

บทที่ 3

มาตรการการคุ้มครองข้อมูลส่วนบุคคลของเด็กตามกฎหมายไทย และกฎหมายต่างประเทศ

สำหรับประเทศไทยมีกฎหมายหลากหลายฉบับที่มีความเกี่ยวข้องกับเด็กแต่เมื่อได้ทำการศึกษาเป็นการเฉพาะแล้วกลับพบว่าในเรื่องของการคุ้มครองสิทธิเด็กทั้งกฎหมายของประเทศไทยและกฎหมายต่างประเทศก็มีแนวทางในการคุ้มครองสิทธิเด็กยึดตามหลักสากลที่ได้มีการกำหนดไว้ในอนุสัญญาว่าด้วยสิทธิเด็กแห่งสหประชาชาติ สำหรับประเทศไทยในปัจจุบันนี้ก็ถือได้ว่ามีกฎหมายหลากหลายฉบับที่มีความเกี่ยวข้องกับเด็ก ผู้เขียนจึงได้ทำการศึกษากฎหมายของประเทศไทยและกฎหมายของต่างประเทศในเฉพาะเรื่องกรณีของการคุ้มครองสิทธิเด็กในข้อมูลส่วนบุคคลของเด็กบนเครือข่ายอินเทอร์เน็ตเพื่อเป็นแนวทางในการเปรียบเทียบเพื่อหาแนวทางแก้ไขปัญหาของการละเมิดสิทธิในข้อมูลส่วนบุคคลของเด็กบนอินเทอร์เน็ต และในส่วนนี้ผู้เขียนจะทำการศึกษาจากกฎหมายของประเทศไทยทั้งหมด 4 ฉบับ ได้แก่ รัฐธรรมนูญแห่งราชอาณาจักรไทย, พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรการต่าง ๆ ของกฎหมายต่างประเทศ ซึ่งมีรายละเอียด ดังนี้

3.1 มาตรการการคุ้มครองข้อมูลส่วนบุคคลของเด็กในประเทศไทย

3.1.1 การคุ้มครองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย

ในการให้ความคุ้มครองข้อมูลส่วนบุคคลตามรัฐธรรมนูญแห่งราชอาณาจักรไทยนั้นเริ่มมีมาตั้งแต่รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2534 แก้ไขเพิ่มเติม (ฉบับที่ 5) พ.ศ. 2538 ซึ่งในรัฐธรรมนูญฉบับนี้อาจจะไม่ได้ทำการกล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นการเฉพาะเจาะจงแต่ก็เป็นการบัญญัติเกี่ยวกับการคุ้มครองสิทธิซึ่งการคุ้มครองสิทธินี้ก็จะนำไปสู่การคุ้มครองข้อมูลส่วนบุคคล เช่น

1) การให้ความคุ้มครองสิทธิของบุคคลในด้านต่าง ๆ ไม่ว่าจะเป็น ครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวของบุคคล

2) การให้ความคุ้มครองสิทธิของการได้รู้หรือทราบข้อมูลข่าวสารแต่เป็นเฉพาะการได้รู้ข้อมูลที่อยู่ในความครอบครองของหน่วยงานของรัฐเท่านั้น

นอกจากนี้ ในมาตรา 3 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยก็ได้มีการวางหลักเกี่ยวกับการคุ้มครองในเรื่องของเสรีภาพที่เกี่ยวข้องกับข้อมูลส่วนบุคคล อันได้แก่ การคุ้มครองเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์และการโฆษณาและโดยวิธีการอื่นโดยเสรีภาพเช่นว่านี้จะไม่สามารถถูกจำกัดไว้ได้ เว้นแต่อาศัยอำนาจทางกฎหมายเพื่อจะรักษาความมั่นคงของรัฐ หรือเพื่อรักษาสิทธิเสรีภาพของครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวของบุคคลอื่น หรือเพื่อรักษาความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน เช่นนี้ จะเห็นได้ว่า ในกรณีที่จะต้องคุ้มครองเสรีภาพในความเป็นอยู่ส่วนตัวของบุคคลหนึ่งก็สามารถที่จะจำกัดเสรีภาพของบุคคลหนึ่งได้ ทั้งนี้ โดยอาศัยอำนาจของกฎหมาย¹

ต่อมาในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 ในมาตรา 30

บัญญัติว่า “บุคคลย่อมเสมอกันในกฎหมายและได้รับความคุ้มครองตามกฎหมายเท่าเทียมกันชายและหญิงมีสิทธิเท่าเทียมกัน

การเลือกปฏิบัติโดยไม่เป็นธรรมต่อบุคคลเพราะเหตุแห่งความแตกต่างในเรื่องถิ่นกำเนิด เชื้อชาติ ภาษา เพศ อายุ สภาพทางกายภาพหรือสุขภาพ สถานะของบุคคล ฐานะทางเศรษฐกิจหรือสังคม ความเชื่อทางศาสนา การศึกษาอบรม หรือความคิดเห็นทางการเมืองอันไม่ขัดต่อบัญญัติแห่งรัฐธรรมนูญจะกระทำมิได้

มาตรการที่รัฐกำหนดขึ้นเพื่อขจัดอุปสรรคหรือส่งเสริมให้บุคคลสามารถใช้สิทธิและเสรีภาพได้เช่นเดียวกับบุคคลอื่น ย่อมไม่ถือเป็นการเลือกปฏิบัติโดยไม่เป็นธรรมตามวรรคสาม”² จะเห็นได้ว่า ได้มีการกล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลไว้ในการให้ความคุ้มครองสิทธิความเป็นอยู่ส่วนตัว เกี่ยวกับ สิทธิในครอบครัว เกียรติยศ ชื่อเสียงหรือความเป็นอยู่ส่วนตัวของบุคคลอันเป็นสิทธิที่ใหญ่กว่า ดังนั้นก็ย่อมครอบคลุมถึงการให้ความคุ้มครองถึงสิทธิของบุคคลในด้านข้อมูลส่วนบุคคลด้วยเช่นกัน

ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 ได้มีการกล่าวถึงสิทธิเสรีภาพส่วนบุคคลไว้ในมาตรา 35 มีการบัญญัติไว้ว่า “สิทธิความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครองสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง

¹ รัฐธรรมนูญแห่งราชอาณาจักรไทย (พ.ศ. 2534 แก้ไขเพิ่มเติม (ฉบับที่ 5) พ.ศ. 2538). มาตรา 3.

² รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540. มาตรา 30.

การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูล ส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ³

เป็นการกล่าวถึงการให้ความคุ้มครองในเรื่องของสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว ซึ่งสิทธิดังกล่าวย่อมได้รับความคุ้มครองตามกฎหมาย บุคคลใด จะกระทำการละเมิดหรือกระทบใดอันเป็นการกระทบสิทธิดังกล่าวนี้มิได้ จะเห็นได้ว่า ในมาตรานี้มิได้มีกล่าวถึงการให้ความคุ้มครอง “สิทธิในข้อมูลส่วนบุคคล” โดยตรง แต่ก็มี การให้ความคุ้มครองสิทธิของบุคคลในความเป็นอยู่ส่วนตัวหรือ “สิทธิส่วนบุคคล” ซึ่งครอบคลุมถึง สิทธิส่วนบุคคลในข้อมูลข่าวสารส่วนบุคคลนั้นก็ย่อมแสดงให้เห็นว่าเป็นการให้ความคุ้มครองสิทธิ ส่วนบุคคลไปด้วยโดยปริยาย

และในปัจจุบันรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้มีการกล่าวถึง สิทธิเสรีภาพส่วนบุคคลไว้ในมาตรา 32 ซึ่งบัญญัติไว้ว่า

“บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำ ข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตาม บทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ⁴

จะเห็นได้ว่าในรัฐธรรมนูญ ฉบับปี พ.ศ. 2560 ก็ยังมีได้มีการกล่าวถึง “สิทธิในข้อมูล ส่วนบุคคล” เป็นการเฉพาะ ซึ่งก็ให้ความหมายครอบคลุมถึงสิทธิส่วนบุคคลในข้อมูลข่าวสาร ส่วนบุคคลด้วย ก็ย่อมแสดงให้เห็นว่าเป็นการให้ความคุ้มครองสิทธิส่วนบุคคลไปด้วยโดยปริยาย แต่อย่างไรก็ตาม แต่ก็มีกำหนดรายละเอียดเพิ่มเติมคือหากมีการละเมิด สิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัวนำไปใช้ประโยชน์ไม่ว่าทางใดก็ตาม แต่ก็มี การให้ช้อยกเว้นเอาไว้ ในกรณีที่กฎหมายตราขึ้นว่าเพื่อประโยชน์สาธารณะก็จะสามารถนำออกมาเผยแพร่ได้

3.1.2 การคุ้มครองตามพระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546

พระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 เริ่มมีการประกาศใช้เมื่อวันที่ 29 มีนาคม พ.ศ. 2547 โดยมี การประกาศยกเลิกประกาศของคณะปฏิวัติ ฉบับที่ 132 ลงวันที่ 22 เมษายน พ.ศ. 2515 และ ประกาศของคณะปฏิวัติ ฉบับที่ 294 ลงวันที่ 27 พฤศจิกายน พ.ศ. 2515 ที่ใช้บังคับเกี่ยวกับวิธีการ

³ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550. มาตรา 35.

⁴ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560. มาตรา 32.

สงเคราะห์ ค้ำครองสวัสดิภาพและส่งเสริมความประพฤติมานานแล้ว ซึ่งไม่เหมาะสมกับสภาพสังคมปัจจุบันที่เปลี่ยนแปลงไปจึงได้มีการปรับปรุงขั้นตอนและวิธีการที่ใช้ปฏิบัติต่อเด็กให้มีความเหมาะสมยิ่งขึ้นเพื่อให้เด็กได้รับการอุปการะเลี้ยงดู การอบรมสั่งสอน และมีพัฒนาการที่เหมาะสมอันเป็นการส่งเสริมความมั่นคงของสถาบันครอบครัว รวมทั้งป้องกันมิให้เด็กถูกทารุณกรรมตกเป็นเครื่องมือในการแสวงหาผลประโยชน์โดยมิชอบหรือถูกเลือกปฏิบัติอย่างไม่เป็นธรรมและยังส่งเสริมความร่วมมือในการคุ้มครองเด็กระหว่างหน่วยงานของรัฐและเอกชนให้เหมาะสมยิ่งขึ้นเพื่อให้สอดคล้องกับรัฐธรรมนูญแห่งราชอาณาจักรไทย แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ และอนุสัญญาว่าด้วยสิทธิเด็ก ค.ศ. 1990 จึงจำเป็นต้องตราพระราชบัญญัตินี้ขึ้นมา⁵

สาระสำคัญของพระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 คือ พระราชบัญญัติฉบับนี้ตั้งอยู่บนหลักการที่กำหนดไว้ในอนุสัญญาสหประชาชาติว่าด้วยสิทธิเด็ก ระบุถึงวิธีอันหลากหลายซึ่งความรุนแรง และการแสวงหาผลประโยชน์โดยมิชอบ ที่สามารถทำร้ายเด็ก พระราชบัญญัตินี้ให้การปกป้องคุ้มครองเด็กไทยทั้งหมดไม่ว่าพวกเขาจะมีสถานะทางเศรษฐกิจ สังคม กฎหมาย ชาติพันธุ์ หรือนับถือศาสนาใด เนื้อหาจะประกาศอย่างแจ่มชัดว่า การดูแลให้เด็กมีความเป็นอยู่ที่ดีคือหน้าที่รับผิดชอบของทุกคน และจะไม่ยอมให้มีการทารุณกรรมเด็ก พร้อมทั้งระบุถึงความมุ่งมั่นของประเทศไทยที่จะให้การช่วยเหลือเด็กโดยผ่านทาง การเสริมสร้างความเข้มแข็งของครอบครัว⁶

นอกจากนี้มีบทบัญญัติทั้งสิ้น 88 มาตราซึ่งเป็นหลักเกณฑ์ให้ความคุ้มครองสิทธิเด็กในด้านต่าง ๆ แต่ในส่วนที่กล่าวถึงในที่นี้ได้แก่ส่วนที่สอดคล้องและเกี่ยวกับการคุ้มครองเด็กเกี่ยวกับการเผยแพร่ข้อมูลเกี่ยวกับตัวเด็ก อันได้แก่ มาตรา 27 แห่งพระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 ได้มีการวางหลักเกี่ยวกับการให้ความคุ้มครองเด็กเกี่ยวกับเรื่องของข้อมูลส่วนตัวของเด็กเอาไว้ว่า คือ ห้ามมิให้ผู้ใดโฆษณาหรือเผยแพร่ข้อมูลส่วนตัวของเด็ก อันมีเจตนาทำให้เด็กเสียหายแก่จิตใจ ชื่อเสียง เกียรติคุณหรือสิทธิประโยชน์อื่น ๆ ของเด็กหรือเพื่อแสวงหาประโยชน์ของตัวเองหรือผู้อื่น โดยมิชอบ

และในมาตรา 50 ก็มีการกำหนดห้ามมิให้ผู้ปกครองสวัสดิภาพหรือผู้คุ้มครองสวัสดิภาพของเด็ก เปิดเผย ชื่อตัว ชื่อสกุล ภาพ หรือข้อมูลใด ๆ เกี่ยวกับตัวเด็ก ผู้ปกครองในลักษณะที่น่าจะเกิดความเสียหายแก่ชื่อเสียงเกียรติคุณ หรือสิทธิประโยชน์อย่างใดอย่างหนึ่งของเด็กหรือผู้ปกครอง

⁵ เหตุผลท้ายพระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546.

⁶ Aneesahkimeahblog. (2560). *กฎหมายและการประกันคุณภาพการศึกษา: พระราชบัญญัติคุ้มครองเด็ก พ.ศ.2546*. (ออนไลน์). เข้าถึงได้จาก : <https://aneesahkimeahblog.wordpress.com/2017/02/02/%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%A7%E0%B8%B1%E0%B8%95%E0%B8%B4%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%95%E0%B8%B1%E0%B8%A7/>. [2564, 18 เมษายน].

มีวางหลักเกณฑ์ในเรื่องเกี่ยวกับการบังคับแก่พนักงานเจ้าหน้าที่นักสังคมสงเคราะห์ นักจิตวิทยา และผู้มีหน้าที่คุ้มครองสวัสดิภาพเด็กสอดคล้องตามมาตรา 24 ซึ่งได้ล่วงรู้ข้อมูลดังกล่าว เนื่องในการปฏิบัติหน้าที่ของตนด้วยไว้ในวรรคที่สองของมาตรา 50 และส่วนในวรรคที่สามก็ทำการ กำหนดห้ามมิให้ผู้ใดโฆษณาหรือเผยแพร่ทางสื่อมวลชนหรือสื่อสารสนเทศประเภทใดซึ่งข้อมูล ที่เปิดเผยโดยฝ่าฝืนในวรรคหนึ่งหรือวรรคสอง

จะเห็นได้ว่า ในเรื่องที่เกี่ยวข้องกับการให้ความคุ้มครองในข้อมูลส่วนบุคคลของเด็ก ในพระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 นั้นได้มีการกำหนดประเด็นสาระสำคัญไว้ในมาตรา 27 และมาตรา 50 และมีการวางหลักการให้ความคุ้มครองเด็กเกี่ยวกับข้อมูลส่วนบุคคลของเด็กโดยการ กำหนดห้ามมิให้มีการเผยแพร่ โฆษณา เกี่ยวกับข้อมูลส่วนบุคคลของเด็ก ซึ่งเจตนาจะทำให้เด็กเสียหาย แก่จิตใจ ชื่อเสียง เกียรติคุณ หรือสิทธิประโยชน์อื่นใดของเด็ก หรือเพื่อที่จะแสวงหาประโยชน์ ต่อตนเอง หรือต่อผู้อื่นโดยไม่ชอบด้วยกฎหมายซึ่งเป็นการกำหนดห้ามการ โฆษณา เผยแพร่ของสื่อ เป็นหลักการห้ามเผยแพร่ของผู้ที่ได้ล่วงรู้ข้อมูลส่วนบุคคลเด็กในการปฏิบัติหน้าที่ หรือผู้ที่ เป็น ผู้ปกครองของเด็กซึ่งล่วงรู้ข้อมูลส่วนบุคคลของเด็ก⁷

ทำให้ทราบว่าในหลักการดังกล่าวไม่ได้มีการกล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลของเด็ก บนสื่อออนไลน์หรืออินเทอร์เน็ตแต่อย่างใด ไม่มีข้อกำหนดหรือหลักการปฏิบัติของผู้ประกอบการ เว็บไซต์หรือผู้ให้บริการอินเทอร์เน็ตในการควบคุมดูแลข้อมูลส่วนบุคคลของเด็กแม้แต่น้อย ไม่ว่าจะเป็นข้อกำหนดเกี่ยวกับการจัดเก็บ การประมวลผล หรือการเผยแพร่ข้อมูลส่วนบุคคลของเด็ก บนอินเทอร์เน็ต ดังนั้นในการให้การคุ้มครองสิทธิเด็กตามพระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 ยังไม่ครอบคลุมถึงการคุ้มครองข้อมูลส่วนบุคคลของเด็กบนอินเทอร์เน็ตปัญหาเกี่ยวกับการละเมิด ข้อมูลส่วนบุคคลของเด็กอันเป็นสาเหตุที่นำไปสู่ปัญหาการละเมิดสิทธิเด็กจึงมีให้เห็นอยู่ทั่วไป ในยุคปัจจุบันนี้

แต่ในการประชุมของคณะกรรมการเด็กครั้งที่ 5/2550 ก็ได้มีการแต่งตั้งคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคลของเด็กบนระบบเทคโนโลยีสารสนเทศ โดยมีหน้าที่ออกมาตรการ ให้ความคุ้มครองเด็ก เพื่อป้องกันไม่ให้ผู้ให้บริการเว็บไซต์และอินเทอร์เน็ตกระทำการละเมิดสิทธิ เด็กโดยการเปิดเผยข้อมูลส่วนตัวของเด็กที่มีอายุต่ำกว่า 18 ปี และขอความร่วมมือจากผู้ประกอบการ ให้ปฏิบัติตามในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลของเด็ก ซึ่งมีรายละเอียด ดังนี้

1) ผู้ให้บริการเว็บไซต์ จะต้องไม่เปิดเผยข้อมูลส่วนตัวของเด็กที่ใช้บริการที่เป็นเด็ก อายุไม่เกิน 18 ปี ซึ่งข้อมูลที่เปิดเผยแล้วนั้นจะทำให้ผู้อื่นเข้าถึงตัวเด็กได้ อันได้แก่

⁷ พนิดา พูลสวัสดิ์. (2556). *มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของเด็กบนเครือข่ายอินเทอร์เน็ต*. วิทยานิพนธ์หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์. หน้า 38-39.

(1) ภาพถ่ายของเด็ก ที่แสดงร่วมกับเบอร์โทรศัพท์ อีเมล ที่อยู่ หรือชื่อผู้ใช้ระบบสนทนาออนไลน์ เช่น msn หรือ ชื่อ โรงเรียน

(2) อายุของเด็ก ที่แสดงร่วมกับเบอร์โทรศัพท์ อีเมล ที่อยู่ หรือชื่อผู้ใช้ระบบสนทนาออนไลน์

(3) เพศของเด็ก ที่แสดงร่วมกับเบอร์โทรศัพท์ อีเมล ที่อยู่ หรือชื่อผู้ใช้ระบบสนทนาออนไลน์

2) ลักษณะการเปิดเผยข้อมูลส่วนตัวของเด็กอายุต่ำกว่า 18 ปีที่ไม่อนุญาต ได้แก่

(1) การแสดงข้อมูลส่วนตัวของเด็กในหน้าประวัติผู้ใช้ (Profile)

(2) การอนุญาตให้ผู้ใช้ค้นหาข้อมูลส่วนตัวของเด็กผ่านระบบค้นหา (Search)

(3) การแสดงรายชื่อผู้ใช้ที่เป็นเด็กบนหน้าเว็บไซต์ที่ผู้ใช้ให้บริการสามารถควบคุมเนื้อหาได้ (สามารถกรองรายชื่อของผู้ใช้ที่เป็นเด็กอายุไม่เกิน 18 ปีออกได้) เช่น สารบัญผู้ใช้ในลักษณะที่สามารถเชื่อมโยงไปถึงข้อมูลส่วนตัวของเด็กได้ (Browse)

(4) การเปิดเผยข้อมูลลักษณะอื่น ๆ ที่อาจทำให้ผู้อื่นเข้าถึงข้อมูลส่วนตัวของเด็ก และอยู่ในวิสัยของผู้ประกอบการที่สามารถยกเลิก ป้องกัน หรือระงับการเปิดเผยข้อมูลดังกล่าวได้ เช่น การโพสต์ข้อมูลส่วนตัวลงกระดานสนทนา⁸

โดยสรุปแล้วในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลของเด็กบนอินเทอร์เน็ตนั้น หลักเกณฑ์ต่าง ๆ ในพระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 นั้น เป็นเพียงแค่มาตรการคุ้มครองเด็กในเรื่องของลักษณะเป็นการทั่วไป กล่าวคือ เป็นการคุ้มครองในเชิงกว้าง ในการเผยแพร่ โฆษณาผ่านสื่อหากข้อมูลเหล่านั้นทำให้เด็กได้รับความเสียหาย แม้กระทั่งการออกประกาศของคณะกรรมการที่ออกมาตรการขอความร่วมมือกับผู้ประกอบการเว็บไซต์แล้วก็ตาม แต่ยังไม่มีความคุ้มครองข้อมูลส่วนบุคคลของเด็กโดยตรงแต่อย่างใด อีกทั้งยังมีไม่บทบังคับหรือบทลงโทษที่ชัดเจนด้วย

3.1.3 การคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

พระราชบัญญัติฉบับนี้เป็นการเปิดโอกาสให้ประชาชนได้รับรู้ข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่าง ๆ ของรัฐ และยังคุ้มครองสิทธิส่วนบุคคลในส่วนที่เกี่ยวข้องกับข้อมูลข่าวสารของราชการไปพร้อมกัน โดยมีการกำหนดความหมาย “ข้อมูลข่าวสารส่วนบุคคล” ไว้ในมาตรา 4 ว่าหมายถึง “ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือ มีหมายเลข รหัส

⁸ มุลนิธิเด็ก. (2564). *ประชุมคณะกรรมการคุ้มครองเด็กแห่งชาติ ครั้งที่ 5/2550*. (ออนไลน์). เข้าถึงได้จาก: <http://www.ffc.or.th>. [2564, 19 กรกฎาคม].

สิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้อื่นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย”

นอกจากนี้ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้มีการวางหลักเกณฑ์ไว้โดยเฉพาะในข้อมูลข่าวสารส่วนบุคคลเพื่อทำการป้องกันมิให้เกิดการกระทบต่อสิทธิในเรื่องของความเป็นอยู่ส่วนตัวของบุคคล เพราะตามปกติของมนุษย์ทุกคนจะได้รับความเป็นส่วนตัวในการใช้ชีวิตระดับหนึ่งที่ไม่ต้องการให้ผู้อื่นนำไปทำการเปิดเผยต่อสาธารณะ เพราะนอกจากจะเป็นได้รับความส่วนตัวแล้วยังรวมไปถึงเรื่องศักดิ์ศรีความเป็นมนุษย์ที่พึงได้รับความคุ้มครองความเป็นส่วนตัว โดยรัฐจะนำข้อมูลเหล่านี้ไปเปิดเผยต่อสาธารณะโดยเจ้าของข้อมูลไม่ยินยอมไม่ได้

3.1.3.1 สาระสำคัญของการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้มี 3 ประการ ได้แก่

1) กำหนดหน้าที่ต่าง ๆ เกี่ยวกับการจัดระบบข้อมูลส่วนบุคคลของหน่วยงานของรัฐ เพื่อให้การคุ้มครองข้อมูลข่าวสารส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและปลอดภัย

2) กำหนดข้อห้ามในการเปิดเผยข้อมูลข่าวสารส่วนบุคคล โดยกำหนดให้ต้องได้รับความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลก่อนที่ทำการเปิดเผยข้อมูลนั้น เว้นแต่เป็นกรณีตามที่กฎหมายบัญญัติ

3) ให้สิทธิแก่เจ้าของข้อมูลในการตรวจสอบข้อมูลข่าวสารส่วนบุคคลของตนเองที่อยู่ในความครอบครองของหน่วยงานของรัฐ และให้สิทธิในการขอแก้ไขข้อมูลให้ถูกต้องตามความเป็นจริง อีกทั้งให้สิทธิในการอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร¹⁰

ในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีหลักสำคัญ 2 ประการ ดังนี้

- 1) “หลักที่ว่าบุคคลไม่จำเป็นต้องเป็นผู้มีส่วนได้เสียกับข้อมูลข่าวสารที่ขอ”
- 2) “เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น”

แต่หากเป็นการให้ความคุ้มครองข้อมูลข่าวสารส่วนบุคคลกฎหมายต้องการคุ้มครองความเป็นส่วนตัวของบุคคลจึงจำเป็นที่ต้องมีการกำหนดหลักเกณฑ์ที่แตกต่างจากข้อมูลข่าวสารของราชการ โดยกำหนดให้เจ้าของข้อมูลข่าวสารนั่นเองหรือบุคคลที่ผู้เป็นเจ้าของข้อมูลข่าวสารส่วนบุคคลและผู้มีสิทธิตามกฎหมายเท่านั้นที่จะเข้าถึงข้อมูลข่าวสารส่วนบุคคลได้ ทั้งนี้ตามหลัก

⁹ ธาริณี มณีรอด. (2559). *ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล*. วิทยานิพนธ์หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิต. หน้า 129.

¹⁰ ETDA. ICTLAW CENTER. (2564). *คุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540*. (ออนไลน์). เข้าถึงได้จาก: <https://ictlawcenter.etchda.or.th/laws/detail>. [2564, 19 กรกฎาคม].

ในพระราชบัญญัติข้อมูลข่าวสารของราชการ มาตรา 24 ที่มีหลักว่า ข้อมูลข่าวสารส่วนบุคคลจะเปิดเผยต่อบุคคลอื่นโดยปราศจากความยินยอมของเจ้าของข้อมูลส่วนบุคคลไม่ได้ เว้นแต่จะเข้าข้อยกเว้น¹¹ ซึ่งมีหลักเกณฑ์ ดังนี้

หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ทำให้ไว้ล่วงหน้าหรือ ในขณะที่นั้นมีได้ เว้นแต่เป็นการเปิดเผยได้ในกรณี ดังต่อไปนี้

(1) ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตนเพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

(2) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

(3) ต่อหน่วยงานของรัฐที่ทำงานด้านการวางแผนหรือการสถิติ หรือสำมะโนต่าง ๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูล ข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

(4) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อ หรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่ เกี่ยวกับบุคคลใด

(5) ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา 26 วรรคหนึ่ง เพื่อการตรวจดู คุณค่าในการเก็บรักษา

(6) ต่อเจ้าหน้าที่ของรัฐเพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการ ฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

(7) เป็นการให้ซึ่งจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(8) ต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริง ดังกล่าว

(9) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

การเปิดเผยข้อมูลข่าวสารส่วนบุคคลตามวรรคหนึ่ง (3) (4) (5) (6) (7) (8) และ (9) ให้มีการจัดทำบัญชีแสดง การเปิดเผยกำกับไว้กับข้อมูล ข่าวสารนั้น ตามหลักเกณฑ์และวิธีการที่กำหนดในกฎกระทรวง¹²

ในการเปิดเผยข้อมูลข่าวสารนั้น ไม่สามารถทำการเปิดเผยได้ยกเว้นกฎหมายได้ทำการบัญญัติเป็นข้อยกเว้นเอาไว้ในกรณีสำคัญ เช่น เพื่อเป็นการรักษาประโยชน์สาธารณะ หรือเป็นการ

¹¹ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540. มาตรา 24.

¹² พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540. มาตรา 24.

รักษาชีวิตของบุคคล รัฐก็จะสามารถทำการเปิดเผยข้อมูลข่าวสารส่วนบุคคลดังกล่าวได้ แม้บุคคลนั้นหรือเจ้าของข้อมูลไม่ได้ให้ความยินยอม แต่ในการจะเปิดเผยข้อมูลก็จะต้องคำนึงถึงการคุ้มครองประโยชน์ส่วนบุคคลประกอบไปด้วย

3.1.3.2 ประเภทของข้อมูลข่าวสารของราชการ

“ข้อมูลข่าวสาร” หมายความว่า สิ่งสื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูลหรือสิ่งใด ๆ ไม่ว่าจะสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผ่นพับ แผนที่ ภาพวาดภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียงการบันทึก โดยเครื่องคอมพิวเตอร์หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“ข้อมูลข่าวสารของราชการ” หมายความว่า ข้อมูลข่าวสารที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐไม่ว่าจะเป็นข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐหรือข้อมูลข่าวสารเกี่ยวกับเอกชน

1) ข้อมูลข่าวสารที่ต้องเปิดเผยเป็นการทั่วไป

(1) ข้อมูลข่าวสารที่ลงพิมพ์ในราชกิจจานุเบกษา

(1.1) โครงสร้างและการจัดองค์กรในการดำเนินงานของหน่วยงานของรัฐนั้น

(1.2) สรุปรายงานหน้าที่ที่สำคัญและวิธีการดำเนินงาน

(1.3) สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสาร หรือคำแนะนำในการติดต่อกับหน่วยงานของรัฐ

กับหน่วยงานของรัฐ

(1.4) กฎมติคณะรัฐมนตรี ข้อบังคับคำสั่งหนังสือเวียนระเบียบแบบแผนนโยบายหรือการตีความทั้งนี้เฉพาะที่จัดให้มีขึ้นโดยมีสภาพอย่างกฎเพื่อให้มีผลเป็นการทั่วไปต่อเอกชนที่เกี่ยวข้อง

(1.5) ข้อมูลข่าวสารอื่นตามที่คณะกรรมการกำหนดข้อมูลข่าวสารใดที่ได้มีการจัดพิมพ์เพื่อให้แพร่หลายตามจำนวนพอสมควรแล้วถ้ามีการลงพิมพ์ในราชกิจจานุเบกษา โดยอ้างอิงถึงสิ่งพิมพ์นั้นก็ให้ถือว่าเป็นการปฏิบัติตามบทบัญญัติดังกล่าวแล้ว (มาตรา 7)

(2) ข้อมูลข่าวสารที่ต้องลงพิมพ์ตามมาตรา 7 (4) ถ้ายังไม่ได้ลงพิมพ์ในราชกิจจานุเบกษา จะนำมาใช้บังคับในทางไม่เป็นคุณแก่ผู้ใดไม่ได้เว้นแต่ผู้นั้นจะรู้ถึงข้อมูลข่าวสารนั้นตามความเป็นจริงมาก่อนแล้วเป็นเวลาสมควร (มาตรา 8)

(3) ข้อมูลข่าวสารที่หน่วยงานของรัฐต้องจัดไว้ให้ประชาชนเข้าตรวจดู ตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนดได้แก่

(3.1) ผลการพิจารณาหรือคำวินิจฉัยที่มีผลโดยตรงต่อเอกชน รวมทั้งความเห็นแย้งและคำสั่งที่เกี่ยวข้องในการพิจารณาวินิจฉัยดังกล่าว

(3.2) นโยบายหรือการตีความที่ไม่เข้าข่ายต้องลงพิมพ์ในราชกิจจานุเบกษามาตรา 7 (4)

(3.3) แผนงาน โครงการ และงบประมาณรายจ่ายประจำปีที่กำลังดำเนินการ

(3.4) คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงานของเจ้าหน้าที่ของรัฐซึ่งมีผลกระทบต่อสิทธิหน้าที่ของเอกชน

(3.5) สิ่งพิมพ์ที่ได้มีการอ้างอิงถึงตามมาตรา 7 วรรคสอง

(3.6) สัญญาสัมปทานสัญญาที่มีลักษณะเป็นการผูกขาดตัดตอนหรือสัญญาร่วมทุนกับเอกชนในการจัดทำบริการสาธารณะ

(3.7) มติคณะรัฐมนตรี หรือมติคณะกรรมการที่แต่งตั้งโดยกฎหมายหรือโดยมติคณะรัฐมนตรีทั้งนี้ให้ระบุรายชื่อรายงานทางวิชาการรายงานข้อเท็จจริงหรือข้อมูลข่าวสารที่นำมาใช้ในการพิจารณาไว้ด้วย

(3.8) ข้อมูลข่าวสารอื่นตามที่คณะกรรมการกำหนด (มาตรา 9)

(4) ข้อมูลข่าวสารอื่นใดของราชการนอกเหนือจากข้อมูลข่าวสารตามมาตรา 7, มาตรา 8 และ มาตรา 9 (มาตรา 11)

(5) ข้อมูลข่าวสารที่คัดเลือกไว้ให้ประชาชนศึกษาค้นคว้า (เอกสารประวัติศาสตร์) ได้แก่ ข้อมูลข่าวสารของราชการที่หน่วยราชการของรัฐไม่ประสงค์จะเก็บรักษาไว้หรือข้อมูลข่าวสารของราชการ ตามมาตรา 14 เมื่อมีอายุครบ 75 ปีและข้อมูลข่าวสารตาม มาตรา 15 เมื่อมีอายุครบ 20 ปี นับแต่วันที่เสร็จสิ้นการจัดให้มีข้อมูลข่าวสารนั้นให้หน่วยงานของรัฐส่งมอบให้แก่หอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามที่กำหนดในพระราชกฤษฎีกา เพื่อให้ประชาชนศึกษาค้นคว้า (มาตรา 26)

2) ข้อมูลข่าวสารของราชการที่เปิดเผยเป็นการเฉพาะข้อมูลข่าวสารส่วนบุคคล หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมายรหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย (มาตรา 4) บุคคลหมายความว่าบุคคลธรรมดาที่มีสัญชาติไทยและบุคคลธรรมดาที่ไม่มีสัญชาติไทย แต่มีถิ่นที่อยู่ในประเทศไทย (มาตรา 21)

3) ข้อมูลข่าวสารที่ไม่ต้องเปิดเผย

(1) ข้อมูลข่าวสารของราชการที่เปิดเผยไม่ได้ ข้อมูลข่าวสารของราชการที่อาจก่อให้เกิดความเสียหายต่อสถาบันพระมหากษัตริย์จะเปิดเผยมิได้ (มาตรา 14)

(2) ข้อมูลข่าวสารของราชการที่เจ้าหน้าที่หรือหน่วยงานของรัฐอาจมีคำสั่งมิให้เปิดเผย โดยคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานของรัฐ ประโยชน์สาธารณะและประโยชน์ของประชาชนที่เกี่ยวข้องประกอบกัน

(2.1) การเปิดเผยจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศหรือความมั่นคงในทาง เศรษฐกิจหรือการคลังของประเทศ

(2.2) การเปิดเผยจะทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพหรือไม่อาจสำเร็จตามวัตถุประสงค์ได้ไม่ว่าจะเกี่ยวกับการฟ้องคดีการป้องกันการปราบปรามการทดสอบ การตรวจสอบหรือการรู้แหล่งที่มาของข้อมูลข่าวสารหรือไม่ก็ตาม

(2.3) ความเห็นหรือคำแนะนำภายในหน่วยงานของรัฐในการดำเนินการ เรื่องหนึ่งเรื่องใดแต่ทั้งนี้ไม่รวมถึงรายงานทางวิชาการรายงานข้อเท็จจริงหรือข้อมูลข่าวสารที่นำมาใช้ในการทำความเห็นหรือคำแนะนำภายในดังกล่าว

(2.4) การเปิดเผยจะก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยของบุคคลหนึ่งบุคคลใด

(2.5) รายงานการแพทย์หรือข้อมูลข่าวสารส่วนบุคคล ซึ่งการเปิดเผยจะเป็นการรุกรานสิทธิส่วนบุคคลโดยไม่สมควร

(2.6) ข้อมูลข่าวสารของราชการที่มีกฎหมายคุ้มครองมิให้เปิดเผยหรือข้อมูลข่าวสารที่มีผู้ให้มาโดยไม่ประสงค์ให้ทางราชการนำไปเปิดเผยต่อผู้อื่น

(2.7) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกาคำสั่งมิให้เปิดเผยข้อมูลข่าวสารของราชการจะกำหนดเงื่อนไขอย่างใดก็ได้แต่ต้องระบุไว้ด้วยว่าที่เปิดเผยไม่ได้เพราะเป็นข้อมูลข่าวสารประเภทใดและเพราะเหตุใดและให้ถือว่าการมีคำสั่งเปิดเผยข้อมูลข่าวสารของราชการเป็นดุลพินิจโดยเฉพาะของเจ้าหน้าที่ของรัฐตามลำดับสายการบังคับบัญชาแต่ผู้ขออาจอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารได้ตามที่กำหนดในพระราชบัญญัตินี้ (มาตรา 15)¹³

การคุ้มครองข้อมูลข่าวสารตามพระราชบัญญัติฉบับนี้จะเน้นในเรื่องของการคุ้มครองเกี่ยวกับข้อมูลข่าวสารที่อยู่ในอำนาจหน้าที่ของรัฐหรือทางราชการจะให้ความสำคัญสิทธิในการยึดถือข้อมูลข่าวสารที่อยู่ในขอบเขตหรืออำนาจของรัฐโดยไม่คำนึงถึงเนื้อหาสาระสำคัญของข่าวสารนั้นว่า

¹³ สำนักงานศิลปวัฒนธรรมร่วมสมัย. (2564). *สรุปสาระสำคัญของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540*. (ออนไลน์). เข้าถึงได้จาก: <http://ocac.go.th>. [2564, 17 กรกฎาคม].

จะเกี่ยวกับเรื่องใด โดยจะให้ความสำคัญในข้อมูลข่าวสารส่วนบุคคลของประชาชนทุกคนไม่รวมนิติบุคคล ซึ่งเป็นไปตามมาตรา 34 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยที่ทำการรับรองในเรื่องของสิทธิในความเป็นอยู่ส่วนตัว

ในการรับรองคุ้มครองข้อมูลข่าวสารตามพระราชบัญญัติฉบับนี้จะเน้นให้ความสำคัญคุ้มครองข้อมูลข่าวสารที่อยู่ในการครอบครองของรัฐ การที่จะเปิดเผย การรับแจ้งต่าง ๆ และรวมไปถึงการตรวจสอบข้อมูลข่าวสารส่วนบุคคลจะยึดหลักผู้มีอำนาจทำการแทนตามกฎหมาย เช่น กรณีของบิดามารดากระทำการแทนบุตรผู้เยาว์ เป็นต้น จากการศึกษาแล้วพบว่าในพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 ยังไม่มีการกำหนดหลักเกณฑ์หรือข้อกำหนดใด ๆ ที่เกี่ยวกับการรวบรวมข้อมูลส่วนบุคคลของเด็กบนอินเทอร์เน็ตไว้ ไม่ว่าจะในแง่ การนำไปใช้แล้วทำให้เด็กได้รับความเสียหาย หรือการนำข้อมูลส่วนบุคคลของเด็กนำไปเปิดเผย หรือเผยแพร่โดยไม่ได้รับความยินยอมแต่อย่างใด

3.1.4 การคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งได้ประกาศในราชกิจจานุเบกษาไปเมื่อ 27 พฤษภาคม พ.ศ. 2562 และมีผลบังคับใช้เมื่อ 28 พฤษภาคม พ.ศ. 2562 แล้วในบางส่วน โดยวันที่ 27 พฤษภาคม พ.ศ. 2563 เป็นวันที่พระราชบัญญัตินี้มีผลบังคับใช้ตามกฎหมายทั้งฉบับ

สาเหตุหลักที่ประเทศไทยต้องมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากสหภาพยุโรป (European Union: EU) ได้มีการออก GDPR (General Data Protection Regulation) ที่เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคล บังคับใช้เมื่อ 25 พฤษภาคม พ.ศ. 2561 ซึ่งนอกจากมีผลบังคับใช้แก่การส่งข้อมูลภายในประเทศสมาชิกสหภาพยุโรปแล้ว ผู้ประกอบการในไทยที่ต้องติดต่อรับส่งข้อมูลส่วนบุคคลของประชาชนในประเทศที่เป็นสมาชิกสหภาพยุโรป (Cross-Border Data Transfer Issues) ก็ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอด้วย

ที่สำคัญกว่านั้นคือ ความน่าเชื่อถือในมาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศ มีผลกระทบต่อการค้าระหว่างประเทศ และการทำธุรกิจระหว่างประเทศ หากประเทศไทยไม่มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ย่อมทำให้เสียโอกาสและความเชื่อมั่นจากกลุ่มประเทศในสหภาพยุโรป และอาจรวมไปถึงประชาคมโลกที่กำลังตื่นตัวเรื่อง Data Protection เพราะเหตุการณ์ใหญ่ ๆ ที่เกิดขึ้นแล้ว เช่น การรั่วไหลของข้อมูลส่วนบุคคลของผู้ใช้ Facebook หลายล้านบัญชี เป็นต้น¹⁴

¹⁴ ACinfotec Co., Ltd. (2564). *สรุปใจความสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ผู้ประกอบการควรรู้*. (ออนไลน์). เข้าถึงได้จาก: <https://www.acinfotec.com/2019/07/23/data-protection-law-2562/>. [2564, 22 กรกฎาคม].

นอกจากนี้ PDPA (Personal Data Protection Act, B.E. 2562 (2019)) เนื่องมาจากเทคโนโลยี มีความก้าวหน้าขึ้น ช่องทางสื่อสารต่าง ๆ ก็มีหลากหลายขึ้น ทำให้การละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลทำได้ง่ายขึ้นเช่นกัน และหลายครั้งก็นำมาซึ่งความเดือดร้อนรำคาญหรือสร้างความเสียหายให้แก่เจ้าของข้อมูล ตลอดจนสามารถส่งผลกระทบต่อเศรษฐกิจโดยรวมของประเทศได้ด้วย จึงต้องมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลขึ้นเพื่อกำหนดหลักเกณฑ์ กติกา หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่รวมถึงการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลขึ้น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีบทบัญญัติต่าง ๆ ไว้โดยมีการจำแนกได้ดังต่อไปนี้

3.1.4.1 บทบัญญัติทั่วไป (มาตรา 1 ถึงมาตรา 7)

บทบัญญัติกลุ่มนี้ จะเกี่ยวข้องกับเรื่องผลบังคับใช้ของกฎหมาย บทนิยามของสำคัญ

3.1.4.2 หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 8 ถึงมาตรา 18)

หมวดนี้จะมีความเกี่ยวข้องกับการจัดตั้งองค์กร หน่วยงาน และเจ้าหน้าที่ที่มีอำนาจบังคับใช้กฎหมาย ได้แก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีลักษณะเป็นองค์กรหรือหน่วยงานควบคุมกำกับ รวมทั้งมีอำนาจในการออกกฎหมายลำดับรอง

3.1.4.3 หมวด 2 การคุ้มครองส่วนบุคคล ในหมวดนี้มีการจำแนกแบ่งออก 3 ส่วนได้แก่ ส่วนที่ 1 บททั่วไป (มาตรา 19 ถึงมาตรา 21)

บทบัญญัติส่วนนี้มีการกำหนดเงื่อนไขหลักของกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ เหตุแห่งการเก็บรวบรวม ใช้ เปิดเผย (Lawful basic of processing)

ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล (มาตรา 22 ถึงมาตรา 26)

บทบัญญัติส่วนนี้อยู่ภายใต้เงื่อนไขทั่วไปดังกล่าวในส่วนที่ 1 โดยในส่วนนี้มีการกำหนดรายละเอียดของพฤติกรรมการเก็บรวบรวมข้อมูลส่วนบุคคล รวมทั้งหลักการเฉพาะสำหรับข้อมูลบางชนิด ซึ่งกฎหมายสหภาพยุโรปเรียกว่า ข้อมูลส่วนบุคคลชนิดพิเศษ (Special categories of personal data) โดยกฎหมายไทยอยู่ในมาตรา 26 บทบัญญัติในส่วนนี้รวมถึงการกำหนดหน้าที่ควบคุมข้อมูลในการแจ้งรายละเอียดตามมาตรา 23

ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล (มาตรา 27 ถึงมาตรา 29)

บทบัญญัติในส่วนนี้อยู่ภายใต้เงื่อนไขทั่วไปในส่วนที่ 1 โดยในส่วนนี้กำหนดรายละเอียดของพฤติกรรมการใช้และเปิดเผยข้อมูลส่วนบุคคล รวมไปถึงหลักเกณฑ์เฉพาะสำหรับกรณีการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

3.1.4.4 หมวดที่ 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล (มาตรา 30 ถึงมาตรา 42)

ในส่วนนี้มีการกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคล (Right of data subject) การใช้สิทธิชนิดต่าง ๆ หน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลการกำหนดหน้าที่และเงื่อนไขเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

3.1.4.5 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 43 ถึงมาตรา 70)

บทบัญญัติส่วนนี้กำหนดให้มีการตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอำนาจหน้าที่ของสำนักงาน คุณสมบัติของพนักงานเจ้าหน้าที่ของสำนักงาน

3.1.4.6 การร้องเรียน (มาตรา 71 ถึงมาตรา 78)

บทบัญญัติในส่วนนี้กำหนดถึงขั้นตอนการร้องเรียนเกี่ยวกับการฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลต่อสำนักงาน และขั้นตอนในการพิจารณาเรื่องร้องเรียน หลักการส่วนนี้มีลักษณะเป็นกระบวนการหรือวิธีการพิจารณาความ (Procedure)

3.1.4.7 หมวดที่ 6 ความรับผิดทางแพ่ง (มาตรา 77 ถึงมาตรา 78)

บทบัญญัติส่วนนี้กำหนดความรับผิดทางแพ่งเกี่ยวกับการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล รวมถึงให้ศาลมีอำนาจสั่งให้จ่ายค่าสินไหมทดแทนเชิงลงโทษ (Punitive damage)

3.1.4.7 หมวดที่ 7 บทกำหนดโทษ แบ่งออกเป็น

ส่วนที่ 1 โทษอาญา (มาตรา 79 ถึงมาตรา 81)

ส่วนที่ 2 โทษทางปกครอง (มาตรา 82 ถึงมาตรา 90)

3.1.4.9 บทเฉพาะกาล (มาตรา 91 ถึงมาตรา 96)

บทบัญญัติส่วนนี้วางหลักเกี่ยวกับขั้นตอนการเตรียมของหน่วยงานของรัฐที่เกี่ยวข้องกับการกำกับหรือควบคุมกฎหมาย ผู้ดำรงตำแหน่งต่าง ๆ ระหว่างที่ยังไม่มีการแต่งตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมทั้ง การจัดการข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมมาก่อน พระราชบัญญัตินี้จะมีผลบังคับใช้¹⁵

สำหรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฉบับนี้เน้นในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาต่อเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล ซึ่งการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้จะมีความสอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยและเนื่องจากสถานการณ์ในปัจจุบันมีการล่วงละเมิดสิทธิ

¹⁵ ภาณุกร ทอกรวิวงศ์. (2564). *คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล*. คณะนิติศาสตร์ และสถาบันกฎหมายสื่อดิจิทัล มหาวิทยาลัยเกษมบัณฑิต. หน้า 39-41.

ความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจ จึงถือได้ว่าสมควรมีการกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลขึ้น เพื่อใช้เป็นแนวทางและกำหนดหลักเกณฑ์ กติกา หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไปด้วยและควรที่จะมีบทลงโทษที่เจาะจงในกรณีที่มีการนำข้อมูลส่วนบุคคลของเด็กไปใช้หรือแสวงหาประโยชน์อันมิชอบแต่อย่างใด

นอกจากนี้ ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีประเด็นที่ต้องใช้ประกอบการพิจารณาในเรื่องของเด็กประกอบ รวมไปถึงมีฐานหรือเหตุทางกฎหมายในการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล ที่อาจจะต้องใช้ในการพิจารณาไปถึงเจตนาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่กำหนดให้การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล หรือที่ GDPR เรียกว่า “การประมวลผลข้อมูลส่วนบุคคล” ดังนั้นต้องมีฐานหรือทางกฎหมายรองรับ ซึ่งตามกฎหมายไทยแยกออกเป็น 2 กรณี คือ ฐานหรือเหตุสำหรับ การเก็บรวบรวมข้อมูลส่วนบุคคล ปรากฏในมาตรา 24 และฐานหรือเหตุสำหรับ การใช้และเปิดเผยข้อมูลส่วนบุคคล ปรากฏในมาตรา 27 ซึ่งกฎหมายวางเจตนาไว้สำหรับการเก็บรวบรวม ใช้และเปิดเผย โดยแยกเป็นสองมาตราและอยู่ภายใต้หลักการเดียวกัน กล่าวคือ โดยหลักแล้ว “ห้าม” เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูล และกำหนดเหตุหรือฐานอื่นที่ไม่ต้องอาศัยความยินยอม ซึ่งผู้เขียนสรุปฐาน หรือเหตุทั้งหมด 7 ประการ ได้แก่ ฐานความยินยอม (มาตรา 19 และ 24) ฐานการปฏิบัติตามสัญญาเกี่ยวกับเจ้าของข้อมูล (มาตรา 24 (3)) ฐานปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุม (มาตรา 24 (6)) ฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (มาตรา 24 (2)) ฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ (มาตรา 24 (4)) ฐานประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (มาตรา 24 (5)) และฐานจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือการศึกษาวิจัย หรือสถิติ (มาตรา 24 (1)) จากที่กล่าวมานั้น ได้นำฐานบางฐานมาพิจารณาถึงกรณีของเด็ก ดังนี้

1) ฐานความยินยอม

หากกล่าวถึงในประเด็นของเรื่องความยินยอม ความยินยอม (Consent) ถือเป็นเหตุหรือฐานทางกฎหมายที่เชื่อมโยงกับแนวคิดการคุ้มครองข้อมูลส่วนบุคคลในแง่ของสิทธิการตัดสินใจ กำหนดตัวตนและการควบคุมข้อมูลส่วนบุคคลของตนเอง (Control theory) ตาม GDPR ที่มีบทบัญญัติเกี่ยวกับความยินยอม คือมาตรา 6 กำหนดให้ความยินยอมเป็นหนึ่งในเหตุหรือฐานของการประมวลผลข้อมูล โดยชอบด้วยกฎหมาย¹⁶ และมาตรา 4 กำหนดถึงองค์ประกอบหรือเงื่อนไขของความยินยอม

¹⁶ General Data Protection Regulation (GDPR). Article 6 (1) (a).

ไว้หลายประการ เช่น อีสระ เฉพาะเจาะจง ได้รับข้อมูลแจ้งข้อมูลประกอบ แสดงความประสงค์ เจ้าของข้อมูลอย่างชัดเจน ไม่คลุมเครือ เป็นต้น

การขอความยินยอมหากทำการศึกษา นั้นจะมีการกำหนดไว้ในมาตรา 19 วรรคสาม ว่า การขอความยินยอมนั้นจะต้องมีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย โดยเงื่อนไขนี้เปรียบเทียบกับ GDPR มาตรา 7 ที่มีการวางหลัก ความยินยอมในรูปแบบลายลักษณ์อักษรและเกี่ยวข้องกับเรื่องอื่นด้วยนั้น การขอความยินยอมต้องแสดงออกในรูปแบบที่เข้าใจได้และเข้าถึงง่าย ใช้ภาษาที่ชัดเจน¹⁷ นอกจากนี้ ยังมีการขยายอธิบายว่า การขอความยินยอมตามรูปแบบที่ผู้ควบคุมข้อมูลกำหนดไว้แล้ว จะต้องอยู่ในรูปแบบที่เข้าใจได้และเข้าถึงง่าย ใช้ภาษาที่ง่ายและชัดเจน และไม่มีข้อกำหนดที่ไม่เป็นธรรม¹⁸

การขอความยินยอมสำหรับผู้เยาว์ คนไร้ความสามารถ คนเสมือนไร้ความสามารถ

กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดหลักการและเงื่อนไขเกี่ยวกับความยินยอมเป็นการเฉพาะสำหรับบุคคลบางประเภท ดังนี้

มาตรา 20 ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะ โดยการสมรส หรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้วตามมาตรา 27 แห่งประมวลกฎหมายแพ่งและพาณิชย์ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าวดำเนินการดังต่อไปนี้

(1) กรณีที่ให้การยินยอมของผู้เยาว์ไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจจะให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ในมาตรา 22 มาตรา 23 หรือมาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

(2) ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนไร้ความสามารถ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนเสมือนไร้ความสามารถ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

¹⁷ General Data Protection Regulation (GDPR). Article 7.

¹⁸ General Data Protection Regulation (GDPR). Article 42.

ให้นำความในวรรคหนึ่ง วรรคสอง และวรรคสาม มาใช้บังคับกับการถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การร้องเรียนของเจ้าของข้อมูลส่วนบุคคล และการอื่นใดตามพระราชบัญญัตินี้ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถโดยอนุโลม

การขอความยินยอมตามมาตรา 20 สามารถแยกพิจารณาตามลักษณะของบุคคล 8 กลุ่ม ดังนี้

(1) บุคคลที่บรรลุนิติภาวะตามกฎหมายแพ่งและพาณิชย์ ได้แก่ บุคคลที่มีอายุยี่สิบปีบริบูรณ์¹⁹ บุคคลเหล่านี้ไม่ใช่ผู้เยาว์ สามารถทำนิติกรรมสัญญาใดเอง ดังนั้น หากผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ เปิดเผย ข้อมูลของเจ้าของข้อมูลที่อายุยี่สิบปีบริบูรณ์ โดยอาศัยฐานหรือเหตุความยินยอมก็ไม่ต้องพิจารณามาตรา 20 แต่เป็นไปตามมาตรา 24 ประกอบมาตรา 19 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลสัญญา โดยตนเองเช่นเดียวกับกลุ่มที่หนึ่ง จึงสามารถขอความยินยอมตามกฎหมายคุ้มครองข้อมูล

(2) บุคคลที่บรรลุนิติภาวะโดยการสมรส²⁰ บุคคลเหล่านี้สามารถแสดงเจตนาทำสัญญาโดยตนเองเช่นเดียวกับกลุ่มหนึ่ง จึงสามารถขอความยินยอมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลจากเจ้าของข้อมูลโดยตรง

(3) บุคคลที่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้วตามมาตรา 27 แห่งประมวลกฎหมายแพ่งและพาณิชย์²¹ กล่าวคือ ผู้เยาว์ที่ทำการประกอบธุรกิจการค้าหรือธุรกิจอื่นหรือทำสัญญาเป็นลูกจ้างในสัญญาจ้างแรงงาน โดยผู้แทนโดยชอบธรรมให้ความยินยอมแล้ว กฎหมายแพ่งและพาณิชย์ถือว่า ในความเกี่ยวพันกับการประกอบธุรกิจหรือการจ้างแรงงานกล่าวนั้น ให้ผู้เยาว์มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้ว

(4) ผู้เยาว์ อายุตั้งแต่ 10 ปี แต่ไม่ถึง 20 ปีบริบูรณ์ ในกรณีการใด ๆ ที่ผู้เยาว์ดังกล่าวให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ในมาตรา 22 มาตรา 23 หรือมาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์

ตามมาตรา 20 วรรคหนึ่ง (1) การขอความยินยอมบุคคลกลุ่มนี้ แยกเป็น 3 กรณีย่อย ดังนี้

¹⁹ ประมวลกฎหมายแพ่งและพาณิชย์. มาตรา 19.

²⁰ ประมวลกฎหมายแพ่งและพาณิชย์. มาตรา 20.

²¹ ประมวลกฎหมายแพ่งและพาณิชย์. มาตรา 27.

1) การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ใน มาตรา 22 แห่งประมวลกฎหมายแพ่งและพาณิชย์ กล่าวคือ หากผู้เยาว์ทำการเพื่อได้ไปซึ่งสิทธิและ มีการเก็บรวมข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการใด ๆ ที่ผู้เยาว์ทำเพื่อได้ไปซึ่งสิทธิ จะเป็นกรณีที่ไม่ต้องขอความยินยอมเกี่ยวกับข้อมูลส่วนบุคคลจากผู้ใช้อำนาจปกครอง ผู้เยาว์อาจทำการใด ๆ ได้ทั้งสิ้น หากเป็นเพียงเพื่อจะได้ไปซึ่งสิทธิอันใดอันหนึ่ง หรือเป็นการเพื่อให้หลุดพ้นอันใดอันหนึ่ง

2) การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอม โดยลำพังได้ตามที่บัญญัติไว้ใน มาตรา 23 แห่งประมวลกฎหมายแพ่งและพาณิชย์ กล่าวคือเป็นกรณีผู้เยาว์ต้องแสดงเจตนาทำนิติกรรมเอง โดยเฉพาะไม่อาจให้ผู้อื่นทำการแทนได้ เช่น การทำพินัยกรรมซึ่งผู้เยาว์สามารถกระทำได้เมื่อมีอายุสิบห้าปีบริบูรณ์ เป็นต้น

3) การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ใน มาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์ กล่าวคือ เป็นการใด ๆ ซึ่งสมแก่ฐานานุรูป และจำเป็นในการดำรงชีพของผู้เยาว์

(5) ผู้เยาว์ อายุตั้งแต่ 10 ปีแต่ไม่ถึง 20 ปีบริบูรณ์ ในกรณีที่มิใช่การใด ๆ ที่ผู้เยาว์ดังกล่าวให้ความยินยอมโดยลำพังได้ตามบัญญัติไว้ในมาตรา 22 มาตรา 23 หรือมาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์

การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของผู้เยาว์ไม่เกี่ยวข้องกับ นิติกรรม หรือการดำเนินการที่ได้รับการยกเว้นตามประมวลกฎหมายแพ่งและพาณิชย์ ดังกล่าว ในกลุ่มที่สี่ข้างต้น ดังนี้ ตามมาตรา 20 วรรคหนึ่ง (1) ผู้ควบคุมข้อมูลส่วนบุคคล ต้องขอความยินยอมจากผู้เยาว์ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล และขอความยินยอมจากผู้แทนโดยชอบธรรมของผู้เยาว์นั้นด้วย

(6) ผู้เยาว์อายุไม่เกิน 10 ปี

ตามมาตรา 20 วรรคหนึ่ง (2) หากผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของผู้เยาว์กลุ่มนี้ โดยอาศัยหรือฐานความยินยอม จะไม่สามารถขอความยินยอมจากผู้เยาว์ซึ่งเป็นเจ้าของข้อมูลแต่ต้องไปขอความยินยอมจากผู้แทนโดยชอบธรรมของผู้เยาว์นั้น

(7) ในกรณีเจ้าของข้อมูลส่วนบุคคลเป็นคนที่ไร้ความสามารถ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ขอความยินยอมจากผู้อุปการะที่มีอำนาจกระทำการแทน คนไร้ความสามารถ

(8) ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นเสมือนไร้ความสามารถ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ²²

2) ฐานหรือเหตุทางกฎหมายในการเก็บรวบรวมในการ ใ้เปิดเผย ข้อมูลส่วนบุคคลชนิดพิเศษ

ในกรณีนี้ ข้อมูลส่วนบุคคลชนิดพิเศษตามมาตรา 26 ซึ่งกฎหมายกำหนดหลักการเกี่ยวกับฐานหรือเหตุในการเก็บรวบรวม ใ้เปิดเผย เป็นเฉพาะแยกต่างหากจากมาตรา 24 โดยเริ่มจากการชี้ให้เห็นความหมายและขอบเขตของข้อมูลส่วนบุคคลชนิดพิเศษ

มาตรา 26 “...ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรมข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด...”

จากหลักกฎหมายทำให้เห็นได้ว่าการกล่าวถึงกรณี ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ข้อมูลส่วนบุคคลเกี่ยวกับลัทธิ ศาสนาหรือปรัชญา ข้อมูลส่วนบุคคลเกี่ยวกับการพิการ ข้อมูลส่วนบุคคลเกี่ยวกับความคิดเห็นทางการเมือง ข้อมูลส่วนบุคคลเกี่ยวกับพฤติกรรมทางเพศ ข้อมูลประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ²³

นอกจากนี้ ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีการกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น สิทธิถอนความยินยอมหรือสิทธิในการได้รับการแจ้งข้อมูล ตามมาตรา 23 ได้มีการแยกสิทธิของเจ้าของข้อมูล 8 ประการ ดังนี้

(1) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of access)

ตามมาตรา 30 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 วางหลักว่า

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

²² ชาญชีพ ทองรวีวงศ์. (2564). *คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล*. กรุงเทพฯ: นิติธรรม. หน้า 169-173.

²³ เรื่องเดียวกัน, หน้า 222-270.

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอตามวรรคหนึ่ง จะปฏิเสธคำขอได้เฉพาะในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล และการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอตามวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 39

เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม้อาจปฏิเสธคำขอได้ตามวรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่ได้รับคำขอ

คณะกรรมการอาจกำหนดหลักเกณฑ์เกี่ยวกับการเข้าถึงและการขอรับสำเนาตามวรรคหนึ่ง รวมทั้งการขยายระยะเวลาตามวรรคสี่หรือหลักเกณฑ์อื่นตามความเหมาะสมก็ได้

(2) สิทธิในการแก้ไขข้อมูลส่วนบุคคล (Right to rectification)

ในสิทธิข้อนี้นี้มีปรากฏใน GDPR “เจ้าของข้อมูลมีสิทธิเรียกร้องให้ผู้ควบคุมข้อมูลทำการแก้ไขโดยไม่ชักช้าซึ่งข้อมูลส่วนบุคคลที่ไม่ถูกต้องเกี่ยวกับตน รวมทั้งมีสิทธิขอให้ดำเนินการทำให้สมบูรณ์ซึ่งข้อมูลที่ไม่สมบูรณ์ ซึ่งรวมถึงการให้รายละเอียดเพิ่มเติม ทั้งนี้เมื่อพิจารณาถึงวัตถุประสงค์ของการประมวลผล”²⁴ สำหรับกฎหมายไทยหลักการนี้จะมีปรากฏอยู่ในมาตรา 35 และ มาตรา 36

ในมาตรา 35 เป็นหลักความถูกต้องของข้อมูล

ในมาตรา 36 กำหนดว่า “ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการ ตามมาตรา 35 หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคล ต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 39 ให้นำความในมาตรา 34 วรรคสอง มาใช้บังคับโดยอนุโลม”

จากหลักกฎหมายข้างต้น มีประเด็นพิจารณา ดังนี้

แม้มาตรา 35 อยู่ในหมวดสิทธิของเจ้าของข้อมูลแต่วางหลักในลักษณะกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลรักษาความ “ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด” จึงกล่าวได้ว่า แม้เจ้าของข้อมูลไม่มีคำร้องขอ ผู้ควบคุมข้อมูลมีหน้าที่ดำเนินการรักษาคุณภาพหรือมาตรฐานของข้อมูล (Data quality) หากตรวจสอบพบว่าข้อมูลไม่สอดคล้องกับเงื่อนไขเชิงคุณภาพ เช่น ผิดพลาด ไม่สมบูรณ์ ก็ต้องทำการแก้ไข อย่างไรก็ตามมาตรานี้ไม่ได้กำหนดความรับผิดชอบหรือโทษทางปกครอง

²⁴ General Data Protection Regulation (GDPR). Article 16.

เมื่อเจ้าของข้อมูลร้องขอใช้สิทธิมาตรา 36 แต่ผู้ควบคุมข้อมูลปฏิเสธคำร้อง กฎหมายให้บันทึกการและเหตุการณ์ปฏิเสธไว้ตามมาตรา 39 แต่มาตรานี้ไม่ได้กำหนด เหตุเฉพาะเจาะจงที่ผู้ควบคุมข้อมูลส่วนบุคคลจะยกขึ้นอ้างเพื่อปฏิเสธการใช้สิทธินี้ ซึ่งต่างจาก สิทธิอื่นที่กฎหมายกำหนดเหตุปฏิเสธสิทธิ โดยเฉพาะ เช่น สิทธิขอให้ลบตามมาตรา 33 สิทธิคัดค้าน ตามมาตรา 32 อย่างไรก็ตาม ผู้ควบคุมข้อมูลอาจปฏิเสธด้วยเหตุผลว่าข้อมูลนั้นมีคุณภาพตามเงื่อนไข ของมาตรา 35 เช่น ปฏิเสธโดยอ้างว่าข้อมูลถูกต้องหรือเป็นปัจจุบันอยู่แล้ว รวมทั้งอาจเตรียมหลักฐาน เพื่อพิสูจน์ความถูกต้องสมบูรณ์ของข้อมูลส่วนบุคคล หากมีการร้องเรียน

มาตรา 36 วรรคสองกำหนดให้นำมาตรา 34 วรรคสองมาใช้บังคับ โดยอนุโลม กล่าวคือ หากมีการปฏิเสธสิทธิ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ เพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

หากผู้ควบคุมข้อมูลยอมปฏิบัติตามคำร้อง มาตรา 36 ไม่ได้กำหนดให้บันทึก การตามมาตรา 39 สำหรับมาตรา 39 ก็ไม่ได้ระบุชัดเจนให้ต้องบันทึก เนื่องจากมาตรา 39 (4) กำหนดเฉพาะสิทธิเข้าถึง และ 39 (7) กำหนดเฉพาะการปฏิเสธสิทธิบางกรณีที่ไม่รวมถึงสิทธิ ขอแก้ไขตามมาตรา 36 แต่หากบันทึกไว้เพื่อการตรวจสอบก็ไม่มีข้อห้าม

ในกรณีที่ผู้ควบคุมข้อมูลดำเนินการตามมาตรา 35 แล้ว แต่เจ้าของข้อมูล ยังคงมีสิทธิร้องขอแก้ไข หากผู้ควบคุมข้อมูลเห็นว่าตนกระทำการสอดคล้องกับมาตรา 35 ก็สามารถ แสดงหลักฐานเพื่อปฏิเสธ

แม้มาตรา 36 ไม่ได้ระบุถึงสิทธิการร้องขอให้ทำข้อมูลที่ไม่สมบูรณ์ให้สมบูรณ์ โดยการให้รายละเอียดเพิ่มเติม (Providing a supplementary statement) ดังเช่น GDPR แต่มาตรา 35 กำหนดครอบคลุมการทำให้ “สมบูรณ์” เจ้าของข้อมูลจึงมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลเพิ่มเติม ข้อมูลเกี่ยวกับข้อมูลส่วนบุคคลให้สมบูรณ์ด้วย

(3) สิทธิในการขอให้ลบข้อมูลส่วนบุคคล (Right to erasure) หรือ สิทธิที่จะถูกลืม (Right to be forgotten)

ข้อพิจารณาและเปรียบเทียบกับกฎหมายไทย

(3.1) ประเด็นเกี่ยววิธีดำเนินการลบข้อมูลในบริบทของผู้ให้บริการสืบค้น

แม้ GDPR กำหนดคำว่าลบ (Erasure)²⁵ แต่ศาลยุโรปตีความขยายไปถึง การยุติหรือระงับการเชื่อมโยงลิงก์ จะเห็นได้จาก คดี C-136/17 และ คดี C-131/12 เป็นกรณีเจ้าของ ข้อมูลขอให้ยุติการเชื่อมโยงลิงก์ข้อมูลชื่อของตนกับผลการค้นหาเว็บไซต์ต่าง ๆ ที่มีเนื้อหาเกี่ยวกับ

²⁵ Case C-136/17 , GC and Other v Commission nationale de l’imformatique et des libertes (CNIL) , The Court of Justice of the European Union, Judgment of the court (Grand Chamber) of 24 September 2019.

เจ้าของข้อมูล ซึ่งส่งผลให้ผู้ใช้งานอื่นที่ใช้อ้างอิงข้อมูลในการสืบค้นจะไม่ปรากฏผลการค้นหาที่เชื่อมโยงไปยังแหล่งเก็บข้อมูล มิใช่การเรียกร้องให้ “ลบหรือทำลาย” เนื้อหา เปรียบเทียบกับมาตรา 33 กำหนดขอบเขตขงสิทธิ 3 ประการคือ “ลบหรือทำลาย หรือทำให้ข้อมูลที่ไม่สามารถระบุตัวบุคคล” ดังนั้น โดยสภาพข้อเท็จจริงแล้ว ผู้บริการสืบค้นข้อมูลหรือผู้ให้บริการอื่นซึ่งมิได้จัดเก็บหรือเก็บรักษาข้อมูลส่วนบุคคล จึงไม่สามารถดำเนินการดังกล่าว

(3.2) การดำเนินการอื่นนอกเหนือจากการลบ การดำเนินการเหล่านี้ไม่อยู่ในขอบเขตของการลบหรือทำลายตามมาตรา 33 สำหรับมาตรา 35 นั้นเห็นว่าผู้ควบคุมข้อมูลซึ่งไม่ได้เป็นผู้จัดเก็บข้อมูลเนื้อหาไม่มีหน้าที่แก้ไขให้เป็นปัจจุบัน

(4) สิทธิในการคัดค้านการประมวลข้อมูลส่วนบุคคล (Right to object)

สิทธินี้ปรากฏในมาตรา 32 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งเทียบได้กับมาตรา 21 ของ GDPR โดยจะแยกอธิบาย ดังนี้

(1) เงื่อนไขและข้อจำกัดสิทธิคัดค้าน

กฎหมายกำหนดเหตุหรือเงื่อนไขของใช้สิทธิคัดค้าน โดยแยกเป็น 3 กรณี

1. การคัดค้านตามมาตรา 32 (1)

การคัดค้านกรณีนี้ต้องพิจารณาเชื่อมโยงกับเหตุหรือฐานตามมาตรา 24 โดยจำกัดเฉพาะเหตุหรือฐานต่อไปนี้

(ก) ข้อมูลส่วนบุคคลที่เก็บรวบรวมตามมาตรา 24 (4) เช่น การดำเนินการกิจของหน่วยงานรัฐในการเก็บรวบรวม เปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์เกี่ยวกับการสาธารณสุข

(ข) ข้อมูลส่วนบุคคลที่เก็บรวบรวมตามมาตรา 24 (5) เช่น การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อรักษาความปลอดภัยในอาคาร สถานที่ การป้องกันหรือตรวจสอบการทุจริต หรือการบริหารจัดการโดยทั่วไปขององค์กร

แม้จะเป็นข้อมูลส่วนบุคคลที่เข้าเหตุหรือฐานใดฐานหนึ่งข้างต้น แต่ผู้ควบคุมข้อมูลส่วนบุคคลอาจปฏิเสธการใช้สิทธิคัดค้านหากเข้าเงื่อนไขตาม (ก) หรือ (ข)

(5) สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล (Right to restrict processing)

สิทธินี้ปรากฏในมาตรา 34 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งเทียบได้กับมาตรา 18 ของ GDPR

กรณีนี้จะต้องปรากฏว่าเจ้าของข้อมูลใช้สิทธิคัดค้านตามมาตรา 32 และผู้ควบคุมข้อมูลปฏิเสธโดยอาศัยเหตุที่กฎหมายกำหนด ให้ระหว่างการตรวจสอบเพื่อปฏิเสธการคัดค้านนี้

เจ้าของข้อมูลอาจใช้สิทธิตามมาตรา 34 เพื่อขอให้ระงับการใช้ ซึ่งสามารถแยกพิจารณาได้ 2 กรณี ดังนี้

1. การคัดค้านตามมาตรา 32 (1)
2. การคัดค้านตามมาตรา 32 (3)

(6) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (Right to data portability)

สิทธินี้ปรากฏใน มาตรา 31 ดังนี้ “เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ รวมทั้งมีสิทธิ ดังต่อไปนี้

(1) ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ

(2) ขอรับข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น โดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้

ข้อมูลส่วนบุคคลตามวรรคหนึ่งต้องเป็นข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ หรือเป็นข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 (3) หรือเป็นข้อมูลส่วนบุคคลอื่นที่กำหนดในมาตรา 24 ตามที่คณะกรรมการประกาศกำหนด

การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งจะใช้กับการส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ หรือเป็นการปฏิบัติหน้าที่ตามกฎหมายไม่ได้ หรือการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น ทั้งนี้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอด้วยเหตุผลดังกล่าวให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 39

(7) สิทธิในการได้รับแจ้งข้อมูลหรือรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล (Right to be informed)

กฎหมายคุ้มครองข้อมูลส่วนบุคคล กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับแจ้งข้อมูลหรือรายละเอียด (Right to be informed) จากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในหลายกรณี เช่น

สิทธิที่จะได้รับการแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้เปิดเผยข้อมูลส่วนบุคคล (Privacy information หรือ Privacy notice) ตามมาตรา 23 ซึ่งกำหนดประเด็นหรือหัวข้อเรื่องที่ต้องแจ้งให้เจ้าของข้อมูลทราบ เช่น วัตถุประสงค์ในการเก็บรวบรวม ข้อมูลที่เก็บ ระยะเวลาในการเก็บ

สิทธิได้รับการแจ้งรายละเอียดไปพร้อมกับการขอความยินยอม ทั้งนี้ ตามมาตรา 19 ประกอบมาตรา 24 หรือ 27 หากผู้ควบคุมข้อมูลส่วนบุคคลอาศัยเหตุหรือฐานความยินยอมในการเก็บรวบรวม ใช้เปิดเผยข้อมูลส่วนบุคคล จะต้องแจ้งวัตถุประสงค์ไปด้วยพร้อมกับการขอความยินยอมหรือก่อนการขอความยินยอมขึ้นอยู่กับลักษณะและวิธีการขอความยินยอม สำหรับกรณีข้อมูลส่วนบุคคลชนิดพิเศษตามมาตรา 26 หากอาศัยเหตุหรือฐานความยินยอม ก็จะต้องแจ้งรายละเอียดให้เจ้าของข้อมูลทราบเช่นกัน สิทธินี้ได้กล่าวถึงในหัวข้อฐานหรือเหตุความยินยอม

สิทธิได้รับการแจ้งวัตถุประสงค์ใหม่ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดตามมาตรา 23 (Privacy notice) ซึ่งมีการระบุวัตถุประสงค์แล้ว จะมีหน้าที่ไม่กระทำการกับข้อมูลนอกเหนือวัตถุประสงค์ที่แจ้ง หากจะทำการแตกต่างจากวัตถุประสงค์ดังกล่าว มาตรา 21 กำหนดให้แจ้งวัตถุประสงค์ใหม่พร้อมกับต้องขอความยินยอมก่อน สิทธินี้อยู่ภายใต้หลักการประมวลผลข้อมูลส่วนบุคคลเพิ่มเติมหรือแตกต่างจากวัตถุประสงค์ที่แจ้งไว้ (Further processing of personal data)

สิทธิที่จะได้รับการแจ้งให้ทราบถึงผลกระทบจากการถอนความยินยอม มีความสัมพันธ์กับฐานหรือเหตุความยินยอมและสิทธิถอนความยินยอมตามมาตรา 19 ซึ่งวางหลักว่าเจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเมื่อใดก็ได้ และหากการถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล ในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

สิทธิที่จะได้รับการแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เนื่องจากมาตรา 40 กำหนดว่า

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อและวิธีการติดต่อให้เจ้าของข้อมูลส่วนบุคคลทราบ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อในเรื่องเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลและการใช้สิทธิต่าง ๆ นอกจากนี้ ในส่วนของผู้ควบคุมข้อมูลส่วนบุคคล การแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลจัดเป็นส่วนหนึ่งของการแจ้งรายละเอียดตาม มาตรา 23

สิทธิที่จะได้รับการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (มาตรา 37 (4)) (Data breach notification) สิทธินี้อยู่บนพื้นฐานหลักการที่แตกต่างจากสิทธิในการได้รับแจ้งรายละเอียด

เกี่ยวกับการประมวลผล เนื่องจากเชื่อมโยงกับหลักการรักษาความมั่นคงปลอดภัย (Data security) กล่าวคือ เมื่อมีภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล ซึ่งอาจเกิดจากการกระทำของผู้ควบคุมข้อมูล ผู้ประมวลผล หรือบุคคลที่สาม เช่น อาชญากรรมชนิดต่าง ๆ กฎหมายกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลแจ้งให้เจ้าของข้อมูลทราบเมื่อเข้าเงื่อนไขที่กำหนด

3.2 หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลของเด็กในต่างประเทศ

3.2.1 สหรัฐอเมริกา

สหรัฐอเมริกาคือเป็นประเทศที่ประสบพบเจอกับปัญหาละเมิดข้อมูลส่วนบุคคลมากที่สุด เนื่องจากเป็นประเทศที่มีความเจริญทางวิทยาศาสตร์และเทคโนโลยีประเทศหนึ่ง สหรัฐอเมริกามีกฎหมายเป็นระบบคอมมอนลอว์ ดังนั้น การคุ้มครองความเป็นส่วนตัวในประเทศจึงปรากฏในกรณีพิพาทการละเมิดความเป็นส่วนตัวในการพิจารณาคดีของศาล โดยแนวคิดเรื่องการคุ้มครองความเป็นส่วนตัวมักจะอยู่ในรูปของกฎหมายในส่วนที่ว่าด้วยความรับผิดชอบทางละเมิดมากกว่าที่จะปรากฏอยู่ในรูปแบบของกฎหมายรัฐธรรมนูญหรือรัฐบัญญัติ

การคุ้มครองสิทธิความเป็นส่วนตัวได้รับการพัฒนาอีกครั้งเมื่อมีการเผยแพร่บทความเรื่อง “The Right to Privacy”²⁶ ที่ชี้ให้เห็นว่า นอกเหนือจากสิทธิความเป็นส่วนตัวที่ได้รับความคุ้มครองในคอมมอนลอว์ที่อยู่แล้ว บุคคลควรได้รับการคุ้มครองสิทธิความเป็นส่วนตัวที่เกี่ยวกับการเผยแพร่หรือการตีพิมพ์ข้อเท็จจริงที่เกี่ยวกับตนด้วย²⁶

ประสิทธิ์ ปิวาวัฒนพานิช²⁷ ได้ทำการศึกษาถึงเรื่องของลักษณะทั่วไปของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาไว้ในรายงานวิจัย สรุปได้ว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกามีลักษณะเป็นระบบกฎหมายเฉพาะเรื่อง ไม่มีกฎหมายแม่บทหรือกฎหมายกลางวางหลักเกณฑ์เป็นการทั่วไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสภาองเกรสจะตราบัญญัติก็ต่อเมื่อเกิดปัญหาการป้องกันความลับหรือคุ้มครองสิทธิในความเป็นส่วนตัวของประชาชนเมื่อมี

²⁶ นคร เสรีรักษ์. (2557). *ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย*. กรุงเทพฯ: ฟ้ายาม. หน้า 157.

²⁷ ประสิทธิ์ ปิวาวัฒนพานิช. (2547). *กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา* รายงานการวิจัยโครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำร่างงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ.2540. กรุงเทพฯ: สถาบันวิจัยและให้ปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์. หน้า 49-70.

การละเมิด ดังนั้น การออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาจึงมีลักษณะเป็นการแก้ไขปัญหาที่เกิดขึ้นมากกว่าที่จะวางหลักเกณฑ์ทั่วไปเพื่อป้องกันปัญหา

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกานี้มีลักษณะเป็นกฎหมายเฉพาะเรื่อง ซึ่งแต่ละเรื่องจะมุ่งให้ความคุ้มครองข้อมูลส่วนบุคคลในเรื่องใดเรื่องหนึ่งโดยเฉพาะและมีกฎหมายดังกล่าวเป็นจำนวนมาก ทั้งในระดับสหพันธรัฐและในระดับมลรัฐ ในการศึกษานี้จะหยิบยกมาพิจารณาเฉพาะ The Privacy Act of 1974 ซึ่งเป็นกฎหมายที่มีลักษณะเป็นกฎหมายกลางในระดับชาติ และ Safe-Harbor²⁸ ซึ่งเป็นเรื่องที่เกี่ยวข้องกับสหภาพยุโรปในระบบกฎหมายระหว่างประเทศ

The Privacy Act of 1974 มีวัตถุประสงค์เพื่อป้องกันมิให้มีการจัดเก็บ วิเคราะห์ หรือการเผยแพร่ข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐซึ่งนำข้อมูลส่วนบุคคลเหล่านี้ไปใช้ในทางที่มิชอบ ก่อให้เกิดความเสียหายแก่ผู้เป็นเจ้าของข้อมูล นอกจากนี้ยังรับรองสิทธิเจ้าของข้อมูลในการเข้าถึงข้อมูลของตน และมีสิทธิในการโต้แย้งความถูกต้องของข้อมูลของตนที่อยู่ในความครอบครองของรัฐอีกด้วย

เนื่องจากสหรัฐอเมริกาไม่มีองค์กรอิสระที่มีอำนาจหน้าที่ในการควบคุมดูแลสิทธิส่วนบุคคลโดยตรง การคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชนจึงอาศัยกลไกการดำเนินการให้บรรล่วัตถุประสงค์ตามกฎหมายเรียกว่า ระบบควบคุมตนเอง (Self-regulation) ทำให้ปัจจุบันองค์กรที่มีอำนาจหน้าที่จึงได้แก่ องค์กรที่มีอำนาจหน้าที่ตามกฎหมายเฉพาะเรื่องนั้น ๆ เท่านั้น เช่น The Federal Trade Commission (FTC) ที่มีอำนาจในการตรวจสอบเกี่ยวกับข้อมูลความน่าเชื่อถือทางการเงินของผู้บริโภค (Consumer credit) การตรวจสอบข้อมูลเด็กทางอินเทอร์เน็ตและการตรวจสอบข้อมูลเกี่ยวกับการแข่งขันทางการค้าที่ไม่เป็นธรรม เป็นต้น

ในปี ค.ศ. 1998 เด็กเกือบ 10 ล้านคนใช้อินเทอร์เน็ตเป็นประจำ บริษัทการตลาดและผู้โฆษณาได้ชักชวนให้เด็กเหล่านี้ให้ข้อมูลส่วนบุคคลที่พวกเขาจะเพิ่มลงในฐานข้อมูลของพวกเขา เด็กส่วนใหญ่ไม่เข้าใจถึงปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นจากการให้รายละเอียดส่วนบุคคล ดังนั้นพวกเขาจึงไม่รีรอที่จะป้อนข้อมูลนี้เพื่อเข้าถึงเกมออนไลน์ยอดนิยม

แม้ว่าเด็ก ๆ จะสามารถเข้าถึงเกมได้โดยการให้ข้อมูลส่วนบุคคล แต่ธุรกิจการตลาดกำลังรวบรวมข้อมูลนี้และจัดเก็บไว้ในฐานข้อมูล ในทางกลับกันข้อมูลนี้จะถูกจัดเป็นหมวดหมู่และขายให้กับธุรกิจอื่น ๆ เป็นรายการโฆษณา ตัวอย่างเช่น ร้านขายของเล่นอาจได้รับประโยชน์อย่างมาก

²⁸ เป็นผลจากการที่สหภาพยุโรปประกาศใช้ The European Commission's Directive on Data Protection.

จากการซื้อรายชื่อลูกค้าเป้าหมายที่มีข้อมูลส่วนบุคคลเกี่ยวกับเด็กอายุระหว่างห้าถึงสิบสามปี เนื่องจากพวกเขาสามารถใช้โอกาสในการขายเหล่านี้เพื่อทำการตลาดผลิตภัณฑ์ของตนได้²⁹

กฎหมายคุ้มครองความเป็นส่วนตัวของเด็ก (Children's Privacy Protection Act หรือ COPPA) ในปี 2541 กฎหมายฉบับนี้มีผลบังคับใช้ในปี 2543 กำกับดูแลคณะกรรมการการค้าแห่งสหพันธรัฐ (FTC)³⁰ ให้จัดทำและบังคับใช้กฎระเบียบเกี่ยวกับความเป็นส่วนตัวทางออนไลน์ของเด็ก ในเดือนธันวาคม ค.ศ. 2012 FTC ได้ทำการเปลี่ยนแปลงกฎ COPPA ซึ่งมีผลบังคับใช้ในวันที่ 1 กรกฎาคม ค.ศ. 2013

3.2.1.1 ความหมายของคำนิยามของข้อมูลส่วนบุคคลของเด็กตามบทบัญญัติของ COPPA

คำจำกัดความของ “ข้อมูลส่วนบุคคล” คือ คำจำกัดความของข้อมูลส่วนบุคคลของ COPPA คือข้อมูลที่ระบุตัวบุคคลได้เกี่ยวกับบุคคลที่รวบรวมทางออนไลน์ ซึ่งรวมถึง ชื่อและนามสกุล บ้านหรือที่อยู่ทางกายภาพอื่น ๆ รวมถึงชื่อถนนและชื่อเมืองหรือเมือง ที่อยู่อีเมล หมายเลขโทรศัพท์ หมายเลขประกันสังคม ตัวระบุอื่นใดที่คณะกรรมการกำหนดอนุญาตให้มีการติดต่อทางกายภาพหรือออนไลน์ของบุคคลใดบุคคลหนึ่ง ข้อมูลเกี่ยวกับเด็กหรือผู้ปกครองของเด็กที่เว็บไซต์รวบรวมทางออนไลน์จากเด็กและรวมกับตัวระบุที่อธิบายไว้ในย่อหน้านี้

กฎหมายได้แก้ไขโดยขยายขอบเขตและเสริมความแข็งแกร่งของ COPPA อย่างมีนัยสำคัญเพื่อสะท้อนถึงเทคโนโลยีที่พัฒนาและการเปลี่ยนแปลงวิธีที่เด็กใช้และเข้าถึงอินเทอร์เน็ตได้ดีขึ้น รวมถึงการใช้สมาร์ทโฟนและอุปกรณ์มือถือที่เพิ่มขึ้น

ในคำจำกัดความของ “ข้อมูลส่วนบุคคล” ของ COPPA นั้นได้ให้ความหมายกว้าง ๆ ซึ่งรวมถึงชื่อของเด็ก บ้านหรืออีเมล หมายเลขโทรศัพท์ หมายเลขประกันสังคม ข้อมูลตำแหน่งทางภูมิศาสตร์ รูปภาพ วิดีโอ หรือเสียงของเด็ก ตัวระบุอุปกรณ์ที่ไม่ซ้ำกัน หรือที่อยู่ IP³¹

²⁹ Millicent Kelly. (2021). *Children's Online Privacy Protection Act (COPPA): Definition & Compliance.* (online). Available: <https://study.com/academy/lesson/childrens-online-privacy-protection-act-coppa-definition-compliance.html>. [2021, August 14].

³⁰ FTC (Federal Trade Commission) คือ คณะกรรมการการค้าแห่งสหพันธรัฐ (FTC) เป็นหน่วยงานของรัฐบาลที่จัดตั้งขึ้นในปี พ.ศ. 2457 เพื่อป้องกันการแข่งขันทางธุรกิจ การหลอกลวง หรือไม่เป็นธรรม FTC ถูกกำหนดให้มีการกิจสองประการคือ: (1) ปกป้องผู้บริโภค; และ (2) ส่งเสริมการแข่งขัน ความเชื่อชาญและทรัพยากรของหน่วยงานมีให้สำหรับสถานีวิทยุของรัฐบาลกลางและของรัฐ ตลอดจนหน่วยงานรัฐบาลอื่น ๆ ของสหรัฐอเมริกา FTC บังคับใช้กฎหมายคุ้มครองผู้บริโภคและต่อต้านการผูกขาด และยังทำงานเพื่อพัฒนาผลประโยชน์ของผู้บริโภคและจัดทำโปรแกรมการศึกษา.

³¹ Education Foundation consumer federation.

ทำให้คำนิยามของเด็กได้ถูกบัญญัติไว้ใน Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 ในข้อที่ §6501 ดังนี้

คำจำกัดความในบทนี้:

(1) เด็ก

คำว่า “เด็ก” หมายถึงบุคคลที่มีอายุต่ำกว่า 13 ปี

COPPA ได้มีการกำหนดคำนิยามขึ้นมาชัดเจนและมุ่งใช้กับผู้ให้บริการเว็บไซต์และบริการออนไลน์มุ่งเป้าไปที่เด็กที่มีอายุต่ำกว่า 13 ปี เพื่อเป็นการให้ความคุ้มครองข้อมูลส่วนบุคคลของเด็กโดยตรง

3.2.1.2 หน้าที่ของผู้ให้บริการและเว็บไซต์ทางออนไลน์³² (Operator)³³ ตามบทบัญญัติของ COPPA และความยินยอม

สำหรับ Children's Online Privacy Protection Act (COPPA) ตั้งแต่มีการแก้ไข COPPA กฎระเบียบบางอย่างก็มีการเปลี่ยนแปลง ทำให้เว็บไซต์หรือผู้ให้บริการมีข้อบังคับที่ต้องปฏิบัติตามเพื่อให้สอดคล้องกับ COPPA ดังนี้

1) โปสเตอร์นโยบายความเป็นส่วนตัวออนไลน์ที่ชัดเจนและครอบคลุมซึ่งอธิบายแนวทางปฏิบัติด้านข้อมูลสำหรับข้อมูลส่วนบุคคลที่รวบรวมทางออนไลน์จากเด็ก

2) แจ้งผู้ปกครองโดยตรงและขอความยินยอมจากผู้ปกครองที่ตรวจสอบได้ โดยมีข้อยกเว้นอย่างจำกัด ก่อนรวบรวมข้อมูลส่วนบุคคลทางออนไลน์จากเด็ก

³² เว็บไซต์หรือบริการออนไลน์ที่มุ่งเป้าไปที่เด็ก หมายถึงเว็บไซต์เชิงพาณิชย์หรือบริการออนไลน์ หรือส่วนหนึ่งของเว็บไซต์ที่มุ่งเป้าไปที่เด็ก.

³³ ผู้ดำเนินการ หมายถึง บุคคลใด ๆ ที่ดำเนินการเว็บไซต์ที่อยู่บนอินเทอร์เน็ตหรือบริการออนไลน์ และรวบรวมหรือรักษาข้อมูลส่วนบุคคลจากหรือเกี่ยวกับผู้ใช้หรือผู้เยี่ยมชมเว็บไซต์หรือบริการออนไลน์ดังกล่าว หรือผู้ที่ข้อมูลดังกล่าวถูกรวบรวมหรือบำรุงรักษาในนามของ หรือเสนอผลิตภัณฑ์หรือบริการเพื่อขายผ่านเว็บไซต์หรือบริการออนไลน์นั้น โดยที่เว็บไซต์หรือบริการออนไลน์ดังกล่าวดำเนินการเพื่อวัตถุประสงค์ทางการค้าที่เกี่ยวข้องกับการค้าระหว่างหลายรัฐหรือกับ 1 ประเทศขึ้นไป ในดินแดนใด ๆ ของสหรัฐอเมริกาหรือในเขตโคลัมเบียหรือระหว่างอาณาเขตดังกล่าวกับอาณาเขตอื่น ๆ หรือรัฐหรือประเทศอื่น ๆ หรือระหว่าง District of Columbia และรัฐดินแดน หรือประเทศอื่น ๆ คำจำกัดความนี้ไม่รวมถึงองค์กรที่ไม่แสวงหาผลกำไรใด ๆ ที่ได้รับการยกเว้นจากความคุ้มครองภายใต้มาตรา 5 ของ Federal Trade Commission Act (15 U.S.C. 45) ข้อมูลส่วนบุคคลจะถูกรวบรวมหรือรักษาไว้ในนามของผู้ประกอบการเมื่อ:

(1) รวบรวมหรือบำรุงรักษาโดยตัวแทนหรือผู้ให้บริการของผู้ประกอบการ หรือ

(2) ผู้ประกอบการได้รับประโยชน์โดยการอนุญาตให้บุคคลอื่นเก็บข้อมูลส่วนบุคคลโดยตรงจากผู้ใช้เว็บไซต์หรือบริการออนไลน์ดังกล่าว.

3) ให้ทางเลือกแก่ผู้ปกครองในการยินยอมให้ผู้ดำเนินการเก็บรวบรวมและใช้งาน ข้อมูลของเด็กภายใน แต่ห้ามไม่ให้ผู้ดำเนินการเปิดเผยข้อมูลนั้นแก่บุคคลที่สาม (เว้นแต่การเปิดเผย จะเป็นส่วนหนึ่งของเว็บไซต์หรือบริการ ในกรณีนี้ จะต้องชี้แจงให้ชัดเจน ผู้ปกครอง)

4) ให้ผู้ปกครองเข้าถึงข้อมูลส่วนบุคคลของบุตรหลานเพื่อตรวจสอบและ/หรือ ลบข้อมูล

5) ให้โอกาสผู้ปกครองในการป้องกันการใช้ต่อไปหรือการรวบรวมข้อมูลส่วนบุคคล ของเด็กทางออนไลน์

6) รักษาความลับ ความปลอดภัย และความสมบูรณ์ของข้อมูลที่รวบรวมจากเด็ก รวมถึงการทำตามขั้นตอนที่เหมาะสมเพื่อเปิดเผยข้อมูลดังกล่าวเฉพาะกับฝ่ายที่สามารถรักษา ความลับและความปลอดภัย และ

7) เก็บรักษาข้อมูลส่วนบุคคลที่เก็บรวบรวมทางออนไลน์จากเด็กไว้นานเท่าที่จำเป็น เพื่อให้บรรลุวัตถุประสงค์ในการเก็บรวบรวมและลบข้อมูล โดยใช้มาตรการที่เหมาะสมเพื่อป้องกันการเข้าถึงหรือการใช้โดยไม่ได้รับอนุญาต³⁴

กฎหมายคุ้มครองข้อมูลส่วนบุคคลออนไลน์ของเด็ก Children's Online Privacy Protection Act (COPPA) ได้ให้สิทธิเต็มที่แก่พ่อแม่ หรือผู้ปกครองเด็ก ในการควบคุมข้อมูลของ เด็กที่ผู้ให้บริการเก็บรวบรวมประมวลผลและการเปิดเผยข้อมูลส่วนบุคคลของเด็กผ่านการออนไลน์

ความยินยอมของผู้ปกครองที่ตรวจสอบได้คือความยินยอมจากพ่อแม่หรือผู้ปกครอง ซึ่งยืนยันตัวตนของพ่อแม่หรือผู้ปกครองได้อย่างสมเหตุสมผล ภายใต้ COPPA คุณต้องได้รับความยินยอมนี้ก่อนที่จะรวบรวมข้อมูลจากเด็ก

วิธีการที่ยอมรับได้ในการขอความยินยอมจากผู้ปกครองและรับรองความถูกต้อง ของตัวตน

- 1) แบบฟอร์มยินยอมที่ลงนามแล้ว
- 2) การใช้บัตรเครดิตหรือบัตรเดบิต (ในขณะที่ทำธุรกรรมทางการเงิน)
- 3) โทรศัพท์
- 4) การประชุมทางวิดีโอทางโทรศัพท์
- 5) ทำหายคำถามที่อาจจะยากสำหรับคนอื่นที่ไม่ใช่ผู้ปกครองที่จะตอบให้ถูกต้อง
- 6) บัตรประจำตัวที่มีรูปถ่าย

³⁴ Children's Online Privacy Protection Act (COPPA). §312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

หากข้อมูลที่ถูกรวบรวมมีไว้เพื่อใช้ภายในธุรกิจของคุณเท่านั้น คุณอาจใช้วิธี “Email Plus” เพื่อรวบรวมความยินยอมจากผู้ปกครอง เพียงส่งอีเมลถึงผู้ปกครองเพื่อขอให้ตอบกลับด้วยความยินยอม จากนั้นยืนยันว่าคุณได้รับแล้ว

กฎหมายฉบับนี้ได้ตราขึ้นเพื่อแก้ไขปัญหาคำถามเป็นส่วนตัวของเด็กในโลกออนไลน์ เพื่อให้ทันกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็วซึ่งนำไปใช้กับผู้ประกอบการเชิงพาณิชย์ที่เก็บรวบรวมประมวลผลหรือเปิดเผยข้อมูลส่วนตัวของเด็กที่มีอายุต่ำกว่า 13 ปี โดยจะต้องได้รับการตรวจสอบหรือยินยอมจากผู้ปกครองก่อนในการจัดเก็บรวบรวมประมวลผลหรือเปิดเผยข้อมูลของเด็ก โดยอาจมีการกำหนดให้ผู้ดำเนินการเว็บไซต์เชิงพาณิชย์และบริการออนไลน์มีหน้าที่จะต้องทำการปิดประกาศนโยบายในการขอข้อมูลส่วนบุคคล บนเว็บไซต์อย่างชัดเจน หากเว็บไซต์มีการขอข้อมูลจากเด็กจะต้องมีการแจ้ง การขออนุญาตพ่อแม่หรือผู้ปกครองของเด็ก ก่อนที่จะมีการจัดเก็บประมวลผลหรือเปิดเผยข้อมูลของเด็ก และพ่อแม่หรือผู้ปกครองมีสิทธิเข้าไปทำการตรวจสอบ แก้ไข หรือลบข้อมูลเด็กที่มีการจัดเก็บประมวลผลได้ตลอดเวลา และมีสิทธิในการดำเนินการป้องกันกรณีมีการขอข้อมูลเพิ่มเติม การนำไปใช้หรือการนำเปิดเผย และผู้ประกอบการไม่มีสิทธิที่จะนำข้อมูลที่เก็บรวบรวมไปเปิดเผยต่อบุคคลที่สาม แต่มีหน้าที่ดูแลรักษาข้อมูลให้ถูกต้อง ปลอดภัย และเป็นความลับอยู่เสมอ³⁵

Children’s Online Privacy Protection Act (COPPA) มีผลบังคับใช้ ได้แก่ เว็บไซต์ในเชิงพาณิชย์ที่มีความเกี่ยวข้องกับเด็ก อาจมีการพิจารณาจาก ภาษา เนื้อหาสาระ การโฆษณา บนเว็บไซต์ที่เกี่ยวข้องกับเด็ก อายุของเด็กเฉลี่ยที่เข้าไปดูหรือใช้บริการเว็บไซต์ เป็นต้น โดยคณะกรรมการค้าแห่งสหพันธรัฐ Federal Trade Commission (FTC) เป็นผู้รับผิดชอบดูแลให้เป็นไปตามกฎหมายดังกล่าว แต่เนื่องจากกฎหมายไม่ได้กล่าวถึงรายละเอียดการปฏิบัติ เพื่อให้เป็นไปตามกฎหมาย คณะกรรมการค้าแห่งสหพันธรัฐจึงได้มีการระเบียบปฏิบัติในเรื่องนี้ เพื่อให้ผู้ประกอบการถือปฏิบัติตามและ โดยเฉพาะอย่างยิ่งอนุสัญญาว่าด้วยสิทธิเด็ก (Convention on the Right of the Child) ซึ่งเป็นข้อตกลงร่วมกันระหว่างประเทศ ที่มีประเทศเข้าตกลงเข้าร่วมมากถึง 196 ประเทศทั่วโลก ยกเว้นเพียงสหรัฐอเมริกาที่ยังไม่ได้เข้าเป็นภาคี ดังนั้นสหรัฐอเมริกาจึงไม่มีความจำเป็นต้องกำหนดเกณฑ์อายุเด็กที่อายุ 18 ปีตามอนุสัญญาว่าด้วยสิทธิเด็กแต่อย่างใด³⁶

³⁵ พนิดา พูลสวัสดิ์. อังแล้ว เจริญรอดที่ 7. หน้า 38-39.

³⁶ สุชาวสา ถมรงค์ยศศักดิ์. (2562). การคุ้มครองข้อมูลส่วนบุคคลของเด็กบนสื่ออิเล็กทรอนิกส์. *วารสารเกษมบัณฑิต*, 20 (1), หน้า 139-140.

3.2.1.3 บทลงโทษกรณีฝ่าฝืนบทบัญญัติของ COPPA

The Federal Trade Commission (FTC)³⁷ ใช้วิธีการต่าง ๆ ในการบังคับใช้ COPPA และกำหนดบทลงโทษที่สูงสำหรับบริษัทที่ไม่ปฏิบัติตามในการค้นหาผู้ฝ่าฝืน FTC สนับสนุนให้ผู้ใช้อินเทอร์เน็ตยื่นคำร้องเรียนสำหรับเว็บไซต์ที่พวกเขาคิดว่าละเมิดหลักเกณฑ์

รัฐและหน่วยงานของรัฐบาลกลางอื่น ๆ ก็มีเขตอำนาจในการบังคับใช้กฎหมายเช่นกัน ตัวอย่างเช่น ในกรณีปี 2016 อัยการสูงสุดของนิวยอร์กพบว่า Viacom, Mattel, JumpStart และ Hasbro ล้วนละเมิด COPPA เนื่องจากพาร์ทเนอร์โฆษณาที่พวกเขาทำงานร่วมกับลูกค้าที่ใช้เพื่อติดตามข้อมูลส่วนบุคคลของผู้ใช้

ในอดีตโทษสูงสุดต่อการละเมิดหนึ่งครั้งคือ 16,000 ดอลลาร์ อย่างไรก็ตาม ในปี 2559 บทลงโทษสูงสุดได้เพิ่มขึ้นเป็น 40,654 ดอลลาร์ต่อการละเมิดหนึ่งครั้ง

ดังนั้น หากทำการรวบรวมข้อมูลส่วนบุคคลจากเด็กเพียง 10 คน แต่ไม่ปฏิบัติตาม COPPA คุณจะถูกปรับสูงสุด 4,065,400 ดอลลาร์ โดยทั่วไปจำนวนเงินที่ธุรกิจจะถูกลงโทษขึ้นอยู่กับว่าการละเมิดนั้นชัดเจนเพียงใด และบริษัทได้รับจากข้อมูลส่วนบุคคลมากน้อยเพียงใด³⁸

จะเห็นได้ว่าสหรัฐอเมริกาได้ให้ความสำคัญในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลของเด็กประกอบกับกฎหมายข้อมูลส่วนบุคคลของสหรัฐอเมริกามีลักษณะเข้มงวด ดังนั้นในการให้คุ้มครองสิทธิของเด็กกรณีข้อมูลส่วนบุคคลของเด็กบนอินเทอร์เน็ตจึงมีกฎหมายที่ใช้บังคับเป็นการเฉพาะโดยตรง มีความชัดเจน ครอบคลุมและสามารถบังคับใช้ได้โดยตรงจุดและมีประสิทธิภาพเพื่อไม่ให้เกิดปัญหาต่าง ๆ ตามมาภายหลัง นอกจากนี้ประเทศสหรัฐอเมริกาก็ได้มีการกำหนดโทษปรับไว้สูงสำหรับกรณีที่มีผู้ฝ่าฝืนเป็นกรณี เช่น กรณีที่คณะกรรมการหลักที่บริหารควบคุมกิจกรรมต่าง ๆ ในพาณิชย์อิเล็กทรอนิกส์ หรือ FTC (Federal Trade Commission) ของสหรัฐอเมริกาได้ทำการสืบสวน YouTube เพื่อเตรียมการฟ้องร้องเกี่ยวกับประเด็นที่ YouTube มีการละเมิดความเป็นส่วนตัวส่วนตัวเด็กอายุต่ำกว่า 13 ปี โดยในการสืบสวนพบว่า YouTube ไม่มีความสามารถในการปกป้องสิทธิความเป็นส่วนตัวส่วนตัวเด็ก ซึ่งขัดต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคลทางอินเทอร์เน็ตของเด็ก COPPA (Children's Online Privacy Protection Act) ที่ห้ามเก็บข้อมูลเด็กหรือใช้เด็กเป็นกลุ่มเป้าหมายในการทำโฆษณา ในการฟ้องร้องดังกล่าวได้มีการเรียกค่าปรับแก่ Youtube รวมถึงบังคับให้ YouTube เปลี่ยนกฎและนโยบายเพื่อยกระดับคุ้มครองข้อมูลเด็กให้รัดกุม

³⁷ คณะกรรมการการการค้าแห่งสหพันธรัฐ (FTC) เป็นหน่วยงานอิสระของรัฐบาลสหรัฐฯ ที่ได้รับมอบหมายให้ปกป้องผู้บริโภคและสร้างความมั่นใจให้กับตลาดที่มีการแข่งขันสูง.

³⁸ KJ Dearie. (2019). *COPPA: Children's Online Privacy Protection Act Compliance Guide*. (Online). Available: <https://termly.io/resources/articles/coppa/#how-to-comply-with-coppa-law>. [2021, August 14].

กว่าเดิม นอกจากนี้ FTC ยังเผยอีกว่า ไม่ใช่เพียงแค่ Youtube เท่านั้นที่ถูกฟ้องร้องในเรื่องนี้ เพราะเมื่อปี 2014 ก็เคยฟ้องร้อง เรียกค่าปรับ 5.7 พันล้านดอลลาร์ จาก TikTok ฐานละเมิดความเป็นส่วนตัวของเด็ก³⁹ เป็นต้น

3.2.2 สหภาพยุโรป

General Data Protection Regulation (GDPR) ของสหภาพยุโรป เป็นกฎหมายที่คุ้มครองข้อมูลส่วนบุคคลของพลเมืองที่อาศัยอยู่ในเขตสหภาพยุโรป เพื่อตอบรับกระแสของการใช้อินเทอร์เน็ต ธุรกิจ E-commerce การโฆษณาและการตลาดออนไลน์ในโลกยุคดิจิทัล GDPR ได้รวบรวมกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลของผู้บริโภคหลายฉบับไว้ด้วยกัน แต่เพิ่มบทลงโทษที่รุนแรงขึ้นกว่าเดิม เช่น การเสียค่าปรับที่มีจำนวนเงินสูงถึง 20 ล้านยูโร ที่สำคัญคือ GDPR ทำให้ประเทศสมาชิกใช้กฎหมายการคุ้มครองข้อมูลส่วนบุคคลฉบับเดียวกัน ซึ่งช่วยให้ง่ายต่อการดำเนินธุรกิจระหว่างกลุ่มประเทศสมาชิกอีกด้วย⁴⁰

General Data Protection Regulation (GDPR) ถือเป็นหลักการคุ้มครองข้อมูลส่วนบุคคลที่สหภาพยุโรปได้ทำการลงมติเห็นชอบผ่านกฎหมายไปเมื่อปี 2016 และจะมีผลบังคับใช้ 25 พฤษภาคม 2018 (พ.ศ. 2561) และมีการบังคับใช้แทนกฎหมายฉบับปัจจุบัน คือ EU Data Protection Directive ที่บังคับใช้โดยหน่วยงานที่กำกับดูแลของแต่ละประเทศสมาชิกตั้งแต่ปี พ.ศ. 2538

โดยมีวัตถุประสงค์หลักเพื่อให้ประชาชนมีสิทธิในการควบคุมข้อมูลส่วนบุคคลของตนเอง ถือเป็นสิทธิขั้นพื้นฐาน สหภาพยุโรปมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เป็นอันหนึ่งอันเดียวเพื่อให้เกิดการเคลื่อนย้ายข้อมูลได้อย่างเสรีและโดยทั่วไปคือให้ประชาชนสามารถเข้าถึงข้อมูลส่วนบุคคลของตนเองได้และไม่มีค่าใช้จ่าย (Free and Easy Access) ต้องมีการแจ้งให้ทราบถึงวัตถุประสงค์และความโปร่งใสในการรวบรวมข้อมูลส่วนบุคคล เมื่อมีการนำข้อมูลไปทำการประมวลผลก็จะต้องมีการได้รับความยินยอมชัดเจนจากเจ้าของข้อมูล และการใช้ข้อมูลเหล่านั้นจะต้องเป็นไปตามวัตถุประสงค์เท่านั้น

ให้สิทธิประชาชนในการเข้าถึงข้อมูลส่วนบุคคลตนเองจากผู้ประกอบการเพื่อโอนข้อมูลเหล่านั้นไปยังผู้ประกอบการอื่นได้ ทั้งยังให้สิทธิเจ้าของข้อมูลส่วนบุคคลเรียกร้องให้มีการลบ

³⁹ Tony Romm, Elizabeth Dwoskin and Craig Timberg. (2019). *YouTube under federal investigation over allegations it violates children's privacy*. (Online). Available: <https://www.washingtonpost.com/technology/2019/06/19/facing-federal-investigation-youtube-is-considering-broad-changes-childrens-content/>. [2021, August 14].

⁴⁰ McAfee. (2018). *The GDPR Basics: What Consumers Need to Know*. (Online). Available: <https://www.mcafee.com/blogs/consumer/consumer-threat-reports/gdpr-basics/>. [2021, August 14].

ข้อมูลของคนออกจากระบบได้ในกรณีที่ตนมีความประสงค์จะลบข้อมูลส่วนบุคคลของคนออกจากระบบเมื่อไม่มีความจำเป็นที่ผู้ประกอบการนั้นจะต้องเก็บข้อมูลเหล่านั้นไว้⁴¹

3.2.2.1 ความหมายของคำนิยามของข้อมูลส่วนบุคคลของเด็กตามบทบัญญัติของ GDPR

คำจำกัดความของ “ข้อมูลส่วนบุคคล” หมายถึงข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุหรือระบุตัวตนได้ (เจ้าของข้อมูล) บุคคลธรรมดาที่สามารถระบุตัวตนได้คือบุคคลที่สามารถระบุได้โดยตรงหรือโดยอ้อม โดยเฉพาะอย่างยิ่งโดยการอ้างอิงถึงตัวระบุ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลตำแหน่ง ตัวระบุออนไลน์ หรือปัจจัยหนึ่งหรือหลายปัจจัยเฉพาะทางกายภาพ สรีรวิทยา อัตลักษณ์ทางพันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคลธรรมดานั้น

จะเห็นได้ว่า GDPR ไม่มีการกำหนดคำนิยามไว้เป็นการเฉพาะแต่อย่างใด แต่มีการกำหนดเงื่อนไขที่ใช้กับความยินยอมของเด็กที่เกี่ยวข้องกับบริการสังคมข้อมูล ไว้ในอนุมาตรา 1 ให้ผู้เยาว์ในที่นี้หมายถึงเด็กที่มีอายุต่ำกว่า 16 ปี (GDPR) หรือต่ำกว่า 13 ปี (รัฐสมาชิก EU) และกล่าวถึงในกรณีที่เด็กควรที่จะได้รับการคุ้มครองเฉพาะในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เนื่องจากเด็กอาจไม่ค่อยตระหนักถึงความเสี่ยง ผลที่ตามมา และการป้องกันที่เกี่ยวข้อง และสิทธิ์ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่ง การป้องกันดังกล่าวควรนำไปใช้กับการใช้ข้อมูลส่วนบุคคลของเด็กเพื่อวัตถุประสงค์ทางการตลาดหรือการสร้างบุคลิกภาพหรือโปรไฟล์ผู้ใช้ และการรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเด็กเมื่อใช้บริการที่เสนอให้กับเด็กโดยตรง ความยินยอมจากผู้รับผิดชอบของผู้ปกครองไม่ควรมีความจำเป็นในบริบทของบริการป้องกันหรือให้คำปรึกษาที่เสนอให้เด็กโดยตรง⁴²

3.2.2.2 หน้าที่ของผู้ควบคุม (Controller) และผู้ประมวลผล (Processor) ตามบทบัญญัติของ GDPR และความยินยอม

1) หน้าที่ของผู้ควบคุม (Controller)

ผู้ควบคุมต้องใช้มาตรการที่เหมาะสมเพื่อให้ข้อมูลใด ๆ ที่อ้างอิงที่เกี่ยวข้องกับการประมวลผลกับเจ้าของข้อมูลในรูปแบบที่กระชับ โปร่งใส เข้าใจได้ และเข้าถึงได้ง่าย โดยใช้ข้อความที่ชัดเจนและชัดเจน ภาษา โดยเฉพาะอย่างยิ่งสำหรับข้อมูลใด ๆ ที่ส่งถึงเด็ก โดยเฉพาะข้อมูลจะต้องจัดทำเป็นลายลักษณ์อักษรหรือโดยวิธีการอื่นรวมถึงตามความเหมาะสมโดยวิธีการทางอิเล็กทรอนิกส์ เมื่อได้รับการร้องขอจากเจ้าของข้อมูล ข้อมูลอาจถูกจัดให้ด้วยวาจา โดยมีเงื่อนไขว่าตัวตนของเจ้าของข้อมูลนั้นได้รับการพิสูจน์ด้วยวิธีการอื่น

⁴¹ สุวสา ธมรงค์ศักดิ์. อ่างแล้ว เจริญรอดที่ 36. หน้า 140-141.

⁴² General Data Protection Regulation (GDPR). Recital 38.

ผู้ควบคุมต้องอำนวยความสะดวกในการใช้สิทธิของเจ้าของข้อมูล ผู้ควบคุมจะต้องไม่ปฏิเสธที่จะดำเนินการตามคำขอของเจ้าของข้อมูลเพื่อใช้สิทธิของตน เว้นแต่ผู้ควบคุมจะแสดงให้เห็นว่าไม่อยู่ในฐานะที่จะระบุเจ้าของข้อมูลได้

ผู้ควบคุมต้องให้ข้อมูลที่เกี่ยวข้องกับการดำเนินการต่าง ๆ แก่เจ้าของข้อมูลโดยไม่ชักช้า และไม่ว่าในกรณีใด ๆ ภายในหนึ่งเดือนหลังจากได้รับคำขอ ระยะเวลาดังกล่าวอาจขยายออกไปอีกสองเดือนหากจำเป็น โดยคำนึงถึงความซับซ้อนและจำนวนคำขอ ผู้ควบคุมต้องแจ้งให้เจ้าของข้อมูลทราบถึงการขยายเวลาดังกล่าวภายในหนึ่งเดือนหลังจากได้รับคำขอ พร้อมเหตุผลของความล่าช้า ในกรณีที่เจ้าของข้อมูลส่งคำขอโดยใช้แบบฟอร์มอิเล็กทรอนิกส์ ข้อมูลจะต้องจัดเตรียมโดยวิธีการทางอิเล็กทรอนิกส์หากเป็นไปได้ เว้นแต่เจ้าของข้อมูลจะร้องขอเป็นอย่างอื่น

หากผู้ควบคุมไม่ดำเนินการตามคำขอของเจ้าของข้อมูล ผู้ควบคุมต้องแจ้งให้เจ้าของข้อมูลทราบโดยไม่ชักช้าและอย่างช้าที่สุดภายในหนึ่งเดือนหลังจากได้รับคำขอถึงเหตุผลที่ไม่ดำเนินการและความเป็นไปได้ในการยื่นคำร้อง ร้องทุกข์กับหน่วยงานกำกับดูแลและขอวิธีแก้ไขทางศาล

ข้อมูลที่ให้ไว้ในข้อ 13⁴³ และ 14⁴⁴ และการสื่อสารและการดำเนินการใด ๆ ที่ดำเนินการจะให้บริการฟรี ในกรณีที่คำขอจากเจ้าของข้อมูลไม่มีมูลความจริงอย่างชัดเจนหรือมากเกินไป โดยเฉพาะอย่างยิ่งเนื่องจากลักษณะซ้ำซาก ผู้ควบคุม อาจ

(a) เรียกเก็บค่าธรรมเนียมที่เหมาะสมโดยคำนึงถึงค่าใช้จ่ายในการดำเนินการในการให้ข้อมูลหรือการสื่อสารหรือดำเนินการตามที่ร้องขอ หรือ

(b) ปฏิเสธที่จะดำเนินการตามคำขอ

ผู้ควบคุมต้องแบกรับภาระในการแสดงคำขอที่ไม่มีมูลหรือเกินความจำเป็นอย่างชัดเจน

โดยปราศจากอคติต่อมาตรา 11⁴⁵ ซึ่งผู้ควบคุมมีข้อสงสัยตามสมควรเกี่ยวกับตัวตนของบุคคลธรรมดาที่ส่งคำขอที่อ้างถึงในมาตรา 15⁴⁶ ถึง 21⁴⁷ ผู้ควบคุมอาจร้องขอการจัดหาข้อมูลเพิ่มเติมที่จำเป็นเพื่อยืนยันตัวตนของเจ้าของข้อมูล

⁴³ General Data Protection Regulation (GDPR). Recital 13.

⁴⁴ General Data Protection Regulation (GDPR). Recital 14.

⁴⁵ General Data Protection Regulation (GDPR). Recital 11.

⁴⁶ General Data Protection Regulation (GDPR). Recital 15.

⁴⁷ General Data Protection Regulation (GDPR). Recital 21.

ข้อมูลที่จะให้แก่เจ้าของข้อมูลตามมาตรา 13 และ 14 อาจใช้ร่วมกับไอคอนมาตรฐาน เพื่อให้มองเห็นภาพรวมที่มีความหมายของการประมวลผลที่ตั้งใจไว้ในลักษณะที่มองเห็นได้ง่าย เข้าใจได้ และอ่านได้ชัดเจน ในกรณีที่ไอคอนถูกนำเสนอทางอิเล็กทรอนิกส์จะต้องสามารถอ่านได้ด้วยเครื่อง

คณะกรรมการมีอำนาจดำเนินการที่ได้รับมอบหมายตามมาตรา 92⁴⁸ เพื่อวัตถุประสงค์ในการกำหนดข้อมูลที่จะนำเสนอโดยไอคอนและขั้นตอนในการจัดเตรียมไอคอนที่ได้มาตรฐาน⁴⁹

2) หน้าที่ของผู้ประมวลผล (Processor)

ในกรณีที่มีการดำเนินการในนามของผู้ควบคุม ผู้ควบคุมจะต้องใช้เฉพาะผู้ประมวลผลที่ให้การรับประกันที่เพียงพอเพื่อใช้มาตรการทางเทคนิคและองค์กรที่เหมาะสมในลักษณะที่การประมวลผลจะเป็นไปตามข้อกำหนดของระเบียบนี้และรับรองการคุ้มครองสิทธิของหัวเรื่องของข้อมูล

จะต้องไม่มีส่วนร่วมกับผู้ประมวลผลอื่น โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรเป็นการเฉพาะหรือทั่วไปของผู้ควบคุม ในกรณีของการอนุญาตเป็นลายลักษณ์อักษรทั่วไป ผู้ประมวลผลจะต้องแจ้งให้ผู้ควบคุมทราบถึงการเปลี่ยนแปลงที่ตั้งใจไว้เกี่ยวกับการเพิ่มหรือเปลี่ยนผู้ประมวลผลอื่น ซึ่งจะทำให้ผู้ควบคุมมีโอกาสคัดค้านการเปลี่ยนแปลงดังกล่าว

การประมวลผลโดยผู้ประมวลผลจะอยู่ภายใต้สัญญาหรือการกระทำทางกฎหมายอื่น ๆ ภายใต้กฎหมายของสหภาพหรือรัฐสมาชิกซึ่งมีผลผูกพันกับผู้ประมวลผลโดยคำนึงถึงผู้ควบคุม และกำหนดเรื่องและระยะเวลาของการประมวลผล ลักษณะและวัตถุประสงค์ ของการประมวลผล ประเภทของข้อมูลส่วนบุคคลและประเภทของเจ้าของข้อมูล และภาระหน้าที่และสิทธิของผู้ควบคุม สัญญานั้นหรือการดำเนินการทางกฎหมายอื่น ๆ จะต้องกำหนดโดยเฉพาะอย่างยิ่งว่าผู้ประมวลผล

(a) ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่เป็นเอกสารจากผู้ควบคุมเท่านั้น ซึ่งรวมถึงการถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์กรระหว่างประเทศ เว้นแต่จำเป็นต้องทำโดยสหภาพหรือกฎหมายของรัฐสมาชิกที่ผู้ประมวลผลอยู่ภายใต้บังคับ; ในกรณีดังกล่าว ผู้ประมวลผลจะต้องแจ้งให้ผู้ควบคุมทราบถึงข้อกำหนดทางกฎหมายนั้นก่อนดำเนินการ เว้นแต่กฎหมายดังกล่าวจะห้ามข้อมูลดังกล่าวโดยมีเหตุผลสำคัญที่เป็นสาธารณประโยชน์

(b) ตรวจสอบให้แน่ใจว่าบุคคลที่ได้รับอนุญาตให้ประมวลผลข้อมูลส่วนบุคคลได้ให้คำมั่นว่าจะรักษาความลับหรืออยู่ภายใต้ภาระผูกพันตามกฎหมายที่เหมาะสมในการรักษาความลับ

⁴⁸ General Data Protection Regulation (GDPR). Recital 92.

⁴⁹ General Data Protection Regulation (GDPR). Recital 12.

(c) ใช้มาตรการทั้งหมดที่จำเป็นตามมาตรา 32⁵⁰

(d) เคารพเงื่อนไขที่อ้างถึงในวรรคสอง และ วรรคสี่ สำหรับการมีส่วนร่วมของผู้ประมวลผลรายอื่น

(e) โดยคำนึงถึงธรรมชาติของการประมวลผล ช่วยเหลือผู้ควบคุมด้วยมาตรการทางเทคนิคและองค์กรที่เหมาะสม ครอบคลุมที่เป็นไปได้ เพื่อให้เป็นไปตามภาระหน้าที่ของผู้ควบคุมในการตอบสนองต่อคำขอใช้สิทธิ์ของเจ้าของข้อมูลที่กำหนดไว้ในบทที่ 3

(f) ช่วยผู้ควบคุมในการตรวจสอบการปฏิบัติตามภาระผูกพันตามมาตรา 32 ถึง มาตรา 36⁵¹ โดยคำนึงถึงลักษณะของการประมวลผลและข้อมูลที่มีให้สำหรับผู้ประมวลผล

(g) เมื่อเลือกผู้ควบคุม ลบหรือส่งคืนข้อมูลส่วนบุคคลทั้งหมดไปยังผู้ควบคุมหลังจากสิ้นสุดการให้บริการที่เกี่ยวข้องกับการประมวลผล และลบสำเนาที่มีอยู่ เว้นแต่กฎหมายของสหภาพหรือรัฐสมาชิกกำหนดให้มีการจัดเก็บข้อมูลส่วนบุคคล

(h) ทำให้ผู้ควบคุมมีข้อมูลทั้งหมดที่จำเป็นในการแสดงการปฏิบัติตามพันธกรณีที่กำหนดไว้ในบทความนี้ และอนุญาตและมีส่วนสนับสนุนในการตรวจสอบ ซึ่งรวมถึงการตรวจสอบที่ดำเนินการโดยผู้ควบคุมหรือผู้ตรวจสอบรายอื่นที่ได้รับคำสั่งจากผู้ควบคุม

ในส่วนที่เกี่ยวข้องกับข้อ (h) ของอนุวรรคแรก ผู้ประมวลผลจะต้องแจ้งให้ผู้ควบคุมทราบทันที หากเห็นว่าคำสั่งละเมิดระเบียบนี้หรือข้อกำหนดการคุ้มครองข้อมูลอื่นของสหภาพหรือรัฐสมาชิก

ในกรณีที่ผู้ประมวลผลมีส่วนร่วมกับผู้ประมวลผลรายอื่นเพื่อดำเนินกิจกรรมการประมวลผลเฉพาะในนามของผู้ควบคุม ภาระผูกพันในการปกป้องข้อมูลเดียวกันกับที่กำหนดไว้ในสัญญาหรือการดำเนินการทางกฎหมายอื่น ๆ ระหว่างผู้ควบคุมและผู้ประมวลผลตามที่อ้างถึงในวรรค 3 จะถูกกำหนด ผู้ประมวลผลอื่นตามสัญญาหรือการดำเนินการทางกฎหมายอื่น ๆ ภายใต้กฎหมายของสหภาพหรือรัฐสมาชิก โดยเฉพาะอย่างยิ่งการให้การรับประกันที่เพียงพอเพื่อใช้มาตรการทางเทคนิคและองค์กรที่เหมาะสมในลักษณะที่การประมวลผลจะเป็นไปตามข้อกำหนดของระเบียบนี้ ในกรณีที่ผู้ประมวลผลรายอื่นไม่สามารถปฏิบัติตามภาระผูกพันในการปกป้องข้อมูลได้ ผู้ประมวลผลเริ่มต้นจะยังคงมีความรับผิดชอบเพิ่มเติมที่ต่อผู้ควบคุมสำหรับประสิทธิภาพของภาระผูกพันของผู้ประมวลผลอื่นนั้น

⁵⁰ General Data Protection Regulation (GDPR). Recital 32.

⁵¹ General Data Protection Regulation (GDPR). Recital 36.

การขีตมันของผู้ประมวลผลตามหลักจรรยาบรรณที่ได้รับอนุมัติตามที่อ้างถึงใน มาตรา 40 หรือกลไกการรับรองที่ได้รับอนุมัติตามที่อ้างถึงในมาตรา 42⁵² อาจใช้เป็นองค์ประกอบ ในการแสดงการรับประกันที่เพียงพอตามที่อ้างถึงในวรรคหนึ่ง และ วรรคดี ของข้อนี้

โดยปราศจากอคติต่อสัญญาส่วนบุคคลระหว่างผู้ควบคุมและผู้ประมวลผล สัญญา หรือการดำเนินการทางกฎหมายอื่น ๆ ที่อ้างถึงในวรรคสาม และ วรรคดี ของบทความนี้อาจอิงตาม ข้อสัญญามาตรฐานที่อ้างถึงในวรรคเจ็ด และบางส่วนทั้งหมดหรือบางส่วน 8 ของข้อนี้ รวมถึง เมื่อเป็นส่วนหนึ่งของการรับรองที่มอบให้แก่ผู้ควบคุมหรือผู้ประมวลผลตามมาตรา 42 และ มาตรา 43⁵³

คณะกรรมการอาจวางข้อสัญญามาตรฐานสำหรับเรื่องที่เกี่ยวข้องในวรรค 3 และ 4 ของข้อนี้และตามขั้นตอนการตรวจสอบที่อ้างถึงในมาตรา 93(2)⁵⁴

หน่วยงานกำกับดูแลอาจนำข้อสัญญามาตรฐานมาใช้กับเรื่องที่เกี่ยวข้องในวรรค 3 และ 4 ของข้อนี้ และตามกลไกความสอดคล้องที่อ้างถึงในมาตรา 63⁵⁵

สัญญาหรือนิติกรรมอื่น ๆ ที่อ้างถึงในวรรค 3 และ 4 ต้องทำเป็นลายลักษณ์อักษร รวมถึงในรูปแบบอิเล็กทรอนิกส์

โดยไม่กระทบต่อมาตรา 82⁵⁶, 83⁵⁷ และ 84⁵⁸ หากผู้ประมวลผลละเมิดระเบียบนี้ โดยการกำหนดวัตถุประสงค์และวิธีการในการประมวลผล ผู้ประมวลผลจะถือว่าเป็นผู้ควบคุม ในส่วนที่เกี่ยวข้องกับการประมวลผลนั้น⁵⁹

และนอกจากนี้ ในกฎระเบียบให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคของ สหภาพยุโรปยังกำหนดให้บริษัทนอกสหภาพยุโรปต้องปกป้องข้อมูลส่วนบุคคลอีกด้วย ราชการ ตรวจสอบการปฏิบัติตามข้อกำหนดของ GDPR ครอบคลุมเฉพาะสำหรับบริษัทในสหรัฐอเมริกา

GDPR เป็นกฎหมายความเป็นส่วนตัวของข้อมูลในสหภาพยุโรปที่กำหนดให้องค์กร ต้องรักษาข้อมูลให้ปลอดภัย ในขณะที่เดียวกันก็ให้ผู้ควบคุมวิธีการใช้งานข้อมูลของตนได้มากขึ้น กฎหมายยังรวมถึงการที่จะต้องเสียค่าปรับจำนวนมากสำหรับการไม่ปฏิบัติตาม ซึ่งสามารถเข้าถึง ร้อยละ 4 ของรายรับทั่วโลกหรือ 20 ล้านยูโร ขึ้นอยู่กับความรุนแรงและสถานการณ์ของการละเมิด

⁵² General Data Protection Regulation (GDPR). Recital 42.

⁵³ General Data Protection Regulation (GDPR). Recital 43.

⁵⁴ General Data Protection Regulation (GDPR). Recital 93.

⁵⁵ General Data Protection Regulation (GDPR). Recital 63.

⁵⁶ General Data Protection Regulation (GDPR). Recital 82.

⁵⁷ General Data Protection Regulation (GDPR). Recital 83.

⁵⁸ General Data Protection Regulation (GDPR). Recital 84.

⁵⁹ General Data Protection Regulation (GDPR). Recital 28.

มีกฎเกณฑ์ใหม่ที่เข้มงวดเกี่ยวกับสิ่งที่ถือว่าได้รับความยินยอมจากเจ้าของข้อมูลในการประมวลผลข้อมูลของตน

- (1) ความยินยอมจะต้อง “ให้โดยเสรี เฉพาะเจาะจง ไร้ทราบบ และไม่คลุมเครือ”
- (2) การขอความยินยอมต้อง “แยกแยะได้ชัดเจนจากเรื่องอื่น ๆ” และนำเสนอด้วย “ภาษาที่ชัดเจนและชัดเจน”
- (3) เจ้าของข้อมูลสามารถเพิกถอนความยินยอมก่อนหน้านั้นได้ทุกเมื่อที่ต้องการ และคุณต้องเคารพการตัดสินใจของพวกเขา คุณไม่สามารถเปลี่ยนพื้นฐานทางกฎหมายของการประมวลผลไปเป็นเหตุผลอื่นได้
- (4) เด็กอายุต่ำกว่า 13 ปีสามารถให้ความยินยอมได้ก็ต่อเมื่อได้รับอนุญาตจากผู้ปกครองเท่านั้น

(5) คุณต้องเก็บเอกสารหลักฐานแสดงความยินยอม⁶⁰

3) เงื่อนไขที่ใช้กับความยินยอมของเด็กที่เกี่ยวข้องกับบริการสังคมข้อมูล

อนุมาตรา 1 “ในกรณีที่มีการใช้ข้อ (a) ของข้อ 6 (1) ในส่วนที่เกี่ยวข้องกับข้อเสนอของบริการสังคมข้อมูลโดยตรงกับเด็ก การประมวลผลข้อมูลส่วนบุคคลของเด็กจะต้องถูกกฎหมายเมื่อเด็กมีอายุอย่างน้อย 16 ปี ในกรณีที่เด็กอายุต่ำกว่า 16 ปี การดำเนินการดังกล่าวจะชอบด้วยกฎหมายก็ต่อเมื่อและในขอบเขตที่ได้รับความยินยอมหรือได้รับอนุญาตจากผู้ถือความรับผิดชอบของผู้ปกครองที่มีต่อเด็กเท่านั้น ประเทศสมาชิกอาจกำหนดโดยกฎหมายสำหรับอายุที่ต่ำกว่าสำหรับวัตถุประสงค์เหล่านั้น โดยมีเงื่อนไขว่าอายุที่ต่ำกว่านั้นต้องไม่ต่ำกว่า 13 ปี”

อนุมาตรา 2 “ผู้ควบคุมต้องใช้ความพยายามตามสมควรในการตรวจสอบในกรณีที่ได้รับอนุญาตจากผู้ถือความรับผิดชอบของผู้ปกครองที่มีต่อเด็กโดยคำนึงถึงเทคโนโลยีที่มีอยู่”

อนุมาตรา 3 “อนุมาตรา 1 จะไม่กระทบต่อกฎหมายสัญญาทั่วไปของประเทศสมาชิก เช่น กฎเกณฑ์เกี่ยวกับความสมบูรณ์ การก่อตัว หรือผลกระทบของสัญญาที่เกี่ยวกับเด็ก”⁶¹

3.2.2.3 บทลงโทษกรณีฝ่าฝืนบทบัญญัติของ GDPR

รัฐสมาชิกจะวางกฎเกณฑ์เกี่ยวกับบทลงโทษอื่น ๆ ที่ใช้กับการละเมิดระเบียบนี้ โดยเฉพาะอย่างยิ่งสำหรับการละเมิดซึ่งไม่ต้องเสียค่าปรับทางปกครองตามมาตรา 83 และจะต้องดำเนินการทั้งหมดที่จำเป็นเพื่อให้แน่ใจว่ามีการดำเนินการตามนั้น

⁶⁰ Ben Welford. (2021). *What is GDPR, the EU's new data protection law?* (Online). Available: <https://gdpr.eu/what-is-gdpr/>. [2021, August 14].

⁶¹ General Data Protection Regulation (GDPR). Recital 8.

บทลงโทษดังกล่าวจะมีผลบังคับ ตามสัดส่วน และห้ามปราม

รัฐสมาชิกแต่ละรัฐจะต้องแจ้งให้คณะกรรมการทราบถึงบทบัญญัติของกฎหมายที่บังคับใช้ตามวรรค 1 ภายในวันที่ 25 พฤษภาคม 2018 และโดยไม่ชักช้า การแก้ไขใด ๆ ที่ส่งผลกระทบต่อพวกเขาในภายหลัง⁶²

สำหรับ General Data Protection Regulation (GDPR) ของสหภาพยุโรปนั้นเป็นเสมือน Model ของกฎหมายหลาย ๆ ฉบับ หลาย ๆ ประเทศก็ได้นำไปเป็นต้นแบบในการร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล เนื่องจาก GDPR ถือได้ว่าเป็นกฎหมายกลาง ที่หลายประเทศนำพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคลตาม GDPR มาปรับใช้ให้เข้ากับประเทศของตน ลักษณะเป็นกฎหมายกลางในความหมายที่ครอบคลุมการดำเนินการของบุคคลหรือนิติบุคคลใดก็ตามที่ทำการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล ประเทศที่นำมาเป็นต้นแบบอย่าง เช่น ประเทศไทย และประเทศแคนาดา

1) ประเทศแคนาดา

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (Personal Information Protection and Electronic Document Act of 2000 หรือ PIPEDA) เป็นกฎหมายความเป็นส่วนตัวส่วนตัวของรัฐบาลกลางสำหรับองค์กรภาคเอกชนในแคนาดาซึ่งถือเป็นกฎหมายที่ได้รับแรงกดดันและผลกระทบมาจาก European Union (EU) เช่นเดียวกับสหรัฐอเมริกาและประเทศอื่น ๆ ที่ต้องมีการพัฒนากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้เทียบเท่ามาตรฐานของ EU

สมศักดิ์ นวตระกูลพิสุทธิ์ ได้ศึกษากฎหมายฉบับนี้และได้อธิบายขอบเขตของกฎหมายฉบับนี้ว่าใช้บังคับแก่องค์กรทั้งหลาย (organization) ที่มีการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผยเพื่อการประกอบกิจการขององค์กร หรือที่เกี่ยวกับลูกจ้างขององค์กรหรือข้อมูลส่วนบุคคลที่ใช้ในกิจการหรือธุรกิจของสหพันธรัฐ ทั้งนี้ กฎหมายได้กำหนดกฎเกณฑ์ที่ใช้บังคับแก่การเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลโดยให้ความสำคัญกับการซึ่งนำหน้าระหว่างสิทธิความเป็นส่วนตัวส่วนตัวของบุคคล (the right of privacy of individuals) ในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของบุคคลนั้น กับความจำเป็นขององค์กรในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ซึ่งวิญญูชนเห็นว่าเหมาะสมกับสถานการณ์

ภายใต้กฎหมายนี้ กำหนดให้มีการจัดตั้งสำนักงานกรมการสิทธิความเป็นส่วนตัวแห่งแคนาดา (Office of the Privacy Commissioner of Canada) เป็นองค์กรที่คอยช่วยเหลือ ให้คำปรึกษาแก่บุคคลเกี่ยวกับสิทธิในความเป็นส่วนตัวและความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลทางอิเล็กทรอนิกส์ที่ได้รับการคุ้มครองภายใต้กฎหมายฉบับนี้โดยกฎหมายนี้

⁶² General Data Protection Regulation (GDPR). Recital 84.

มีอำนาจควบคุมองค์กรต่าง ๆ (organization) ซึ่งหมายความรวมถึง สมาคม ห้างหุ้นส่วนนิติบุคคล และสหภาพแรงงาน กฎหมายได้กำหนดไว้ว่าองค์กรทั้งหลายมีภาระหน้าที่ที่กำหนดไว้ในเอกสาร 1 (Schedule 1) แบบทำยกฎหมายซึ่งเป็นแบบปฏิบัติเพื่อการคุ้มครองข้อมูลส่วนบุคคล (Model Code for the Protection of Personal Information) ตามหลักเกณฑ์มาตรฐานแห่งชาติแคนาดา (National Standard of Canada) ดังนี้⁶³

- 1) หลักความรับผิดชอบ (Accountability)
- 2) หลักการแจ้งวัตถุประสงค์ (Identifying Purposes)
- 3) หลักความยินยอม (Consent)
- 4) หลักการเก็บรวบรวมข้อมูลอย่างจำกัด (Limiting Collection)
- 5) หลักการจำกัดการใช้ การเปิดเผย และการเก็บรักษา (Limiting Use, Disclosure and Retention)
- 6) หลักความถูกต้อง (Accuracy)
- 7) หลักการรักษาความปลอดภัย (Safeguards)
- 8) หลักการเปิดเผย (Openness)
- 9) หลักการเข้าตรวจดูข้อมูลของบุคคล (Individual Access)

Personal Information Protection and Electronic Document Act of 2000 (PIPEDA) กลายเป็นกฎหมายในวันที่ 13 เมษายน 2000 เพื่อส่งเสริมความไว้วางใจและความเป็นส่วนตัวของข้อมูลในอเมริกา และตั้งแต่นั้นมาก็ได้ขยายไปสู่อุตสาหกรรมต่าง ๆ เช่น การธนาคาร การออกอากาศ และภาคสุขภาพ

วัตถุประสงค์หลักของกฎหมาย คือ “เพื่อควบคุมการรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในลักษณะที่ตระหนักถึงสิทธิความเป็นส่วนตัวของบุคคลในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของตนและความต้องการขององค์กรในการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ที่บุคคลผู้มีเหตุผลจะเห็นว่าเหมาะสมในสถานการณ์” เช่นเดียวกับกฎระเบียบให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค (GDPR) ของสหภาพยุโรป ภายใต้ Personal Information Protection and Electronic Document Act of 2000 (PIPEDA) บุคคลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่ถือครองโดยองค์กร รู้ว่าใครเป็นผู้รับผิดชอบในการรวบรวม ทำความเข้าใจว่าทำไมจึงมีการรวบรวม และทำลายความถูกต้องของข้อมูล

นี่เป็นส่วนสำคัญของ Personal Information Protection and Electronic Document Act of 2000 (PIPEDA) เนื่องจากให้ความมั่นใจกับสหภาพยุโรปว่ากฎหมายความเป็นส่วนตัวของ

⁶³ สุวสา ถม้งรักษ์สัตว. อ่างแล้ว เจริญรอดที่ 36. หน้า 97.

แคนาดาปกป้องข้อมูลที่ละเอียดอ่อนของพลเมืองยุโรปอย่างเพียงพอ อีกแง่มุมที่สำคัญของ PIPEDA คือข้อเท็จจริงที่ได้รับการออกแบบเพื่อให้ข้อกำหนดการแจ้งเตือนการละเมิดข้อมูลของแคนาดา สอดคล้องกับคู่ค้าของประเทศรวมถึงสหภาพยุโรป จากการวิเคราะห์ผลกระทบด้านกฎระเบียบ โดยรัฐบาลแคนาดาในปี 2560 ปัจจุบัน PIPEDA ถือว่าให้การคุ้มครองความเป็นส่วนตัวในระดับที่ เทียบเท่ากับสหภาพยุโรป ซึ่งช่วยให้ถ่ายโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปไปยังองค์กร ในแคนาดาได้ฟรี⁶⁴

เมื่อมีการแสวงหาประโยชน์จากเด็กอย่างต่อเนื่องทำให้ คณะกรรมการ รัฐบาล การพาณิชย์และองค์กรได้ตกลงที่จะทำงานร่วมกันเพื่อดำเนินกิจกรรมการศึกษาของรัฐเพื่อสร้างความตระหนักในความเป็นส่วนตัวของกลุ่มเด็กและเยาวชนที่มีกับกิจกรรมออนไลน์มากยิ่งขึ้น พวกเขาโดยกฎหมายที่ให้ความคุ้มครองในข้อมูลส่วนบุคคลในประเทศแคนาดาในปัจจุบัน ได้แก่ กฎหมายเอกสารอิเล็กทรอนิกส์และการคุ้มครองข้อมูลส่วนบุคคล “PIPEDA”⁶⁵ ซึ่งการคุ้มครอง ข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ตามพระราชบัญญัติดังกล่าวยังไม่มีประสิทธิภาพในการจัดการกับปัญหาในเรื่องของการปกป้องความเป็นส่วนตัวทางด้านออนไลน์ของเด็ก ทำให้ กฎหมายเอกสารอิเล็กทรอนิกส์และการคุ้มครองข้อมูลส่วนบุคคล Personal Information Protection and Electronic Document Act of 2000 (PIPEDA) เป็นที่รู้จักในปี 1990 ที่ไม่มีประสิทธิภาพในการ บังคับใช้กับการคุ้มครองข้อมูลส่วนบุคคลของเด็กบนอินเทอร์เน็ต ทำให้เกิดการทบทวนกฎหมาย ที่บังคับใช้อยู่ ซึ่งการทบทวนครั้งล่าสุดได้สังเกตเห็นถึงความสำคัญของข้อมูลส่วนบุคคลของเด็ก จึงได้มีการเสนอแนะการปฏิรูปกฎหมายในพื้นที่ของความเป็นส่วนตัวของเด็ก คำแนะนำหนึ่งเกี่ยวกับ กฎหมายเอกสารอิเล็กทรอนิกส์และการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายที่คล้ายกันอย่างใน สาระสำคัญในระดับจังหวัดสามารถนำมาแก้ไขได้ เพื่อเสริมการเรียกร้องความยินยอมตามความ ต้องการในเรื่องของอายุที่มีการกำหนด ประกอบกับระดับความแตกต่างกันของความยินยอมตาม ประเภทของอายุ ที่จะกล่าวต่อไปเป็นโครงการที่เสนอความต้องการความยินยอมที่แตกต่างกัน เสนอแนะโดยศูนย์พิทักษ์ผลประโยชน์ประชาชนในปี ค.ศ. 2008 รายงานเกี่ยวกับความเป็นส่วนตัว ออนไลน์ของเด็ก

(1) ต่ำกว่า 13 ปี ข้อห้ามทั่วไปเกี่ยวกับการเก็บรวบรวมการใช้และการเปิดเผย ข้อมูลส่วนบุคคลทั้งหมดจากเด็กที่มีอายุต่ำกว่า 13 ปี

⁶⁴ Abi Tyas Tunggal. (2021). *What is PIPEDA (Personal Information Protection and Electronic Documents Act)?*. (Online). Available: <https://www.upguard.com/blog/pipeda>. [2021, August 3].

⁶⁵ กฎหมายเอกสารอิเล็กทรอนิกส์และการคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection and Electronic Document Act: (“PIPEDA”), S.C. 2000, c-5.

(2) อายุ 13 -15 ปี เว็บไซต์อาจได้รับอนุญาตในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลแต่เพียงผู้เดียวที่เกี่ยวข้องกับเว็บไซต์ดังกล่าวพร้อมกับความยินยอมที่ชัดเจนของเด็กและผู้ปกครอง รวมทั้งอาจจะไม่ได้รับอนุญาตในการเปิดเผยข้อมูลส่วนบุคคลของพวกเขาในอนาคต

(3) อายุ 16 ปี เว็บไซต์อาจได้รับอนุญาตในการเก็บรวบรวมข้อมูลโดยความยินยอมของเด็กและในเปิดเผยข้อมูลส่วนบุคคลของเด็กนั้นจะต้องได้รับความยินยอมของเด็กและความยินยอมที่ชัดเจนของผู้ปกครอง

หลังจากอายุบรรลุนิติภาวะแล้ว (18 หรือ 19 ปี) เว็บไซต์และบริษัทอาจจะไม่ได้รับอนุญาตในการเก็บข้อมูลที่ได้รวบรวมไว้ก่อนเด็กบรรลุนิติภาวะและอาจได้รับการร้องขอให้ลบข้อมูลทันทีโดยไม่ต้องได้รับความยินยอมที่ชัดเจนจากบุคคลที่มีอายุบรรลุนิติภาวะ

ความแตกต่างระหว่างการปฏิรูปกฎหมายที่ได้เสนอแนะนี้กับ กฎหมายคุ้มครองความเป็นส่วนตัวของเด็กบนเว็บไซต์ (Child Online Privacy and Protect Act of 1998 (COPPA) ของสหรัฐอเมริกา คือ การปฏิรูปกฎหมายนี้เรียกร้องให้มีการห้ามเกี่ยวกับการเก็บรวบรวม การใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่มีอายุต่ำกว่า 13 ปีทั้งหมด ในขณะที่กฎหมายคุ้มครองความเป็นส่วนตัวของเด็กบนเว็บไซต์ (Child Online Privacy and Protect Act of 1998 (COPPA) จะเน้นในเรื่องของการเรียกร้องความยินยอมจากผู้ปกครองเท่านั้น

เนื่องจากขาดการประสบความสำเร็จของกฎหมายคุ้มครองความเป็นส่วนตัวของเด็กบนเว็บไซต์ (Child Online Privacy and Protect Act of 1998 (COPPA) ห้ามเกี่ยวกับการเก็บรวบรวม การใช้หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่มีอายุต่ำกว่า 13 ปีทั้งหมดอาจเป็นทางเลือกที่เหมาะสมกฎหมายเอกสารอิเล็กทรอนิกส์และการคุ้มครองข้อมูลส่วนบุคคล Personal Information Protection and Electronic Document Act of 2000 (PIPEDA) หรือการออกกฎหมายที่คล้ายกันอย่างมีนัยสำคัญในระดับภูมิภาคมีโอกาที่จะใช้อิทธิพลเพื่อให้แน่ใจว่าการออกกฎหมายนำมาแก้ไขเพิ่มเติมในลักษณะที่จะทำให้มีประสิทธิภาพมากขึ้นในการปกป้องความเป็นส่วนตัวบนเว็บไซต์ของเด็ก ทำให้กฎหมายเอกสารอิเล็กทรอนิกส์และการคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection and Electronic Document Act of 2000 (PIPEDA) สามารถนำมาแก้ไขเพิ่มเติมได้รวมถึงกฎระเบียบที่ได้รับความยินยอมที่ชัดเจนสำหรับการเก็บรวบรวมการใช้และการเปิดเผยข้อมูลส่วนบุคคลของเด็ก ซึ่งการพัฒนาช่องว่างการปฏิบัติบนเว็บไซต์ที่ไม่ใช่เชิงพาณิชย์ควรได้รับการส่งเสริม กฎหมายที่มีความจำเป็นทั้งในระดับจังหวัดหรือระดับชาติในการห้ามทั้งการโฆษณาที่ฝังอยู่ในเว็บไซต์มุ่งเน้นไปที่เด็กและความพยายามด้านการตลาดที่มีการกำหนดเป้าหมายไปที่เด็ก ซึ่งกฎหมายคุ้มครองผู้บริโภคของเมืองควิเบก (Quebec) ควบคุมสัญญาบางส่วนในประเด็นนี้ แต่สามารถนำมาปรับปรุงในยุคข้อมูลข่าวสารและคัดลอกในเขตอำนาจศาลแคนาดาอื่น ๆ

นอกจากนี้ ผู้เชี่ยวชาญในของการด้านบังคับใช้กฎหมายได้มีการกำหนดให้ใช้ในทางใดทางหนึ่งโดยเฉพาะอย่างมีประสิทธิภาพ โดยเฉพาะการหาผู้กระทำผิดเกี่ยวกับสื่อลามกอนาจารเด็กโดยส่งเสริมกฎหมายเกี่ยวกับวิธีการทางกฎหมายที่จะกำหนดให้ผู้ให้บริการอินเทอร์เน็ต (“ISPs”) ช่วยในการบังคับใช้กฎหมายสื่อลามกอนาจาร และรวมไปถึงการระบุหลักฐานของผู้กระทำผิดเหล่านี้ได้มากขึ้น โดยการเริ่มนำการออกกฎหมายที่เรียกร้องให้มีการรายงานข้อกำหนดเกี่ยวกับการพบสื่อลามกอนาจารเด็ก การค้นพบความสมดุลที่โดดเด่นระหว่างสิทธิส่วนบุคคลของลูกค้าของผู้ให้บริการอินเทอร์เน็ต (“ISPs”) กับสิทธิตามกฎหมายความเป็นส่วนตัวของเด็กที่ถูกบุกรุกโดยสื่อลามกอนาจารจะต้องมีการพิจารณาอย่างรอบคอบ แต่ความพยายามเกี่ยวกับการให้คำปรึกษาร่วมกันโดยคณะกรรมการความเป็นส่วนตัวและที่ปรึกษาเด็กและและเยาวชนส่วนใหญ่มีแนวโน้มที่จะกำหนดพื้นฐานที่มั่นคงสำหรับการแก้ปัญหาที่เป็นฉันทามติในเรื่องนี้⁶⁶

3.2.3 สาธารณรัฐประชาชนจีน

เมื่อวันที่ 22 สิงหาคม 2019 หน่วยงาน Cyberspace Administration of China (CAC) ได้ออกกฎระเบียบความเป็นส่วนตัวเป็นส่วนตัวของข้อมูลฉบับใหม่ที่เกี่ยวข้องกับเด็ก คือ Provisions on Cyber Protection of Personal Information of Children (PCPPIC) กฎระเบียบดังกล่าวจะมีผลบังคับใช้ในวันที่ 1 ตุลาคม 2019 และจะมีผลบังคับใช้ภายในสาธารณรัฐประชาชนจีน (PRC) วัตถุประสงค์ที่ระบุไว้ของ PCPPIC คือ “การปกป้องความปลอดภัยของข้อมูลส่วนบุคคลของเด็กและส่งเสริมการเติบโตอย่างแข็งแรงของเด็กใน PRC” ในบทความ 29 ฉบับ PCPPIC ระบุไว้ในระดับสูงข้อกำหนดระดับสำหรับการรวบรวม การจัดเก็บ การใช้ การถ่ายโอน และการเปิดเผยข้อมูลส่วนบุคคลของเด็กภายในอาณาเขตของสาธารณรัฐประชาชนจีน

กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ (CSL) กำหนดหลักการทั่วไปเกี่ยวกับการปกป้องข้อมูลในสาธารณรัฐประชาชนจีน แต่ยังไม่มีการระบุเฉพาะเจาะจงเกี่ยวกับการคุ้มครองความเป็นส่วนตัวของเด็กทางออนไลน์ จนกว่าจะมีกฎระเบียบใหม่ มาตรฐานความปลอดภัยของข้อมูลส่วนบุคคล (มาตรฐานความปลอดภัย) เป็นชุดของมาตรฐานที่แนะนำสำหรับการปกป้องข้อมูลส่วนบุคคลซึ่งมีผลบังคับใช้ในวันที่ 1 พฤษภาคม ค.ศ. 2018 สิ่งเหล่านี้กำหนดให้ผู้ควบคุมข้อมูลปฏิบัติต่อข้อมูลส่วนบุคคลของเด็กเป็นข้อมูลส่วนบุคคลที่ละเอียดอ่อนและต้องได้รับความยินยอมอย่างชัดแจ้งจาก ผู้ปกครองเด็กสำหรับการประมวลผลข้อมูลส่วนบุคคล มาตรการป้องกันพิเศษที่ใช้กับข้อมูลส่วนบุคคลที่ละเอียดอ่อนภายใต้มาตรฐานความปลอดภัยจะนำไปใช้กับข้อมูลส่วนบุคคลของเด็กด้วย มาตรการที่จำเป็นเหล่านี้ ซึ่งรวมถึงความยินยอมแยกต่างหากสำหรับแต่ละฟังก์ชันของบริการหรือผลิตภัณฑ์ การเข้ารหัสข้อมูลสำหรับการจัดเก็บและการส่ง การอนุญาต

⁶⁶ พนิดา พูลสวัสดิ์. อ่างแล้ว เจริญรอดที่ 7. หน้า 54-56.

การเข้าถึงภายในตามคำขอ การแจ้งล่วงหน้าและความยินยอมโดยชัดแจ้งก่อนการแบ่งปันหรือถ่ายโอนข้อมูล นโยบายความเป็นส่วนตัวแบบจำลองที่แนบมากับมาตรฐานความปลอดภัยยังรวมถึงส่วนเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของเด็กด้วย

3.2.3.1 ความหมายของคำนิยามของข้อมูลส่วนบุคคลของเด็กตามบทบัญญัติของ PCPPIC

ภายใต้บทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของเด็กทางออนไลน์ ได้มีการกำหนดเนื้อหาไว้ว่า คำว่า “เด็ก” ตามข้อกำหนดเหล่านี้ หมายถึง ผู้เยาว์ที่มีอายุต่ำกว่า 14 ปี⁶⁷ ถูกกำหนดให้เป็นผู้เยาว์ ระเบียบใหม่มีผลบังคับใช้กับการรวบรวม การจัดเก็บ การใช้ การถ่ายโอน และการเปิดเผยข้อมูลส่วนบุคคลของเด็กที่ดำเนินการภายในอาณาเขตของ (PRC หรือ People's Republic of China) ทางออนไลน์

บทบัญญัติกำหนดให้ผู้ให้บริการเครือข่ายปฏิบัติตามหลักการของความชอบธรรม ความจำเป็น ความยินยอมที่ได้รับการบอกกล่าว วัตถุประสงค์ที่ชัดเจน รับประกันความปลอดภัย และการใช้งานที่ถูกต้องตามกฎหมายเมื่อรวบรวม จัดเก็บ ใช้ โอน หรือเปิดเผยข้อมูลส่วนบุคคลของเด็ก ภายใต้ข้อกำหนดนี้ ผู้ให้บริการเครือข่ายต้องกำหนดนโยบายและข้อตกลงผู้ใช้เฉพาะเพื่อปกป้องข้อมูลส่วนบุคคลของเด็ก

ในกรณีหากเด็กหรือผู้ปกครองพบว่าข้อมูลส่วนบุคคลของเด็กที่รวบรวม จัดเก็บ ใช้ หรือเปิดเผยโดยผู้ให้บริการเครือข่ายนั้นไม่ถูกต้อง พวกเขามีสิทธิขอให้ผู้ให้บริการเครือข่ายแก้ไข ผู้ให้บริการเครือข่ายควรใช้มาตรการในการแก้ไขอย่างทันท่วงที⁶⁸

3.2.3.2 หน้าที่ของผู้ให้บริการ ตามบทบัญญัติของ PCPPIC และความยินยอม

มีการกำหนดห้ามมิให้องค์กรหรือบุคคลใดผลิต ดิจิทัล หรือเผยแพร่ข้อมูลที่ละเมิดความปลอดภัยของข้อมูลส่วนบุคคลของเด็ก⁶⁹

เมื่อผู้ให้บริการเครือข่ายได้ทำการรวบรวม จัดเก็บ ใช้ โอน และเปิดเผยข้อมูลส่วนบุคคลของเด็ก พวกเขาจะต้องปฏิบัติตามหลักการของเหตุผลและความจำเป็น การรับทราบ และให้ความยินยอม วัตถุประสงค์ที่ชัดเจน การประกันความปลอดภัย และการใช้ตามกฎหมาย⁷⁰ และเมื่อผู้ให้บริการเครือข่ายที่รวบรวม ใช้ โอน หรือเปิดเผยข้อมูลส่วนบุคคลของเด็กจะต้องแจ้งให้ผู้ปกครองของเด็กทราบอย่างชัดเจนและต้องได้รับความยินยอมจากผู้ปกครองของเด็ก⁷¹

⁶⁷ Provisions on Cyber Protection of Personal Information of Children (PCPPIC). Article 2.

⁶⁸ Provisions on Cyber Protection of Personal Information of Children (PCPPIC). Article 19.

⁶⁹ Provisions on Cyber Protection of Personal Information of Children (PCPPIC). Article 4.

⁷⁰ Provisions on Cyber Protection of Personal Information of Children (PCPPIC). Article 7.

⁷¹ Provisions on Cyber Protection of Personal Information of Children (PCPPIC). Article 9.

นอกจากนี้ ในเรื่องของความยินยอมจากผู้ปกครอง เด็กที่มีอายุต่ำกว่า 14 ปี ต้องได้รับความยินยอมจากผู้ปกครองก่อนที่จะมีการรวบรวมหรือใช้ข้อมูลส่วนบุคคลของเด็ก ผู้ให้บริการเครือข่ายต้องมีตัวล็อกในการระงับความยินยอมด้วย ในการขอรับความยินยอม กล่าวคือ ผู้ให้บริการเครือข่ายต้องแจ้งให้ผู้ปกครองทราบถึงข้อมูลที่พวกเขาจะรวบรวม การใช้งานที่จะนำไปใช้ และเหตุผลที่พวกเขาต้องการและต้องถ่ายทออย่างชัดเจนและเห็นได้ชัด ดังต่อไปนี้

- 1) วัตถุประสงค์ วิธีการ และขอบเขตของการรวบรวม การจัดเก็บ การใช้ การถ่ายโอน และการเปิดเผยข้อมูลส่วนบุคคลของเด็ก
- 2) สถานที่จัดเก็บ ระยะเวลาในการจัดเก็บ และการจัดการข้อมูลหลังจากสิ้นสุดระยะเวลาการจัดเก็บที่ตกลงกันไว้
- 3) มาตรการรักษาความปลอดภัยในการปกป้องข้อมูลส่วนบุคคลของเด็ก
- 4) ผลที่ตามมาของการปฏิเสธที่จะอนุญาตให้ใช้ ถ่ายโอน เปิดเผย และจัดเก็บข้อมูลส่วนบุคคลของเด็ก
- 5) วิธีการรายงานการละเมิดหรือยื่นเรื่องร้องเรียนกับผู้ให้บริการเครือข่าย
- 6) วิธีการแก้ไขและลบข้อมูลส่วนบุคคลของเด็ก
- 7) เรื่องอื่น ๆ ว่าผู้ให้บริการเครือข่ายรายใดต้องให้ข้อมูล

ข้อบังคับนี้ห้ามไม่ให้ผู้ให้บริการเครือข่ายจัดเก็บข้อมูลส่วนบุคคลของเด็กเกินระยะเวลาที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ในการรวบรวมและใช้งาน และกำหนดให้ผู้ให้บริการต้องรับรองความปลอดภัยของข้อมูลด้วยการเข้ารหัสหรือวิธีการอื่น ๆ

การใช้ข้อมูลส่วนบุคคลของเด็กโดยผู้ให้บริการเครือข่ายต้องไม่ละเมิดกฎหมายและระเบียบข้อบังคับด้านการบริหารหรือวัตถุประสงค์และขอบเขตการใช้งานที่ตกลงกัน โดยทั้งสองฝ่าย ภายใต้หลักการของการอนุญาตขั้นต่ำ ผู้ให้บริการเครือข่ายจะต้องกำหนดข้อจำกัดการเข้าถึงที่เข้มงวดสำหรับบุคลากรของคนที่ได้รับอนุญาตให้จัดการข้อมูลส่วนบุคคลของเด็ก ผู้ให้บริการเครือข่ายต้องดำเนินการประเมินความปลอดภัยก่อนที่จะจ้างผู้ขายบุคคลที่สามหรือถ่ายโอนข้อมูลส่วนบุคคลของเด็กไปยังบุคคลที่สาม

3.2.3.3 บทลงโทษกรณีฝ่าฝืนบทบัญญัติของ PCPPIC

ใครก็ตามที่ฝ่าฝืนข้อบังคับจะได้รับการจัดการโดยแผนกความปลอดภัยทางไซเบอร์ และการให้ข้อมูลและหน่วยงานที่เกี่ยวข้องอื่น ๆ ตามหน้าที่และสอดคล้องกับ “กฎหมายความปลอดภัยเครือข่ายของสาธารณรัฐประชาชนจีน” “มาตรการการจัดการบริการข้อมูลทางอินเทอร์เน็ต” และ

กฎหมายและข้อบังคับอื่น ๆ ที่เกี่ยวข้อง หากก่ออาชญากรรมขึ้น จะถูกสอบสวนตามกฎหมายว่าด้วยความรับผิดชอบทางอาญา⁷²

อย่างไรก็ตาม PCPPIC ยังไม่มีความชัดเจนบทบัญญัติที่ว่ามาตรการบริการข้อมูลจะนำไปใช้กับการละเมิดถูกระเบียบข้อมูลส่วนบุคคลของเด็กอย่างไร โดยเฉพาะอย่างยิ่งเนื่องจากมาตรการบริการข้อมูลทางอินเทอร์เน็ตมุ่งเน้นไปที่การควบคุมกิจกรรมบริการข้อมูล (เช่น การขออนุมัติ บางเว็บไซต์) แต่ไม่อ้างอิงถึงการปกป้องข้อมูลส่วนบุคคล หรืออาจกล่าวได้ว่ายังไม่มียกเว้นโทษเฉพาะสำหรับการละเมิด ในทางกลับกัน ผู้ฝ่าฝืนบทบัญญัติจะได้รับบทลงโทษ รวมถึงบทลงโทษทางอาญาภายใต้กฎหมายและข้อบังคับอื่น ๆ ที่เกี่ยวข้อง เช่น กฎหมายความปลอดภัยทางไซเบอร์ และมาตรการทางปกครองเกี่ยวกับบริการข้อมูลทางอินเทอร์เน็ต

3.2.4 สาธารณรัฐไอร์แลนด์ (Data Protection Commission Ireland)

คณะกรรมการคุ้มครองข้อมูล (Data Protection Commission หรือ DPC) เป็นหน่วยงานอิสระระดับชาติที่รับผิดชอบในการรักษาสิทธิขั้นพื้นฐานของบุคคลในสหภาพยุโรปในการปกป้องข้อมูลส่วนบุคคล DPC เป็นหน่วยงานกำกับดูแลของสาธารณรัฐไอร์แลนด์สำหรับกฎระเบียบให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค (GDPR) และยังมีหน้าที่และอำนาจที่เกี่ยวข้องกับการกำกับดูแลที่สำคัญอื่น ๆ ซึ่งรวมถึงระเบียบ ePrivacy ของสาธารณรัฐไอร์แลนด์ (2011) และคำสั่งของสหภาพยุโรปที่เรียกว่าคำสั่งบังคับใช้กฎหมาย

DPC ได้เผยแพร่ร่างเอกสารแนวทางที่ครอบคลุมเมื่อปลายปีที่แล้วในหัวข้อ “The Fundamentals for a Child-Oriented Approach to Data Processing” กำหนดหลักการสำคัญ 14 ข้อ สำหรับองค์กรที่ต้องปฏิบัติตามเมื่อประมวลผลข้อมูลเด็ก และองค์กรทั้งหมดที่ประมวลผลข้อมูลเด็กควรปฏิบัติตาม ซึ่งรวมถึงบริการที่มุ่งเป้าไปที่ / มีไว้สำหรับ หรือมีแนวโน้มที่จะเข้าถึงได้โดยเด็ก ในสาธารณรัฐไอร์แลนด์เพื่อวัตถุประสงค์ในการปกป้องข้อมูล เด็กคือบุคคลที่มีอายุต่ำกว่า 18 ปี

หลักการสำคัญ 14 ข้อของพื้นฐาน มีดังนี้

1) เกณฑ์พื้นฐานขั้นต่ำในการคุ้มครอง ผู้ให้บริการควรจะกำหนดเกณฑ์พื้นฐานในการคุ้มครองผู้ใช้บริการทุกคนในขั้นสูงสุด เว้นแต่จะจัดให้มีระบบยืนยันอายุของผู้ใช้บริการ (verifying age)

2) ความยินยอมที่ชัดเจน/ชัดเจน ในกรณีที่เด็กให้ความยินยอมในการประมวลผลข้อมูลของตน ความยินยอมนั้นต้องได้รับการยินยอมโดยเสรี เฉพาะเจาะจง ได้รับแจ้ง และไม่คลุมเครือ

⁷² Provisions on Cyber Protection of Personal Information of Children (PCPPIC). Article 26.

3) ปราศจากการแทรกแซง ในกรณีประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ โดยอาศัยฐานเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้เยาว์ ควรมีการประเมินและทำให้มั่นใจว่าการประมวลผลข้อมูลนั้นจะไม่สร้างผลกระทบในเชิงลบต่อด้านอื่น ๆ ของผู้เยาว์

4) การระบุตัวตนของผู้ใช้บริการ ผู้ให้บริการควรดำเนินการระบุตัวตนของผู้ใช้บริการ เพื่อให้สามารถทำให้แน่ใจได้ว่าเนื้อหาหรือการใช้งานของการให้บริการแต่ละประเภทเหมาะสมกับผู้ให้บริการที่เป็นผู้เยาว์

5) ข้อมูลในทุกกรณี เด็กมีสิทธิ์ได้รับข้อมูลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของตนเองโดยไม่คำนึงถึงพื้นฐานทางกฎหมายที่ นี่เป็นกรณีที่ได้รับคามยินยอมจากผู้ปกครอง ในนามของพวกเขาในการประมวลผลข้อมูลส่วนบุคคลของพวกเขา

6) ความโปร่งใสและเข้าใจง่ายที่มุ่งเป้าไปที่เด็ก ข้อมูลความเป็นส่วนตัวเกี่ยวกับวิธีการใช้ข้อมูลส่วนบุคคลจะต้องจัดให้มีวิธีการที่กระชับ โปร่งใส เข้าใจได้ และเข้าถึงได้ โดยใช้ภาษาที่ชัดเจนและเข้าใจง่ายที่เข้าใจง่ายและเหมาะสมกับอายุของเด็กและวัยของผู้เยาว์

7) ผู้เยาว์ต้องสามารถใช้สิทธิในฐานะเจ้าของข้อมูลส่วนบุคคลได้ กล่าวคือ จำไว้ว่าเด็ก ๆ เป็นเจ้าของข้อมูลในสิทธิของตนเองและมีสิทธิที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของพวกเขา ในทุกช่วงอายุ ด้วยเหตุนี้ DPC จึงพิจารณาว่าพวกเขาควรได้รับอนุญาตให้ใช้สิทธิในการปกป้องข้อมูลของตนได้ในทุกช่วงอายุ トラบใดที่พวกเขาสามารถทำเช่นนั้นได้ และอยู่ในผลประโยชน์สูงสุดของพวกเขา

8) ความยินยอมไม่เปลี่ยนแปลงสถานะความเป็นผู้เยาว์ ไม่ว่าจะการได้รับความยินยอมจากตัวของผู้เยาว์หรือผู้ปกครอง ไม่ควรเป็นเหตุให้ปฏิบัติต่อผู้เยาว์ในเรื่องนั้น ๆ เสมือนว่าผู้เยาว์เป็นบุคคลที่บรรลุนิติภาวะแล้ว

9) ความรับผิดชอบของเจ้าของแพลตฟอร์ม ความรับผิดชอบของคุณ บริษัทที่ได้รับรายได้จากการให้บริการหรือขายบริการผ่านเทคโนโลยีดิจิทัลและออนไลน์จะมีความเสี่ยงต่อสิทธิและเสรีภาพของเด็กโดยเฉพาะ ในกรณีที่บริษัทดังกล่าวใช้การตรวจสอบอายุและ/หรืออาศัยความยินยอมของผู้ปกครองในการประมวลผล DPC คาดหวังว่าจะต้องผู้ให้บริการควรรับภาระในการจัดทำมาตรการในการระบุตัวตนของผู้ใช้งาน และการยืนยันตัวตนของผู้เยาว์และ โดยเฉพาะการตรวจสอบความยินยอมของผู้ปกครอง

10) ไม่ตัดหรือลดการให้บริการแก่ผู้เยาว์ ผู้ให้บริการต้องไม่ทำการยกเลิกการให้บริการแก่ผู้เยาว์ หรือลดฟังก์ชันการใช้งานที่ผู้เยาว์ควรจะได้รับลง เพื่อเป็นการตัดภาระในเรื่องความรับผิดชอบต่อการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

11) การกำหนดอายุขั้นต่ำไม่ใช่ข้อยกเว้น การกำหนดอายุขั้นต่ำในการเข้าใช้บริการ เว็บไซต์หรือแพลตฟอร์มไม่ใช่ข้อยกเว้นที่จะทำให้ผู้ให้บริการไม่ต้องดำเนินการต่าง ๆ ตามข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในเรื่องของผู้เยาว์

หากบริการของแพลตฟอร์มหรือเว็บไซต์ไม่ได้มีไว้สำหรับเด็กที่อายุต่ำกว่าเกณฑ์ จะต้องดำเนินการเพื่อให้แน่ใจว่ากลไกการตรวจสอบอายุของคุณมีประสิทธิภาพในการป้องกันไม่ให้เด็กที่อายุต่ำกว่านั้นเข้าถึงบริการ หากวิธีนี้ใช้ไม่ได้ผล ต้องแน่ใจว่ามีมาตรการปกป้องข้อมูลที่เหมาะสมเพื่อปกป้องตำแหน่งของผู้ใช้ที่เป็นเด็ก ทั้งที่อายุต่ำกว่าเกณฑ์และสูงกว่าเกณฑ์อายุผู้ใช้ อย่างเป็นทางการ

12) ไม่ควรใช้การประมวลผลข้อมูลอัตโนมัติ ข้อเสนอแนะกำหนดว่าผู้ให้บริการไม่ควรใช้ระบบอัตโนมัติในการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์รวมถึงไม่ควรใช้ข้อมูลของผู้เยาว์เพื่อวัตถุประสงค์ทางการตลาดและการโฆษณา เนื่องจากผู้เยาว์มีความอ่อนไหวและเสี่ยงต่อการถูกชี้นำทางพฤติกรรม

13) จัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ผู้ให้บริการต้องจัดทำประเมินผลกระทบเพื่อลดความเสี่ยงที่อาจเกิดขึ้นต่อตัวผู้เยาว์จากการประมวลผลข้อมูลส่วนบุคคล โดยการจัดทำประเมินดังกล่าวต้องถือหลักเพื่อประโยชน์สูงสุดแก่ตัวผู้เยาว์ (principle of the best interest of child) และในกรณีที่มีความขัดกันระหว่างผลประโยชน์ทางเศรษฐกิจขององค์กรกับผลประโยชน์ของผู้เยาว์ผู้ให้บริการต้องเลือกที่จะคุ้มครองผลประโยชน์ของผู้เยาว์เป็นลำดับแรกเสมอ

14) การออกแบบระบบในเบื้องต้นด้วยมาตรการที่ดีที่สุด ผู้ให้บริการที่มีการประมวลผลข้อมูลของผู้เยาว์อย่างสม่ำเสมอควรออกแบบระบบของตนให้มีค่าเริ่มต้นในการปกป้องข้อมูลระดับสูงและสำหรับผู้เยาว์โดยเฉพาะ

DPC ได้ตรวจสอบรายละเอียดการคุ้มครองเพิ่มเติมที่จำเป็นภายใต้ GDPR ที่เกี่ยวข้องกับผู้ใช้ที่เป็นเด็ก ได้ระบุมาตรการที่แนะนำในทางปฏิบัติจำนวนหนึ่งเพื่อสร้างสภาพแวดล้อมออนไลน์ที่ปลอดภัยยิ่งขึ้น เหมาะสมกว่าและเคารพความเป็นส่วนตัวมากขึ้นเพื่อให้เด็กเล่น โต้ตอบ เรียนรู้ และสร้างสรรค์มากกว่าที่เป็นอยู่ในปัจจุบัน นอกจากนี้ DPC ตั้งข้อสังเกตว่าการปฏิบัติตามระบบการปกป้องข้อมูลตามความเหมาะสมกับวัยเด็กจะมีค่าใช้จ่ายและใช้ความคิดสร้างสรรค์ในส่วนของนักออกแบบบริการ อย่างไรก็ตาม เด็ก ๆ เป็นผู้ใช้หนึ่งในสามและเป็นตัวแทนของตลาด

สำหรับผู้ใหญ่ในอนาคต ผลประโยชน์และสนับสนุนความสัมพันธ์ที่ดีกับเด็กในระยะยาว เพื่อประโยชน์ของแบรนด์และธุรกิจในทุกภาคส่วน⁷³

3.2.4.1 อายุ ความยินยอมทางดิจิทัล

แนวคิดที่เรียกว่า “ยุคแห่งความยินยอมทางดิจิทัล” ที่เกี่ยวข้องกับบริการสังคมข้อมูล เกิดขึ้นจากมาตรา 8 ของ GDPR ซึ่งระบุว่าหากบริการสังคมข้อมูล (เช่น เว็บไซต์หรือแอปที่ให้บริการ เช่น เกม สื่อสังคม การแชร์วิดีโอ ฯลฯ) มีการเสนอให้กับเด็กโดยตรง และบริการนั้นอาศัยความยินยอมเป็นพื้นฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลของผู้ใช้ที่เป็นเด็ก จากนั้นจึงได้รับความยินยอมจากผู้ปกครอง (อธิบายไว้ใน GDPR ว่าเป็นความยินยอมจากผู้ถือความรับผิดชอบของผู้ปกครอง) หากเด็กอายุต่ำกว่า 16 ปี ต้องได้รับความยินยอมในสาธารณรัฐไอร์แลนด์

หากผู้ให้บริการออนไลน์ขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลเพื่อให้เด็กเข้าถึงบริการได้ (เช่น ในการสร้างและใช้งานบัญชีผู้ใช้ในภายหลัง) ต้องได้รับความยินยอมจากผู้ปกครองในการประมวลผลข้อมูลส่วนบุคคลของเด็กนั้น จุดเริ่มต้นนี้คือต้องได้รับความยินยอมจากบุคคลที่ถือเป็นการรับผิดชอบของผู้ปกครอง กล่าวคือ ต้องได้รับจาก พ่อแม่/ผู้ปกครองของเด็ก อย่างไรก็ตาม ในแง่ของระดับความแน่นอนที่กำหนดโดยผู้ให้บริการออนไลน์ที่ได้รับความยินยอมจากผู้ถือความรับผิดชอบของผู้ปกครอง GDPR กำหนดให้ผู้ให้บริการออนไลน์ต้อง “พยายามอย่างสมเหตุสมผล” เพื่อตรวจสอบ “โดยคำนึงถึงเทคโนโลยีที่มีอยู่”

สิ่งที่สำคัญอย่างยิ่งคือข้อกำหนดเกี่ยวกับอายุของความยินยอมทางดิจิทัลไม่ได้กำหนดข้อจำกัดในการเข้าถึงบริการของเด็กแต่อายุของการยินยอมทางดิจิทัลจะกำหนดเกณฑ์สำหรับอายุที่เด็กสามารถให้ความยินยอมของตนเองกับผู้ให้บริการออนไลน์ในการประมวลผลข้อมูลส่วนบุคคลของตนได้ อย่างไรก็ตาม ตามที่กล่าวไว้ข้างต้น องค์กรที่ประมวลผลข้อมูลของเด็กอาจอาศัยฐานทางกฎหมายอีกห้าฐานภายใต้ GDPR แทนที่จะอาศัยความยินยอมในการทำเช่นนั้น กล่าวอีกนัยหนึ่งภายใต้ GDPR ความยินยอมไม่ได้เป็นเพียงพื้นฐานทางกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคลของเด็ก

สิ่งสำคัญคือต้องเน้นว่าอายุของความยินยอมทางดิจิทัล จึงไม่ใช่มาตรการในการป้องกันการเข้าถึงเว็บไซต์และแอปบางอย่างของเด็ก ๆ ฯลฯ และไม่ใช่มาตรการความปลอดภัยออนไลน์

⁷³ Children front and center. (2020). *Fundamentals for a child-oriented approach to data processing. Draft version for public consultation.* (Online). Available: https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf. [2021, August 3].

แต่เป็นมาตรการในการปกป้องข้อมูลส่วนบุคคลของเด็กในบางกรณีแทน อายุของการยินยอมทางดิจิทัลยังเป็นเครื่องหมายสำหรับบริการออนไลน์เพื่อพิจารณาลักษณะและการออกแบบของบริการ และวิธีการทำให้เหมาะสมกับอายุของผู้ใช้ ความยินยอมทางดิจิทัลที่ได้รับจากเด็กที่อายุเกินเกณฑ์ความยินยอมทางดิจิทัล (เช่น อายุ 16 ปีขึ้นไปในสาธารณรัฐไอร์แลนด์) หรือจากผู้ปกครอง/ผู้ปกครองของเด็กอายุต่ำกว่าที่ได้รับ ความยินยอมทางดิจิทัล ไม่ควรใช้เป็นเส้นทางในการปฏิบัติต่อเด็กทุกวัยเสมือนกับเป็นผู้ใหญ่ การยินยอมจะต้องให้โดยเสรี เฉพาะเจาะจง ได้รับแจ้ง และไม่คลุมเครือ และควรจัดให้มีกลไกที่ง่ายต่อการใช้งานแก่เด็ก/ผู้ปกครองหรือผู้ปกครอง เพื่อให้สามารถเพิกถอนความยินยอมได้ทุกเมื่อ⁷⁴ การรวบรวมความยินยอมตามมาตรา 8 ยังเป็นโอกาสสำหรับบริการทางออนไลน์ เพื่อให้ระบบการปกป้องข้อมูลที่เหมาะสมกับวัย โดยค่าเริ่มต้นปรับให้เข้ากับช่วงอายุของผู้ใช้

3.2.4.2 การตรวจสอบความยินยอมของผู้ปกครอง

การตรวจสอบอายุเพื่อให้มั่นใจว่าองค์กรใช้มาตรฐานการปกป้องข้อมูลสูงสุดกับผู้ใช้ที่เป็นเด็กนั้นแตกต่างไปจากวัตถุประสงค์ในการตรวจสอบอายุที่องค์กรอาศัยความยินยอมเป็นพื้นฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลของเด็ก แม้ว่าวิธีการตรวจสอบอายุเดียวกันอาจใช้ในทั้งสองกรณี ในอดีตการตรวจสอบอายุคือการพิจารณาว่าผู้ใ้รายหนึ่งมีอายุต่ำกว่า 18 ปีหรือไม่ และยังเป็นเด็กตามวัตถุประสงค์ของกฎหมายไอร์แลนด์และสหภาพยุโรป ดังนั้นจึงสมควรได้รับการคุ้มครองพิเศษตามที่ระบุไว้ใน GDPR ในทางกลับกัน อายุการตรวจสอบเพื่อวัตถุประสงค์พื้นฐานทางกฎหมายโดยทั่วไปจะมุ่งสร้าง (ในสาธารณรัฐไอร์แลนด์อย่างน้อย) ไม่ว่าผู้ใ้จะอายุต่ำกว่า 16 ปีได้รับความยินยอมทางดิจิทัลหรือไม่ โดยเฉพาะอย่างยิ่ง GDPR ไม่ต้องการให้องค์กรดำเนินการตรวจสอบอายุเพื่อปฏิบัติตาม ด้วยมาตรา 8 GDPR องค์กรต่าง ๆ จะต้อง “พยายามอย่างสมเหตุสมผล” ในการตรวจสอบ โดยที่เด็กนั้นอายุต่ำกว่า 16 ปี (ในสาธารณรัฐไอร์แลนด์) ได้รับความยินยอม/อนุญาตจากผู้ถือความรับผิดชอบของผู้ปกครองที่มีต่อเด็ก ไม่มีภาระระบุหรือแนะนำวิธีการในการปฏิบัติตามภาระผูกพันนี้และ GDPR กำหนดให้ต้องมีการพิจารณา “เทคโนโลยีที่มีอยู่” ซึ่งหมายความว่าองค์กรต้องสำรวจเทคโนโลยีทั้งหมดอย่างเต็มที่ ตัวเลือกที่มีให้ และเพิ่มนวัตกรรมสูงสุด ด้วยขนาดของความเชี่ยวชาญทางเทคนิคและทรัพยากรที่มีให้ สำหรับบริษัทเทคโนโลยีและอินเทอร์เน็ตการนำเทคโนโลยีดิจิทัลและออนไลน์มาใช้ และความเสี่ยงที่สูงขึ้นต่อสิทธิในการปกป้องข้อมูลของผู้ใช้ที่ใช้บริการของตน โดยเฉพาะเด็ก DPC พิจารณาว่าองค์กรดังกล่าวมีภาระที่สูงขึ้นในความพยายามในการตรวจสอบอายุ และตรวจสอบว่าผู้ปกครอง/ผู้ปกครองของผู้ใช้ที่เป็นเด็ก ได้รับความยินยอม

⁷⁴ In accordance with Article 7.3 GDPR

วิธีการที่ใช้ในการตรวจสอบว่าได้รับความยินยอมจากผู้ถือการยินยอมของผู้ปกครองที่แท้จริง ไม่ล่วงล้ำจนเกินไปและยึดถือหลักการของข้อมูลการป้องกัน เช่นเดียวกับการตรวจสอบอายุเพื่อวัตถุประสงค์ในการจัดตั้งไม่ว่าผู้ใช้จะเป็นเด็กหรือไม่ DPC จะถือว่าควรใช้วิธีการตามสัดส่วนและตามความเสี่ยง สิ่งนี้ทำให้ออกข้อกำหนดสำหรับความเข้มงวดที่มากขึ้น/ระดับความแน่นอน โดยกระบวนการตรวจสอบเฉพาะที่การประมวลผลข้อมูลส่วนบุคคลดำเนินการโดยองค์กรที่มีความเสี่ยงสูงต่อผู้ใช้ตามเกณฑ์ที่ระบุไว้

ซึ่งสอดคล้องกับตำแหน่ง EDPB ที่แนะนำตามสัดส่วนวิธีการตรวจสอบความยินยอมของผู้ปกครองที่อาจรวมถึงการได้รับข้อมูลจำนวนจำกัดจากผู้ปกครองในกรณีที่เป็น (เช่น ติดต่อรายละเอียด) ในสถานการณ์ที่มีความเสี่ยงต่ำ EDPB ระบุว่าในขณะที่การประมวลผลที่มีความเสี่ยงต่ำโดยองค์กรอาจต้องการการตรวจสอบเท่านั้นประกอบด้วยการส่งอีเมลยืนยันให้ผู้ปกครอง (เช่นที่พวกเขาต้องตอบสนอง) การประมวลผลที่มีความเสี่ยงสูงอาจเรียกร้องให้มีความละเอียดรอบคอบมากขึ้นวิธีการตรวจสอบ เช่น การขอพิสูจน์บัตรประชาชน หรือ การขอการชำระเงินของจำนวนเงินโทเคนโดยการโอนเงินผ่านธนาคาร EDPB แนะนำว่าบริการตรวจสอบบุคคลที่สามที่เชื่อถือได้ อาจเป็นคำตอบสำหรับคำถามเกี่ยวกับวิธีการตรวจสอบความยินยอมของผู้ปกครองโดยไม่ต้องรวบรวมข้อมูลส่วนบุคคลมากเกินไป⁷⁵

แม้ว่าสิ่งเหล่านี้จะเป็นตัวแทนของวิธีการบางประเภทที่อาจนำไปใช้เพื่อตรวจสอบการให้ความยินยอมของผู้ปกครอง DPC ถือว่าวิธีการที่ได้รับการรับรองโดยหน่วยงานกำกับดูแลที่เทียบเท่าในอื่น ๆ เขตอำนาจศาลยังสามารถทำหน้าที่เป็นพิมพ์เขียวสำหรับประเภทของวิธีการซึ่งอาจนำไปใช้อย่างเท่าเทียมกันเพื่อวัตถุประสงค์ในการปฏิบัติตาม GDPR ในสหรัฐอเมริกา Federal Trade Commission (FTC)⁷⁶ ได้รับความรับรองต่อไปนี้วิธีการปฏิบัติตามภาระผูกพันที่คล้ายคลึงกัน⁷⁷

1) ลงนามในแบบฟอร์มยินยอมแล้วส่งให้องค์กรทางโทรสาร ไปรษณีย์ หรือการสแกนทางอิเล็กทรอนิกส์

2) การใช้บัตรเครดิต บัตรเดบิต หรือการชำระเงินออนไลน์อื่น ๆ ระบบที่แข็งแกร่งแต่ละแยกการทำธุรกรรมกับเจ้าของบัญชี

⁷⁵ See the EDPB [updated] Guidelines 05/2020 on Consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020, Section 7.

⁷⁶ The FTC has published a “Six Step Compliance Plan” to help online service operators in the US ensure that they fulfil the requirements of the COPPA rule. Step four of this plan sets out a series of acceptable methods for obtaining verifiable consent from parents before collecting personal data from their children.

⁷⁷ Under the Children’s Online Privacy Protection Act (COPPA).

- 3) โทรฟรีเมอร์ที่มีเจ้าหน้าที่ผ่านการอบรม
- 4) การเชื่อมต่อกับบุคลากรที่ผ่านการฝึกอบรมผ่านการประชุมทางวิดีโอ
- 5) จัดเตรียมสำเนาบัตรประจำตัวที่ทางราชการออกให้ซึ่งองค์กรตรวจสอบกับฐานข้อมูลซึ่งจะถูกปล่อยออกมาเมื่อพบสรุปของกระบวนการตรวจสอบ
- 6) ตอบคำถามทำทายตามความรู้ที่จะเป็นเรื่องยากสำหรับคนอื่นที่ไม่ใช่ผู้ปกครองที่จะตอบ หรือ
- 7) การตรวจสอบภาพใบอนุญาตขับรถหรือบัตรประจำตัวที่มีรูปถ่ายอื่น ๆ ที่ส่งโดยผู้ปกครองแล้วเปรียบเทียบกับรูปภาพนั้นกับรูปภาพที่สองที่ส่งมาโดยผู้ปกครองโดยใช้เทคโนโลยีการจดจำใบหน้า

3.2.4.3 วัตถุประสงค์ในการตรวจสอบอายุ

เพื่อไปยังจุดที่สามารถตรวจสอบได้ว่าบิดามารดา/ผู้ปกครองให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของบุตรหลาน อาจเป็นกรณีที่ต้องกรอกออนไลน์ต้องตรวจสอบก่อนว่าผู้ใช้นั้นเป็นเด็กภายใต้ อายุ 16 ปี แม้ว่า GDPR จะไม่มีข้อกำหนดที่ชัดเจนในการยืนยันอายุของผู้ใช้เพื่อระบุว่าผู้ใช้นี้อายุต่ำกว่าเกณฑ์ที่ได้รับคามยินยอมทางดิจิทัลหรือไม่ แต่ส่วนใหญ่แล้วจะเป็นการปฏิบัติตามมาตรา 8 ตามที่กล่าวไว้ข้างต้น GDPR ไม่ได้อ้างถึงการตรวจสอบอายุอย่างชัดเจนและจะไม่พิจารณาถึงสิ่งนี้อาจถือว่าเป็นกลไกการตรวจสอบอายุที่เหมาะสมอย่างเท่าเทียมกัน การพิจารณากลไกดังกล่าวมีรายละเอียดเพิ่มเติมด้านล่าง

จากที่กล่าวไว้ข้างต้น การตรวจสอบอายุเมื่อดำเนินการโดยองค์กรที่สนับสนุนการพึ่งพาความยินยอมภายใต้มาตรา 8 อันเป็นพื้นฐานทางกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคลเป็นเพียงสถานการณ์หนึ่งที่สามารถใช้วิธีการตรวจสอบอายุ DPC ตระหนักดีว่ามีวัตถุประสงค์อื่นสำหรับการตรวจสอบอายุที่ดำเนินการโดยองค์กร รวมถึง

- 1) อนุญาตให้เข้าถึงบริการของตนได้ เช่น เมื่อองค์กรให้บริการสำหรับผู้ใหญ่เท่านั้น ซึ่งตามกฎหมายไม่สามารถให้บริการแก่ผู้ที่มีอายุต่ำกว่า 18 ปีได้ เช่น บริการที่เกี่ยวข้องกับการพนัน
- 2) การให้บริการในรูปแบบที่ “เป็นมิตรกับเด็ก” ซึ่งดึงดูดผู้ชมที่เป็นผู้ใช้แบบผสม กล่าวคือ โดยนำเสนอการตั้งค่า/คุณสมบัติการปกป้องข้อมูลที่ได้รับการปรับปรุงสำหรับผู้ที่เป็นเด็ก โดยสอดคล้องกับข้อกำหนดของพื้นฐานเหล่านี้

3.2.4.4 การตรวจสอบอายุและประสบการณ์การใช้งานของเด็ก

เมื่อตรวจสอบคำตอบของการปรึกษาหารือในปี ค.ศ. 2019 แล้ว DPC ได้ตั้งข้อสังเกตถึงข้อกังวลที่ว่าเด็กอาจมองว่ามาตรการตรวจสอบอายุทางออนไลน์เป็นการขัดขวางพวกเขาจากการเสนอบริการ “เต็มรูปแบบ” ที่สมบูรณ์ยิ่งขึ้น หรือเป็นการขัดขวางไม่ให้พวกเขาเข้าถึงคุณสมบัติอื่น ๆ

ของบริการที่พวกเขาเป็น แสวงหาการใช้งาน⁷⁸ DPC ตั้งข้อสังเกตว่าความเป็นไปได้ของการรับรู้นี้ โดยผู้ใช้ที่เป็นเด็กได้รับการเลี้ยงดูจากผู้เชี่ยวชาญในด้านสิทธิเด็ก ความปลอดภัยของเด็ก และการสนับสนุนเด็ก

ในขณะที่ทางเลือกขององค์กรว่าจะเสนอบริการให้กับใครนั้นอยู่นอกขอบเขตของการปกป้องข้อมูล แต่จุดยืนของ DPC คือข้อกำหนดเฉพาะของมาตรา 8 (รวมถึงความหมายที่เกี่ยวข้องกับการตรวจสอบอายุสนับสนุนการตรวจสอบของความยินยอมของผู้ปกครอง) หรือภาระผูกพันอื่นใดภายใต้ GDPR รวมถึงการปฏิบัติตามข้อกำหนดของพื้นฐานเหล่านี้ ไม่ได้พิสูจน์ให้เห็นถึงความเหมาะสมในการ “ปิดกั้น” เด็กจากประสบการณ์การใช้งานที่หลากหลายเพียงบนพื้นฐานของการปฏิบัติตามข้อกำหนดในการปกป้องข้อมูลโดยอ้างว่า ในทำนองเดียวกัน การจัดหาแนวทางแบบสองระดับที่มีระดับบริการและคุณลักษณะส่วนกลางที่ด้อยกว่าที่เสนอให้กับผู้ใช้ที่เป็นเด็ก ในทางกลับกัน ผู้ใช้ที่เป็นผู้ใหญ่จะได้รับบริการที่เหนือกว่า ซึ่งเสี่ยงต่อการละเมิดสิทธิโดยสมบูรณ์ของเด็กภายใต้ UNCRC ตัวอย่างเช่น ความเสี่ยงนี้จะกระทบต่อสิทธิในการแสดงความคิดเห็นของเด็กอย่างเต็มที่⁷⁹ สิทธิในเสรีภาพในการแสดงออกและเพื่อแสวงหา ทบทวน และเผยแพร่ข้อมูลและความคิดทุกประเภท⁸⁰ และอื่น ๆ แนวทางดังกล่าว โดยที่องค์กรกำหนดมาตรการตรวจสอบอายุเพื่อกรองผู้ใช้เด็กจากผู้ใช้ที่เป็นผู้ใหญ่ ส่งผลให้ระดับการบริการเสื่อมเสีย เสี่ยงต่อการข่มขู่เด็ก “ไต่ด้น” กล่าวอีกนัยหนึ่งที่พวกเขา รู้สึกว่าถูกบังคับให้โกหกเรื่องอายุเพื่อเข้าถึงสิ่งที่พวกเขามองว่าเป็นบริการ “สำหรับผู้ใหญ่” ที่สมบูรณ์ยิ่งขึ้น สิ่งนี้สามารถต่อต้านการผลิตได้ในส่วนขององค์กร ซึ่งอาจส่งผลให้ผู้ที่เป็นเด็กหลีกเลี่ยงมาตรการตรวจสอบอายุและการเข้าถึงบริการที่ไม่ปฏิบัติตามระดับการปกป้องข้อมูลสูงสุดตามที่กำหนดภายใต้ GDPR สำหรับเด็ก

⁷⁸ For example, Google noted in its submission that “In many cases, [children] may be relying on these online service providers as their primary vehicle for access to important educational content and information. Thus, the unintended consequence of locking out users is that [...] they could be deprived of not only access to the service, but access to important content and information that they have stored online such as homework assignments” see in <https://www.dataprotection.ie/sites/default/files/uploads/201909/Submission%20from%20Google.pdf>. Technology Ireland also noted that “Locking users out of services may deprive data subjects of the tools they use to access information or educational resources they need for school, as well as records of prior activity —such as documents or pictures — that they may want to retain.” See in : <https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Submission%20from%20Technology%20Ireland.pdf>. [2021, August 3].

⁷⁹ UNCRC. Article 12.

⁸⁰ UNCRC. Article 13.

DPC พิจารณาว่าประสบการณ์ของผู้ใช้ที่เสนอให้กับผู้ใช้ที่เป็นเด็กควรได้รับการปรับ เพื่อลดความเสี่ยงที่เกิดขึ้นกับเด็กจากการประมวลผลข้อมูลส่วนบุคคลในบริบทของการใช้/ การเข้าถึงบริการให้น้อยที่สุดเท่าที่จะเป็นไปได้ ในประสบการณ์ผู้ใช้โดยรวมและความพร้อมใช้งาน ของคุณสมบัติส่วนกลาง ซึ่งเด็ก ๆ เข้าถึงบริการเป็นหลัก การปกป้องข้อมูลในระดับสูงโดยการ ออกแบบและค่าเริ่มต้นยังช่วยให้มั่นใจได้ว่าเด็กไม่ได้กำหนดเป้าหมายด้วยเนื้อหาที่ไม่เหมาะสมกับวัย เช่น ภาพลามกอนาจาร ซึ่งเด็ก ๆ อธิบายว่าเป็นประสบการณ์เชิงลบ⁸¹

3.2.4.5 อายุผู้ใช้นั้นต่ำ

DPC ยังตั้งข้อสังเกตด้วยว่าเป็นเรื่องปกติในหมู่ ผู้ให้บริการออนไลน์น้อยนิยมสมัคร ขั้นต่ำผู้ใช้อายุ 13 ปี อย่างไรก็ตาม DPC ไม่ได้พิจารณาว่าการตั้งค่าอายุผู้ใช้นั้นต่ำขัดต่อข้อกำหนด ของผู้ให้บริการดังกล่าวในการปฏิบัติตามภาระหน้าที่ของตนที่มีต่อผู้ใช้ที่เป็นเด็กที่อายุต่ำกว่านี้ ซึ่งเด็กมีแนวโน้มที่จะใช้บริการที่เป็นปัญหา ในกรณีที่ผู้ให้บริการกำหนดว่าบริการของตนไม่ได้มีไว้ สำหรับการใช้งานของเด็กที่อายุต่ำกว่าเกณฑ์ ควรดำเนินการเพื่อให้แน่ใจว่ากลไกการตรวจสอบ อายุของตนมีประสิทธิภาพในการป้องกันเด็ก ที่อายุน้อยกว่านั้นจากการเข้าถึงบริการของตน หากองค์กรเห็นว่าไม่สามารถป้องกันเด็กที่อายุต่ำกว่าเกณฑ์ไม่ให้เข้าถึงบริการได้ องค์กรควร ตรวจสอบให้แน่ใจว่ามีมาตรการป้องกันข้อมูลที่มีมาตรฐานเหมาะสมเพื่อปกป้องตำแหน่งของ ผู้ใช้ที่เป็นเด็ก ทั้งที่ต่ำกว่าและสูงกว่าผู้ที่เป็นทางการขององค์กร อายุ เกณฑ์ ซึ่งหมายความว่า ในความเป็นจริงแล้ว เด็กสามารถหรือทำจริง ๆ หลีกเลียงกลไกการตรวจสอบอายุและการเข้าถึง บริการมีภาระผูกพันในองค์กรที่ต้องปฏิบัติตามภาระผูกพันของผู้ควบคุมภายใต้ GDPR และ มาตรฐานและความคาดหวังที่กำหนดไว้ในปัจจัยพื้นฐานเหล่านี้ เกี่ยวกับผู้ใช้ “ที่ยังไม่บรรลุนิติภาวะ” เช่นเดียวกับผู้ใช้ที่อายุต่ำกว่า 18 ปี แม้ว่าพวกเขาจะอายุเกินขั้นต่ำ ดังนั้น DPC ไม่ยอมรับขั้นต่ำ ตามทฤษฎี เกณฑ์อายุของผู้ใช้แทนที่ภาระหน้าที่ของผู้ควบคุม GDPR ขององค์กรที่เกี่ยวข้อง กับผู้ใช้ที่ “ยังไม่บรรลุนิติภาวะ”

ตามที่ได้อธิบายไว้ก่อนหน้านี้ว่าบริการขององค์กรมุ่งไปที่/มีไว้สำหรับหรือมีแนวโน้ม ที่จะเข้าถึงได้โดยเด็ก โดยไม่คำนึงถึงมาตรการตรวจสอบอายุใด ๆ ที่องค์กรปรับใช้ องค์กรควร ตรวจสอบให้แน่ใจว่ามีการใช้มาตรการปกป้องข้อมูลเด็กเป็นการเฉพาะเพื่อเพิ่มระดับการป้องกัน ให้กับผู้ใช้ที่เป็นเด็ก (โดยไม่คำนึงถึง อายุขั้นต่ำที่เป็นทางการของผู้ใช้งาน) ต่อความเสี่ยงที่เกิดจาก การใช้/การเข้าถึงบริการ

⁸¹ “I wasn’t sure it was normal to watch it”: A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people. NSPCC, Children’s Commissioner and Middlesex University London. May 2017.

3.2.4.6 กลไกการตรวจสอบอายุ

พื้นที่เทคโนโลยีของกลไกและเครื่องมือการตรวจสอบอายุยังอยู่ในการพัฒนาอย่างมาก ในฐานะที่เป็นส่วนหนึ่งของการปรึกษาหารือปี 2019 DPC ได้ขอข้อมูลจากอุตสาหกรรมเกี่ยวกับสิ่งที่ถือว่เป็นวิธีการที่เหมาะสมสำหรับการตรวจสอบอายุ อย่างไรก็ตาม การตอบสนองจากอุตสาหกรรมโดยรวมนั้นค่อนข้างจำกัดในแง่ของนวัตกรรม โดยการส่งผลงานจำนวนมากไม่เต็มใจที่จะเสนอคำแนะนำเฉพาะใด ๆ คำแนะนำบางส่วนที่ส่งมามีรายละเอียดอยู่ในแถบด้านข้างความเป็นไปได้อื่น ๆ สำหรับการตรวจสอบอายุรวมถึงมาตรการทางเทคนิค เช่น ประตูลายที่เป็นกลาง การใช้วิธีการบัญชีประดิษฐ์ (เช่น การวิเคราะห์การโต้ตอบของผู้ใช้กับบริการ) เช่นเดียวกับการประกาศตนเอง การระบุอย่างเป็นทางการ และข้อมูลบัญชีที่มีอยู่ ตามที่กล่าวต่อไปด้านล่าง วิธีการที่เหมาะสมที่สุดสำหรับการกำหนดอายุของผู้ใช้จะขึ้นอยู่กับลักษณะของบริการออนไลน์และความเสี่ยงที่เกิดกับเด็กจากการประมวลผลข้อมูล

DPC เห็นว่าท้ายที่สุดแล้ว อุตสาหกรรมจะต้องดำเนินต่อไป สร้างสรรค์สิ่งใหม่ ๆ ในพื้นที่นี้ อย่างไรก็ตาม กลไกการตรวจสอบอายุใด ๆ ที่พัฒนาและใช้งานต้องเป็นไปตามภาระหน้าที่ของการปกป้องข้อมูลโดยการออกแบบและการผิมนัด และต้องอยู่ภายใต้การประเมินผลกระทบต่อ การปกป้องข้อมูลด้วย เพื่อประเมินว่ากลไกที่เป็นปัญหานั้นสอดคล้องกับหลักการปกป้องข้อมูลหรือไม่ โดยเฉพาะอย่างยิ่ง การลดข้อมูล วัตถุประสงค์ ข้อจำกัด ข้อจำกัดในการจัดเก็บ และความปลอดภัย ไม่น่าจะมีวิธีแก้ไขปัญหาการตรวจสอบอายุแบบหนึ่งขนาดกลไกการตรวจสอบอายุที่เหมาะสมมักจะแตกต่างกันไปตามบริบท ขึ้นอยู่กับปัจจัยต่าง ๆ เช่น บริการที่มีให้ และความละเอียดอ่อนของข้อมูลส่วนบุคคลที่กำลังประมวลผล เป็นต้น ไม่ว่าในกรณีใด มาตรการดังกล่าวควรเป็นไปตามสัดส่วนและตั้งอยู่บนแนวทางที่อิงตามความเสี่ยง ซึ่งหมายความว่าควรจะมี ความเข้มงวดมากขึ้น/ ระดับความแน่นอน โดยกระบวนการตรวจสอบเฉพาะที่การประมวลผล ข้อมูลส่วนบุคคลที่ดำเนินการโดยองค์กรมีความเสี่ยงสูงต่อผู้ใช้ตามเกณฑ์ที่ระบุไว้ ตัวอย่างเช่น การประกาศตนเองอาจเหมาะสำหรับการประมวลผลที่มีความเสี่ยงต่ำหรือเมื่อใช้ควบคู่ไปกับ เทคนิคอื่น ๆ ในขณะที่บริการออนไลน์บางอย่างที่มีความเสี่ยงสูงที่เกิดจากการประมวลผลข้อมูล อาจต้องใช้วิธีการตรวจสอบอายุที่เข้มงวดมากขึ้น สิ่งนี้สามารถเกิดขึ้นได้โดยใช้มาตรการทางเทคนิคที่ไม่สนับสนุนการประกาศอายุหรือระบุอายุที่เป็นเท็จ

สุดท้ายนี้ สิ่งสำคัญที่ต้องจำไว้คือการตรวจสอบอายุเป็นเพียงหนึ่งในสองประเภทของ เครื่องมือที่ผู้ใช้บริการออนไลน์อาจใช้เพื่อปฏิบัติตามหลักพื้นฐาน ตามที่ระบุไว้ในตอนเริ่มต้น ทางเลือกอื่นคือ “พื้นที่แห่งการปกป้อง” ทัวทั้งบริการที่ให้การปกป้องข้อมูลในระดับสูงสำหรับ ผู้ใช้ที่เป็นผู้ใหญ่และเด็กโดยไม่แยกความแตกต่างระหว่างสอง

3.2.4.7 เกณฑ์สำหรับแนวทางตามความเสี่ยงการตรวจสอบอายุ

หากองค์กรตัดสินใจที่จะใช้กลไกการตรวจสอบอายุ มีเกณฑ์ขั้นต่ำบางอย่างที่ควรพิจารณาเมื่อกำหนดแนวทาง สิ่งนี้อาจถือเป็นแนวทางที่เหมาะสมสำหรับองค์กรหนึ่งอาจไม่เหมาะสมกับอีกองค์กรหนึ่งโดยสิ้นเชิง รายการต่อไปนี้เป็นประกอบด้วยการเลือกเกณฑ์โดยย่อ⁸² ซึ่งควรนำมาพิจารณาในการนำวิธีการตามความเสี่ยงในการตรวจสอบ ดังนี้

1) ประเภทของข้อมูลส่วนบุคคลที่กำลังประมวลผล เช่น ข้อมูลด้านสุขภาพ รูปภาพ/วิดีโอ ตัวระบุทางเทคนิคออนไลน์ รายละเอียดการติดต่อ (เช่น ชื่อ-นามสกุล/อายุ/ที่อยู่/อีเมลที่อยู่/หมายเลขโทรศัพท์) ข้อมูลเกี่ยวกับความเชื่อทางศาสนาหรือรสนิยมทางเพศ ข้อมูลเกี่ยวกับงานอดิเรกหรือความสนใจ ฯลฯ

2) ความละเอียดอ่อนของข้อมูลส่วนบุคคลดังกล่าว เช่น ข้อมูลส่วนบุคคลประเภทพิเศษ หรือข้อมูลที่ถือว่าละเอียดอ่อนด้วยเหตุผลอื่น เช่น ข้อมูลทางการเงิน ข้อมูลเกี่ยวกับสถานการณ์ของครอบครัว หรือสถานะการเกิด หรือข้อมูลที่รวมเอาข้อมูลของบุคคลที่สาม เช่น สมาชิกในครอบครัวหรือเพื่อน เป็นต้น

3) ประเภทของบริการที่เสนอให้เด็ก เช่น บริการ แพลตฟอร์มการโฮสต์วิดีโอหรือรูปภาพ บริการด้านการศึกษา บริการดูแลสุขภาพหรือสนับสนุนทางสังคม แอปโซเชียลมีเดียที่อำนวยความสะดวกในการเชื่อมต่อกับบุคคลที่รู้จักหรือกับคนแปลกหน้า เว็บ ไซต์เกม แพลตฟอร์มการช้อปปิ้ง ฯลฯ

4) การเข้าถึงข้อมูลส่วนบุคคลที่รวบรวมโดยบุคคลอื่น เช่น ไม่ว่าลักษณะของบริการคือการเผยแพร่หรือทำให้ข้อมูลส่วนบุคคลหรือองค์ประกอบของข้อมูลสามารถเข้าถึงได้ทั่วโลก

5) การประมวลผลข้อมูลส่วนบุคคลเพิ่มเติมรวมถึงการแบ่งปันข้อมูลที่รวบรวมกับองค์กรอื่นและเหตุผลในการทำเช่นนั้นหรือไม่ เช่น เพื่อวัตถุประสงค์ในการโฆษณา การตลาด หรือการสร้างโปรไฟล์โดยองค์กรหรือบุคคลที่สามที่มีการแบ่งปันข้อมูล

วิธีการตรวจสอบอายุที่เข้มงวดที่สุดจะมีความจำเป็นสำหรับบริการออนไลน์เสมอ ซึ่งความเสี่ยงที่เกิดจากการประมวลผลข้อมูลหรือกิจกรรมที่ดำเนินการผ่านบริการดังกล่าวเป็นสิ่งที่ผิดกฎหมายสำหรับเด็กที่จะเข้าร่วม ตัวอย่างเช่น เมื่อองค์กรให้บริการสำหรับผู้ใหญ่เท่านั้น เช่น การพนันซึ่งตามกฎหมายไม่สามารถให้บริการแก่ผู้ที่มีอายุต่ำกว่า 18 ปี

⁸² Some of these criteria take into account certain suggestions which were submitted by participants as part of their responses to in the DPC's public consultation.

3.2.4.8 ความยินยอมในการทำตลาดให้เด็ก

กฎเกณฑ์เกี่ยวกับอายุของความยินยอมทางดิจิทัลมักจะใช้กับข้อความการตลาดทางตรงแบบอิเล็กทรอนิกส์ที่ส่งทาง SMS และอีเมล ซึ่งหมายความว่าไม่มีเด็กที่อายุ 16 ปีขึ้นไปเท่านั้นที่สามารถยินยอมในนามของตนเองเพื่อรับข้อความดังกล่าว สำหรับข้อความการตลาดแบบตรงรูปแบบอื่น ไม่มีข้อกำหนดอายุขั้นต่ำสำหรับ เด็กยินยอมให้ประมวลผลข้อมูลส่วนบุคคลของตนตามทฤษฎีแล้ว นี่หมายความว่าองค์กรสามารถดำเนินกิจกรรมทางการตลาดบางอย่างต่อเด็ก ๆ เมื่อได้รับความยินยอมจากพวกเขา อย่างไรก็ตาม ในกรณีที่ต้องมีการพิจารณาที่จะดำเนินกิจกรรมทางการตลาดให้เด็ก ๆ ก็ควรระมัดระวังเป็นอย่างยิ่งเกี่ยวกับ ทำอย่างนั้น⁸³ องค์กรต้องตรวจสอบให้แน่ใจก่อนว่าความยินยอมจากเด็กที่พึ่งพานั้นเป็นไปตามข้อกำหนดของ GDPR กล่าวคือ ให้โดยเสรี เฉพาะเจาะจง ได้รับแจ้ง และไม่คลุมเครือ ซึ่งหมายความว่าเด็กที่ “เลือก” หรือลงทะเบียนเพื่อรับสื่อการตลาดควรได้รับแจ้งอย่างครบถ้วนเกี่ยวกับการใช้ข้อมูลส่วนบุคคลของตน ในกรณีนี้ ภาระผูกพันด้านความโปร่งใสที่กล่าวถึงในส่วนที่ 3 มีผลบังคับใช้อย่างสมบูรณ์ เด็กควรจะสามารถเข้าใจได้ว่าผลที่ตามมาสำหรับพวกเขาเป็นอย่างไร ในแง่ของอายุ/ความสามารถ อันเป็นผลมาจากการยินยอมให้มีการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการตลาด⁸⁴

⁸³ The DPC also notes Article 19 (4) of the International Chamber of Commerce Advertising and Marketing Communications Code which states that “Personal data collected from children should not be used to address marketing communications to them, the children’s parents or other family members without the consent of the parents.”

⁸⁴ Children front and center. (2020). *Fundamentals for a child-oriented approach to data processing. Draft version for public consultation*. (Online). Available: https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf. [2021, August 3].

3.3 สรุปเปรียบเทียบกฎหมายไทยและกฎหมายต่างประเทศ

ประเทศ ประเด็น	ประเทศไทย (PDPA)	สหรัฐอเมริกา (COPPA)	สหภาพยุโรป (GDPR)	สาธารณรัฐ ประชาชนจีน (PCPPIC)	ประเทศ ไอร์แลนด์ (DPC)
1. นิยามคำว่า 'ข้อมูลส่วนบุคคล'	มีการบัญญัติ ไว้ใน มาตรา 6	มีบัญญัติไว้ใน มาตรา 6501	มีบัญญัติไว้ใน มาตรา 4	ไม่มีคำนิยาม	ไม่มีคำนิยาม
2. มาตรการให้ ความยินยอม	มีกำหนดถึง กรณีของเด็กไว้ใน มาตรา 20	มีกำหนดไว้ใน The FTC's Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business	มีกำหนดถึง กรณีของเด็กไว้ใน มาตรา 8	มีกำหนดถึงกรณี ของเด็กไว้ในข้อ 10	มีกำหนดถึง กรณีของเด็กไว้ใน ข้อ 2,8
3. การประมวลผล	มีการกำหนด ถึงกรณีผู้ ประมวลผล ไว้ในมาตรา 6, 40	มีการพิจารณา จากภาษาเนื้อหา สาระการโฆษณา บนเว็บไซต์ที่ เกี่ยวข้องกับผู้ เด็กอายุของ เด็กเฉลี่ยที่เข้า ไปดูหรือใช้ บริการเว็บไซต์	กระชับ โปร่งใส เข้าใจได้ และ เข้าถึงได้ง่าย โดยใช้ข้อความ ที่ชัดเจนและ ชัดเจน ภาษา โดยเฉพาะอย่างยิ่ง สำหรับข้อมูล ใดๆ ที่ส่งถึงเด็ก โดยเฉพาะ	จะต้องปฏิบัติตาม หลักการของ ความจำเป็นที่ สมเหตุสมผล ความยินยอมที่ได้รับ การบอกกล่าว วัตถุประสงค์ที่ ชัดเจน การประกัน ความปลอดภัย และการใช้กฎหมาย	ไม่แทรกแซง ขัดแย้ง หรือ ส่งผลกระทบต่อ ในทางลบ ใน ทุกระดับของ เด็ก และห้าม ประมวลผล โดยอัตโนมัติ
4. โทษ	ยังไม่มี บทลงโทษใน เรื่องความรับผิดชอบ ของแพลตฟอร์ม หรือเว็บไซต์	โทษปรับ เช่น กรณีปี 2016 อัยการสูงสุด ของนิวยอร์ก พบว่า Viacom, Mattel, Jump Start และ Hasbro ล้วนละเมิด COPPA เนื่องจากพาร์ท	ไม่มีโทษที่ กล่าวถึงกรณี ละเมิดเด็กเป็น การเฉพาะแต่ อย่างไรก็ตามมีการ วางหลักเกณฑ์ ต่างๆ -มีการกำหนด โทษทางปกครอง โดยแบ่งออก 2	ไม่มีบทลงโทษ เฉพาะสำหรับการ ละเมิดในทาง กลับกัน ผู้ฝ่าฝืน บทบัญญัติจะ ได้รับบทลงโทษ รวมถึงบทลงโทษ ทางอาญาภายใต้ กฎหมายและ ข้อบังคับอื่นๆ ที่	ความรับผิดชอบ เจ้าของ แพลตฟอร์ม ความรับผิดชอบ ของคุณ บริษัท ที่ได้รับรายได้ จากการ ให้บริการหรือ ขายบริการผ่าน เทคโนโลยี

ประเทศ ประเด็น	ประเทศไทย (PDPA)	สหรัฐอเมริกา (COPPA)	สหภาพยุโรป (GDPR)	สาธารณรัฐ ประชาชนจีน (PCPPIC)	ประเทศ ไอร์แลนด์ (DPC)
		เนอรัโฆษณาที่ พวกเขาทำงาน ร่วมกับคุกก็ที่ ใช้เพื่อติดตาม ข้อมูล ส่วน บุคคลของผู้ใช้	ฐาน หลักคือ ฐานความคิดที่ หนึ่ง(มาตรา83(4)) โทษปรับทาง ปกครองสูงสุด 10,000,000 ยูโร หรือร้อยละ 2 ของรายได้ทั่ว โลกในปีงบประมาณที่ผ่านมา และฐานที่สอง โทษปรับทาง ปกครองสูงสุด 20,000,000 ยูโร หรือร้อยละ 4 รายได้ทั่วโลก ในงบประมาณที่ ผ่านมา	เกี่ยวข้องกับ เช่น กฎหมายความ ปลอดภัยทางไซ เบอร์และมาตรการ ทางปกครองเกี่ยวกับ บริการข้อมูลทาง อินเทอร์เน็ต	ดิจิทัล และ ออนไลน์จะมี ความเสี่ยงต่อ สิทธิ และ เสรีภาพของเด็ก โดยเฉพาะ ใน กรณีของบริษัท ดังกล่าวใช้การ ตรวจสอบอายุ และ/หรืออาศัย ความยินยอม ของผู้ปกครองใน การประมวลผล DPC คาดหวังว่า จะต้องผู้ให้ บริการควร รับภาระในการ จัดทำมาตรการ ในการระบุตัวตน ของผู้ใช้งาน และการยืนยัน ตัวตนของผู้เยาว์ และโดยเฉพาะ การตรวจสอบ ความยินยอม ของผู้ปกครอง