

ปัญหาการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์  
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

นางสาวชยาภรณ์ มั่นสกุล

เอกัตศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรมหาบัณฑิต  
สาขาวิชากฎหมายเศรษฐกิจ  
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย  
ปีการศึกษา 2565

หัวข้อเอกัตศึกษา ปัญหาการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์  
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โดย นางสาวชยาภรณ์ มั่นสกุล

รหัสประจำตัว 648 01994 34

หลักสูตร ศิลปศาสตรมหาบัณฑิต สาขาวิชากฎหมายเศรษฐกิจ  
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย


หมวดวิชา กฎหมายธุรกิจทั่วไป

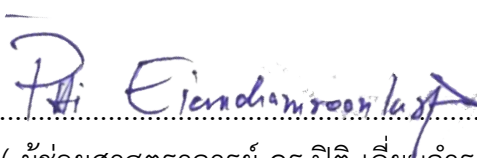
อาจารย์ที่ปรึกษาหลัก ผู้ช่วยศาสตราจารย์ ดร.ศารทูล สันติวาสะ  
อาจารย์ที่ปรึกษาร่วม ผู้ช่วยศาสตราจารย์ ดร.ปิติ เอี่ยมจำรูญลาภ

ปีการศึกษา 2565

---

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้เอกัตศึกษานี้เป็นส่วนหนึ่ง  
ของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรมหาบัณฑิต สาขาวิชากฎหมายเศรษฐกิจ

ลงชื่อ..........อาจารย์ที่ปรึกษาหลัก  
( ผู้ช่วยศาสตราจารย์ ดร.ศารทูล สันติวาสะ )

ลงชื่อ..........อาจารย์ที่ปรึกษาร่วม  
( ผู้ช่วยศาสตราจารย์ ดร.ปิติ เอี่ยมจำรูญลาภ )

## กิติกรรมประกาศ

เอกัตศึกษาดับนี้ไม่อาจสำเร็จได้หากไม่ได้รับความอนุเคราะห์อย่างยิ่งจาก ผู้ช่วยศาสตราจารย์ ดร.ศารทูล สันติवासะ และผู้ช่วยศาสตราจารย์ ดร.ปิติ เอี่ยมจำรูญลาภ ที่ได้รับกรุณาเป็นอาจารย์ที่ปรึกษาแก่ผู้เขียนและได้กรุณาสละเวลาอันมีค่าให้แนวคิดในการศึกษาค้นคว้า เรียบเรียงแนะนำทางด้านวิชาการและแก้ไขปรับปรุงตลอดระยะเวลาหลายเดือนที่ผ่านมาด้วยความเมตตา ผู้เขียนจึงขอน้อมรำลึกถึงความกรุณาที่มีให้ และขอกราบขอบพระคุณมา ณ ที่นี้ด้วยค่ะ

ผู้เขียนขอกราบขอบพระคุณท่านคณะกรรมการผู้ช่วยศาสตราจารย์ ดร.ธิดารัตน์ ศิลปภิมย์สุข ศาสตราจารย์ ทักษิณ ฤกษ์สุต ที่ได้ให้ข้อคิดรวมทั้งแนวทางเสนอแนะเกี่ยวกับการแก้ไขปรับปรุง เพื่อให้เอกัตศึกษาดับนี้มีความสมบูรณ์มากยิ่งขึ้น

ขอขอบพระคุณคณาจารย์คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัยทุกท่านที่กรุณาประสิทธิ์ประสาทความรู้ทางกฎหมายให้แก่ผู้เขียน พร้อมทั้งขอขอบคุณเจ้าหน้าที่คณะนิติศาสตร์ทุกท่าน ที่ให้ความช่วยเหลือและมีน้ำใจในการติดต่อประสานงานให้แก่ผู้เขียนตลอดมา สุดท้ายขอกราบขอบพระคุณบิดา มารดา พี่สาว และเพื่อนๆ สำหรับความรักความเข้าใจและคอยให้กำลังใจสนับสนุนผู้เขียน รวมถึงผู้บังคับบัญชาและเพื่อนร่วมงานทุกท่านที่คอยให้คำปรึกษาและช่วยเหลือในระหว่างการจัดทำเอกัตศึกษานี้ด้วยดีตลอดมา

ผู้เขียนหวังเป็นอย่างยิ่งว่าเอกัตศึกษาดับนี้จะเป็นประโยชน์แก่ผู้สนใจหรือหน่วยงานต่างๆ ไม่มากนักน้อย และหากมีข้อบกพร่องประการใด ผู้เขียนต้องขอภัยมา ณ โอกาสนี้ด้วย

นางสาวชยาภรณ์ มั่นสกุล

## บทคัดย่อ

เอกัตศึกษาฉบับนี้มีวัตถุประสงค์เพื่อศึกษาเรื่องการลบทำลายข้อมูลส่วนบุคคลในทางปฏิบัติบนระบบอิเล็กทรอนิกส์ เพื่อให้คณะกรรมการหรือผู้ควบคุมข้อมูลสามารถปฏิบัติตามขั้นตอนได้ในทางกฎหมาย มาตรา 33 วรรคท้ายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 “คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้” โดยปัจจุบันเทคโนโลยีมีความเจริญก้าวหน้าเป็นอย่างมาก และได้ถูกนำมาใช้งานอย่างแพร่หลาย มีเครือข่ายสื่อสารอินเทอร์เน็ตเป็นส่วนสำคัญในสังคมชีวิตประจำวันของมนุษย์ ทั้งนี้ไม่ว่าจะเป็นการติดต่อสื่อสาร การค้นคว้าหาข้อมูลหรือความรู้ การค้นคว้าหาข้อมูลหรือความรู้ การขายสินค้าหรือบริการหรือธุรกรรมในทางธุรกิจทั้งหลายบนโลกอินเทอร์เน็ต ในปัจจุบันการเก็บข้อมูลส่วนบุคคลของผู้ที่เข้าใช้งานโดยที่บุคคลผู้เข้าใช้งานไม่รู้ตัว Digital Footprint หรือรอยเท้าบนโลกดิจิทัล เปรียบเสมือนประวัติทางพฤติกรรมที่ผู้ใช้งานกระทำในโลกอินเทอร์เน็ต ทั้งการพิมพ์ข้อความ การคลิกเข้าสู่เว็บไซต์ การกดไลก์เพจ หรือการแชร์ข้อความทางโซเชียลมีเดีย ซึ่งข้อมูลดังกล่าวอาจมีผลกระทบต่อด้านสิทธิในความเป็นอยู่ส่วนตัวของเจ้าของข้อมูลได้ หรือในบางกรณีที่มีการจัดเก็บข้อมูลส่วนบุคคลในรูปแบบของข้อมูลอิเล็กทรอนิกส์ จึงทำให้ข้อมูลเหล่านี้สามารถถ่ายโอนกันได้โดยสะดวกรวดเร็ว และปัจจุบันพบว่ามีกรล่วงละเมิดสิทธิของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือเสียหายแก่เจ้าของข้อมูล

จากการศึกษาแนวปฏิบัติของกฎหมายการลบทำลายข้อมูลส่วนบุคคล มาตรา 17 General Data Protection Regulation: GDPR สิทธิของเจ้าของข้อมูลส่วนบุคคลได้เล็งเห็นข้อกำหนดกฎหมายที่ชัดเจน เพื่อเป็นแนวทางในเชิงปฏิบัติของการลบและทำลายข้อมูลบนระบบอิเล็กทรอนิกส์ของประเทศไทยได้ เนื่องจากกฎหมายของประเทศไทยยังไม่มีข้อกำหนดหลักเกณฑ์ที่ชัดเจน ซึ่งส่งผลให้ผู้ควบคุมข้อมูลไม่อาจปฏิบัติตามได้ เช่น การลบทำลายข้อมูลบนระบบอิเล็กทรอนิกส์ แพลตฟอร์ม Digital Footprint ต่างๆ ในทางเทคนิคของระบบซอฟต์แวร์ ควรมีการกำหนดมาตรฐานในทางกฎหมายทางด้านการปฏิบัติและขอบเขต จากการศึกษาแนวปฏิบัติของกฎหมายการลบทำลายข้อมูลส่วนบุคคลของสหภาพยุโรปนั้น กล่าวคือการลบทำลายหรือทำให้ข้อมูลส่วนบุคคล กลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้ การบัญญัติกฎหมายในลักษณะดังกล่าวแตกต่างไปจากถ้อยคำที่ปรากฏ Article 17 of the UK ของ GDPR ที่มีคำว่า “Right to be Forgotten” ควบคู่ไปกับ “Right to Erasure” ดังนั้น มาตรา 33

มาตรา 37 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นบัญญัติของกฎหมายยังขาดแนวทางในทางปฏิบัติในการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ ซึ่งกฎหมายสหภาพยุโรป ได้กำหนดโครงสร้างและรายละเอียดการลบทำลายข้อมูลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลที่มีหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถปฏิบัติตามได้ในทางกฎหมาย โดยแต่ละหน่วยงานหรือองค์กร ต้องเตรียมระบบสนับสนุนระบบไม่ว่าจะเป็นระบบซอฟต์แวร์ แอปพลิเคชัน โปรแกรมเฉพาะเพื่อจัดเก็บฐานข้อมูลและประมวลผลเพื่อให้ข้อมูลสามารถลบออกไปอย่างง่ายดาย โดยมีการดำเนินการโดยระบบไอที ฟังก์ชันต่างๆ ที่เตรียมพร้อมไว้ก่อนหน้า และองค์กรต้องมีโครงสร้างการกำกับดูแลเป็นกระบวนการเพื่อตอบกลับคำขอข้อมูลเพื่อให้แน่ใจว่าองค์กรครอบคลุมพื้นที่ทั้งหมดในระหว่างการลบ โดยปฏิบัติตามขั้นตอนที่ได้มีการวางแผนไว้ตามนโยบายของแต่ละองค์กร เพื่อให้เป็นที่เข้าใจตรงกันแก่พนักงานทุกคน และต้องการยืนยันตัวตนเจ้าของข้อมูล เกี่ยวกับขั้นตอนการจัดเก็บหรือลบ เป็นต้น โดยดำเนินการกรอข้อมูลของเวลาที่กำหนดในฐานะผู้ควบคุมข้อมูลต้องตอบกลับ คำขอให้ลบข้อมูลโดยไม่ชักช้าและไม่เกินหนึ่งเดือนหลังจากได้รับคำขอ

ดังนั้นนักศึกษานี้จึงขอเสนอให้มีการออกกฎหมายลำดับรองจาก มาตรา 33 และมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากมาตรา 33 วรรคท้ายนั้น ได้ระบุว่า “อาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้” ทำให้เจ้าของข้อมูลและผู้ควบคุมข้อมูล ยังไม่สามารถปฏิบัติตามได้และยังไม่อาจทราบได้ว่าถูกกฎหมายหรือไม่ กฎหมายควรมีเพิ่มกฎหมายลำดับรอง เพิ่มบัญญัติรายละเอียดเกี่ยวกับการนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์สามารถปฏิบัติตามกฎหมายได้จากการศึกษา Article 17 of the UK GDPR ของกฎหมายสหภาพยุโรป โดยมีขั้นตอนในการลบทำลายข้อมูลส่วนบุคคลโดย 1) การเตรียมระบบสนับสนุนการลบข้อมูล 2) การสร้างโครงสร้างการกำกับดูแล 3) การวางแผนนโยบายและขั้นตอนต่างๆ 4) การยืนยันตัวตนของเจ้าของข้อมูล 5) การกำหนดค่าใช้จ่าย และ 6) เรื่องของกรอบเวลาของการลบข้อมูล โดยให้กฎหมายได้มีการกำหนดโครงสร้างต่างๆ ในทางปฏิบัติและกำหนดถึงหลักเกณฑ์และรายละเอียดในทางกฎหมายเกี่ยวกับการลบทำลาย หรือทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้

## สารบัญ

กิตติกรรมประกาศ .....	1
บทคัดย่อ.....	2
บทที่ 1 บทนำ.....	1
1.1 ความเป็นมาและความสำคัญของปัญหา .....	1
1.2 วัตถุประสงค์ของการศึกษา.....	2
1.3 สมมติฐานของการศึกษา .....	2
1.4 ขอบเขตการศึกษา.....	3
1.5 วิธีดำเนินการศึกษา .....	3
1.6 ประโยชน์ที่คาดว่าจะได้รับ .....	4
บทที่ 2 .....	5
หลักการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การลบทำลาย ข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ .....	5
2.1 ข้อมูลส่วนบุคคล (Personal Data).....	6
2.1.1 สิทธิมนุษยชน (Human Right) .....	6
2.2 สิทธิที่จะถูกลืม (Right to be Forgotten) .....	6
2.3 แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล.....	8
2.3.1 ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller).....	14
2.4 Digital Footprint .....	15
2.5 Data Erasure.....	15
2.5.1 การเตรียมระบบสนับสนุนการลบข้อมูล.....	16
2.5.2 การสร้างโครงสร้างการกำกับดูแลข้อมูล .....	16
2.5.3 การวางนโยบายและขั้นตอนต่างๆ .....	17
2.5.4 การยืนยันตัวตนของเจ้าของข้อมูล.....	17
2.5.5 ค่าใช้จ่ายในการลบข้อมูล.....	17
2.5.6 ระยะเวลาของการลบข้อมูล .....	17

2.6	ข้อยกเว้นการลบทำลายข้อมูลส่วนบุคคลทั่วไป (Personal Data).....	18
<b>บทที่ 3</b>	<b>การเปรียบเทียบบทกฎหมายไทยและต่างประเทศในการลบทำลายข้อมูลส่วนบุคคล....</b>	<b>20</b>
3.1	การลบทำลายข้อมูลส่วนบุคคลพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 .....	20
3.2	ข้อเปรียบเทียบระหว่างกฎหมายไทยและกฎหมายต่างประเทศ.....	21
3.2.3	กำหนดข้อจำกัดของสิทธิที่จะถูกลืม.....	23
3.3	ตัวบทกฎหมายและแนวปฏิบัติสหภาพยุโรป (GDPR) .....	24
3.4	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 และมาตรา 37.....	51
<b>บทที่ 4</b>	<b>วิเคราะห์ปัญหากฎหมายการลบทำลายข้อมูลส่วนบุคคลของประเทศไทย เกี่ยวกับ</b>	
	<b>แนวทางการแก้ไขการลบและทำลายข้อมูลส่วนบุคคล .....</b>	<b>61</b>
4.1	การบัญญัติถึงตัวผู้ทรงสิทธิที่จะถูกลืม .....	61
4.1.2	เจ้าของข้อมูลส่วนบุคคล (Data Subject) .....	61
4.2	การบัญญัติถึงเนื้อหาการคุ้มครองสิทธิที่จะถูกลืม .....	62
4.3	การลบหรือทำลายข้อมูลเมื่อข้อมูลส่วนบุคคลหมดความจำเป็นที่จะต้องถูกประมวลผลตาม	
	วัตถุประสงค์ .....	63
4.3.1	การพิจารณาข้อเท็จจริงในเรื่องเวลาผ่านไป.....	63
4.3.2	การสิ้นสุดของเวลา.....	64
4.3.3	การกำหนดรายละเอียดเกี่ยวกับการลบทำลายและทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่	
	สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ .....	65
4.4	การบัญญัติถึงข้อจำกัดการใช้สิทธิที่จะถูกลืม .....	67
4.5	การนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลที่ถูกแสดงอินเทอร์เน็ต.....	67
4.6	ตารางแนวปฏิบัติในการลบทำลายข้อมูลส่วนบุคคลภายใต้ GDPR.....	69
4.7	วงกลมความแตกต่างทางด้านมุมมองการลบทำลายข้อมูลของบุคคลทั่วไป ในทางเทคนิคของ	
	ระบบอิเล็กทรอนิกส์ หรือมุมมองในทางกฎหมาย .....	70
<b>บทที่ 5</b>	<b>บทสรุปและข้อเสนอแนะ .....</b>	<b>74</b>
5.1	บทสรุป .....	74
5.2	ข้อเสนอแนะ .....	75
	<b>บรรณานุกรม.....</b>	<b>77</b>

# บทที่ 1

## บทนำ

### 1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันยุคแห่งดิจิทัลหลายสิ่งหลายอย่างถูกขับเคลื่อนผ่านโลกออนไลน์ ปัจจุบันการสื่อสารและส่งผ่านข้อมูลไปได้ทั่วโลกด้วยอินเทอร์เน็ต มาตรฐานการดูแลข้อมูลส่วนบุคคลของผู้ใช้งานได้เข้ามามีบทบาทสำคัญเป็นอย่างมาก<sup>1</sup> ทั้งในแง่ของการดำเนินกิจกรรมส่วนบุคคลหรือการดำเนินการในทางธุรกิจ ดังนั้นจึงให้ความสำคัญต่อการคุ้มครองข้อมูลส่วนบุคคลอย่างยิ่งในการรักษาข้อมูลส่วนบุคคลเป็นอย่างดี อีกทั้งยังสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562<sup>2</sup>

ทั้งนี้แนวคิดดังกล่าวได้ถูกกล่าวถึงในยุโรปตั้งแต่การพัฒนาเทคโนโลยีสารสนเทศ มีความเจริญก้าวหน้าและมีข้อมูลจำนวนมากถูกรวบรวมจัดเก็บในหลายหลายรูปแบบบนอินเทอร์เน็ต ซึ่งทำให้สามารถถูกสืบค้นข้อมูลได้โดยง่ายและในบางกรณีข้อมูลที่อาจถูกผู้อื่นสืบค้นได้ง่าย ก็เป็นผลเสียต่อเจ้าของข้อมูลส่วนบุคคลนั้น ในต่างประเทศจึงมีการกำหนดวิธีการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์อย่างชัดเจน ทั้งการพัฒนาทางด้านเทคโนโลยีนี้ได้นำไปสู่ภัยคุกคามต่อความเป็นส่วนตัว ในหลายๆประเทศได้ตระหนักถึงความสำคัญต่อภัยคุกคามนี้ จึงได้นำไปสู่แนวคิดในการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลภายใต้หลักการคุ้มครองความเป็นส่วนตัว สหภาพยุโรปจึงได้บัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคล Article 17 of the UK GDPR ได้กำหนดสิทธิการลบหรือทำลายเพื่อลดผลเสียต่อภัยคุกคามดังกล่าวว่า เจ้าของข้อมูลมีสิทธิขอให้ผู้ควบคุมลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ และกฎหมายไทยมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้บัญญัติถึงการกำหนดแนวทางปฏิบัติและขั้นตอนวิธีการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์เอาไว้โดยชัดแจ้ง บทบัญญัติดังกล่าวก็ยิ่งขาดความครอบคลุมในบางกรณี อีกทั้งยังขาดการกำหนดวิธีการในทางปฏิบัติ

<sup>1</sup> สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ [ออนไลน์]. แหล่งที่มา : <https://www.etda.or.th/th/PrivacyCenter/Privacy-Protection.aspx> [เข้าถึงเมื่อ 12 กุมภาพันธ์ 2565]

<sup>2</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 มาตรา 37 ราชกิจจานุเบกษา [ออนไลน์]. แหล่งที่มา : <http://www.ratchakitcha.soc.go.th> [เข้าถึงเมื่อ 12 กุมภาพันธ์ 2565]



ที่ชัดเจนเกี่ยวกับการบังคับใช้บทบัญญัติแห่งกฎหมายเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ดังกล่าว<sup>3</sup>

ด้วยเหตุนี้จึงศึกษาแนวทางการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ของกฎหมายที่ยังไม่มีการกำหนดหลักเกณฑ์ที่ชัดเจน จากที่ระบุไว้ในวรรคท้ายค่อนข้างยากต่อการปฏิบัติ ตามในทางกฎหมายของการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ แพลตฟอร์ม ที่เป็นมาตรฐานสากลในการลบทำลายข้อมูลส่วนบุคคล และได้ศึกษาจากการเปรียบเทียบกฎหมายของสหภาพยุโรป Article 17 of the UK GDPR ('right to be forgotten') ที่เกี่ยวข้องกับการบัญญัติกฎหมายและหลักเกณฑ์เกี่ยวกับประเด็นดังกล่าว ตลอดจนคำพิพากษาของศาลที่น่าสนใจ เพื่อให้ทราบกระบวนการในการลบและทำลายข้อมูลส่วนบุคคลในทางกฎหมายและทางปฏิบัติต่อไป

## 1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาแนวทางในการกำหนดวิธีการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
2. เพื่อศึกษาหลักเกณฑ์ในการปฏิบัติตามขั้นตอนในการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์อย่างไรและแนวปฏิบัติของคณะกรรมการในการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

## 1.3 สมมติฐานของการศึกษา

การออกประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลตามมาตรา 33 วรรคท้ายแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีส่วนให้ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถปฏิบัติหน้าที่เพื่อคุ้มครองสิทธิตามมาตรา 33 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ในทางปฏิบัติ

<sup>3</sup> อ.ดร.ปิติ เอี่ยมจารุณุลาก (2564) บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten). หน้า 10

#### 1.4 ขอบเขตการศึกษา

1. ศึกษากระบวนการวิธีในการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ มาตรา 33 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. ศึกษากฎหมายการกำหนดวิธีการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ของต่างประเทศบนระบบอิเล็กทรอนิกส์
3. เพื่อวิเคราะห์กฎหมายต่างประเทศในการกำหนดวิธีการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์และนำมาปรับใช้กับมาตรา 33 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

#### 1.5 วิธีดำเนินการศึกษา

การศึกษาวิจัยนี้ใช้วิธีการวิจัยเอกสารด้วยการค้นคว้าและรวบรวมข้อมูลทางเอกสารที่เกี่ยวข้อง (Documentary Research) โดยเป็นการศึกษาหลักกฎหมาย (Doctrinal Legal Research) และการวิเคราะห์เปรียบเทียบกฎหมาย (Comparative Law) โดยจะทำการศึกษาและวิเคราะห์ข้อมูลระหว่างกฎหมายประเทศไทยและกฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) เอกสารทางวิชาการ วิทยานิพนธ์ วารสารกฎหมาย ฐานข้อมูลทางอินเทอร์เน็ต รวมถึงการวิจัยเอกัตศึกษา โดยต้องดำเนินการให้เข้าช้กับวิจัยเรื่อง “บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) และแนวทางแก้ไขกฎหมายที่เกี่ยวข้อง” (ดร.ปิติ เอี่ยมจำรุงญู เผยแพร่โดยสถาบันพระปกเกล้า 1 ธ.ค. 2565) ซึ่งได้เสนอแนวทางในการออกหลักเกณฑ์การลบทำลายข้อมูลเอาไว้ในเบื้องต้น

เพื่อประโยชน์ในการวิธีกฎหมายในเชิงการเปรียบเทียบ กฎหมายต่างประเทศที่ถูกนำมาเปรียบเทียบได้แก่ กฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) เนื่องจากเป็นกฎหมายที่มีวัตถุประสงค์ และกลไกการคุ้มครองข้อมูลส่วนบุคคลที่คล้ายคลึงและเปรียบเทียบได้กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

## 1.6 ประโยชน์ที่คาดว่าจะได้รับ

เอกัตศึกษานี้สามารถนำไปใช้เพื่อเป็นแนวทางในการปรับใช้การกำหนดวิธีการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. เพื่อเป็นแนวทางในการกำหนดวิธีการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ ให้เป็นไปตามหลักการสากลและหลักกฎหมายในต่างประเทศ โดยเฉพาะอย่างยิ่งกรณีที่มีข้อมูลส่วนบุคคลนั้นอยู่บนระบบอิเล็กทรอนิกส์

2. เพื่อกำหนดหลักเกณฑ์ในการปฏิบัติตามขั้นตอนในการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์เสนอแนะแนวทางในการแก้ไขมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

## บทที่ 2

### หลักการที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์

การลบทำลายข้อมูลบนระบบอิเล็กทรอนิกส์ สามารถทำได้หลากหลายวิธีและมีความแตกต่างกันในการรับรู้และเป็นแนวทางในการปฏิบัติ การดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลให้เข้ากับยุคการพัฒนาของเทคโนโลยีต่างๆ รวมถึงการเกิดขึ้นของเครือข่ายอินเทอร์เน็ตทำให้การดำเนินชีวิตของมนุษย์เปลี่ยนแปลงไป หรือการถ่ายโอนหรือแลกเปลี่ยนข้อมูลข่าวสารที่ทำได้ง่ายมากขึ้น บุคคลทุกคนที่สามารถเข้าถึงอินเทอร์เน็ตได้จะสามารถสืบค้นข้อมูลต่างๆ ได้จากทั่วทุกมุมโลกและสามารถนำข้อมูลที่ได้มาไปเผยแพร่ต่อได้อย่างไม่มีข้อจำกัด ทำให้เกิดความเสี่ยงในการถูกล่วงละเมิดสิทธิในความเป็นส่วนตัวรูปแบบใหม่ ลักษณะของการให้ความคุ้มครองสิทธิในความเป็นส่วนตัวจึงเปลี่ยนแปลงไป โดยมีการพัฒนาแนวความคิดของสิทธิในความเป็นส่วนตัวให้ครอบคลุมถึงความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่อยู่บนอินเทอร์เน็ตด้วย<sup>4</sup>

ส่วนผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นผู้ให้บริการสืบค้นข้อมูลออนไลน์สามารถอาจปฏิบัติหน้าที่เพื่อคุ้มครองสิทธิตามมาตรา 33 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ข้อมูลส่วนบุคคลของตนได้ตามเงื่อนไขที่กฎหมายกำหนด การเข้าถึงข้อมูลของบุคคลอื่นในสังคมเจ้าของข้อมูลส่วนบุคคลที่ข้อมูลส่วนบุคคลของตนจะถูกลบทำลายหรือทำให้ไม่สามารถระบุตัวตนได้เมื่อหมดความจำเป็น ไม่ว่าจะโดยการที่เจ้าของข้อมูลส่วนบุคคลร้องขอหรือผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการหรือโดยปราศจากการร้องขอ เพื่อทำความเข้าใจเนื้อหา วัตถุประสงค์ ซึ่งจะแสดงให้เห็นถึงความสำคัญของเจ้าของข้อมูลส่วนบุคคลและเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลของบุคคลอื่น<sup>5</sup>

<sup>4</sup> ยุคต์กฤต กัณทมนี. การคุ้มครองสิทธิที่จะถูกลืม มหาบัณฑิตจุฬาลงกรณ์มหาวิทยาลัย, 2561.

<sup>5</sup> ผู้ช่วยศาสตราจารย์ดร. ปิติ เอี่ยมจารุญลาภ (2564) บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten). หน้า 34

## 2.1 ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ และนามสกุล วันเดือนปี สถานภาพ เลขบัตรประจำตัวประชาชน เลข หนังสือเดินทาง รหัสพนักงาน อีเมล ภาพถ่าย ลายเซ็น เลขบัญชีธนาคาร ที่อยู่ หมายเลขโทรศัพท์ Line ID IP Address ช่องทางติดต่อในสื่อสังคมออนไลน์ สถานที่ ทำงาน ตำแหน่งงาน ฯลฯ<sup>6</sup>

### 2.1.1 สิทธิมนุษยชน (Human Right)

สิทธิที่มนุษย์ทุกคนมีความเท่าเทียมกัน มีศักดิ์ศรีของความเป็นมนุษย์ สิทธิเสรีภาพ และความเสมอภาคของบุคคลที่ได้รับการรับรอง ทั้งความคิดและการกระทำที่ไม่มีการล่วงละเมิดได้ โดยได้รับการคุ้มครองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย และสนธิสัญญาระหว่างประเทศ<sup>7</sup> ซึ่งประกอบไปด้วยสิทธิตามธรรมชาติและสิทธิที่มีกฎหมายรับรอง เพื่อให้ทุกคนตระหนักในความสำคัญ ของสิทธิมนุษยชนและเป็นแนวทางปฏิบัติต่อกัน ในฐานะเพื่อนมนุษย์อย่างเท่าเทียมกัน โดยตระหนักว่าทุกคนมีสิทธิในชีวิต ในการยอมรับนับถือและในการดำรงชีวิต รวมทั้งในการพัฒนาตนเองตามแนวทางที่ถูกต้อง<sup>8</sup>

## 2.2 สิทธิที่จะถูกลืม (Right to be Forgotten)

ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) การให้ความคุ้มครองข้อมูลส่วนบุคคลโดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล<sup>9</sup> จำกัดการเข้าถึงบุคคลอื่น เผยแพร่และใช้ข้อมูลเกี่ยวกับบุคคลอื่นในมิติของความสัมพันธ์ระหว่างปัจเจกบุคคลกับรัฐนั้น สิทธิในความเป็นอยู่ส่วนตัวมุ่งที่จะจำกัดขอบเขตของอำนาจรัฐในการเข้าแทรกแซงความเป็นส่วนตัวของปัจเจกบุคคล นอกเหนือจากความเป็นส่วนตัวในเชิงของข้อมูลแล้ว ความเป็นส่วนตัวยังมีความหมายรวมถึงการไม่ถูกบุคคลอื่นและรัฐแทรกแซงทางกายภาพและในทางทรัพย์สินอีกด้วย สิทธิในการนำออกจากการแสดงข้อมูลบนเว็บไซต์ของเจ้าของข้อมูลส่วนบุคคลที่อาจเป็นผู้ใช้งาน โปรแกรมสืบค้นข้อมูล ทำการใช้สิทธิดังกล่าวต่อผู้ให้บริการโปรแกรมสืบค้นข้อมูล

<sup>6</sup> กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ผู้ช่วยศาสตราจารย์ดร. สุภัตรา แผนวิจิต มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2565.

<sup>7</sup> คณะกรรมการ สิทธิมนุษยชนแห่งชาติ [ออนไลน์]. แหล่งที่มา: <https://sites.google.com/site/krukarn17825/hlak-siththi-mnusy-chn> [เข้าถึงเมื่อ 27 กุมภาพันธ์ 2565]

<sup>8</sup> พล.อ.ท.ณรงค์ เหล่าธีระเชาวน์ บทความ : สิทธิมนุษยชน. หน้า 3.

<sup>9</sup> จริยธรรมสำหรับคอมพิวเตอร์ธุรกิจ [ออนไลน์]. แหล่งที่มา: [http://katethanpitcha.blogspot.com/2013/08/blog-post\\_9949.html](http://katethanpitcha.blogspot.com/2013/08/blog-post_9949.html) [เข้าถึงเมื่อ 27 กุมภาพันธ์ 2565]

เพื่อให้ทำการนำเอา ลิงค์ที่ปรากฏข้อมูลส่วนบุคคลของตนออกจากหน้าการแสดงผลการค้นหา<sup>10</sup> สิทธินี้มีใช้การลบข้อมูลส่วนบุคคลออกไปโดยสิ้นเชิง ข้อมูลส่วนบุคคลดังกล่าวจะยังคงแสดงหรือปรากฏอยู่บนหน้าเว็บเพจหรือเว็บไซต์ที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลเดิม (Original Controller) อาจกล่าวได้ว่าการดำเนินการของผู้ให้บริการ ระบบสืบค้นออนไลน์ในการลบลิงค์ (Link) แสดงผลการสืบค้นทางอินเทอร์เน็ต (Right to De-Listing) นั้นมีความ แตกต่างจาก “สิทธิที่จะถูกลืมจากโลกดิจิทัล (Right to Digital Oblivion) อย่างแท้จริง<sup>11</sup>

### 2.2.1 สิทธิในการลบข้อมูลส่วนบุคคล (Right to Erasure)

สิทธิในการลบข้อมูลส่วนบุคคลรับรองถึงสิทธิที่เจ้าของข้อมูลส่วนบุคคลอาจใช้สิทธิร้องขอ เพื่อให้มีการลบข้อมูลส่วนบุคคลออกเนื่องจากว่าเจ้าของข้อมูลส่วนบุคคลนั้นไม่ประสงค์จะให้มีการประมวลผลข้อมูลอีกต่อไป โดยสำนักงานคณะกรรมการคุ้มครองข้อมูล (Information Commissioner's Office: ICO) ของสหราชอาณาจักร ได้ให้ความเห็นเอาไว้ว่าสิทธิในการลบข้อมูลนี้เป็นที่รู้จักกันในชื่อ "สิทธิที่จะถูกลืม " โดยได้อธิบายว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ลบข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

- (1) ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมไว้ ไม่มีความจำเป็นต่อวัตถุประสงค์การเก็บรวมอีกต่อไป
- (2) ผู้ควบคุมข้อมูลส่วนบุคคลอาศัยความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเป็นฐานในการประมวลผลแต่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอมแล้ว
- (3) ผู้ควบคุมข้อมูลส่วนบุคคลอาศัยประโยชน์อันชอบด้วยกฎหมายเป็นฐานในการประมวลผล แต่เจ้าของข้อมูลส่วนบุคคลได้คัดค้าน และไม่ปรากฏว่ามีประโยชน์อันชอบด้วยกฎหมายที่สามารถใช้เป็นฐานให้ประมวลผลข้อมูลต่อไป
- (4) ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลเพื่อการตลาดแบบตรง แต่เจ้าของข้อมูลส่วนบุคคลได้คัดค้านการประมวลผลดังกล่าวแล้ว
- (5) ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

<sup>10</sup> ยุคต์กฤต กัณทมนณี (อ้างแล้ว, เจียงอรธที่ 28), หน้า 18.

<sup>11</sup> อรรถกร สุขบุณพันธ์, “สิทธิที่จะถูกลืม (Right to be forgotten): จากคำวินิจฉัยสมัยใหม่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล , หน้า 14.

- (6) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องลบข้อมูลตามกฎหมาย
- (7) ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลของผู้เยาว์เพื่อให้บริการสังคมข้อมูลข่าวสาร (Information Society Services)

อย่างไรก็ตาม ต่างประเทศได้จำแนกสิทธิที่จะถูกลืมออกจากสิทธิในการลบข้อมูลและไม่ถือว่าเป็นสิทธิในการลบข้อมูลส่วนบุคคลนั้นเป็นหนึ่งในสิทธิที่จะถูกลืม ยกตัวอย่างเช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศไม่มีการให้สิทธิที่จะถูกลืมแก่เจ้าของข้อมูลส่วนบุคคล แต่มีเพียงการอนุญาตให้มีการลบข้อมูลส่วนบุคคลออกเมื่อสิ้นสุดระยะเวลาการเก็บรักษาข้อมูล<sup>12</sup>

### 2.2.2 สิทธิในการนำออกจากการแสดงข้อมูลบนเว็บไซต์ (Right to Delisting/Delinking)

สิทธิในการนำออกจากการแสดงข้อมูลบนเว็บไซต์ ครอบคลุมถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลที่อาจเป็นผู้ใช้งาน โปรแกรมสืบค้นข้อมูล ทำการใช้สิทธิดังกล่าวต่อผู้ให้บริการ โปรแกรมสืบค้นข้อมูล เพื่อให้ทำการนำเอาลิงก์ที่ปรากฏข้อมูลส่วนบุคคลของตนออกจากหน้าการแสดงผลการค้นหา<sup>13</sup> อย่างไรก็ตาม สิทธินี้มิใช่การลบข้อมูลส่วนบุคคลออกไปโดยสิ้นเชิง ข้อมูลส่วนบุคคลดังกล่าวจะยังคงแสดงหรือปรากฏอยู่บนหน้าเว็บเพจหรือเว็บไซต์ที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลเดิม (Original Controller) อาจกล่าวได้ว่าการดำเนินการของผู้ให้บริการระบบสืบค้นออนไลน์ในการลบลิงก์ (Link แสดงผลการสืบค้นทางอินเทอร์เน็ต (Right to De-Listing) นั้นมีความแตกต่างจาก "สิทธิที่จะถูกลืมจากโลกดิจิทัล (Right to Digital Oblivion) อย่างแท้จริง<sup>14</sup>

## 2.3 แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล

กำหนดกรอบการทำงานเป็นขั้นตอนการปฏิบัติของผู้ควบคุมข้อมูล (Data Controller) โดยอ้างอิงจากมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เรื่องหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ดังนี้

<sup>12</sup> Nadia Yeo, 'Does Singapore Have a "Right to be Forgotten"?' in David N Alfred, Justin Blaze George, and Adeline Chung (eds), Personal Data Protection Digest (Personal Data Protection Commission 2019), p. 108.

<sup>13</sup> ยุคต์กฤต กัณทมนันท์ (อั้งแล้ว, เชียงอรรถที่ 28), หน้า 18.

<sup>14</sup> อรรถกร สุขปนพันธ์, "สิทธิที่จะถูกลืม (Right to be forgotten): จากคำวินิจฉัยสมัยใหม่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพ ยุโรป" (Krisdika) สืบค้นเมื่อ 6 ตุลาคม พ.ศ. 2564, หน้า 4.

**มาตรา 37 (1)** จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และ ต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่ คณะกรรมการประกาศกำหนด

ให้อธิบายมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลครอบคลุมอย่างน้อย 3 ประเด็นดังนี้ 1) การดำรงไว้ซึ่งความลับ (confidentiality) 2) ความถูกต้องครบถ้วน (integrity) และ 3) สภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล

ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดย มิชอบโดยอย่างน้อยควรประกอบด้วยการดำเนินการ ดังต่อไปนี้

1. มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)

1.1 มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความ มั่นคงปลอดภัย เช่น กำหนดให้มีบันทึกการเข้าออกพื้นที่ กำหนดให้เจ้าหน้าที่รักษา ความปลอดภัยตรวจสอบผู้มีสิทธิผ่านเข้าออก มีการกำหนดรายชื่อผู้มีสิทธิเข้าถึง

ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูก ทำลาย โดยมิชอบ

1.2 มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล ของผู้ใช้งาน (user responsibilities) แบ่งเป็น รูปแบบต่าง ๆ เช่น สิทธิในการเข้า ดู แก้ไข เพิ่มเติม เผยแพร่ และการตรวจสอบคุณภาพข้อมูล ตลอดจนการ ลบทำลาย

2. มาตรการป้องกันด้านเทคนิค (technical safeguard)

a. การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ใน การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

b. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อ ควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เผยแพร่ ตลอดจนการลบทำลาย



- c. จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง

3. มาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)

- 3.1 มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีบันทึกการเข้าออกพื้นที่ มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง มีการล้อมรั้วและล็อกประตูทุกครั้ง มีระบบบัตรผ่านเฉพาะผู้มีสิทธิเข้าออก

ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมีขอบ

- 3.2 กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

**มาตรา 37 (2)** ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

สิ่งที่ดำเนินการอย่างน้อยควรประกอบด้วยการดำเนินการ ดังต่อไปนี้

1. การประเมินก่อนส่งมอบข้อมูล
  - a. ให้ดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และ/หรือ นิติบุคคลรายอื่นนั้น ใช้เพื่อร้องขอข้อมูลส่วนบุคคล
  - b. ให้สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด (เช่น จำเป็นต้องทราบวัน-เดือน-ปีเกิด หรือบ้านเลขที่ หรือไม่ หรือเพียงปี พ.ศ. เกิด และ รหัสไปรษณีย์ ก็เพียงพอ) และ จำเป็นต้องทราบข้อมูลที่ชี้เฉพาะบุคคล (เช่น ชื่อ-นามสกุล เลขประจำตัว 13 หลัก) หรือไม่ หากแปลงข้อมูลที่ชี้เฉพาะบุคคลแทนด้วยรหัสใหม่ที่เป็นนิรนามจะเพียงพอ การนำไปใช้ประโยชน์หรือไม่

## 2. เมื่อส่งมอบข้อมูล

- a. จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อจุดประสงค์การใช้งาน
- b. ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปี ที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน
- c. แจ้งให้บุคคล หรือ นิติบุคคลนั้น ทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้น เช่นเดียวกัน ตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้

## 3. หลังส่งมอบข้อมูล

- a. ติดตามการใช้งานเป็นครั้งคราว เช่น ทุก 3 เดือน 6 เดือน หรือ 1 ปี เพื่อบันทึกสถานะล่าสุดในการใช้งานข้อมูลนั้น หากไม่มีความจำเป็นใช้งานตามวัตถุประสงค์ที่แจ้งไว้เดิม ควรแจ้งให้บุคคล หรือ นิติบุคคลนั้น ลบทำลายข้อมูล
- b. กำหนดวิธีการในการปรับปรุงข้อมูลให้ทันสมัยต่อการใช้งานของผู้ใช้อยู่เสมอ เช่น มีโปรแกรมคอมพิวเตอร์สำหรับเชื่อมต่อปรับปรุงให้ข้อมูลต้นทางและปลายทางมีความทันสมัยเท่ากันโดยอัตโนมัติตลอดเวลา

**มาตรา 37 (3)** จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความในมาตรา 33 วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

สิ่งที่ดำเนินการอย่างน้อยควรประกอบด้วยการดำเนินการ ดังต่อไปนี้

1. ติดตามสม่ำเสมอ (เช่น ทุกสัปดาห์ หรือ ทุกเดือน) ว่าข้อมูลส่วนบุคคลที่อยู่ในความดูแลของตนนั้น (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) มีรายการหรือมีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษาหรือไม่ (ตามที่แจ้งเจ้าของข้อมูลส่วนบุคคล (Data Subject) ไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) หรือตามที่ขอความยินยอมไว้ ทั้งนี้เพื่อ

ดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

2. กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล (หรือขอลอนความยินยอม) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามแต่กรณี
3. การลบทำลายข้อมูล หรือ การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ อาจยกเว้นไม่กระทำก็ได้ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล เช่น

(ก) เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัยหรือสถิติ

(ข) เพื่อการสร้างประโยชน์สาธารณะตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น

(ค) เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

(ง) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์

ทั้งนี้ต้องจัดให้มีมาตรการดูแลข้อมูลที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

**มาตรา 37 (4)** แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

สิ่งที่ดำเนินการอย่างน้อยควรประกอบด้วย การดำเนินการ ดังต่อไปนี้

1. กำหนดตัวพนักงานผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่ตัวแทนของสำนักงานให้ชัดเจน เช่น การส่งอีเมลล์ และ แจ้งทางโทรศัพท์กรณีเป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน
2. กำหนดวิธีปฏิบัติให้ตัวแทนสำนักงานต้องดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายใน 72 ชั่วโมง (นับแต่ทราบเหตุ)
3. การแจ้งเหตุละเมิดอาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้ หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ตัวอย่างการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่น
  - a. ตัวอย่างกรณีความเสี่ยงต่ำ: ข้อมูลส่วนบุคคลถูกเข้ารหัส (ไม่สามารถเปิดอ่านได้หากไม่ทราบรหัสผ่าน) ถูกซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เข้ารหัสจนไม่สามารถใช้งานได้ และไม่ได้ถูกโจรกรรมข้อมูลออกไป อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลมีระบบสำรองรับบริการได้อย่างต่อเนื่อง กรณีนี้ถือได้ว่ามีความเสี่ยงต่ำที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบและไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ
  - b. ตัวอย่างกรณีความเสี่ยงสูง: เว็บไซต์รับสมัครงานออนไลน์ถูกละเมิด โดยผู้โจมตีทำการฝังมัลแวร์เพื่อเข้าถึงข้อมูลใบสมัครงานออนไลน์(ตรวจพบ 1 เดือนหลังมัลแวร์ถูกติดตั้ง) เนื้อหาข้อมูลเป็นข้อมูลทั่วไปเพื่อการสมัครงาน อย่างไรก็ตาม ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึก (เป็นการภายใน) ว่าเคยมีเหตุโจรกรรม พร้อมทั้งแจ้งเหตุดังกล่าว (ภายใน 72 ชั่วโมง) ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย
  - c. ตัวอย่างกรณีความเสี่ยงต่ำ: เจ้าหน้าที่ของหน่วยงานส่งอีเมลล์ไปยังผู้รับผิดชอบ ซึ่งแนบไฟล์รายชื่อผู้เข้าอบรมหลักสูตรภาษาอังกฤษ ซึ่งประกอบไปด้วย ชื่อ-นามสกุลที่อยู่อีเมลล์ และข้อจำกัดในการทานอาหาร ซึ่งมีเพียง 2 คน ใน 15 คนที่ระบุว่า แพ้น้ำตาลแลคโตสในนม (ถือเป็นข้อมูลสุขภาพ) กรณีนี้อีเมลล์ถูกส่งไปยังผู้เข้าอบรมในรุ่นก่อนหน้าแทนที่จะเป็นเจ้าหน้าที่ของโรงแรมที่จัดอาหาร ซึ่งถือเป็นการทำให้ข้อมูลส่วนบุคคลรั่วไหล อย่างไรก็ตามแม้ข้อมูลสุขภาพจะถูกเผยแพร่ไปยังผู้ไม่

เกี่ยวข้อง แต่ก็ไม่สามารถระบุความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้แน่ชัด เช่นนี้ ถือว่าเป็นกรณีที่มีความเสี่ยงต่ำ ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพื่งบั่นทึงเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบและไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

### 2.3.1 ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและจะประมวลผลข้อมูลส่วนบุคคลได้ตามขอบเขตที่ได้รับตามยินยอม หรืออาศัยฐานทางกฎหมายในการประมวลผลอื่นๆ เป็นผู้รับผิดชอบในวางแผนการปฏิบัติตามกฎหมายขั้นสูงสุด โดยทำหน้าที่วางแผนนโยบายกิจกรรม กำหนดวิธีหรือขั้นตอนต่างๆ ในการดำเนินงาน เป็นผู้ตัดสินใจดูแลควบคุม และต้องทำให้เห็นว่องค์กรมีตระหนักและปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลและข้อกำหนดอื่นๆ ตามกฎหมาย<sup>15</sup> แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ควบคุมและผู้ประมวลผลข้อมูลผู้ควบคุมข้อมูล (Data Controller) ผู้ควบคุมข้อมูลจะประมวลผลข้อมูลส่วนบุคคลได้ตามขอบเขตที่ได้รับตามยินยอมหรืออาศัยฐานทางกฎหมายในการประมวลผลอื่นๆ ในการนี้ผู้ควบคุมข้อมูลจะต้องมีมาตรการเชิงเทคนิค (Technical Measure) และมาตรการเชิงบริหารจัดการ (Organizational Measure) เพื่อประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมาย ผู้ควบคุมข้อมูลจะต้องแจ้งเจ้าของข้อมูลเมื่อได้รับข้อมูลส่วนบุคคลไม่ว่าจะได้รับข้อมูล โดยตรงจากเจ้าของข้อมูลหรือได้รับข้อมูลจากแหล่งอื่น ผู้ควบคุมข้อมูลส่วนบุคคลคือบุคคลหรือนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้หรือเผยแพร่ข้อมูลส่วนบุคคล โดยจะมีหน้าที่ในการดำเนินการ โดยมีการจัดให้มีมาตรการในการรักษาความปลอดภัยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลให้ดีและดำเนินการป้องกันไม่ให้มีการใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม และจัดให้มีการลบหรือทำลายข้อมูลส่วนบุคคลหลังจากพ้นระยะเวลาในการเก็บข้อมูลในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลนั้นแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับตั้งแต่ทราบเรื่อง

<sup>15</sup> PDPA คือ [ออนไลน์]. แหล่งที่มา : <https://t-reg.co> [เข้าถึงเมื่อ 12 มิถุนายน 2565]

## 2.4 Digital Footprint

รอยเท้าดิจิทัลอาจจะดูเหมือนไม่มีพิษภัยใดๆ แต่ร่องรอยนี้จะไม่หายไป และจะคงอยู่ตลอดและสามารถติดตามร่องรอยได้ แม้ผู้ใช้งานจะปิดเว็บไซต์หรือออกจากบัญชีการใช้งานไปแล้ว ดังนั้นในวันข้างหน้า ร่องรอยนี้อาจส่งผลดีหรือผลเสียต่อผู้ใช้งานได้ รอยเท้าดิจิทัลยังทำให้เราสูญเสียความเป็นส่วนตัวเนื่องจากคนอื่นยังสามารถเห็นรอยเท้าดิจิทัลของเราได้ หรือแกะรอยได้จากดาต้าเบส ที่ได้บันทึกกิจกรรมออนไลน์ของเราไว้ นอกจากนี้ บริษัทและหน่วยงานที่จัดเก็บข้อมูลของผู้ใช้งาน สื่อดิจิทัลยังหาประโยชน์ทางการค้าจากรอยเท้าดิจิทัลของผู้ใช้งานอินเทอร์เน็ต โดยมอนิเตอร์รอยเท้าดิจิทัลและนำไปวิเคราะห์กลุ่มเป้าหมายทางการตลาด พฤติกรรมการใช้สื่อออนไลน์ และอื่นๆ ผู้ใช้งานอินเทอร์เน็ตจึงควรตระหนักว่า รอยเท้าดิจิทัลเปิดเผยข้อมูลส่วนตัวของเราได้ และข้อมูลเหล่านี้จะคนอื่นสามารถที่จะ ค้นหา เผยแพร่ ทำซ้ำ โขโมย และติดตามได้เพราะร่องรอยนั้นจะไม่หายไปไหนในโลกไซเบอร์<sup>16</sup> บันทึกไว้ รอยเท้าดิจิทัลมี 2 ประเภทคือ 1. Active Digital Footprints รอยเท้าดิจิทัลที่ผู้ใช้งานเจตนาบันทึกไว้ในโลกออนไลน์ เช่น สิ่งที่เราพูดหรือโพสต์ลงในอีเมลหรือในสื่อสังคมออนไลน์, สิ่งที่เรากดไลค์ รีทวีต หรือแชร์, ที่ตั้งสถานที่ ที่เราอยู่หรือเคยไป 2. Passive Digital Footprints รอยเท้าดิจิทัลที่ผู้ใช้งานไม่มีเจตนาบันทึกเอาไว้ในโลกออนไลน์ เช่น สิ่งที่เราเคยคลิกเข้าไป, ประวัติการค้นหาในโลกออนไลน์, การซื้อสินค้าออนไลน์ของเรา IP addressของเรา, การเปิดระบบ GPS ของเรา<sup>17</sup>

## 2.5 Data Erasure

กระบวนการลบข้อมูลที่ได้รับการยอมรับโดยการใช้ซอฟต์แวร์ในการเขียนทับข้อมูลที่มีอยู่ แล้วบนฮาร์ดดิสก์ไดรฟ์หรืออุปกรณ์อื่นๆ เพื่อทำการลบข้อมูลทั้งหมด เป็นการล้างข้อมูลเพื่อให้ยากต่อการกู้ข้อมูลกลับมาใช้ใหม่ได้ แต่ฮาร์ดดิสก์ยังคงสามารถใช้งานได้อยู่ ซึ่งการทำ Data Erasure จะมีการใช้ระยะเวลาในการทำที่ค่อนข้างนาน แต่ถึงแม้การลบข้อมูลจะมีระยะเวลาในการทำที่ค่อนข้างนาน แต่เราจะสังเกตเห็นได้ว่าหลายๆองค์กรในต่างประเทศยังคงให้ความสำคัญและไม่มองข้ามขั้นตอนดังกล่าว เนื่องจากการบังคับใช้ GDPR ในยุโรป ๆ ทำให้องค์กรให้ความสำคัญเรื่องข้อมูลมาก

<sup>16</sup> การลบข้อมูลเป็นบริการ (EaaS) - ตลาดดิจิทัล [ออนไลน์]. แหล่งที่มา : <https://digitalmarketplace.service.gov.uk> [เข้าถึงเมื่อ 5 ตุลาคม 2565]

<sup>17</sup> ดร.สรานนท์ อินทนนท์. ใน เข็มพร วิรุณราพันธ์, ลักษณ์ คงลาภ. การรักษาความปลอดภัยบนโลกไซเบอร์ (Cybersecurity) หน้า 11. บริษัท วอลล์ ออน คลาวด์ จำกัด : ปี 2563

ยิ่งขึ้น ความสำคัญของ Data Erasure การลบข้อมูลให้ถูกวิธี และปลอดภัยต่อการกู้ข้อมูลเพื่อนำกลับมาใช้ใหม่ได้ เป็นสิ่งสำคัญที่จะช่วยลดช่องโหว่ให้กับองค์กร หน่วยงานหรือภาคธุรกิจต่างๆ ในด้านของข้อมูลและยังเป็นการปฏิบัติตามกฎระเบียบ ข้อบังคับด้านการปกป้องข้อมูลจำนวนมาก เพราะบนอุปกรณ์ IT ของหน่วยงานมักมีข้อมูลที่เป็นความลับ ไม่ว่าจะเป็นหมายเลขประกันสังคม หมายเลขบัตรเครดิต รายละเอียดธนาคาร ประวัติทางการแพทย์ ของพนักงานและข้อมูลส่วนบุคคลอื่นๆของลูกค้า เพื่อให้เข้าใจว่าทำไมการทำลายข้อมูลให้ถูกวิธี จึงมีความสำคัญสำหรับธุรกิจ เพื่อป้องกันข้อมูลที่มีความสำคัญจากปัญหาที่จะตามมาข้อดีของการลบข้อมูลให้ถูกวิธีในภาคธุรกิจ<sup>18</sup>

### 2.5.1 การเตรียมระบบสนับสนุนการลบข้อมูล

ระบบแอปพลิเคชันและฐานข้อมูลที่จัดเก็บและประมวลผลข้อมูล ช่วยให้องค์กรสามารถค้นหาและลบข้อมูลได้อย่างง่ายดาย ดังนั้นองค์กรจำเป็นต้องดำเนินการตรวจสอบระบบไอทีที่ปัจจุบันเพื่อดูว่าพวกเขาสามารถจัดการฟังก์ชันได้ หลังจากการตรวจสอบองค์กรสามารถระบุได้ว่าระบบจำเป็นต้องอัปเดตเพื่อให้ทันกับงาน สิ่งสำคัญคือต้องทราบว่า GDPR ไม่อนุญาตให้องค์กรอ้างว่าการลบข้อมูลเป็นไปไม่ได้ ดังนั้นการป้องกันการประมวลผลข้อมูลเพิ่มเติมจึงไม่ถือเป็นการลบ ทางเลือกที่ใกล้เคียงกว่าคือการปกปิดข้อมูลของบุคคล เนื่องจากข้อมูลที่ไม่ระบุตัวตนไม่สามารถเชื่อมโยงกลับไปได้จึงไม่ถือว่าเป็นข้อมูลส่วนบุคคลอีกต่อไป

### 2.5.2 การสร้างโครงสร้างการกำกับดูแลข้อมูล

จะต้องมีโครงสร้างการกำกับดูแลข้อมูลเพื่อตอบกลับคำขอลบข้อมูล การกำกับดูแลข้อมูลฟังก์ชันต่างๆ เช่น การทำแผนกระบวนการของข้อมูลข้ามระบบ แผนก และบุคคลที่สาม นอกจากนี้ยังรับประกันคุณภาพของข้อมูล ดูแลปัญหา เช่น รายการที่ซ้ำกันซึ่งสามารถพบได้ในการสำรองข้อมูล และฉบับพิมพ์โดยเฉพาะอย่างยิ่งข้อมูลบางอย่างอาจเรียกกรองให้มีภาระผูกพันเพิ่มเติม การมีโครงสร้างการกำกับดูแลข้อมูลช่วยให้มั่นใจได้ว่าเรื่องดังกล่าวจะได้รับการดูแลเพื่อให้แน่ใจว่าองค์กรครอบคลุมพื้นที่ทั้งหมดในระหว่างการลบ

<sup>18</sup> Data Erasure สำคัญกับธุรกิจของคุณอย่างไร [ออนไลน์]. แหล่งที่มา : <https://9krpalnm.com/data-erasure> [เข้าถึงเมื่อ 5 มีนาคม 2565]

### 2.5.3 การวางนโยบายและขั้นตอนต่างๆ

GDPR ไม่ได้กำหนดให้องค์กรต้องมีนโยบายหรือขั้นตอนในการดำเนินการ อย่างไรก็ตาม ความเป็นไปได้ที่องค์กรจะกำหนดให้พวกเขาปฏิบัติตามอย่างเต็มที่ นโยบายและขั้นตอนเหล่านี้จะให้ความรู้แก่นักพัฒนาและพนักงานคนอื่นๆ ขององค์กรเกี่ยวกับขั้นตอนที่จำเป็นในวงจรชีวิตการลบข้อมูลการจัดทำเอกสารนโยบายและขั้นตอนเหล่านี้ยังเป็นข้อพิสูจน์ว่าองค์กรปฏิบัติตามข้อผูกพันต่อสิทธิในข้อมูลของแต่ละบุคคล นโยบายและขั้นตอนต้องได้รับการจัดการจากส่วนกลาง เพื่อให้แน่ใจว่ามีความสม่ำเสมอในองค์กร

### 2.5.4 การยืนยันตัวตนของเจ้าของข้อมูล

ก่อนที่ผู้ควบคุมข้อมูลจะสามารถลบข้อมูลของหัวเรื่องได้เมื่อมีการร้องขอพวกเขาจะต้องสามารถยืนยันตัวตนของหัวเรื่องได้ หากผู้ควบคุมข้อมูลมีข้อสงสัยเกี่ยวกับตัวตน สามารถขอข้อมูลเพิ่มเติมเพื่อยืนยันได้ GDPR ไม่ได้ระบุขั้นตอนขององค์กรในการยืนยันตัวตน เช่น หากผู้ควบคุมได้ตรวจสอบตัวตนของหัวเรื่องตามข้อตกลง สามารถยืนยันตัวตนได้ หากผู้ควบคุมข้อมูลต้องการปฏิเสธคำขอลบข้อมูล เนื่องจากข้อกังวลด้านการยืนยันตัวตน จะต้องแจ้งให้บุคคลนั้นทราบ อย่างไรก็ตามในบางกรณีไม่จำเป็นต้องยืนยันตัวตนของเจ้าของข้อมูล นั่นคือกรณีหากข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่ระบุตัวตน ไม่จำเป็นในการประมวลผล

### 2.5.5 ค่าใช้จ่ายในการลบข้อมูล

ตามหลักการแล้วการใช้สิทธิในการลบนั้นไม่มีค่าใช้จ่าย อย่างไรก็ตามหากคำขอไม่มีมูลความจริงหรือมากเกินไปผู้ควบคุมข้อมูลสามารถเรียกเก็บค่าธรรมเนียมภายในช่วงที่เหมาะสมหรือปฏิเสธคำขอได้ คุณสามารถถือว่าคำขอไม่มีมูลความจริงหรือมากเกินไปหากเจ้าของข้อมูลร้องขอให้ลบบ่อยครั้ง

### 2.5.6 ระยะเวลาของการลบข้อมูล

ในฐานะผู้ควบคุมข้อมูลต้องตอบกลับคำขอให้ลบข้อมูลโดยไม่ชักช้าและไม่เกินหนึ่งเดือนหลังจากได้รับคำขอ ในการตอบกลับควรแจ้งให้เจ้าของข้อมูลทราบถึงมาตรการเพื่อตอบสนองต่อคำขอ หากได้รับคำขอที่ซับซ้อนสามารถตอบกลับโดยบอกเจ้าของข้อมูลว่าคุณต้องการเวลามากขึ้นในการ



ทำงานตามคำขอ ในกรณีนี้กำหนดเวลาสามารถขยายได้ไม่เกินสองเดือนหากคุณปฏิเสธคำขอของเจ้าของข้อมูล จะต้องแจ้งให้ทราบภายในหนึ่งเดือนหลังจากได้รับคำขอ

## 2.6 ข้อยกเว้นการลบทำลายข้อมูลส่วนบุคคลทั่วไป (Personal Data)

ข้อยกเว้น ไม่ให้นำมาใช้บังคับกับการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บ รักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) ฐานประวัติศาสตร์/วิจัย หรือ (4) ฐานภารกิจของรัฐ หรือการ ยกขึ้นต่อผู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ข้อจำกัดการคุ้มครองสิทธิที่จะถูกลืม นั้น การบัญญัติข้อยกเว้นตามข้อ 33 วรรคสองของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- จัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ ที่เกี่ยวข้องกับ การศึกษาวิจัยหรือการจัดทำสถิติ
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
- จำเป็นเพื่อปฏิบัติตามสัญญากับเจ้าของข้อมูล เช่น การซื้อขายของออนไลน์ จำเป็นเพื่อประโยชน์สาธารณะ และการปฏิบัติหน้าที่ในการใช้อำนาจรัฐ
- จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลอื่น
- เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล เช่น ส่งข้อมูลพนักงานให้กรมสรรพากรเรื่องภาษี
- การดำเนินกิจกรรมที่ชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของ มูลนิธิ สมาคม องค์กรไม่แสวงหากำไร เช่น เรื่องศาสนาหรือความคิดเห็นทางการเมือง ซึ่งจำเป็นต้องเปิดเผยให้ทราบก่อนเข้าองค์กรนั้น ๆ
- เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล เช่น บุคคลสาธารณะที่มีข้อมูลที่เปิดเผยต่อสาธารณะอยู่แล้วในความยินยอมของเจ้าของข้อมูล
- เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อผู้สิทธิเรียกร้องตามกฎหมาย เช่น เก็บลายนิ้วมือของผู้ที่บุกรุกเพื่อนำไปใช้ในชั้นศาล เป็นต้น
- เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ เกี่ยวกับ เวชศาสตร์ ป้องกันหรืออาชีวเวชศาสตร์ เช่น การเก็บข้อมูลสุขภาพของพนักงานซึ่งเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) องค์กรมักใช้ข้อนี้ในการอ้างสิทธิที่

จำเป็นต้องเก็บข้อมูลนี้ไว้ เป็นต้น / ประโยชน์ด้านสาธารณสุข, การคุ้มครองแรงงาน, การประกันสังคม, หลักประกันสุขภาพแห่งชาติ / การศึกษาวิจัยทางวิทยาศาสตร์, ประวัติศาสตร์, สถิติ, หรือประโยชน์สาธารณะอื่น / ประโยชน์สาธารณะที่สำคัญ<sup>19</sup>

---

<sup>19</sup> Authgear - The Right to Erasure and How You Can Follow It for Your Apps [ออนไลน์]. แหล่งที่มา :

<https://www.authgear.com/post/the-right-to-erasure-and-how-you-can-follow-it-for-your-apps#erasure-process>

[เข้าถึงเมื่อ 8 มีนาคม 2565]

## บทที่ 3

### การเปรียบเทียบบทกฎหมายไทยและต่างประเทศในการลบทำลายข้อมูลส่วนบุคคล

การศึกษาถึงบทบัญญัติแห่งกฎหมายและแนวปฏิบัติหรือมาตรการกำกับดูแลและกรณีศึกษาเกี่ยวกับการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ในประเทศไทยและสหภาพยุโรป ทั้งนี้ การกล่าวถึงบทบัญญัติแห่งกฎหมายของสหภาพยุโรปจะเป็นการวิเคราะห์และเปรียบเทียบกับบทกฎหมายมาตรา 33 และ 37 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีขึ้นเพื่อคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป เพื่อกำหนดหลักเกณฑ์หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไปในการลบและทำลายข้อมูล ในส่วนของการคุ้มครองสิทธิที่จะถูกลืมนั้นถูกสะท้อนผ่านสิทธิในการเรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามมาตรา 33 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการลบทำลายข้อมูลส่วนบุคคลตามมาตรา 37(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

#### 3.1 การลบทำลายข้อมูลส่วนบุคคลพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

นอกจากบทบัญญัติในส่วนของ "สิทธิของเจ้าของข้อมูลส่วนบุคคล" แล้วพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังบัญญัติเรื่องการลบหรือทำลายข้อมูลส่วนบุคคลในส่วนของ "หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล" เอาไว้ในมาตรา 37(3) อีกด้วย โดยบัญญัติว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ "จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมายหรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ให้นำความในมาตรา 33 วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคล อันเป็นการ

ฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้คืนใหม่ทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าจะการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า (1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั่นเอง หรือ (2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย<sup>20</sup> หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการลบทำลายข้อมูลส่วนบุคคลตามมาตรา 37(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นแสดงให้เห็นว่าสิทธิที่จะถูกลืมในระบบกฎหมายไทยนั้นไม่ได้ถูกคุ้มครองเฉพาะกรณีที่เจ้าของข้อมูลส่วนบุคคลเรียกร้องให้มีการลบทำลายข้อมูลส่วนบุคคลเท่านั้น ตัวผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายจะต้องลบทำลายหรือข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นนอกเหนือจากการลบทำลายจากการร้องขอของเจ้าของข้อมูลส่วนบุคคลอีกด้วย<sup>21</sup>

### 3.2 ข้อเปรียบเทียบระหว่างกฎหมายไทยและกฎหมายต่างประเทศ

วิเคราะห์บทบาทของกฎหมายในการคุ้มครองสิทธิที่จะถูกลืมโดยการเปรียบเทียบกฎหมายไทยและกฎหมายต่างประเทศโดยตั้งประเด็นในการวิเคราะห์ ได้แก่ การกำหนดตัวผู้ทรงสิทธิที่จะถูกลืม การกำหนดตัวผู้มีหน้าที่คุ้มครองสิทธิ การกำหนดรายละเอียดการคุ้มครองสิทธิที่จะถูกลืม และการกำหนดข้อจำกัดของสิทธิที่จะถูกลืม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 บัญญัติให้ "เจ้าของข้อมูลส่วนบุคคล" มีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ การบัญญัติให้เจ้าของข้อมูลส่วนบุคคลเป็นผู้ทรงสิทธิ อันเป็นแนวทางการบัญญัติกฎหมายที่สอดคล้องกับ Article 17 of the UK GDPR ซึ่งสามารถกล่าวได้ว่าการที่กฎหมายจะคุ้มครองสิทธิที่จะถูกลืมได้นั้นมีจุดเริ่มต้นจากการที่กฎหมายกำหนดตัวผู้ทรงสิทธิเสียก่อน<sup>22</sup>

<sup>20</sup> Ibid, มาตรา 77

<sup>21</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ราชกิจจานุเบกษา [ออนไลน์]. แหล่งที่มา : <http://www.ratchakitcha.soc.go.th> [เข้าถึงเมื่อ 18 กุมภาพันธ์ 2565]

<sup>22</sup> ปีติ เอี่ยมจำรูญลาภ, 'สิทธิที่จะถูกลืมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562' (2565) 3 วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ หน้า 717

### 3.2.1 การลบหรือทำลายข้อมูลเมื่อข้อมูลส่วนบุคคลหมดความจำเป็นถูกประมวลผลตามวัตถุประสงค์

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศนั้นบัญญัติให้มีการลบทำลายหรือทำให้ข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในกรณีที่ข้อมูลส่วนบุคคล "หมดความจำเป็น" ที่จะต้องถูกใช้ตามวัตถุประสงค์ของการเก็บรวบรวม เช่น GDPR ซึ่งใช้ถ้อยคำว่า "เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นเพื่อการประมวลผลข้อมูลอีกต่อไป" หน่วยงานรัฐหรือองค์กรนอกภาครัฐจะต้องลบหรือหยุดประมวลผลข้อมูล กล่าวได้ว่าแนวทางในการบัญญัติมาตรา 33 และมาตรา 37(3) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 นั้นสอดคล้องกับแนวทางของกฎหมายต่างประเทศในบางประเทศ บทกฎหมายเหล่านี้ถูกบัญญัติขึ้นโดยใช้ถ้อยคำที่มีความยืดหยุ่นและเปิดโอกาสให้มีการปรับใช้กฎหมายให้เหมาะสมกับกรณี ด้วยเหตุนี้ การปรับใช้กฎหมายจึงมีอาจหลีกเลี่ยงการพิจารณาข้อเท็จจริงเป็นรายกรณีซึ่งสามารถแสดงได้ตามตัวอย่างดังต่อไปนี้

(ก) ข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้การพิจารณาว่า "ข้อมูลส่วนบุคคลหมดความจำเป็นหรือไม่และเมื่อใด" นั้นเป็นข้อพิจารณาสำคัญในการคุ้มครองสิทธิที่จะถูกลืม เช่น คดี *Hurbain v. Belgium* แสดงให้เห็นว่าสำนักพิมพ์ (*Le soir*) นั้นมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลเนื่องจากเป็นผู้ทำการเผยแพร่ข้อมูลส่วนบุคคลของคนขับรถซึ่งเป็นต้นเหตุให้เกิดอุบัติเหตุที่ทำให้มีคนเสียชีวิต ศาลได้ทำการวินิจฉัยถึงระยะเวลาได้ผ่านไปนับจากวันที่ได้มีการเผยแพร่ข้อมูลครั้งแรก (โดยศาลได้พิจารณาและชั่งน้ำหนักถึงเสรีภาพในการแสดงความคิดเห็นของหนังสือพิมพ์ด้วย) โดยในคดีนี้ศาลได้สรุปว่าเวลานับจากวันเกิดอุบัติเหตุได้ผ่านมานานแล้วและผู้ก่อเหตุก็ไม่ได้เป็นบุคคลสาธารณะ กรณีไม่ปรากฏคุณค่าของการที่ยังคงมีชื่อและสกุลของบุคคลที่ก่อเหตุในข่าว การเกิดสติของอุบัติเหตุบนท้องถนนนั้นยังคงทำได้โดยไม่ต้องมีชื่อของบุคคลอยู่<sup>23</sup> และเมื่อการกระทำความผิดได้ขึ้นเมื่อนานมาแล้ว เมื่อเวลาผ่านไปก็ไม่มี ความจำเป็นที่สาธารณชนจะต้องเข้าถึงประวัติอาชญากรรมดังกล่าวอีก ในส่วนที่เกี่ยวกับการพิจารณาการสิ้นสุดของเวลาของเวลานั้น สื่อมวลชนย่อมมีเสรีภาพในการนำเสนอข้อมูลข่าวสารต่างๆ ข้อมูลที่สื่อมวลชน เช่น สำนักข่าวนำเสนอโดยผ่านฐานหนังสือพิมพ์ออนไลน์ อาจถูกค้นหาและเข้าถึงโดยบุคคลทั่วไปในสังคม ศาลในคดี *Plaintiff X v. PrimaDanoi* ยอมรับถึงความสำคัญของสิทธิในการรายงานข้อมูล แต่ก็ได้วินิจฉัยว่า "ข้อมูลที่มีความอ่อนไหว

<sup>23</sup> Global Freedom of Expression, Case 57292/16 'Hurbain v. Belgium' (Columbia University, June 2021) accessed 11 March 2022.

(sensitive information) และข้อมูลส่วนตัว (private information) ไม่ควรจะถูกทำให้เข้าถึงได้โดยสาธารณชนโดยปราศจากการจำกัดเวลา เว้นแต่สำนักพิมพ์จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล แม้บทความดังกล่าวจะถูกเผยแพร่โดยชอบด้วยกฎหมายและเคยมีประโยชน์สาธารณะ แต่การที่ยังทำให้บทความนี้สามารถเข้าถึงได้อย่างไม่ได้สัดส่วนก่อให้เกิดผลกระทบต่อสิทธิในความเป็นอยู่ส่วนตัวของบุคคล การบัญญัติโดยใช้ถ้อยคำที่ยืดหยุ่น เช่น เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 33 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ย่อมเปิดโอกาสให้บุคคลที่เกี่ยวข้องสามารถใช้ดุลพินิจให้เหมาะกับกรณี และช่วยเปิดโอกาสให้มีการชั่งน้ำหนักประโยชน์ต่างๆ ที่เกี่ยวข้องและอาจขัดแย้งกันในบางกรณี

(ข) การพ้นระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศนั้นไม่ได้บัญญัติถึงจุดสิ้นสุด ของระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลเอาไว้ในกฎหมาย เช่น ข้อ 11.2(c) ของหลักการคุ้มครองความเป็นส่วนตัวของประเทศออสเตรเลีย (Australia Privacy Principle) ในส่วนที่ว่าด้วยการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล กำหนดให้บุคคลที่ตกอยู่ในบังคับของ AUS PA 1988 ("APP entity") จะต้องดำเนินการใดอันเป็นการสมเหตุสมผลเพื่อทำลายข้อมูลส่วนบุคคลหรือทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลเมื่อข้อมูลนั้นหมดความจำเป็นที่จะถูกประมวลผลตามวัตถุประสงค์ที่ถูกเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นองค์กรสามารถยึดถือเป็นแนวทางในการปฏิบัติให้เป็นตามข้อกำหนดเรื่องการลบข้อมูลส่วนบุคคลได้

### 3.2.3 กำหนดข้อจำกัดของสิทธิที่จะถูกลืม

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศนั้นแสดงให้เห็นอย่างชัดเจนว่าสิทธิที่จะถูกลืมนั้นมิใช่สิทธิเด็ดขาด หากแต่ถูกจำกัดด้วยเงื่อนไขตามที่กฎหมายบัญญัติได้ในหลายประการ ดังนั้น วัตถุประสงค์กฎหมายที่จะถูกใช้เพื่อคุ้มครองสิทธิที่จะถูกลืมย่อมจะต้องบัญญัติถึงข้อจำกัดดังกล่าวด้วยโดยกฎหมายจะต้องเปิดโอกาสให้มีการสร้างความสมดุลระหว่างสิทธิในความเป็นส่วนตัวกับเสรีภาพในการเข้าถึงข้อมูลและการแสดงออกและการสร้างความสมดุลระหว่างความเป็นส่วนตัวและสิทธิในการได้รับการฟื้นฟูกับประโยชน์สาธารณะ<sup>24</sup>

<sup>24</sup> ผู้ช่วยศาสตราจารย์ ดร. ปิติ เอี่ยมจรรย์ลาภ (2564) บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten).

### 3.3 ตัวบทกฎหมายและแนวปฏิบัติสหภาพยุโรป (GDPR)

ตามมาตรา 17 ของ GDPR เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับการลบข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคล และกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้อง "ลบ" โดยไม่ชักช้าเมื่อมีเหตุใดเหตุหนึ่งดังต่อไปนี้

- (a) ข้อมูลส่วนบุคคลไม่จำเป็นอีกต่อไปเมื่อพิจารณาถึงความสัมพันธ์ระหว่างข้อมูลกับวัตถุประสงค์ที่ข้อมูลเหล่านั้นถูกเก็บรวบรวมหรือการประมวลผลด้วยวิธีอื่น ๆ
- (b) ผู้ถูกประมวลผลข้อมูลยกเลิกการยินยอมให้มีการประมวลผลโดยเป็นไปตามข้อ (a) ในอนุมาตรา 1 ของมาตรา 6 หรือข้อ (a) ในอนุมาตรา 2 ของมาตรา 9 และเมื่อไม่มีเหตุผลทางกฎหมายอื่น ๆ รองรับการประมวลผล
- (c) ผู้ถูกประมวลผลข้อมูลแย้งการประมวลผลโดยเป็นไปตามอนุมาตรา 1 ในมาตรา 21 และไม่มีเหตุโดยชอบสำหรับการประมวลผลอื่นใดสำคัญกว่าหรือผู้ถูกประมวลผลข้อมูลแย้งการประมวลผลโดยเป็นไปตามอนุมาตรา 2 ในมาตรา 21
- (d) ข้อมูลส่วนบุคคลถูกประมวลผลโดยมิชอบด้วยกฎหมาย
- (e) ข้อมูลส่วนบุคคลต้องถูกลบเพื่อให้เป็นไปตามพันธกรณีตามกฎหมายในกฎหมายของสหภาพหรือรัฐสมาชิกที่มีอำนาจเหนือผู้ควบคุม
- (f) ข้อมูลส่วนบุคคลถูกเก็บรวบรวมโดยสัมพันธ์กับการเสนอของสมาคมบริการสารสนเทศตามที่ถูกอ้างถึงในอนุมาตรา 1 ของมาตรา 8<sup>25</sup> เมื่อผู้ควบคุมทำให้ข้อมูลส่วนบุคคลเป็นสาธารณะและมีพันธกรณีตามอนุมาตรา 1 ของมาตรา 17 แห่ง GDPR ในการลบข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตามขั้นตอนที่เหมาะสม อันรวมถึงมาตรการทางเทคนิคด้วยโดยพิจารณาถึงเทคโนโลยีที่มีอยู่และค่าใช้จ่ายในการนำมาปฏิบัติร่วมด้วยโดยละเอียดเพื่อแจ้งข้อมูลต่อผู้ควบคุมข้อมูลส่วนบุคคลที่ประมวลผลข้อมูลส่วนบุคคลที่ผู้ถูกประมวลผลข้อมูลได้ขอให้ลบการเชื่อมต่อหรือสำเนาหรือการทำซ้ำใดๆ ของข้อมูลส่วนบุคคลเหล่านั้นโดยผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าว<sup>26</sup>

การบัญญัติให้มีสิทธิในการลบข้อมูล (สิทธิที่จะถูกลืม) ใน GDPR เป็นผลจากปัญหาข้อพิพาทระหว่างเจ้าของข้อมูลส่วนบุคคลที่ประสงค์จะให้มีการลบข้อมูลส่วนบุคคลของตนออกจากระบบการ

<sup>25</sup> โปรตดู นคร เสรีรักษ์ ณรงค์ใจหาญ ประสิทธิ์ ปิวาวัฒนพานิช ศุภเกียรติ ศุภศักดิ์ศึกษาร และนิชานันท์ นันทศิริธรรม, GDPR ฉบับภาษาไทย (บริษัท พี.เพรส จ กัด, ธันวาคม 2562), หน้า 130.

<sup>26</sup> Ibid, หน้า 131.

ค้นหาข้อมูลออนไลน์ในคดีที่ศาลยุติธรรมสหภาพยุโรป (Court of Justice of the European Union: CJEU) ได้ตัดสินเมื่อวันที่ 13 พฤษภาคม ค.ศ. 2014 (คดี Google Spain v AEPD and Mario Costeja Gonzalez) ซึ่งศาลมีคำตัดสินว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้บริการโปรแกรมสืบค้นข้อมูล ลบลิงก์ที่เชื่อมต่อไปยังข้อมูลส่วนบุคคลออกจากรายการแสดงผลที่ปรากฏตามการค้นหาโดยการใช้ชื่อของเจ้าของข้อมูลส่วนบุคคล

### 3.3.1.1 แนวปฏิบัติที่เกี่ยวกับประเภทหรือลักษณะของสิทธิที่จะถูกลืมที่อยู่บนโปรแกรมสืบค้นข้อมูล

หลังจากที่ CJEU ได้มีคำวินิจฉัยในคดี Google Spain v AEPD and Mario Costeja González เจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกให้ผู้ให้บริการสืบค้นข้อมูลออนไลน์ดำเนินการลบ Links ที่เชื่อมต่อไปยังเว็บไซต์จากหน้าแสดงผลการค้นหา ในส่วนของชื่อของเจ้าของข้อมูลส่วนบุคคล นั้น เพื่อประโยชน์ในการสร้างแนวปฏิบัติที่เกี่ยวข้อง EDPB จึงได้มีการประกาศแนวปฏิบัติที่เกี่ยวกับประเภทหรือลักษณะของสิทธิที่จะถูกลืมที่อยู่บนโปรแกรมสืบค้นข้อมูล<sup>27</sup> (Guideline 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR: Guideline 5/2019) โดยได้อธิบายสิทธิที่จะถูกลืมในแง่มุมมองของสิทธิในการร้องขอให้นำออกจากโปรแกรมสืบค้นข้อมูลนั้นมิใช่สิ่งเดียวกับการในการลบข้อมูลส่วนบุคคล<sup>28</sup> โดยระบุว่ากิจกรรมการประมวลผลข้อมูลของโปรแกรมสืบค้นข้อมูลนั้นควรต้องถูกนิยามให้แตกต่างจากการประมวลผลข้อมูลที่ดำเนินการโดยผู้เผยแพร่ข้อมูลที่เป็นบุคคลภายนอก เช่น สื่อต่างๆ (Media Outlets) ที่ให้ข้อมูลข่าวสารออนไลน์<sup>29</sup> เนื่องจากการนำข้อมูลส่วนบุคคลออกจากโปรแกรมสืบค้นข้อมูลนี้เป็นการนำเอาเนื้อหาหรือข้อมูลของ เจ้าของข้อมูลส่วนบุคคลนั้นๆ ออกจากรายการแสดงผลการค้นหาที่เป็นผลการแสดงผลการค้นหาจากการใช้คำค้นหาด้วยชื่อของเจ้าของข้อมูลส่วนบุคคลเท่านั้น แต่เนื้อหาหรือข้อมูลดังกล่าวยังคงสามารถถูกค้นหาด้วยการใช้คำค้นหาอย่างอื่นที่ไม่ใช่ชื่อของเจ้าของข้อมูลส่วนบุคคลเมื่อพิจารณาลักษณะทางเทคนิคของการนำข้อมูลออกจากส่วนการแสดงผลข้างต้น จะเห็นได้ว่าการใช้สิทธินำออกจากโปรแกรมสืบค้นข้อมูลนี้จึงไม่ได้เป็นการใช้สิทธิที่สามารถร้องขอให้ข้อมูลส่วนบุคคลนั้นถูกลบออกไปจากระบบอินเทอร์เน็ตโดยสิ้นเชิง ข้อมูลส่วนบุคคลจะยังคงไม่ถูกลบออกจาก

<sup>27</sup> Guideline 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (Part 1), para 4

<sup>28</sup> Ibid, para 6

<sup>29</sup> Ibid, para 7.



แหล่งข้อมูลทั้งที่เป็นเว็บไซต์และการแสดงผลและหน่วยความจำขนาดเล็กที่มีความเร็วสูงซึ่งเก็บข้อมูลหรือคำสั่งที่ถูกเรียกใช้หรือเรียกใช้บ่อยๆ (Cache) ของผู้ให้บริการโปรแกรมสืบค้นข้อมูลแต่เป็นเพียงการนำผลแสดงการค้นหาออกจากการแสดงการค้นหาบนหน้าโปรแกรมสืบค้นข้อมูลเท่านั้น จึงทำให้เนื้อหาอันเป็นข้อมูลส่วนบุคคลนั้นยังคงอยู่ในความควบคุมของเจ้าของเว็บไซต์ และยังคงอาจเข้าถึงได้โดยสาธารณะแม้ว่าข้อมูลส่วนบุคคลนั้นจะไม่ปรากฏบนผลการแสดงการค้นหาอีกต่อไป

Guideline 5/2019 อธิบายหลักเกณฑ์อันเกี่ยวข้องกับสิทธินำออกจากโปรแกรมสืบค้นข้อมูลออกเป็น ดังนี้(1) เหตุผลที่เจ้าของข้อมูลส่วนบุคคลอาจใช้เพื่อการส่งคำร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูล ไปยังเจ้าของโปรแกรมสืบค้นข้อมูลตามมาตรา 17.1 ของ GDPR โดยที่เจ้าของข้อมูลส่วนบุคคลอาจใช้เหตุผล มากกว่าหนึ่งเหตุผลเพื่ออ้างประกอบการใช้สิทธิร้องขอนั้นได้และ (2) ข้อยกเว้นของการใช้สิทธิขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลตามมาตรา 17.3 ของ GDPR 107 (1) เหตุผลที่เจ้าของข้อมูลส่วนบุคคลอาจใช้เพื่อการส่งคำร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลไปยังเจ้าของโปรแกรมสืบค้นข้อมูลตามมาตรา 17 วรรคหนึ่งของ GDPR.08 Guideline 5/2019 อธิบายว่ามาตรา 17 ของ GDPR กำหนดถึงหลักการทั่วไปในนำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลออกเป็น 6 กรณีซึ่งครอบคลุมกรณี (1) ข้อมูลส่วนบุคคลหมดความจำเป็นต่อวัตถุประสงค์ของการเก็บรวบรวม หรือประมวลผลของผู้ให้บริการโปรแกรมสืบค้นข้อมูลต่อข้อมูลส่วนบุคคล (2) เจ้าของข้อมูลถอนความยินยอม (3) เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล (4) ข้อมูลส่วนบุคคลได้ถูกประมวลผลโดยมิชอบด้วยกฎหมาย (5) ข้อมูลส่วนบุคคลต้องถูกลบออกเพื่อการปฏิบัติหน้าที่ตามกฎหมาย และ (6) เมื่อข้อมูลส่วนบุคคลถูกเก็บรวบรวมอันเนื่องมาจากการเสนอขอของบริการด้านสังคมข่าวสาร

กรณีที่ 1: เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นต่อวัตถุประสงค์ของการเก็บรวบรวม หรือประมวลผลของผู้ให้บริการโปรแกรมสืบค้นข้อมูลต่อข้อมูลส่วนบุคคลนั้น (มาตรา 17 วรรคหนึ่ง (a))<sup>30</sup>

กรณีนี้เป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลนั้นเห็นว่าข้อมูลส่วนบุคคลของตนที่สามารถเข้าถึงได้นั้นไม่มีความจำเป็นต่อการประมวลผลของผู้ให้บริการโปรแกรมสืบค้นข้อมูลอีกต่อไปและมีความประสงค์ให้ข้อมูลส่วนบุคคลของตนถูกนำออกจากการแสดงผลบนโปรแกรมสืบค้นข้อมูล โดยที่เจ้าของข้อมูลสามารถส่งคำร้องไปยังเจ้าของโปรแกรมสืบค้นข้อมูลได้โดยตรงพร้อมผลการค้นหาที่ปรากฏข้อมูลส่วนบุคคลที่ซึ่งเจ้าของข้อมูลส่วนบุคคลค้นพบโดยการใช้ชื่อของตนเป็นคำค้นหา Guideline 5/2019 ได้ให้ตัวอย่างของกรณีที่เจ้าของข้อมูลส่วนบุคคลอาจใช้สิทธินำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลไว้ว่าเป็นกรณีที่ข้อมูลส่วนบุคคลที่บริษัทผู้ควบคุมข้อมูลส่วนบุคคลมีไว้อยู่ในนั้นได้ถูกลบออกจากทะเบียนสาธารณะหรือในกรณีที่ข้อมูลการติดต่อของเจ้าของข้อมูลส่วนบุคคลยังคงปรากฏอยู่บนหน้าเว็บไซต์ของบริษัทแห่งหนึ่งทั้งที่ในปัจจุบันเจ้าของข้อมูลไม่ได้ทำงานในบริษัทดังกล่าวอีกต่อไปแล้ว หรืออาจเป็นกรณีที่ข้อมูลบางอย่างนั้นจำเป็นต้องถูกทำให้เป็นสาธารณะอันเนื่องมาจากการปฏิบัติหน้าที่ตามกฎหมาย โดยที่ข้อมูลนั้นยังคงปรากฏบนสื่อออนไลน์แม้ระยะเวลาในการประกาศหรือทำข้อมูลให้เป็นสาธารณะตามที่กฎหมายกำหนดไว้นั้นจะได้สิ้นสุดลงแล้วก็ตาม นอกจากนี้ ในกรณีที่ข้อมูลส่วนบุคคลที่ปรากฏบนสื่อออนไลน์นั้นเป็นข้อมูลที่ผิดหรือไม่ถูกต้องอันเนื่องมาจากระยะเวลา (Course of Time) หรือข้อมูลเหล่านั้นล้าสมัยไม่เป็นปัจจุบัน (Outdated) เจ้าของข้อมูลส่วนบุคคลก็อาจส่งคำร้องไปยังผู้ใช้บริการโปรแกรมสืบค้นข้อมูลเพื่อให้ดำเนินการนำเอาข้อมูลที่ผิดหรือไม่ถูกต้องนั้นออกจากการแสดงผลบนโปรแกรมสืบค้นข้อมูลได้การใช้สิทธิตามมาตรา 17 วรรคหนึ่ง (a) จะต้องพิจารณาถึงความสมดุลระหว่างการคุ้มครองความเป็นส่วนตัวและประโยชน์ของผู้ใช้อินเทอร์เน็ต เนื่องจากเหตุผลที่สำคัญในการประมวลผลข้อมูลส่วนบุคคลของโปรแกรมสืบค้นข้อมูลนี้มีลักษณะเป็นไปเพื่อให้ผู้ใช้งานอินเทอร์เน็ตสามารถเข้าถึงข้อมูลได้ง่ายขึ้น ดังนั้นในการใช้สิทธิดังกล่าวต้องมีการประเมินว่าการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการกระทำเกินเวลาการเก็บตามวัตถุประสงค์ หรือข้อมูลส่วนบุคคลนั้นล้าสมัยไม่เป็นปัจจุบันหรือไม่ได้ถูกทำให้เป็นปัจจุบันหรือไม่ ทั้งนี้ระยะเวลาในการเก็บข้อมูลส่วนบุคคลไว้ย่อมขึ้นอยู่กับวัตถุประสงค์เดิม (Original Purpose) ในการประมวลผลข้อมูลดังกล่าวด้วย

<sup>30</sup> สิทธิของเจ้าของข้อมูล (Data Subject) ตาม PDPA มีอะไรบ้าง และผู้ประกอบการควรเตรียมพร้อมอย่างไร Apps [ออนไลน์]. แหล่งที่มา :<https://pdpa.pro/blogs/rights-of-data-subject-pdpa>เข้าถึงเมื่อ 20 เมษายน 2565]

กรณีที่ 2 : เมื่อเจ้าของข้อมูลโอนความยินยอมต่อการประมวลผลข้อมูลส่วนบุคคลในมาตรา 6(1)(a)<sup>31</sup> หรือมาตรา 9(2)<sup>32</sup> และไม่มีฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลอื่น<sup>33</sup>

เมื่อเจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของตนแล้ว เจ้าของข้อมูลส่วนบุคคลย่อมมีสิทธิร้องขอให้มีการลบข้อมูลส่วนบุคคลของตนออกเนื่องจากการประมวลผลข้อมูลส่วนบุคคลในกรณีนี้ตั้งอยู่บนฐานของความยินยอม โดยมีข้อสังเกตว่า การให้ความยินยอมในกรณีนี้จะต้องทำ "โดยการเฉพาะ" และต้องเกี่ยวข้องกับการประมวลผลข้อมูลที่จำต้องเป็นไปตามการทำงานของโปรแกรมสืบค้นข้อมูลเท่านั้น ในทางปฏิบัตินั้น เป็นไปได้ว่าผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะทำการขอรับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนที่จะทำการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการทำการอ้างอิง (Referencing Activity) ดังนั้น ไม่ว่าจะกรณีจะเป็นอย่างไรก็ตามหากเมื่อเจ้าของข้อมูลส่วนบุคคลทำการร้องขอให้ยุติการทำการอ้างอิงนั้น (De-Referencing) ย่อมเท่ากับว่าเจ้าของข้อมูลส่วนบุคคลรายดังกล่าวนั้นไม่ประสงค์หรือยินยอมให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูลทำการประมวลผลข้อมูลส่วนบุคคลของตนอีกต่อไปหากเจ้าของข้อมูลส่วนบุคคลทำการถอนความยินยอมการใช้ข้อมูลส่วนบุคคลโดยแสดงเจตนาไปยัง เว็บไซต์โดยเฉพาะ เจ้าของเว็บไซต์นั้นควรแจ้งไปยังผู้ให้บริการโปรแกรมสืบค้นข้อมูลที่ทำกรแสดงผล (Index) ข้อมูลของเจ้าของข้อมูลส่วนบุคคลคนดังกล่าวอยู่ด้วยตามมาตรา 17 วรรคสอง

กรณีที่ 3 : เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตน มาตรา 17 วรรคหนึ่ง (C)<sup>34</sup>

มาตรา 17 วรรคหนึ่ง (c) ของ GDPR กำหนดให้เจ้าของข้อมูลส่วนบุคคลอาจร้องขอให้ทำการลบข้อมูลส่วนบุคคลของตนหลังจากที่ได้ทำการคัดค้านการประมวลผลข้อมูลส่วนบุคคลนั้นตามมาตรา 21.1 แล้วได้ อย่างไรก็ตาม การใช้สิทธิดังกล่าวนี้จำเป็นต้องเป็นกรณีที่ไม่มีเหตุผลอันชอบธรรม (Legitimate Ground) อื่นใดที่อาจแทนที่ได้ โดย GDPR ได้กำหนดการพิจารณาพิสูจน์ที่เอื้อต่อประโยชน์

<sup>31</sup> มาตรา 6.1 (a) บัญญัติว่า การประมวลผลจะชอบด้วยกฎหมายก็ต่อเมื่อและอยู่ในขอบเขตของข้อใดข้อหนึ่งต่อไปนี้ (a) ผู้ถูกประมวลผลข้อมูลได้ ยินยอมให้ประมวลผลข้อมูลส่วนบุคคลของตนเพื่อวัตถุประสงค์เฉพาะอย่างหนึ่งหรือมากกว่า.

<sup>32</sup> มาตรา 9.2 (a) บัญญัติว่า ผู้ถูกประมวลผลได้ให้ความยินยอมอย่างชัดเจนถึงการประมวลผลข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ โดยเฉพาะอย่างใด อย่างหนึ่งหรือมากกว่า เว้นแต่ว่าเมื่อกฎหมายของสหภาพหรือรัฐสมาชิกได้กำหนดการห้ามตามที่อ้างไว้ในอนุมาตรา 1 จะไม่สามารถถูกยกเว้นได้โดยผู้ ถูกประมวลผลข้อมูล.

<sup>33</sup> Guideline 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (Part 1), para 22 to para 25

<sup>34</sup> Ibid, para 26 to para 33

ของเจ้าของข้อมูลส่วนบุคคลโดยที่ถือเป็นหน้าที่ของผู้ให้บริการโปรแกรมสืบค้นข้อมูลที่มีภาระการพิสูจน์และจำต้องแสดงให้เห็นถึงเหตุผลอันชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลที่ไม่อาจปฏิเสธได้นั้นว่ามีอยู่จริง จึงจะทำให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูลสามารถปฏิเสธการใช้สิทธิลบข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลร้องขอได้ ทั้งนี้เหตุผลอันชอบธรรมเช่นว่านั้น จำต้องเป็นเหตุผลอันชอบธรรมที่เหนือกว่าโดยมีลักษณะที่เหนือกว่าประโยชน์รวมถึงสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลเท่านั้น แต่หากผู้ให้บริการโปรแกรมสืบค้นข้อมูล ไม่อาจแสดงให้เห็นถึงเหตุผลอันชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลที่ไม่อาจปฏิเสธได้ เจ้าของข้อมูลส่วนบุคคลก็ชอบที่จะใช้สิทธิร้องขอให้นำข้อมูลเหล่านั้นออกตาม มาตรา 17 วรรคหนึ่ง

จะเห็นได้ว่าการร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลนั้นตั้งอยู่บนพื้นฐานของความสมดุลระหว่างสถานการณ์พิเศษของเจ้าของข้อมูลส่วนบุคคล และเหตุผลอันชอบธรรมที่ไม่อาจปฏิเสธได้ของผู้ให้บริการโปรแกรมสืบค้นข้อมูล โดยแนวปฏิบัติได้อธิบายและยกตัวอย่างของสถานการณ์พิเศษของเจ้าของข้อมูลส่วนบุคคลที่ปรากฏในลักษณะเป็นผลแสดงการค้นหาที่สร้างความเสียหาย หรือทำลายชื่อเสียงของเจ้าของข้อมูลส่วนบุคคลในกรณีดังต่อไปนี้<sup>35</sup>

- เจ้าของข้อมูลส่วนบุคคลมิได้มีบทบาทในชีวิตสาธารณะ
- ข้อมูลพิพาทดังกล่าวมิได้เกี่ยวข้องกับชีวิตการทำงานของเจ้าของข้อมูลส่วนบุคคล แต่กลับกระทบต่อความเป็นส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- ข้อมูลนั้นก่อให้เกิดประทุษวาจา (Hate Speech) การหมิ่นประมาท การพูดให้ร้าย หรือการกระทำ ความผิดที่เกี่ยวกับการแสดงออกอันเป็นปรปักษ์ต่อเจ้าของข้อมูลอันเนื่องมาจากคำสั่งของศาล
- ข้อมูลเป็นข้อมูลที่ได้รับการยืนยันข้อเท็จจริงแต่กลับพบว่าข้อมูลบางส่วนที่ไม่ถูกต้อง
- ข้อมูลที่เกี่ยวกับการกระทำความผิดอาญาของผู้เยาว์ที่เกิดขึ้นในอดีตและก่อให้เกิดความเสียหายแก่ เจ้าของข้อมูล
- ทั้งนี้การใช้สิทธิตามกรณีดังกล่าวนี้พึงต้องพิจารณาถึงสิทธิส่วนบุคคลและสิทธิในข้อมูล ข่าวสารควบคู่กันไปด้วย

<sup>35</sup> Ibid, para 32.

กรณีที่ 4 : เมื่อข้อมูลส่วนบุคคลได้ถูกประมวลผลโดยมิชอบด้วยกฎหมาย (มาตรา 17 วรรคหนึ่ง (d))<sup>36</sup> การประมวลผลโดยมิชอบด้วยกฎหมายอาจตีความได้จากมาตรา 6 ของ GDPR ที่กำหนดลักษณะของการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมายไว้ทั้งหมด 6 กรณี อย่างไรก็ตามการประมวลผลที่ไม่ชอบด้วย กฎหมายอาจให้เป็นหน้าที่ของเจ้าหน้าที่ควบคุมดูแล (Supervisory Authority) ของแต่ละรัฐสมาชิกในการกำหนดและตีความขอบเขตของการประมวลผลที่ไม่ชอบด้วยกฎหมาย โดยการตีความว่าอย่างไร จึงจะเป็นการประมวลผลที่มิชอบด้วยกฎหมายอาจพิจารณาได้จากหลักเกณฑ์อื่นใน Chapter 2 ของ GDPR ได้เช่นเดียวกับการใช้สิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลได้ตามกรณีนี้ เป็นกรณีที่ผู้ให้บริการโปรแกรมสืบค้นข้อมูลไม่อาจแสดงให้เห็นได้ว่าการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลเป็นไปตามการ ประมวลผลที่ชอบด้วยกฎหมาย ทั้งนี้ยังต้องพิจารณาต่อไปด้วยว่าการประมวลผลข้อมูลส่วนบุคคลดั้งเดิมนั้นมีได้ เป็นการประมวลผลข้อมูลส่วนบุคคลที่มิชอบด้วยกฎหมายอีกด้วย หากปรากฏว่าการประมวลผลข้อมูลส่วนบุคคล ดั้งเดิมมีลักษณะที่ไม่เข้าข่ายตามมาตรา 6 ของ GDPR ผู้ให้บริการโปรแกรมสืบค้นข้อมูลก็ไม่อาจอ้างเหตุแห่งการ ปฏิเสธการใช้สิทธิร้องขอให้ นำออกของเจ้าของข้อมูลส่วนบุคคลได้ และเจ้าของข้อมูลส่วนบุคคลย่อมมีสิทธิร้อง ขอให้ นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลได้

กรณีที่ 5 : เมื่อข้อมูลส่วนบุคคลต้องถูกลบออกเพื่อการปฏิบัติหน้าที่ตามกฎหมาย (มาตรา 17 วรรคหนึ่ง (e))<sup>37</sup> สิทธิในการนำออกจากโปรแกรมสืบค้นข้อมูลตามมาตรา 17 วรรคหนึ่ง (e) ของ GDPR รวมถึงกรณีเป็น หน้าที่ตามกฎหมายที่อนุญาตให้เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ทำการลบผลแสดงการค้นหาข้อมูลส่วนบุคคลของตนเนื่องจากการปฏิบัติหน้าที่ให้เป็นไปตามกฎหมาย โดยอาจเป็นกรณีที่ผู้ให้บริการสืบค้นออนไลน์ นั้นมีหน้าที่ต้องปฏิบัติตามกฎหมายอันเป็นผลมาจากคำสั่งที่ออกโดยกฎหมายของรัฐหรือของสหภาพยุโรป ซึ่งอาจเรียกได้ว่าเป็นหน้าที่ตามกฎหมายที่ต้องปฏิบัติตามกฎหมาย หรืออาจเป็นกรณีที่ผู้ให้บริการโปรแกรมสืบค้นข้อมูลได้ ฝ่าฝืนระยะเวลาในการเก็บรักษาข้อมูล อย่างไรก็ตามสำหรับระยะเวลาในการเก็บรักษาข้อมูลที่ Guideline 5/2019 ได้ให้ตัวอย่างไว้ นั้น อาจเป็นกรณีที่มีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลไว้เป็นลายลักษณ์อักษร แต่มีการละเมิดหรือไม่ปฏิบัติตาม ระยะเวลาดังกล่าว ซึ่งกรณีตัวอย่างดังกล่าวนี้มีลักษณะที่เกี่ยวข้อง

<sup>36</sup> Ibid, para 34 to para 36.

<sup>37</sup> Ibid, para 37 to para 38.

กับไฟล์สาธารณะมากกว่าโดยที่อาจครอบคลุม ไปถึงกรณีที่เกี่ยวข้องกับข้อมูลที่ไม่ได้ทำให้เป็นนิรนาม หรือข้อมูลที่ระบุตัวตนที่มีสภาพพร้อมใช้งานบนข้อมูลเปิด (Open Data)<sup>38</sup>

กรณีที่ 6 : เมื่อข้อมูลส่วนบุคคลถูกเก็บรวบรวมอันเนื่องมาจากการเสนอของบริการด้านสังคมข่าวสาร ต่อเด็ก ตามที่ถูกต้องถึงใน มาตรา 8(1) (มาตรา 17 วรรคหนึ่ง (f))<sup>39</sup>

Guideline 5/2019 ได้อ้างอิงนิยามของคำว่า “บริการด้านสังคมข่าวสาร” มาจาก Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 ที่ได้กำหนดนิยาม ของบริการด้านสังคมข่าวสารเอาไว้ว่าเป็นการให้บริการใด ๆ ที่โดยปกติแล้วมุ่งให้มีการตอบสนองเพื่อการให้บริการ ตามที่ได้รับกรร้องขอระหว่างบุคคลซึ่งอยู่ห่างกันโดยระยะทาง<sup>40</sup> กรณีจึงมีความเป็นไปได้ว่าลักษณะของกิจกรรม ของผู้ให้บริการโปรแกรมสืบค้นข้อมูลตกอยู่ในบังคับของมาตรา 17 วรรคหนึ่ง (f) ของ GDPR แม้ผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะไม่ได้ให้ความสนใจว่าข้อมูลส่วนบุคคลที่แสดงผลนั้นเป็นของข้อมูล ส่วนบุคคลของเด็กหรือไม่ แต่ก็ก็เป็นหน้าที่รับผิดชอบ โดยเฉพาะและผู้ให้บริการโปรแกรมสืบค้นข้อมูล ต้องนำข้อมูลที่เกี่ยวกับเด็กออกจากระบบการสืบค้นเมื่อเจ้าข้อมูลส่วนบุคคลหรือผู้มีอำนาจใช้สิทธิคัดค้านการประมวลผล ข้อมูลทำการคัดค้านการประมวลผลข้อมูลส่วนบุคคล และร้องขอให้นำข้อมูลออกตามมาตรา 17 วรรคหนึ่ง (c) กรณีดังกล่าว จึงเป็นการยอมรับว่าสถานะของการเป็นเด็กนั้นถือเป็นเหตุผลที่เป็นสถานการณ์พิเศษของเจ้าของข้อมูลส่วนบุคคลได้ ตามมาตรา 21 ของ GDPR และยังเป็นกรคุ้มครองสิทธิประโยชน์ของเด็กที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของเด็ก ตามมาตรา 38 ของ GDPR อีกด้วย เช่นนี้ จึงต้องพิจารณาถึงการประมวลผลข้อมูลส่วนบุคคลของเด็กเดิมของผู้ควบคุมข้อมูลส่วนบุคคล ประกอบกับระยะเวลาเริ่มต้นของการประมวลผลข้อมูลส่วนบุคคลโดย เว็บไซต์เดิมเมื่อเจ้าของข้อมูลทำการร้องขอให้นำข้อมูลออก อีกด้วย

แนวการปฏิบัติเกี่ยวกับการนำข้อมูลส่วนบุคคลออกจากโปรแกรมสืบค้นข้อมูลทั้ง 6 กรณี ตามที่ปรากฏใน Guideline 5/2019 นั้นแสดงให้เห็นว่าผู้ให้บริการโปรแกรมสืบค้นข้อมูลนั้นเป็นผู้มีบทบาทสำคัญในการดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเพื่อการคุ้มครองสิทธิที่จะถูกลืมตามมาตรา 17 ของ GDPR เนื่องจากผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะต้องพิจารณาว่าจะดำเนินการลบ

<sup>38</sup> Ibid, para 38.

<sup>39</sup> Ibid, para 39 to para 41

<sup>40</sup> Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015, Article 1 para 1

หรือทำลายข้อมูลตามคำร้องหรือไม่ กรณีที่ 1 นั้นผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะต้องพิจารณาถึงความจำเป็นต่อวัตถุประสงค์ของการเก็บรวบรวม หรือประมวลผลของผู้ให้บริการโปรแกรมสืบค้นข้อมูลต่อข้อมูลส่วนบุคคลนั้นซึ่งจะต้องพิจารณาความจำเป็นเป็นรายกรณีและรับผิดชอบการขังน้ำหนักความสมดุลระหว่างการคุ้มครองความเป็นส่วนตัวและประโยชน์ของผู้ใช้อินเทอร์เน็ต

ส่วนกรณีที่ 2 นั้นแสดงให้เห็นว่าผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะต้องพิจารณาถึงรูปแบบและลักษณะของการ "ถอนความยินยอม" ของเจ้าของข้อมูลส่วนบุคคลซึ่งรวมไปถึงการร้องขอให้ยุติการทำการอ้างอิงถึงนั้น (De-Referencing) ด้วย นอกจากนี้

ผู้ให้บริการโปรแกรมสืบค้นข้อมูลยังมีหน้าที่ที่จะต้องประสานงานกับเว็บไซต์ซึ่งรับการแสดงผลจากเจ้าของข้อมูลส่วนบุคคลอีกด้วยผู้ให้บริการโปรแกรมสืบค้นข้อมูลมีภาระหน้าที่ในการพิสูจน์ว่าตนมีเหตุผลอันชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลที่ไม่อาจปฏิเสธ Compelling Legitimate Ground หากเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตน หรือแสดงให้เห็นได้ว่าการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลเป็นไปตามการประมวลผลที่ชอบด้วยกฎหมายในกรณีที่จะต้องมีการลบข้อมูลเนื่องเป็นการประมวลผลข้อมูลส่วนบุคคลที่ไม่ชอบด้วยกฎหมาย

นอกจากนี้ ผู้ให้บริการโปรแกรมสืบค้นข้อมูลยังต้องตรวจสอบหน้าที่ของตนในการลบข้อมูลส่วนบุคคลตามกฎหมายซึ่งอาจเกิดขึ้นในกรณีที่ได้รับคำสั่งโดยชอบด้วยกฎหมาย การสิ้นระยะเวลาการเก็บข้อมูลส่วนบุคคลหรือหน้าที่ในนำข้อมูลที่เกี่ยวกับเด็กออกจากระบบการสืบค้นซึ่งปรากฏตามกรณีที่ 5 และกรณีที่ 6 ของ Guideline 5/2019 จากกรณีทั้ง 6 นี้ สามารถสรุปได้ว่าการคุ้มครองสิทธิที่จะถูกลืมในกรณีที่ข้อมูลส่วนบุคคลถูกแสดงผ่านระบบการสืบค้นออนไลน์ในทางปฏิบัตินั้นมีความจำเป็นที่ผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์ตลอดจนผู้ให้บริการเว็บไซต์ นั้นจะต้องเข้าใจถึงบทบาทและหน้าที่ของตนอย่างชัดเจน

### 3.3.2.1 มาตรการบังคับตามกฎหมายสภาพบังคับในโลกดิจิทัล

GDPR Article 3 เน้นย้ำถึงสภาพบังคับใช้ทั่วโลกของกฎหมายฉบับนี้ต่อการประมวลผลข้อมูลของบุคคลที่อยู่ในสหภาพยุโรปในโดยไม่คำนึงถึงว่าการประมวลผลข้อมูลในทางปฏิบัติจะได้กระทำในเขตพื้นที่ของสหภาพยุโรปหรือไม่ รวมตลอดถึงเปิดช่องให้มีการใช้บังคับ GDPR ต่อผู้ประมวลผลข้อมูลที่มีที่ตั้งอยู่นอกเขตพื้นที่สหภาพยุโรปแต่ตกอยู่ใต้บังคับกฎหมายของประเทศสมาชิกเนื่องจากสภาพบังคับตามกฎหมายระหว่างประเทศแผนกคดีเมือง เช่น มีความตกลงระหว่างประเทศ

ระหว่างกัน GDPR ยังได้กำหนดมาตรการบังคับตามกฎหมายที่เพิ่มความเข้มข้นและสอดคล้องกันทั่วทั้งสหภาพยุโรป ยกตัวอย่างเช่น มาตรการเกี่ยวกับโทษปรับทางปกครอง ซึ่งใน Article 83 วรรคห้า (b) นั้นสามารถปรับใช้ในการบังคับให้ผู้ประมวลผลข้อมูลที่ทำผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนของ right to be forgotten ตาม Article 17 ต้องรับโทษปรับทางปกครองไม่เกิน 20 ล้านยูโร หรือไม่เกินร้อยละ 4 ของผลประกอบการรวมรายปีทั่วโลกของผู้ประมวลผลข้อมูลรายนั้น ตามแต่จำนวนใดจะสูงกว่า อีกทั้งมาตรการต่าง ๆ ตาม GDPR นั้นมีผลบังคับใช้ได้โดยทันทีในทุกประเทศอย่างสอดคล้องกันเนื่องจากถือเป็นส่วนหนึ่งของกฎหมายภายในของทุกประเทศสมาชิกโดยอัตโนมัติ Article 77 และ Article 79 ยังเพิ่มการอำนวยความสะดวกในการบังคับใช้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลโดยได้ยืนยันหลักการใหม่เกี่ยวกับสิทธิที่จะยื่นข้อร้องเรียนและได้รับมาตรการเยียวยาทางศาลที่มีประสิทธิภาพ โดยกำหนดให้เจ้าของข้อมูลส่วนบุคคลสามารถยื่นข้อร้องเรียนหรือเริ่มกระบวนการในชั้นศาลต่อองค์กรคุ้มครองข้อมูลส่วนบุคคลหรือศาลที่ตนมีภูมิลำเนาอยู่ได้ตามลำดับ ยิ่งกว่านั้น ตาม Article 4(17) ประกอบ Article 27 ได้กำหนดหน้าที่ให้ผู้ประมวลผลข้อมูลที่ตั้งอยู่นอกสหภาพยุโรปจะต้องจัดตั้งตัวแทนขึ้นภายในเขตพื้นที่ของสหภาพยุโรปทั้งนี้ เพื่อประกันการบังคับใช้มาตรการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพผ่านทางตัวแทนที่ผู้ประมวลผลข้อมูลดังกล่าวจัดตั้งขึ้นภายในเขตพื้นที่ของสหภาพยุโรปได้ต่อไป<sup>41</sup>

โดยสรุปอาจพิจารณาในเบื้องต้นได้ว่าสิทธิที่จะถูกลืม หรือ right to be forgotten นั้นกำลังอยู่ในระหว่างพัฒนาโดยประเทศสมาชิกสหภาพยุโรป จากสิทธิอย่างแคบเฉพาะการลบ link แสดงผลการค้นหาของผู้ให้บริการ search engine ที่ได้รับการรับรองผ่านคำวินิจฉัยของ CJEU เข้าสู่มติใหม่ของสิทธิที่ได้รับการรับรองชัดเจนโดยกฎหมายที่จะเรียกร้องให้ผู้ประมวลผลข้อมูลลบข้อมูลส่วนบุคคลออกจากโลกดิจิทัลอย่างถาวรและเป็นรูปธรรม ข้อจำกัดและสภาพปัญหาในการตีความและบังคับใช้ Directive 95/46/EC ซึ่งขาดความเหมาะสมกับสภาพการณ์ทางสังคมและเทคโนโลยีที่เปลี่ยนแปลงไปอย่างมากภายในช่วง 20 ปีที่ผ่านมาอันดูเหมือนจะได้รับการพิจารณาปรับปรุงในหลายประเด็น ในวันที่ 25 พฤษภาคม ค.ศ. 2018 ประชาชนในสหภาพยุโรปจะได้รับสิทธิที่พัฒนาขึ้นมาใหม่ให้เกิดความชัดเจนขึ้นทั้งในส่วนของเนื้อหาแห่งสิทธิ ผู้มีหน้าที่ขอยกเว้นแห่งสิทธิและสภาพบังคับที่เหมาะสมกับการประมวลผลข้อมูลในโลกออนไลน์ ตลอดจนมาตรการบังคับทางกฎหมายที่สอดคล้องและมีประสิทธิภาพมากยิ่งขึ้น ซึ่งเวลาจะเป็นผู้ให้คำตอบถึงผลลัพธ์ในทางปฏิบัติของบทบัญญัติตาม

<sup>41</sup> ผศ.ดร.ปิติ เอี่ยมจรรย์ลาภ, เรื่อง บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten)



กฎหมายใหม่ของสหภาพยุโรปฉบับนี้ว่าจะมีประสิทธิภาพในการบังคับใช้จริงมากน้อยเพียงไร ทั้งนี้ ประสบการณ์และสภาพปัญหาของสหภาพยุโรปในการบังคับใช้ Directive 95/46/EC ผ่านคำวินิจฉัยในคดี Google Spain และการบังคับใช้สิทธิดังกล่าวที่ได้รับรองโดย GDPR ในอนาคตอันใกล้นี้ จะเป็นตัวอย่างที่สมควรให้ความสนใจสำหรับประเทศที่อยู่ระหว่างการพิจารณากำหนดให้มีหรือแก้ไขกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลว่าจะให้การรับรอง right to be forgotten หรือไม่ ในขอบเขตเพียงใด ตลอดจนมาตรการทางกฎหมายใดบ้างที่สำคัญและจำเป็น สมควรกำหนดเพื่อบังคับใช้สิทธิดังกล่าวให้เกิดประสิทธิภาพและสอดคล้องกับมาตรฐานสากลสำหรับโลกดิจิทัลที่กำลังจะมาถึง ในปัจจุบันประเทศไทยได้มีการกำหนดรับรองสิทธิในความเป็นส่วนตัวและข้อมูลส่วนบุคคลไว้ในรัฐธรรมนูญ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 และได้มีกฎหมายที่บังคับใช้กับการคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นทางการในปี พ.ศ. 2562 โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับใช้ในวันที่ 28 พฤษภาคม พ.ศ. 2562 แต่เฉพาะหมวดบทบัญญัติในหมวด 2 หมวด 3 หมวด 5 หมวด 6 หมวด 7 และความในมาตรา 95 และมาตรา 96 ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษา เป็นต้นไป ต่อมาได้มีพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ฉบับที่ 2) พ.ศ. 2564 ให้ ยกเลิกความในมาตรา 2 เกี่ยวกับช่วงเวลาในการบังคับใช้ตามพระราชกฤษฎีกา พ.ศ. 2563 เป็นพระราชกฤษฎีกานี้ ให้ใช้บังคับตั้งแต่วันที่ 27 พฤษภาคม พ.ศ. 2563 จนถึงวันที่ 31 พฤษภาคม พ.ศ. 2565 ซึ่ง Search Engines ถือได้ว่าเป็นหน่วยงานหรือกิจการตามบัญชีท้ายพระราชกฤษฎีกานี้ลำดับที่ 13 กิจการด้านการสื่อสาร โทรคมนาคม คอมพิวเตอร์ และดิจิทัล ส่งผลให้จะบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เกี่ยวกับสิทธิในการถูกลืมกับ Search Engines ได้ตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิใช้สิทธิในการถูกลืมให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีรูปแบบในการใช้สิทธิ ที่คล้ายคลึงกับการใช้สิทธิในการถูกลืม มาตรา 17 ของข้อบังคับสหภาพยุโรปโดยมีรูปแบบคล้ายคลึงกันตั้งแต่โครงสร้างการใช้ สิทธิที่แบ่งเป็น 3 ส่วน (1) เหตุแห่งการใช้สิทธิในการลบ (2) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูล ที่เปิดเผยต่อสาธารณะและถูกร้องขอใช้สิทธิในการลบดังกล่าว

ต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่นๆ (3) ข้อยกเว้นการใช้สิทธิในการลบโดยกฎหมายดังกล่าว ปรากฏรูปแบบที่ชัดเจนเป็นรูปธรรมของการคุ้มครอง "สิทธิในการถูกลืม" ในมาตรา 33 ซึ่งอยู่ใน หมวด 3 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคล เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ตามหลักเกณฑ์ ที่กำหนดไว้ ทั้งนี้แม้มาตรา 33 จะกำหนดหลักเกณฑ์ในการใช้สิทธิในการถูกลืมและข้อยกเว้นแต่ หลักเกณฑ์รายละเอียดในการใช้สิทธิในการดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็น ข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้อาจจะออกประกาศโดยคณะกรรมการคุ้มครอง ข้อมูลส่วนบุคคลภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับตามมาตรา 96 โดยเป็นอำนาจ หน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ที่จะออกประกาศกำหนดข้อปฏิบัติในการคุ้มครอง ข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติ ตามมาตรา 16 (3) ซึ่งจะมีลักษณะเป็นกฎหมายลำดับรอง ซึ่งปัจจุบันยังไม่มีการออกประกาศดังกล่าว ต่อมาในปี 2563 หลังจากที่ข้อบังคับว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป มีผลบังคับ ใช้กับรัฐสมาชิก ในปี 2561 คณะกรรมการคุ้มครองข้อมูลแห่งสหภาพยุโรปได้มีการพัฒนาแนวปฏิบัติ เกี่ยวกับเกณฑ์ในการใช้สิทธิในการถูกลืมในกรณีของ Search Engines ขึ้นจนสำเร็จเป็นแนวปฏิบัติ 5/2019 เกี่ยวกับเกณฑ์ในการใช้สิทธิในการถูกลืมในกรณีของ Search Engines ภายใต้ข้อบังคับว่า ด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปส่วนที่ 1 (Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) ) โดย แนวปฏิบัตินี้จะเน้นเฉพาะผู้ควบคุมข้อมูลที่เป็น Search Engines และลบข้อมูลส่วนบุคคลตามคำขอ ใช้สิทธิในการถูกลืมที่ส่งโดยเจ้าของข้อมูลส่วนบุคคลเท่านั้น<sup>42</sup>

ทั้งนี้ในการออกประกาศหลักเกณฑ์ในการใช้สิทธิดังกล่าวของไทยจึงต้องศึกษาแนวทางการ ใช้สิทธิดังกล่าวตามแนวปฏิบัติ 5/2019 เกี่ยวกับเกณฑ์ในการใช้สิทธิในการถูกลืมภายใต้ข้อบังคับว่า ด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปสิทธิ เพื่อเป็นแนวทางในการคุ้มครองสิทธิในการ ถูกลืมให้มีความครอบคลุมชัดเจนยิ่งขึ้นนอกจากนี้ ยังมีปัญหาขอบเขตในการบังคับใช้สิทธิดังกล่าว รวมถึงในส่วนขององค์กรบังคับใช้กฎหมายมีการวางโครงสร้างที่ให้มีกรรมการในคณะกรรมการ ผู้เชี่ยวชาญอาจเป็นบุคคลภายนอกที่เป็นผู้เชี่ยวชาญแต่เป็นบุคคลที่มาจากภาครัฐหรือเอกชนได้และ ไม่ใช่การปฏิบัติงานเต็มเวลาซึ่งอาจจะทำให้การปฏิบัติหน้าที่ไม่มีประสิทธิภาพเท่าที่ควร ตลอดจนถึง

<sup>42</sup> ผศ.ดร.ปิติ เอี่ยมจำรูญลาภ, เรื่อง บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) . หน้า 81.

ไม่มีบทลงโทษทางปกครองที่ชัดเจนหากผู้ควบคุมข้อมูลส่วนบุคคลไม่ยอมลบข้อมูลส่วนบุคคลตามที่เจ้าของข้อมูลร้องขอโดยชอบด้วยกฎหมายมีเพียงการเรียกค่าสินไหมทดแทนและค่าสินไหมทดแทนในเชิงลงโทษทางแพ่ง เป็นต้น โดยปัญหาดังกล่าวเกิดจากการที่ประเทศไทยยังไม่เคยมีกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปรวมถึงการมีบทบัญญัติเกี่ยวกับสิทธิในการถูกลืม โดยปัญหาดังกล่าวเกิดจากการที่ประเทศไทยยังไม่เคยมีกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปรวมถึงการมีบทบัญญัติเกี่ยวกับสิทธิในการถูกลืมจึงทำให้ต้องศึกษาเกี่ยวกับประเด็นปัญหาทางกฎหมายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เกี่ยวกับการใช้สิทธิในการถูกลืม โดยวิเคราะห์เปรียบเทียบจากแนวคิดกฎหมายระหว่างประเทศ กฎหมายต่างประเทศและประเทศไทย แนวปฏิบัติเกี่ยวกับเกณฑ์ในการใช้สิทธิในการถูกลืมของสหภาพยุโรป เพื่อกำหนดแนวทางในการคุ้มครองสิทธิในการถูกลืมบนระบบอินเทอร์เน็ตที่เหมาะสมในประเทศไทยต่อไปจากการศึกษาและวิเคราะห์พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เปรียบเทียบกับกฎหมายระหว่างประเทศและกฎหมายต่างประเทศ และแนวปฏิบัติในการใช้สิทธิพบว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังมีประเด็นปัญหาเกี่ยวกับสิทธิในการถูกลืมที่ยังไม่ครอบคลุมชัดเจนในประเด็น ดังต่อไปนี้

1. ปัญหาในเรื่องขอบเขตการใช้สิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กล่าวคือ การใช้สิทธิในการถูกลืมสามารถใช้สิทธิดังกล่าวบนราชอาณาจักรไทยคือ ลบทุก Domain Name ของ Google และรวมถึง Google.com ที่อยู่นอกราชอาณาจักรไทยได้หรือไม่ซึ่งประเด็นนี้ในสหภาพยุโรปได้มีคำตัดสินคดีคำตัดสินคดี case C-507/17, Google v. Commission nationale de l'informatique et des libertés (CNIL) ศาลยุติธรรมของสหภาพยุโรปฯ ได้ตัดสินว่าหากไม่มีข้อบังคับภายใต้กฎหมายของสหภาพยุโรปสำหรับ Google และ Search Engines อื่น ๆ เพื่อให้สิทธิของสหภาพยุโรป ในการใช้สิทธิในการถูกลืมลบข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลในทุก Domain Name ของ google ศาลได้ตัดสินให้กำหนดขอบเขตของสิทธิแต่ละบุคคลในการยกเลิกการอ้างอิง Google จำเป็นต้องลบลงไปยังข้อมูลส่วนบุคคลของแต่ละบุคคล จากการสืบค้นทางอินเทอร์เน็ตที่ดำเนินการภายในสหภาพยุโรปเท่านั้น อย่างไรก็ตาม ในการใช้สิทธิในการถูกลืมลบข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลในทุก Domain Name ของ google ถือเป็นการใช้สิทธิบนราชอาณาจักร ดังนั้น หากเทียบเคียงกับการใช้สิทธิในการถูกลืมในประเทศไทยตามขอบเขตในการใช้สิทธิดังกล่าว อาจจะจำกัดการใช้สิทธิในการถูกลืมได้เฉพาะ Search Engines Domain Name

ของไทย เช่น google. co.th แต่ใช้สิทธิ Domain Name google.com ที่อยู่นอกราชอาณาจักรไม่ได้ เนื่องจากเป็น การใช้สิทธิในราชอาณาจักรไทยและเป็นการใช้สิทธิฝ่ายเดียวก้าวล่วงอำนาจอธิปไตยของรัฐอื่น และไม่สอดคล้องกับกฎหมายระหว่างประเทศโดยไม่มีสนธิสัญญาหรือความตกลงระหว่างประเทศเกี่ยวกับการใช้สิทธิดังกล่าว รวมถึงปัญหาในการบังคับใช้สิทธิข้ามพรมแดน ตั้งแต่เริ่มต้นสอบสวน รวมถึงการบังคับใช้ และเป็นการจำกัดประสิทธิภาพของสื่อทั่วโลก โดยอาจเกิดความขัดแย้งทางกฎหมายระหว่างสองประเทศ โดยการละเมิดอธิปไตย ของประเทศอื่นและอาจทำให้ความสัมพันธ์ทางการทูตที่ไม่ดี และผลกระทบของการใช้สิทธิในเขตอำนาจศาลนอกราชอาณาจักรที่ขัดต่อกฎหมายของชาติอื่นๆ ซึ่งอาจเป็นการแทรกแซงอย่างไม่สมเหตุสมผลต่อกฎหมายของประเทศนั้นๆได้

2. ประเด็นปัญหาเกี่ยวกับสิทธิในการถูกลืมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเทศไทย สิทธิขอให้ลบทำลาย หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้นั้น จะเห็นได้ว่าการใช้สิทธิในการถูกลืม มีการกำหนดรูปแบบที่หลากหลายกว่าของประเทศอื่นๆ เช่น กรณีการประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการในบริบทของกิจกรรมของ Search Engines จะมีการแตกต่างจากการประมวลผลที่ดำเนินการ โดยผู้เผยแพร่เว็บไซต์ของบุคคลที่สาม เช่น เว็บไซต์สื่อที่ให้เนื้อหาหนังสือพิมพ์ออนไลน์ หากเจ้าของข้อมูลได้รับการลบเนื้อหาข้อมูลส่วนบุคคลที่เฉพาะเจาะจงจะส่งผลให้มีการลบเนื้อหานั้น ออกจากรายการผลการสืบค้นที่เกี่ยวข้องกับหัวเรื่องข้อมูล เมื่อมีการสืบค้นตามชื่อของบุคคลนั้น ไม่ได้ขยายการลบไปถึงเนื้อหาทั้งหมดบนระบบอินเทอร์เน็ต (Stefania Alessi, 2017) โดยเป็นการลบหรือตัดการเชื่อมต่อ (Delink หรือ unlink) กับเว็บไซต์ต่างๆ ที่ได้รวบรวมประมวลผลออกมาเท่านั้นไม่มีสิทธิไปลบถึงข้อมูลส่วนบุคคลในเว็บไซต์ต้นฉบับได้ เพราะข้อมูลส่วนบุคคลนั้นยังอยู่ในความควบคุมขององค์กรหรือหน่วยงานที่เป็นเจ้าของเว็บไซต์ดังกล่าว (Sangsuwan, 2021) โดยที่เนื้อหาดังกล่าวจะยังคงสามารถใช้ได้โดยใช้เกณฑ์การสืบค้นอื่นๆ คำขอให้ลบไม่ส่งผลให้ข้อมูลส่วนบุคคลถูกลบอย่างสมบูรณ์ ข้อมูลส่วนบุคคลจะไม่ถูกลบออกจากเว็บไซต์ต้นทางหรือจากดัชนีและแคชของ Search Engines ตัวอย่างเช่น เจ้าของข้อมูลอาจขอให้ลบข้อมูลส่วนบุคคลออกจากดัชนีของ Search Engines ซึ่งมีที่มาจากสื่อเช่นบทความในหนังสือพิมพ์ ในกรณีนี้ลิงก์ไปยังข้อมูลส่วนบุคคลอาจถูกลบออกจากดัชนีของ Search Engines แต่อย่างไรก็ตามบทความที่เป็นปัญหาจะยังคงอยู่ในการควบคุมของสื่อและอาจยังคงเปิดเผยต่อสาธารณะและเข้าถึงได้แม้ว่าจะไม่ปรากฏในผลการสืบค้นอีกต่อไปตามคำค้นหาชื่อของเจ้าของข้อมูล ทั้งนี้เนื่องจากเจ้าของข้อมูลส่วนบุคคลเป็นผู้มีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือ

ทำลายหรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้และหากเจ้าของข้อมูลส่วนบุคคลเลือกที่จะร้องขอให้ทำลายข้อมูลหรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลอาจไม่สามารถทำได้ เพราะไม่สามารถไปทำลายข้อมูลหรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลกับข้อมูลเว็บไซต์ต้นฉบับโดยตรง ดังนั้นเพื่อแก้ไขปัญหาในการร้องขอใช้สิทธิในการถูกลืมอาจต้องกำหนดรูปแบบในการใช้สิทธิในลักษณะเป็นตัวเลือก เช่น ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคล ให้ทำได้ในรูปแบบใดรูปแบบหนึ่งหรืออาจเป็นการกำหนดตัวเลือกอันดับแรกที่ต้องการใช้สิทธิหากทำไม่ได้ให้ใช้สิทธิในรูปแบบตัวเลือกว่าอันดับรองลงมาในการใช้สิทธิ เพราะหากร้องขอใช้สิทธิในการถูกลืมในรูปแบบตัวเลือกเพียงรูปแบบเดียวที่ Search Engines ไม่สามารถทำได้ย่อมส่งผลให้เจ้าของข้อมูลส่วนบุคคลก็ยังคงไม่ได้รับประโยชน์ตามที่ต้องการจากการใช้สิทธิดังกล่าว โดยออกมาเป็นประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล ซึ่งจะมีลักษณะเป็นกฎหมายลำดับรอง เพื่อให้การใช้สิทธิในการถูกลืมมีความครอบคลุมชัดเจนมากขึ้น

3. หลักเกณฑ์การใช้สิทธิในการถูกลืมของประเทศไทยแม้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดหลักเกณฑ์ในการใช้สิทธิในการถูกลืมตามมาตรา 33 แต่ยังไม่ได้มีการประกาศกำหนดหลักเกณฑ์ในการใช้สิทธิดังกล่าวอย่างชัดเจนจึงต้องศึกษาแนวปฏิบัติ 5/2019 เกี่ยวกับเกณฑ์ในการใช้สิทธิในการถูกลืมมาตรา 17 ในกรณีของ Search Engines ภายใต้อำนาจบังคับว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เปรียบเทียบกับสหภาพยุโรปส่วนที่ 1 เนื่องจากหลักเกณฑ์การใช้สิทธิในการถูกลืมของประเทศไทยมีความคล้ายคลึงกับของสหภาพยุโรปเพื่อเป็นแนวทางในการกำหนดหลักเกณฑ์ใช้สิทธิดังกล่าว ดังนี้

(1) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเจ้าของข้อมูลส่วนบุคคลอาจร้องขอใช้สิทธิในการถูกลืมต่อ Search Engines หลังจากพบว่าข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่แสดงในผลการสืบค้นเหล่านั้นหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวมหรือการประมวลผลโดย Search Engines เหตุแห่งการใช้สิทธินี้ทำให้เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ลบข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเอง ซึ่งถูกทำให้เข้าถึงได้นานเกินกว่าที่จำเป็นสำหรับการประมวลผลของ Search Engines โดยการใช้สิทธิในการขอให้ลบต้องบนความสมดุลระหว่างการปกป้องความเป็นส่วนตัวส่วนตัวและผลประโยชน์ของผู้ใช้อินเทอร์เน็ตในการเข้าถึงข้อมูลโดยการดำเนินการลบจะต้องมีการ

ประเมินว่าในช่วงเวลาที่ผ่านมาข้อมูลส่วนบุคคลนั้นล้าสมัยหรือไม่ได้รับการอัปเดตหรือไม่ เช่น เจ้าของข้อมูลส่วนบุคคลอาจใช้สิทธิ์ในการถูกลืม เมื่อลิงก์ไปยังเว็บไซต์ของบริษัทมีรายละเอียดการติดต่อของเจ้าของข้อมูลส่วนบุคคล แม้ว่าเจ้าของข้อมูลส่วนบุคคลดังกล่าวจะไม่ได้ทำงานในบริษัทนั้นอีกต่อไป หรือข้อมูลได้รับการเผยแพร่บนอินเทอร์เน็ตเป็นเวลาหลายปีเพื่อให้เป็นไปตามข้อผูกพันทางกฎหมายและยังคงออนไลน์นานกว่าเวลาที่กำหนดโดยกฎหมายนั้น เจ้าของข้อมูลอาจร้องขอให้ลบเนื้อหาที่เห็นได้ชัดว่าข้อมูลส่วนบุคคลไม่ถูกต้องเนื่องจากระยะเวลาหรือล้าสมัย การประเมินดังกล่าวจึงขึ้นอยู่กับวัตถุประสงค์ของการประมวลผลของข้อมูลดังกล่าวและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลเดิมเพื่อวิเคราะห์คำขอใช้สิทธิ์ดังกล่าว

(2) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไปในการใช้สิทธิ์ดังกล่าวไม่ควรให้เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการประมวลผลข้อมูลของ Search Engines เนื่องจากผู้ควบคุมข้อมูลเป็นเจ้าของข้อมูลให้ความยินยอมคือ ผู้เผยแพร่เว็บไม่ใช่ Search Engines ที่ทำดัชนีข้อมูล และคำยินยอมต้องเป็นการเฉพาะเจาะจงเกี่ยวข้องกับการประมวลผลโดยเฉพาะคำยินยอมที่ดำเนินการโดยเชื่อมต่อกับกิจกรรมของ Search Engines ในทางปฏิบัติจึงแทบเป็นไปไม่ได้เลยที่ Search Engines จะขอความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อนที่จะประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตามในกรณีที่เจ้าของข้อมูลถอนความยินยอมในการใช้ข้อมูลของตนบนหน้าเว็บหนึ่งๆ ผู้เผยแพร่ต้นฉบับของหน้าเว็บนั้นควรแจ้ง Search Engines ที่จัดทำดัชนีข้อมูลดังกล่าวด้วยดังนั้นในกรณีนี้เจ้าของข้อมูลจึงไม่อาจจะใช้สิทธิ์ในการถูกลืมด้วยเหตุจาก Search Engines ได้โดยตรง

(3) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) ได้ หรือเป็นการคัดค้านตามมาตรา 32 (2) เจ้าของข้อมูลสามารถร้องขอใช้สิทธิ์ต่อ Search Engines ในการลบผลการสืบค้นข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเจ้าของข้อมูลเมื่อเจ้าของข้อมูลคัดค้านการประมวลผลและในกรณีที่ไม่มีเหตุผลที่ถูกต้องตามกฎหมายสำหรับการประมวลผลโดยผู้ควบคุมข้อมูลส่วนบุคคล Search Engines ต้องมีภาระการพิสูจน์ให้เห็นถึงเหตุผลอันชอบธรรมที่ปฏิเสธไม่ได้ในการประมวลผลส่วนบุคคลที่สำคัญยิ่งกว่าผลประโยชน์และสิทธิเสรีภาพของผู้ถูกประมวลผลข้อมูลส่วนบุคคล รวมถึงข้อยกเว้นใดๆ ที่มีให้ภายใต้มาตราในกรณีนี้ "สถานการณ์เฉพาะ" ของเจ้าของข้อมูลจะอยู่ภายใต้การ

ร้องขอการลบข้อมูลส่วนบุคคล ตัวอย่างเช่นผลการสืบค้นสร้างความเสียหายให้กับเจ้าของข้อมูลเมื่อสมัครงานหรือทำลายชื่อเสียงของเขาในชีวิตส่วนตัว และเมื่อต้องคำนึงถึงความสมดุลระหว่างสิทธิส่วนบุคคลและสิทธิในข้อมูลนอกเหนือไปจากเกณฑ์ในการจัดการคำร้องใช้สิทธิในการถูกลืม เช่น เจ้าของข้อมูลส่วนบุคคลไม่ได้มีบทบาทเป็นบุคคลสาธารณะ ข้อมูลส่วนบุคคลไม่เกี่ยวข้องกับชีวิตการทำงานของเจ้าของข้อมูลแต่ส่งผลกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูล ข้อมูลส่วนบุคคลดังกล่าวถือเป็นการแสดงความเกลียดชัง การใส่ร้าย การหมิ่นประมาทหรือความผิดที่คล้ายคลึงกันที่แสดงต่อเจ้าของข้อมูลตามคำสั่งศาล ข้อมูลส่วนบุคคลดูเหมือนจะเป็นข้อเท็จจริงที่ได้รับการยืนยันแต่ไม่ถูกต้องตามความเป็นจริง ข้อมูลส่วนบุคคลเกี่ยวข้องกับความผิดทางอาญาที่มีโทษต่ำที่เกิดขึ้นเมื่อนานมาแล้วและก่อให้เกิดอคติต่อเจ้าของข้อมูลส่วนบุคคล

(4) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ในหมวดนี้เจ้าของข้อมูลอาจขอให้ลบข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเจ้าของข้อมูลซึ่งได้รับการประมวลผลโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ในหมวดนี้ คือ เฉพาะหมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล เท่านั้น หากเป็นการประมวลผลโดยไม่ชอบด้วยกฎหมายเรื่องอื่นๆ นอกจากหมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคลไม่อาจเข้าหลักเกณฑ์การใช้สิทธิในการถูกลืมมาตรา 33 วรรค1(4) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ที่กล่าวมา 4 ประเด็นปัญหาเกี่ยวกับการใช้สิทธิในการถูกลืมของเจ้าของข้อมูลส่วนบุคคลในกรณีต้องการให้ลบข้อมูลส่วนบุคคลที่มีอยู่ทั้ง Search Engines และเว็บไซต์เผยแพร่สื่อออนไลน์ โดยแบ่งออกเป็น 2 กรณีกรณีแรกหากเจ้าของข้อมูลส่วนบุคคลเลือกใช้สิทธิต่อเว็บไซต์เผยแพร่สื่อออนไลน์ ซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลต้นฉบับซึ่งเป็นผู้เริ่มต้นเผยแพร่ข้อมูลส่วนบุคคลนั้นจะทำให้ผลการใช้สิทธิในการถูกลืมมีประสิทธิภาพที่สุดเพราะเมื่อเว็บไซต์เผยแพร่สื่อออนไลน์ ลบข้อมูลในเว็บไปจะทำให้ไม่สามารถค้นหาข้อมูลนั้นทาง Search Engines ทั้งหมดต่อไปและเป็นการร่นระยะเวลาและจำนวนครั้งในการใช้สิทธิและเมื่อเมื่อเว็บไซต์เผยแพร่สื่อออนไลน์ลบข้อมูลส่วนบุคคลไปแล้วมีหน้าที่แจ้งให้ Search Engines ทราบเกี่ยวกับการใช้สิทธิดังกล่าวตามมาตรา 33 วรรค 2 กรณีสอง หากเจ้าของข้อมูลส่วนบุคคลใช้สิทธิในการ ถูกลืมต่อ Search Engines โดยตรง ข้อมูลส่วนบุคคลจะถูกลบออกจากผลการสืบค้นเฉพาะรายนั้นๆ เท่านั้น แต่ข้อมูลส่วนบุคคลยังคงสามารถเข้าถึงโดย Search Engines รายอื่นๆ หรือเข้าทางเว็บไซต์เผยแพร่สื่อออนไลน์ ทำให้การใช้สิทธิในการถูกลืมไม่มีประสิทธิภาพอย่างแท้จริง และอาจต้องไปร้องขอใช้สิทธิไป Search Engines รายอื่นๆ อีกทำให้เกิด

ความล่าช้าในการใช้สิทธิ ดังนั้น การใช้สิทธิในการถูกลืมหากเจ้าของข้อมูลส่วนบุคคลเลือกใช้สิทธิต่อเว็บไซต์เผยแพร่สื่อออนไลน์ซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลต้นฉบับ จึงเป็นแนวทางที่ง่ายและเร็วที่สุด ในการลบข้อมูลส่วนบุคคลได้ทั้งเว็บไซต์ต้นฉบับและทาง Search Engines ทั้งหมด ซึ่งจะเป็นประโยชน์และได้ผลรวดเร็วในการลบข้อมูลของเจ้าของข้อมูลส่วนบุคคลมากกว่าการที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิผ่านทาง Search Engines โดยตรงดังกล่าว (Verschaeve, 2020)

5. ประเด็นปัญหาเกี่ยวกับข้อยกเว้นการใช้สิทธิในการถูกลืมของประเทศไทย ในกรณีของ Search Engines การใช้สิทธิในการถูกลืมไม่ใช่สิทธิเด็ดขาดที่เจ้าของข้อมูลจะร้องขอใช้สิทธิได้ในทุกกรณีแม้เข้าหลักเกณฑ์ในการใช้สิทธิตามมาตรา 33 วรรค 1 แต่หากเข้าข้อยกเว้นตามมาตรา 33 วรรค 2 ก็ไม่สามารถใช้สิทธิได้ และแม้มาตรา 33 วรรคท้ายจะมีการให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจออกประกาศกำหนดหลักเกณฑ์ในการใช้สิทธิในการถูกลืม แต่อย่างไรก็ตามมาตรา 33 วรรค 1 ก็ไม่ได้มีบทบัญญัติให้อำนาจคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลออกประกาศกำหนดหลักเกณฑ์เกี่ยวกับข้อยกเว้นการใช้สิทธิในการถูกลืมตามมาตรา 33 วรรค 2 แต่อย่างใด ซึ่งตรงนี้อาจเป็นอำนาจหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่จะออกประกาศหนดข้อปฏิบัติเกี่ยวกับข้อยกเว้นในการใช้สิทธิในการถูกลืมในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามมาตรา 16(3) ซึ่งจะมีลักษณะเป็นกฎหมายลำดับรองโดยอาจนำแนวปฏิบัติของสหภาพยุโรปมาเป็นแนวทางในออกประกาศเกี่ยวกับข้อยกเว้นการใช้สิทธิในการถูกลืมของประเทศไทย ดังนี้ ข้อยกเว้น(1) การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น ข้อยกเว้นนี้ แบ่งเป็น 2 กรณี

1. คำขอสำหรับการลบที่เกิดขึ้นกับผู้เผยแพร่ต้นฉบับซึ่งข้อมูลได้รับการคุ้มครองโดยสิทธิเสรีภาพในการแสดงออก ซึ่งของไทยหากเป็นกรณีบุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชนงานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้นจะไม่ใช้พระราชบัญญัตินี้บังคับ จึงใช้สิทธิในการถูกลืมขอให้ลบข้อมูลไม่ได้ตามมาตรา 4(3)

2. คำขอต่อ Search Engines ซึ่งไม่ได้เป็นผู้เผยแพร่ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลดังกล่าว แต่เป็นการประมวลผลระบุข้อมูลที่มีอยู่เกี่ยวกับบุคคลนี้และการสร้างโปรไฟล์ของเจ้าของข้อมูลกรณีนี้จะต้องพิจารณาว่าสิทธิของเจ้าของข้อมูลส่วนบุคคลจะมีเหนือกว่าผลประโยชน์ของผู้ให้บริการอินเทอร์เน็ตโดยทั่วไป โดยการสร้างความสมดุลขึ้นอยู่กับข้อเท็จจริงหลายประการที่อาจ



ส่งผลต่อการตัดสินใจดังกล่าวซึ่งรวมถึงลักษณะของข้อมูลและความอ่อนไหวของข้อมูลของชีวิตส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และโดยเฉพาะอย่างยิ่งความสนใจของผู้ใช้อินเทอร์เน็ตในการเข้าถึงข้อมูล โดยความสนใจดังกล่าวมีแตกต่างกันไปขึ้นอยู่กับบทบาทของเจ้าของข้อมูลในชีวิตสาธารณะว่าเป็นบุคคลสาธารณะหรือไม่ ซึ่ง Search Engines อาจปฏิเสธที่จะลบเนื้อหาออกในกรณีที่สามารถแสดงให้เห็นว่าการประมวลผลข้อมูลโดยแสดงรายการผลการสืบค้นดังกล่าวเป็นสิ่งที่จำเป็นอย่างยิ่งสำหรับการปกป้องเสรีภาพในข้อมูลของผู้ใช้อินเทอร์เน็ต (2) การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือ (4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุม ข้อมูลส่วนบุคคลหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล แบ่งออกเป็น 2 กรณี

2.1 การเก็บรักษาไว้เพื่อวัตถุประสงค์ ตามมาตรา 24(1) Search Engines ต้องสามารถแสดงให้เห็นว่าการลบเนื้อหาบางส่วนในหน้าผลการสืบค้นเป็นอุปสรรคร้ายแรงหรือขัดขวางไม่ให้อำนาจรัฐดำเนินการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์หรือวัตถุประสงค์ทางสถิติโดยสิ้นเชิง

2.2 การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24(4) โดยหลัก Search Engines ในไทย ไม่ใช่หน่วย งานสาธารณะดังนั้นจึงไม่ใช้อำนาจสาธารณะด้วยตนเอง แต่สามารถใช้อำนาจเหล่านั้นได้ หากเป็นผลมาจากกฎหมายของรัฐในการให้อำนาจหลัก Search Engines ปัจจุบันยังไม่มี การให้อำนาจดังกล่าว ดังนั้น ข้อ ยกเว้นนี้จึงไม่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของ Search Engines (3) การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 26(5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุ วัตถุประสงค์เกี่ยวกับ (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคม สงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา

เวชภัณฑ์ หรือเครื่องมือแพทย์ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ Search Engines ในไทย ไม่ได้มีการประมวลผลข้อมูลส่วนบุคคลเพื่อเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านสาธารณสุข ซึ่ง Search Engines จะทำได้ต้องได้รับอำนาจตามกฎหมายจากรัฐ ซึ่งปัจจุบันยังไม่มี การให้อำนาจดังกล่าว ดังนั้น ข้อยกเว้นนี้จึงไม่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของ Search Engines (4) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย Search Engines ในไทยจะใช้ข้อยกเว้นนี้เพื่อปฏิเสธคำขอลบได้ยากเช่นกัน เนื่องจากโดย Search Engines ไม่ได้ประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมายหรือเพื่อการปฏิบัติตามกฎหมาย แต่เป็นการประมวลผลข้อมูลส่วนบุคคลที่มีอยู่แล้วเกี่ยวกับบุคคลนั้นๆและจัดทำรายการดัชนี 6 ประเด็นปัญหาเกี่ยวกับคณะกรรมการผู้เชี่ยวชาญ

เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายใหม่ที่เพิ่งมีขึ้นในประเทศไทยโดยที่ยังไม่มีกฎหมายลำดับรองกำหนดทางปฏิบัติในรายละเอียดและยังไม่มีแนวการตีความหรือบังคับใช้กฎหมายมาก่อน บุคคลที่จะมาทำหน้าที่บังคับใช้กฎหมายนี้จึงมีความสำคัญมากที่จะเริ่มต้นวางบรรทัดฐานการใช้กฎหมายว่าจะใช้เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นได้จริง หรือ จะใช้เพื่อตีความข้อยกเว้นให้กว้างขวางจนเป็นประโยชน์ต่อฝ่ายรัฐหรือธุรกิจขนาดใหญ่ โดยกรรมการในคณะกรรมการผู้เชี่ยวชาญนั้น ไม่มีข้อกำหนดห้ามมิให้เป็นข้าราชการ เจ้าหน้าที่ในหน่วยงานของรัฐอื่น ลูกจ้างพนักงานผู้บริหารของรัฐวิสาหกิจหรือองค์กรเอกชนเป็นกรรมการอีกทั้งตามกฎหมายกำหนด ยังมีใช้การปฏิบัติงานเต็มเวลาโดยให้ได้รับเบี้ยประชุมและค่าตอบแทนอื่นตามที่กำหนดเท่านั้น ทำให้กรรมการเหล่านี้จะไม่มีเวลาในการทำงานในหน้าที่ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเต็มที่ ทำให้ปราศจากหน่วยงานการบังคับใช้หรือกลไกที่มีประสิทธิภาพส่งผลทำให้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่สามารถเป็นเครื่องมือในคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพโดยการใช้สิทธิในการถูกลืมตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิในการถูกลืม เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการ

ผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้ทั้งนี้ โอกาสที่เจ้าของข้อมูลส่วนบุคคลจะใช้สิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญหลังจากมีการพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะบังคับใช้กับ Search Engines จริงในเดือนมิถุนายน 2565 มีแนวโน้มจะมีการร้องเรียนค่อนข้างมากและสูง เมื่อพิจารณาจากการร้องเรียนการใช้สิทธิในสหภาพยุโรปต่อ Search Engines ซึ่งหากจำนวนคณะกรรมการผู้เชี่ยวชาญหากไม่เพียงพอ และจะต้องเป็นกรรมการผู้เชี่ยวชาญที่มีความรู้ความเชี่ยวชาญเกี่ยวกับการทำงานของ Search Engines โดยตรง หรือหากกรรมการผู้เชี่ยวชาญไม่มีความเป็นอิสระในการทำงานหรือการทำงานเต็มเวลาอาจทำให้ไม่สามารถเครื่องมือในคุ้มครองการใช้สิทธิในการถูกลืมได้อย่างมีประสิทธิภาพ

7. ประเด็นปัญหาเกี่ยวกับความรับผิดชอบของ Search Engines สิทธิในการถูกลืมปัจจุบันพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดเกี่ยวกับความรับผิดชอบทางแพ่งของ Search Engines กรณีสิทธิในการถูกลืม แต่มีเพียงค่าสินไหมทดแทนทางแพ่งอย่างเดียว จึงยังถือว่าไม่เหมาะสมกับสถานการณ์ในปัจจุบันดังนั้น จึงควรมีบทกำหนดโทษทางปกครองและอาญาไว้ในความรับผิด โดยอาจกำหนดในส่วนของโทษปรับทางปกครองเพิ่มขึ้นในกรณี Search Engines ผ่าฝืนไม่ปฏิบัติตามการใช้สิทธิในการถูกลืมของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 33 โดยกำหนดระวางโทษปรับสอดคล้องกับโทษปรับทางปกครองในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คือระวางโทษปรับทางปกครองอยู่ระหว่างไม่เกินหนึ่งถึงห้าล้านบาท เพื่อให้สอดคล้องระวางโทษปรับในพระราชบัญญัติดังกล่าวสอดคล้องกับบริบทสังคมไทยและเพื่อให้ความรับผิดในกรณีละเมิดสิทธิในการถูกลืมมีประสิทธิภาพมากขึ้น

สรุปจากการศึกษาเรื่องสิทธิที่ถูกลืมบนระบบอินเทอร์เน็ตจะเห็นได้ว่าแม้ประเทศไทยจะมีการคุ้มครองสิทธิในการถูกลืมตามมาตรา 33 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีการกำหนดหลักเกณฑ์ในการใช้สิทธิในการถูกลืมและช้อยกเว้นแต่ยังไม่ครอบคลุมชัดเจน โดยเฉพาะกรณีการใช้สิทธิในการถูกลืมในกรณีของ Search Engines ซึ่งถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ดังกล่าวโดยปัญหาดังกล่าวเกิดจากการที่ประเทศไทยยังไม่เคยมีกฎหมายที่ให้ความคุ้มครองเกี่ยวกับสิทธิในการถูกลืมดังกล่าว โดยในการใช้สิทธิในการถูกลืมในการดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลในกรณีของ Search Engines จะมีรายละเอียดหลักเกณฑ์ในการใช้อย่างใดในแต่ละกรณี รวมถึงช้อยกเว้นในการใช้สิทธิดังกล่าวอย่างไรควรออกเป็นประกาศกำหนดหลักเกณฑ์และช้อยกเว้นใน

การใช้สิทธิดังกล่าวโดยเป็นอำนาจหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งจะมีลักษณะเป็นกฎหมายลำดับรอง โดยในการออกประกาศหลักเกณฑ์ในการใช้สิทธิดังกล่าวของไทยจึงต้องศึกษาแนวทางการใช้สิทธิดังกล่าวตามแนวปฏิบัติ 5/2019 เกี่ยวกับเกณฑ์ในการใช้สิทธิในการถูกลืมในกรณีของ Search Engines ภายใต้ข้อบังคับว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปซึ่งแนวปฏิบัตินี้จะเน้นเฉพาะผู้ควบคุมข้อมูลที่เป็น Search Engines เพื่อเป็นแนวทางในการคุ้มครองสิทธิในการถูกลืมในกรณี Search Engines ให้มีความครอบคลุมชัดเจนยิ่งขึ้น

นอกจากบทบัญญัติในส่วนของ “สิทธิของเจ้าของข้อมูลส่วนบุคคล” แล้วพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังบัญญัติเรื่องการลบหรือทำลายข้อมูลส่วนบุคคลในส่วนของ “หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล” เอาไว้ในมาตรา 37(3) อีกด้วย โดยบัญญัติว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคล ร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพ ในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือ การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ให้นำความในมาตรา 33 บรรทัดห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม” ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลต้องชดเชยค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า (1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำ ของเจ้าของข้อมูลส่วนบุคคลนั่นเอง หรือ (2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติกรตามหน้าที่และอำนาจตามกฎหมาย<sup>43</sup> หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการลบทำลายข้อมูลส่วนบุคคลตามมาตรา 37(3) ของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นแสดงให้เห็นว่าสิทธิที่จะถูกลืมในระบบกฎหมายไทยนั้น ไม่ได้ถูกคุ้มครองเฉพาะ

<sup>43</sup> Ibid, มาตรา 77

กรณีที่เจ้าของข้อมูลส่วนบุคคลเรียกร้องให้มีการลบทำลายข้อมูลส่วนบุคคลเท่านั้น ตัวผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายจะต้องลบทำลายหรือข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นนอกเหนือจากการลบทำลายจากการร้องขอของเจ้าของข้อมูลส่วนบุคคลอีกด้วย

ผู้ควบคุมถูกผูกมัดโดยภาระผูกพันทางกฎหมายในการลบข้อมูลพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ก่อนวันที่ 25 พฤษภาคม ค.ศ. 2018 ซึ่งเป็นวันที่ GDPR จะมีผลใช้บังคับนั้น การคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปเป็นไปตาม Directive 95/46/EC84 ซึ่งบัญญัติรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลในการ เข้าถึงข้อมูลส่วนบุคคล (Right of Access) โดยรวมไปถึงการลบข้อมูล (Erasure) ที่ถูกประมวลผลโดยฝ่าฝืนต่อ กฎระเบียบฉบับนี้หรือเนื่องจากเป็นกรณีที่ข้อมูลมีความไม่สมบูรณ์หรือมีลักษณะคลาดเคลื่อน<sup>44</sup> โดยไม่ได้บัญญัติ ถึง “สิทธิที่จะถูกลืม” เอาไว้ในตัวบทกฎหมาย หลักการเกี่ยวกับการขอให้มีการลบข้อมูลนั้นได้ถูกพัฒนา<sup>45</sup> และส่งต่อมายังมาตรา 17 ของ GDPR ในฐานะที่เป็น “สิทธิในการลบข้อมูล” และได้บัญญัติสิทธิของเจ้าของข้อมูลส่วนบุคคลนี้สามารถเรียกได้ว่า “สิทธิที่จะถูกลืม (Right to be Forgotten)”<sup>46</sup>

GDPR ของสหภาพยุโรปได้ระบุไว้ชัดเจน ในมาตรา 17 ซึ่งให้สิทธิ์ที่ชัดเจนในการลบข้อมูลออก (GDPR 2016/679) สิทธิในการลบข้อมูลจะไม่มีผลบังคับใช้หากประมวลข้อมูลจำเป็นสำหรับการใช้เสรีภาพ ในการแสดงออก หรือเพื่อผลประโยชน์สาธารณะ เช่น วัตถุประสงค์ด้านสุขภาพ ประวัติศาสตร์ และวิทยาศาสตร์ ในชั้นการพิจารณาร่าง GDPR นั้น คณะมนตรียุโรปได้กล่าวถึงเหตุผลที่มีการกล่าวถึง “สิทธิที่จะถูกลืม” ควบคู่ไปกับสิทธิในการลบข้อมูล โดยอธิบายว่าการอ้างอิงถึงสิทธิที่จะถูกลืมนั้นจำเป็นต่อสิทธิในการลบข้อมูลใน บริบทของโลกยุคดิจิทัล (Digital Context)<sup>47</sup> เมื่อเจ้าของข้อมูลส่วนบุคคลประสงค์จะถูกลืมหลังจากที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เผยแพร่ข้อมูลส่วนบุคคลต่อสาธารณะ มีหน้าที่ต้องดำเนินการใดๆ ต้องแจ้งให้ผู้ควบคุมข้อมูล ส่วนบุคคลอื่นทราบถึงความประสงค์ของเจ้าของข้อมูลส่วนบุคคล และระบุให้สำนักงานคณะกรรมการคุ้มครอง ข้อมูลส่วนบุคคลยุโรป (European Data Protection Board: EDPB) ทำการออกแนวปฏิบัติที่เกี่ยวข้องต่อไป

<sup>44</sup> Ibid, มาตรา 12(b).

<sup>45</sup> อรรถกร สุขปนพันธ์(อ้างแล้ว เจริญธรรมที่ 35), หน้า 14.

<sup>46</sup> มาตรา 17 ของ GDPR บัญญัติโดยใช้อ้อยคำว่า “Right to erasure (‘right to be forgotten’)”

<sup>47</sup> Statement of the Council’s reasons: Position (EU) No 6/2016 (2016/c 159/02), para 4.6.

เป็นสิทธิของบุคคลที่จะร้องขอให้ผู้มีข้อมูลส่วนบุคคลของเขา ไว้ในความครอบครองทำการลบข้อมูลส่วนบุคคลออก เนื่องจากไม่ยินยอมให้มีการใช้ข้อมูลนั้นอีกต่อไป แนวคิดดังกล่าวเป็นแนวคิดที่ถูกกล่าวถึงในยุโรปตั้งแต่การพัฒนาเทคโนโลยีสารสนเทศมีความเจริญก้าวหน้าและมีข้อมูล ข่าวสารจำนวนมากถูกรวบรวม จัดเก็บและประมวลผลบนอินเทอร์เน็ตซึ่งทำให้สามารถถูกสืบค้นข้อมูลได้โดยง่าย และในบางกรณี ข้อมูลที่อาจถูกผู้อื่นสืบค้นได้ง่ายนี้ก็เป็นผลเสียต่อเจ้าของข้อมูลส่วนบุคคลนั้น ทั้งนี้ สิทธิที่จะถูกลืมเริ่มได้รับการรับรองอย่างชัดเจนในยุโรปเป็นครั้งแรกว่าเป็นส่วนหนึ่งของการคุ้มครอง ข้อมูลส่วนบุคคล ในรูปแบบของการวางหลักเกณฑ์เบื้องต้นจากคำวินิจฉัยของศาล (Preliminary Ruling) ผ่านการ ตีความของศาลยุติธรรมสหภาพยุโรป (Court of Justice of European Union: CJEU) ว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกร้องให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูล ทางการลบลิงค์ (Link) เชื่อมต่อแสดงผลการค้นหาชื่อ นามสกุลของตนไปยังหน้าอื่นๆ ได้ และท้ายที่สุดสิทธิที่จะถูกลืมก็ถูกบัญญัติรับรองในกฎระเบียบว่าด้วยการ คุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR) ส่วนประเด็นเกี่ยวกับสิทธิที่จะถูกลืมในระบบกฎหมายไทยนั้น มาตรา 33 ของพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการ “ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลนั้นกลายเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้” ในบางกรณี ได้แก่ ข้อมูลส่วนบุคคลที่หมดความจำเป็นในการเก็บรวบรวมไว้ตามวัตถุประสงค์ หรือเมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล หรือเมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) 1 ได้หรือเป็นการคัดค้านตามมาตรา 32 (2) เป็นต้น อย่างไรก็ตาม มาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้บัญญัติถึงสิทธิที่จะถูกลืม<sup>48</sup>

ระเบียบการคุ้มครองข้อมูลทั่วไปเป็นหน่วยงานที่มีอำนาจหน้าที่ในการควบคุมวิธีการรวบรวมประมวลผลและลบข้อมูลส่วนบุคคล ในขั้นต้นสิทธิในการลบเกิดขึ้นหลังจากข้อพิพาทถูกนำตัวขึ้นศาลกับเครื่องมือค้นหา ในการดำเนินคดีเสิร์ชเอนจินอยู่ในด้านการป้องกันสำหรับการถือครองวัสดุเก่าในดัชนีแม้ว่าพวกเขาจะไม่ถูกต้องหรือเป็นข่าวอีกต่อไป

<sup>48</sup> “สิทธิ” ที่จะถูกลืมกับการอภิบาลอินเทอร์เน็ต [ออนไลน์]. แหล่งที่มา : <https://www.chula.ac.th/cuinside/2509/> [เข้าถึงเมื่อ 23 มีนาคม 2565]

ดังนั้นศาลยุติธรรมยุโรปจึงยอมรับสิทธิในการลบในปี 2014 นับตั้งแต่นั้นเป็นต้นมาเครื่องมือค้นหาได้อนุญาตให้ผู้ใช้สามารถควบคุมรอยเท้าดิจิทัลของตนได้มากขึ้น ผู้มีส่วนได้ส่วนเสียอื่นๆ ก็รับตามไปด้วย ตัวอย่างเช่น Apple ประกาศว่าแอปทั้งหมดที่อนุญาตให้ผู้ใช้สร้างบัญชีควรอนุญาตให้พวกเขาเริ่มลบบัญชีภายในแอปพลิเคชันด้วย ข้อกำหนดนี้มีกำหนดจะมีผลบังคับใช้ในวันที่ 31 มกราคม 2022 แต่ขยายไปถึงวันที่ 30 มิถุนายน 2022 เพื่อให้ให้นักพัฒนาซอฟต์แวร์สามารถเตรียมพร้อมสำหรับข้อกำหนดนี้ได้ดียิ่งขึ้น

ดังที่เราได้กล่าวไว้ก่อนหน้านี้ต้องปฏิบัติตามเงื่อนไขบางประการเพื่อให้ผู้ควบคุมข้อมูลปฏิบัติตามสิทธิในการลบ ภายใต้ GDPR ข้อมูลส่วนบุคคลไม่ได้ตอบสนองวัตถุประสงค์ในการเก็บรวบรวมหรือประมวลผลอีกต่อไป เจ้าของข้อมูลเพิกถอนความยินยอมและไม่มีเหตุผลอื่นใดสำหรับการประมวลผลที่ขอบด้วยกฎหมาย ข้อมูลส่วนบุคคลได้รับการประมวลผลอย่างผิดกฎหมาย ผู้ควบคุมมีภาระผูกพันทางกฎหมายในการลบข้อมูล หัวเรื่องข้อมูลมีการคัดค้านการประมวลผลที่ถูกต้อง ข้อมูลได้รับการรวบรวมเกี่ยวกับการให้บริการสังคมข้อมูลแก่เด็ก

ประเด็นความเป็นส่วนตัวออนไลน์มีความสำคัญมากขึ้น ความกังวลจึงมุ่งเน้นไปที่ความสามารถในการลบข้อมูลส่วนบุคคลที่ล้าสมัย เป็นการตอบโต้กฎหมายหลายฉบับที่เลียนแบบสิทธิที่จะถูกลืมของยุโรปได้รับการแนะนำในระดับรัฐและรัฐบาลกลางในสหรัฐอเมริกา แม้ว่าจะมีการวัดความคิดเห็นของประชาชน เนื่องจากผู้กำหนดนโยบายและศาลมักพิจารณาความคิดเห็นของสาธารณชนเมื่อตัดสินใจว่าจะทำกฎหมายใดและจะตีความกฎหมายเหล่านั้น ความคิดเห็นของสาธารณชนจึงเป็นข้อพิจารณาที่สำคัญเมื่อนึกถึงศักยภาพในการถูกลืมในสหรัฐอเมริกา เช่นเดียวกับสิ่งที่คาดการณ์การสนับสนุนสาธารณะของกฎหมายดังกล่าว การสำรวจที่รวบรวมจาก Mechanical Turk ของ Amazon พบว่าผู้หญิงมีแนวโน้มที่จะสนับสนุนกฎหมายมากกว่า ผู้หญิงมีความกังวลเกี่ยวกับความเป็นส่วนตัวทางออนไลน์ และผู้ที่แสดงความมั่นใจใน Google มากที่สุด บรรดาผู้ที่คิดว่ารัฐบาลใหญ่เกินไปมักไม่ค่อยสนับสนุนกฎหมายดังกล่าวสิ่งนี้ชี้ให้เห็นถึงหนทางที่ซับซ้อนในการเดินหน้าเพื่อสิทธิที่จะถูกลืมในสหรัฐอเมริกา<sup>49</sup>

<sup>49</sup> ผศ.ดร.ปิติ เอี่ยมจำรูญลาภ, เรื่อง บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten)

### 3.3.2.2 การลบ link

ภายใต้ Article 17 ของ GDPR สิทธิดังกล่าวได้ก้าวไปไกลกว่า "right to de-listing" หรือการลบ link แสดงผลการค้นหาจากผู้ให้บริการ search engine เนื่องจากการเน้นย้ำในเนื้อหาแห่งสิทธิใหม่ว่าเป็น "right to erasure" หรือการลบซึ่งข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเจ้าของข้อมูลอย่างแท้จริง โดยไม่ชักช้า และสามารถใช้ยื่นได้ต่อผู้ประมวลผลข้อมูลทั้งหมด ทั้งเจ้าของ webpage ต้นฉบับที่ต้องด้วยบทนิยามตาม GDPR ว่าเป็นผู้ดำเนินการตัดสินใจว่าจะประมวลผลข้อมูลส่วนบุคคลหรือไม่ หรือผู้ให้บริการ search engine จากแนวทางการตีความในคดี Google Spain ทั้งนี้การคงถ้อยคำในวงเล็บว่า right to be forgotten หลัง right to erasure นั้น มีเจตนารมณ์เพื่อเน้นย้ำถึงความสำคัญในการพัฒนา right to erasure เดิมตาม Directive 95/46/EC เข้าสู่การลบเลือนข้อมูลส่วนบุคคลในบริบททางดิจิทัล<sup>50</sup>

ใน Article 17 วรรคหนึ่ง (a) ถึง (f) ได้กำหนดถึงเหตุที่เจ้าของข้อมูลส่วนบุคคลอาจเรียกร้องให้ผู้ประมวลผลข้อมูลลบข้อมูลส่วนบุคคลของตนเสียไว้อย่างละเอียดชัดเจนยิ่งขึ้น อาทิ ข้อมูลส่วนบุคคลดังกล่าวไม่มีความจำเป็นต่อการประมวลผลอีกต่อไป เจ้าของข้อมูลส่วนบุคคลได้ยกเลิกความยินยอมที่เคยได้ให้ไว้สำหรับการประมวลผลข้อมูลและไม่มีเหตุอันชอบด้วยกฎหมายอื่นๆ ที่ผู้ประมวลผลข้อมูลจะทำการประมวลผลข้อมูลต่อไป เจ้าของข้อมูลส่วนบุคคลได้คัดค้านการประมวลผลข้อมูลนั้นและไม่มีเหตุอันชอบด้วยกฎหมายอื่นๆ ที่ได้รับความคุ้มครองเหนือกว่าสำหรับการประมวลผลข้อมูลต่อไป ข้อมูลส่วนบุคคลนั้นถูกประมวลผลโดยมิชอบด้วยกฎหมายหรือมีความจำเป็นต้องถูกลบเพื่อให้เป็นไปตามที่กฎหมายบัญญัติ รวมตลอดถึงกรณีที่ข้อมูลส่วนบุคคลเกี่ยวกับเยาวชนถูกจัดเก็บโดยผู้ให้บริการสังคมข้อมูลข่าวสาร (information society services)<sup>51</sup>

ยิ่งกว่านั้น Article 17 วรรคสอง ของ GDPR ยังได้กำหนดมาตรการใหม่เพื่อให้การใช้ right to be forgotten นั้นมีประสิทธิภาพมากยิ่งขึ้น โดยได้กำหนดหน้าที่ให้ผู้ประมวลผลข้อมูล เมื่อได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคลให้ลบข้อมูลข้อมูลส่วนบุคคลดำเนินการแจ้งผู้ประมวลผลข้อมูลอื่น ๆ ที่ประมวลผลข้อมูลที่เกี่ยวข้องกับคำร้องขอนั้น ให้ดำเนินการลบ link สำเนาหรือผลลัพธ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าวด้วย ทั้งนี้ โดยพิจารณาความเป็นไปได้ในทางเทคโนโลยี และต้นทุนค่าใช้จ่าย ตามสมควรแก่กรณี<sup>52</sup>

<sup>50</sup> The GDPR, Statement of the Council's Reasons: Position (EU) No 6/2016

<sup>51</sup> The GDPR "Article 17 Right to erasure ('right to be forgotten')

<sup>52</sup> The GDPR "Article 17 Right to erasure ('right to be forgotten')



มาตรการใหม่นี้แม้มีข้ออ่อนตรงที่ยังไม่มีการกำหนดสภาพบังคับแก่ผู้ประมวลผลข้อมูลรายอื่นที่ได้รับแจ้งการร้องขอลบข้อมูลส่วนบุคคล จากผู้ประมวลผลข้อมูลรายแรกให้มีผลเสมือนเป็นการได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคลโดยตรงเพื่อให้กระบวนการยื่นคำร้องต่อผู้ประมวลผลข้อมูลทั้งหมดมีผลด้วยการยื่นคำร้องเพียงฉบับเดียว แต่ก็เป็นที่คาดการณ์กันว่าเมื่อพิจารณาประกอบกับหลักเกณฑ์ที่ชัดเจนว่าเจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ลบข้อมูลส่วนบุคคลต่อผู้ประมวลผลข้อมูลได้เป็นการทั่วไปแล้ว ย่อมสามารถเพิ่มโอกาสให้เจ้าของข้อมูลส่วนบุคคลมีโอกาสได้รับการเยียวยาความเสียหายโดยการลบข้อมูลส่วนบุคคลจากผู้ประมวลผลรายอื่นมากยิ่งขึ้น ยกตัวอย่างเช่น กรณีมีการร้องขอให้ Google ลบข้อมูลส่วนบุคคล โดยนัยของวรรคนี้ Google ย่อมต้องดำเนินการแจ้งไปยังเจ้าของ webpage ที่ปรากฏ link ผลการค้นหาทั้งหมด รวมตลอดจนผู้ให้บริการ search engine รายอื่น เพื่อให้ทราบถึงคำร้องที่ Google ได้รับ และผลการตัดสินใจลบของ Google ย่อมเพิ่มความเป็นไปได้ที่ผู้ประมวลผลข้อมูลรายอื่นจะได้ทำการลบข้อมูลส่วนบุคคลในส่วนของตนตามแบบอย่างของ Google เพื่อหลีกเลี่ยงความรับผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลหากเจ้าของข้อมูลส่วนบุคคลดำเนินการร้องขอต่อตนโดยตรงในภายหลัง<sup>53</sup>

ในส่วนของข้อยกเว้นนั้น Article 17 วรรคสาม (a) ถึง (e) ของ GDPR ได้กำหนดข้อยกเว้นหน้าที่ของผู้ประมวลผลข้อมูลตามวรรคหนึ่งและวรรคสองไว้ อย่างชัดเจนหลายประการ อาทิ เพื่อเป็นการใช้สิทธิในเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลข่าวสาร (right of freedom of expression and information) เพื่อให้เป็นไปตามหน้าที่ตามที่กฎหมายบัญญัติหน้าที่เพื่อประโยชน์สาธารณะ หรือการดำเนินการในนามขององค์กรของรัฐ ซึ่งผู้ประมวลผลจะต้องประมวลผลข้อมูลต่อไป กรณีประโยชน์สาธารณะเกี่ยวกับการสาธารณสุข กรณีประโยชน์สาธารณะเกี่ยวกับการวิจัยทางวิทยาศาสตร์และประวัติศาสตร์เฉพาะเหตุที่หากไม่ใช้ข้อยกเว้นดังกล่าวจะทำให้ประโยชน์สาธารณะดังกล่าวไม่อาจบรรลุผลหรือส่งผลเสียต่อประโยชน์ดังกล่าวอย่างร้ายแรง รวมตลอดถึงกรณีเพื่อประโยชน์ในการใช้เป็นข้อต่อสู้ในทางกฎหมาย<sup>54</sup>

<sup>53</sup> Alessi (n14) p.159 see also Witzleb and others (n3) p.317.

<sup>54</sup> The GDPR "Article 17 Right to erasure ('right to be forgotten') 3. Paragraphs 1 and 2

การกำหนดหลักเกณฑ์ในการร้องขอใช้สิทธิลบข้อมูลส่วนบุคคล ตลอดจนข้อยกเว้นที่ชัดเจนตาม Article 17 ย่อมเป็นการสร้างความชัดเจนแก่ผู้ที่เกี่ยวข้องกับการบังคับใช้กฎหมาย ทั้งเจ้าของข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูล ตลอดจนองค์กรคุ้มครองข้อมูลส่วนบุคคลหรือศาลให้มีความรู้ความเข้าใจ ตลอดจนการใช้ดุลพินิจบนหลักเกณฑ์เดียวกัน ตลอดจนยังประโยชน์ต่อการพัฒนาหลักกฎหมายผ่านการใช้การตีความหลักเกณฑ์ดังกล่าวในระยะยาวอีกด้วย

### 3.4 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 และมาตรา 37

จากการศึกษาเรื่องสิทธิที่ถูกลืมบนระบบอินเทอร์เน็ต จะเห็นได้ว่าแม้ประเทศไทยจะมีการคุ้มครองสิทธิในการถูกลืม ตามมาตรา 33 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีการกำหนดหลักเกณฑ์ในการใช้สิทธิในการถูกลืมและข้อยกเว้นแต่ยังไม่ครอบคลุมชัดเจน โดยเฉพาะกรณีการใช้สิทธิในการถูกลืมในกรณีของ Search Engines ซึ่งถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ดังกล่าวโดยปัญหา ดังกล่าวเกิดจากการที่ประเทศไทยยังไม่เคยมีกฎหมายที่ให้ความคุ้มครองเกี่ยวกับสิทธิในการถูกลืมดังกล่าวโดยในการใช้สิทธิในการถูกลืมในการดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลใน กรณีของ Search Engines จะมีรายละเอียดหลักเกณฑ์ในการใช้ข้อมูลใดในแต่ละกรณี รวมถึงข้อยกเว้นในการใช้สิทธิดังกล่าวอย่างไร ควรออกเป็นประกาศกำหนดหลักเกณฑ์และข้อยกเว้นในการใช้ สิทธิดังกล่าวโดยเป็นอำนาจหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งจะมีลักษณะเป็นกฎหมายลำดับรอง โดยในการออกประกาศหลักเกณฑ์ในการใช้สิทธิดังกล่าวของไทยจึงต้องศึกษาแนวทางการใช้สิทธิดังกล่าวตามแนวปฏิบัติ 5/2019 เกี่ยว กับเกณฑ์ในการใช้สิทธิในการถูกลืมในกรณีของ Search Engines ภายใต้ข้อบังคับว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพ<sup>55</sup>

เจ้าของข้อมูลส่วนบุคคล (data subject) ทั้งที่จริงและเท็จและเจ้าของข้อมูลส่วนบุคคลเอง ต้องประสบกับความทุกข์ เพราะไม่ประสงค์ที่จะให้มีการเผยแพร่ข้อมูลเช่นนั้น เนื่องจากอาจเป็นผลเสียต่อชีวิตที่ต้องดำเนินต่อไปทั้งความน่าเชื่อถือในชีวิตการทำงาน การประกอบธุรกิจหรือกระทั่งความสงบสุขในการใช้ชีวิตส่วนตัว เช่น ผลการศึกษาในอดีตที่ประกาศบน website ของมหาวิทยาลัยที่ระบุชื่อของตนกำกับอยู่ ประวัติการเป็นผู้ต้องหาในคดีซึ่งเป็นข่าวครึกโครมทั้งที่อาจต่อสู้อันชั้นศาลจน

<sup>55</sup> วารสารสหวิทยาการสังคมศาสตร์และการสื่อสาร สิทธิในการถูกลืมบนระบบอินเทอร์เน็ต Right to Be Forgotten on the Internet [ออนไลน์]. แหล่งที่มา :<https://so02.tci-thaijo.org/index.php/ISSC/article/view/254961> [เข้าถึงเมื่อ 20 เมษายน 2565]

พิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำความผิดในขั้นที่สุด หรือแม้ต้องโทษแต่ก็พ้นจากโทษไปแล้วเป็นเวลายาวนาน ประวัติการหย่าร้าง คำสั่งศาลให้เป็นบุคคลล้มละลายหรือประกาศขายทอดตลาดทรัพย์สิน ฯลฯ<sup>56</sup>

ปัญหามีอยู่ว่าตัวเจ้าของข้อมูลส่วนบุคคลเหล่านั้นจะอย่างไรได้บ้างเพื่อให้เกิดกระบวนการที่ประวัติต่างๆ ของตนนั้นถูกลบเลือนหรือลืมนำไปเสียจากโลกดิจิทัล (digital obviation) เนื่องจากหากปรับใช้แต่เพียงกฎหมายว่าด้วยละเมิดหรือหมิ่นประมาทเพื่อบังคับให้ลบข้อมูลประวัติต่างๆ ดังกล่าวออกไปแล้วนั้น ก็สู้จะไม่เพียงพอต่อการเยียวยาในยุคดิจิทัล เนื่องจากอาจจะต้องดำเนินการฟ้องร้องดำเนินคดีกับเจ้าของ webpage ต่างๆ ในศาลเป็นจำนวนมากมายทั้งในประเทศและต่างประเทศที่ดำเนินการประมวลผลข้อมูลส่วนบุคคล (data processing) โดยการเผยแพร่ข้อมูลนั้นบน webpage ต่างๆ นับไม่ถ้วน

เรียกได้ว่าคงจะสิ้นเปลืองทรัพยากร เงินทอง แรงกาย แรงใจ และเวลาไปอย่างมหาศาล แตกต่างจากในอดีตที่ข้อมูลส่วนบุคคลจะถูกเผยแพร่โดยสื่อกระแสหลัก เช่น หนังสือพิมพ์ของสำนักพิมพ์เพียงไม่กี่แห่งเท่านั้น

สำหรับประเทศสมาชิกสหภาพยุโรปนั้น แม้ว่าพัฒนาการในการคุ้มครองข้อมูลส่วนบุคคลถือว่าก้าวหน้าเป็นอย่างมาก โดยจะสังเกตได้จากการที่กฎบัตรสิทธิขั้นพื้นฐานของสหภาพยุโรป (Charter of Fundamental Rights of the European Union : CFR) ถึงกับบัญญัติรับรองสิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคล (right to protection of personal data) แยกต่างหากเป็นการเฉพาะ (lex specialist) จากสิทธิในชีวิตส่วนตัวและครอบครัว (right to respect for private and family life) และยังมี Directive 95/46/EC ที่กำหนดแนวทางให้มีและใช้บังคับกฎหมายภายในว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกเป็นการทั่วไป

อย่างไรก็ตาม ไม่มีบัญญัติในส่วนใดใน Directive 95/46/EC ที่กล่าวถึง "สิทธิที่จะถูกลืม" (right to be forgotten) เพื่อให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลถูกลบเลือนหรือลืมนำไปเสียจากโลกออนไลน์เป็นลายลักษณ์อักษรแต่อย่างใด ซึ่งก็เป็นการสอดคล้องกับข้อเท็จจริงของพัฒนาการทางเทคโนโลยีภายในสหภาพยุโรปเอง โดยในปี ค.ศ. 1998 อันเป็นปีที่ Directive ฉบับดังกล่าวมีผลใช้

<sup>56</sup> หนังสือพิมพ์ไทยโพสต์ สิทธิที่จะถูกลืมจากโลกดิจิทัล [ออนไลน์]. แหล่งที่มา

:[https://www.parliament.go.th/ewtadmin/ewt/parliament\\_parcy/ewt\\_news.php?nid=48921&filename=index](https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_news.php?nid=48921&filename=index) [เข้าถึงเมื่อ 2 สิงหาคม 2565]

บังคับนั้น จากสถิติพบว่าประชาชนชาวยุโรปน้อยกว่าร้อยละ 10 เท่านั้นที่ใช้บริการอินเทอร์เน็ตในชีวิตประจำวัน และ Google Inc. เพิ่งก่อตั้งบริษัทเพื่อประกอบธุรกิจเป็นผู้ให้บริการ search engine ได้เพียงหนึ่งปี right to be forgotten จึงเป็นเพียงข้อกังวลที่ได้รับการกล่าวถึงและพัฒนาในวงวิชาการ จนเมื่อปรากฏการณ์ทางสังคมที่เปลี่ยนแปลงไปสู่ยุคสังคมข้อมูลข่าวสาร (information society) ซึ่งข้อมูลจำนวนมากในโลกออนไลน์ (big data) มีแนวโน้มที่จะถูกรวบรวม (collected) จัดเก็บ (stored) และประมวลผล (processed) อย่างต่อเนื่องและอัตโนมัติบนเครือข่ายอินเทอร์เน็ตที่สามารถสืบค้นได้ง่าย (searchable) และด้วยเหตุที่ความมีอยู่ของข้อมูลดังกล่าวอาจก่อให้เกิดผลเสียแก่เจ้าของข้อมูล แนวโน้มข้อห่วงกังวลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลในโลกออนไลน์ จึงกลับด้านเป็นว่า "จะอย่างไรให้ข้อมูลส่วนบุคคลถูกจดจำในโลกออนไลน์น้อยที่สุดและสิ่งใดบ้างที่ควรถูกลบเลือนไป" (how to remember less and what should be forgotten)

ท้ายที่สุดในเดือนพฤษภาคม ค.ศ.2014 right to be forgotten จึงได้รับการรับรองและคุ้มครองว่าเป็นส่วนหนึ่งของ right to protection of personal data อย่างเป็นทางการเป็นครั้งแรกในรูปแบบของการวางหลักเกณฑ์เบื้องต้นจากคำวินิจฉัยของศาล (preliminary ruling) ผ่านการตีความ Directive 95/46/EC ของศาลยุติธรรมสหภาพยุโรป (Court of Justice of the European Union : CJEU) ในคดี Google Spain ซึ่งมีผลผูกพันการใช้การตีความกฎหมายขององค์กรของรัฐในสหภาพยุโรป โดยให้สิทธิเจ้าของข้อมูลส่วนบุคคลที่จะเรียกร้องให้ผู้ให้บริการ search engine ลบ link เชื่อมต่อที่แสดงผลการค้นหาชื่อและนามสกุลของตนไปยัง webpage ต่างๆ ออกจากเครือข่ายอินเทอร์เน็ต (delist) ทั้งนี้ แม้ว่าผลคำวินิจฉัยดังกล่าวได้รับการวิพากษ์วิจารณ์ในแวดวงวิชาการเกี่ยวกับประสิทธิภาพในทางปฏิบัติที่จะให้ความคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลในโลกดิจิทัลในท้ายที่สุด right to be forgotten ก็ได้ถูกรับรองโดยการบัญญัติขึ้นอย่างชัดเจนในกฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรป (General Data Protection Regulation : GDPR) ที่จะใช้บังคับแทน Directive 95/46/EC ในวันที่ 25 พฤษภาคม ค.ศ.2018 โดยได้มีการปรับปรุงและพัฒนาทั้งในด้านเนื้อหาแห่งสิทธิ ผู้มีหน้าที่ และข้อยกเว้นแห่งสิทธิที่ชัดเจนและกว้างขวางมากยิ่งขึ้น

บทความฉบับนี้จะได้นำเสนอสภาพปัญหาของการพยายามปรับใช้กฎหมายของสหภาพยุโรปเท่าที่มีอยู่กับโลกดิจิทัล ผ่านการตีความของ CJEU ในคดี Google Spain และพัฒนาการในกฎหมายฉบับใหม่ของสหภาพยุโรปที่กำลังจะมาถึง อันอาจยังประโยชน์ในการพิจารณาร่างกฎหมายว่าด้วยการคุ้มครอง

ข้อมูลส่วนบุคคลของประเทศไทยที่อาจมีประเด็นต้องพิจารณาระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอต่อ GDPR เพื่อประโยชน์ในการรับโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปต่อไปในอนาคต

1.Right to be forgotten จากแนวทางการตีความของ CJEU ในคดี Google Spain

1.1 มูลเหตุอันเป็นที่มาแห่งคดีโดยสังเขป

นาย Mario Costeja Gonz lez นักธุรกิจและทนายความที่มีชื่อเสียงชาวสเปน ได้ยื่นข้อร้องเรียนสำนักพิมพ์ La Vanguardia Ediciones SL บริษัท Google Spain และบริษัท Google Inc. ต่อองค์กรคุ้มครองข้อมูลส่วนบุคคลของประเทศสเปน (Agencia Espa ñola de Protecci3n de Datos : AEPD) ว่าได้กระทำการละเมิดสิทธิในข้อมูลส่วนบุคคลของตน โดยพบว่าเมื่อผู้ใช้บริการอินเทอร์เน็ตได้สืบค้นชื่อและนามสกุลของนาย Gonz lez ใน website ของ Google แล้วจะพบ link ที่นำไปสู่ webpage ต่างๆ ที่ปรากฏข้อมูลส่วนบุคคลของตน โดยเฉพาะอย่างยิ่ง ข้อมูลเกี่ยวกับการขายทอดตลาดทรัพย์สินเพื่อนำมาชำระหนี้ที่นาย Gonz lez เคยตกเป็นผู้ล้มละลายในอดีต โดยมีข้อเรียกร้องให้สำนักพิมพ์ดังกล่าวและ Google ลบ webpage และ link ที่เชื่อมผลการค้นหาจากชื่อของตนไปยัง webpage ตามลำดับ

AEPD ได้มีคำสั่งปฏิเสธข้อร้องเรียนในส่วนของสำนักพิมพ์ La Vanguardia Ediciones SL โดยยืนยันว่าการเผยแพร่ข้อมูลดังกล่าวบน website ของสำนักพิมพ์นั้นชอบด้วยกฎหมายเนื่องจากเป็นข้อมูลที่เผยแพร่อย่างเป็นทางการจากหน่วยงานของรัฐ แต่ AEPD ก็เห็นพ้องด้วยกับข้อร้องเรียนต่อ Google เมื่อพิจารณาแล้วเห็นว่าผู้ให้บริการ search engine มีหน้าที่ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่จะต้องดำเนินการตามคำร้องเรียนของผู้ร้อง

อย่างไรก็ตาม Google ได้โต้แย้งคำสั่งทางปกครองไปยังศาลของประเทศสเปนว่าลักษณะการให้บริการสืบค้นข้อมูลทางอินเทอร์เน็ตของตนนั้นมิได้ตกอยู่ภายใต้นิยามคำว่าผู้ประมวลผลข้อมูล (data processor) และข้อพิพาทได้ถูกนำเสนอขึ้นสู่การพิจารณาของ CJEU โดยคำร้องขอของศาลประเทศสเปนให้ตีความบทบัญญัติของ Directive 95/46/EC ในเบื้องต้นก่อนว่ามีผลบังคับใช้ต่อผู้คัดค้าน คือ Google ในคดีนี้หรือไม่ ตามลำดับ

1.2 ประเด็นในส่วนเนื้อหาแห่งสิทธิ

CJEU วินิจฉัยวางแนวทางการคุ้มครอง right to be forgotten อย่างแคบ โดยจำกัดขอบเขตแต่เพียงสิทธิในการเรียกร้องให้ผู้ให้บริการ search engine (Google สำหรับคดีนี้) ลบ link ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลอันเป็นผลมาจากการสืบค้นผ่านชื่อและ

นามสกุลของเจ้าของข้อมูลส่วนบุคคล โดยไม่มีการวินิจฉัยวางหลักให้สิทธิในการเรียกร้องให้เจ้าของ webpage ซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคลในขั้นต้นเนื่องจากเป็นผู้เผยแพร่ข้อมูลบน webpage ของตนอันก่อให้เกิด link เชื่อมโยงมายังผลการค้นหาของ Google นั้นต้องดำเนินการลบข้อมูลส่วนบุคคลดังกล่าวแต่อย่างไร

ผลโดยนัยของคำวินิจฉัยฉบับนี้จึงเป็นการจำกัดขอบเขตของ right to be forgotten ภายใต้ Directive 95/46/EC เพียง "สิทธิที่จะลบ link แสดงผลการสืบค้นทางอินเทอร์เน็ต (right to de-listing) แทนที่จะเป็น "สิทธิที่จะถูกลืมจากโลกดิจิทัล (right to digital oblivion)" อย่างแท้จริง

หลักการดังกล่าวนี้ได้ถูกยืนยันจากเอกสารกำหนดแนวทางทางดำเนินการตามคำพิพากษา โดยคณะทำงานตาม Article 29 แห่ง Directive (Article 29 of the Data Protection Working Party : AWP29) ซึ่งเป็นองค์กรที่ปรึกษาและกำกับดูแลความสอดคล้องในการบังคับใช้ Directive แก่ องค์กรคุ้มครองข้อมูลส่วนบุคคลของทุกประเทศสมาชิก ว่าการบังคับขอเรียกร้องของเจ้าของข้อมูลส่วนบุคคลตามสิทธิที่ได้รับการรับรองตามคำวินิจฉัยในคดี Google Spain นั้น ไม่รวมถึงการลบข้อมูลส่วนบุคคลออกจาก webpage ต้นฉบับที่ปรากฏข้อมูลส่วนบุคคลนั้นๆ ในการนี้ webpage ต้นฉบับดังกล่าวจะยังสามารถเข้าถึงได้ผ่านการสืบค้นโดยใช้ถ้อยคำอื่นที่ไม่ใช่ชื่อและชื่อสกุลของเจ้าของข้อมูลส่วนบุคคล หรือโดยการเข้าถึงโดยตรงผ่าน URL

กรณีจึงเห็นได้ว่าผลของคำวินิจฉัยลดทอนประสิทธิภาพในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลที่ประสงค์จะให้มีการลบเลือนความเสียหายจากข้อมูลส่วนบุคคลดังกล่าว ออกจากโลกออนไลน์อย่างถาวร เพราะแม้ว่าในทางปฏิบัติแล้วการลบ link แสดงผลการค้นหาออกก็ ยังผลให้เป็นเรื่องยากที่ผู้ใช้อินเทอร์เน็ตจะสามารถสืบค้นเพื่อเข้าถึงข้อมูลส่วนบุคคลดังกล่าวใน webpage ต้นฉบับ แต่หากผู้ใช้ดังกล่าวได้เคยสืบค้นและบันทึก URL ของ webpage ดังกล่าวเอาไว้ก่อนแล้ว หรือเจ้าของ webpage ต้นฉบับดำเนินการจัดพิมพ์เผยแพร่หน้า webpage เดิมซ้ำใน URL ใหม่อยู่เรื่อยๆ ประวัติส่วนตัวอันเป็นความเสียหายของเจ้าของข้อมูลส่วนบุคคลจะไม่สามารถลบเลือนได้ตลอดไป

ภายใต้หลักการที่จำกัดอยู่ที่ right to de-listing นี้ CJEU กลับวางหลักเกณฑ์ที่ค่อนข้าง กว้างขวางเพื่อเอื้อให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิในการลบ link แสดงผลการสืบค้นได้ง่าย ขึ้น โดยได้วางหลักเกณฑ์กว้างๆ เกี่ยวกับลักษณะของข้อมูลส่วนบุคคลที่จะสามารถใช้สิทธิลบ link แสดงผลการสืบค้นได้นั้น เพียงแต่ "ไม่มีความสำคัญจำเป็นไม่มีความเกี่ยวข้องไม่เกี่ยวข้องอีกต่อไป

หรือเพียงแต่ไม่เป็นที่ปรารถนาสำหรับเจ้าของข้อมูลส่วนบุคคล ก็เป็นการเพียงพออีกทั้งเจ้าของข้อมูลส่วนบุคคลไม่มีภาระการพิสูจน์ในความเสียหาย และในการลบ link แสดงผลการสืบค้นนั้นไม่จำกัดอยู่แต่เพียงกรณีที่ webpage ต้นฉบับนั้นแสดงข้อมูลไม่ถูกต้อง ไม่สมบูรณ์หรือไม่ชอบด้วยกฎหมายเท่านั้น

นัยหนึ่งเท่ากับว่าแม้ข้อมูลดังกล่าวจะถูกต้องสมบูรณ์และชอบด้วยกฎหมายทุกประการ แต่หากเจ้าของข้อมูลส่วนบุคคลนั้นไม่ประสงค์ในความคงอยู่ของข้อมูลในโลกออนไลน์แล้ว ก็สามารถเรียกร้องต่อผู้ให้บริการ search engine ให้ดำเนินการลบผลการค้นหาได้เสมอโดยไม่ต้องนำสืบพิสูจน์ความเสียหาย (ซึ่งในประเด็นนี้จะเห็นได้ว่ามีความแตกต่างจากการใช้สิทธิตามกฎหมายแพ่งลักษณะละเมิดหรือกฎหมายอาญาฐานหมิ่นประมาท) แต่ไม่สามารถขอให้เจ้าของ webpage ต้นฉบับลบข้อมูลดังกล่าวได้ ทั้งนี้ CJEU ได้พยายามปรับใช้ Directive 95/46/EC Article 12 (b) ว่าด้วยสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับตน และดำเนินการแก้ไข ลบ หรือป้องกันการเข้าถึง ซึ่งข้อมูลส่วนบุคคลที่ไม่เป็นไปตาม Directive นี้ กับผู้ให้บริการ search engine แม้โดยเนื้อแท้แล้วสิทธิดังกล่าวควรจะใช้ยันกับเจ้าของ webpage ซึ่งเป็นผู้ประมวลผลข้อมูลขึ้นต้น และแม้ว่าผลของคำวินิจฉัยคัดค้านข้างเอื้อประโยชน์ต่อเจ้าของข้อมูลส่วนบุคคลให้สามารถบังคับใช้สิทธิได้ค่อนข้างกว้างขวาง

อย่างไรก็ตาม CJEU มิได้วางแนวทางกำหนดหลักเกณฑ์ในการพิจารณาคำร้องขอให้ลบผลการสืบค้นที่ชัดเจนไว้ ดังปรากฏในคำวินิจฉัยฉบับนี้ว่าข้อเท็จจริงเกี่ยวกับระยะเวลาที่เนิ่นนานผ่านไปกว่า 16 ปี ความทุกข์ทรมานใจที่ได้รับจากความคงอยู่ของข้อมูลดังกล่าวในโลกออนไลน์ ตลอดจนข้อเท็จจริงเกี่ยวกับสถานะทางการเงินที่เปลี่ยนไปของนาย Gonz lez ในปัจจุบันที่ไม่มีปัญหาสุขภาพคล่องอีกแล้วนั้น ไม่ได้ถูกหยิบยกขึ้นมาเป็นข้อพิจารณาในการอนุญาตให้มีการลบผลการสืบค้นในคดีแต่อย่างใด

โดยผลของคำวินิจฉัยฉบับนี้ก่อให้เกิดมาตรการเยียวยาขึ้นต้นอย่างไม่เป็นทางการโดยผู้ให้บริการ search engine ที่ได้รับมอบอำนาจโดยพฤตินัยให้ทำการพิจารณาลักษณะของข้อมูลส่วนบุคคลว่าสามารถดำเนินการลบ link แสดงผลการสืบค้นตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลได้หรือไม่ เป็นรายกรณี ซึ่งมีดุลพินิจที่ค่อนข้างกว้างขวาง ขึ้นต่อมาจึงเป็นขั้นตอนของการยื่นข้อร้องเรียนโต้แย้งดุลพินิจของผู้ให้บริการ search engine ในกรณีที่ตอบปฏิเสธคำร้องขอของเจ้าของข้อมูลส่วนบุคคลไปยังองค์กรคุ้มครองข้อมูลส่วนบุคคลหรือศาลของแต่ละประเทศเพื่อทบทวนดุลพินิจและบังคับการให้เป็นไปตามสิทธิของเจ้าของข้อมูลส่วนบุคคล ในเบื้องต้นแม้จะดูเหมือนว่าแนวทางที่ CJEU วางไว้จะเป็นการอำนวยความสะดวกและประหยัดค่าใช้จ่ายในการเรียกร้องสิทธิโดยตรงไปยัง

ผู้ให้บริการ search engine แทนที่จะเริ่มต้นกระบวนการไปยังองค์กรคุ้มครองข้อมูลส่วนบุคคลหรือศาล โดยมีหลักฐานสนับสนุนจากผู้ตอบแบบสอบถามชาวสหราชอาณาจักรในปี ค.ศ.2014 ว่า มีเพียงร้อยละ 1 ของผู้ตอบแบบสอบถามเท่านั้นที่มีความรู้เกี่ยวกับองค์กรคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร (Information Commissioner's Office : ICO) ในขณะที่ Google นั้นเป็นที่รู้จักแพร่หลายและเป็นเจ้าตลาดการให้บริการ search engine ในประเทศสมาชิก EU โดยครองส่วนแบ่งการตลาดกว่าร้อยละ 90

สำหรับ Google นั้น เพื่อปฏิบัติตามคำวินิจฉัยในคดี Google Spain นี้ Google ได้ดำเนินการจัดตั้ง web platform เพื่อรับพิจารณาคำร้องขอจำนวนมากจากผู้ร้องที่อยู่ในสหภาพยุโรปเป็นการเฉพาะ อย่างไรก็ตาม จากรายงานผลการดำเนินงานเพื่อความโปร่งใสของ Google ข้อมูล ณ เดือนเมษายน ค.ศ.2018 นั้น ชี้ให้เห็นว่า จำนวน URL ที่ Google ใช้ดุลพินิจลบตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลมีจำนวนน้อยกว่าจำนวน URL ที่ได้รับการปฏิเสธไม่ดำเนินการลบ กล่าวคือ จากจำนวน 665,612 คำร้องขอที่ Google ได้รับคิดเป็นจำนวน 2,470,351 URLs นั้น Google ใช้ดุลพินิจลบ link แสดงผลการค้นหาเพียงร้อยละ 43 ของจำนวน URL ขณะที่ปฏิเสธคำร้องขอถึงร้อยละ 56.2 จากจำนวน URL ทั้งหมด

ดังนั้นจึงสรุปผลในด้านของประสิทธิภาพในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลในภาพรวมได้ว่า ในขณะที่ผู้ร้องส่วนน้อยสามารถเร่งรัดการใช้สิทธิลบผลการสืบค้นประวัติส่วนตัวของตนให้สำเร็จผ่านการร้องขอโดยตรงไปยังผู้ให้บริการ search engine นั้น อีกกว่าครึ่งหนึ่งของผู้ยื่นคำร้องที่สุดแล้วจะต้องกลับเข้าสู่การดำเนินการในชั้นองค์กรคุ้มครองข้อมูลส่วนบุคคลหรือศาลจึงนับได้ว่าขั้นตอนการยื่นคำร้องโดยตรงไปยังผู้ให้บริการ search engine อาจเป็นความล่าช้าที่เกิดขึ้นโดยไม่จำเป็น (undue delay) สำหรับผู้ร้องกลุ่มหลัง

CJEU ปรึบใช้ Article 2 (b) ของ Directive 95/46/EC โดยตีความอย่างกว้างให้กิจกรรมการให้บริการของผู้ให้บริการ search engine ต้องด้วยการกระทำของผู้ประมวลผลข้อมูล (data controller) ดังนั้น search engine มีหน้าที่ต้องปฏิบัติตาม Directive ในฐานะดังกล่าว โดย CJEU ได้ให้เหตุผลว่า กิจกรรมของผู้ให้บริการ search engine อันประกอบด้วย การจัดพื้นที่แสดงผล (Locating) การจัดลำดับการแสดงผล (Indexing) และกระทำให้อบบนหน้า webpage ต้นฉบับอยู่ในสถานะที่สามารถสืบค้นได้ (making available to a searcher) นั้น ต้องด้วยลักษณะของการประมวลผลข้อมูล แม้ว่าโดยเนื้อแท้แล้วการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลในชั้นต้นนั้น



เกิดขึ้นจากการประมวลผลข้อมูลโดยแสดงข้อมูลส่วนบุคคลดังกล่าวบนหน้า webpage ต้นฉบับของบุคคลที่สามก็ตาม<sup>57</sup>

CJEU ได้เน้นย้ำว่ากิจกรรมของผู้ให้บริการ search engine ช่วยให้ผู้ใช้งานอินเทอร์เน็ตสามารถเข้าถึงข้อมูลส่วนบุคคลที่ปรากฏอยู่บน webpage ต้นฉบับได้อย่างง่ายดายมากขึ้นเพียงแค่นำค้นหาโดยใช้ชื่อและนามสกุลของเจ้าของข้อมูลส่วนบุคคล มิเช่นนั้นแล้วย่อมจะเข้าถึงยากลำบากหากจะต้องเข้าถึงผ่าน URL ของ webpage นั้นๆ โดยตรง ดังนั้น การตีความอย่างกว้างดังกล่าวนี้จึงเป็นการดำเนินการเพื่อให้เกิดความมั่นใจซึ่งประสิทธิภาพและความครบถ้วนสมบูรณ์ในมาตรการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล มิเช่นนั้นแล้ว มาตรการคุ้มครองสิทธิดังกล่าวย่อมแทบไม่มีความหมาย

อย่างไรก็ตาม ในประเด็นนี้ยังมีข้อควรพิจารณาอยู่เช่นกันว่า ในความเป็นจริงแล้วผู้ให้บริการ search engine ที่กิจกรรมของผู้ให้บริการต้องด้วยลักษณะการกระทำของผู้ประมวลผลข้อมูลตาม Directive นั้นมิใช่มีแต่เพียง Google เท่านั้น แต่รวมถึงผู้ให้บริการรายอื่นๆ เช่น Bing Yahoo หรือ Baidu ด้วย กรณีจึงอาจเกิดปัญหาในทางปฏิบัติขึ้นได้ว่าแม้ในกรณีที่ Google เห็นพ้องด้วยกับคำร้องขอให้ลบ link แสดงผลการสืบค้น แต่หากเจ้าของข้อมูลส่วนบุคคลมิได้ยื่นคำร้องขอไปยังผู้ให้บริการรายอื่นด้วย หรือได้ยื่นคำร้องขอแต่ผู้ให้บริการรายอื่นนั้นใช้ดุลพินิจที่แตกต่างออกไปพร้อมทั้งปฏิเสธคำร้องขอนั้น ผู้ใช้บริการอินเทอร์เน็ตย่อมสามารถสืบค้นประวัติข้อมูลส่วนบุคคลผ่านชื่อและนามสกุลของเจ้าของข้อมูลส่วนบุคคลได้เพิ่มเติม เพียงแต่ย้ายการสืบค้นไปดำเนินการกับผู้ให้บริการรายอื่นๆ

คำวินิจฉัยในคดี Google Spain มิได้วางหลักเกณฑ์โดยตั้งอยู่บนพื้นฐานของ right to digital oblivion ซึ่งโดยผลลัพธ์จากการลบข้อมูลส่วนบุคคลบน webpage ต้นฉบับย่อมสามารถทำให้ผลการสืบค้นบนทุกผู้ให้บริการ search engine เลือนหายไปโดยอัตโนมัติเมื่อไม่มีข้อมูลต้นฉบับคงเหลือให้ค้นหา กลับกันคำวินิจฉัยฉบับนี้กลับมิได้มีการวางกลไกใดๆ เพื่อที่จะช่วยให้การบังคับใช้ right to delisting มีความรวดเร็วและครอบคลุมทุกผู้ให้บริการ search engine การยื่นคำร้องขอเพียงฉบับเดียว ดังนั้น สรุปเป็นขั้นตอนในภาพรวมสำหรับการบังคับใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลให้เป็นไปอย่างครบถ้วน จะประกอบด้วยการยื่นคำร้องแต่ละคำร้องไปยังผู้ให้บริการ search engine แต่ละรายรอผลการพิจารณาจากแต่ละผู้ให้บริการ ตลอดจนการยื่นข้อร้องเรียนเพื่อทบทวนดุลพินิจของผู้

<sup>57</sup> ผศ.ดร.ปิติ เอี่ยมจำรูญลาภ, เรื่อง บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten)

ให้บริการรายที่ปฏิเสธคำร้องขอไปยังองค์กรคุ้มครองข้อมูลส่วนบุคคลหรือศาล ซึ่งจะเห็นได้ว่าขั้นตอนกระบวนการทั้งหมดค่อนข้างซับซ้อนและล่าช้าในทางปฏิบัติ<sup>58</sup>

การศึกษาตัวบทกฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายลำดับรองแนวปฏิบัติคำวินิจฉัย และคำพิพากษาของศาลทั้งในประเทศไทยและต่างประเทศนี้ แสดงให้เห็นถึงสาระสำคัญของกฎหมายซึ่งมีภารกิจในการคุ้มครองสิทธิที่จะถูกลืม กฎหมายคุ้มครองข้อมูลส่วนบุคคลระบุถึงตัวผู้ทรงสิทธิกล่าวคือตอบคำถามที่ว่า "ใคร" เป็นผู้ทรงสิทธิที่จะสามารถเรียกร้องให้มีการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้ กฎหมายของทุกประเทศระบุว่าผู้ทรงสิทธิ ได้แก่ "เจ้าของข้อมูลส่วนบุคคล" โดยมีข้อสังเกตว่าสิทธิดังกล่าวถูกบัญญัติให้ตัวเจ้าของข้อมูลส่วนบุคคลมีสิทธิ "เรียกร้อง" ให้มีการลบทำลายหรือทำให้ข้อมูลส่วนบุคคล โดยมีเพียงมาตรา 17 ของ GDPR เท่านั้นที่บัญญัติเจาะจงถึง "สิทธิที่จะถูกลืม (Right to be Forgotten)" ส่วนกฎหมายของประเทศอื่นๆ รวมถึงของประเทศไทยไม่ได้เรียกสิทธิในการขอให้ลบข้อมูลว่าสิทธิที่จะถูกลืม

ประการที่สอง กฎหมายคุ้มครองข้อมูลส่วนบุคคลระบุถึงผู้มีหน้าที่ดำเนินการลบทำลาย หรือทำให้ข้อมูลส่วนบุคคลซึ่งไม่ได้ถูกเรียกว่าผู้ควบคุมข้อมูลส่วนบุคคลในทุกๆ กรณีกฎหมายของประเทศไทย GDPR กำหนดหน้าที่ลบข้อมูลตามคำขอแก่ "ผู้ควบคุมข้อมูลส่วนบุคคล"

ประการที่สาม ในส่วนเนื้อหาของสิทธิที่จะถูกลืมนั้นกฎหมายของทุกประเทศให้ความสำคัญกับการลบข้อมูลส่วนบุคคล (โดยไม่เน้นที่การถูกลืม) เพื่อประโยชน์ในการดำเนินการของบุคคลที่เกี่ยวข้อง จึงมีการออกแนวปฏิบัติที่เกี่ยวข้องกับการลบข้อมูลส่วนบุคคลกล่าวคือ แนวปฏิบัติที่เกี่ยวข้องกับประเภทหรือลักษณะของสิทธิที่จะถูกลืมที่อยู่บนโปรแกรมสืบค้นข้อมูลของสหภาพยุโรปโดย EDPB แนวปฏิบัติที่เกี่ยวข้องกับวิธีการลบข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคล (ในส่วนของ การลบข้อมูล) ของสหราชอาณาจักรโดย CO แนวทางการปฏิบัติเกี่ยวหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศออสเตรเลีย กฎเพื่อบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของไต้หวัน แนวปฏิบัติในการลบข้อมูลส่วนบุคคลและการทำข้อมูลนิรนามของฮ่องกง และแนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ อย่างไรก็ตามกรณีศึกษาและคำวินิจฉัยต่างๆ แสดงให้เห็นว่าการลบผลการค้นหาอาจไม่ได้ทำให้มีการลบข้อมูลโดยผู้เผยแพร่ข้อมูลอื่น

<sup>58</sup> หนังสือพิมพ์ไทยโพสต์ [ออนไลน์]. เข้าถึงได้จาก [http://lawdrafter.blogspot.com/2018/05/blog-post\\_22.html](http://lawdrafter.blogspot.com/2018/05/blog-post_22.html)

ประการที่สี่ สิทธิที่จะถูกลืมถูกจำกัดได้โดยความจำเป็นที่บุคคลอื่นมีสิทธิในการเข้าถึงข้อมูล และเสรีภาพในการแสดงความคิดเห็น ประโยชน์สาธารณะอื่นอันเกิดจากการที่ข้อมูลไม่ถูกลบ และข้อจำกัดของกฎหมายที่ไม่อาจมีผลบังคับในต่างประเทศไทย จากองค์ประกอบทั้งสี่ข้อนี้ มีความจำเป็นต้องวิเคราะห์ต่อไปว่ามาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นสามารถคุ้มครองสิทธิที่จะถูกลืมได้เพียงใดและมีข้อจำกัดประการใดหรือไม่หากเปรียบเทียบกับกฎหมายของต่างประเทศ<sup>59</sup>

---

<sup>59</sup> ผศ.ดร.ปิติ เอี่ยมจำรูญลาภ, เรื่อง บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) หน้า 165

## บทที่ 4

### วิเคราะห์ปัญหากฎหมายการลบทำลายข้อมูลส่วนบุคคลของประเทศไทย เกี่ยวกับแนวทางการแก้ไขการลบและทำลายข้อมูลส่วนบุคคล

การศึกษาการลบทำลายข้อมูลในกฎหมายไทย มาตรา 33 และมาตรา 37 (3) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ว่ามีหลักเกณฑ์ตลอดจนแนวทางในทางปฏิบัติใช้อย่างไร ด้วยเหตุนี้ การศึกษากฎหมาย GDPR สหภาพยุโรปและวิเคราะห์กฎหมายในเชิงเปรียบเทียบการวิเคราะห์และเปรียบเทียบแนวทางในกรปฏิบัติในทางกฎหมายการลบทำลายข้อมูลส่วนบุคคล เพื่อให้เกิดความเข้าใจถึงความคล้ายคลึงและแตกต่างของกฎหมายไทยและกฎหมายของสหภาพยุโรปท้ายที่สุดเพื่อเผยให้เห็นถึงแนวทางปฏิบัติของกฎหมายเพื่อประโยชน์ในการพัฒนา บทบัญญัติอันจะได้นำเสนอในบทที่ 5 ต่อไป การเปรียบเทียบกับบทกฎหมายและข้อเท็จจริงในสังคมโดยวิเคราะห์จากบทกฎหมายสหภาพยุโรป กับองค์ประกอบอันเป็นสาระสำคัญของกฎหมาย

#### 4.1 การบัญญัติถึงตัวผู้ทรงสิทธิที่จะถูกลืม

บัญญัติให้ “เจ้าของข้อมูลส่วนบุคคล” มีสิทธิขอให้ ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัว บุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ การบัญญัติให้เจ้าของข้อมูลส่วนบุคคลเป็นผู้ทรงสิทธิอันเป็นแนวทางการ บัญญัติกฎหมายที่สอดคล้องกับมาตรา 17 ของ GDPR ซึ่งสามารถกล่าวได้ว่าการที่กฎหมายจะคุ้มครองสิทธิที่จะถูกลืมได้นั้นมีจุดเริ่มต้นจากการที่กฎหมายกำหนดตัวผู้ทรงสิทธิเสียก่อน<sup>60</sup>

##### 4.1.2 เจ้าของข้อมูลส่วนบุคคล (Data Subject)

มาตรา 17 ของ GDPR บัญญัติให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบหรือทำลายข้อมูลส่วนบุคคลและได้ให้นิยามคำว่า “เจ้าของข้อมูลส่วนบุคคล” ตามมาตรา 4(1) เอาไว้ว่าเจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง บุคคลที่สามารถถูกระบุอัตลักษณ์ได้ไม่ว่าจะโดยตรงหรือโดยอ้อม โดยเฉพาะอย่างยิ่งด้วยการอ้างอิงจากสิ่งระบุอัตลักษณ์เป็นการเฉพาะ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลสถานที่ สิ่งระบุอัตลักษณ์ออนไลน์ หรือปัจจัยอย่างหนึ่ง

<sup>60</sup> ผศ.ดร.ปิติ เอี่ยมจำรุงลาภ, เรื่อง บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) หน้า 168

หรือมากกว่าที่เจาะจงไปยังอัตลักษณ์ทางกายภาพ กายวิถยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคลธรรมดา นั้น บัญญัติรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลให้สามารถร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบหรือทำลายข้อมูล ส่วนบุคคลได้ให้นิยามว่าเจ้าของข้อมูลส่วนบุคคลเอาไว้ตามนิยามของ เจ้าของข้อมูลส่วนบุคคลที่กำหนดไว้ใน GDPR เช่นเดียวกับแนวทางที่ปรากฏในสหภาพยุโรป กำหนดให้สิทธิเจ้าของข้อมูลส่วนบุคคลมีสิทธิในการลบข้อมูลส่วนบุคคลเช่นเดียวกัน โดยให้นิยามคำว่า “เจ้าของข้อมูลส่วนบุคคล (Data Subject)” ว่าหมายถึง บุคคลธรรมดาที่เป็นเจ้าของข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม ประมวลผลและใช้งาน มาตรา 16 (e) ของ PH PDPA 2012 กำหนดให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) มีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบหรือทำลายข้อมูลส่วนบุคคล โดยได้ให้นิยามว่าเจ้าของข้อมูลส่วนบุคคลหมายถึงบุคคลธรรมดา ซึ่งข้อมูลส่วนบุคคลของบุคคลคนนั้นถูกประมวลผล ได้กำหนดนิยามของเจ้าของข้อมูลส่วนบุคคล (Data Subject) เอาไว้ว่าเป็นปัจเจกบุคคล (Individual) ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตาม มีข้อสังเกตว่า มาตรา 26 ของ HK PDPO 1996 นั้นมิได้บัญญัติโดยรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลที่จะร้องขอให้มีการลบทำลาย ข้อมูลส่วนบุคคลโดยตรง หากแต่บัญญัติให้ตัวผู้ใช้ข้อมูล (Data User) (ซึ่งได้แก่บุคคลที่มีอำนาจในการเก็บ รวบรวม ถือครอง ประมวลผล และใช้ข้อมูลส่วนบุคคล) 266 มีหน้าที่ในการลบทำลายข้อมูลส่วนบุคคลที่หมดความ จำเป็นที่จะต้องถูกประมวลผลตามวัตถุประสงค์อีกต่อไป จึงอาจกล่าวได้ว่ามาตรา 26 ของ HK PDPO 1996 นี้มี ลักษณะที่สอดคล้องกับหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 37(3) ของพระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคล พ.ศ. 2562 มากกว่าจะเป็นบทบัญญัติในส่วนของสิทธิที่ของเจ้าของข้อมูลส่วนบุคคลมาตรา 33 โดยตรง<sup>61</sup>

#### 4.2 การบัญญัติถึงเนื้อหาการคุ้มครองสิทธิที่จะถูกลืม

การศึกษาตัวบทกฎหมาย แนวปฏิบัติคำวินิจฉัยและคำพิพากษาของศาลในต่างประเทศ ทำให้เห็นว่ากฎหมายจำเป็นต้องระบุถึงรายละเอียดเกี่ยวกับการคุ้มครองสิทธิที่จะถูกลืมโดยมีประเด็นที่ต้องพิจารณาความครอบคลุมของกฎหมายในประเด็น ได้แก่ การร้องขอผู้ทรงสิทธิและหน้าที่ดำเนินการโดยผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม ข้อจำกัดการคุ้มครองจากการไม่มีคำว่าสิทธิที่จะถูกลืม การลบหรือทำลายข้อมูลเมื่อข้อมูลส่วนบุคคลหมดความจำเป็นที่จะต้องถูกประมวลผลตาม

<sup>61</sup> ผศ.ดร.ปิติ เอี่ยมจารุณุลาก (2564) บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten). หน้า 170

วัตถุประสงค์ และการกำหนด รายละเอียดเกี่ยวกับการลบทำลายและทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของ ข้อมูลส่วนบุคคลได้

#### 4.3 การลบหรือทำลายข้อมูลเมื่อข้อมูลส่วนบุคคลหมดความจำเป็นที่จะต้องถูกประมวลผลตามวัตถุประสงค์

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศนั้นบัญญัติให้มีการลบทำลายหรือทำให้ข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในกรณีที่ข้อมูลส่วนบุคคล “หมดความจำเป็น” ที่จะต้องถูกใช้ตามวัตถุประสงค์ของการเก็บรวบรวม เช่น GDPR ซึ่งใช้ถ้อยคำว่า “เมื่อข้อมูลส่วนบุคคลหมดความจำเป็น เพื่อการประมวลผลข้อมูลอีกต่อไป”<sup>62</sup> ซึ่งอาจเป็นผลจากการผ่านไปของเวลา หน่วยงานรัฐหรือองค์กรนอกภาครัฐจะต้องลบหรือหยุด ประมวลผลข้อมูล”<sup>63</sup> ซึ่งสอดคล้องกับตัวบทกฎหมายของมาตรา 33 และมาตรา 37(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างไรก็ตามกรณีมีข้อสังเกตว่าตัวบทกฎหมายเหล่านี้ถูกบัญญัติขึ้นโดยใช้ถ้อยคำที่มีความยืดหยุ่นและเปิดโอกาสให้มีการปรับใช้กฎหมายให้เหมาะสมกับกรณี ด้วยเหตุนี้การปรับใช้กฎหมายจึงมีอาจหลีกเลี่ยงการพิจารณาข้อเท็จจริงเป็นรายกรณี

##### 4.3.1 การพิจารณาข้อเท็จจริงในเรื่องเวลาผ่านไป

การพิจารณาว่า “ข้อมูลส่วนบุคคลหมดความจำเป็นหรือไม่และเมื่อใด” นั้นเป็นข้อพิจารณาสำคัญในการคุ้มครองสิทธิที่จะถูกลืม เช่น คดี Hurbain v. Belgium แสดงให้เห็นว่าสำนักพิมพ์ (Le Soir) นั้นมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลเนื่องจากเป็นผู้ทำการเผยแพร่ข้อมูลส่วนบุคคลของคนขับรถซึ่งเป็นต้นเหตุให้เกิดอุบัติเหตุ ที่ทำให้มีคนอื่นเสียชีวิต ศาลได้ทำการวินิจฉัยถึงระยะเวลาได้ผ่านไปนับจากวันที่ได้มีการเผยแพร่ข้อมูลครั้งแรก (โดยศาลได้พิจารณาและชั่งน้ำหนักถึงเสรีภาพในการแสดงความคิดเห็นของหนังสือพิมพ์ด้วย) โดยในคดีนี้ศาลได้ สรุปว่าเวลานับจากวันเกิดอุบัติเหตุได้ผ่านมานานแล้วและผู้ก่อเหตุก็ไม่ได้เป็นบุคคลสาธารณะ กรณีไม่ปรากฏ คุณค่าของการที่ยังคงมีชื่อและสกุลของบุคคลที่ก่อเหตุในข่าว การเกิดสถิติของอุบัติเหตุบนท้องถนนนั้นยังคงทำได้ โดยไม่ต้องมีชื่อของบุคคลอยู่

<sup>62</sup> ผศ.ดร.ปิติ เอี่ยมจารุญญลาภ (2564) บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten). หน้า 183

<sup>63</sup> Personal Data Protection Act 2015, Article 11.

#### 4.3.2 การสิ้นสุดของเวลา

สื่อมวลชนย่อมมีเสรีภาพในการนำเสนอข้อมูลข่าวสารต่างๆ ข้อมูลที่สื่อมวลชน เช่น สำนักข่าวนำเสนอ โดยผ่านฐานหนังสือพิมพ์ออนไลน์ อาจถูกค้นหาและเข้าถึงโดยบุคคลทั่วไปในสังคม ศาลในคดี Plaintiff X v. PrimaDanoi ยอมรับถึงความสำคัญของสิทธิในการรายงานข้อมูล แต่ก็ได้วินิจฉัยว่า “ข้อมูลที่มีความอ่อนไหว (Sensitive Information) และข้อมูลส่วนตัว (Private Information) ไม่ควรจะถูกทำให้เข้าถึงได้โดยสาธารณชน โดยปราศจากการจำกัดเวลา (เว้นแต่สำนักพิมพ์จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล) การบัญญัติโดยใช้ถ้อยคำที่ยืดหยุ่น เช่น “เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตาม วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล” ตามมาตรา 33 ของพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562 ย่อมเปิดโอกาสให้บุคคลที่เกี่ยวข้องสามารถใช้ดุลพินิจให้เหมาะกับกรณี และช่วยเปิด โอกาสให้มีการข่งน้ำหนักประโยชน์ต่างๆ ที่เกี่ยวข้องและอาจขัดแย้งกันในบางกรณี อย่างไรก็ตามในบางกรณี ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลอาจไม่ได้ระบุว่าหากสิ้นสุดระยะเวลาของ ข้อมูลส่วนบุคคลจำต้องถูกทำลายหรือลบทิ้งไปไว้อย่างชัดเจน แต่เป็นการบัญญัติในทำนองให้ผู้ควบคุมข้อมูล ส่วนบุคคลปฏิบัติตามกฎหมายอื่นที่ไม่ใช่กฎหมายคุ้มครองข้อมูลส่วนบุคคล

เมื่อวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นไม่มีประโยชน์ต่อการเก็บรักษาข้อมูลส่วนบุคคลอีกต่อไป และการเก็บรักษาข้อมูลนั้นไม่มีความจำเป็นต่อวัตถุประสงค์ด้านกฎหมายหรือธุรกิจอีก แม้กฎหมายฉบับดังกล่าวไม่ได้กำหนดระยะเวลาในการเก็บข้อมูลส่วนบุคคลไว้อย่างชัดเจน แต่ผู้ควบคุมข้อมูลส่วนบุคคลอาจยึดถือ ระยะเวลาการเก็บรักษาข้อมูลตามมาตรฐานที่กำหนดโดยกฎหมายที่เกี่ยวข้องกับธุรกิจของผู้ควบคุมข้อมูลส่วนบุคคล หรืออาจกำหนดระยะเวลาการสิ้นสุดของการเก็บรักษาข้อมูลนั้นเองโดยพิจารณาจากปัจจัยที่กำหนด อีกทั้งในมาตรา 5(1)(e) ของ GDPR ที่เป็นหนึ่งในหลักการคุ้มครองข้อมูลส่วนบุคคลไว้ว่าข้อมูลส่วนบุคคล จำต้องเก็บไว้ไม่เกินกว่าที่จำเป็นเพื่อวัตถุประสงค์ในการเก็บรวบรวม โดยเรียกเงื่อนไขตามบทบัญญัติข้อนี้ว่าเป็น “ข้อจำกัดของการเก็บ (Storage Limitation)” โดยไม่ได้กำหนดระยะเวลาในการเก็บว่าควรต้องเก็บไว้นาน เพียงใด แต่เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่อาจกำหนดระยะเวลาการสิ้นสุดของการเก็บข้อมูลส่วนบุคคลไว้เอง

#### 4.3.3 การกำหนดรายละเอียดเกี่ยวกับการลบทำลายและทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

มาตรา 33 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติเนื้อหาของสิทธิที่จะถูกลืมเอาไว้ ได้แก่การลบ ทำลาย หรือทำให้ข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้โดยไม่ได้บัญญัติ รายละเอียดของการดำเนินการเอาไว้ว่าในการลบหรือทำลายข้อมูลส่วนบุคคลนั้นจะต้องดำเนินการอย่างไร ซึ่งเป็น แนวทางที่สอดคล้องกับแนวทางของ GDPR การที่ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม นั้นไม่ทราบถึงรายละเอียดการดำเนินการย่อมส่งผลให้เกิดปัญหาการปฏิบัติตามกฎหมายในทางปฏิบัติได้ เช่น อาจมีคำถามขึ้นได้ว่าการดำเนินการใดที่จะถือได้ว่าผู้ควบคุมข้อมูลส่วนบุคคลได้ดำเนินการตามกฎหมายเพื่อคุ้มครองสิทธิที่ จะถูกลืมแล้ว เพื่อแก้ปัญหาดังกล่าวหน่วยงานคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศมิได้ดำเนินการแก้ไข บทบัญญัติในกฎหมายคุ้มครองข้อมูลส่วนบุคคลหากแต่ได้ออกแนวปฏิบัติหรือกฎหมายลำดับรองเพื่อขยายความ และให้รายละเอียดเกี่ยวกับการลบหรือทำลายข้อมูลส่วนบุคคล

##### 4.3.3.1 การบัญญัติถ้อยคำในเรื่องการลบทำลายข้อมูลส่วนบุคคลข้อแตกต่างระหว่างกฎหมายเกี่ยวกับการลบทำลายข้อมูลส่วนบุคคล

กฎหมายต่างประเทศไม่ได้บัญญัตินิยามของการลบทำลายข้อมูลส่วนบุคคลเอาไว้ แต่ ICO ได้ให้คำอธิบายว่า ข้อมูลส่วนบุคคลนั้นจะต้องถูกลบโดยไม่สามารถกู้คืนกลับมาได้ นอกจากกรณีของการลบข้อมูลส่วนบุคคลแล้ว ยังมีแนวทางอื่นที่เป็นการจัดการกับการลบข้อมูลในรูปแบบอื่น ดังเช่นในการทำให้ข้อมูลอยู่เหนือการใช้งาน แนวปฏิบัติฉบับนี้ระบุให้การทำให้ออกเหนือการใช้งาน หากปรากฏว่าข้อมูลดังกล่าวไม่ได้ถูกลบออกไปจริงจำเป็นต้องเป็นกรณีที่ปรากฏด้วยว่าผู้ควบคุมข้อมูลส่วนบุคคลนั้นได้ปฏิบัติให้เป็นไปกรณีดังนี้ (1) ไม่สามารถหรือจะไม่พยายามใช้ข้อมูลส่วนบุคคลเพื่อแจ้งให้ทราบถึงการตัดสินใจใดๆ ที่เกี่ยวข้องกับบุคคลใดๆ หรือในลักษณะที่ส่งผลกระทบต่อบุคคลใดๆ และไม่ว่าด้วยวิธีใดก็ตาม (2) ไม่อนุญาตให้หน่วยงานอื่นใดสามารถเข้าถึงข้อมูลส่วนบุคคลนั้นได้ (3) จัดให้มีการมั่นคงปลอดภัยทางด้านเทคนิคและด้านการบริหารจัดการและ (4) ให้คำมั่นว่าจะลบข้อมูลนั้นทิ้งอย่างถาวร เมื่อหรือหากสามารถดำเนินการเช่นนั้นได้<sup>64</sup> แม้กฎหมายต่างประเทศไม่ได้บัญญัติถึงแนวปฏิบัติในเรื่องการลบทำลายข้อมูลส่วนบุคคล แนวการปฏิบัติจะออก โดย OAIIC ซึ่งได้กล่าวถึงการทำลาย

<sup>64</sup> ICO, 'Deleting personal data' (ICO, February 2014) accessed 3 October 2021, p. 5.



และการทำให้ข้อมูลกลายเป็นข้อมูลที่บ่งชี้ตัวตนไม่ได้เป็นส่วนหนึ่งของ มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลโดยระบุว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องใช้ความพยายามตามสมควรในการทำลายหรือทำให้ข้อมูลกลายเป็นข้อมูลที่บ่งชี้ตัวตนไม่ได้เมื่อหมดความจำเป็นที่จะต้องครอบครองข้อมูลนั้น สำนักงาน คณะกรรมการความเป็นส่วนบุคคลของข้อมูลส่วนบุคคลได้อธิบายว่าแนวทางในการ “ลบ” ข้อมูลส่วนบุคคลทั้งหมด ความจำเป็นในการประมวลผลแล้วนั้นหมายถึงการทำให้ข้อมูลถูกลบหรือทำลายโดยไม่อาจกลับคืนมาได้

#### 4.3.3.2 ปัญหาการลบทำลายข้อมูลส่วนบุคคลโดยผู้ให้บริการสืบค้นข้อมูลออนไลน์

มาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้” ในขณะที่มาตรา 37(3) บัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล ในกรณีที่ผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์เป็นผู้ควบคุมข้อมูลส่วนบุคคลซึ่งได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคลหรือเป็นกรณี ที่มีหน้าที่จัดให้มีระบบการลบหรือทำลายข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าวย่อมสามารถทำได้ เพียงการลบลิงค์หรือข้อมูลที่ทำให้ผู้ใช้งานอินเทอร์เน็ตเข้าถึงข้อมูลส่วนบุคคลเท่านั้น โดยอาจไม่สามารถลบข้อมูล จากฐานข้อมูลต้นทางที่ถูกเผยแพร่โดยบุคคลอื่น เช่น สำนักพิมพ์

ในคดี Google Spain v AEPD and Mario Costeja González ข้อมูลการขายทรัพย์สินทอดตลาดอัน เป็นข้อมูลส่วนบุคคลของ Mario Costeja González นั้นปรากฏอยู่ในโปรแกรมสืบค้นข้อมูลของ Google ที่เป็นผู้ให้บริการโปรแกรมสืบค้นข้อมูลที่ถูกใช้งานทั่วโลก ซึ่งระบบการสืบค้นของ Google นั้นถูกสร้างขึ้นเพื่อเป็นเครื่องมือเพื่อการเข้าถึงเท่านั้น Google เพียงแต่ทำให้ข้อมูลดังกล่าวที่ถูกประกาศโดยบุคคลอื่นสามารถเข้าถึงได้ อย่างรวดเร็วมากขึ้นเท่านั้นมิได้เป็นผู้เผยแพร่ข้อมูลโดยดั้งเดิม หากผู้เผยแพร่ข้อมูลตัดสินใจที่จะลบข้อมูลดังกล่าว ออกจากเว็บไซต์ของตน ข้อมูลส่วนบุคคลของ Mario Costeja González ก็ย่อมถูกลบออกจากรายการข้อมูลของ Google และไม่สามารถปรากฏบนผลแสดงการค้นหาได้ด้วยเช่นกัน CJEU สั่งให้ Google ดำเนินการลบ “ลิงค์” ในส่วนของ “ชื่อ” เท่านั้น อย่างไรก็ตาม ข้อมูลที่ถูกเผยแพร่ เดิมยังคงถูกเข้าถึงได้โดยการอาศัยคำค้นหาอื่น ๆ หรือการเข้าถึงจากฐานข้อมูลของผู้เผยแพร่โดยตรง โดยมี ข้อสังเกตว่าตัวเจ้าของข้อมูลส่วนบุคคลนั้น ไม่ได้มีหน้าที่ต้องติดต่อกับผู้เผยแพร่ข้อมูลเดิมผ่านระบบสืบค้น จากคำวินิจฉัยดังกล่าวแสดงให้เห็นว่า

สิ่งที่ Google สามารถดำเนินการได้เพื่อ “ลืม” ข้อมูลส่วนบุคคลของ Mario Costeja González นั้น มีเพียงการลบลิงก์เท่านั้นมีอาจลบหรือทำลายข้อมูลส่วนบุคคลที่ถูกเผยแพร่โดยผู้ควบคุม ข้อมูลส่วนบุคคลอื่นได้ ดังนั้น หากตีความกฎหมายว่าผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์เป็นผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบหรือทำลายข้อมูลซึ่งถูกเผยแพร่โดยผู้ควบคุมข้อมูลส่วนบุคคลอื่น เช่น สำนักพิมพ์ แล้วผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์ย่อมไม่สามารถปฏิบัติหน้าที่ตามกฎหมายได้ เนื่องจากเป็นกรณีที่เกิดขึ้น ความสามารถที่ตนจะกระทำได้

#### 4.4 การบัญญัติถึงข้อจำกัดการใช้สิทธิที่จะถูกลืม

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศนั้นแสดงให้เห็นอย่างชัดเจนว่าสิทธิที่จะถูกลืมนั้นมิใช่ เด็ดขาดหากแต่ถูกจำกัดด้วยเงื่อนไขตามที่กฎหมายบัญญัติได้ในหลายประการ ดังนั้น ตัวบทกฎหมายที่จะถูกใช้ เพื่อคุ้มครองสิทธิที่จะถูกลืมย่อมจะต้องบัญญัติถึงข้อจำกัดดังกล่าวด้วย เหตุ ปฏิเสธการใช้สิทธิที่จะถูกลืมตาม มาตรา 33 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นมีแนวทางที่สอดคล้องกับกฎหมายคุ้มครอง ข้อมูลส่วนบุคคลของต่างประเทศ โดยข้อจำกัด ประการสำคัญได้แก่ความจำเป็นในการคุ้มครองเสรีภาพในการ เข้าถึงข้อมูลและการแสดงความคิดเห็นซึ่งปรากฏอย่างชัดเจนในตัวบทกฎหมาย เช่น มาตรา 17 วรรคสามของ GDPR และการ คุ้มครองประโยชน์สาธารณะ เช่น มาตรา 26 ของ HK PDPO 1996<sup>65</sup>

#### 4.5 การนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลที่ถูกแสดงอินเทอร์เน็ต

ในกรณีที่เป็นการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้ โดยผู้ให้บริการสืบค้นข้อมูลนั้น กรณีมีประเด็นต้องพิจารณาต่อไปว่าในกรณีที่ผู้ให้บริการมีสิทธินำ ข้อมูลออกจากการแสดงข้อมูลบนเว็บไซต์ (delisting/deinking) สิทธินี้มิใช่การลบข้อมูลส่วนบุคคล ออกไปโดยสิ้นเชิง ข้อมูลส่วนบุคคลดังกล่าวจะยังคงแสดงหรือปรากฏอยู่บนหน้าเว็บเพจหรือเว็บไซต์ที่ ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลเดิม (original controller)<sup>66</sup> นั้นเป็นการดำเนินการตาม ที่ มาตรา 33 และมาตรา 37(3) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่สิทธิ ในการขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลนั้นมีผลเฉพาะต่อ "ผลลัพธ์" ในส่วนของ "ชื่อ" ที่

<sup>65</sup> ผศ.ดร.ปิติ เอี่ยมจารุญญา (2564) บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten). หน้า 171

<sup>66</sup> ยุคต์กฤต กัณทมนณี (อ้างแล้ว, เชียงรรถที่ 28), หน้า 18

ปรากฏจากการสืบค้นเท่านั้น และไม่ส่งผลให้ต้องมีการลบลิงก์จากดัชนีแสดงผลการค้นหาของระบบสืบค้นทั้งหมด ส่งผลให้ข้อมูลที่ถูกเผยแพร่เดิมยังคงถูกเข้าถึงได้โดยการอาศัยคำค้นหาอื่น ๆ หรือการเข้าถึงจากฐานข้อมูลของผู้เผยแพร่โดยตรงดังนั้น ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นผู้ให้บริการสืบค้นข้อมูลส่วนบุคคลอาจดำเนินการเพียงการนำข้อมูลออกจากผลการค้นหาก็คือได้ว่าเป็นการดำเนินการเพื่อความคุ้มครองความเป็นส่วนตัวส่วนตัวของเจ้าของข้อมูลส่วนบุคคลแล้วโดยไม่ต้องทำการลบหรือทำลายข้อมูลส่วนบุคคลซึ่งอาจเป็นข้อมูลที่ถูกเผยแพร่โดยบุคคลอีกคนหนึ่ง เช่น สำนักพิมพ์ เป็นต้น

## 4.6 ตารางแนวปฏิบัติในการลบทำลายข้อมูลส่วนบุคคลภายใต้ GDPR

### การลบภายใต้ GDPR ผู้ใช้แอปหรือซอฟต์แวร์ที่มีสิทธิ์ในการลบหรือสิทธิ์ที่จะถูกลบ

การลบข้อมูลบนระบบอิเล็กทรอนิกส์	การลบทำลายข้อมูล
Online	Offline
<p><b>1. การเตรียมระบบสนับสนุน</b></p> <p>องค์กรจำเป็นต้องดำเนินการตรวจสอบระบบไอทีปัจจุบันเพื่อดูว่าพวกเขาสามารถจัดการฟังก์ชันได้ หลังจากการตรวจสอบองค์กรสามารถระบุได้ว่าระบบจำเป็นต้องอัปเดตเพื่อให้ทันกับงาน สิ่งสำคัญคือต้องทราบว่า GDPR การปกป้องข้อมูลของบุคคล เนื่องจากข้อมูลที่ไม่ระบุตัวตนไม่สามารถเชื่อมโยงกลับไปได้จึงไม่ถือว่าเป็นข้อมูลส่วนบุคคลอีกต่อไป</p>	<p>การเตรียมข้อมูลเอกสาร รูปถ่าย หรืออื่นๆ ที่ต้องการลบเพื่อนำส่งผู้ควบคุมข้อมูล</p>
<p><b>2. การสร้างโครงสร้างการกำกับดูแล</b></p> <p>องค์กรหรือหน่วยงานต้องมีโครงสร้างการกำกับดูแลข้อมูลเพื่อตอบกลับคำขอลบข้อมูล การกำกับดูแลข้อมูลฟังก์ชันต่างๆ เช่น การทำแผนกระบวนการของข้อมูลข้ามระบบ แผนก และบุคคลที่สาม นอกจากนี้ยังรับประกันคุณภาพของข้อมูล ดูแลปัญหา เช่น รายการที่ซ้ำกันซึ่งสามารถพบได้ในการสำรองข้อมูลและฉบับพิมพ์โดยเฉพาะอย่างยิ่งข้อมูลบางอย่างอาจเรียกร้องให้มีภาระผูกพันเพิ่มเติม</p>	<p>ผู้ควบคุมข้อมูลทำการตอบรับเพื่อทราบและดำเนินการนำไปลบและทำลายข้อมูล</p>
<p><b>3. การวางแผนขั้นตอนและนโยบายต่างๆ</b></p> <p>GDPR ไม่ได้กำหนดให้องค์กรต้องมีนโยบายหรือขั้นตอนในการดำเนินการ อย่างไรก็ตามมีความเป็นไปได้ที่องค์กรจะกำหนดให้พวกเขาปฏิบัติตามเพิ่มเติมที่ นโยบายและขั้นตอนเหล่านี้จะให้ความรู้แก่นักพัฒนาและพนักงานคนอื่นๆ ขององค์กรเกี่ยวกับขั้นตอนที่จำเป็นในวงจรชีวิตการลบข้อมูลการจัดทำเอกสารนโยบายและขั้นตอนเหล่านี้ยังเป็นข้อพิสูจน์ว่าองค์กรปฏิบัติตามข้อผูกพันต่อสิทธิ์ในข้อมูลของแต่ละบุคคล นโยบายและขั้นตอนต้องได้รับการจัดการจากส่วนกลาง เพื่อให้แน่ใจว่ามีความสม่ำเสมอและครอบคลุมในองค์กร</p>	<p>ผู้ควบคุมข้อมูลของแต่ละองค์กรปฏิบัติตามการลบข้อมูลการจัดทำเอกสาร นโยบายและขั้นตอน</p>
<p><b>4. การยืนยันตัวตนเจ้าของข้อมูล</b></p> <p>ก่อนที่ผู้ควบคุมข้อมูลจะสามารถลบข้อมูลของหัวเรื่องได้เมื่อมีการร้องขอพวกเขาจะต้องสามารถยืนยันตัวตนของหัวเรื่องได้ หากผู้ควบคุมข้อมูลมีข้อสงสัยเกี่ยวกับตัวตน สามารถขอข้อมูลเพิ่มเติมเพื่อยืนยันได้ GDPR ไม่ได้ระบุขั้นตอนขององค์กรในการยืนยันตัวตน เช่น หากผู้ควบคุมได้ตรวจสอบตัวตนของหัวเรื่องตามข้อตกลง สามารถยืนยันตัวตนได้ หากผู้ควบคุมข้อมูลต้องการปฏิเสธคำขอลบข้อมูล เนื่องจากข้อกังวลด้านการยืนยันตัวตน จะต้องแจ้งให้บุคคลนั้นทราบ อย่างไรก็ตามในบางกรณีไม่จำเป็นต้องยืนยันตัวตนของเจ้าของข้อมูล นั่นคือกรณีหากข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่ระบุตัวตน ไม่จำเป็นในการประมวลผล</p>	<p>ผู้ควบคุมข้อมูลมีการตรวจสอบเอกสารว่าเป็นข้อสงสัยคำขอลบทำลายจริงหรือไม่</p>
<p><b>5. ค่าใช้จ่ายในการลบ</b></p> <p>ผู้ควบคุมข้อมูลจะสามารถลบข้อมูลของหัวเรื่องได้เมื่อมีการร้องขอพวกเขาจะต้องสามารถยืนยันตัวตนของหัวเรื่องได้ หากผู้ควบคุมข้อมูลมีข้อสงสัยเกี่ยวกับตัวตน สามารถขอข้อมูลเพิ่มเติมเพื่อยืนยันได้ GDPR ไม่ได้ระบุขั้นตอนขององค์กรในการยืนยันตัวตน เช่น หากผู้ควบคุมได้ตรวจสอบตัวตนของหัวเรื่องตามข้อตกลง สามารถยืนยันตัวตนได้ หากผู้ควบคุมข้อมูลต้องการปฏิเสธคำขอลบข้อมูล เนื่องจากข้อกังวลด้านการยืนยันตัวตน จะต้องแจ้งให้บุคคลนั้นทราบ อย่างไรก็ตามในบางกรณีไม่จำเป็นต้องยืนยันตัวตนของเจ้าของข้อมูล นั่นคือกรณีหากข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่ระบุตัวตน ไม่จำเป็นในการประมวลผล</p>	
<p><b>6. ระยะเวลา</b></p> <p>ในฐานะผู้ควบคุมข้อมูลต้องตอบกลับคำขอให้ลบข้อมูลโดยไม่มีค่าใช้จ่ายและไม่เกินหนึ่งเดือนหลังจากได้รับคำขอ ในการตอบกลับควรแจ้งให้เจ้าของข้อมูลทราบถึงมาตรการเพื่อตอบสนองต่อคำขอ หากได้รับคำขอที่ซับซ้อนสามารถตอบกลับโดยบอกเจ้าของข้อมูลว่าคุณต้องการเวลามากขึ้นในการทำงานตามคำขอ ในกรณีนี้กำหนดเวลาสามารถขยายได้ไม่เกินสองเดือนหากคุณปฏิเสธคำขอของเจ้าของข้อมูล จะต้องแจ้งให้ทราบภายในหนึ่งเดือนหลังจากได้รับคำขอ</p>	

#### 4.7 วงกลมความแตกต่างทางด้านมุมมองการลบทำลายข้อมูลของบุคคลทั่วไป ในทางเทคนิคของระบบอิเล็กทรอนิกส์ หรือมุมมองในทางกฎหมาย



การลบข้อมูลส่วนบุคคลทั่วไปแบบออฟไลน์นั้นอาจทำได้โดยการทิ้งลงถังขยะแบบปกติ แต่ในทางกฎหมายนั้นต้องเป็นการทำลายโดยทำให้เข้าเครื่องบดหรือย่อยให้ข้อมูลนั้นสลายหายไป ส่วนการลบข้อมูลแบบออนไลน์บนระบบอิเล็กทรอนิกส์นั้นบุคคลทั่วไป แค่ทำการกดลบไฟล์และลบใน Recycle Bin บุคคลทั่วไปก็จะถือเป็นการลบข้อมูลแล้ว

แต่ในทางกฎหมายของ GDPR นั้นต้องมีขั้นตอนโดยการเตรียมระบบเพื่อให้ลบอัตโนมัติ และการคณะกรรมการกำกับดูแล อีกทั้งยังต้องปฏิบัติตามขั้นตอนต่างๆ โดยมีระบุไว้ 6 ขั้นตอน โดยมีการยืนยันตัวตนของเจ้าของข้อมูลและมีเรื่องระยะเวลาที่ต้องตอบกลับคำขอให้ลบโดยไม่ชักช้าและอย่างช้าที่สุดภายในหนึ่งเดือนเพื่อแจ้งให้บุคคลนั้นทราบ

ส่วนทางเทคนิคของระบบอิเล็กทรอนิกส์ ข้อมูลที่เราลบไปแล้วสามารถกู้คืนข้อมูลที่ลบไปแล้วขึ้นมาใหม่ได้ โดย Malware หรือโปรแกรมอื่นๆ ที่ Cyber hacker ใช้เพื่อล้วงข้อมูลสำคัญ เพื่อประโยชน์บางอย่าง ดังนั้นเพื่อเป็นแนวทางและขั้นตอนที่กำหนดในทางปฏิบัติที่ชัดเจนในเรื่องนี้ ทำให้คณะกรรมการหรือผู้ควบคุมข้อมูล ของกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ประเทศไทยจึงควรมีแนวทางปฏิบัติให้คณะกรรมการทราบเกี่ยวกับขั้นตอนในการลบข้อมูลและรูป

แบบอย่างชัดเจน เพื่อไม่ให้สามารถกู้ข้อมูลที่ถูกลบไปแล้วกลับขึ้นมาได้ในทางกฎหมาย ดังตัวอย่างต่อไป

ตัวอย่างการลบข้อมูล Offline: การลบทำลายข้อมูลของพนักงานทรัพยากรบุคคลในการรับสมัครงานขององค์กรแห่งหนึ่ง ได้ดำเนินการรับสมัครโดยขอข้อมูลของผู้สมัครงานไว้ โดยมีสำเนาบัตรประชาชน สำเนาทะเบียนบ้านและรูปถ่าย หากมีการสัมภาษณ์งานและผู้สมัครไม่ได้รับคัดเลือกหรือไม่ได้ใช้ข้อมูลเมื่อหมดความจำเป็น ทางบริษัทควรมีการเตรียมระบบสนับสนุนหรือนโยบายของบริษัท เพื่อมีโครงสร้างให้มีผู้กำกับดูแล ให้อยู่ในกรอบของเวลา หากพ้นเวลาที่เก็บและหมดความจำเป็นแล้ว พนักงานทรัพยากรส่วนบุคคลหรือ DPO ควรปฏิบัติตามขั้นตอนโดยการส่งข้อมูลไปให้ผู้ควบคุม เพื่อทำลายข้อมูลสำคัญต่างๆของผู้สมัคร โดยการลบหรือทำลายข้อมูลทำให้เอกสารย่อยสลายไป เช่น นำเข้าเครื่องบดย่อย

ตัวอย่างการลบข้อมูลแบบ Online: โรงพยาบาลแห่งหนึ่งมีคนไข้ ที่เข้ามารักษาและเลิกเป็นคนไข้ไปและทางคนไข้ขอให้ทางโรงพยาบาลลบข้อมูลของคนไข้เมื่อเลิกเป็นคนไข้และไม่มีเหตุอื่นที่ต้องเก็บข้อมูลนั้นแล้ว โรงพยาบาลจึงลบโดยการส่ง Recycle Bin ในความเข้าใจของบุคคลทั่วไปก็ถือเป็นการลบข้อมูลส่วนบุคคลแล้ว แต่ในทางเทคนิคของระบบอิเล็กทรอนิกส์ Cyber hacker นั้นข้อมูลดังกล่าวสามารถกู้ข้อมูลของคนไข้ขึ้นมาได้หลากหลายวิธีอาจโดยวิธี Malware ซึ่งตอนนี้กฎหมายมาตรา 33 กับรรรคท้ายที่มีการกำหนดให้คณะกรรมการผู้ควบคุมข้อมูลมาตรา 37 ค่อนข้างกว้างและสามารถปฏิบัติตามได้ยากและ ผู้ควบคุมข้อมูลหรือคณะกรรมการนั้นปฏิบัติไปแล้ว ก็ไม่อาจทราบได้ว่าที่ปฏิบัติไปจะถูกต้องตามกฎหมายหรือไม่ หากคนไข้คนดังกล่าวมีข้อมูลที่มี Value มาก หรือหากคนไข้เป็นคนดังอาจมีผลทางด้านใดด้านหนึ่งทำให้ hacker อยากรู้ข้อมูลนี้มาก ทางโรงพยาบาลนี้ก็เข้าใจว่าลบแล้ว แต่ในทางกฎหมายของ GDPR นั้นอาจยังไม่ถึงขั้นที่ถูกต้องทางกฎหมาย โดยโรงพยาบาลหรือหน่วยงานของรัฐต้องมีผู้ควบคุมข้อมูล เช่น การสร้างระบบทางซอฟต์แวร์ หรือลบข้อมูลได้ตามแนวทางของกฎหมายโดยการเตรียมระบบจัดเก็บของโรงพยาบาลให้เป็นโปรแกรมเฉพาะที่เก็บข้อมูลแล้วทำลายข้อมูลเพื่อไม่ให้สามารถระบุตัวตนได้และมีการทำลายออกไป

ตัวอย่างการลบข้อมูล Online: พนักงานเลขานุการต้องการลบข้อมูลสำคัญของผู้บริหารจากการลบข้อมูลประเภทไฟล์บนระบบโน้ตบุ๊ก วินโดว์ คอมซีพียูตั้งโต๊ะ หรือทางไลน์ก็ตาม พนักงานเลขานุการได้กดลบข้อมูลโดยการคลิกขวา กด Delete ไปยัง Recycle Bin และกดลบจาก Recycle

Bin ในมุมมองของเลขานุการก็อาจจะเพียงพอแล้ว แต่ในทางระบบอิเล็กทรอนิกส์นั้นข้อมูลดังกล่าวสามารถกู้คืนมาได้โดยการโหลดแอปพลิเคชันหรือ ซอฟต์แวร์ หรือโปรแกรม อื่น เช่น Malware จึงทำให้การลบของเลขานุการนั้น อาจเกิดความเสียหายต่อตัวบุคคล หรือบริษัทได้ หรือหากมีการลบไปแล้วอาจไม่เป็นไปตามหลักของกฎหมายเนื่องจากกฎหมายของประเทศไทยยังไม่มีแนวทางในการกำหนดให้ผู้ควบคุมข้อมูลอย่างชัดเจน ดังนั้นองค์กรจึงต้องมีระบบไอทีเข้ามาเป็นผู้ควบคุมและจัดการฟังก์ชันเพื่อลบข้อมูลสำคัญที่ต้องการได้ตามกฎหมาย GDPR กำหนด

จากตารางที่อธิบายแนวทางในการลบตามกฎหมายสหภาพยุโรป GDPR และวงกลมข้างต้น จะสรุปได้ว่า ปัจจุบันถ้อยคำว่า “ลบ” เป็นไปตาม Standard โลกของบุคคลทั่วไป ในความหมายที่ทุกท่านเข้าใจ คือการทำให้อายุหายไป สำหรับบุคคลทั่วไปอาจเข้าใจได้ว่าการลบออกก็ถือว่าเป็นการทำลายแล้ว แต่ยุคสมัยที่เปลี่ยนไปได้มีการพัฒนาระบบต่างๆบนโลกออนไลน์ ทำให้การลบทำลายนั้นทางเทคโนโลยีคอมพิวเตอร์ในปัจจุบัน จะมีโปรแกรมของระบบซอฟต์แวร์ หรือ แอปพลิเคชันต่างๆ ไม่ว่าจะเป็นการค้นหาข้อมูลของ Digital Footprint รอยเท้าบนโลกดิจิทัล เปรียบเสมือนประวัติทางพฤติกรรมที่ผู้ใช้งานกระทำในโลกอินเทอร์เน็ต ทั้งการพิมพ์ข้อความ การคลิกเข้าสู่เว็บไซต์ การกดไลค์เพจ หรือการแชร์ข้อความทางโซเชียลมีเดีย ข้อมูลต่างๆที่สามารถกู้ขึ้นมาใหม่ได้ จากการที่เราลบทำลายไปแล้ว

ในทางกฎหมายของ GDPR จึงมีแนวทางในการปฏิบัติของการลบทำลายข้อมูลส่วนบุคคลโดยมีขั้นตอนในทางปฏิบัติเช่น องค์กรหรือหน่วยงานต่างๆต้องมีการเตรียมระบบสนับสนุนเพื่อรองรับการลบทำลายข้อมูล มีการเขียนโครงสร้างของบริษัทแต่ละแผนก เพื่อให้ครอบคลุมการลบทำลายและเป็นไปตามนโยบายขั้นตอนที่วางไว้ โดยมีการให้ยืนยันตนในการร้องขอในการลบทำลาย โดยอยู่ในกรอบเวลาที่กำหนดไว้ ดังนั้นจากการศึกษาแนวทางปฏิบัติของสหภาพยุโรปทำให้สามารถเป็นแนวทางในทางปฏิบัติให้กับมาตรา 33 และมาตรา 37(3) ของกฎหมายประเทศไทย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้เพื่อให้ผู้ควบคุมข้อมูลนั้นสามารถเข้าใจได้ว่าควรปฏิบัติอย่างไร สิทธิที่จะถูกลืมนั้นมีขอบเขตที่สามารถถูกพัฒนาไปได้ไกลกว่าการลบหรือทำลายข้อมูลส่วนบุคคลโดยรับรู้ว่าการถูกลืมนั้นอาจเกิดขึ้นจากการลบหรือทำลายข้อมูลในเชิงกายภาพหากข้อมูลนั้นเป็นวัตถุที่จับต้องได้ และขณะเดียวกันก็รับรู้ว่าการลบสิ่งทีระบบสืบค้นข้อมูลออนไลน์แสดงผลผ่านอินเทอร์เน็ตก็นับได้กว่าเป็นการคุ้มครองสิทธิที่จะถูกลืมได้เช่นกัน แม้ว่าข้อมูลส่วนบุคคลนั้นอาจจะยังไม่ถูกลบหรือทำลายในฐานะข้อมูลหรือระบบของผู้เผยแพร่ข้อมูลรายอื่น เช่น สำนักพิมพ์หรือหน่วยงานรัฐกล่าวได้ว่าการพัฒนากฎหมายเพื่อคุ้มครองสิทธิที่จะถูกลืมนั้นจะต้องเป็นได้โดยสอดคล้องและพร้อมที่จะตอบสนองต่อสภาพของข้อเท็จจริงในสังคมโดยเฉพาะถึงความก้าวหน้าในการสื่อสารและระบบฐานข้อมูลอิเล็กทรอนิกส์ในโลกยุคดิจิทัล โดยจะเป็นการช่วยสร้างความชัดเจนว่าผู้ให้บริการสืบค้น

ข้อมูลออนไลน์ซึ่งมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายสามารถมีส่วนคุ้มครองสิทธิที่จะ  
ข้อมูลส่วนบุคคลนั้นได้ และในทางกฎหมายได้จัดให้มีความมั่นคงปลอดภัยทางด้านเทคนิคและด้าน  
การบริหารจัดการและให้ค้ำประกันว่าจะลบข้อมูลนั้นทิ้งอย่างถาวร



## บทที่ 5

### บทสรุปและข้อเสนอแนะ

จากการศึกษาถึงแนวทางในการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ปฏิบัติของกฎหมายการลบทำลายข้อมูลส่วนบุคคลของมาตรา 17 General Data Protection Regulation : GDPR Right to erasure ('right to be forgotten') กล่าวคือการลบทำลายหรือทำให้ข้อมูลส่วนบุคคล กลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้ การบัญญัติกฎหมายในลักษณะดังกล่าวแตกต่างไปจากถ้อยคำที่ปรากฏ ของ GDPR ที่มีคำว่า "Right to be Forgotten" ควบคู่ไปกับ "Right to Erasure" สิทธิของเจ้าของข้อมูลส่วนบุคคลตาม มาตรา 33 ประกอบมาตรา 37(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ของประเทศไทย ทำให้คณะกรรมการคุ้มครองข้อมูลหรือผู้ควบคุมข้อมูลยังไม่สามารถปฏิบัติตามในทางกฎหมายได้หรือค่อนข้างยากต่อการปฏิบัติ รูปแบบของการลบทำลายข้อมูลส่วนบุคคลควรมีการจัดทำเป็นแพลตฟอร์ม ที่เป็นมาตรฐานในการลบข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์

#### 5.1 บทสรุป

จากการศึกษากฎหมายของสหภาพยุโรปทำให้เห็นว่า มาตรา 17 General Data Protection Regulation : GDPR Right to erasure ('right to be forgotten') มีการกำหนดขั้นตอนและแนวทางในการลบทำลายหรือทำให้ข้อมูลระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ที่จะสามารถให้คณะกรรมการและผู้ควบคุมข้อมูลสามารถปฏิบัติตามขั้นตอน ดังตาราง 4.6 ตารางแนวปฏิบัติในการลบทำลายข้อมูลส่วนบุคคลภายใต้ GDPR และหากคณะกรรมการและผู้ควบคุมข้อมูลส่วนบุคคล นิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับรักษาความปลอดภัยลบหรือทำลายข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล หากปฏิบัติตามแล้วจะสามารถมั่นใจได้ว่าปฏิบัติจะไม่ผิดกฎหมายตามมาตรา 33 มาตรา 37 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างไรก็ตามการศึกษาแนวปฏิบัติของ GDPR ซึ่งกำหนดรายละเอียดการลบทำลายข้อมูลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลที่มีหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถปฏิบัติตามได้ทางกฎหมาย โดยแต่ละหน่วยงานหรือองค์กรต้องเตรียมระบบสนับสนุนระบบแอปพลิเคชันและฐานข้อมูลที่จัดเก็บและประมวลผลข้อมูลเพื่อให้ข้อมูลสามารถลบออกไปอย่างง่ายดาย โดยมีการดำเนินการโดยระบบไอทีที่มีฟังก์ชันที่เตรียมพร้อมไว้

ก่อนหน้า และองค์กรต้องมีโครงสร้างการกำกับดูแลเป็นกระบวนการเพื่อตอบกลับคำขอข้อมูลเพื่อให้แน่ใจว่าองค์กรครอบคลุมพื้นที่ทั้งหมดในระหว่างการลบ โดยปฏิบัติตามขั้นตอนที่ได้มีการวางแผนไว้ตามนโยบายของแต่ละองค์กร เพื่อให้เป็นที่เข้าใจตรงกันแก่พนักงานทุกคน เกี่ยวกับขั้นตอนการจัดเก็บหรือลบ เป็นต้น โดยเฉพาะอย่างยิ่งเพื่อให้มั่นใจในการลบทำลายข้อมูลของผู้ควบคุมข้อมูล ควรมีการยืนยันตัวตนเจ้าของข้อมูลและดำเนินการกรอบข้อมูลของเวลาที่กำหนด ในฐานะผู้ควบคุมข้อมูลต้องตอบกลับคำขอให้ลบข้อมูลโดยไม่ชักช้าและไม่เกินหนึ่งเดือนหลังจากได้รับคำขอ

## 5.2 ข้อเสนอแนะ

จากมาตรา 33 และมาตรา 37(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กฎหมายวรรคท้ายได้กล่าวว่า “อาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคล เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้” นั้น ยังไม่มีแนวทางปฏิบัติทำให้เจ้าของข้อมูลและผู้ควบคุมข้อมูลยังไม่มีขั้นตอนที่สามารถปฏิบัติตามได้ และยังไม่อาจทราบได้ว่าถูกกฎหมายหรือไม่

เอกกตศึกษาจึงขอเสนอให้มีการออกกฎหมายลำดับรอง จากมาตรา 33 และมาตรา 37(3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพิ่มบัญญัติรายละเอียดเกี่ยวกับการนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูล เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์สามารถปฏิบัติตามกฎหมายได้โดยเพิ่มโครงสร้าง จากแนวทางปฏิบัติของกฎหมาย มาตรา 17 General Data Protection Regulation : GDPR Right to erasure (‘right to be forgotten’) ขั้นตอนและแนวทางในการลบทำลายหรือทำให้ข้อมูลระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ที่จะสามารถให้คณะกรรมการและผู้ควบคุมข้อมูลสามารถปฏิบัติตามขั้นตอนของกฎหมายสหภาพยุโรปดังนี้ (1) การเตรียมระบบสนับสนุนการลบข้อมูล (2) การสร้างโครงสร้างการกำกับดูแล (3) การวางนโยบายและขั้นตอนต่างๆ (4) การยืนยันตัวตนของเจ้าของข้อมูล (5) การกำหนดค่าใช้จ่าย และ (6) เรื่องของกรอบเวลาของการลบข้อมูล โดยให้กฎหมายลูกมีการกำหนดโครงสร้างต่างๆขึ้นมาแล้วในทางปฏิบัติ และกำหนดถึงหลักเกณฑ์และรายละเอียดในทางกฎหมายเกี่ยวกับการ “ลบทำลาย” หรือ “ทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้” อีกด้วย

หากมีการออกกฎหมายลำดับรองเพื่อให้คณะกรรมการและผู้ควบคุมข้อมูลทราบโครงสร้างการลบทำลายข้อมูลส่วนบุคคลบนระบบอิเล็กทรอนิกส์ในทางปฏิบัติที่กำหนดไว้ในทางกฎหมายแล้ว

จะช่วยสร้างความชัดเจนให้กับคณะกรรมการและผู้ควบคุมข้อมูลให้ผู้บริการสืบค้นข้อมูลออนไลน์ซึ่งมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมาย สามารถมีส่วนคุ้มครองสิทธิที่จะถูกลืมของเจ้าของข้อมูลส่วนบุคคลได้ โดยการนำเอาผลการแสดงการค้นหาออกจากระบบการสืบค้น โดยไม่จำเป็นต้องมีการลบข้อมูลในฐานะข้อมูลซึ่งถูกเผยแพร่โดยบุคคลอื่น และเมื่อผู้ให้บริการสืบค้นข้อมูลได้ดำเนินการนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลแล้วก็ย่อมถือได้ว่าปฏิบัติหน้าที่ตามกฎหมายแล้วโดยไม่ต้องกังวลว่าจะผิดกฎหมาย ทั้งนี้เพื่อรองรับข้อเท็จจริงที่ว่า การสื่อสารแลกเปลี่ยนความคิดของคนในสังคมนั้นเกิดขึ้นในโลกดิจิทัลมากขึ้น โดยมีแนวทางการเพิ่มกฎหมายลำดับรองจากขั้นตอนในทางปฏิบัติของการลบทำลายข้อมูลส่วนบุคคลตาม มาตรา 17 ของ GDPR ให้ครอบคลุมมากยิ่งขึ้น

## บรรณานุกรม

### ตัวบทกฎหมาย

กฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป General Data Protection Regulation (GDPR)  
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

### หนังสือ

นคร เสรีรักษ์, ณรงค์ ใจหาญ, ประสิทธิ์ ปิวาวัฒนพานิช, ศุภเกียรติ ศุภศักดิ์ศึกษากร, และนิชานันท์  
นันทศิริศรีธรรม. General Data Protection Regulation ฉบับภาษาไทย. พิมพ์ครั้งที่ 1  
กรุงเทพฯ: บริษัท พี.เพรส จำกัด, 2562

ปิติ เอี่ยมจำรูญลาภ, ดนพร จิตต์จรุงเกียรติ, ภัทริน จิตต์จรุงเกียรติ, ประสงค์ดี ชาวชาติ, ดุขตี ดุขฎี  
พาณิชย์ และ จุฑาทกมล เตติ. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับ  
ผู้ประกอบการ. พิมพ์ครั้งที่ 2. กรุงเทพฯ: บริษัท แดเน็กซ์ อินเทอร์เน็ตเซอร์วิส จำกัด, 2565.

ปิยะบุตร บุญอรามเรือง, พัฒนพร โกวพัฒน์กิจ, พีรพัฒน์ โชคสุวัฒน์สกุล, เสกสิริ นวัตกรรมวงศ, ปติ  
เอี่ยมจำรูญลาภ, ชวิน อุณภัก, ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, ภูมิศิริ ดำรงวุฒิ และโมกขพิศุทธิ์  
รตราวุฒ. Thailand Data Protection Guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครอง  
ข้อมูลส่วนบุคคล. พิมพ์ครั้งที่ 1 กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2563

### บทความ

ดร.สรานนท์ อินทนนท์. ใน เข้มพร วิรุณราชพันธ์, ลักษณ์ี คงลาภ. การรักษาความปลอดภัยบนโลกไซเบอร์  
(Cybersecurity) หน้า 11. บริษัท วอล์ค ออน คลาวด์ จำกัด . 2563

ปิติ เอี่ยมจำรูญลาภ. บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) และ  
แนวทางแก้ไขกฎหมายที่เกี่ยวข้อง. โครงการวิจัยสำนักส่งเสริมวิชาการรัฐสภา สถาบัน  
พระปกเกล้า. 2564

พล.อ.ท.ณรงค์ เหล่าธีระเชาวน์. “สิทธิมนุษยชน (2556)”. สำนักงานศาลรัฐธรรมนูญ.สืบค้นเมื่อ 9  
พฤศจิกายน พ.ศ. 2565,

อรรถกร สุขพัฒน์พันธ์, “สิทธิที่จะถูกลืม (Right to be forgotten) จากคำวินิจฉัยผู้วินิจฉัยใหม่ภายใต้  
กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพ ยุโรป” (Krisdika). สืบค้นเมื่อ 6 ตุลาคม พ.ศ.  
2564, หน้า 4.

Nadia Yeo, “Does Singapore Have a “Right to be Forgotten” in David N Alfred, Justin Blaze George, and Adeline Chung (eds), Personal Data Protection Digest (Personal Data Protection Commission 2019), p. 108.

### งานวิจัย

นคร เสรีรักษ์ ณรงค์ใจหาญ, ประสิทธิ์ ปิวาวัฒนพานิช. ศุภเกียรติ ศุภศักดิ์ศึกษากร และนิชานันท์ นันทศิริศรี, GDPR ฉบับภาษาไทย (บริษัท พี.เพรส จำกัด, ธันวาคม 2562), หน้า 130.

ปิติ เอี่ยมจำรูญลาภ. บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) และแนวทางแก้ไขกฎหมายที่เกี่ยวข้อง. โครงการวิจัยสำนักส่งเสริมวิชาการรัฐสภา สถาบันพระปกเกล้า. 2564.

ยุกต์กฤต กัณทมนั, สุทธิปริทัศน์. “การคุ้มครองสิทธิที่จะถูกลืม” (2019). มหาบัณฑิตจุฬาลงกรณ์มหาวิทยาลัย, 2561.

ICO, ‘Deleting personal data’ (ICO, February 2014) accessed 3 October 2021, p. 5.

### แหล่งข้อมูลอิเล็กทรอนิกส์

กรุงเทพธุรกิจ. หน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม. [ออนไลน์]. แหล่งที่มา : <https://www.bangkokbiznews.com/columnist/973755> [เข้าถึงเมื่อ 29 ตุลาคม 2565]

การลบข้อมูลเป็นบริการ (EaaS). ตลาดดิจิทัล [ออนไลน์]. แหล่งที่มา: <https://digitalmarketplace.service.gov.uk> [เข้าถึงเมื่อ 27 พฤศจิกายน 2565]

คณะกรรมการ สิทธิมนุษยชนแห่งชาติ [ออนไลน์]. แหล่งที่มา : <https://sites.google.com/site/krukarn17825/hlak-siththi-mnusy-chn>[เข้าถึงเมื่อ 27 พฤศจิกายน 2565]

จริยธรรมสำหรับคอมพิวเตอร์ธุรกิจ [ออนไลน์]. แหล่งที่มา : [http://katethanpitcha.blogspot.com/2013/08/blog-post\\_9949.html](http://katethanpitcha.blogspot.com/2013/08/blog-post_9949.html)[เข้าถึงเมื่อ 27 กุมภาพันธ์ 2565]

- ปิติ เอี่ยมจำรูญลาภ. กลุ่มย่อยที่ 1 ประชาธิปไตยและความท้าทายของเทคโนโลยีสมัยใหม่ [ออนไลน์]. การประชุมวิชาการสถาบันพระปกเกล้า ครั้งที่ 24. แหล่งที่มา: <https://web.facebook.com/kpi.ac.th/videos/559497936180043> [22 พฤศจิกายน 2565]
- สุพิศตรา แผนวิจิต. กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA). [ออนไลน์]. แหล่งที่มา: [https://pr.moph.go.th/\\_WEBADMIN/uploads/attfiles/6tkphu5ano8ws4gwkg.pdf](https://pr.moph.go.th/_WEBADMIN/uploads/attfiles/6tkphu5ano8ws4gwkg.pdf) [เข้าถึงเมื่อ 27 ธันวาคม 2565]
- วารสารสหวิทยาการสังคมศาสตร์และการสื่อสาร. สิทธิในการถูกลืมบนระบบอินเทอร์เน็ต Right to Be Forgotten on the Internet [ออนไลน์]. แหล่งที่มา : <https://so02.tci-thaijo.org/index.php/ISSC/article/view/254961> [เข้าถึงเมื่อ 20 ตุลาคม 2565]
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. การคุ้มครองข้อมูลส่วนบุคคล. [ออนไลน์]. แหล่งที่มา : <https://www.etrda.or.th/th/PrivacyCenter/Privacy-Protection.aspx> [เข้าถึงเมื่อ 12 ธันวาคม 2565]
- สิทธิของเจ้าของข้อมูล (Data Subject) ตาม PDPA มีอะไรบ้าง และผู้ประกอบการควรเตรียมพร้อมอย่างไร Apps [ออนไลน์]. แหล่งที่มา : <https://pdpa.pro/blogs/rights-of-data-subject-pdpa> [เข้าถึงเมื่อ 20 มิถุนายน 2565]
- หนังสือพิมพ์ไทยโพสต์. สิทธิที่จะถูกลืมจากโลกดิจิทัล. [ออนไลน์]. แหล่งที่มา: [https://www.parliament.go.th/ewtadmin/ewt/parliament\\_parcy/ewt\\_news.php?nid=48921&filename=index](https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_news.php?nid=48921&filename=index) [เข้าถึงเมื่อ 2 สิงหาคม 2565]
- อรรถกร สุขปูนพันธ์, “สิทธิที่จะถูกลืม (Right to be forgotten): จากคำวินิจฉัยยุติใหม่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล [ออนไลน์]. แหล่งที่มา : [https://www.parliament.go.th/ewtadmin/ewt/parliament\\_parcy/ewt\\_news.php?nid=48921&filename=index](https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_news.php?nid=48921&filename=index) [เข้าถึงเมื่อ 27 เมษายน 2565]
- Authgear. The Right to Erasure and How You Can Follow It for Your Apps [Online]. Available from: <https://www.authgear.com/post/the-right-to-erasure-and-how-you-can-follow-it-for-your-apps#erasure-process> [26 December 2022]

Edpb. [Online]. Available from: [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021examples-regarding-data-breach\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021examples-regarding-data-breach_en) [19 November 2022]

Krapalm. Data Erasure. [Online]. Available from: <https://9krapalm.com/data-erasure> [28 November 2022]

Guidelines 01/2021 on Examples regarding Data Breach Notification [Online]. Available from: [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en) [22 November 2022]

### ประวัติผู้เขียน

ชื่อ-สกุล	นางสาวชยาภรณ์ มั่นสกุล
วัน เดือน ปี เกิด	3 มีนาคม พ.ศ.2537
สถานที่เกิด	หัวหิน, จังหวัดประจวบคีรีขันธ์
วุฒิการศึกษา	ประถมศึกษาโรงเรียนเซนต์โยเซฟเพชรบุรี มัธยมศึกษาโรงเรียนพรหมานุสรณ์จังหวัดเพชรบุรี ปริญญาตรี บริหารธุรกิจบัณฑิต มหาวิทยาลัยเกษตรศาสตร์