่อเป็นแนวปฏิบัติแก่สาธารณะเพื่อให้หน่วยงานต่าง ๆ ปฏิบัติตามได้โดยง่าย ได้แก่ แนวปฏิบัติ (Guidelines) และหลักปฏิบัติด้านจรรยาบรรณ (Code of Conduct)

---

[54] มาตรา 4 “...ผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง (2) (3) (4) (5) และ (6) และผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานที่ได้รับยกเว้นตามที่กำหนดในพระราชกฤษฎีกาตามวรรคสอง ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไป*ตามมาตรฐาน*ด้วย”

มาตรา 22 (3) “...ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้*ตามมาตรฐาน*ของการเก็บรวบรวม”

มาตรา 28 “ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมี*มาตรฐาน*การคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ...” เป็นต้น

อีกข้อสังเกตหนึ่งก็คือ การเปลี่ยนแปลงการคุ้มครองจากพื้นฐานกฎหมายละเมิดมาเป็นมาตรการป้องกันนั้นทำให้ฐานทางกฎหมาย (Legal Basis) ที่ใช้เปลี่ยนไปด้วย กล่าวคือ หลักกฎหมายบางอย่างที่ใช้ได้กับกฎหมายละเมิด อาจไม่สามารถนำมาใช้กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่เป็นมาตรฐานทางธุรกิจได้ ตัวอย่างเช่น กรณีของการได้รับความยินยอมที่มีหลักเกณฑ์และเงื่อนไขในการได้รับต่างกันอย่างชัดเจน[55]

ความยินยอมในกฎหมายลักษณะละเมิด	เป็นไปตามหลัก “Volenti non fit injuria” หรือ "to a willing person, injury is not done" กล่าวคือ ความยินยอมไม่ก่อให้เกิดความเสียหายหรือไม่ทำให้เป็นละเมิด เนื่องจากการฟ้องร้องละเมิดถือเป็นเรื่องของปัจเจกชนในการใช้สิทธิทางกฎหมายของตนในการได้รับการเยียวยาค่าเสียหาย ดังนั้นถ้าผู้เสียหายไม่ติดใจที่จะเรียกค่าสินไหมทดแทน การกระทำนั้นก็ไม่เป็นละเมิด โดยความยินยอมนี้จะได้รับเมื่อใดและรูปแบบใดก็ได้
ความยินยอมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	การที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเป็นมาตรการป้องกัน ทำให้ไม่สามารถใช้หลัก “Volenti non fit injuria” ได้ เนื่องจากผู้ควบคุมข้อมูลจำเป็นต้องปฏิบัติตามมาตรการซึ่งถือเป็นมาตรฐานขั้นต่ำของกฎหมาย ไม่สามารถใช้หลักความยินยอมของเจ้าของข้อมูลเพื่อปฏิบัติให้แตกต่างจากกฎหมายนี้ได้ นอกจากนี้ การได้รับความยินยอมยังมีมาตรฐานอีกด้วย กล่าวคือ ต้องเป็นไปตามพระราชบัญญัติคุ้มครองส่วนบุคคลมาตรา 19 จึงจะเป็นความยินยอมที่ชอบกฎหมายและมีผลผูกพัน[56]

9.2 ข้อพิจารณาเกี่ยวกับมาตรฐานทางธุรกิจ

(1) มาตรการตามกฎหมายที่เป็นการรับรองมาตรฐานทางธุรกิจ

---

[55] CNIL. Record of processing activities. Accessed 8 November, 2022, Available from: https://www.cnil.fr/en/record-processing-activities.; มาตรฐานที่ต้องปฏิบัติเหล่านี้ยังรวมถึงหน้าที่บางประการที่มิได้เป็นมาตรการป้องกันในตัวเองอีกด้วย ตัวอย่างเช่น การจัดทำบันทึกรายการกิจกรรมการประมวลผล ตามมาตรา 39 ที่มีจุดประสงค์เพื่อให้ผู้ควบคุมข้อมูลได้ประเมินตนเองในขณะประมวลผลข้อมูล ว่าข้อมูลเหล่านั้นมีความจำเป็นต่อวัตถุประสงค์หรือไม่ และมีการรักษาความปลอดภัยที่เพียงพอแล้วหรือไม่ หรือการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล(Data Protection Impact Assessment : DPIA) ตาม GDPR ซึ่งเป็นการประเมินความเสี่ยงเพื่อที่จะออกแบบมาตรการป้องกันให้สอดคล้องกับความเสี่ยงนั้น สิ่งเหล่านี้แม้ไม่ใช่มาตรการป้องกันในตัวเอง แต่ก็เป็นมาตรฐานที่จำต้องปฏิบัติตามทั้งสิ้น

[56] มาตรา 19 ความยินยอมต้องได้รับก่อนหรือในขณะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล, ต้องขอโดยชัดแจ้ง, ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล, ต้องเข้าใจได้ง่าย, ต้องไม่เป็นเงื่อนไขในการเข้าถึงบริการ เว้นแต่เป็นฐานในการทำสัญญา, เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่าย

ในการดำเนินธุรกิจ ย่อมมีกฎหมายเข้ามาควบคุมในหลายภาคส่วน ไม่เพียงแต่องค์กรจำต้องปฏิบัติตามกฎหมายที่เกี่ยวกับการดำเนินกิจการของตนเท่านั้น แต่ยังต้องคำนึงถึงสิทธิของลูกจ้างและบุคคลภายนอกด้วย เช่น กฎหมายแรงงาน กฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นที่มุ่งคุ้มครองสิทธิมนุษยชน อันจะละเมิดไม่ได้ กฎหมายเหล่านี้เปรียบเสมือนข้อจำกัด หรือหน้าที่ขององค์กรธุรกิจในการต้องปฏิบัติตาม แต่ในทางกลับกัน หากองค์กรปฏิบัติตามกฎหมายเหล่านี้อย่างเคร่งครัด ย่อมเป็นการแสดงถึงความใส่ใจต่อบุคคลเหล่านั้นในการให้พวกเขาได้รับความคุ้มครองที่พึงได้รับ ไม่ว่าในฐานะลูกจ้าง เจ้าของข้อมูลส่วนบุคคล หรือบุคคลภายนอกอื่น ๆ เช่น ในการจัดตั้งโรงงาน ย่อมต้องคำนึงถึงทรัพยากรธรรมชาติและสิ่งแวดล้อม อันส่งผลโดยตรงต่อคุณภาพชีวิตของชุมชนโดยรอบ หากองค์กรดำเนินการโดยคำนึงถึงสิทธิมนุษยชนได้ดี ย่อมเป็นการสร้างความสัมพันธ์ที่ดีกับผู้มีส่วนได้เสีย[57] ซึ่งสามารถสร้างภาพลักษณ์และชื่อเสียงที่ดี และได้รับความไว้วางใจจากสาธารณชน จึงกล่าวได้ว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคล ที่เดิมทีมีจุดประสงค์เพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคลอันเป็นการเพิ่มหน้าที่ให้กับองค์กร แต่ในอีกแง่หนึ่งก็ได้กลายเป็นเครื่องมือในการสร้างชื่อเสียงที่ดีให้แก่บริษัท[58] ยิ่งเป็นเรื่องข้อมูลส่วนบุคคลที่ผู้มีส่วนได้เสียมีหลายกลุ่ม รวมถึงกลุ่มลูกค้าของบริษัท ยิ่งเห็นได้ชัด เนื่องจากในปัจจุบัน หลายองค์กรมีระบบให้ลูกค้าสมัครสมาชิกเพื่อนำข้อมูลไปประมวลผล จึงไม่แปลกใจที่เรามักเห็นบริษัทต่าง ๆ ให้ความสำคัญกับ PDPA เพื่อซื้อความไว้เนื้อเชื่อใจจากกลุ่มลูกค้าและรักษาภาพลักษณ์ขององค์กร อันเป็นผลดีต่อทั้งสองฝ่าย โดย GDPR มีมาตราซึ่งว่าด้วยการรับรอง ซึ่งสร้างแรงจูงใจให้องค์กรต่าง ๆ ที่ GDPR บังคับใช้เกิดความสนใจและปฏิบัติตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดด้วย

มาตรา 42 ของ GDPR สนับสนุนให้มีการจัดตั้งกลไกการรับรองการคุ้มครองข้อมูล โดยหน่วยงานกำกับดูแลที่มีอำนาจสามารถทำการรับรองได้ว่าองค์กรนั้นได้ปฏิบัติตามมาตรฐานที่ GDPR กำหนดครบถ้วนสมบูรณ์แล้ว[59] ซึ่งการรับรองนี้เป็นรูปแบบเครื่องหมายรับรอง (Certification Mark) หรือซีล (Seal) สัญลักษณ์เหล่านี้ เมื่อได้รับและเป็นที่ปรากฏต่อสาธารณชน ย่อมสร้างความเชื่อมั่นและเพิ่มความสามารถในการแข่งขันบนเวทีธุรกิจได้ เหมือน

---

[57] Business and Human Rights ธุรกิจกับสิทธิมนุษยชน. สืบค้น 8 พฤศจิกายน 2565, จาก https://www.setsustainability.com/page/business-and-human-rights?fbclid=IwAR3ExJ3pKTKvvhQeY-opoNbCCPwnCNuaeEeNY9d-G465cB4Pu3QyTZYwjSc.

[58] Here's Why Regulatory Compliance is Important. Accessed 8 November, 2022, Available from: https://reciprocity.com/blog/heres-why-regulatory-compliance-is-important/?fbclid=IwAR2uFCmIGa3TXqaTKiqwNKxF5dKC7bRS8a3_xWgSFWrDtawWOV2eUi3Ce2s.

[59] GDPR Article 42

ดั่งเวลาที่ผู้บริโภคไว้วางใจเมื่อเห็นสัญลักษณ์ประหยัดไฟเบอร์ 5 หรือเครื่องหมาย อย. บนผลิตภัณฑ์นั่นเอง

สำหรับ PDPA ในประเทศไทยนั้นมิได้นำบทบัญญัติว่าด้วยการรับรองมาจาก GDPR ด้วย แต่ในทางปฏิบัติ องค์กรธุรกิจต่างต้องการสร้างความเชื่อมั่นแก่สาธารณชนเพื่อเพิ่มความสามารถในการแข่งขันของบริษัท บางบริษัทจึงได้ให้บริษัทอื่นซึ่งเป็นบุคคลภายนอก และมีความชำนาญด้านการตรวจประเมินคุณสมบัติขององค์กรให้เข้ารับรองว่าบริษัทของตนมีระบบการจัดการต่าง ๆ ที่สอดคล้องกับ PDPA รวมถึงมีการให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) เข้ารับหลักสูตรอบรมและมีการออกใบรับรองคุณวุฒิ ทั้งที่ตามกฎหมายแล้วมิได้มีข้อบังคับเรื่องการรับรองเหล่านั้น[60] ทั้งหมดเพื่อสร้างฐานความเชื่อมั่นให้กับองค์กรของตน อันเป็นสิ่งสำคัญในการดำเนินกิจการทางธุรกิจ

(2) ปัญหาในทางปฏิบัติที่ภาคธุรกิจต้องปรับตัวตามมาตรฐานใหม่ที่ไม่เคยทำมาก่อน

กฎหมายคุ้มครองข้อมูลส่วนบุคคล เป็นการมอบหมายหน้าที่ให้องค์กรธุรกิจปฏิบัติตาม ซึ่งเนื่องจากที่เป็นกฎหมายบังคับใช้ใหม่ ภาคธุรกิจจึงยังไม่คุ้นชินและต้องใช้เวลาปรับตัวเพื่อให้สอดคล้องกับกฎหมายนี้ โดยเฉพาะธุรกิจขนาดกลางหรือขนาดเล็กที่จำเป็นต้องใช้ทุนทรัพย์ในการยกระดับมาตรฐานความปลอดภัยของบริษัท

ในการบังคับใช้กฎหมาย ต้องบังคับใช้อย่างเป็นธรรม เท่าเทียม และทั่วถึง แต่ในความเป็นจริงนั้น ถึงการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลจะมีความ ‘เท่าเทียม’ อันเป็นการใช้อย่างทั่วถึง แต่ยังไม่สามารถทำให้เกิดความ ‘เป็นธรรม’ อย่างแท้จริงได้ เนื่องจากบริษัทบางบริษัท ได้รับผลกระทบจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลน้อยกว่าบริษัทอื่น นั่นคือบริษัทเกี่ยวกับเทคโนโลยีแพลตฟอร์มดิจิทัล (Digital Platform)

แพลตฟอร์มดิจิทัล (Digital Platform) คือ แหล่งในการเชื่อมโยง เพื่อให้เกิดการแลกเปลี่ยนข้อมูล สินค้า และบริการระหว่างผู้ผลิต ผู้บริโภค หรือในชุมชนหนึ่ง ๆ [61] ตัวอย่างเช่น Google, Facebook, Twitter, Amazon, Microsoft จะเห็นได้ว่าองค์กรเหล่านี้มีมูลค่าที่สูงมาก

---

[60] EasyPDPA. DPO คือใคร? ทำไมองค์กรยุคใหม่ถึงขาดตำแหน่งนี้ไปไม่ได้. Accessed 8 November, 2022, Available from: https://easypdpa.com/article/easypdpa-dpo-document.

[61] Stephen Watts. Digital Platforms: A Brief Introduction. Accessed 8 November, 2022, Available from: https://www.bmc.com/blogs/digital-platforms/.

เมื่อเทียบกับแวดวงธุรกิจอื่น โดยสิ่งที่ทำให้บริษัทเหล่านี้แตกต่าง คือความสามารถในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน

หัวใจหลักของ Digital Platform คือการให้บริการแอปพลิเคชันโดยไม่เสียค่าใช้จ่าย แลกเปลี่ยนกับการเก็บข้อมูลการใช้บริการของเจ้าของข้อมูล เพื่อนำไปประมวลผล และใช้งานหรือเสนอขายให้แก่บริษัทอื่นๆ นำไปใช้ประโยชน์ ลักษณะเช่นนี้ทำให้ Digital Platform ซึ่งเป็นตัวกลางในการแลกเปลี่ยนข้อมูล เป็นผู้มีอำนาจโดยสมบูรณ์ในการควบคุมการไหลของข้อมูลระหว่างผู้ใช้งานแพลตฟอร์ม, ผู้จัดหาคอนเทนต์ (Content provider) และผู้โฆษณา[62] อันเป็นการผูกขาดข้อมูลในการกำหนดว่าผู้ใดมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่บริษัทได้รวบรวมมาและเข้าถึงได้มากน้อยเพียงใด ซึ่ง Digital Platform เหล่านี้ เป็นแรงบันดาลใจหลักเบื้องหลังการออกกฎหมาย GDPR เพื่อเข้าควบคุม และกำกับดูแลการประมวลผลข้อมูล[63] โดยหลังจาก GDPR ถูกบังคับใช้ ปัญหาที่บริษัทเหล่านี้ประสบคือ การระบุวัตถุประสงค์ในการเก็บข้อมูล เนื่องจากการดำเนินการของบริษัทเหล่านี้เป็นการรวบรวมข้อมูลส่วนบุคคล และประมวลผลเพื่อให้ได้มาซึ่งข้อมูลพฤติกรรมการใช้งาน หรือการบริโภคซึ่งมีความละเอียดและแม่นยำสูง นับเป็นข้อมูลที่บริษัทอื่นต้องการเป็นอย่างมากเพื่อใช้ในการออกแบบสินค้าและบริการที่ตอบโจทย์ผู้บริโภคมากที่สุด โดยในการเก็บรวบรวมข้อมูลนั้นมีลักษณะเป็นการหว่านแห หรือเก็บข้อมูลทุกอย่างโดยกว้าง และนำไปคัดกรอง รวมถึงประมวลผลเป็นข้อมูลที่มีประโยชน์ในภายหลัง จึงเป็นไปได้ยากที่บริษัทเหล่านี้จะชี้แจงต่อเจ้าของข้อมูลส่วนบุคคลว่า จะเก็บข้อมูลส่วนนี้ไปทำไม เนื่องจากในขณะที่เก็บข้อมูล แพลตฟอร์มเหล่านั้นก็ยังไม่มีวัตถุประสงค์ที่แน่ชัดว่าข้อมูลส่วนนี้จะนำไปใช้ทำอะไรกันแน่ แต่จะทราบวัตถุประสงค์เมื่อผ่านการคัดกรองข้อมูลแล้วเท่านั้น[64]

ในด้านสิทธิของปัจเจกชนต่อ Digital Platform นั้น กฎหมาย GDPR รวมถึง PDPA มีแก่นสำคัญในการคุ้มครองสิทธิส่วนบุคคลโดยการให้อำนาจเจ้าของข้อมูลในการตัดสินใจให้ความ

---

[62] Tuulia Karjalainen. (2022). The battle of power: Enforcing data protection law against companies holding data power. ScienceDirect. Available from: https://www.sciencedirect.com/science/article/pii/S0267364922000851?fbclid=IwAR2U3Bfk6qTqTe35c0_8_tc3s9qee_koWda-3xWvsarzgZjeTy194MT7Rlk.

[63] European Commission. Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into application of the General Data Protection Regulation. Accessed 8 November, 2022, Available from: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3889.

[64] Bart van der Sloot, Sascha van Schendel. Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study. Accessed 8 November, 2022, Available from: https://www.jipitec.eu/issues/jipitec-7-2-2016/4438.

ยินยอมให้เก็บข้อมูล ขอแก้ไขเปลี่ยนแปลงข้อมูล รวมถึงขอให้ลบหรือทำลายข้อมูลที่ตนเคยให้ความยินยอมไว้ได้ อย่างไรก็ดี มาตรการนี้ก็ยังไม่ตอบโจทย์ในการใช้งานจริง เนื่องจากในชีวิตประจำวัน การเก็บรวบรวมข้อมูลในโลกออนไลน์นั้นมีเยอะมาก และยากต่อการเข้าใจ กล่าวได้ว่าเกือบทุกเว็บไซต์นั้นมีการขอความยินยอมคุกกี (Cookie Consent) เพื่อเก็บข้อมูลการใช้งานของเจ้าของข้อมูล รวมถึงข้อกำหนดหรือกฎเกณฑ์การใช้งานข้อมูลส่วนบุคคลที่เว็บไซต์นำเสนอก็ทำความเข้าใจได้ยาก ทำให้เจ้าของข้อมูลไม่สามารถตัดสินใจได้อย่างถูกต้อง นอกจากนี้เว็บไซต์หรือแพลตฟอร์มส่วนใหญ่มิได้กำหนดให้ความยินยอมเป็น ‘ตัวเลือก’ แต่เป็น ‘เงื่อนไข’ ในการเข้าใช้เว็บไซต์หรือแพลตฟอร์ม กล่าวคือ ถ้าเจ้าของข้อมูลไม่ยินยอม และสงวนสิทธิในข้อมูลส่วนบุคคลของตนไว้ ก็จะไม่สามารถเข้าใช้บริการในส่วนนั้นได้ ซึ่งสามารถทำได้ยากในสังคมปัจจุบันที่ชีวิตประจำวันของเราล้วนต้องพึ่งพาเว็บไซต์หรือแพลตฟอร์มเหล่านั้นไม่ทางใดก็ทางหนึ่ง ไม่ว่าด้านการทำงาน การหาข้อมูล การติดต่อสื่อสาร หรือเพื่อความบันเทิง ตัวอย่างเช่น หากเราไม่ยินยอมเงื่อนไขการให้บริการของ Facebook หรือ Messenger อันทำให้เราไม่ได้รับบริการเหล่านี้ ย่อมมีผลเสียในหลาย ๆ ด้าน ปัจเจกชนส่วนใหญ่จึงยอมรับเงื่อนไขเหล่านั้น และยินยอมให้แพลตฟอร์มประมวลผลข้อมูลส่วนบุคคลของตนโดยไม่รู้แม้แต่วิธีการหรือวัตถุประสงค์ในการเก็บข้อมูลหรือประมวลผล อันเป็นการตัดสินใจโดยขาดข้อมูล และไม่ได้ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้น

สำหรับบทลงโทษในการไม่ปฏิบัติตามกฎหมาย การลงโทษโดยการปรับอาจเป็นการไม่เพียงพอในการทำให้บริษัทเหล่านี้ปฏิบัติตามได้ หากค่าปรับไม่ได้สัดส่วนกับรายได้ที่บริษัทได้รับในการไม่ปฏิบัติตามกฎหมาย จึงเป็นความท้าทายของผู้ร่างกฎหมายในการกำหนดสัดส่วน หรือเพิ่มโทษให้สามารถโน้มน้าวให้บริษัทปฏิบัติตามได้ รวมถึงผู้บังคับใช้กฎหมายต้องบังคับใช้อย่างเคร่งครัด เพื่อให้การคุ้มครองข้อมูลมีประสิทธิภาพและใช้ได้จริง

โดยสรุป ถึงแม้ PDPA จะเป็นกฎหมายที่บังคับใช้อย่างเท่าเทียม แต่ผู้ที่ได้รับผลกระทบมากที่สุดกลับเป็นบริษัทเล็ก ๆ ที่จำต้องใช้ทรัพยากรเพื่อออกแบบการดำเนินการให้สอดคล้องกับหน้าที่ที่เพิ่มเข้ามาจากการบังคับใช้ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล ในทางกลับกัน บริษัทขนาดใหญ่นั้นไม่มีปัญหากับการจัดการตามข้อบังคับนี้ เนื่องจากมีความพร้อมด้านทรัพยากร เหตุเพราะ PDPA กำหนดกฎเกณฑ์ของบริษัทขนาดเล็กและใหญ่ไม่ต่างกันมาก ยิ่งกว่านั้น บริษัท Digital Platform ยังขาดแรงจูงใจในการปฏิบัติตามกฎหมายนี้ เนื่องจากการเพิ่มข้อจำกัดในการรวบรวม ประมวลผล และเปิดเผยข้อมูลส่วนบุคคลนั้นส่งผลโดยตรงต่อรายได้ของบริษัท นอกจากนี้ บทลงโทษโดยการปรับก็ยังไม่ตอบโจทย์ในการโน้มน้าวให้บริษัทเหล่านี้ปฏิบัติตาม

เนื่องจากการผูกขาดข้อมูลสามารถสร้างรายได้มหาศาล ค่าปรับจากการลงโทษนี้จึงถือว่าเล็กน้อยและไม่ได้สัดส่วน สำหรับแนวทางการแก้ไขในการบังคับใช้ให้เกิดความทั่วถึง ข้าพเจ้าเห็นว่า ควรมีการออกกฎหมายเฉพาะขึ้นเพื่อกำกับดูแล Digital Platform เหล่านั้นโดยเฉพาะ โดยแยกส่วนกับ PDPA ในปัจจุบัน เหตุเพราะการนำมาตรฐานหนึ่งมาบังคับใช้ร่วมกับทั้งบริษัทที่ทำธุรกิจด้านการรวบรวมและประมวลผลข้อมูลส่วนบุคคลโดยเฉพาะ และธุรกิจอื่น ค่อนข้างไม่เพียงพอ ควรออกกฎหมายพิเศษขึ้นโดยยกระดับการกำกับดูแล เพื่อคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลให้ได้ประสิทธิภาพอย่างแท้จริง ซึ่งในปัจจุบันสหภาพยุโรป (European Union) ได้มีการตระหนัก และอยู่ระหว่างหาทางแก้ไขปัญหานี้เช่นกัน