บทบัญญัติทางกฎหมาย ว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) และแนวทางแก้ไขกฎหมาย

ดร.ปิติ เอี่ยมจำรูญลาภ

บทบัญญัติทางกฎหมาย ว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) และแนวทางแก้ไขกฎหมาย

ดร.ปิติ เอี่ยมจำรูญลาภ

เรื่อง บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) และแนวทางแก้ไขกฎหมายที่เกี่ยวข้อง

ผู้เขียน ดร.ปิติ เอี่ยมจำรูญลาภ

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

ปิติ เอี่ยมจำรูญลาภ.

บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) และแนวทางแก้ไขกฎหมายที่เกี่ยวข้อง. -- กรุงเทพฯ : สถาบันพระปกเกล้า, 2565.
268 หน้า.

1. สิทธิที่จะถูกลืม. I. ชื่อเรื่อง.

323
ISBN 978-616-476-288-6

รหัสสิ่งพิมพ์	สสว.65-57-200.0
ประสานงาน	นางกันธรัตน์ ลาเทศ
พิมพ์ครั้งที่ 1	กันยายน 2565
จำนวนหน้า	268 หน้า
พิมพ์ที่	บริษัท กู๊ดเฮด พริ้นท์ติ้ง แอนด์ แพคเกจจิ้ง กรุ๊ป จำกัด 6/1 ซอยเสรีไทย 58 แขวงมีนบุรี เขตมีนบุรี กรุงเทพมหานคร 10510 โทรศัพท์ 0-2136-7042 โทรสาร 0-2136-7043
จัดทำโดย	สถาบันพระปกเกล้า ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษาฯ อาคารรัฐประศาสนภักดี ชั้น 5 (โซนทิศใต้) เลขที่ 120 หมู่ 3 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210 โทรศัพท์ 0-2141-9550 โทรสาร 0-2143-8174 http://www.kpi.ac.th

คำนำสถาบันพระปกเกล้า

แนวคิดเรื่องสิทธิที่จะถูกลืม (Right to be Forgotten) ซึ่งเป็นสิทธิของบุคคลที่จะร้องขอให้ผู้มีข้อมูลส่วนบุคคลของบุคคลนั้นไว้ในความครอบครองดำเนินการลบข้อมูลส่วนบุคคลดังกล่าวออก เนื่องจากไม่ยินยอมให้มีการใช้ข้อมูลส่วนบุคคลนั้นอีกต่อไปนั้น ได้รับการพัฒนาขึ้นในทวีปยุโรป ตั้งแต่เริ่มมีการพัฒนาเทคโนโลยีสารสนเทศที่ก่อให้เกิดการจัดเก็บและประมวลผลข้อมูลในรูปแบบอิเล็กทรอนิกส์โดยสามารถสืบค้นข้อมูลดังกล่าวผ่านระบบอินเทอร์เน็ตได้ ซึ่งบางกรณีอาจก่อให้เกิดผลเสียต่อเจ้าของข้อมูลส่วนบุคคลนั้น ทั้งนี้ สิทธิที่จะถูกลืมดังกล่าวได้รับการรับรองอย่างชัดเจนในทวีปยุโรป ผ่านคำวินิจฉัยของศาลและกฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล แม้ว่าประเทศไทยจะมีการบัญญัติประเด็นที่คล้ายคลึงกันไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่ก็ไม่ได้บัญญัติถึงเรื่องสิทธิที่จะถูกลืมนี้อย่างชัดแจ้ง

สถาบันพระปกเกล้า จึงจัดให้มีการศึกษาเรื่อง “บทบัญญัติว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) และแนวทางแก้ไขกฎหมายที่เกี่ยวข้อง” ภายใต้โครงการศึกษาวิเคราะห์กฎหมายที่มีผลใช้บังคับอยู่ ซึ่งศึกษาวิจัยโดย ดร.ปิติ เอี่ยมจำรูญลาภ อาจารย์ประจำคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย โดยมุ่งศึกษาแนวคิดเกี่ยวกับสิทธิที่จะถูกลืม ผ่านคำวินิจฉัยของศาลต่างประเทศและบทบัญญัติแห่งกฎหมายของต่างประเทศ เพื่อถอดบทเรียนและให้ข้อเสนอแนะสำหรับพัฒนาและปรับปรุงกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเด็นของสิทธิที่จะถูกลืมในประเทศไทย สถาบันพระปกเกล้าหวังเป็นอย่างยิ่งว่ารายงานการศึกษาวิจัยฉบับนี้ จะเป็นข้อมูลสำคัญสำหรับฝ่ายนิติบัญญัติในการนำไปประกอบการพิจารณาเพื่อปรับปรุงกฎหมายที่เกี่ยวข้องต่อไป

ศาตราจารย์วุฒิสาร ตันไชย
เลขาธิการสถาบันพระปกเกล้า

บทสรุปผู้บริหาร

สิทธิที่จะถูกลืม (Right to be Forgotten) หมายถึง สิทธิของเจ้าของข้อมูลส่วนบุคคลที่ข้อมูลส่วนบุคคลของตนจะถูกลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนได้เมื่อหมดความจำเป็นที่ข้อมูลนั้นจะต้องถูกประมวลผลหรือเข้าถึงได้อีกต่อไป ไม่ว่าจะโดยการที่เจ้าของข้อมูลส่วนบุคคลร้องขอหรือผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการโดยปราศจากการร้องขอของเจ้าของข้อมูลส่วนบุคคล

สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 33 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกอบกับหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 37 (3) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นมีคุณสมบัติที่จะเรียกได้ว่า “สิทธิที่จะถูกลืม” สอดคล้องกับหลักการทางทฤษฎีสากลเกี่ยวกับสิทธิที่จะถูกลืม ตัวบทกฎหมายคุ้มครองข้อมูลส่วนบุคคล บรรทัดฐานการใช้บังคับและแนวปฏิบัติที่เกี่ยวข้องในต่างประเทศ ได้แก่ สหภาพยุโรป สหราชอาณาจักร ประเทศออสเตรเลีย ประเทศญี่ปุ่น เขตปกครองพิเศษไต้หวัน เขตปกครองพิเศษฮ่องกง ประเทศฟิลิปปินส์ และประเทศสิงคโปร์ แม้ว่าพระราชบัญญัติคุ้มครอง

ข้อมูลส่วนบุคคล พ.ศ. 2562 จะไม่ได้บัญญัติถึงสิทธิที่จะถูกลืมเอาไว้โดยชัดแจ้งในตัวบทกฎหมาย

อย่างไรก็ตาม จากการศึกษาและวิเคราะห์กฎหมายในเชิงเปรียบเทียบงานวิจัยนี้ พบว่า การไม่บัญญัติถึงสิทธิที่จะถูกลืมและรายละเอียดเกี่ยวกับการนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลโดยไม่จำเป็นต้องลบหรือทำลายข้อมูลส่วนบุคคลนั้น อาจส่งผลให้ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นผู้ให้บริการสืบค้นข้อมูลออนไลน์ไม่อาจปฏิบัติหน้าที่เพื่อคุ้มครองสิทธิที่จะถูกลืมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้

เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นบุคคลธรรมดา สามารถอาศัยสิทธิตามมาตรา 33 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งหมายรวมถึงทั้งผู้ทำการเก็บรวบรวมและเผยแพร่ข้อมูลส่วนบุคคล (เช่น สำนักพิมพ์) และผู้ให้บริการสืบค้นข้อมูลออนไลน์ (เช่น Google) ทำการ “ลบ” “ทำลาย” หรือ “ทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้” อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นผู้ให้บริการสืบค้นข้อมูลส่วนบุคคล เช่น Google อาจดำเนินการได้เพียงนำข้อมูลส่วนบุคคลของผู้ร้องออกจากผลการค้นหา ซึ่งก็ถือได้ว่าเป็นการดำเนินการเพื่อความคุ้มครองความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลแล้ว โดยไม่ต้องทำการลบหรือทำลายข้อมูลส่วนบุคคล ซึ่งอาจเป็นข้อมูลที่ถูกเผยแพร่โดยผู้ควบคุมข้อมูลส่วนบุคคลอีกรายหนึ่ง เช่น สำนักพิมพ์ เป็นต้น

งานวิจัยนี้ พบข้อจำกัดในการคุ้มครองสิทธิที่จะถูกลืมอันเนื่องมาจากความแตกต่างของกฎหมายเกี่ยวกับการคุ้มครองสิทธิที่จะถูกลืมนั้นไม่ได้เป็นอันหนึ่งอันเดียวกันในทุกประเทศ ด้วยเหตุนี้ การคุ้มครองสิทธิในความเป็นส่วนตัวในมิติของการร้องขอให้นำข้อมูลออกจากระบบซึ่งถูกคุ้มครองในประเทศหนึ่งนั้น อาจไม่ได้มีการคุ้มครองในอีกประเทศหนึ่ง

กรณีความเป็นไปได้ที่ผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์จะให้บริการสืบค้นและแสดงผลการค้นหาแก่ผู้ใช้งานซึ่งอยู่ในประเทศไทย แต่ผู้ให้บริการดังกล่าวอาจมีสถานที่ประกอบตั้งอยู่ในต่างประเทศ และอาจเป็นไปได้ที่กฎหมายในประเทศที่ผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์นั้นไม่ได้รับรองและคุ้มครองสิทธิที่จะถูกลืมในระดับที่เท่าเทียมกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

ดังนั้น เพื่อให้เกิดความชัดเจนเกี่ยวกับการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งในกรณีของผู้ให้บริการสืบค้นข้อมูลออนไลน์ และเพื่อรองรับข้อเท็จจริงที่ว่าการสื่อสารแลกเปลี่ยนความคิดของคนในสังคมนั้นเกิดขึ้นในโลกดิจิทัลมากขึ้น **งานวิจัยนี้จึงเสนอให้เพิ่มเติมคำว่า “สิทธิที่จะถูกลืม” ในมาตรา 33 และมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562** การแก้ไขกฎหมายตามข้อเสนอดังกล่าวจะช่วยให้เกิดความชัดเจนว่าหากผู้ให้บริการสืบค้นข้อมูลได้ดำเนินการนำเอาข้อมูลส่วนบุคคลออกจากการแสดงผลการค้นหาแล้วก็ย่อมถือได้ว่าปฏิบัติหน้าที่ตามกฎหมายแล้ว โดยไม่ต้องดำเนินการเพื่อลบหรือทำลายข้อมูล และเมื่อผู้ให้บริการสืบค้นข้อมูลได้ดำเนินการนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลแล้ว ก็ย่อมถือได้ว่าปฏิบัติหน้าที่ตามกฎหมายแล้วโดยไม่ต้องกังวลว่าจะมีความรับผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากการฝ่าฝืนกฎหมาย

นอกจากนี้ งานวิจัยนี้ยังเสนอให้**คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้ตามมาตรา 33 วรรคท้ายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การออกกฎหมายลำดับรอง (หรือแนวปฏิบัติ)** ดังกล่าวอาจดำเนินการโดยอาศัยแนวปฏิบัติของต่างประเทศ

โดยครอบคลุมประเด็นต่าง ๆ ได้แก่

(1) กำหนด “ลักษณะ” ของการดำเนินการที่ถือได้ว่าเป็นการ “ลบ” หรือ “ทำลาย” ข้อมูลส่วนบุคคล โดยคำนึงถึงหลักเกณฑ์ เช่น การทำให้ข้อมูลส่วนบุคคลที่หมดความจำเป็นในการประมวลผลแล้วนั้น หมายถึงการทำให้ข้อมูลถูกลบหรือทำลายโดยไม่อาจกลับคืนมาได้อีก

(2) รับรองแนวทางอื่นเพื่อการจัดการกับการลบข้อมูลในรูปแบบอื่น เช่น การทำให้ข้อมูลอยู่เหนือการใช้งานโดยมิได้มีการลบข้อมูล

(3) กำหนดหลักเกณฑ์และวิธีการในการทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้และขั้นตอนในการทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้

(4) กำหนดหลักเกณฑ์และวิธีการนำข้อมูลส่วนบุคคลออกจากการแสดงผล ระบุว่ากิจกรรมการประมวลผลข้อมูลของโปรแกรมสืบค้นข้อมูล โดยกำหนดให้มีความแตกต่างไปจากการลบข้อมูลโดยผู้ตีพิมพ์ข้อมูลดั้งเดิม

Executive Summary

Right to be forgotten can be referred to as the data subject's right to have his or her personal data erased, destroyed or anonymized when the data is no longer required for processing or required to be accessible. These activities can be carried out as a response to a request made by the data subject, or automatically carried out by the data controller, regardless of the data subject's request.

Without explicitly referring to the term "right to be forgotten", the data subject's right under Section 33 of the Personal Data Protection Act B.E. 2561 (2019), and the data controller's duty under Section 37 (3) of the Personal Data Protection Act B.E. 2561 (2019), these two provisions are both capable of protecting right to be forgotten in accordance with universal theories on right to be forgotten, legal provisions, precedents, and guidelines in several foreign countries.

These countries include the European Union, Australia, Japan, Hong Kong, Taiwan, the Philippines and Singapore.

However, based on a comparative method of legal research, this research finds that an absence of the term "right to be forgotten" and details on personal data delisting, without erasing or destroying personal data, can cause compliance challenges to the data controller who provides search engine services.

A data subject may exercise his or her right as guaranteed by Section 33 of the Personal Data Protection Act B.E. 2561 (2019) to request a data controller, including an original publisher (for example the press) and a search engine provider (for example Google) to "erase" "destroy" or "anonymize". However, a search engine provider such as Google may only delist the search results which can be deemed as an action that helps protect the privacy of a data controller without directly erasing or destroying personal data published by another personal data controller such as the press.

This research finds that challenges of protecting right to be forgotten may stem from the fact that personal data protection may differ among countries. A right to request for delisting personal data as guaranteed in one country may not exist in another country. It is possible that a search engine provider providing services and displaying search results to users residing in Thailand may have its business operation in a foreign country.

That foreign country may neither recognize nor guarantee a right to be forgotten at the same level as that of Thailand.

To facilitate clarity on how the data controller can fully comply with the Personal Data Protection Act B.E. 2561 (2019), especially when it comes to a data controller who provides search engine service, as well as to recognize the fact that communication between people is increasingly done through digital platforms, this research proposes that Section 33 and Section 37 (3) of the Personal Data Protection Act B.E. 2561 (2019) should be amended to explicitly recognize the term “right to be forgotten”. This amendment will help making it clear that if a search engine provider already delisted the displayed personal data, its action shall be deemed to be fully compliant with the law without erasing or destroying the said personal data. Once deemed legally-sound, a search engine provider can avoid a risk associated with noncompliance with the Personal Data Protection Act B.E. 2561 (2019).

In addition, this research recommends that the Personal Data Protection Commission should announce criteria for erasing, destroying, or anonymizing personal data by exercising its power under Section 33 paragraph 5 of the Personal Data Protection Act B.E. 2561 (2019). This subordinate law (or guidelines) can be developed by taking into account erasure, destruction, and anonymization guidelines in foreign countries, and should cover the following issues :

(1) Prescription of “nature” of personal “erasure” or “destroying”, for example making the personal data that is no longer necessary for processing “irrecoverable”;

(2) Recognition of other erasing or destruction methods for example putting personal data beyond use without erasing such personal data;

(3) Prescription of criteria and methods for anonymizing personal data as well as anonymization processes; and

(4) Prescription of criteria and methods for delisting the displayed personal data from search engine programs and differentiating this process from data erasing activities to be carried out by an original publisher.

สารบัญ

หน้า

คำศัพท์และอักษรย่อ

ตัวย่อ	ความหมาย
AEPD	Agencia Española de Protección de Datos (หน่วยงานของรัฐที่มีหน้าที่รับผิดชอบเกี่ยวกับการบังคับใช้กฎหมายคุ้มครองข้อมูลของประเทศสเปน)
APP	Australian Privacy Principles (หลักการความเป็นส่วนตัวออสเตรเลีย)
AUS PA 1988	Privacy Act 1988 (กฎหมายคุ้มครองความเป็นส่วนตัวของประเทศออสเตรเลีย)
CJEU	Court of Justice of European Union (ศาลยุติธรรมสหภาพยุโรป)
ECHR	European Convention on Human Rights (อนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน)
EDPB	European Data Protection Board (คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยุโรป)
GDPR	General Data Protection Regulation (กฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป)
Guideline 5/2019	Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (แนวปฏิบัติ 5/2013 ว่าด้วยหลักเกณฑ์เกี่ยวกับสิทธิที่จะถูกลืมในกรณีของการให้บริการสืบค้นออนไลน์ภายใต้กฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป)

ตัวย่อ	ความหมาย
HK PCPD	Office of the Privacy Commissioner for Personal Data of Hong Kong (คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของเขตปกครองพิเศษฮ่องกง)
HK PDPO 1996	Hong Kong Personal Data (Privacy) Ordinance (กฎหมายคุ้มครองข้อมูลส่วนบุคคลของเขตปกครองพิเศษฮ่องกง)
ICO	Information Commissioner's Office (สำนักงานคณะกรรมการข้อมูลข่าวสารของสหราชอาณาจักร)
JP APPI 2020	Act on Protection of Personal Information of Japan (กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น)
OAIC	Australian Government Office of the Australian Information Commissioner (คณะกรรมการที่มีอำนาจหน้าที่ในการกำกับดูแลเรื่องความเป็นส่วนบุคคลภายในประเทศออสเตรเลีย)
PH IRR	Implementing Rules and Regulations of the Data Privacy Act of 2012 (กฎและข้อบังคับเพื่อบังคับการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศฟิลิปปินส์)
PH PDA 2012	Data Protection 2012 (กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศฟิลิปปินส์)
SG PDPA 2012	Personal Data Protection Act 2012 (กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์)
SG PDPC	(Personal Data Protection Commission (Singapore) (คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์)
TW PDPA 2015	Personal Data Protection Act 2015 (กฎหมายคุ้มครองข้อมูลส่วนบุคคลของเขตปกครองพิเศษไต้หวัน)
UDHR	Universal Declaration of Human Rights (ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน)
UK DPA 2018	Data Protection Act 2018 (กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร)

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

สิทธิที่จะถูกลืม (Right to be Forgotten) เป็นสิทธิของบุคคลที่จะร้องขอให้ผู้มีข้อมูลส่วนบุคคลของเขาไว้ในความครอบครองทำการลบข้อมูลส่วนบุคคลออก เนื่องจากไม่ยินยอมให้มีการใช้ข้อมูลนั้นอีกต่อไป แนวคิดดังกล่าวเป็นแนวคิดที่ถูกกล่าวถึงในยุโรปตั้งแต่การพัฒนาเทคโนโลยีสารสนเทศมีความเจริญก้าวหน้าและมีข้อมูลข่าวสารจำนวนมากถูกรวบรวม จัดเก็บ และประมวลผลบนอินเทอร์เน็ตซึ่งทำให้สามารถถูกสืบค้นข้อมูลได้โดยง่าย และในบางกรณีข้อมูลที่อาจถูกผู้อื่นสืบค้นได้ง่ายนี้ก็เป็นผลเสียต่อเจ้าของข้อมูลส่วนบุคคลนั้น

ทั้งนี้ สิทธิที่จะถูกลืมเริ่มได้รับการรับรองอย่างชัดเจนในยุโรปเป็นครั้งแรกว่าเป็นส่วนหนึ่งของการคุ้มครองข้อมูลส่วนบุคคล ในรูปแบบของการวางหลักเกณฑ์เบื้องต้นจากคำวินิจฉัยของศาล (Preliminary Ruling) ผ่านการตีความของศาลยุติธรรมสหภาพยุโรป (Court of Justice of European Union : CJEU) ว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกร้องให้ผู้ให้บริการ

โปรแกรมสืบค้นข้อมูลทำการลบลิงค์ (Link) เชื่อมต่อแสดงผลการค้นหาชื่อนามสกุลของตนไปยังหน้าอื่น ๆ ได้ และท้ายที่สุด สิทธิที่จะถูกลืมก็ถูกบัญญัติรับรองในกฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation : GDPR)

ส่วนประเด็นเกี่ยวกับสิทธิที่จะถูกลืมในระบบกฎหมายไทยนั้น มาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการ “ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลนั้นกลายเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้” ในบางกรณี ได้แก่ ข้อมูลส่วนบุคคลที่หมดความจำเป็นในการเก็บรวบรวมไว้ตามวัตถุประสงค์ หรือเมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล หรือเมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข)[1] ได้ หรือเป็นการคัดค้านตามมาตรา 32 (2)[2] เป็นต้น

---

[1] มาตรา 32 (1) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ ดังต่อไปนี้ (1) กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 (4) หรือ (5) เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่า (ก) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นผู้ควบคุมข้อมูลส่วนบุคคลได้แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า (ข) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

[2] มาตรา 32 (2) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ ดังต่อไปนี้ (2) กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง

อย่างไรก็ตาม มาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้บัญญัติถึงสิทธิที่จะถูกลืมเอาไว้โดยชัดแจ้ง บทบัญญัติดังกล่าวก็ยังขาดความครอบคลุมในบางกรณี อีกทั้งยังขาดหลักเกณฑ์ที่ชัดเจนเกี่ยวกับการบังคับใช้บทบัญญัติแห่งกฎหมายเพื่อคุ้มครองสิทธิที่จะถูกลืมของเจ้าของข้อมูลส่วนบุคคลดังกล่าวด้วย

ด้วยเหตุนี้ จึงมีความจำเป็นที่จะต้องศึกษาแนวคิดที่เกี่ยวข้องกับสิทธิที่จะถูกลืมและกรณีศึกษาต่างประเทศที่เกี่ยวข้องกับการบัญญัติกฎหมายและหลักเกณฑ์เกี่ยวกับประเด็นดังกล่าว ตลอดจนคำพิพากษาของศาลที่น่าสนใจในต่างประเทศ ซึ่งสะท้อนให้เห็นการตีความและการบังคับใช้กฎหมายที่เกี่ยวกับการคุ้มครองสิทธิที่จะถูกลืม ทั้งนี้ เพื่อให้ข้อเสนอแนะเกี่ยวกับการปรับปรุงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในส่วนที่เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคลในการขอให้ผู้ควบคุมข้อมูลลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลนั้น กลายเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ โดยมุ่งศึกษาและวิเคราะห์ว่าสิทธิของเจ้าของข้อมูลส่วนบุคคลที่ปรากฏดังกล่าวนั้นหมายถึงสิทธิที่จะถูกลืมหรือไม่และเพียงใด

1.2 วัตถุประสงค์

1.2.1 เพื่อศึกษาการบัญญัติเกี่ยวกับสิทธิที่จะถูกลืมในกฎหมายไทยว่ามีความครอบคลุมเพียงใด และมีหลักเกณฑ์ตลอดจนแนวทางในการบังคับใช้อย่างไร

1.2.2 เพื่อศึกษาแนวคิด หลักเกณฑ์ และบทบัญญัติแห่งกฎหมายเกี่ยวกับสิทธิที่จะถูกลืมในต่างประเทศ

1.2.3 เพื่อให้ได้ข้อเสนอแนะต่อรัฐสภาเกี่ยวกับการแก้ไขเพิ่มเติมกฎหมายที่บัญญัติเกี่ยวกับสิทธิที่จะถูกลืมในประเทศไทย

1.3 สมมติฐานการวิจัย

แม้ว่าจะไม่ได้บัญญัติถึงสิทธิที่จะถูกลืมเอาไว้โดยชัดแจ้ง ในตัวบทกฎหมาย สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีส่วนในการคุ้มครองสิทธิที่จะถูกลืมในมิติของการลบ ทำลายหรือทำให้ข้อมูลระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ อย่างไรก็ตาม การไม่บัญญัติถึงสิทธิที่จะถูกลืมและรายละเอียดเกี่ยวกับการนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลโดยไม่จำเป็นต้องลบหรือทำลายข้อมูลส่วนบุคคลนั้น อาจส่งผลให้ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นผู้ให้บริการสืบค้นข้อมูลออนไลน์ไม่อาจปฏิบัติหน้าที่เพื่อคุ้มครองสิทธิที่จะถูกลืมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ นอกจากนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลควรออกประกาศหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลมีแนวการปฏิบัติเพื่อคุ้มครองสิทธิที่จะถูกลืมของเจ้าของข้อมูลส่วนบุคคลได้ในทางปฏิบัติ

1.4 ขอบเขตการวิจัย

1.4.1 ศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้องกับหลักสิทธิที่จะถูกลืมและบทบัญญัติขององค์กรระหว่างประเทศที่บัญญัติหลักเกี่ยวกับสิทธิที่จะถูกลืม

1.4.2 ศึกษากฎหมายที่เกี่ยวกับการคุ้มครองสิทธิที่จะถูกลืมต่างประเทศ คำพิพากษาของศาล กรณีศึกษาที่เกิดขึ้นในต่างประเทศซึ่งรวมถึงคำวินิจฉัยของหน่วยงานรัฐ และแนวปฏิบัติที่ออกโดยหน่วยงานรัฐ

1.4.3 วิเคราะห์และเสนอแนะเพื่อให้นำไปสู่การปรับปรุงบทบัญญัติเกี่ยวกับสิทธิที่จะถูกลืมในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.5 วิธีการศึกษาวิจัย

งานวิจัยนี้เป็นการวิจัยเชิงเอกสาร (documentary research) โดยเป็นการวิจัยหลักกฎหมาย (Doctrinal Legal Research) และการวิเคราะห์เปรียบเทียบกฎหมาย (Comparative Law) โดยวิธีการศึกษาและวิเคราะห์ตัวบท (Textual Analysis) ของตัวบทกฎหมาย แนวปฏิบัติ และคำวินิจฉัยของศาลที่เกี่ยวกับการคุ้มครองสิทธิที่จะถูกลืมของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อทำให้เกิดความเข้าใจถึงความเหมือนและความแตกต่างของกฎหมายซึ่งทำหน้าที่ในการคุ้มครองสิทธิที่จะถูกลืมของกฎหมายไทยและต่างประเทศ[3]

เพื่อประโยชน์ในการศึกษาวิธีกฎหมายเชิงการเปรียบเทียบ กฎหมายต่างประเทศที่ถูกนำมาเปรียบเทียบ ได้แก่ กฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) เนื่องจากเป็นกฎหมายที่มีวัตถุประสงค์และกลไกการคุ้มครองข้อมูลส่วนบุคคลที่คล้ายคลึงและเปรียบเทียบได้กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร (Data Protection Act 2018 : UK DPA 2018) ซึ่งเป็นกฎหมายที่สะท้อนให้เห็นถึงการนำ GDPR มาบังคับใช้ในทางปฏิบัติในสหราชอาณาจักร ทั้งนี้ เพื่อให้เห็นถึงรายละเอียดการปฏิบัติในการทำลายและการทำข้อมูลให้กลายเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้ ซึ่งมีรายละเอียดตามกฎหมายคุ้มครองความเป็นส่วนตัวของประเทศออสเตรเลีย (Privacy Act 1988 : AUS PA 1988) นอกจากนี้ การศึกษาและวิเคราะห์ในเชิงเปรียบเทียบยังครอบคลุมไปถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศในทวีปเอเชีย ได้แก่ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น (Act on Protection of Personal Information of Japan : APPI)

---

[3] Edward J. Eberle, 'The Method and Role of Comparative Law' (2009) Washington University Global Studies Law Review 8 (3) 451, p. 452.

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของเขตปกครองพิเศษไต้หวัน (Personal Data Protection Act 2015 : TW PDPA 2015) กฎหมายคุ้มครองข้อมูลส่วนบุคคลของเขตปกครองพิเศษฮ่องกง (Hong Kong Personal Data (Privacy) Ordinance : HK PDPO 1996) กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศฟิลิปปินส์ (Data Protection 2012 : PH PDA 2012) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ (Personal Data Protection Act 2012 : SG PDPA 2012) เหล่านี้จะช่วยให้การเปรียบเทียบครอบคลุมไปถึงการคุ้มครองสิทธิที่จะถูกลืมนอกสหภาพยุโรป

อย่างไรก็ตาม การวิจัยกฎหมายในเชิงเปรียบเทียบนั้น จำเป็นที่จะต้องก้าวออกจากการวิเคราะห์เพียงตัวบทกฎหมายและศึกษาถึงข้อเท็จจริงในสังคมในประเทศเพื่อแสดงให้เห็นว่ากฎหมายนั้นสามารถคุ้มครองสิทธิที่จะถูกลืมในทางปฏิบัติได้เพียงใด[4] ข้อเท็จจริงดังกล่าวถูกแสดงผ่านคำวินิจฉัยของศาลและคำวินิจฉัยของหน่วยงานรัฐซึ่งเผยให้เห็นถึงข้อเท็จจริงและความท้าทายของการบังคับใช้กฎหมายเพื่อคุ้มครองสิทธิที่จะถูกลืมในทางปฏิบัติคำวินิจฉัยกลุ่มที่หนึ่งเป็นคำวินิจฉัยที่แสดงให้เห็นถึงปัญหาและความจำเป็นที่จะต้องคุ้มครองสิทธิที่จะถูกลืม โดยเฉพาะอย่างยิ่งในบริบทของข้อมูลส่วนบุคคลที่ปรากฏในระบบสืบค้นออนไลน์[5] คำวินิจฉัยของศาลกลุ่มที่สองเป็นคำวินิจฉัยที่แสดงให้เห็นถึงเนื้อหาของสิทธิที่จะถูกลืมและหน้าที่ในการดำเนินการของบุคคลที่มีหน้าที่ต้องดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล[6] คำวินิจฉัยของศาลกลุ่มที่สามเป็นคำวินิจฉัยที่แสดงถึงข้อจำกัด

---

[4] Ibid.

[5] เช่น คดี *Google Spain v AEPD and Mario Costeja González* (ในสหภาพยุโรป) กรณี Uber B.V. ในประเทศออสเตเรีย และ *X v Privacy Commissioner for Personal Data (Administistrative Appeal No. 15/2019)* (ในฮ่องกง)

[6] คดี Google ในศาลฎีกาของประเทศญี่ปุ่นและกรณี David Webb Case (ในฮ่องกง)

ในการคุ้มครองสิทธิที่จะถูกลืมและปัญหาทางปฏิบัติในการชั่งน้ำหนักระหว่างสิทธิความเป็นส่วนบุคคลกับสิทธิในการแสดงออกและประโยชน์สาธารณะ[7]

1.6 ประโยชน์ที่คาดว่าจะได้รับ

รายงานวิจัยนี้ สามารถนำไปใช้เป็นข้อมูลประกอบการพิจารณาของรัฐสภาในการแก้ไขเพิ่มเติมบทบัญญัติที่กำหนดเรื่องสิทธิที่จะถูกลืมในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่

1.6.1 แนวทางในการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวกับการคุ้มครองสิทธิที่จะถูกลืมตามหลักการสากลและการบัญญัติกฎหมายในต่างประเทศ

1.6.2 ข้อจำกัดและความท้าทายของการคุ้มครองสิทธิที่จะถูกลืมในทางปฏิบัติ โดยเฉพาะอย่างยิ่งกรณีที่ข้อมูลส่วนบุคคลนั้นถูกแสดงผ่านระบบสืบค้นออนไลน์

1.6.3 เสนอแนะแนวทางในการแก้ไขมาตรา 33 ของพระราช-บัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และการออกประกาศหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

---

[7] เช่น คดี *Plaintiff X v. PrimaDanoi* คดี *NT1 & NT2 v Google LLC* คดี *Supreme Administrative Court 106 Pan Zi No. 54* (ในสหภาพยุโรป) คดี Segerstedt-Wiberg and Others v. Sweden (ในสหภาพยุโรป) กรณี Re Credit Bureau (Singapore) Pte Ltd (ในสิงคโปร์)

บทที่ 2
แนวคิดและทฤษฎีที่เกี่ยวข้อง

แม้จะยังไม่มีนิยามที่ได้รับการยอมรับเป็นการทั่วไป “สิทธิที่จะถูกลืม” สามารถถูกนิยามว่าหมายถึง สิทธิของปัจเจกบุคคลที่จะลบ จำกัด หรือเปลี่ยนแปลงข้อมูลในอดีต (Past Records) ซึ่งอาจส่งผลให้เกิดความเข้าใจผิด มีความคลาดเคลื่อนในเชิงเวลา กวนใจ หรือมีข้อมูลที่ไม่เกี่ยวกับตัวปัจเจกบุคคล[8] เมื่อข้อมูลนั้นหมดความจำเป็นหรือปราศจากฐานทางกฎหมายที่จะรองรับการประมวลผลข้อมูลนั้นอีกต่อไป[9] สิทธินี้ไม่ได้รับรองให้ปัจเจกบุคคล “แก้ไข” อดีตของตน แต่เป็นการให้ปัจเจกบุคคลสามารถ “ควบคุม (Control)” ข้อมูลส่วนบุคคลของตนได้ตามเงื่อนไข

[8] Michael J. Kelly and David Satola, ‘The Right to be Forgotten’ (2017) University of Illinois Law Review 1, p. 3.

[9] Cécile de Terwangne, ‘The Right to be Forgotten and the Informational Autonomy in the Digital Environment’ (EU Commission, 2013) <file :///C :/Users/admin/Downloads/jrc86750_cecile_fv.pdf> accessed 2 October 2021, p. 2.

ที่กฎหมายกำหนด[10] โดยเฉพาะอย่างยิ่ง การคุ้มครองเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลของบุคคลอื่นในสังคม[11] ในงานวิจัยนี้ **สิทธิที่จะถูกลืม หมายถึง สิทธิของเจ้าของข้อมูลส่วนบุคคลที่ข้อมูลส่วนบุคคลของตนจะถูกลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนได้ เมื่อหมดความจำเป็นที่ข้อมูลนั้นจะต้องถูกประมวลผลหรือเข้าถึงได้อีกต่อไป ไม่ว่าจะโดยการที่เจ้าของข้อมูลส่วนบุคคลร้องขอหรือผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการโดยปราศจากการร้องขอของเจ้าของข้อมูลส่วนบุคคล**

เพื่อทำความเข้าใจเนื้อหา วัตถุประสงค์ และผลของการใช้สิทธิที่จะถูกลืม บทที่ 2 นี้จะเริ่มด้วยการกล่าวถึงฐานและเนื้อหาของสิทธิที่จะถูกลืม (2.1) ซึ่งจะแสดงให้เห็นถึงความสำคัญของการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคล และจะแสดงถึงข้อจำกัดและความท้าทายของสิทธิที่จะถูกลืม (2.2) โดยแสดงถึงความท้าทายในการสร้างความสมดุลระหว่างการคุ้มครองความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลของบุคคลอื่น

---

[10] Maja Ovcak Kos, ‘The Right to be Forgotten and the Media’ (2019) LeXonomica 11 (2) 195, p. 195.

[11] Kamrul Faisal, ‘Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions’ (2021) Security Privacy 4, p. 2.

2.1 ฐานและเนื้อหาของสิทธิที่จะถูกลืม

สิทธิที่จะถูกลืมนั้น มีรากฐานทางประวัติศาสตร์สิทธิที่จะถูกลืมในกระบวนยุติธรรมทางอาญา กล่าวคือ สิทธิของบุคคลซึ่งถูกลงโทษในการคัดค้านการเผยแพร่ประวัติอาชญากรรมของตนหลังจากที่การลงโทษเสร็จสิ้นแล้ว[12] สิทธิที่จะถูกลืมมุ่งที่จะคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคล โดยมีเนื้อหาแห่งสิทธิที่หลากหลาย เช่น การขอให้มีการลบข้อมูลหรือการลืมไปจากฐานข้อมูล ทั้งนี้ สิทธิที่จะถูกลืมนั้นมีวิวัฒนาการไปตามความก้าวหน้าของเทคโนโลยี โดยเฉพาะอย่างยิ่งการที่ข้อมูลเกี่ยวกับตัวปัจเจกบุคคลนั้นถูกเก็บรวบรวมและแสดงผลในฐานข้อมูลอิเล็กทรอนิกส์และเครือข่ายอินเทอร์เน็ต

2.1.1 สิทธิในความเป็นอยู่ส่วนตัว (Right to Privacy)

สิทธิในความเป็นอยู่ส่วนตัวในเชิงของข้อมูล (Informational Privacy) เป็นการจำกัดการเข้าถึงบุคคลอื่นในการเข้าถึง เผยแพร่ และใช้ข้อมูลเกี่ยวกับบุคคลอื่น[13] ในมิติของความสัมพันธ์ระหว่างปัจเจกบุคคลกับรัฐนั้น สิทธิในความเป็นอยู่ส่วนตัวมุ่งที่จะจำกัดขอบเขตของอำนาจรัฐในการเข้าแทรกแซงความเป็นส่วนตัวของปัจเจกบุคคล[14] นอกเหนือจากความเป็นส่วนตัวในเชิงของข้อมูลแล้ว ความเป็นส่วนตัวยังหมายรวมถึงการไม่ถูกบุคคลอื่นและรัฐแทรกแซงทางกายภาพและในทางทรัพย์สินอีกด้วย[15]

---

[12] Adian Forde, 'Implication of the Right to Be Forgotten' (2015) Tulane Journal of Technology and Intellectual Property 18 83, p. 85.

[13] Jed Rubemfeld, 'The Right of Privacy' (1989) Harvard Law Review 102 (4) 737, p. 740.

[14] Ibid, p. 737.

[15] Anita L. Allen, 'Privacy-as-Data Control : Conceptual, Practical, and Moral Limits of the Paradigm' (2000) Connecticut Law Review 32 861, p. 866.

แนวคิดที่เกี่ยวกับหลักสิทธิที่จะถูกลืมนั้น ยึดโยงอยู่กับสิทธิในความเป็นอยู่ส่วนตัว (โดยเฉพาะอย่างยิ่งความเป็นอยู่ส่วนตัวในเชิงข้อมูล) ซึ่งถูกรับรองโดยปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights : UDHR) ว่าบุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย การสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น[16] สิทธิในความเป็นอยู่ส่วนตัวของปัจเจกบุคคลนั้นอาจถูกแทรกแซงได้โดยการเข้าถึงข้อมูลส่วนบุคคลของตนโดยบุคคลอื่น ซึ่งสามารถยกตัวอย่างได้เช่น การเข้าถึงประวัติอาชญากรรม ข้อมูลส่วนบุคคลในฐานข้อมูลของรัฐ และข้อมูลในอดีตของปัจเจกบุคคลในสื่อสังคมออนไลน์

2.1.1.1 การกระทำความผิดในอดีต

สิทธิในความเป็นอยู่ส่วนตัวของปัจเจกบุคคลนั้น อาจถูกแทรกแซงได้โดยการที่บุคคลอื่นสามารถเข้าถึงข้อมูลส่วนบุคคลของบุคคลอื่น เช่น การที่สาธารณชนยังคงสามารถเข้าถึงประวัติอาชญากรรมของบุคคลหลังจากที่ระยะเวลาหนึ่งได้ผ่านพ้นไป (โดยเฉพาะอย่างในกรณีที่การกระทำความผิดได้เกิดขึ้นเมื่อนานมาแล้ว เมื่อเวลาพ้นผ่านไปก็ไม่มีความจำเป็นที่สาธารณชนจะต้องเข้าถึงประวัติอาชญากรรมดังกล่าวอีก)[17] อย่างไรก็ตาม ประเด็นเรื่องการผ่านพ้นไปของเวลานั้นก่อให้เกิดปัญหาให้ต้องพิจารณาต่อไปว่า

---

[16] Universal Declaration of Human Rights, Article 12.

[17] Rolf H. Weber, 'The Right to Be Forgotten More Than a Pandora's Box?' (2011) Journal of Intellectual Property, Information Technology and E-Commerce 2 (2) 120, p. 121.

เวลาที่พ้นไปนั้นจะต้องนานเพียงใด[18]

ยกตัวอย่างเช่น การที่ศาลสิทธิมนุษยชนของยุโรปมีคำสั่งในคดี *Hurbain v. Belgium* ปี ค.ศ. 2021 ให้หนังสือพิมพ์ชื่อ “Le Soir” ปิดบังชื่อของคนขับรถซึ่งเป็นต้นเหตุให้เกิดอุบัติเหตุที่ทำให้มีคนเสียชีวิต โดยที่ Le Soir ได้มีการรายงานถึงชื่อและสกุลเต็มของคนขับรถในการรายงานข่าวในรูปแบบดิจิทัลซึ่งถูกเผยแพร่ใน ค.ศ. 1994 และบทความดังกล่าวได้ถูกรวมเข้ากับการทำหอจดหมายเหตุออนไลน์ ใน ค.ศ. 2008 ซึ่งศาลได้ทำการวินิจฉัยถึงระยะเวลาได้พ้นผ่านไปนับจากวันที่ได้มีการเผยแพร่ข้อมูลครั้งแรก (โดยศาลได้พิจารณาและชั่งน้ำหนักถึงเสรีภาพในการแสดงความคิดเห็นของหนังสือพิมพ์ด้วย) โดยในคดีนี้ศาลได้สรุปว่า เวลานับจากวันเกิดอุบัติเหตุได้ผ่านมานานแล้วและผู้ก่อเหตุก็ไม่ได้เป็นบุคคลสาธารณะ กรณีไม่ปรากฏคุณค่าของการที่ยังคงมีชื่อและสกุลของบุคคลที่ก่อเหตุในข่าว การเกิดสถิติของอุบัติเหตุบนท้องถนนนั้นยังคงทำได้โดยไม่ต้องมีชื่อของบุคคลอยู่[19]

2.1.1.2 ข้อมูลส่วนบุคคลในฐานข้อมูลของรัฐ

ข้อมูลส่วนบุคคลอาจถูกเก็บรวบรวมในฐานข้อมูลของรัฐ เช่น ข้อมูลเกี่ยวกับพฤติกรรมที่ถูกกล่าวหาว่าไม่ชอบด้วยกฎหมายอาจถูกเก็บรวบรวมโดยเจ้าหน้าที่ของรัฐในกระบวนยุติธรรมทางอาญา โดยมีกรณีศึกษาได้แก่ คดี *U.S. Department of Justice v. Reporters Committee* ซึ่งถูกพิพากษาโดยศาลฎีกาของสหรัฐอเมริกาในปี ค.ศ. 1989 ในคดีดังกล่าวนักข่าวได้ยื่นคำร้องข้อมูลเกี่ยวกับพี่น้องสี่คนซึ่งถูกกล่าวหาว่าได้รับข้อมูล

---

[18] Antoon De Baets, ‘A historian’s view on the right to be forgotten’ (2016) International Review of Law, Computers & Technology 30 (1) 57, p. 64.

[19] Hurbain v. Belgium – 57292/16 (European Court of Human Rights) June 2021.

จากเจ้าหน้าที่รัฐสภาที่มีพฤติกรรมทุจริตตามกฎหมายว่าด้วยเสรีภาพในข้อมูลข่าวสาร (Freedom of Information Act)[20] เมื่อคำขอถูกปฏิเสธ นักข่าวจึงได้ฟ้องคดีต่อศาลโดยอาศัยฐานที่ว่าการปฏิเสธนั้นจำกัดสิทธิในการเข้าถึงข้อมูลที่เข้าถึงได้โดยสาธารณะ

ศาลฎีกาของสหรัฐอเมริกาวินิจฉัยว่า ข้อมูลที่ถูกร้องขอนั้นแม้จะเคยเป็นข้อมูลสาธารณะอยู่ ณ เวลาหนึ่ง แต่เมื่อคำนึงถึงต้นทุนในการระบุถึงข้อมูล ตำแหน่งที่เก็บ และการเข้าถึง ทำให้เกิดความความคาดหวังอย่างสมเหตุสมผลในความเป็นส่วนตัว[21] ข้อมูลเกี่ยวกับตัวพี่น้องทั้งสี่คนนั้นไม่ได้เป็นข้อมูลสาธารณะเพียงเพราะครั้งหนึ่งเคยเป็นข้อมูลสาธารณะ แต่ความคาดหวังอย่างสมเหตุสมผลในความเป็นส่วนตัวนั้นมีอยู่เนื่องจากความยุ่งยากในการเข้าถึงข้อมูลนั้น[22]

นอกเหนือจากข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในกระบวนยุติธรรมแล้ว รัฐยังอาจเก็บรวบรวมข้อมูลส่วนบุคคลอันเกิดจากการเฝ้าระวัง (Surveillance) เช่น การที่เจ้าหน้าที่รัฐสามารถถ่ายภาพคนขับรถซึ่งแสดงภาพใบหน้าของคนขับได้อย่างชัดเจน หรือการใช้โดรน (Drones) เพื่อประโยชน์ในการตรวจตราและเฝ้าระวัง[23] อย่างไรก็ตาม กรณีนี้ยังมีปัญหาให้ต้องพิจารณาตามมาว่าความเป็นส่วนตัวในพื้นที่สาธารณะ (Privacy in Public) นั้นยังมีอยู่หรือไม่และเพียงใด[24]

---

[20] Christopher Kotfila, 'This Message Will Self-Destruct : The Growing Role of Obscurity and Self-Destructing Data in Digital Communication' (2014) Bulletin of the Association for Information Science and Technology 40 (2) 12, p. 13.

[21] Ibid.

[22] Ibid.

[23] Woodrow Hartzog and Evan Selinger, 'Surveillance as Loss of Obscurity' (2015) Washington and Law Law Review 72 (3) 1343, pp. 1347-1348.

[24] Ibid, p. 1349.

2.1.1.3 ข้อมูลในอดีตของปัจเจกบุคคลที่ถูกเผยแพร่และเข้าถึงได้ผ่านอินเทอร์เน็ต

ในปัจจุบัน อินเทอร์เน็ตได้กลายมาเป็นตัวเชื่อมการมีปฏิสัมพันธ์ระหว่างบุคคล เช่น การแลกเปลี่ยนความคิดเห็น ความรู้ คุณค่าต่าง ๆ ตลอดจนวัฒนธรรม หรือแม้กระทั่งเป็นรากฐานในการก่อการปฏิวัติ เช่น อาหรับสปริง (Arab Spring)[25] อย่างไรก็ตาม การที่อินเทอร์เน็ตได้กลายมาเป็นแหล่งข้อมูลที่ครอบคลุมพื้นที่ทั่วโลก และมีการพัฒนาอยู่ตลอดเวลาก็ส่งผลให้ข้อมูลส่วนบุคคลที่ถูกเผยแพร่และเข้าถึงได้ในอินเทอร์เน็ตตกอยู่ในความเสี่ยงที่อาชญากร หรือความเสี่ยงที่ข้อมูลส่วนบุคคลนั้นอาจเป็นอันตรายต่อข้อมูลซึ่งอยู่ในอินเทอร์เน็ตตลอดไป[26]

ในยุคที่เทคโนโลยีการสื่อสารมีความเจริญก้าวหน้า การเข้าถึงและบริหารจัดการข้อมูลได้ถูกพัฒนาจากระบบที่อาศัยหน้ากระดาษมาเป็นระบบอิเล็กทรอนิกส์ซึ่งบุคคลสามารถสื่อสารกันได้โดยง่าย[27] ยกตัวอย่างเช่น การที่บุคคลได้เข้าถึงงานสื่อสังคมออนไลน์ (Social Media) และได้มีการนำเอาข้อมูลส่วนบุคคลของตนไม่ว่าจะเป็นรูปภาพหรือความเห็นต่าง ๆ (รวมถึงข้อมูลที่ผู้ให้ข้อมูลไม่ต้องการให้มีคนอื่นเห็นอีกในอนาคต) เข้าสู่ระบบฐานข้อมูลในระบบคลาวด์ ข้อมูลส่วนบุคคลเหล่านี้แสดงถึง “อดีต” ของบุคคลที่สามารถเก็บรวบรวมข้อมูลดังกล่าวได้เป็นเวลานาน และสามารถถูกสืบค้นได้โดยบุคคลอื่น[28]

---

[25] Hunter Criscione, ‘Forgetting the Right to Be Forgotten : The Everlasting Negative Implications of a Right to Be Deferrenced on Global Freedom in the Wake of Google v. CNIL’ (2020) Pace International Law Review 32 (2) 315, p. 316.

[26] Ibid, pp. 316-317.

[27] Kamrul Faisal, *op. cit.*, p. 2.

[28] Jeffrey Rosen, ‘The Right to Be Forgotten’ (Standford Law Review (Online) 2012) <https ://www.Stanfordlawreview. org/online/privacy-paradox-the-right-to-be-forgotten/> accessed 30 September 2021.

โดยปรากฏความท้าทายเกี่ยวกับการลบข้อมูลที่ถูกเก็บรวบรวมอยู่ในระบบอินเทอร์เน็ต กล่าวคือ ข้อมูลที่เคยถูกแสดงผลในอินเทอร์เน็ตแล้ว ไม่ว่าจะเป็นการแสดงผลโดยความตั้งใจหรือโดยอุบัติเหตุ ย่อมเป็นการยากที่จะถูกลบทำลายได้[29] โดยเฉพาะอย่างยิ่งเมื่อผู้ใช้งานอินเทอร์เน็ตรายอื่นได้คัดลอกหรือดาวน์โหลดข้อมูลนั้นไป ซึ่งอาจเกิดขึ้นหลังจากที่ผู้ให้ข้อมูลได้ลบข้อมูลเหล่านั้นแล้ว ในกรณีนี้ผู้ให้ข้อมูลอาจไม่มีสิทธิตามกฎหมายที่จะเรียกให้บุคคลอื่นลบข้อมูลส่วนบุคคลของตน[30]

2.1.2 ประเภทและเนื้อหาของสิทธิที่จะถูกลืม

ในปัจจุบัน นิยามของสิทธิที่จะถูกลืมยังมีความไม่ชัดเจน[31] ในสถานการณ์ที่ตัวเจ้าของข้อมูลส่วนบุคคลไม่ประสงค์จะให้บุคคลอื่นสามารถเข้าถึงหรือสืบค้นข้อมูลเกี่ยวกับตนเองได้หรือเป็นกรณีที่หมดความจำเป็นที่สาธารณชนจะเข้าถึงข้อมูลส่วนบุคคล (เช่น ประวัติอาชญากรรมซึ่งเหตุการณ์ผ่านมานานมากแล้ว) จึงมีประเด็นให้ต้องพิจารณาต่อไปว่า การใช้สิทธิที่จะถูกลืมของเจ้าของข้อมูลส่วนบุคคลนั้น สามารถแบ่งออกได้เป็นกี่ประเภท และสิทธิแต่ละประเภทมีความแตกต่างกันอย่างไร ประเภทของสิทธิที่จะถูกลืมสามารถแบ่งออกได้ ดังนี้

---

[29] Jongwon Lee, 'What the Right to be Forgotten Means to Companies : Threat or Opportunities?' (2016) Procedia Computer Science 91 542, p. 543.

[30] Ibid.

[31] David Erdos, 'The 'right to be forgotten' beyond the EU : an analysis of wider G20 regulatory action and potential next steps' (2021) Journal of Media Law 13 (1) 1, pp. 5-6.

2.1.2.1 สิทธิในการฟื้นฟูสภาพ (Right to Rehabilitation)

สิทธิในการฟื้นฟูสภาพรับรองถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลในการร้องขอให้มีการลบประวัติที่ปรากฏในฐานข้อมูลตำรวจแห่งชาติที่ไม่ได้ถูกตัดสินว่ามีความผิด หรือเป็นประวัติที่เป็นเพียงการกล่าวหา เนื่องจากมีเหตุต้องสงสัยว่าบุคคลดังกล่าวได้กระทำผิดเท่านั้น[32] ยกตัวอย่างเช่น ในคดี *Hurbain v. Belgium* ซึ่งมีศาลสิทธิมนุษยชนของยุโรปได้วินิจฉัยว่าในการชั่งน้ำหนักระหว่างการคุ้มครองความเป็นส่วนตัวและเสรีภาพในการแสดงออกนั้น จะต้องคำนึงโอกาสของผู้กระทำความผิดในการกลับคืนสู่สังคมหลังจากที่ถูกฟื้นฟู (Rehabilitated) และรับโทษครบแล้ว[33]

2.1.2.2 สิทธิในการลบข้อมูลส่วนบุคคล (Right to Erasure)

สิทธิในการลบข้อมูลส่วนบุคคลรับรองถึงสิทธิที่เจ้าของข้อมูลส่วนบุคคลอาจใช้สิทธิร้องขอเพื่อให้มีการลบข้อมูลส่วนบุคคลออก เนื่องจากว่าเจ้าของข้อมูลส่วนบุคคลนั้นไม่ประสงค์จะให้มีการประมวลผลข้อมูลอีกต่อไป[34] โดยสำนักงานคณะกรรมการคุ้มครองข้อมูล (Information Commissioner's Office : ICO) ของสหราชอาณาจักรได้ให้ความเห็นเอาไว้ว่าสิทธิในการลบ

---

[32] ยุกต์กฤต กัณฑมณี, 'การคุ้มครองสิทธิที่จะถูกลืม' (2019) สุทธิปริทัศน์ 33 (108) 14, หน้า 18.

[33] KOD Lyons, 'Strengthening the Right to be Forgotten : The Implications of Hurbain v. Belgium' (KOD Lyons, 2021) <https :// kodlyons.ie/strengthening-the-right-to-be-forgotten-the-implications-of-hurbain-v-belgium/> accessed 2 October 2021.

[34] ยุกต์กฤต กัณฑมณี (อ้างแล้ว เชิงอรรถที่ 32), หน้า 18.

ข้อมูลนี้เป็นที่รู้จักกันในชื่อ “สิทธิที่จะถูกลืม”[35] โดยได้อธิบายว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ลบข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้[36]

- ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมไว้ ไม่มีความจำเป็นต่อวัตถุประสงค์การเก็บรวมอีกต่อไป
- ผู้ควบคุมข้อมูลส่วนบุคคลอาศัยความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเป็นฐานในการประมวลผล แต่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอมแล้ว
- ผู้ควบคุมข้อมูลส่วนบุคคลอาศัยประโยชน์อันชอบด้วยกฎหมายเป็นฐานในการประมวลผล แต่เจ้าของข้อมูลส่วนบุคคลได้คัดค้าน และไม่ปรากฏว่ามีประโยชน์อันชอบด้วยกฎหมายที่สามารถใช้เป็นฐานให้ประมวลผลข้อมูลต่อไป
- ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลเพื่อการตลาดแบบตรง แต่เจ้าของข้อมูลส่วนบุคคลได้คัดค้านการประมวลผลดังกล่าวแล้ว
- ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย
- ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องลบข้อมูลตามกฎหมาย
- ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลของผู้เยาว์เพื่อให้บริการสังคมข้อมูลข่าวสาร (Information Society Services)

---

[35] ICO, ‘Guide to the General Data Protection Regulation (GDPR)’ (ICO, January 2021) <https ://ico.org.uk/media/for-organisations/ guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf> accessed 1 October 2021, 119.

[36] Ibid.

อย่างไรก็ตาม บางประเทศได้จำแนกสิทธิที่จะถูกลืมออกจากสิทธิในการลบข้อมูลและไม่ถือว่าสิทธิในการลบข้อมูลส่วนบุคคลนั้นเป็นหนึ่งในสิทธิที่จะถูกลืม ยกตัวอย่างเช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ ได้กล่าวว่าในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของหลายประเทศไม่มีการให้สิทธิที่จะถูกลืมแก่เจ้าของข้อมูลส่วนบุคคล แต่มีเพียงการอนุญาตให้มีการลบข้อมูลส่วนบุคคลออกเมื่อสิ้นสุดระยะเวลาการเก็บรักษาข้อมูล[37]

2.1.2.3 สิทธิในการนำออกจากการแสดงข้อมูลบนเว็บไซต์ (Right to Delisting/Delinking)

สิทธิในการนำออกจากการแสดงข้อมูลบนเว็บไซต์ รับรองถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลที่อาจเป็นผู้ใช้งาน โปรแกรมสืบค้นข้อมูล ทำการใช้สิทธิดังกล่าวต่อผู้ให้บริการ โปรแกรมสืบค้นข้อมูล เพื่อให้ทำการนำเอาลิงค์ที่ปรากฏข้อมูลส่วนบุคคลของตนออกจากหน้าการแสดงผลการค้นหา[38] อย่างไรก็ตาม สิทธินี้มิใช่การลบข้อมูลส่วนบุคคลออกไปโดยสิ้นเชิง ข้อมูลส่วนบุคคลดังกล่าวจะยังคงแสดงหรือปรากฏอยู่บนหน้าเว็บเพจหรือเว็บไซต์ที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลเดิม (Original Controller) อาจกล่าวได้ว่าการดำเนินการของผู้ให้บริการระบบสืบค้นออนไลน์ในการลบลิงค์ (Link) แสดงผลการสืบค้นทางอินเทอร์เน็ต (Right to De-Listing) นั้นมีความแตกต่างจาก “สิทธิที่จะถูกลืมจากโลกดิจิทัล (Right to Digital

---

[37] 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.

[38] ยุกต์กฤต กัณฑมณี (อ้างแล้ว, เชิงอรรถที่ 28), หน้า 18.

Oblivion) อย่างแท้จริง[39]

2.1.2.4 สิทธิในการทำให้คลุมเครือ (Right to Obscurity)

สิทธิในการทำให้คลุมเครือ เป็นสิทธิในการทำให้บุคคลใด ๆ ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือทำให้เข้าถึงยากกว่าปกติ เช่น การเข้ารหัส การจำกัดการเข้าถึงข้อมูล[40] ในโลกออนไลน์นั้น การทำให้อัตลักษณ์ของบุคคลเกิดความคลุมเคลือ หมายถึง การดำเนินการให้ข้อมูลสำคัญ ๆ เช่น ข้อมูลเกี่ยวกับตัวตน ความเชื่อมโยงทางสังคม (Social Connections) และข้อมูลส่วนบุคคลอื่น ๆ นั้น ไม่อยู่ในสภาพพร้อมใช้ (Readily Available) หรือสามารถถูกถอดรหัสได้โดยบุคคลอื่น[41] อาจกล่าวอีกนัยหนึ่งได้ว่า ความคลุมเคลือในโลกออนไลน์ (Online Obscurity) หมายถึง การที่ข้อมูลยังคงอยู่ แต่ขาดองค์ประกอบอันสำคัญซึ่งทำให้ข้อมูลสามารถถูกค้นพบหรือทำความเข้าใจได้[42]

---

[39] อรรถกร สุขปุณพันธ์, “สิทธิที่จะถูกกลืม (Right to be forgotten) : จากคำวินิจนิจฉัยสู่มิติใหม่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป” (Krisdika) <https ://www.krisdika.go.th/data/activity/act352.pdf> สืบค้นเมื่อ 6 ตุลาคม พ.ศ. 2564, หน้า 4.

[40] Ibid.

[41] Alexandra Rengel, ‘Privacy as an International Human Right and the Right to Obscurity in Cyberspace’ (2014) Groningen Journal of International Law 2 (2) 33, p. 50.

[42] Ibid.

2.2 ข้อจำกัดและความท้าทายของสิทธิที่จะถูกลืม

สิทธิที่จะถูกลืมนั้นไม่ใช่สิทธิสมบูรณ์หากแต่ตกอยู่ภายใต้ข้อจำกัดหลายประการ โดยเฉพาะอย่างยิ่งในกรณีที่การใช้สิทธิที่จะถูกลืมของบุคคลหนึ่งอาจกระทบต่อสิทธิในการแสดงความเห็นหรือเข้าถึงข้อมูล[43] ดังที่ได้กล่าวในคดี *U.S. Department of Justice v. Reporters Committee* และคดี *Hurbain v. Belgium* ด้วยเหตุนี้ การทำความเข้าใจถึงข้อจำกัดของสิทธิที่จะถูกลืมนั้น ควรเริ่มต้นจากการกล่าวถึงเสรีภาพในการแสดงความคิดเห็นและเข้าถึงข้อมูล (2.2.1) และจะได้กล่าวถึงข้อพิจารณาในการสร้างความสมดุลของสิทธิที่จะถูกลืมและเสรีภาพในการแสดงความคิดเห็นและเข้าถึงข้อมูลต่อไป (2.2.2) ตลอดจนความท้าทายในการลบข้อมูลในทางปฏิบัติ (2.2.3)

2.2.1 สิทธิในการแสดงออกและเข้าถึงข้อมูลข่าวสาร

สิทธิในการแสดงออกและเข้าถึงข้อมูลข่าวสาร (Right to Freedom of Expression and Information) ปรากฏอยู่ในมาตรา 19 ของ UDHR ซึ่งบัญญัติว่า “ทุกคนมีสิทธิในอิสรภาพแห่งความเห็นและการแสดงออก สิทธินี้รวมถึงอิสรภาพในการที่จะถือเอาความเห็นโดยปราศจากการแทรกสอด และที่จะแสวงหา รับและแจกจ่ายข่าวสารและความคิดเห็นไม่ว่าโดยวิธีใด ๆ และโดยไม่คำนึงถึงเขตแดน” ในขณะที่มาตรา 10 ของอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention on Human Rights : ECHR) ก็ได้รับรองทั้งเสรีภาพในการแสดงออกและเข้าถึงข้อมูลเอาไว้เช่นกัน โดยบัญญัติว่า “ให้สิทธิเสรีภาพในการแสดงความคิดเห็นภายใต้ข้อจำกัดบางประการที่ ‘เป็นไปตามกฎหมาย’ และ ‘จำเป็นในสังคมประชาธิปไตย’” สิทธินี้รวมถึงเสรีภาพในการแสดงความคิดเห็นและในการรับและให้ข้อมูลและแนวคิด

---

[43] Rolf H. Weber, *op. cit*., p. 122.

2.2.1.1 เสรีภาพในการแสดงออก

เสรีภาพในการแสดงออกโดยเฉพาะอย่างยิ่งของสื่อมวลชนนั้นมีความสำคัญต่อสังคม ในสังคมประชาธิปไตยนั้นการรายงานข้อมูล เช่น ข้อมูลที่เกี่ยวกับประโยชน์สาธารณะนั้นเป็นสิ่งสำคัญ เนื่องจากสาธารณชนที่ได้รับข้อมูลอย่างเพียงพอและมีความถูกต้องจึงจะสามารถเข้ามีส่วนร่วมในการบริหารจัดการใด ๆ ที่เกี่ยวกับประโยชน์ของสังคม[44] ข้อมูลที่ถูกรายงานนั้นอาจมีลักษณะที่อยู่ในเชิงรุกราน (Offensive) ก่อความตื่นตระหนก หรือน่าขยะแขยงก็ได้[45] การจำกัดเสรีภาพในการแสดงออกนั้นจะต้องเป็นไปโดยจำกัดและต้องมีความสมเหตุสมผล[46]

ยกตัวอย่างเช่น ในคดี *Hurbain v. Belgium* นั้น ศาลสิทธิมนุษยชนของยุโรปได้แสดงให้เห็นว่าเสรีภาพในการแสดงความเห็นของหนังสือพิมพ์ (Freedom of Expression of the Newspaper) นั้น ส่งผลกระทบต่อสิทธิในความส่วนตัว (Private Life) ของผู้ขับรถที่ก่อให้เกิดอุบัติเหตุ โดยศาลมีหน้าที่ต้องชั่งน้ำหนักเพื่อสร้างความสมดุลของสิทธิทั้งสอง

2.2.1.2 เสรีภาพในการเข้าถึงข้อมูล

UDHR และ ECHR มิได้ให้ความสำคัญเฉพาะสิทธิของ “ผู้พูด” เท่านั้น หากแต่ยังให้ความสำคัญกับ “ผู้ฟัง” อีกด้วย ยกตัวอย่างเช่น การที่สาธารณชนจำเป็นที่จะต้องเข้าถึงข้อมูลที่อาจก่อความไม่พอใจให้กับรัฐได้

---

[44] Maja Ovcak Kos, ‘The Right to be Forgotten and the Media’ (2019) LeXonomica 11 (2) 195, pp. 204-205.

[45] Ibid.

[46] Ibid.

ในกรณีที่ข้อมูลนั้นได้มาโดยชอบ[47] ในปัจจุบันการเก็บรวบรวมข้อมูลจำนวนมากนั้นเกิดขึ้นผ่านเครือข่ายอินเทอร์เน็ต โดยผู้ให้บริการต่าง ๆ ไม่ว่าจะเป็นสำนักพิมพ์หรือผู้ให้บริการสืบค้นข้อมูลออนไลน์ การยอมให้มีลบข้อมูลออกอาจเป็นทางหนึ่งในการทำลายหลักฐานที่ถูกสืบค้นทางออนไลน์ได้[48]

นอกจากนี้ ยังปรากฏข้อโต้แย้งว่าการที่ข้อมูลมีความเกี่ยวข้องกับปัจเจกบุคคลไม่ได้หมายความว่าข้อมูลเป็นของปัจเจกบุคคลคนนั้นหรือบุคคลคนนั้นมีสิทธิควบคุมข้อมูลนั้นโดยอาศัยสิทธิในทางทรัพย์สิน[49] โดยเฉพาะอย่างยิ่ง ปัจเจกบุคคลไม่ควรจะจำกัดสิทธิของบุคคลอื่นที่จะเข้าถึงข้อมูลเกี่ยวกับตนซึ่งถูกเผยแพร่โดยบุคคลอื่น เว้นแต่เป็นข้อมูลส่วนบุคคลหรือก่อให้เกิดความเสียหายต่อชื่อเสียง[50] หรือกล่าวอีกนัยหนึ่งได้ว่าข้อมูลเกี่ยวกับปัจเจกบุคคลก็เป็นของสาธารณชนอย่างเท่าเทียมกับตัวปัจเจกบุคคล[51] ยกตัวอย่างเช่น ข้อมูลที่บุคคลธรรมดาถูกประกาศให้เป็นคนล้มละลายเมื่อสิบปีก่อน ไม่ได้เป็นเพียงข้อมูลของบุคคลคนนั้นเท่านั้น แต่ยังเกี่ยวข้องกับลูกหนี้ที่เกี่ยวข้องและการประกาศโดยศาลอย่างเปิดเผยอีกด้วย[52]

---

[47] Shaniqua Singleton, 'Balancing Right to Be Forgotten with A Right to Freedom of Expression in the Wake of Google vs AEPD' (2015) Georgia Journal of International and Comparative Law (44) 165, p. 179.

[48] Melanie Dulong de Rosnay and Andres Guadamuz, 'Memory Hole or Right to Delist? Implications of the Right to be Forgotten for Web Archiving' (RESET, 19 April 2019) <file :///F :/reset-807.pdf> accessed 2 October 2021, p. 1.

[49] Article 19, 'The Right to be Forgotten" : Remembering Freedom of Expression' (Article 19, 2015) <file :///F :/The_right_to_be_ forgotten_A5_ EHH_HYPERลิงค์.pdf> accessed 2 October 2021, p. 15.

[50] Ibid.

[51] Ibid.

[52] Ibid.

อย่างไรก็ตาม มีข้อสังเกตว่าข้อมูลส่วนบุคคลที่อยู่ในฐานข้อมูลสาธารณะโดยไม่ชอบด้วยกฎหมายย่อมไม่ควรถูกเข้าถึงได้ หรือกล่าวอีกนัยหนึ่ง คือ ไม่อยู่ในความคุ้มครองของสิทธิในการเข้าถึงข้อมูล ยกตัวอย่างเช่น ภาพที่ส่วนตัว (Intimate Photos) ซึ่งถูกเผยแพร่ทางอินเทอร์เน็ตโดยปราศจากความยินยอม ในกรณีนี้บุคคลอื่นย่อมไม่มีเหตุผลที่จะเข้าถึงภาพนั้น ๆ[53]

2.2.2 การสร้างความสมดุลของสิทธิที่จะถูกลืมและเสรีภาพในการแสดงความคิดเห็นและเข้าถึงข้อมูล

สิทธิที่จะถูกลืมนั้นไม่อาจดำรงอยู่ได้โดยปราศจากการคำนึงถึงเสรีภาพในการแสดงความคิดเห็น ทั้งสิทธิที่จะถูกลืมและเสรีภาพในการแสดงความคิดเห็นนั้นไม่อาจเอาชนะอีกฝ่ายได้อย่างเด็ดขาดแต่ต้องอยู่ร่วมกันได้[54] กล่าวอีกนัยถึง คือ จะต้องมีการสร้างความสมดุลของสิทธิและเสรีภาพโดยมีข้อพิจารณาที่สำคัญ คือ การพิจารณาถึงประโยชน์สาธารณะที่ถูกคุ้มครองจากการที่ข้อมูลส่วนบุคคลยังคงถูกเข้าถึงหรือแสดงได้ต่อไป

2.2.2.1 การพิจารณาถึงประโยชน์สาธารณะ

สื่อมวลชนย่อมมีเสรีภาพในการนำเสนอข้อมูลข่าวสารต่าง ๆ ข้อมูลที่สื่อมวลชน เช่น สำนักข่าวนำเสนอโดยผ่านฐานหนังสือพิมพ์ออนไลน์อาจถูกค้นหาและเข้าถึงโดยบุคคลทั่วไปในสังคม อย่างไรก็ตาม บุคคลที่มีชื่อปรากฏในข่าวนั้นอาจไม่ประสงค์ให้ชื่อของตนอยู่ในข่าวไปตลอด ด้วยเหตุนี้จึงมีปัญหาที่จะต้องมีการชั่งน้ำหนักระหว่างเสรีภาพในการรายงานข่าว

---

[53] Ibid.

[54] Shaniqua Singleton, *op. cit.*, p. 181.

ของสำนักข่าวและการเข้าถึงข้อมูลของสาธารณชนกับสิทธิในความส่วนตัวของเจ้าของข้อมูลส่วนบุคคล ในกรณีนี้สามารถศึกษาได้จากคดี *Plaintiff X v. PrimaDanoi* ซึ่งคดีที่ถูกพิพากษาโดยศาลฎีกาของประเทศอิตาลี

คดี *Plaintiff X v. PrimaDanoi* ใน ค.ศ. 2008 เกิดจากการที่มีบุคคลธรรมดาสี่คนได้ก่อเหตุทะเลาะวิวาทกันนอกร้านอาหาร โดยมีบุคคลคนหนึ่งในนั้นเป็นเจ้าของร้านอาหาร ระหว่างการต่อสู้มีบุคคลคนหนึ่งถูกแทง ต่อมาเจ้าหน้าที่ตำรวจมาถึงและจับบุคคลที่เกี่ยวข้องกับเหตุต่อสู้ทะเลาะวิวาทนั้น หนังสือพิมพ์ออนไลน์ชื่อ PrimaDanoi ได้เผยแพร่เรื่องดังกล่าวในเครือข่ายอินเทอร์เน็ต[55] ต่อมาในเดือนกันยายน ค.ศ. 2010 เจ้าของร้านอาหารได้ร้องขอให้ Prima Danoi นำข้อมูลเกี่ยวกับเหตุการณ์ต่อสู้ทะเลาะวิวาทออก เนื่องจากตามความเห็นของเขาข้อมูลเหล่านี้ล้าสมัยแล้ว แต่ Prima Danoi ปฏิเสธการนำข้อมูลออกจากระบบ[56]

ในเดือนตุลาคม ค.ศ. 2010 เจ้าของร้านอาหารฟ้องคดีต่อศาล โดยอ้างว่าการเผยแพร่ข้อมูลออนไลน์นั้นส่งผลต่อชื่อเสียงของเขา “โดยปราศจากประโยชน์สาธารณะในบทความ”[57] ก่อนที่ศาลจะมีคำพิพากษา Prima Danoi สมัครใจนำบทความดังกล่าวออกจากระบบ แต่เจ้าของร้านอาหารยังคงดำเนินคดีต่อไป ศาลฎีกาของประเทศอิตาลีวินิจฉัยว่าแม้บทความดังกล่าวจะถูกเผยแพร่โดยชอบด้วยกฎหมายและเคยมีประโยชน์สาธารณะ แต่การที่ยังทำให้บทความนี้สามารถเข้าถึงได้ อย่างไม่ได้สัดส่วนก่อให้เกิดผลกระทบต่อสิทธิ

---

[55] Global Freedom of Expression, ‘Plaintiff X v. PrimaDaNoi’ (Columbia University, 2015) <https ://globalfreedomofexpression. columbia.edu/cases/plaintiff-x-v-primadanoi/> accessed 1 October 2021.

[56] Ibid.

[57] Ibid.

ในความเป็นอยู่ส่วนตัวของบุคคล[58] ศาลยอมรับถึงความสำคัญของสิทธิในการรายงานข้อมูล แต่ก็ได้วินิจฉัยว่า “ข้อมูลที่มีความอ่อนไหว (Sensitive Information) และข้อมูลส่วนตัว (Private Information) ไม่ควรจะถูกทำให้เข้าถึงได้โดยสาธารณชนโดยปราศจากการจำกัดเวลา (เว้นแต่สำนักพิมพ์จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล)” ศาลจึงพิพากษาให้ Prima Danoi ชดใช้ค่าเสียหายแก่เจ้าของร้านอาหารจำนวน 10,000 ยูโร[59]

2.2.2.2 การพิจารณาถึงความคาดหวังว่าข้อมูลจะถูกเก็บเป็นความลับ

ในคดี *U.S. Department of Justice v. Reporters Committee* นั้น ศาลฎีกาของสหรัฐอเมริกาได้วินิจฉัยว่า การคำนึงถึงต้นทุนในการระบุถึงข้อมูล ตำแหน่งที่เก็บ และการเข้าถึง ทำให้เกิดความคาดหวังอย่างสมเหตุสมผลในความเป็นส่วนตัวได้ หรือกล่าวอีกนัยหนึ่ง คือ หากข้อมูลส่วนบุคคลนั้นถูกทำให้เข้าถึงได้ยากหรือยากที่จะทำความเข้าใจได้ เจ้าของข้อมูลส่วนบุคคลอาจคาดหวังให้มีความคลุมเครือของข้อมูลส่วนบุคคลของตนได้[60]

---

[58] Marko Milosavljevic, Melita Poler, and Rok Ceferin, ‘In the Name of the Right to be Forgotten : New Legal and Policy Issues and Practices regarding Unpublishing Requests in Slovenian Online News Media’ (2020) Digital Journalism 8 (6) 780, p. 783.

[59] Ibid.

[60] Patrick C. File, ‘A History of Practical Obscurity : Clarifying and Contemplating the Twentieth Century Roots of a Digital Age : Concept of Privacy’ (2017) UB Journal of Media Law & Ethics 6 (1/2) 1, pp. 4-5.

2.2.3 ปัญหาของผู้ควบคุมข้อมูลในทางปฏิบัติ

เมื่อต้องเคารพต่อสิทธิที่จะถูกลืม ผู้ควบคุมข้อมูลส่วนบุคคล เช่น สำนักพิมพ์หรือผู้ให้บริการระบบสืบค้นออนไลน์ย่อมประสบความท้าทายในการพิจารณาถึงปัจจัยที่จะต้องนำมาชั่งน้ำหนัก ระหว่างเสรีภาพที่ตนมีกับความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล เช่น การพิจารณาถึงเวลาที่ได้ผ่านพ้นไป ดังเช่นในคดี *Hurbain v. Belgium* ที่ผู้เผยแพร่ข้อมูลเกี่ยวกับอุบัติเหตุนั้นจะต้องพิจารณาว่าเวลาที่ตนได้เผยแพร่ข้อมูลซึ่งมีชื่อและสกุลของผู้กระทำความผิดนั้นได้ผ่านพ้นมานานเพียงใดและนานเพียงพอหรือยัง การคงชื่อและสกุลของผู้ก่อเหตุยังเป็นประโยชน์ต่อสาธารณะอีกหรือไม่

ในคดี *Plaintiff X v. Prima Danoi* ได้เน้นย้ำว่า ข้อมูลส่วนบุคคลที่เคยเป็นประโยชน์ต่อสาธารณชน ณ เวลาใดเวลาหนึ่งอาจหมดความสำคัญลงเมื่อเวลาพ้นผ่านไป ดังนั้น ในเชิงกฎหมายแล้วผู้ควบคุมข้อมูล (ตลอดจนหน่วยงานของรัฐที่เกี่ยวข้องกับการคุ้มครองสิทธิที่จะถูกลืม) ย่อมจะต้องพิจารณาถึงปัจจัยดังกล่าว ตลอดจนมาตรการที่สามารถดำเนินการได้ เช่น การทำให้ไม่ปรากฏข้อมูลที่ระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้

บทสรุป

“สิทธิที่จะถูกลืม” นั้น ถูกพัฒนาขึ้นจากแนวคิดเรื่องความเป็นส่วนตัวซึ่งเป็นสิทธิมนุษยชนประการหนึ่ง ไม่ว่าจะในส่วนความเป็นส่วนตัวในคดีอาญา และความเป็นอยู่ส่วนตัวในเชิงของข้อมูล โดยสารัตถะแล้วสิทธิชนิดนี้เรียกให้ข้อมูลส่วนบุคคลของบุคคลนั้นถูกลบ ทำลาย หรือเข้าถึงไม่ได้เมื่อหมดความจำเป็นที่ข้อมูลส่วนบุคคลนั้นจะต้องถูกประมวลผลแสดง หรือเข้าถึงได้โดยบุคคลอื่น การหมดลงของความจำเป็นดังกล่าวนั้นอาจเกิดขึ้นโดยหลากหลายสาเหตุ เช่น การพ้นผ่านไปของเวลา

ข้อมูลส่วนบุคคลที่จำเป็นจะต้องถูกแสดงหรือเข้าถึงได้ ณ เวลาหนึ่งในอดีต อาจไม่มีความจำเป็นที่จะต้องถูกเข้าถึงหรือแสดงผลได้อีกต่อไปในปัจจุบัน ซึ่งจะต้องพิจารณาเป็นรายกรณี

อย่างไรก็ตาม สิทธิที่จะถูกลืมของบุคคลนั้น ไม่ได้เป็นสิทธิที่ปราศจากข้อจำกัด เนื่องจากการลบ ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลของคนหนึ่งเข้าถึงไม่ได้นั้น กระทบต่อสิทธิในการเข้าถึงข้อมูลและกระทบต่อเสรีภาพในการแสดงความคิดเห็นของบุคคลอื่นในสังคมได้ ด้วยเหตุนี้ การคุ้มครองสิทธิที่จะถูกลืมนั้นจึงถูกท้าทายด้วยความจำเป็นในการชั่งน้ำหนักระหว่างการคุ้มครองความเป็นส่วนตัวของบุคคลคนหนึ่งกับสิทธิในการเข้าถึงข้อมูล และเสรีภาพในการแสดงความคิดเห็นของบุคคลอื่น นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลยังประสบปัญหาในทางเทคนิคว่าจะทำการลบ ทำลาย หรือทำให้ข้อมูลไม่อาจระบุถึงตัวตนของบุคคลซึ่งถูกแสดงหรือสามารถถูกเข้าถึงได้ในอินเทอร์เน็ตผ่านระบบการสืบค้นข้อมูลออนไลน์นั้นอย่างไร

เพื่อประโยชน์ในการส่งเสริมและพัฒนาการคุ้มครองสิทธิที่จะถูกลืมในประเทศไทย ในบทถัดไปจะได้อธิบายถึงเนื้อหาสิทธิในความเป็นส่วนตัวและสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และบทบัญญัติแห่งกฎหมาย แนวปฏิบัติ และกรณีศึกษาเกี่ยวกับการคุ้มครองสิทธิที่จะถูกลืมของต่างประเทศ

บทที่ 3
มาตรการทางกฎหมายเกี่ยวกับสิทธิที่จะถูกลืมในกฎหมายไทยและกฎหมายต่างประเทศ

การรับรองและคุ้มครองสิทธิที่จะถูกลืมซึ่งปรากฏตามทฤษฎีและหลักการที่เกี่ยวข้องตามที่ได้กล่าวในบทที่ 2 นั้น จะต้องอาศัยทั้งการตรากฎหมายรับรองและเงื่อนไขในการใช้สิทธิดังกล่าว ตลอดจนการกำหนดรายละเอียดของสิทธิในการแก้ไขกฎหมายว่าด้วยการคุ้มครองสิทธิที่จะถูกลืม ดังนั้น ในบทที่ 3 นี้จึงจะกล่าวถึงบทบัญญัติแห่งกฎหมาย แนวปฏิบัติและกรณีศึกษาเกี่ยวกับการคุ้มครองสิทธิที่จะถูกลืมใน (3.1) ประเทศไทย (3.2) สหภาพยุโรป (3.3) สหราชอาณาจักร (3.4) ประเทศออสเตรเลีย (3.5) ประเทศญี่ปุ่น (3.6) เขตปกครองพิเศษไต้หวัน (3.7) เขตปกครองพิเศษฮ่องกง (3.8) ประเทศฟิลิปปินส์ และ (3.9) ประเทศสิงคโปร์ โดยเนื้อหาในบทที่ 3 นี้ให้ความสำคัญกับแนวทางการบัญญัติกฎหมายและแนวปฏิบัติที่เกี่ยวข้องของแต่ละประเทศเพื่อประโยชน์ในการวิเคราะห์กฎหมายในเชิงเปรียบเทียบดังจะได้กล่าวในบทที่ 4 ต่อไป

3.1 ประเทศไทย

ก่อนที่จะมีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ระบบกฎหมายไทยได้รับรองถึง “สิทธิในความเป็นส่วนตัว” ในกฎหมายหลายฉบับ เช่น รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และประมวลกฎหมายแพ่งและพาณิชย์ ซึ่งแสดงให้เห็นถึงความจำเป็นในการสร้างความสมดุลระหว่างการคุ้มครองสิทธิในความเป็นส่วนตัว และเสรีภาพในการแสดงความคิดเห็น ดังที่ได้กล่าวในหัวข้อที่ 2.2 ในบทที่ 2 นอกจากนี้ ยังปรากฏการบังคับใช้กฎหมายเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวในคำพิพากษาของศาลฎีกาอีกด้วย ซึ่งฐานทางกฎหมายและกระบวนการบังคับใช้กฎหมายดังกล่าวสามารถช่วยสนับสนุนการคุ้มครองสิทธิที่จะถูกลืม และร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามมาตรา 33 ของพระราชบัญญัติต่อไป

3.1.1 ตัวบทกฎหมาย

3.1.1.1 รัฐธรรมนูญและความรับผิดในฐานละเมิดตามประมวลกฎหมายแพ่งและพาณิชย์

ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว[61] การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลดังกล่าว หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัย

[61] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560, มาตรา 32 วรรคหนึ่ง.

อำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ[62] ในขณะเดียวกันรัฐธรรมนูญก็ได้รับรองให้บุคคลมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น การจำกัดเสรีภาพดังกล่าวจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเฉพาะเพื่อรักษาความมั่นคงของรัฐ เพื่อคุ้มครองสิทธิหรือเสรีภาพของบุคคลอื่น เพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเพื่อป้องกันสุขภาพของประชาชน[63]

การคุ้มครองทั้งสิทธิเสรีภาพตามรัฐธรรมนูญในเวลาเดียวกันอาจก่อให้เกิดปัญหาในทางปฏิบัติได้ การที่สื่อมวลชนสามารถเข้าถึงข้อมูลส่วนบุคคลของบุคคลอื่นมาเพื่อรายงานข่าวอันถือได้ว่าเป็นการใช้เสรีภาพในการแสดงความคิดเห็น แต่ขณะเดียวกันการรายงานข่าวโดยปราศจากขอบเขตก็อาจกระทบต่อสิทธิในความเป็นส่วนตัวของบุคคลได้ อาจเกิดเป็นข้อพิพาททางกฎหมายขึ้น กรณีปัญหาดังกล่าวสามารถศึกษาได้จากคำพิพากษาศาลฎีกาที่ 4893/2558

ในคดีดังกล่าว สื่อมวลชนสองรายนำข่าวการมีเพศสัมพันธ์ของชายหญิงคู่หนึ่งซึ่งหนังสือพิมพ์ฉบับอื่น ๆ เคยนำเสนอภาพและข่าวไปก่อนหน้านั้น เนื้อข่าวว่าชายในภาพที่กำลังมีเพศสัมพันธ์กับหญิงคนรักคือโจทก์ ศาลฎีกาวินิจฉัยว่าแม้สื่อมวลชนจะมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณาหรือสื่อความหมายโดยวิธีอื่น ๆ แต่ก็หาอาจกระทำการใด ๆ ที่เป็นการก้าวล่วงหรือกระทบกระเทือนต่อสิทธิในความเป็นส่วนตัวของบุคคลอื่น ย่อมถือได้ว่าเป็นการกระทำที่เป็นการก้าวล่วงหรือกระทบกระเทือนต่อสิทธิในความเป็นส่วนตัวของโจทก์

---

62 Ibid, มาตรา 32 วรรคสอง.

63 Ibid, มาตรา 34 วรรคหนึ่ง.

จึงเป็นการละเมิดต่อโจทก์ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420[64] จะเห็นได้ว่า ศาลฎีกาได้อาศัยหลักกฎหมายในเรื่องละเมิดตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 มาเป็นฐานในการวินิจฉัยความรับผิดของสื่อมวลชนทั้งที่ มาตรา 420 นั้น ไม่ได้บัญญัติถึงสิทธิในความส่วนตัวโดยตรงแต่บัญญัติถึง “ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใด”

3.1.1.2 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

ในคดี *U.S. Department of Justice v. Reporters Committee* ได้แสดงให้เห็นว่า ข้อมูลที่ถูกเก็บรวบรวมโดยรัฐนั้น อาจก่อให้เกิดสถานการณ์ที่จะต้องมีการใช้สิทธิที่จะถูกลืมได้ เช่น เป็นกรณีที่ข้อมูลส่วนบุคคลของปัจเจกบุคคลถูกเก็บรวบรวมโดยเจ้าหน้าที่รัฐในกระบวนการยุติธรรม การเปิดเผยข้อมูลข่าวสารที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐนั้นเป็นหน้าที่ประการหนึ่งของหน่วยงานรัฐในประเทศไทยตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ทั้งนี้ เพื่อให้ประชาชนมีโอกาสกว้างขวางในการได้รับข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่าง ๆ ของรัฐเป็นสิ่งจำเป็น และเพื่อที่ประชาชนจะสามารถแสดงความคิดเห็นและใช้สิทธิทางการเมืองได้โดยถูกต้องกับความเป็นจริง ที่เป็นการส่งเสริมให้มีความเป็นรัฐบาลโดยประชาชนมากยิ่งขึ้นอันเป็นการส่งเสริมระบอบประชาธิปไตย[65]

โดยหลักแล้ว ข้อมูลข่าวสารที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐหรือข้อมูลข่าวสารเกี่ยวกับเอกชน (ข้อมูลข่าวสารของราชการ)

---

[64] คาพิพากษาศาลฎีกาที่ 4893/2558.

[65] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540, หมายเหตุ.

ต้องถูกพิมพ์ลงในราชกิจจานุเบกษา[66] จัดให้ประชาชนเข้าตรวจดูได้[67] จัดหาข้อมูลข่าวสารนั้นให้แก่ผู้ขอภายในเวลาอันสมควร[68] อย่างไรก็ตาม กฎหมายก็ได้กำหนดข้อจำกัดประการหนึ่งเอาไว้ว่าการรายงานการแพทย์ หรือ “ข้อมูลข่าวสารส่วนบุคคล” ซึ่งการเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควรนั้น หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยก็ได้ โดยคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานของรัฐ ประโยชน์สาธารณะ และประโยชน์ของเอกชนที่เกี่ยวข้องประกอบกัน[69]

อย่างไรก็ตาม ข้อมูลบางประเภทที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐบางประเภท ซึ่งรวมถึงข้อมูลส่วนบุคคลนั้น หน่วยงานของรัฐอาจมีคำสั่งมิให้เปิดเผยก็ได้ โดยคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานของรัฐ ประโยชน์สาธารณะ และประโยชน์ของเอกชนที่เกี่ยวข้องประกอบกันตามมาตรา 15 (5) ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ถ้าเจ้าหน้าที่เห็นว่าการเปิดเผยข้อมูลรายงานการแพทย์หรือข้อมูลข่าวสารส่วนบุคคลซึ่งการเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร เจ้าหน้าที่อาจมีคำสั่งไม่เปิดเผยข้อมูลข่าวสารส่วนบุคคลก็ได้[70]

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้บัญญัตินิยามของ “ข้อมูลข่าวสารส่วนบุคคล” เอาไว้ว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมายรหัส

---

[66] Ibid, มาตรา 7.

[67] Ibid, มาตรา 9.

[68] Ibid, มาตรา 11.

[69] Ibid, มาตรา 15 (5).

[70] สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, *สิทธิรับรู้ข้อมูลข่าวสารของประชาชน* (พิมพ์ครั้งที่ 2) (สามเจริญพาณิชย์, มีนาคม พ.ศ. 2549) หน้า 28.

หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย[71]

อย่างไรก็ตาม มีข้อสังเกตว่าข้อยกเว้นการที่เจ้าหน้าที่อาจมีคำสั่งไม่เปิดเผยรายงานการแพทย์หรือข้อมูลข่าวสารส่วนบุคคลนั้น แม้ว่าจะมีวัตถุประสงค์ในการคุ้มครองความเป็นส่วนตัวของบุคคล กล่าวคือ ป้องกันมิให้มีการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร แต่อำนาจของหน่วยงานรัฐนั้นมิได้มีลักษณะเป็นสิทธิที่จะถูกลืม เนื่องจากไม่ได้กำหนดถึงการลบ ทำลาย หรือทำให้รายงานการแพทย์และข้อมูลข่าวสารส่วนบุคคลกลายเป็นข้อมูลที่ระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้เมื่อหมดความจำเป็นที่หน่วยงานรัฐจะต้องประมวลผลข้อมูลส่วนบุคคลอีกต่อไป

3.1.1.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ถูกตราขึ้นเพื่อคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป[72] ในส่วนของการคุ้มครองสิทธิที่จะถูกลืมนั้น ถูกสะท้อนผ่านสิทธิในการ“เรียกร้อง” ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการลบทำลายข้อมูลส่วนบุคคลตามมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

---

[71] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540, มาตรา 4.

[72] Ibid, หมายเหตุ,

(ก) นิยามของข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัตินิยามของ “ข้อมูลส่วนบุคคล” เอาไว้ว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ[73] นิยามของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น มีถ้อยคำที่แตกต่างไปจากนิยามของคำว่า “ข้อมูลข่าวสารส่วนบุคคล” ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เนื่องจากพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้บัญญัตินิยามของข้อมูลข่าวสารส่วนบุคคล โดยเริ่มต้นนิยามจากตัวอย่างของข้อมูลส่วนบุคคลเอาไว้ ในขณะที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้บัญญัตินิยามโดยเริ่มต้นจากลักษณะของข้อมูลส่วนบุคคล กล่าวคือ ข้อมูลใด ๆ ซึ่งสามารถระบุถึงตัวตนของบุคคลได้ อย่างไรก็ตาม ทั้งข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 นั้นมีสารัตถะตรงกันเนื่องจากข้อมูลข่าวสารส่วนบุคคลรวมถึง “สิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้” อีกด้วย

ความแตกต่างของนิยามระหว่างข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จะอยู่ในส่วนของข้อมูลของผู้ที่ถึงแก่กรรมแล้ว ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลไม่รวมถึงข้อมูลของบุคคลที่ถึงแก่กรรมแล้ว[74] ในขณะที่ข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติ

---

[73] Ibid, มาตรา 6.

[74] สอดคล้องกับแนวทางของ GDPR ดังปรากฏตาม Recital 27 ของ GDPR ซึ่งบัญญัติไว้อย่างชัดเจนว่า GDPR ไม่ใช้บังคับแก่ข้อมูลของบุคคลที่ถึงแก่กรรมแล้ว

ข้อมูลข่าวสารของราชการ พ.ศ. 2540 นั้นรวมถึงข้อมูลของบุคคลผู้ถึงแก่กรรม[75] ความแตกต่างดังกล่าวส่งผลให้เกิดประเด็นในการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่เก็บรวบรวมข้อมูลที่เกี่ยวกับบุคคลที่ถึงแก่กรรมแล้ว

กรณีที่หนึ่ง หากหน่วยงานของรัฐซึ่งเก็บรวบรวมข้อมูลบุคคล (เช่น ข้อมูลเกี่ยวกับประวัติการรักษาพยาบาลก่อนถึงแก่กรรมและข้อมูลเกี่ยวกับญาติของผู้ที่ถึงแก่กรรมแล้ว) ที่ถึงแก่กรรมแล้วได้รับคำร้องจากบุคคลขอให้เปิดเผยข้อมูลเกี่ยวกับบุคคลที่ถึงแก่กรรมแล้ว หากหน่วยงานของรัฐพิจารณาแล้วเห็นว่าการเปิดเผยข้อมูลของบุคคลที่ถึงแก่กรรมแล้วจะเป็นการล่วงล้ำความเป็นส่วนตัวของผู้ถึงแก่กรรมมากเกินสมควร หน่วยงานของรัฐอาจใช้อำนาจตามมาตรา 15 (5) ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ปฏิเสธคำขอการเข้าถึงข้อมูลเกี่ยวกับผู้ถึงแก่กรรมได้ อย่างไรก็ตาม เหตุปฏิเสธการเปิดเผยตามมาตรา 15 (5) ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มิได้กำหนดให้มีการลบ ทำลาย หรือทำให้รายงานการแพทย์และข้อมูลข่าวสารส่วนบุคคลแต่ประการใด

กรณีที่สอง หากเปลี่ยนข้อเท็จจริงเป็นว่าผู้ควบคุมข้อมูลส่วนบุคคลนั้นเป็นบุคคลเอกชน ผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าวย่อมไม่ตกอยู่ในบังคับของมาตรา 15 (5) ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่จะปฏิเสธคำขอเข้าถึงข้อมูลเกี่ยวกับบุคคลที่ถึงแก่กรรม และไม่ตกอยู่ในบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในเรื่องการลบ ทำลาย หรือทำให้ข้อมูลกลายเป็นข้อมูลที่ระบุตัวตนของบุคคลมิได้

[75] สอดคล้องกับแนวทางของพระราชบัญญัติว่าด้วยเสรีภาพในการเข้าถึงข้อมูลของสหราชอาณาจักร (Freedom of Information Act 2000) ซึ่งไม่ได้บัญญัติยกเว้นข้อมูลของผู้ถึงแก่กรรม โปรดดู ICO, 'Information about the deceased : Freedom of Information Act & Environmental Information Regulations' (ICO, May 2013) <https ://ico.org.uk/media/for-organisations/documents/1202/information-about-the-deceased-foi-eir.pdf> accessed 13 November 2021, p. 3.

(ข) การลบทำลายหรือทำให้ข้อมูลระบุตัวตนของบุคคลไม่ได้

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เจ้าของข้อมูลส่วนบุคคลมีสิทธิ “เรียกร้อง” ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีตามตารางที่ 3-1 ดังต่อไปนี้[76]

ตารางที่ 3-1 : สิทธิในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล
• เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
• เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป
• เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 32 (1) และ - <u>ผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) :</u> การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลได้แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า หรือ

[76] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 33 วรรคหนึ่ง.

ตารางที่ 3-1 : สิทธิในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล
- ผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ข) : การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือ - เป็นการคัดค้านตามมาตรา 32 (2) : กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง
• เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยต่อสาธารณะ และผู้ควบคุมข้อมูลส่วนบุคคลถูกขอให้ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลต้องเป็นผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำขอนั้น โดยแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ เพื่อให้ได้รับคำตอบในการดำเนินการให้เป็นไปตามคำขอ[77]

เมื่อสิทธิในการลบทำลายหรือทำให้ข้อมูลระบุตัวตนของบุคคลไม่ได้เป็นสิทธิสัมบูรณ์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[77] Ibid, มาตรา 33 วรรคสาม.

จึงได้บัญญัติถึง “ข้อยกเว้น” ในการใช้สิทธิในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลเช่นเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศที่จะได้กล่าวต่อไปในหัวข้อที่ 3.2 ถึง 3.9 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งข้อยกเว้นการใช้สิทธิตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สามารถแสดงได้ตามตารางที่ 3-2 ดังนี้[78]

ตารางที่ 3-2 : ข้อยกเว้นในการใช้สิทธิในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล
• การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
• การเก็บรักษาไว้เพื่อวัตถุประสงค์ - เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด[79] - การเก็บรักษาไว้ หรือเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล[80]

[78] Ibid, มาตรา 33 วรรคสอง.

[79] Ibid, มาตรา 24 (1).

[80] Ibid, มาตรา 24 (4).

ตารางที่ 3-2 : ข้อยกเว้นในการใช้สิทธิในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล

- เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์[81]
- ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ[82]

[81] Ibid, มาตรา 26 (5) (ก).

[82] Ibid, มาตรา 26 (5) (ข).

ตารางที่ 3-2 : ข้อยกเว้นในการใช้สิทธิในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล
- การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

ข้อยกเว้นการใช้สิทธิในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลตามมาตรา 33 วรรคสอง ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น แสดงให้เห็นว่าการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลนั้น มีความจำกัดและจะต้องตั้งอยู่บนพื้นฐานของความสมดุลกับประโยชน์อื่น ๆ **ประการแรก** ได้แก่ การเก็บรักษาข้อมูลส่วนบุคคลไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น เช่น ความจำเป็นที่สื่อมวลชนหรือสำนักพิมพ์จำเป็นต้องเก็บข้อมูลส่วนบุคคลเอาไว้เพื่อประโยชน์ในการเข้าถึงข้อมูลของสาธารณชน ดังที่ปรากฏเป็นประเด็นการชั่งน้ำหนักระหว่างสิทธิในความเป็นส่วนตัวและสิทธิในการเข้าถึงข้อมูลในคดี *Hurbain v. Belgium* และคดี *Plaintiff X v. PrimaDanoi* **ประการที่สอง** การจำกัดสิทธิในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลนั้นสามารถถูกจำกัดได้ด้วย “ประโยชน์สาธารณะ” เช่น ความจำเป็นที่จะไม่ลบหรือทำลายข้อมูลส่วนบุคคลที่จำเป็นต่อประโยชน์สาธารณะด้านการสาธารณสุข และ**ประการที่สาม** การจำกัดสิทธิในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลนั้นสามารถถูกจำกัดได้ด้วยความจำเป็นในการใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมายและปฏิบัติตามกฎหมาย

(ค) หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการลบ ทำลายข้อมูลส่วนบุคคล

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 การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมายหรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความในมาตรา 33 วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม”*

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า (1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง หรือ (2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่

และอำนาจตามกฎหมาย[83]

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการลบ ทำลายข้อมูลส่วนบุคคลตามมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นแสดงให้เห็นว่าสิทธิที่จะถูกลืมในระบบกฎหมายไทยนั้นไม่ได้ถูกคุ้มครองเฉพาะกรณีที่เจ้าของข้อมูลส่วนบุคคลเรียกร้องให้มีการลบ ทำลายข้อมูลส่วนบุคคลเท่านั้น ตัวผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายจะต้องลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น นอกเหนือจากการลบ ทำลายจากการร้องขอของเจ้าของข้อมูลส่วนบุคคลอีกด้วย

3.1.2 กรอบในการวิเคราะห์สิทธิที่จะถูกลืมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สิทธิในการร้องขอให้มีการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลโดยเจ้าของข้อมูลส่วนบุคคลมาตรา 33 และหน้าที่ในการลบทำลายข้อมูลส่วนบุคคลตามมาตรา 37 (3) แสดงให้เห็นว่าสิทธิที่จะถูกลืมในมิติของข้อมูลส่วนบุคคลตามแนวคิดและทฤษฎีที่เกี่ยวข้องดังที่กล่าวในบทที่ 2 นั้นได้ถูกรับรองโดยเฉพาะในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย อย่างไรก็ตาม มีประเด็นให้ต้องศึกษาและวิเคราะห์ต่อไปว่ามาตรการทางกฎหมายข้างต้นสอดคล้องกับมาตรฐานการคุ้มครองสิทธิที่จะถูกลืมในระดับสากลหรือไม่ เพื่อประโยชน์ในการศึกษาและวิเคราะห์ดังกล่าว งานวิจัยนี้จึงขอเสนอกรอบในการวิเคราะห์องค์ประกอบของสิทธิที่จะถูกลืมของกฎหมายต่างประเทศในประเด็นดังกล่าวสามารถแสดงได้ตามตารางที่ 3-3 ดังนี้

---

[83] Ibid, มาตรา 77.

ตารางที่ 3-3 : กรอบในการวิเคราะห์องค์ประกอบของสิทธิที่จะถูกลืมของกฎหมายต่างประเทศ		
ประเด็น	**รายละเอียดตามกฎหมายไทย**	**ข้อพิจารณาในการเปรียบเทียบกับกฎหมายต่างประเทศ**
1. ผู้ทรงสิทธิ	เจ้าของข้อมูลส่วนบุคคล	มาตรการทางกฎหมายของต่างประเทศมีรายละเอียดเกี่ยวกับตัวผู้ทรงสิทธิอย่างไร
2. ผู้มีหน้าที่	ผู้ควบคุมข้อมูลส่วนบุคคล	มาตรการทางกฎหมายของต่างประเทศมีรายละเอียดเกี่ยวกับตัวผู้มีหน้าที่อย่างไร
3. ขอบเขตในการดำเนินการ	การลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล	• การดำเนินการในแต่ละกรณีมีลักษณะอย่างไร • การดำเนินการในแต่ละกรณีจะถูกเลือกใช้อย่างไร • บุคคลที่มีหน้าที่นั้นมีแนวทางในการปฏิบัติตนอย่างไร จึงจะถือเป็นการปฏิบัติที่ชอบด้วยกฎหมาย
4. เหตุปฏิเสธ	• เสรีภาพในการแสดงความคิดเห็น • ประโยชน์สาธารณะ • การก่อตั้งสิทธิเรียกร้องตามกฎหมาย	• การชั่งน้ำหนักระหว่างสิทธิในความเป็นส่วนตัวกับเสรีภาพในการแสดงความคิดเห็นจะมีแนวทางอย่างไร • การชั่งน้ำหนักระหว่างสิทธิในความเป็นส่วนตัวกับประโยชน์สาธารณะจะมีแนวทางอย่างไร

3.2 สหภาพยุโรป

ก่อนวันที่ 25 พฤษภาคม ค.ศ. 2018 ซึ่งเป็นวันที่ GDPR จะมีผลใช้บังคับนั้น การคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปเป็นไปตาม Directive 95/46/EC[84] ซึ่งบัญญัติรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลส่วนบุคคล (Right of Access) โดยรวมไปถึงการลบข้อมูล (Erasure) ที่ถูกประมวลผลโดยฝ่าฝืนต่อกฎระเบียบฉบับนี้ หรือเนื่องจากเป็นกรณีที่ข้อมูลมีความไม่สมบูรณ์หรือมีลักษณะคลาดเคลื่อน[85] โดยไม่ได้บัญญัติถึง “สิทธิที่จะถูกลืม” เอาไว้ในตัวบทกฎหมาย หลักการเกี่ยวกับการขอให้มีการลบข้อมูลนั้นได้ถูกพัฒนา[86] และส่งต่อมายังมาตรา 17 ของ GDPR ในฐานะที่เป็น “สิทธิในการลบข้อมูล” และได้บัญญัติสิทธิของเจ้าของข้อมูลส่วนบุคคลนี้สามารถเรียกได้ว่า “สิทธิที่จะถูกลืม (Right to be Forgotten)”[87]

ในชั้นการพิจารณาร่าง GDPR นั้น คณะมนตรียุโรปได้กล่าวถึงเหตุผลที่มีการกล่าวถึง “สิทธิที่จะลูกลืม” ควบคู่ไปกับสิทธิในการลบข้อมูล โดยอธิบายว่าการอ้างอิงถึงสิทธิที่จะถูกลืมนั้น จำเป็นต่อสิทธิในการลบข้อมูลในบริบทของโลกยุคดิจิทัล (Digital Context)[88] เมื่อเจ้าของข้อมูลส่วนบุคคลประสงค์จะถูกลืม หลังจากที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เผยแพร่ข้อมูลส่วนบุคคลต่อสาธารณะ มีหน้าที่ต้องดำเนินการใด ๆ ต้องแจ้งให้ผู้ควบคุม

---

[84] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[85] Ibid, มาตรา 12 (b).

[86] อรรถกร สุขปุณพันธ์ (อ้างแล้ว เชิงอรรถที่ 35), หน้า 14.

[87] มาตรา 17 ของ GDPR บัญญัติโดยใช้ถ้อยคำว่า “ Right to erasure (‘right to be forgotten’)”

[88] Statement of the Council’s reasons : Position (EU) No 6/2016 (2016/c 159/02), para 4.6.

ข้อมูลส่วนบุคคลอื่นทราบถึงความประสงค์ของเจ้าของข้อมูลส่วนบุคคล[89] และระบุให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยุโรป (European Data Protection Board : EDPB) ทำการออกแนวปฏิบัติที่เกี่ยวข้องต่อไป[90]

3.2.1 ตัวบทกฎหมายและแนวปฏิบัติ

3.2.1.1 GDPR

ตามมาตรา 17 ของ GDPR เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับการลบข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคล และกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้อง “ลบ” โดยไม่ชักช้า เมื่อมีเหตุใดเหตุหนึ่งดังต่อไปนี้

(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

---

[89] Ibid.

[90] Ibid.

(d) ข้อมูลส่วนบุคคลถูกประมวลผลโดยมิชอบด้วยกฎหมาย

(e) ข้อมูลส่วนบุคคลต้องถูกลบเพื่อให้เป็นไปตามพันธกรณีตามกฎหมายในกฎหมายของสหภาพหรือรัฐสมาชิกที่มีอำนาจเหนือผู้ควบคุม

(f) ข้อมูลส่วนบุคคลถูกเก็บรวบรวมโดยสัมพันธ์กับการเสนอของสมาคมบริการสารสนเทศตามที่ถูกอ้างถึงในอนุมาตรา 1 ของมาตรา 8[91]

เมื่อผู้ควบคุมทำให้ข้อมูลส่วนบุคคลเป็นสาธารณะและมีพันธกรณีตามอนุมาตรา 1 ของมาตรา 17 แห่ง GDPR ในการลบข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตามขั้นตอนที่เหมาะสม อันรวมถึงมาตรการทางเทคนิคด้วย โดยพิจารณาถึงเทคโนโลยีที่มีอยู่และค่าใช้จ่ายในการนำมาปฏิบัติร่วมด้วยโดยละเอียด เพื่อแจ้งข้อมูลต่อผู้ควบคุมข้อมูลส่วนบุคคลที่ประมวลผลข้อมูลส่วนบุคคลที่ผู้ถูกประมวลผลข้อมูลได้ขอให้ลบการเชื่อมต่อหรือสำเนาหรือการทำซ้ำใด ๆ ของข้อมูลส่วนบุคคลเหล่านั้นโดยผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าว[92]

การบัญญัติให้มีสิทธิในการลบข้อมูล (สิทธิที่จะถูกลืม) ใน GDPR เป็นผลจากปัญหาข้อพิพาทระหว่างเจ้าของข้อมูลส่วนบุคคลที่ประสงค์จะให้มีการลบข้อมูลส่วนบุคคลของตนออกจากระบบการค้นหาข้อมูลออนไลน์ในคดีที่ศาลยุติธรรมสหภาพยุโรป (Court of Justice of the European Union : CJEU) ได้ตัดสินเมื่อวันที่ 13 พฤษภาคม ค.ศ. 2014 (คดี *Google*

---

[91] โปรดดู นคร เสรีรักษ์ ณรงค์ ใจหาญ ประสิทธิ์ ปิวาวัฒนพานิช ศุภเกียรติ ศุภศักดิ์-ศึกษากร และนิชานันท์ นันทศิริศรณ์, *GDPR ฉบับภาษาไทย* (บริษัท พี.เพรส จำกัด, ธันวาคม 2562), หน้า 130.

[92] Ibid, หน้า 131.

Spain v AEPD and Mario Costeja González) ซึ่งศาลมีคำตัดสินว่า เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอผู้ให้บริการโปรแกรมสืบค้นข้อมูล ลบลิงค์ที่เชื่อมต่อไปยังข้อมูลส่วนบุคคลออกจากรายการแสดงผลที่ปรากฏ ตามการค้นหาโดยการใช้ชื่อของเจ้าของข้อมูลส่วนบุคคลได้ซึ่งจะได้กล่าว โดยละเอียดในหัวข้อ 3.2.2 ต่อไป

เพื่อส่งเสริมการบังคับใช้กฎเกณฑ์เกี่ยวกับการคุ้มครองข้อมูล ส่วนบุคคลซึ่งรวมไปถึงการคุ้มครองสิทธิที่จะถูกลืมของเจ้าของข้อมูล ส่วนบุคคลด้วย GDPR กำหนดว่ารัฐสมาชิกควรกำหนด “โทษปรับทางปกครอง (Administrative Fines)” สำหรับการฝ่าฝืน GDPR เพิ่มเติมหรือแทนที่ จากมาตรการเพื่อบังคับใช้กฎหมายอื่น[93] โดยหน่วยงานคุ้มครองข้อมูล ส่วนบุคคลของรัฐสมาชิกควรมีอำนาจกำหนดโทษปรับทางปกครองโดยคำนึงถึง ความมีประสิทธิภาพ ความได้สัดส่วน และให้ผลในเชิงการยับยั้ง (Dissuasive)[94] ซึ่งการกำหนดจำนวนค่าปรับทางปกครองนั้น จะต้องพิจารณาพฤติการณ์ และความร้ายแรงตามข้อเท็จจริงเป็นรายกรณี[95] โดยคำนึงถึงปัจจัย ดังนี้

- สภาพ ความร้ายแรง และระยะเวลาของการกระทำอันเป็น การละเมิดหรือฝ่าฝืนนั้น โดยพิจารณาจากขอบเขตของสภาพ หรือวัตถุประสงค์ของการประมวลผลข้อมูลที่เกี่ยวข้อง รวมไปถึงจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ และระดับความเสียหายที่เจ้าของส่วนบุคคลนั้นได้รับ

---

93 GDPR, Recital (148).

94 Ibid, Article 83 para 1.

95 Article 29 Data Protection Working Party, ‘Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679’ (EU Commission, October 2017) <file :///C :/Users/admin/Downloads/wp253_en_obX4dfnXKom9J QamiJInhjcWvyc_80836.pdf> accessed 15 Novmber 2021, p. 6.

- ลักษณะพฤติการณ์ของการละเมิดที่เกิดจากความจงใจหรือประมาทเลินเล่อ
- การกระทำใด ๆ ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้ดำเนินการเพื่อบรรเทาความเสียหายของเจ้าของข้อมูลส่วนบุคคล
- ระดับของความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล โดยพิจารณาจากมาตรการทางเทคนิคและมาตรการทางองค์กรที่บังคับใช้ภายในผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
- การละเมิดที่เกี่ยวข้องใด ๆ ในครั้งก่อนของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
- ระดับของการให้ความร่วมมือกับหน่วยงานควบคุมดูแลเพื่อการเยียวยาแก้ไขการละเมิดนั้นและบรรเทาผลกระทบอันร้ายแรงที่อาจเกิดขึ้นของการละเมิดนั้น
- ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด
- ในกรณีที่หน่วยงานควบคุมดูแลได้รับรู้ถึงการละเมิดนั้น ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้ดำเนินการแจ้งการละเมิดไปยังหน่วยงานควบคุมดูแลหรือไม่ และหากได้มีการแจ้งการละเมิดไปแล้ว การแจ้งนั้นเป็นการแจ้งที่ครอบคลุมในลักษณะใด
- ในกรณีที่หน่วยงานควบคุมดูแลได้มีคำสั่งตามมาตรการอื่นต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต่อกรณีการละเมิดที่เป็นการละเมิดในลักษณะเดียวกันมาก่อนแล้ว รวมถึงการปฏิบัติตามมาตรการดังกล่าว

- การยึดถือปฏิบัติตามประมวลจริยธรรมที่ได้รับอนุญาตหรือกลไกการรับรองที่ได้รับอนุญาต และ
- ปัจจัยที่มีลักษณะอาจซ้ำเติมความรุนแรงหรือบรรเทาที่สามารถใช้บังคับกับสถานการณ์ของกรณีดังกล่าว เช่น ประโยชน์ทางการเงินที่ได้รับ หรือความสูญเสียที่หลีกเลี่ยงได้ไม่ว่าทางตรงหรือทางอ้อมจากการละเมิดนั้น[96]

นอกจากปัจจัยในการพิจารณาพฤติการณ์และความร้ายแรงของการฝ่าฝืนกฎหมายแล้ว GDPR ยังกำหนดถึงกรอบของอัตราค่าปรับทางปกครองเอาไว้อีกด้วย ในกรณีที่มีการละเมิดหรือฝ่าฝืนบทบัญญัติที่เกี่ยวข้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งรวมถึงการละเมิดบทบัญญัติเกี่ยวกับสิทธิที่จะถูกลืมตามมาตรา 17 นั้น ค่าปรับทางปกครองควรถูกกำหนดเป็นจำนวนไม่เกิน 20 ล้านยูโร หรือร้อยละ 4 ของรายได้รายปีจากการประกอบธุรกิจทั่วโลกของรอบปีบัญชีที่ผ่านมาในกรณีเป็นหน่วยธุรกิจ (Undertaking) (จำนวนใดจำนวนหนึ่งที่มากกว่า)[97] โดยมีข้อสังเกตว่ากรอบอัตราค่าปรับทางปกครองดังกล่าวใช้บังคับกับหน่วยงานของรัฐที่ประมวลผลข้อมูลส่วนบุคคลซึ่งประมวลผลข้อมูลส่วนบุคคลในพื้นที่ของสหภาพยุโรปอีกด้วย[98] เว้นแต่กรณีของหน่วยงานของรัฐที่มีอำนาจหน้าที่ในการป้องกัน สืบสวน ตรวจสอบและดำเนินคดีอาญาหรือบังคับใช้โทษทางอาญา ซึ่งรวมถึงมาตรการคุ้มครองและป้องกันภัยต่อความมั่นคงของรัฐ[99]

นอกเหนือจากการกำหนดค่าปรับทางปกครองแล้ว GDPR แล้วหน่วยงานคุ้มครองข้อมูลส่วนบุคคลของรัฐสมาชิกควรถูกกำหนดให้มีอำนาจ

---

96 Ibid, Article 83 para 2 (a)- (k).

97 Ibid, Article 83 para 5 (b).

98 Ibid, Article 2 และ Article 3.

99 Ibid, Article 2 (d).

ในการออกมาตรการในเชิงการแก้ไข (Corrective Measure) เช่น การให้คำเตือนแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งมีแนวโน้มจะฝ่าฝืนต่อการคุ้มครองสิทธิที่จะถูกลืม[100] ประณามผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ไม่ลบหรือทำลายข้อมูลส่วนบุคคลที่หมดความจำเป็นต้องถูกเก็บรวบรวมหรือประมวลผล[101] หรือสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลทำการลบหรือทำลายข้อมูลส่วนบุคคลที่หมดความจำเป็นต้องถูกเก็บรวบรวมหรือประมวลผลอีกต่อไป[102]

3.2.1.2 แนวปฏิบัติที่เกี่ยวกับประเภทหรือลักษณะของสิทธิที่จะถูกลืมที่อยู่บนโปรแกรมสืบค้นข้อมูล

หลังจากที่ CJEU ได้มีคำวินิจฉัยในคดี *Google Spain v AEPD and Mario Costeja González* เจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกให้ผู้ให้บริการสืบค้นข้อมูลออนไลน์ดำเนินการลบลิงค์ที่เชื่อมต่อไปยังเว็บไซต์จากหน้าแสดงผลการค้นหา ในส่วนของชื่อของเข้าของข้อมูลส่วนบุคคลนั้น เพื่อประโยชน์ในการสร้างแนวปฏิบัติที่เกี่ยวข้อง EDPB จึงได้มีการประกาศแนวปฏิบัติที่เกี่ยวกับประเภทหรือลักษณะของสิทธิที่จะถูกลืมที่อยู่บนโปรแกรมสืบค้นข้อมูล[103] (Guideline 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR : Guideline 5/2019) โดยได้อธิบายสิทธิที่จะถูกลืมในแง่มุม

---

[100] Ibid, Article 58 para 2 (a).

[101] Ibid, Article 58 para 2 (b).

[102] Ibid, Article 58 (c).

[103] Guideline 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (Part 1), para 4.

ของสิทธิในการร้องขอให้นำออกจากโปรแกรมสืบค้นข้อมูลนั้นมิใช่สิ่งเดียวกับการลบข้อมูลส่วนบุคคล[104] โดยระบุว่า กิจกรรมการประมวลผลข้อมูลของโปรแกรมสืบค้นข้อมูลนั้น ควรต้องถูกนิยามให้แตกต่างจากการประมวลผลข้อมูลที่ดำเนินการโดยผู้เผยแพร่ข้อมูลที่เป็นบุคคลภายนอก เช่น สื่อต่าง ๆ (Media Outlets) ที่ให้ข้อมูลข่าวสารออนไลน์[105] เนื่องจากการนำข้อมูลส่วนบุคคลออกจากโปรแกรมสืบค้นข้อมูลนี้เป็นการนำเอาเนื้อหาหรือข้อมูลของเจ้าของข้อมูลส่วนบุคคลนั้น ๆ ออกจากรายการผลแสดงการค้นหาที่เป็นผลการแสดงการค้นหาจากการใช้คำค้นหาด้วยชื่อของเจ้าของข้อมูลส่วนบุคคลเท่านั้น แต่เนื้อหาหรือข้อมูลดังกล่าวยังคงสามารถถูกค้นหาด้วยการใช้คำค้นหาอย่างอื่นที่ไม่ใช่ชื่อของเจ้าของข้อมูลส่วนบุคคล

เมื่อพิจารณาลักษณะทางเทคนิคของการนำข้อมูลออกจากส่วนการแสดงผลข้างต้น จะเห็นได้ว่าการใช้สิทธินำออกจากโปรแกรมสืบค้นข้อมูลนี้จึงไม่ได้เป็นการใช้สิทธิที่สามารถร้องขอให้ข้อมูลส่วนบุคคลนั้นถูกลบออกไปจากระบบอินเทอร์เน็ตโดยสิ้นเชิง ข้อมูลส่วนบุคคลจะยังคงไม่ถูกลบออกจากแหล่งข้อมูลทั้งที่เป็นเว็บไซต์และการแสดงผลและหน่วยความจำขนาดเล็กที่มีความเร็วสูงซึ่งเก็บข้อมูลหรือคำสั่งที่ถูกเรียกใช้หรือเรียกใช้บ่อย ๆ (Cache) ของผู้ให้บริการโปรแกรมสืบค้นข้อมูลแต่เป็นเพียงการนำผลแสดงการค้นหาออกจากการแสดงการค้นหาบนหน้าโปรแกรมสืบค้นข้อมูลเท่านั้น จึงทำให้เนื้อหาอันเป็นข้อมูลส่วนบุคคลนั้นยังคงอยู่ในความควบคุมของเจ้าของเว็บไซต์ และยังคงอาจเข้าถึงได้โดยสาธารณะแม้ว่าข้อมูลส่วนบุคคลนั้นจะไม่ปรากฏบนผลการแสดงการค้นหาอีกต่อไป[106]

---

[104] Ibid, para 6.

[105] Ibid, para 7.

[106] Ibid, para 9.

Guideline 5/2019 อธิบายหลักเกณฑ์อันเกี่ยวข้องกับสิทธินำออกจากโปรแกรมสืบค้นข้อมูลออกเป็นดังนี้ (1) เหตุผลที่เจ้าของข้อมูลส่วนบุคคลอาจใช้เพื่อการส่งคำร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลไปยังเจ้าของโปรแกรมสืบค้นข้อมูลตามมาตรา 17.1 ของ GDPR โดยที่เจ้าของข้อมูลส่วนบุคคลอาจใช้เหตุผล มากกว่าหนึ่งเหตุผลเพื่ออ้างประกอบการใช้สิทธิร้องขอนั้นได้ และ (2) ข้อยกเว้นของการใช้สิทธิขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลตามมาตรา 17.3 ของ GDPR[107]

(1) เหตุผลที่เจ้าของข้อมูลส่วนบุคคลอาจใช้เพื่อการส่งคำร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูล ไปยังเจ้าของโปรแกรมสืบค้นข้อมูลตามมาตรา 17 วรรคหนึ่งของ GDPR[108]

Guideline 5/2019 อธิบายว่ามาตรา 17 ของ GDPR กำหนดถึงหลักการทั่วไปในนำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลออกเป็น 6 กรณี ซึ่งครอบคลุมกรณี (1) ข้อมูลส่วนบุคคลหมดความจำเป็นต่อวัตถุประสงค์ของการเก็บรวบรวม หรือประมวลผลของผู้ให้บริการโปรแกรมสืบค้นข้อมูลต่อข้อมูลส่วนบุคคล (2) เจ้าของข้อมูลถอนความยินยอม (3) เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล (4) ข้อมูลส่วนบุคคลได้ถูกประมวลผลโดยมิชอบด้วยกฎหมาย (5) ข้อมูลส่วนบุคคลต้องถูกลบออกเพื่อการปฏิบัติหน้าที่ตามกฎหมาย และ (6) เมื่อข้อมูลส่วนบุคคลถูกเก็บรวบรวมอันเนื่องมาจากการเสนอของบริการด้านสังคมข่าวสารต่อเด็ก

---

[107] Ibid, para 11.

[108] Ibid, para 13.

กรณีที่ 1 : เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นต่อวัตถุประสงค์ของการเก็บรวบรวม หรือประมวลผลของผู้ให้บริการโปรแกรมสืบค้นข้อมูลต่อข้อมูลส่วนบุคคลนั้น (มาตรา 17 วรรคหนึ่ง (a))[109]

กรณีนี้เป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลนั้นเห็นว่า ข้อมูลส่วนบุคคลของตนที่สามารถเข้าถึงได้นั้นไม่มีความจำเป็นต่อการประมวลผลของผู้ให้บริการโปรแกรมสืบค้นข้อมูลอีกต่อไป และมีความประสงค์ให้ข้อมูลส่วนบุคคลของตนถูกนำออกจากการแสดงผลบนโปรแกรมสืบค้นข้อมูล โดยที่เจ้าของข้อมูลสามารถส่งคำร้องไปยังเจ้าของโปรแกรมสืบค้นข้อมูลได้โดยตรง พร้อมผลการค้นหาที่ปรากฏข้อมูลส่วนบุคคลที่ซึ่งเจ้าของข้อมูลส่วนบุคคลค้นพบโดยการใช้ชื่อของตนเป็นคำค้นหา

Guideline 5/2019 ได้ให้ตัวอย่างของกรณีที่เจ้าของข้อมูลส่วนบุคคลอาจใช้สิทธินำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลไว้ว่าเป็นกรณีที่ข้อมูลส่วนบุคคลที่บริษัทผู้ควบคุมข้อมูลส่วนบุคคลมีไว้อยู่นั้นได้ถูกลบออกจากทะเบียนสาธารณะหรือในกรณีที่ข้อมูลการติดต่อของเจ้าของข้อมูลส่วนบุคคลยังคงปรากฏอยู่บนหน้าเว็บไซต์ของบริษัทแห่งหนึ่ง ทั้งที่ในปัจจุบันเจ้าของข้อมูลไม่ได้ทำงานในบริษัทดังกล่าวอีกต่อไปแล้ว หรืออาจเป็นกรณีที่ข้อมูลบางอย่างนั้นจำต้องถูกทำให้เป็นสาธารณะอันเนื่องมาจากการปฏิบัติหน้าที่ตามกฎหมาย โดยที่ข้อมูลนั้นยังคงปรากฏบนสื่อออนไลน์แม้ระยะเวลาในการประกาศหรือทำข้อมูลให้เป็นสาธารณะตามที่กฎหมายกำหนดไว้นั้นจะได้สิ้นสุดลงแล้วก็ตาม

นอกจากนี้ ในกรณีที่ข้อมูลส่วนบุคคลที่ปรากฏบนสื่อออนไลน์นั้นเป็นข้อมูลที่ผิดหรือไม่ถูกต้องอันเนื่องมาจากระยะเวลา (Course of Time) หรือข้อมูลเหล่านั้นล้าสมัยไม่เป็นปัจจุบัน (Outdated) เจ้าของข้อมูลส่วนบุคคลก็อาจส่งคำร้องไปยังผู้ใช้บริการโปรแกรมสืบค้นข้อมูลเพื่อให้

---

[109] Ibid, para 18 to para 21.

ดำเนินการนำเอาข้อมูลที่ผิดหรือไม่ถูกต้องนั้นออกจากการแสดงผลบนโปรแกรมสืบค้นข้อมูลได้

การใช้สิทธิตามมาตรา 17 วรรคหนึ่ง (a) จะต้องพิจารณาถึงความสมดุลระหว่างการคุ้มครองความเป็นส่วนตัวและประโยชน์ของผู้ใช้อินเทอร์เน็ต เนื่องจากเหตุผลที่สำคัญในการประมวลผลข้อมูลส่วนบุคคลของโปรแกรมสืบค้นข้อมูลนี้ มีลักษณะเป็นไปเพื่อให้ผู้ใช้งานอินเทอร์เน็ตสามารถเข้าถึงข้อมูลได้ง่ายขึ้น ดังนั้น ในการใช้สิทธิดังกล่าวต้องมีการประเมินว่าการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการกระทำเกินเวลาการเก็บตามวัตถุประสงค์ หรือข้อมูลส่วนบุคคลนั้นล้าสมัยไม่เป็นปัจจุบันหรือไม่ได้ถูกทำให้เป็นปัจจุบันหรือไม่ ทั้งนี้ระยะเวลาในการเก็บข้อมูลส่วนบุคคลไว้ย่อมขึ้นอยู่กับวัตถุประสงค์เดิม (Original Purpose) ในการประมวลผลข้อมูลดังกล่าวด้วย

กรณีที่ 2 : เมื่อเจ้าของข้อมูลถอนความยินยอมต่อการประมวลข้อมูลส่วนบุคคลในมาตรา 6 (1) (a)[110] หรือมาตรา 9 (2)[111] และไม่มีฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลอื่น[112]

เมื่อเจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของตนแล้ว เจ้าของข้อมูลส่วนบุคคลย่อมมีสิทธิร้องขอให้มีการลบข้อมูลส่วนบุคคลของตนออกเนื่องจากการประมวลผลข้อมูลส่วนบุคคล

---

[110] มาตรา 6.1 (a) บัญญัติว่า การประมวลผลจะชอบด้วยกฎหมายก็ต่อเมื่ออยู่ในขอบเขตของข้อใดข้อหนึ่งต่อไปนี้ (a) ผู้ถูกประมวลผลข้อมูลได้ยินยอมให้ประมวลผลข้อมูลส่วนบุคคลของตนเพื่อวัตถุประสงค์เฉพาะอย่างหนึ่งหรือมากกว่า.

[111] มาตรา 9.2 (a) บัญญัติว่า ผู้ถูกประมวลผลได้ให้ความยินยอมอย่างชัดเจนถึงการประมวลผลข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์โดยเฉพาะอย่างใดอย่างหนึ่งหรือมากกว่า เว้นแต่ว่าเมื่อกฎหมายของสหภาพหรือรัฐสมาชิกได้กำหนดการห้ามตามที่อ้างไว้ในอนุมาตรา 1 จะไม่สามารถถูกยกเว้นได้โดยผู้ถูกประมวลผลข้อมูล.

[112] 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.

ในกรณีนี้ตั้งอยู่บนฐานของความยินยอม โดยมีข้อสังเกตว่า การให้ความยินยอมในกรณีนี้จะต้องทำ “โดยการเฉพาะ” และต้องเกี่ยวข้องกับการประมวลผลข้อมูลที่จำต้องเป็นไปตามการทำงานของโปรแกรมสืบค้นข้อมูลเท่านั้น ในทางปฏิบัตินั้น เป็นไปได้ว่าผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะทำการขอรับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนที่จะทำการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการทำการอ้างอิง (Referencing Activity) ดังนั้น ไม่ว่ากรณีจะเป็นอย่างไรก็ตามหากเมื่อเจ้าของข้อมูลส่วนบุคคลทำการร้องขอให้ยุติการทำการอ้างถึงนั้น (De-Referencing) ย่อมเท่ากับว่าเจ้าของข้อมูลส่วนบุคคลรายดังกล่าวนั้นไม่ประสงค์หรือยินยอมให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูลทำการประมวลผลข้อมูลส่วนบุคคลของตนอีกต่อไป

หากเจ้าของข้อมูลส่วนบุคคลทำการถอนความยินยอมการใช้ข้อมูลส่วนบุคคลโดยแสดงเจตนาไปยังเว็บไซต์โดยเฉพาะ เจ้าของเว็บไซต์นั้นควรแจ้งไปยังผู้ให้บริการโปรแกรมสืบค้นข้อมูลที่ทำการแสดงผล (Index) ข้อมูลของเจ้าของข้อมูลส่วนบุคคลคนดังกล่าวอยู่ด้วยตามมาตรา 17 วรรคสอง

กรณีที่ 3 : เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตน

(มาตรา 17 วรรคหนึ่ง (c))[113]

มาตรา 17 วรรคหนึ่ง (c) ของ GDPR กำหนดให้เจ้าของข้อมูลส่วนบุคคลอาจร้องขอให้ทำการลบข้อมูลส่วนบุคคลของตนหลังจากที่ได้ทำการคัดค้านการประมวลผลข้อมูลส่วนบุคคลนั้นตามมาตรา 21.1 แล้วได้ อย่างไรก็ตาม การใช้สิทธิดังกล่าวนี้จำต้องเป็นกรณีที่ว่าไม่มีเหตุผลอันชอบธรรม

[113] Ibid, para 26 to para 33.

(Legitimate Ground) อื่นใดที่อาจแทนที่ได้ โดย GDPR ได้กำหนดภาระการพิสูจน์ที่เอื้อต่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลโดยที่ถือเป็นหน้าที่ของผู้ให้บริการโปรแกรมสืบค้นข้อมูลที่มีภาระการพิสูจน์และจำต้องแสดงให้เห็นถึงเหตุผลอันชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลที่ไม่อาจปฏิเสธได้นั้นว่ามีอยู่จริง จึงจะทำให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูลสามารถปฏิเสธการใช้สิทธิลบข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลร้องขอได้ ทั้งนี้ เหตุผลอันชอบธรรมเช่นว่านั้นจำต้องเป็นเหตุผลอันชอบธรรมที่เหนือกว่า โดยมีลักษณะที่เหนือกว่าประโยชน์รวมถึงสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลเท่านั้น แต่หากผู้ให้บริการโปรแกรมสืบค้นข้อมูลไม่อาจแสดงให้เห็นถึงเหตุผลอันชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลที่ไม่อาจปฏิเสธได้ เจ้าของข้อมูลส่วนบุคคลก็ชอบที่จะใช้สิทธิร้องขอให้นำข้อมูลเหล่านั้นออกตาม มาตรา 17 วรรคหนึ่ง (c)

จะเห็นได้ว่าการร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลนั้นตั้งอยู่บนพื้นฐานของความสมดุลระหว่างสถานการณ์พิเศษของเจ้าของข้อมูลส่วนบุคคล และเหตุผลอันชอบธรรมที่ไม่อาจปฏิเสธได้ของผู้ให้บริการ โปรแกรมสืบค้นข้อมูล โดยแนวปฏิบัติได้อธิบายและยกตัวอย่างของสถานการณ์พิเศษของเจ้าของข้อมูลส่วนบุคคลที่ปรากฏในลักษณะเป็นผลแสดงการค้นหาที่สร้างความเสื่อมเสีย หรือทำลายชื่อเสียงของเจ้าของข้อมูลส่วนบุคคลในกรณี ดังต่อไปนี้[114]

- เจ้าของข้อมูลส่วนบุคคลมิได้มีบทบาทในชีวิตสาธารณะ
- ข้อมูลพิพาทดังกล่าวมิได้เกี่ยวข้องกับชีวิตการทำงานของเจ้าของข้อมูลส่วนบุคคล แต่กลับกระทบต่อความเป็นส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

[114] Ibid, para 32.

- ข้อมูลนั้นก่อให้เกิดประทุษวาจา (Hate Speech) การหมิ่นประมาท การพูดให้ร้าย หรือการกระทำความผิดที่เกี่ยวกับการแสดงออกอันเป็นปรปักษ์ต่อเจ้าของข้อมูลอันเนื่องมาจากคำสั่งของศาล
- ข้อมูลเป็นข้อมูลที่ได้รับการยืนยันข้อเท็จจริงแต่กลับพบว่ามีข้อมูลบางส่วนที่ไม่ถูกต้อง
- ข้อมูลที่เกี่ยวกับการกระทำความผิดอาญาของผู้เยาว์ที่เกิดขึ้นในอดีตและก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล

ทั้งนี้ การใช้สิทธิตามกรณีดังกล่าวนี้พึงต้องพิจารณาถึงสิทธิส่วนบุคคลและสิทธิในข้อมูลข่าวสารควบคู่กันไปด้วย

กรณีที่ 4 : เมื่อข้อมูลส่วนบุคคลได้ถูกประมวลผลโดยมิชอบด้วยกฎหมาย (มาตรา 17 วรรคหนึ่ง (d))[115]

การประมวลโดยมิชอบด้วยกฎหมายอาจตีความได้จากมาตรา 6 ของ GDPR ที่กำหนดลักษณะของการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมายไว้ทั้งหมด 6 กรณี อย่างไรก็ตาม การประมวลผลที่ไม่ชอบด้วยกฎหมายอาจให้เป็นหน้าที่ของเจ้าหน้าที่ควบคุมดูแล (Supervisory Authority) ของแต่ละรัฐสมาชิกในการกำหนดและตีความขอบเขตของการประมวลผลที่ไม่ชอบด้วยกฎหมาย โดยการตีความว่าอย่างไรจึงจะเป็นการประมวลผลที่มิชอบด้วยกฎหมายอาจพิจารณาได้จากหลักเกณฑ์อื่นใน Chapter 2 ของ GDPR ได้เช่นเดียวกัน

การใช้สิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลได้ตามกรณีนี้ เป็นกรณีที่ผู้ให้บริการโปรแกรมสืบค้นข้อมูลไม่อาจแสดงให้เห็นได้ว่า

---

[115] Ibid, para 34 to para 36.

การประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลเป็นไปตามการประมวลผลที่ชอบด้วยกฎหมาย ทั้งนี้ ยังต้องพิจารณาต่อไปด้วยว่าการประมวลผลข้อมูลส่วนบุคคลดั้งเดิมนั้น มิได้เป็นการประมวลผลข้อมูลส่วนบุคคลที่มิชอบด้วยกฎหมายอีกด้วย หากปรากฏว่าการประมวลผลข้อมูลส่วนบุคคลดั้งเดิมมีลักษณะที่ไม่เข้าข่ายตามมาตรา 6 ของ GDPR ผู้ให้บริการโปรแกรมสืบค้นข้อมูลก็ไม่อาจอ้างเหตุแห่งการปฏิเสธการใช้สิทธิร้องขอให้นำออกของเจ้าของข้อมูลส่วนบุคคลได้ และเจ้าของข้อมูลส่วนบุคคลย่อมมีสิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลได้

กรณีที่ 5 : เมื่อข้อมูลส่วนบุคคลต้องถูกลบออกเพื่อการปฏิบัติหน้าที่ตามกฎหมาย

(มาตรา 17 วรรคหนึ่ง (e))[116]

สิทธิในการนำออกจากโปรแกรมสืบค้นข้อมูลตามมาตรา 17 วรรคหนึ่ง (e) ของ GDPR รวมถึงกรณีเป็นหน้าที่ตามกฎหมายที่อนุญาตให้เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ทำการลบผลแสดงการค้นหาข้อมูลส่วนบุคคลของตน เนื่องจากเป็นการปฏิบัติหน้าที่ให้เป็นไปตามกฎหมาย โดยอาจเป็นกรณีที่ผู้ให้บริการสืบค้นออนไลน์นั้นมีหน้าที่ต้องปฏิบัติตามกฎหมายอันเป็นผลมาจากคำสั่งที่ออกโดยกฎหมายของรัฐหรือของสหภาพยุโรป ซึ่งอาจเรียกได้ว่าเป็นหน้าที่ตามกฎหมายที่ต้องลบตามกฎหมาย หรืออาจเป็นกรณีที่ผู้ให้บริการโปรแกรมสืบค้นข้อมูลได้ฝ่าฝืนระยะเวลาในการเก็บรักษาข้อมูล

อย่างไรก็ตาม สำหรับระยะเวลาในการเก็บรักษาข้อมูลที่ Guideline 5/2019 ได้ให้ตัวอย่างไว้นั้น อาจเป็นกรณีที่มีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลไว้เป็นลายลักษณ์อักษร แต่มีการละเมิดหรือไม่ปฏิบัติตามระยะเวลาดังกล่าว ซึ่งกรณีตัวอย่างดังกล่าวนี้มีลักษณะที่เกี่ยวข้องกับไฟล์สาธารณะ

---

[116] Ibid, para 37 to para 38.

มากกว่า โดยที่อาจครอบคลุมไปถึงกรณีที่เกี่ยวข้องกับข้อมูลที่ไม่ได้ทำให้เป็นนิรนามหรือข้อมูลที่ระบุตัวตนที่มีสภาพพร้อมใช้งานบนข้อมูลเปิด (Open Data)[117]

กรณีที่ 6 : เมื่อข้อมูลส่วนบุคคลถูกเก็บรวบรวมอันเนื่องมาจากการเสนอของบริการด้านสังคมข่าวสารต่อเด็ก ตามที่ถูกอ้างถึงใน มาตรา 8 (1) (มาตรา 17 วรรคหนึ่ง (f))[118]

Guideline 5/2019 ได้อ้างอิงนิยามของคำว่า “บริการด้านสังคมข่าวสาร” มาจาก Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 ที่ได้กำหนดนิยามของบริการด้านสังคมข่าวสารเอาไว้ว่า เป็นการให้บริการใด ๆ ที่โดยปกติแล้วมุ่งให้มีการตอบแทนเพื่อการให้บริการตามที่ได้รับการร้องขอระหว่างบุคคลซึ่งอยู่ห่างกันโดยระยะทาง[119] กรณีนี้จึงมีความเป็นไปได้ว่าลักษณะของกิจกรรมของผู้ให้บริการโปรแกรมสืบค้นข้อมูลตกอยู่ในบังคับของมาตรา 17 วรรคหนึ่ง (f) ของ GDPR

แม้ผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะไม่ได้ให้ความสนใจว่าข้อมูลส่วนบุคคลที่แสดงผลนั้นเป็นข้อมูลส่วนบุคคลของเด็กหรือไม่ แต่ก็เป็นหน้าที่รับผิดชอบโดยเฉพาะและผู้ให้บริการโปรแกรมสืบค้นข้อมูลต้องนำข้อมูลที่เกี่ยวกับเด็กออกจากระบบการสืบค้น เมื่อเจ้าของข้อมูลส่วนบุคคลหรือผู้มีอำนาจใช้สิทธิคัดค้านการประมวลผลข้อมูลทำการคัดค้านการประมวลผลข้อมูลส่วนบุคคล และร้องขอให้นำข้อมูลออกตามมาตรา 17 วรรคหนึ่ง (c) กรณีดังกล่าวจึงเป็นการยอมรับว่าสถานะของการเป็นเด็กนั้นถือเป็นเหตุผลที่เป็นสถานการณ์พิเศษของเจ้าของข้อมูลส่วนบุคคลได้ ตามมาตรา 21

---

[117] Ibid, para 38.

[118] Ibid, para 39 to para 41.

[119] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015, Article 1 para 1.

ของ GDPR และยังเป็นการคุ้มครองสิทธิประโยชน์ของเด็กที่เกี่ยวกับข้อมูลส่วนบุคคลของเด็ก ตามมาตรา 38 ของ GDPR อีกด้วย เช่นนี้ จึงต้องพิจารณาถึงการประมวลผลข้อมูลส่วนบุคคลของเด็กแต่เดิมของผู้ควบคุมข้อมูลส่วนบุคคล ประกอบกับระยะเวลาเริ่มต้นของการประมวลผลข้อมูลส่วนบุคคลโดยเว็บไซต์เดิมเมื่อเจ้าของข้อมูลทำการร้องขอให้นำข้อมูลออกอีกด้วย

แนวการปฏิบัติเกี่ยวกับการนำข้อมูลส่วนบุคคลออกจากโปรแกรมสืบค้นข้อมูลทั้ง 6 กรณีตามที่ปรากฏใน Guideline 5/2019 นั้นแสดงให้เห็นว่าผู้ให้บริการโปรแกรมสืบค้นข้อมูลนั้น เป็นผู้มีบทบาทสำคัญในการดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเพื่อการคุ้มครองสิทธิที่จะถูกลืมตามมาตรา 17 ของ GDPR เนื่องจากผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะต้องพิจารณาว่าจะดำเนินการลบหรือทำลายข้อมูลตามคำร้องหรือไม่ กรณีที่ 1 นั้นผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะต้องพิจารณาถึงความจำเป็นต่อวัตถุประสงค์ของการเก็บรวบรวม หรือประมวลผลของผู้ให้บริการโปรแกรมสืบค้นข้อมูลต่อข้อมูลส่วนบุคคลนั้นซึ่งจะต้องพิจารณาความจำเป็นเป็นรายกรณีและรับผิดชอบการชั่งน้ำหนักความสมดุลระหว่างการคุ้มครองความเป็นส่วนตัวและประโยชน์ของผู้ใช้อินเทอร์เน็ต

ส่วนกรณีที่ 2 นั้นแสดงให้เห็นว่าผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะต้องพิจารณาถึงรูปแบบและลักษณะของการ “ถอนความยินยอม” ของเจ้าของข้อมูลส่วนบุคคลซึ่งรวมไปถึงการร้องขอให้ยุติการทำการอ้างถึงนั้น (De-Referencing) ด้วย นอกจากนี้ ผู้ให้บริการโปรแกรมสืบค้นข้อมูลยังมีหน้าที่ที่จะต้องประสานงานกับเว็บไซต์ซึ่งรับการแสดงเจตนาถอนความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอีกด้วย

ผู้ให้บริการโปรแกรมสืบค้นข้อมูลมีภาระหน้าที่ในการพิสูจน์ว่าตนมีเหตุผลอันชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลที่ไม่อาจปฏิเสธ (Compelling Legitimate Ground) หากเจ้าของข้อมูลส่วนบุคคล

ใช้สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตน หรือแสดงให้เห็นได้ว่าการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลเป็นไปตามการประมวลผลที่ชอบด้วยกฎหมายในกรณีที่จะต้องมีการลบข้อมูลเนื่องจากเป็นการประมวลผลข้อมูลส่วนบุคคลที่ไม่ชอบด้วยกฎหมาย

นอกจากนี้ ผู้ให้บริการโปรแกรมสืบค้นข้อมูลยังต้องตรวจสอบหน้าที่ของตนในการลบข้อมูลส่วนบุคคลตามกฎหมายซึ่งอาจเกิดขึ้นในกรณีที่ได้รับคำสั่งโดยชอบด้วยกฎหมาย การสิ้นระยะเวลาการเก็บข้อมูลส่วนบุคคล หรือหน้าที่ในนำข้อมูลที่เกี่ยวกับเด็กออกจากระบบการสืบค้นซึ่งปรากฏตามกรณีที่ 5 และกรณีที่ 6 ของ Guideline 5/2019 **จากกรณีทั้ง 6 นี้ สามารถสรุปได้ว่าการคุ้มครองสิทธิที่จะถูกลืมในกรณีที่ข้อมูลส่วนบุคคลถูกแสดงผ่านระบบการสืบค้นออนไลน์ในทางปฏิบัตินั้น มีความจำเป็นที่ผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์ (ตลอดจนผู้ให้บริการเว็บไซต์) นั้น จะต้องเข้าใจถึงบทบาทและหน้าที่ของตนอย่างชัดเจน**

(2) ข้อยกเว้นของการใช้สิทธิขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูล

สิทธิในการนำออกจากโปรแกรมสืบค้นข้อมูลนั้น มิใช่สิทธิเด็ดขาด เนื่องจากมาตรา 17 วรรคสามของ GDPR ได้กำหนดถึงหลักเกณฑ์ซึ่งถือเป็นข้อยกเว้นของการใช้สิทธิดังกล่าว ซึ่งทำให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูลอาจใช้เป็นเหตุแห่งการปฏิเสธไม่ปฏิบัติคำร้องขอดังกล่าวของเจ้าของข้อมูลส่วนบุคคลได้ เมื่อผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์เป็นผู้มีบทบาทสำคัญในการคุ้มครองสิทธิที่จะถูกลืม ผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์จึงมีความจำเป็นจะต้องสามารถพิจารณาว่าการลบ ทำลายตามคำขอนั้นถูกปฏิเสธได้หรือไม่ และมีปัจจัยใดบ้างที่จะต้องนำมาพิจารณาประกอบ ซึ่งตาม Guideline 5/2019 มีกรณีพิจารณาได้แก่ (1) ความจำเป็นต่อ

การใช้สิทธิในการแสดงออกและเข้าถึงข้อมูลข่าวสาร (2) การปฏิบัติหน้าที่ตามกฎหมายที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตาม และ (3) ความจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ

กรณีที่ 1 : การประมวลผลข้อมูลส่วนบุคคลจำเป็นต่อการใช้สิทธิในการแสดงออกและเข้าถึงข้อมูลข่าวสาร[120]

สิทธิของเจ้าของข้อมูลส่วนบุคคลในการขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูล จะมิใช่สิทธิเด็ดขาดและตั้งอยู่บนพื้นฐานของการชั่งน้ำหนักระหว่างการปกป้องคุ้มครองสิทธิของภาคส่วนที่เกี่ยวข้องและเสรีภาพในการแสดงออกด้วย ในการชั่งน้ำหนักระหว่างสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลและประโยชน์ของผู้ใช้งานอินเทอร์เน็ตในการเข้าถึงข้อมูลผ่านผู้ให้บริการโปรแกรมสืบค้นข้อมูลนั้น จะต้องพิจารณาเป็นรายกรณี เช่น การชั่งน้ำหนักดังกล่าวจะต้องพิจารณาถึงลักษณะความเป็นบุคคลสาธารณะของเจ้าของข้อมูลส่วนบุคคลด้วย

Guideline 5/2019 ได้ให้ข้อสังเกตเอาไว้ว่า ผู้ให้บริการสืบค้นข้อมูลออนไลน์อาจปฏิเสธไม่ลบข้อมูลส่วนบุคคลของการแสดงผลในกรณีที่ผู้ให้บริการสืบค้นข้อมูลออนไลน์สามารถแสดงได้ว่าการยังคงแสดงผลข้อมูลส่วนบุคคลต่อไปนั้น มีความจำเป็นอย่างยิ่งสำหรับการคุ้มครองสิทธิในการเข้าถึงข้อมูลของผู้ใช้อินเทอร์เน็ต[121] อย่างไรก็ตาม ในทางปฏิบัตินั้นการชั่งน้ำหนักดังกล่าวนั้นมีปัจจัยที่เกี่ยวข้องหลายประการและขึ้นอยู่กับข้อเท็จจริงในแต่ละกรณีโดยสามารถแสดงได้ตามตารางที่ 3-4 ดังนี้

---

[120] Guideline 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (Part 1), para 44 to para 54.

[121] Ibid, para 54.

ตารางที่ 3-4 : ปัจจัยในการชั่งน้ำหนักระหว่างสิทธิในความเป็นส่วนตัวและสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอินเทอร์เน็ต[122]	
ปัจจัย	**ข้อพิจารณา**
ลักษณะของข้อมูล	• ความอ่อนไหวของข้อมูล (Sensitivity) • โดยเฉพาะอย่างยิ่งเมื่อข้อมูลนั้นถูกเข้าถึงได้โดยผู้ใช้งานอินเทอร์เน็ต เช่น ประโยชน์ที่บุคคลที่จะเข้ามาทำธุรกรรมกับตัวเจ้าของข้อมูลจะสามารถตรวจสอบสถานะของตัวเจ้าของข้อมูลส่วนบุคคลได้[123]
ผลประโยชน์	• ประโยชน์ที่ผู้ใช้งานอินเทอร์เน็ตจะได้รับ • โดยจะต้องคำนึงถึงบทบาททั้งของตัวผู้เข้าถึงข้อมูล เช่น การเป็นสื่อมวลชนและตัวเจ้าของข้อมูลส่วนบุคคล เช่น ความเป็นบุคคลสาธารณะของตัวเจ้าของข้อมูลส่วนบุคคล

เมื่อนำปัจจัยดังที่ได้แสดงในตารางที่ 3-4 มาปรับใช้สามารถยกตัวอย่างเกี่ยวกับการต้องดำเนินการลบการแสดงผลและการปฏิเสธการแสดงผลได้ ดังนี้ หากผู้ให้บริการสืบค้นข้อมูลออนไลน์ได้รับคำขอให้ลบการแสดงผลจากเจ้าของข้อมูลส่วนบุคคล แต่ไม่อาจพิสูจน์หรือแสดงให้เห็นว่าการไม่ลบการแสดงผลหรือกล่าวอีกนัยหนึ่ง คือ การให้ผู้ใช้งานอินเทอร์เน็ตอื่น

[122] Ibid, para 48.

[123] โปรดดู คดี *Camera di Commercio di Lecce* v. Manni (ซึ่งจะได้อธิบายรายละเอียดในหัวข้อ 3.2.2.3).

สามารถเข้าถึงการแสดงผลได้จะเป็นประโยชน์ต่อการคุ้มครองสิทธิในการเข้าถึงข้อมูลอันเป็นฐานของการใช้เสรีภาพในการแสดงความคิดเห็น อย่างไร กรณีนี้ผู้ให้บริการสืบค้นข้อมูลออนไลน์ย่อมไม่อาจใช้ข้อยกเว้นไม่ลบการแสดงผลตามมาตรา 17 วรรคสามของ GDPR ได้ แต่หากเป็นกรณีที่ผู้ให้บริการสืบค้นข้อมูลออนไลน์สามารถแสดงได้ว่าการแสดงผลนั้นเป็นประโยชน์ต่อการเข้าถึงข้อมูลของผู้ใช้งานอินเทอร์เน็ตอื่นตามบทบาทของผู้เข้าถึง กรณีนี้ผู้ให้บริการสืบค้นข้อมูลออนไลน์ก็อาจปฏิเสธไม่ลบการแสดงผลได้

กรณีที่ 2 : การประมวลผลข้อมูลส่วนบุคคลจำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมายที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตาม[124]

Guideline 5/2019 ระบุว่า มีความเป็นไปได้น้อยว่ากฎหมายแห่งรัฐสมาชิกจะกำหนดให้แก่ผู้ให้บริการโปรแกรมสืบค้นข้อมูลมีหน้าที่ทางกฎหมายในการเป็นผู้เผยแพร่ข้อมูลบางประเภท สาเหตุเนื่องจากโดยสภาพกิจกรรมของผู้ให้บริการโปรแกรมสืบค้นข้อมูล ไม่อาจเอื้ออำนวยต่อการจำแนกประเภทของข้อมูลว่าข้อมูลจำพวกใดที่ผู้ให้บริการโปรแกรมสืบค้นข้อมูล อาจประกาศได้หรือข้อมูลจำพวกใดที่ไม่อาจประกาศได้ เนื่องจากผู้ให้บริการโปรแกรมสืบค้นข้อมูล ไม่ใช่ผู้ที่ทำหน้าที่ผลิตข้อมูล ทำให้มีความเป็นไปได้ว่ากฎหมายแห่งรัฐสมาชิกอาจทำการกำหนดให้เจ้าของเว็บเพจมีหน้าที่ทางกฎหมายในการเผยแพร่ข้อมูลมากกว่า

อย่างไรก็ตาม ก็ยังอาจมีความเป็นไปได้ว่ากฎหมายสหภาพยุโรปหรือกฎหมายแห่งรัฐสมาชิกอาจทำการอนุญาตให้เจ้าหน้าที่รัฐมีอำนาจในการตัดสินใจว่าจะกำหนดให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูลสามารถ

---

[124] Ibid, para 55 to para 65.

ประกาศข้อมูลเองได้โดยตรงโดยไม่ต้องกระทำผ่าน URL ที่เชื่อมโยงไปยังเว็บเพจต่าง ๆ ที่มีข้อมูลส่วนบุคคลอยู่ จึงเท่ากับว่าผู้ให้บริการโปรแกรมสืบค้นข้อมูลถูกกำหนดให้เป็นผู้ที่มีหน้าที่ตามกฎหมาย ที่จำต้องปฏิบัติตามเช่นนี้ ผู้ให้บริการโปรแกรมสืบค้นข้อมูลก็อาจยกเอาข้ออ้างดังกล่าวมาใช้เป็นข้อยกเว้นในการดำเนินการตามการร้องขอใช้สิทธิร้อง ขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลของเจ้าของข้อมูลส่วนบุคคลได้

สิ่งที่พึงพิจารณาในการบังคับใช้ข้อยกเว้นนี้อีกประการหนึ่งคือ การเก็บรักษาข้อมูลส่วนบุคคลนั้นจำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมายในการประกาศหรือไม่ หากว่าในการประกาศเผยแพร่ข้อมูลส่วนบุคคลดังกล่าวมีคำสั่งจากเจ้าหน้าที่กำหนดระยะเวลาในการประกาศ หรือมีการระบุไว้โดยชัดแจ้งว่าประกาศนี้จะบรรลุวัตถุประสงค์ได้ก็ต่อเมื่อได้สิ้นสุดระยะเวลาใดเวลาหนึ่งแล้ว เช่นนี้การใช้สิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลของเจ้าของข้อมูลส่วนบุคคลจึงไม่อาจเกิดขึ้นในระหว่างที่ระยะเวลาดังกล่าวยังไม่สิ้นสุดกำหนดการ ด้วยเหตุเพราะการประกาศนั้นยังเป็นการประกาศที่ดำเนินการภายในระยะเวลาที่ชอบด้วยกฎหมายอยู่นั้นเอง และในทางกลับกันผู้ให้บริการโปรแกรมสืบค้นข้อมูล ก็ไม่อาจอ้างข้อยกเว้นดังกล่าวนี้เพื่อใช้ปฏิเสธไม่ดำเนินการตามการร้องขอใช้สิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลของเจ้าของข้อมูลส่วนบุคคลได้เช่นเดียวกัน หากปรากฏว่าระยะเวลาดังกล่าวได้สิ้นสุดลงแล้ว

อย่างไรก็ตาม มีบางกรณีที่กฎหมายแห่งรัฐสมาชิกได้กำหนดให้เว็บเพจเป็นผู้มีหน้าที่ตามกฎหมายในการเผยแพร่ข้อมูลส่วนบุคคลแทนที่จะเป็นผู้ให้บริการโปรแกรมสืบค้นข้อมูล กรณีดังกล่าวนี้จึงเท่ากับว่าผู้มีหน้าที่ต้องปฏิบัติตามกฎหมาย คือ เว็บเพจนั้น ๆ ที่มีข้อมูลส่วนบุคคลปรากฏอยู่ ทำให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูล ไม่อาจใช้ข้อยกเว้นดังกล่าวนี้ปฏิเสธไม่ยอมดำเนินการตามการร้องขอใช้สิทธิในการลบข้อมูลออกจากผลการค้นหา

ของเจ้าของข้อมูลส่วนบุคคลได้เนื่องจากมิได้เป็นผู้ที่กฎหมายกำหนดให้เป็นผู้มีหน้าที่นั้น ทั้งนี้ การที่กฎหมายกำหนดให้เป็นหน้าที่ของเว็บไซต์ผู้เผยแพร่ข้อมูลที่ต้องปฏิบัติตามกฎหมายนั้น จำต้องมีการคำนึงถึงความสมดุลระหว่างสิทธิของเจ้าของข้อมูลส่วนบุคคล และประโยชน์ของผู้ใช้งานอินเทอร์เน็ตในการเข้าถึงข้อมูลเสมอ

อย่างไรก็ตาม พึงสังเกตว่าการที่กฎหมายหรือเจ้าหน้าที่อนุญาตให้มีการประกาศข้อมูลส่วนบุคคลลงบนระบบออนไลน์ ถือเป็นเครื่องบ่งบอกและแสดงถึงประโยชน์ของสาธารณะในการที่จะสามารถเข้าถึงข้อมูลเหล่านั้น แต่ทั้งนี้การจะพิจารณาชั่งน้ำหนักถึงประโยชน์ของสาธารณะนั้น อาจไม่สามารถนำเอามาพิจารณาได้ในกรณีที่กฎหมายกำหนดให้เป็นหน้าที่ของเจ้าของเว็บเพจ

แม้การที่กฎหมายกำหนดให้เป็นหน้าที่ของเจ้าของเว็บเพจในการเผยแพร่ข้อมูลอาจสรุปได้ว่าข้อมูลข่าวสารดังกล่าวไม่ควรต้องถูกลบออกจากเว็บเพจนั้น แต่กรณีของผลแสดงการค้นหาของผู้ให้บริการโปรแกรมสืบค้นข้อมูลนั้นแตกต่างจากกรณีของเจ้าของเว็บเพจ เนื่องจากมีการใช้ชื่อของเจ้าของข้อมูลส่วนบุคคลเพื่อให้สามารถค้นพบและแสดงผลการค้นหาที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลนั้น ๆ ได้

ดังนั้น ในการประเมินคำร้องขอใช้สิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลในกรณีดังกล่าวนี้ จึงไม่ควรตีความไปว่าหน้าที่ในการประกาศเผยแพร่ซึ่งเป็นหน้าที่ในการปฏิบัติให้เป็นไปตามกฎหมายนั้นเป็นหน้าที่ทางกฎหมายที่มีผลบังคับเฉพาะแก่เจ้าของเว็บเพจเท่านั้น จึงทำให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูลไม่อาจทำการยอมรับคำร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลได้ เนื่องจากมิได้เป็นผู้มีหน้าที่ตามกฎหมาย และในขณะเดียวกันผู้ให้บริการโปรแกรมสืบค้นข้อมูล ก็ไม่อาจอ้างการมีอยู่

ของหน้าที่ตามกฎหมายนั้นเพื่อปฏิเสธคำร้อง ขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลดังกล่าวจากเจ้าของข้อมูลส่วนบุคคล จึงจำต้องมีการตัดสินให้เป็นหลักการโดยทั่วไปโดยการชั่งน้ำหนักระหว่างสิทธิของเจ้าของข้อมูลส่วนบุคคลและประโยชน์ของผู้ใช้งานอินเทอร์เน็ตในการเข้าถึงข้อมูลดังกล่าวผ่านผู้ให้บริการโปรแกรมสืบค้นข้อมูล

กรณีที่ 3 : การประมวลผลข้อมูลส่วนบุคคลจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ[125]

ผู้ให้บริการโปรแกรมสืบค้นข้อมูลที่ไม่มีฐานะเป็นเจ้าหน้าที่ของรัฐย่อมไม่อาจใช้อำนาจของรัฐเองได้โดยตรง อย่างไรก็ตาม ในบางกรณีผู้ให้บริการโปรแกรมสืบค้นข้อมูลอาจเป็นผู้ใช้อำนาจที่รัฐมอบให้เพื่อปฏิบัติภารกิจที่จำเป็นเพื่อประโยชน์สาธารณะหากมีกฎหมายแห่งรัฐสมาชิกบัญญัติมอบอำนาจของรัฐไว้ให้ ซึ่งอาจปรากฏในกรณีที่รัฐสมาชิกกำหนดหน้าที่ทางกฎหมายการประมวลผลข้อมูลข่าวสารต่อผู้ให้บริการโปรแกรมสืบค้นข้อมูล[126]

การที่ผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะใช้ข้อยกเว้นในข้อนี้กล่าวอ้างปฏิเสธการร้องขอใช้สิทธิในการลบข้อมูลออกจากผลการค้นหาได้นั้นต้องปรากฏว่าการเก็บรักษาข้อมูลส่วนบุคคลของผู้ให้บริการโปรแกรมสืบค้นข้อมูลนั้นมีความจำเป็นต่อการบรรลุวัตถุประสงค์ของประโยชน์สาธารณะ[127] ทั้งนี้ ผู้ให้บริการโปรแกรมสืบค้นข้อมูลยังต้องสามารถระบุถึงสาเหตุที่ผู้ให้บริการโปรแกรมสืบค้นข้อมูลพิจารณากิจกรรมการทำงานของตนว่ามีลักษณะเป็นการดำเนินการเพื่อประโยชน์สาธารณะอย่างแท้จริง หากไม่อาจ

---

[125] Ibid, para 66 to para 72.

[126] Ibid, para 67 to para 68.

[127] Ibid, para 69.

แสดงเหตุผลดังกล่าวได้แล้ว ผู้ให้บริการโปรแกรมสืบค้นข้อมูลก็ไม่อาจใช้ข้อยกเว้นตามข้อนี้ในการปฏิเสธการร้องขอใช้สิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลจากเจ้าของข้อมูลส่วนบุคคลได้

ทั้งนี้ “อำนาจ” หรือ “ประโยชน์สาธารณะ” ในลักษณะใดจึงจะถือว่าเป็นการใช้อำนาจและทำเพื่อประโยชน์สาธารณะที่ถูกต้องและชอบด้วยกฎหมายที่ผู้ให้บริการโปรแกรมสืบค้นข้อมูล จะใช้ประโยชน์จากข้อยกเว้นดังกล่าวนี้ได้ถือเป็นหน้าที่ของรัฐสมาชิกในการกำหนดนิยามและขอบเขตของคำดังกล่าวให้ชัดเจนอีกประการหนึ่ง

(ก) ประโยชน์สาธารณะในกรณีของสาธารณสุข[128]

ข้อยกเว้นในกรณีการทำเพื่อประโยชน์สาธารณะด้านสาธารณสุขนี้ต้องปรากฏว่ากฎหมายแห่งรัฐสมาชิกและสหภาพยุโรปได้มีกำหนดฐานทางกฎหมายเอาไว้สำหรับการประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์ด้านสาธารณสุข อย่างไรก็ตาม เนื่องด้วยสภาพกิจกรรมของผู้ให้บริการโปรแกรมสืบค้นข้อมูลที่เพียงให้บริการในการค้นหาข้อมูลใด ๆ ของเจ้าของข้อมูลส่วนบุคคลด้วยการใช้ชื่อของเจ้าของข้อมูลส่วนบุคคลคนนั้น จึงทำให้เป็นการยากที่รัฐสมาชิกจะกำหนดให้มีบทบัญญัติที่จะให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูล มีหน้าที่อันเกี่ยวข้องกับประโยชน์ด้านสาธารณสุข เนื่องจากสภาพกิจกรรมของผู้ให้บริการโปรแกรมสืบค้นข้อมูลมิได้มีลักษณะที่จะเป็นไปเพื่อประโยชน์ด้านสาธารณสุขได้เลย

---

[128] Ibid, para 73 to para 78.

(ข) วัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์หรือการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ หรือวัตถุประสงค์ที่เกี่ยวกับสถิติ[129]

การอ้างข้อยกเว้นข้างต้นนี้ จะสามารถปรับใช้ได้เฉพาะกับผู้ให้บริการโปรแกรมสืบค้นข้อมูลที่เป็นผู้ดำเนินการตามวัตถุประสงค์ดังกล่าวอย่างแท้จริงเท่านั้น โดยที่ข้อยกเว้นนี้จะไม่บังคับใช้กับกรณีการดำเนินการตามวัตถุประสงค์ด้านการศึกษาวิจัยหรือวัตถุประสงค์ทางด้านสถิติที่ดำเนินการโดยผู้ใช้อินเทอร์เน็ต เนื่องจากการจะอ้างถึงเหตุแห่งการปฏิเสธการใช้สิทธิตามข้อยกเว้นนี้ได้ ต้องเป็นกรณีของการดำเนินการตามวัตถุประสงค์ของผู้ให้บริการโปรแกรมสืบค้นข้อมูล ไม่ใช่ผู้ใช้งานอินเทอร์เน็ต ทั้งนี้โดยที่ผู้ให้บริการโปรแกรมสืบค้นข้อมูลจำต้องสามารถแสดงได้ว่าการร้องขอใช้สิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลนั้นเป็นอุปสรรคและขัดขวางต่อการบรรลุวัตถุประสงค์ดังกล่าวอย่างมาก ผู้ให้บริการโปรแกรมสืบค้นข้อมูลจึงอาจอ้างข้อยกเว้นข้างต้นเพื่อปฏิเสธการใช้สิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลของเจ้าของข้อมูลส่วนบุคคลได้

อย่างไรก็ตาม หากเกิดกรณีที่การร้องขอให้นำข้อมูลส่วนบุคคลออกนั้นเป็นการกระทบกระเทือนถึงการบรรลุวัตถุประสงค์ของผู้ใช้อินเทอร์เน็ต กรณีจะเข้าข้อยกเว้นตามหลักเกณฑ์ข้อนี้ได้ก็ต่อเมื่อมีการพิจารณาชั่งน้ำหนักระหว่างสิทธิของเจ้าของส่วนบุคคล และประโยชน์ของผู้ใช้งานอินเทอร์เน็ตในการที่จะสามารถเข้าถึงข้อมูลส่วนบุคคลเพื่อดำเนินการให้บรรลุวัตถุประสงค์ดังกล่าวได้

[129] Ibid, para 79 to para 81.

(ค) การก่อตั้ง ใช้ และปกป้องสิทธิทางกฎหมาย[130]

โดยหลักการแล้ว การใช้ข้อยกเว้นเพื่อปฏิเสธการลบข้อมูลโดยอาศัยเหตุผลเพื่อการก่อตั้ง ใช้ และปกป้องสิทธิทางกฎหมายนี้ มีความเป็นไปได้ยากสำหรับการให้บริการโปรแกรมค้นหาข้อมูล เนื่องจากการร้องขอใช้สิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลนั้น ควรมีจุดมุ่งหมายที่เป็นไปเพื่อวัตถุประสงค์ในการปิดกั้น ผลการค้นหาจากหน้าแสดงผลการค้นหา เมื่อมีการใช้ชื่อของเจ้าของข้อมูลส่วนบุคคลเป็นหลักเกณฑ์ในการค้นหา (Search Criteria) เท่านั้น และโดยที่ข้อมูลส่วนบุคคลดังกล่าวยังคงสามารถเข้าถึงได้โดยการใช้คำค้นหาอื่น ๆ ที่ไม่ใช่ชื่อของเจ้าของข้อมูล

3.2.2 กรณีศึกษา

3.2.2.1 คดี Google Spain v AEPD and Mario Costeja González

คดี Google Spain v AEPD and Mario Costeja González ถือเป็นคดีที่ CJEU ได้ตัดสินเกี่ยวกับสิทธิที่จะถูกลืมเอาไว้เป็นคดีแรกใน ค.ศ. 2014 คดีดังกล่าวถูกยื่นฟ้องต่อศาลในประเทศสเปนโดย นาย Mario Costeja Gonzalez ซึ่งเป็นโจทก์ในคดีนี้ นาย Costeja ได้กล่าวหาว่า Google แสดงผลการค้นหาที่ไม่เป็นความจริงและขอให้ศาลสั่งให้ Google ลบข้อมูลดังกล่าวออก ข้อมูลตามกรณีพิพาทนี้เป็นข้อมูลซึ่งเป็นหนังสือบอกกล่าวทางกฎหมายที่เชื่อมโยงมายังนาย Costeja หนังสือบอกกล่าวทางกฎหมายฉบับนี้ ปรากฏอยู่บนหนังสือพิมพ์ท้องถิ่นที่ชื่อ La Vanguardia ซึ่งเป็นหนังสือพิมพ์ท้องถิ่นที่มีการประกาศเผยแพร่รายการทรัพย์สินที่ถูกยึดและจำต้องถูกขายทอดตลาด

[130] Ibid, para 82 to para 83.

โดยหน่วยงานของรัฐบาล ทรัพย์สินทั้งหมดเป็นทรัพย์สินของลูกหนี้ที่ไม่สามารถชำระหนี้ จึงจำต้องถูกยึดและอายัติไว้เพื่อขายทอดตลาดตีราคาใช้หนี้ โดยหนึ่งในรายการทรัพย์สินที่ถูกประกาศขายทอดตลาดนั้นปรากฏชื่อของนาย Costeja ว่าเป็นเจ้าของและเป็นลูกหนี้ที่จำต้องถูกบังคับคดี[131]

นาย Costeja ระบุว่าเนื้อหาที่แสดงรายการทรัพย์สินขายทอดตลาดนี้อาจทำให้กระทบกระเทือน และเสื่อมเสียต่อชื่อเสียงในด้านการทำงานของเขาได้ เนื่องจากตัวเขามีอาชีพเป็นทนายความและมีสำนักงานกฎหมายที่เป็นธุรกิจของเขาเอง อีกทั้งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เป็นความจริงอีกแล้ว[132] เนื่องจากจำนวนหนี้ค้างชำระดังกล่าวได้ถูกชำระและชดใช้ไปจนหมดสิ้นเป็นระยะเวลากว่าสิบปีแล้ว นาย Costeja ให้เหตุผลว่าเนื่องจากสำนักงานกฎหมายของเขานั้นเป็นสำนักงานกฎหมายขนาดเล็กที่จำต้องพึ่งพาระบบอินเทอร์เน็ตในการขยายและพัฒนาธุรกิจเป็นอย่างมากซึ่งเป็นช่องทางในการรับลูกค้าที่ทำให้สำนักงานกฎหมายของเขาเป็นที่รู้จัก และลูกค้ามักรู้จักสำนักงานกฎหมายของตนโดยผ่านทาง Google นั้นเอง จึงมีความเป็นไปได้ว่าข้อมูลซึ่งเป็นหนังสือบังคับการขายทอดตลาดที่ปรากฏอยู่บนผลแสดงการค้นหาของ Google นั้น อาจส่งผลในด้านชื่อเสียงและทำให้ไม่มีลูกความคนใดต้องการจ้างนาย Costeja เพื่อให้เป็นทนายความ

ในตอนแรกนั้น นาย Costeja ได้ส่งจดหมายไปยังหนังสือพิมพ์ท้องถิ่น La Vanguardia และร้องขอให้ทำการลบหัวข้อข่าวที่เกี่ยวกับหนังสือแจ้งหนี้ฉบับดังกล่าวออก เนื่องจากหนี้ดังกล่าวได้ถูกชำระไปจนหมดสิ้นเป็นระยะเวลาหลายปีก่อนแล้ว จึงทำให้การอ้างอิงถึงหนังสือฉบับนั้นไม่เกี่ยวข้องกับตนอีกต่อไป โดยที่นาย Costeja ได้ใช้สิทธิภายใต้นโยบายการคุ้มครองข้อมูลของประเทศสเปน ที่กำหนดให้ความสำคัญต่อการคุ้มครองและความถูกต้องครบถ้วน (Integrity) ของข้อมูลส่วนบุคคลในฐานะเป็น

[131] Judgment of the Court C-131/12, para 14.

[132] Ibid, para 15.

สิทธิตามรัฐธรรมนูญภายใต้มาตรา 18 แห่งกฎหมายคุ้มครองข้อมูลของประเทศสเปน หนังสือพิมพ์ท้องถิ่น La Vanguardia จึงได้ตอบกลับและแจ้งว่าหนังสือพิมพ์ได้อัพโหลดข้อมูลเดิมที่อยู่ภายในคลังเก็บเอกสารทั้งหมดลงบนระบบอินเทอร์เน็ตเมื่อไม่นานมานี้ เพื่อให้ข้อมูลดังกล่าวสามารถถูกค้นหาได้เป็นการสาธารณะ และหนังสือแจ้งขายทอดตลาดฉบับดังกล่าวก็เป็นหนังสือที่ถูกลงประกาศโดยสาธารณะมาตั้งแต่ต้น ทั้งนี้ก็เพื่อเป็นการรักษาผู้ประมูลทรัพย์สินขายทอดตลาดให้ได้มากที่สุด ทำให้หนังสือพิมพ์ท้องถิ่น La Vanguardia ปฏิเสธคำร้องของนาย Costeja และให้เหตุผลว่าข้อมูลดังกล่าวนั้น เป็นข้อมูลที่ได้รับมาจากบันทึกสาธารณะจึงทำให้การเผยแพร่ในเว็บไซต์ของหนังสือพิมพ์ท้องถิ่นนั้นชอบด้วยกฎหมายแล้ว

อย่างไรก็ตาม ประเด็นสำคัญของการพิพาท ได้แก่ การที่ข้อมูลการขายทรัพย์สินทอดตลาดดังกล่าวนั้นปรากฏอยู่ในโปรแกรมสืบค้นข้อมูลของ Google ที่เป็นผู้ให้บริการโปรแกรมสืบค้นข้อมูลที่ถูกใช้งานทั่วโลก ที่อาจนำไปสู่กรณีที่ทำให้ลูกค้าในอนาคตของสำนักงานกฎหมายของนาย Costeja อาจตัดสินความประพฤติของนาย Costeja จากข้อมูลที่ปรากฏบนโปรแกรมสืบค้นข้อมูลดังกล่าว จึงได้เขียนคำร้องในทำนองเดียวกันไปยัง Google Spain ซึ่งเป็นบริษัทย่อยของ Google Inc. เรียกร้องถึงความรับผิดชอบที่ Google Inc. มีต่อกรณีดังกล่าว คำร้องของนาย Costeja ยังคงถูกปฏิเสธ ทำให้ต่อมานาย Costeja จึงได้ส่งเรื่องร้องเรียนไปยังหน่วยงานคุ้มครองข้อมูลส่วนบุคคลของสเปน (Agencia Española de Protección de Datos : AEPD)

AEPD ปฏิเสธคำร้องขอที่เกี่ยวกับหนังสือพิมพ์ท้องถิ่น La Vanguardia โดยอ้างว่าการเผยแพร่ข้อมูลดังกล่าวนั้นเป็นการกระทำโดยชอบด้วยกฎหมาย[133] และเป็นขั้นตอนปกติทั่วไปของสื่อด้านข่าวสารในการทำข้อมูลดังกล่าวให้เป็นสาธารณะ AEPD ได้มีคำสั่งไปยัง Google โดยระบุว่า Google ไม่ควรแสดงลิงค์ไปยังเว็บเพจดังกล่าวของหนังสือพิมพ์ท้องถิ่น La Vanguardia

[133] อรรถกร สุขปุณพันธ์ (อ้างแล้ว เชิงอรรถที่ 77), หน้า 4.

ในเวลาต่อมา AEPD ได้มีคำสั่งที่มีการพิจารณาให้หน้าที่ผู้ให้บริการโปรแกรมสืบค้นข้อมูลต้องเป็นไปกฎหมายคุ้มครองข้อมูล เนื่องจากกิจกรรมของผู้ให้บริการโปรแกรมสืบค้นข้อมูลนั้น มีลักษณะเป็นการประมวลผลข้อมูลและมีหน้าที่รับผิดชอบและเป็นผู้ดำเนินการในฐานะตัวกลางในสังคมข้อมูลข่าวสาร จึงทำให้ต่อมา Google ได้ยื่นอุทธรณ์คำสั่งของหน่วยงาน AEPD ดังกล่าวไปยังศาลสูงของประเทศสเปน (Audiencia Nacional) ใน ค.ศ. 2011

การยื่นอุทธรณ์คำสั่งต่อศาลสูงสเปนในกรณีนี้ ทำให้เกิดประเด็นปัญหาหลายประเด็นเกี่ยวกับลักษณะกิจกรรมของการเป็นผู้ให้บริการโปรแกรมสืบค้นข้อมูล โดยมีการพิจารณาว่าผู้ให้บริการโปรแกรมสืบค้นข้อมูลนั้นในความเป็นจริงแล้วมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่ และหากพิจารณาให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูลมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลจริง ผู้ให้บริการโปรแกรมสืบค้นข้อมูลจะอยู่ภายใต้ข้อบังคับอันเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ หากว่าผู้ให้บริการโปรแกรมสืบค้นข้อมูลนั้นมีหน้าที่ที่จำต้องปฏิบัติให้เป็นตามกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแล้ว กรณีดังกล่าวจะทำให้หน่วยงานคุ้มครองข้อมูลส่วนบุคคลสามารถใช้อำนาจสั่งให้ผู้ให้บริการโปรแกรมสืบค้นข้อมูลลบข้อมูลส่วนบุคคลออกจากผลแสดงการค้นหาที่เชื่อมต่อไปยังเว็บไซต์ต้นตอที่บรรจุข้อมูลส่วนบุคคลอยู่ โดยที่ไม่จำต้องสั่งการไปยังเว็บไซต์นั้นโดยตรงได้หรือไม่

ศาลสูงของประเทศสเปนได้มีการส่งคดีดังกล่าวต่อไปยัง CJEU เพื่ออาศัยอำนาจในการวินิจฉัยข้อกฎหมาย (the Preliminary Ruling) เนื่องจากมีประเด็นปัญหาในการตีความข้อกฎหมายภายใต้บทบัญญัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล จึงเกิดเป็นคดี *Google Spain v AEPD and Mario Costeja González*

ในชั้นการพิจารณาคดีระดับสหภาพยุโรป คดีมีประเด็นปัญหาที่โต้แย้งกันถึงนิยามของคำว่า “ข้อมูลส่วนบุคคล” และ “Crawling” โดย Crawling ซึ่งเป็นหนึ่งในวิธีการของกิจกรรมของผู้ให้บริการโปรแกรมสืบค้นข้อมูลในการให้บริการโปรแกรมสืบค้นข้อมูล Crawling เป็นวิธีการใช้โปรแกรมซอฟท์แวร์เพื่อการค้นหาเว็บไซต์เพื่อตอบกลับการร้องขอค้นหาข้อมูลออนไลน์ของผู้ใช้บริการโปรแกรมสืบค้นข้อมูล โดยโปรแกรมดังกล่าวจะทำการค้นหาข้อมูลบนอินเทอร์เน็ต ตามเกณฑ์กำหนดที่โปรแกรมดังกล่าวถูกสั่งการให้ทำการค้นหาที่ไหนและค้นหาเมื่อไหร่ และเมื่อเว็บเพจต่าง ๆ ถูกนำเสนอและเก็บรวบรวมไว้ เนื้อหาทั้งหมดภายในเว็บเพจนั้นจะถูกวิเคราะห์และจัดเรียงข้อมูลเป็นดัชนีแสดงรายการต่าง ๆ[134]

อย่างไรก็ตาม Google ได้โต้แย้งว่าการสืบค้นข้อมูลบนอินเทอร์เน็ต (Crawling) ของ Google นั้นเป็นการจัดเรียงเว็บไซต์ต่าง ๆ เป็นรายการและเป็นการจัดเรียงรายการที่ไม่เลือกปฏิบัติซึ่งไม่มีวัตถุประสงค์ในลักษณะเพื่อประมวลผลข้อมูลส่วนบุคคล จึงทำให้กิจกรรมการสืบค้นข้อมูลบนอินเทอร์เน็ตของ Google ไม่อยู่ภายใต้นิยามตามมาตรา 2 (b) ของ Directive 95/46 นอกจากนี้ Google ยังได้โต้แย้งว่าผู้เผยแพร่ข้อมูลดังกล่าวควรจะต้องเป็นผู้ควบคุมข้อมูลแต่เพียงผู้เดียว ไม่ใช่ผู้ให้บริการโปรแกรมสืบค้นข้อมูล โดยลักษณะกิจกรรมของ Google นั้นถูกสร้างขึ้นเพื่อเป็นเครื่องมือเพื่อการเข้าถึงโดยสภาพอย่างแท้จริง โดยที่ Google เพียงแต่ทำให้ข้อมูลดังกล่าวที่ถูกประกาศโดยบุคคลอื่นสามารถเข้าถึงได้อย่างรวดเร็วมากขึ้นเท่านั้น หากผู้เผยแพร่ข้อมูลตัดสินใจที่จะลบข้อมูลดังกล่าวออกจากเว็บไซต์ของเขา ข้อมูลนั้นก็ย่อมถูกลบออกจากรายการข้อมูลของ Google และไม่สามารถปรากฏบนผลแสดงการค้นหาได้ด้วยเช่นกัน ดังนั้น Google จึงควรต้องถูกพิจารณาว่ามีบทบาทเป็นเพียงตัวกลางเท่านั้น

---

[134] Ibid, para 43.

CJEU มีคำตัดสินต่อกรณีพิพาทดังกล่าวใน ค.ศ. 2014 วินิจฉัยว่า Google ในฐานะผู้ให้บริการค้นหาเป็นผู้ควบคุมข้อมูลส่วนบุคคล (เพื่อระบุว่า Google ตกอยู่ในบังคับของ GDPR ในกรณีนี้โดยปฏิเสธว่าการประมวลผลอัตโนมัติโดยไม่มีมนุษย์เข้ามีส่วนร่วมมิได้เป็นเหตุให้การดำเนินการขาดจากลักษณะการประมวลผลข้อมูลส่วนบุคคล)[135] และกำหนดให้ Google ดำเนินการลบลิงค์ที่ปรากฏผลแสดงการค้นหาโดยศาลได้ให้เหตุผลประกอบการวินิจฉัยเอาไว้ว่า

> *“ผลการค้นหาที่เคยถูกแสดงผลโดยชอบด้วยกฎหมายโดยบุคคลที่สาม (เมื่อเวลาผ่านไป) กลายเป็นการแสดงผลที่ฝ่าฝืนต่อมาตรา 6 (1) (c) ถึง (e) เนื่องจาก เมื่อได้พิจารณาพฤติการณ์ทั้งปวงแล้ว ปรากฏว่าข้อมูลนั้นมีความไม่เพียงพอ ไม่เกี่ยวข้องหรือไม่เกี่ยวข้องกับการประมวลผลอีกต่อไป หรือเกินความจำเป็นในการประมวลผลของผู้ให้บริการโปรแกรมการสืบค้น ดังนั้นข้อมูลและลิงค์เกี่ยวกับผลการค้นหาจึงต้องถูกลบ[136]*

คำวินิจฉัยของ CJEU ในคดี *Google Spain v AEPD and Mario Costeja González* นั้น มีข้อสังเกตที่สำคัญ คือ การที่ผู้ให้บริการระบบสืบค้นออนไลน์นั้นมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล โดยกิจกรรมการประมวลผลข้อมูลโดยผู้ให้บริการระบบสืบค้นนี้สามารถพิจารณาโดยแยกต่างหากได้จากผู้เผยแพร่ข้อมูลที่เป็นบุคคลภายนอก[137] การคุ้มครองความส่วนตัวของ

[135] David J. Stute, ‘Privacy Almighty? The CJEU’s Judgment in Google Spain SL v. AEPD’ (2015) Michigan Journal of International Law 36 (4) 649, p. 659.

[136] Ibid, para 94.

[137] Article 29 Data Protection Working Party, ‘Guidelines on the Implementation of the Court of Justice of the European Union Judgment on “Google Spain and Inc v. Agencia Espanola De Proteccion De Datos (AEPD) and Mario Costeja Gonzalez C-131/12’ (Article 29 Data Protection Working Party, November 2014) <file :///C :/Users/User/Downloads/wp225_en_6F61B70D-A130-F778-619246F5CE8DE165_64437.pdf> accessed 5 August 2021, p. 2.

เจ้าของข้อมูลนั้นสามารถเป็นประโยชน์ที่มีน้ำหนักมากกว่าประโยชน์ทางเศรษฐกิจของตัวผู้ให้บริการระบบสืบค้นและผู้ใช้งานอินเทอร์เน็ตอื่น ๆ โดยมีข้อสังเกตว่าในบางกรณีประโยชน์ในการเข้าถึงข้อมูลของผู้ใช้งานอินเทอร์เน็ตอื่นอาจมีน้ำหนักมากกว่าหากว่าเจ้าของข้อมูลส่วนบุคคลมีบทบาทสาธารณะ[138]

อย่างไรก็ตาม คดี *Google Spain v AEPD and Mario Costeja González* ก็แสดงให้เห็นถึงข้อจำกัดของสิทธิที่จะถูกลืมหลายประการ เช่น สิทธิในการขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลนั้นมีผลเฉพาะต่อ “ผลลัพธ์” ในส่วนของ “ชื่อ” ที่ปรากฏจากการสืบค้นเท่านั้น และไม่ส่งผลให้ต้องมีการลบลิงค์จากดัชนีแสดงผลการค้นหาของระบบสืบค้นทั้งหมด ทำให้ข้อมูลที่ถูกเผยแพร่เดิมยังคงถูกเข้าถึงได้โดยการอาศัยคำค้นหาอื่น ๆ หรือการเข้าถึงจากฐานข้อมูลของผู้เผยแพร่โดยตรง[139] โดยมีข้อสังเกตว่าตัวเจ้าของข้อมูลส่วนบุคคลนั้นไม่ได้มีหน้าที่ต้องติดต่อกับผู้เผยแพร่ข้อมูลเดิมผ่านระบบสืบค้น[140]

นอกจากนี้ คำวินิจฉัยยังส่งผลต่อชื่อที่ใช้ระบุลงในคอมพิวเตอร์เพื่อไปค้นหาในระบบ (โดเมน) ซึ่งอาจอยู่ต่างประเทศได้ เพื่อให้สิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลนั้นถูกคุ้มครองอย่างแท้จริง CJEU ได้วินิจฉัยว่าการจำกัดให้การดังกล่าวถูกใช้ได้เฉพาะกับโดเมนในสหภาพยุโรปนั้นส่งผลให้การคุ้มครองไม่อาจเกิดขึ้นอย่างเพียงพอได้ ในทางปฏิบัติสิทธิในการขอให้ข้อมูลออกจากโปรแกรมสืบค้นข้อมูลควรครอบคลุมถึงโดเมนที่เกี่ยวข้องกับทุกโดเมนรวมไปถึงโดเมน “.com” ด้วย[141]

---

[138] Ibid.

[139] Ibid.

[140] Ibid.

[141] Ibid, p. 3.

3.2.2.2 คดี Segerstedt-Wiberg and Others v. Sweden

คดี *Segerstedt-Wiberg and Others v. Sweden* มีประเด็นพิพาทเกี่ยวข้องกับการลบข้อมูลส่วนบุคคลที่ถูกยื่นฟ้องต่อศาลสิทธิมนุษยชนแห่งสหภาพยุโรปใน ค.ศ. 2006 ผู้ร้องเป็นสมาชิกของพรรคการเมืองคอมมิวนิสต์ในประเทศสวีเดน ผู้ร้องได้ยื่นคำร้องไปยังสำนักงานตำรวจความมั่นคงสวีเดน (Swedish Security Police) เพื่อขอตรวจดูประวัติการกระทำความผิด หลังจากนั้นจึงร้องขอให้สำนักงานตำรวจความมั่นคงสวีเดนลบข้อมูลดังกล่าวออกไป โดยอ้างว่าข้อมูลเกี่ยวกับการกระทำความผิดของเธอนั้นได้ถูกเปิดเผยออกไปยังภายนอก[142]

แม้การเก็บรวบรวมข้อมูลประวัติการกระทำความผิดดังกล่าวนั้นได้กระทำโดยอาศัยฐานทางกฎหมายที่ชอบด้วยกฎหมาย และได้ถูกดำเนินการโดยวัตถุประสงค์อันชอบธรรม แต่เมื่อศาลสิทธิมนุษยชนแห่งสหภาพยุโรปตรวจพบว่ายังคงมีการเก็บรักษาข้อมูลบางส่วนอยู่ จึงเป็นกรณีที่ทำให้เกิดการแทรกแซงที่ไม่ได้สัดส่วน (Disproportionate Interference) กับชีวิตส่วนตัวของผู้ร้องบางรายอยู่ ยกตัวอย่างเช่นในกรณีของบุคคลคนหนึ่งที่เจ้าหน้าที่ตำรวจยังคงทำการเก็บรวบรวมข้อมูลที่เป็นประวัติการกระทำความผิดของผู้ร้องรายดังกล่าวเอาไว้ ซึ่งเป็นประวัติการกระทำความผิดที่กล่าวหาว่าผู้ร้องได้กระทำการอันเป็นปรปักษ์ร้ายแรงต่อการควบคุมของเจ้าหน้าที่ตำรวจระหว่างการเดินขบวนใน ค.ศ. 1969 การเก็บข้อมูลดังกล่าวแม้ว่าจะเป็นการเก็บรักษาข้อมูลที่มีความเกี่ยวข้อง อย่างไรก็ตาม การเก็บรักษาข้อมูลดังกล่าวเอาไว้เป็นการแทรกแซงสิทธิในความเป็นส่วนตัวมากเกินสัดส่วน[143]

---

[142] European Court of Human Rights, 'Segerstedt-Wiberg and Others v. Sweden' (European Court of Human Rights, June 2006) <file :///C :/Users/admin/Downloads/003-1688388-1769677%20 (1).pdf> accessed 3 October 2021, p. 2.

[143] Ibid, p. 5.

ศาลสิทธิมนุษยชนแห่งสหภาพยุโรปจึงได้มีคำตัดสินว่าข้อมูลดังกล่าวนั้น ไม่มีความเกี่ยวข้องกับประโยชน์ความมั่นคงของประเทศ และได้พิพากษาตัดสินว่ามีการกระทำการอันเป็นการฝืนฝืนต่อสิทธิตามมาตรา 8 ของ ECHR ของผู้ร้องจำนวนสี่คนดังกล่าว และได้มีคำสั่งให้ชดใช้เป็นเงินจำนวนหนึ่งแก่ผู้ร้องทั้งสี่คนและค่าเสียหายที่มิใช่ตัวเงินแก่อีกผู้ร้องรายหนึ่ง[144] การวินิจฉัยคดีของศาลสิทธิมนุษยชนในกรณีนี้ ได้แสดงให้เห็นถึงความท้าทายในทางปฏิบัติในการชั่งน้ำหนักประโยชน์สาธารณะกับสิทธิในความส่วนตัวของปัจเจกบุคคล ซึ่งก่อให้เกิดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการพิจารณาถึง “ความได้สัดส่วน” ระหว่างประโยชน์สาธารณะกับสิทธิในความส่วนตัว

3.2.2.3 คดี Camera di Commercio di Lecce v. Manni

คดี *Camera di Commercio di Lecce v. Manni*[145] มีประเด็นสำคัญที่ศาลจะต้องวินิจฉัยว่าบุคคลนั้นอาจมีสิทธิในการได้รับการลบข้อมูลส่วนบุคคลของตนได้ที่ถูกประกาศในทะเบียนสาธารณะของบริษัทได้หรือไม่ เมื่อบริษัทของบุคคลดังกล่าวนั้นเลิกกิจการลง[146] นาย Manni ผู้ร้องในคดีนี้ได้ยื่นคำร้องต่อ Lecce Chamber of Commerce ซึ่งเป็นสมาคมการค้าพาณิชย์ในประเทศอิตาลี ให้ทำการลบข้อมูลส่วนบุคคลของเขาออกจากทะเบียนดังกล่าว เนื่องจากอาจเกิดกรณีที่ลูกค้าในอนาคตของผู้ร้องเข้าไปตรวจสอบข้อมูลภายในทะเบียนสาธารณะแห่งบริษัทและพบข้อมูลว่าผู้ร้องเคยเป็นกรรมการของบริษัทที่ถูกประกาศล้มละลายเมื่อหลายสิบปีก่อน ทำให้ผู้ร้องเชื่อว่าข้อมูลดังกล่าวอาจเป็นอุปสรรคต่อภาพลักษณ์ด้านธุรกิจของตนในอนาคต

---

[144] Ibid.

[145] Judgment of the Court Case C-398/15.

[146] Ibid, para 30.

CJEU ตัดสินว่า วัตถุประสงค์ของการเป็นทะเบียนสาธารณะแห่งบริษัทนั้น มีขึ้นเพื่อเปิดเผยข้อมูลที่กฎหมายกำหนด และตามคำสั่งของสหภาพยุโรปที่มีวัตถุประสงค์ต้องการให้บุคคลภายนอกสามารถเข้าถึงข้อมูลดังกล่าวได้ง่าย ดังนั้น บุคคลภายนอกควรจำต้องสามารถเข้าถึงข้อมูลเกี่ยวกับบริษัทดังกล่าวได้ และโดยเฉพาะอย่างยิ่งข้อมูลของบุคคลที่มีอำนาจกระทำการแทนบริษัทนั้น ๆ วัตถุประสงค์ของการเปิดเผยข้อมูลนี้ยังเป็นสิ่งรับประกันความแน่นอนทางกฎหมายในการเจรจาทางการค้าของบริษัทและบุคคลภายนอกระหว่างรัฐสมาชิก และโดยเฉพาะอย่างยิ่งเพื่อปกป้องผลประโยชน์ของบุคคลภายนอกที่เกี่ยวกับบริษัทร่วมทุนและบริษัทจำกัด จึงทำให้ต้องมีการทำให้มั่นใจว่าบุคคลภายนอกจะสามารถเข้าถึงข้อมูลที่เกี่ยวข้องกับบริษัทได้ทั่วทั้งสหภาพยุโรป[147]

นอกจากนี้ CJEU ยังได้ระบุว่า แม้ว่าช่วงระยะเวลาใดเวลาหนึ่งจะได้สิ้นสุดลงไปแล้ว และแม้ว่าบริษัทจะเลิกกิจการไปแล้วก็ตาม สิทธิและหน้าที่ในการปฏิบัติตามกฎหมายที่เกี่ยวกับบริษัทยังคงมีอยู่ ข้อโต้แย้งที่เกี่ยวข้องกับการเลิกบริษัทนั้นอาจเกิดขึ้นและใช้ระยะเวลาที่ยาวนานเพื่อระงับข้อโต้แย้ง และข้อสงสัยต่าง ๆ ที่เกี่ยวกับบริษัท ผู้จัดการ และผู้ชำระบัญชียังอาจเกิดขึ้นได้แม้จะได้เลิกบริษัทไปแล้วเป็นระยะเวลาหลายปี CJEU กล่าวว่าด้วยระยะเวลาในการเปิดเผยข้อมูลทางทะเบียนที่แต่ละรัฐสมาชิกได้กำหนดขึ้นนั้นมีความแตกต่างกัน จึงเป็นเรื่องยากที่จะกำหนดระยะเวลาใดเวลาหนึ่งขึ้นมาเพื่อใช้บังคับกับกรณีทุกกรณีที่เกิดขึ้นภายในสหภาพยุโรป[148]

การแทรกแซงสิทธิพื้นฐานของบุคคล โดยเฉพาะอย่างยิ่งในกรณีนี้คือสิทธิในชีวิตส่วนตัวและสิทธิในการคุ้มครองข้อมูลส่วนบุคคลตามที่ให้สิทธิไว้ภายใต้กฎบัตรสิทธิขั้นพื้นฐานของสหภาพยุโรป (Charter of Fundamental

[147] Ibid, para 50.

[148] Ibid, para 52.

Rights of the Union) มิใช่กรณีของการแทรกแซงที่ไม่ได้สัดส่วนกัน เนื่องจากมีเพียงข้อมูลส่วนบุคคลของคนกลุ่มหนึ่งเท่านั้นที่ใช้ในการก่อตั้งบริษัท และเป็นเรื่องที่ชอบธรรมที่บุคคลธรรมดาที่ได้เข้าร่วมในการค้าระหว่างบริษัทร่วมทุนและบริษัทจำกัดนั้น จำต้องเปิดเผยข้อมูลส่วนบุคคลและหน้าที่ต่าง ๆ ภายในบริษัทอยู่แล้ว

เนื่องด้วยวัตถุประสงค์อันชอบธรรมของการเปิดเผยข้อมูลและความแตกต่างในการกำหนดขอบระยะเวลาของการเปิดเผยหรือการลบข้อมูลออกจากทะเบียนโดยปราศจากการสร้างความเสียหายต่อประโยชน์ของบุคคลภายนอกของแต่ละรัฐสมาชิก ดังนั้น CJEU จึงได้มีคำพิพากษาว่า GDPR มิได้รับประกันสิทธิในการขอให้ลบข้อมูลส่วนบุคคลในกรณีดังกล่าว เนื่องจากสิทธิที่จะถูกลืมมิได้ใช้บังคับต่อข้อมูลส่วนบุคคลที่ปรากฏอยู่ในทะเบียนบริษัท[149]

คำวินิจฉัยของ CJEU ในคดี *Camera di Commercio di Lecce v. Manni* แสดงให้เห็นถึงความท้าทายในทางปฏิบัติของข้อมูลที่ถูกเก็บรวบรวมโดยทะเบียนสาธารณะของบริษัทซึ่งเป็นข้อมูลที่ถูกเก็บรวบรวมอยู่ในฐานข้อมูลของรัฐเพื่อประโยชน์สาธารณะ เช่น เพื่อให้บุคคลภายนอกที่จะทำธุรกรรมกับบริษัทสามารถตรวจสอบสถานะและข้อมูลของบริษัทได้ ในกรณีนี้ประโยชน์สาธารณะมีน้ำหนักมากกว่าความเป็นส่วนตัว โดยมิได้เป็นกรณีของการแทรกแซงที่ไม่ได้สัดส่วน จะเห็นได้ว่ากรณีนี้แตกต่างไปจากคดี *U.S. Department of Justice v. Reporters Committee* ที่ฐานข้อมูลนั้นเป็นเรื่องเกี่ยวกับการกระทำความผิดของปัจเจกบุคคล อย่างไรก็ตาม จะเห็นได้ว่าศาลฎีกาของสหรัฐเอมริกาในคดีดังกล่าวอาศัยหลักการเรื่องการที่ข้อมูลนั้นเข้าถึงได้ยากเป็นฐานในการวินิจฉัย ซึ่งแตกต่างไปจากแนวทางของ CJEU

[149] Ibid, para 64.

3.2.2.4 คดี Google LLC v CNIL

คดี *Google LLC v CNIL*[150] ถูกนำขึ้นสู่ CJEU โดย Council of State เนื่องจากข้อเท็จจริงปรากฏว่า Google นั้นได้ปฏิเสธการจ่ายเงินซึ่งเป็นค่าปรับตามคำสั่งของหน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล (Commission Nationale de l'Informatique et des Libertés : CNIL) จำนวนกว่า 100,000 ยูโร[151] เนื่องจาก Google ได้ปฏิเสธการปฏิบัติตามคำสั่งของ CNIL ในการถอนการอ้างอิงหรือลบลิงค์ที่ปรากฏบนรายการแสดงการค้นหาของ Google โปรแกรมสืบค้นข้อมูล ซึ่งลิงค์ดังกล่าวแสดงข้อมูลส่วนบุคคลที่เชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลและอาจก่อความเสียหายให้แก่บุคคลดังกล่าวได้ลิงค์ดังกล่าวเป็นลิงค์ที่เกิดขึ้นจากโดเมน (Domain) ของ Google ที่ตั้งอยู่นอกอาณาเขตของสหภาพยุโรป[152]

CJEU ในคดีนี้ได้พิพากษาตัดสินให้ Google ชนะคดี โดยอ้างอิงหลักเรื่องเขตอำนาจของการบังคับใช้ GDPR สิทธิที่จะถูกลืมโดยมีคำสั่งให้ Google และโปรแกรมค้นหาข้อมูลอื่นทำการลบลิงค์ผลแสดงการค้นหาออกจากโดเมนเฉพาะภายในอาณาเขตของสหภาพยุโรป[153] แต่ไม่จำเป็นต้องลบออกจากโดเมนที่มิได้ตั้งอยู่ภายในรัฐสมาชิกในสหภาพยุโรป เนื่องจากศาล CJEU เห็นว่ามีหลายประเทศที่ไม่ได้เป็นรัฐสมาชิกสหภาพยุโรปมีการดำเนินการกับสิทธิที่จะถูกลืมที่แตกต่างออกจาก GDPR หรืออาจไม่มีการให้สิทธิดังกล่าวไว้ อีกทั้ง สิทธิในการคุ้มครองข้อมูลส่วนบุคคลนั้นมิได้เป็นสิทธิเด็ดขาด จึงทำให้ต้องมีการชั่งน้ำหนักระหว่างสิทธิพื้นฐานเพื่อให้เป็นไปตามหลักการได้สัดส่วนด้วย นอกจากนี้ สมดุลระหว่างสิทธิในความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล เสรีภาพของผู้ใช้อินเทอร์เน็ตทั่วโลกนั้นมีความแตกต่างกัน

---

[150] Judgment of the Court C-507/17.

[151] Ibid, para 33.

[152] Ibid, para 53.

[153] Ibid, para 51 to 52.

อย่างมีนัยสำคัญ กล่าวคือบางประเทศไม่ได้มีการรับรองสิทธิที่จะยกเลิกการอ้างอิง[154]

ในการวินิจฉัยคดี *Google LLC v CNIL* นั้น CJEU ได้แสดงให้เห็นว่าสิทธิที่จะถูกลืมตามกรอบกฎหมายของสหภาพยุโรปนั้น ไม่ได้กล่าวถึง "ขอบเขตในการบังคับในเชิงพื้นที่" โดยเฉพาะยิ่งในประเด็นที่ว่าคำสั่งให้นำข้อมูลออกจากระบบการสืบค้นนั้นจะมีผลบังคับในประเทศใดบ้าง แม้การนำข้อมูลออกจากระบบ "ควร" จะถูกคุ้มครองในทุกประเทศสมาชิก แต่อย่างไรก็ตาม การคุ้มครองสิทธินี้ก็ยังไม่ได้เป็นอันหนึ่งอันเดียวกันในทุกประเทศ[155] ด้วยเหตุนี้ การคุ้มครองสิทธิในความเป็นส่วนตัวในมิติของการร้องขอให้นำข้อมูลออกจากระบบนั้น จะต้องคำนึงถึงกรอบทางกฎหมายและระดับการคุ้มครองสิทธินี้ในแต่ละประเทศอีกด้วย

เมื่อพิจารณาพัฒนาการทางประวัติศาสตร์ของสิทธิที่จะถูกลืมในสหภาพยุโรปแล้ว ประกอบกับคดีเกี่ยวกับการคุ้มครองสิทธิที่จะถูกลืมซึ่งถูกวินิจฉัยโดย CJEU แล้วกล่าวได้ว่า "สิทธิที่จะถูกลืม" ของเจ้าของข้อมูลส่วนบุคคลนั้นถูกคุ้มครองโดย Directive 95/46/EC ตั้งแต่ก่อนการประกาศใช้ GDPR โดย Directive 95/46/EC ได้กล่าวถึงสิทธิในการขอให้ลบข้อมูล (Erasure) เป็นส่วนหนึ่งของสิทธิเข้าถึงข้อมูล (Right of Access) ต่อมาจึงได้มีการเพิ่มเติมคำว่า "สิทธิที่จะถูกลืม" ในตัวมาตรา 17 ของ GDPR การเพิ่มเติมตัวบทกฎหมายรองรับสิทธิที่จะถูกลืมทำให้สิทธิของเจ้าของข้อมูลส่วนบุคคลนี้มีความชัดเจนในทางเนื้อหามากยิ่งขึ้น เนื่องจากกฎหมายได้บัญญัติถึงรายละเอียดเกี่ยวกับเหตุที่จะต้องมีการลบข้อมูลส่วนบุคคล

---

[154] Ibid, para 59 to 60.

[155] Global Freedom of Expression, 'Google LLC v. National Commission on Informatics and Liberty (CNIL)' (Columbia University, September 2019) <https://globalfreedomofexpression.columbia.edu/cases/google-llc-v-national-commission-on-informatics-and-liberty-cnil/> accessed 3 October 2021.

ตามมาตรา 17 วรรคหนึ่ง และบัญญัติข้อยกเว้นการปฏิเสธที่จะไม่ลบข้อมูลเอาไว้ในมาตรา 17 วรรคสาม โดยระบุถึงการคุ้มครองเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลซึ่งมีลักษณะเช่นเดียวกับมาตรา 33 วรรคหนึ่ง และวรรคสองของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

อย่างไรก็ตาม การบัญญัติรายละเอียดตามมาตรา 17 ของ GDPR นั้นยังไม่เพียงพอต่อการคุ้มครองสิทธิที่จะถูกลืมโดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลส่วนบุคคลนั้นถูกแสดงในระบบการสืบค้นข้อมูลออนไลน์จึงได้มีการออก Guideline 5/2019 นอกจากนี้ การคุ้มครองสิทธิที่จะถูกลืมนั้นยังเผชิญกับความท้าทายในทางปฏิบัติ เช่น การขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลนั้นอาจมีผลเฉพาะต่อ “ผลลัพธ์” ในส่วนของ “ชื่อ” ที่ปรากฏจากการสืบค้นเท่านั้น การลบดังกล่าวไม่ส่งผลให้ต้องมีการลบลิงค์จากดัชนีแสดงผลการค้นหาของระบบสืบค้นทั้งหมด (คดี *Google Spain v AEPD and Mario Costeja González*) ผู้ทรงสิทธิที่จะถูกลืมไม่อาจเรียกให้มีการลบข้อมูลส่วนบุคคลในทะเบียนบริษัท (คดี *Camera di Commercio di Lecce v. Manni*) และการคุ้มครองสิทธิที่จะถูกลืมอาจไม่ได้มีระดับการคุ้มครองเท่าเทียมกันในทุกประเทศ (คดี *Google LLC v CNIL)*

3.3 สหราชอาณาจักร

ในสหราชอาณาจักรมีการประกาศใช้ Data Protection Act 2018 (UK DPA 2018) UK DPA 2018 เป็นการปรับปรุงกฎหมายการคุ้มครองข้อมูลส่วนบุคคลที่จัดทำขึ้นใน ค.ศ. 1998 หรือ Data Protection Act 1998 ต่อมาเมื่อวันที่ 1 มกราคม ค.ศ. 2021 โดย UK DPA 2018 ได้ถูกแก้ไขเพิ่มเติมอีกครั้ง โดยระเบียบภายใต้กฎหมายสหภาพยุโรป (การถอดถอน) ค.ศ. 2018 หรือ European Union (Withdrawal) Act 2018 เพื่อให้สอดคล้องกับสถานะ

ของประเทศอังกฤษที่ ณ ปัจจุบันไม่ได้เป็นรัฐสมาชิกแห่งสหภาพยุโรปแล้ว นอกจากนี้ ประเทศอังกฤษยังได้มีการเพิ่มเติมเรื่อง UK General Data Protection Regulation หรือ “UK GDPR” โดยมีผลใช้บังคับไปเมื่อวันที่ 1 มกราคม พ.ศ. 2564 ไว้ภายใน Chapter 2 ของ Part 2 แห่ง UK DPA 2018

3.3.1 ตัวบทกฎหมายและแนวปฏิบัติ

3.3.1.1 UK Data Protection Act 2018

UK DPA 2018 มีการแบ่งกรอบการคุ้มครองข้อมูลส่วนบุคคลออกเป็น 3 ส่วน ประกอบไปด้วยส่วนที่ 2 (การประมวลผลทั่วไป (UK GDPR)) ส่วนที่ 3 (การประมวลผลเพื่อการบังคับใช้กฎหมาย) และส่วนที่ 4 (การประมวลผลเพื่อบริการด้านข้อมูลข่าวกรอง) โดยใน Part 2 ของ UK DPA 2018 มีวัตถุประสงค์เพื่อเป็นส่วนเสริม GDPR โดยเป็นบทบัญญัติเฉพาะในส่วนที่รัฐสมาชิกมีหน้าที่ในการตีความ และการดำเนินการให้เป็นไปตามบทบัญญัติ (Implementation) นอกจากนี้ ยังมีวัตถุประสงค์เพื่อบังคับใช้ข้อกำหนดที่บัญญัติไว้ใน GDPR ต่อกรณีการประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกเหนือขอบข่ายการประมวลผลที่บัญญัติไว้ใน GDPR ดังนั้น ในส่วนที่ 2 ของ UK DPA 2018 จึงจำเป็นต้องใช้บังคับควบคู่ไปกับ GDPR เมื่อจำต้องพิจารณาถึงกรณีการดำเนินการให้เป็นไปตามข้อกำหนดเรื่องการคุ้มครองข้อมูลส่วนบุคคล

ก่อนการออกจากการเป็นรัฐสมาชิกแห่งสหภาพยุโรปนั้น GDPR ถือเป็นบทบัญญัติที่สร้างกรอบการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลโดยทั่วไปภายในรัฐสมาชิกทั้งหมดที่อยู่ในสหภาพยุโรป โดยที่ GDPR มีผลใช้บังคับกับรัฐสมาชิกโดยตรง โดยที่รัฐสมาชิกทั้งหมดนั้นไม่จำต้องออก

กฎหมายเฉพาะในระดับชาติเพื่อใช้บังคับ GDPR ภายในประเทศของรัฐสมาชิก กรณีดังกล่าวจึงทำให้ UK DPA 2018 ไม่จำต้องทำการ Re-state GDPR เนื่องจาก GDPR นั้นมีผลใช้บังคับภายในประเทศอังกฤษในทุกกรณีอยู่แล้ว[156]

UK DPA 2018 ได้กำหนดให้สิทธิในการลบข้อมูลส่วนบุคคลของเจ้าของข้อมูลต่อข้อมูลที่ถูกประมวลผลเพื่อวัตถุประสงค์ในการบังคับใช้กฎหมายที่แตกต่างไปจากข้อกำหนดเรื่องสิทธิดังกล่าวตาม GDPR โดยตามมาตรา 47 แห่ง UK DPA 2018 ได้กำหนดถึงกรณีการลบข้อมูลส่วนบุคคลเอาไว้เฉพาะว่า ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องลบข้อมูลส่วนบุคคลโดยไม่ล่าช้า[157] หากว่าการประมวลผลข้อมูลส่วนบุคคลนั้นฝ่าฝืนต่อหลักการคุ้มครองข้อมูลส่วนบุคคลที่ 1 - 5[158] หรือผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติให้เป็นไปตามกฎหมาย[159]

อย่างไรก็ตาม ในกรณีที่ผู้ควบคุมข้อมูลจะทำการลบข้อมูลส่วนบุคคล แต่ปรากฏว่าข้อมูลนั้นจำต้องถูกเก็บรักษาไว้เพื่อวัตถุประสงค์ของพยานหลักฐาน ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการระงับการประมวลผลข้อมูลส่วนบุคคลนั้นแทนการลบ[160] นอกจากนี้ หากเจ้าของข้อมูลส่วนบุคคลทำการโต้แย้งต่อความถูกต้องของข้อมูล ไม่ว่าจะเป็นการโต้แย้งโดยการ

---

[156] ICO, 'An Overview of Data Protection Act 2018, Part 2, Data Protection Act – General processing' (ICO, 2018) <https ://ico.org.uk/ media/for-organisations/documents/2614158/ico-introduction-to-the-data-protection-bill.pdf> accessed 3 October 2021.

[157] กฎหมายใช้ถ้อยคำว่า "The controller must erase personal data without undue delay..."

[158] Data Protection Act 2018, Section 35, 36 (1) to (3), 37, 38 (1), 39 (1), 40, 41 or 42.

[159] Ibid, มาตรา 47 (1).

[160] Ibid, มาตรา 47 (2).

ส่งคำร้องขอให้ลบหรือร้องขอให้ทำการแก้ไขข้อมูล หรือด้วยวิธีการอื่นใด แต่ไม่สามารถทำให้มั่นใจได้ว่าข้อมูลนั้นถูกต้องหรือไม่ ผู้ควบคุมข้อมูลต้องระงับการประมวลผลข้อมูลส่วนบุคคลนั้น[161] ทั้งนี้ เจ้าของข้อมูลส่วนบุคคลอาจทำการร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการลบข้อมูลส่วนบุคคลหรือให้ทำการระงับการประมวลผลข้อมูลได้ ทั้งนี้ หน้าที่ในการลบข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลยังคงมีอยู่หากเข้าข่ายตามกรณีที่กำหนดข้างต้น แม้ว่าเจ้าของข้อมูลส่วนบุคคลจะได้ทำการร้องขอไว้เช่นนั้น[162]

ส่วนที่ 4 ของ UK DPA 2018 ได้ระบุเรื่องการประมวลผลของหน่วยงานบริการข้อมูลข่าวกรอง (Intelligence Services Processing) ไว้เพิ่มเติมจาก GDPR ซึ่งการประมวลผลข้อมูลเพื่อการบริการข้อมูลข่าวกรองนี้เป็นการประมวลผลข้อมูลส่วนบุคคลโดยหน่วยงานบริการข้อมูลข่าวกรอง ซึ่งได้แก่ หน่วยงานบริการด้านความมั่นคงปลอดภัย (Security Service) หน่วยงานบริการด้านข้อมูลข่าวกรองลับ (Secret Intelligence Service) และสำนักงานการติดต่อสื่อสารรัฐบาล (Government Communications Headquarters)[163] ซึ่งทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล[164] ทั้งนี้ การประมวลผลข้อมูลส่วนบุคคลของหน่วยงานดังกล่าว ต้องมีลักษณะเป็นการประมวลผลข้อมูลโดยวิธีการอัตโนมัติ (Automated Means) ที่เป็นการกระทำเพื่อสร้างระบบไฟล์ข้อมูล (Filing System)[165]

---

[161] Ibid, มาตรา47 (3).

[162] Ibid, มาตรา 47 (4).

[163] Ibid, มาตรา82 (2).

[164] Ibid, มาตรา 83.

[165] Ibid, มาตรา 82 (1).

ภายใต้ส่วนที่ 4 นี้ได้มีการกำหนดให้สิทธิในการขอให้ลบข้อมูลส่วนบุคคลเฉพาะกับกรณีการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านบริการข้อมูลข่าวกรองเช่นเดียวกัน โดยต้องปรากฏกรณีว่า หากกรณีเป็นที่พอใจแก่ศาล[166] ว่าการประมวลผลข้อมูลส่วนบุคคลที่ร้องขอตามคำร้องของเจ้าของข้อมูลส่วนบุคคลนั้นมีลักษณะเป็นการฝ่าฝืนต่อมาตรา 86 ถึง 91 ศาลอาจออกคำสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบข้อมูลส่วนบุคคลนั้นโดยไม่ล่าช้าได้[167] หรือหากเป็นกรณีที่ข้อมูลส่วนบุคคลนั้นจำต้องถูกเก็บรักษาไว้เพื่อวัตถุประสงค์ของพยานหลักฐาน ศาลอาจออกคำสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลนั้นระงับการประมวลผลข้อมูลส่วนบุคคลดังกล่าวโดยไม่ล่าช้า แทนการออกคำสั่งให้ลบข้อมูลส่วนบุคคลนั้นได้[168] หรือเป็นกรณีที่เจ้าของข้อมูลได้โต้แย้งว่าข้อมูลส่วนบุคคลนั้นไม่ถูกต้อง และกรณีเป็นที่พอใจแก่ศาลว่าผู้ควบคุมข้อมูลส่วนบุคคลนั้น ไม่สามารถทำให้แน่ใจได้ว่าข้อมูลนั้นถูกต้องหรือไม่ ศาลอาจออกคำสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลนั้นระงับการประมวลผลข้อมูลส่วนบุคคลดังกล่าวโดยไม่ล่าช้าแทนการออกคำสั่งให้ลบข้อมูลส่วนบุคคลนั้นได้[169] ทั้งนี้ศาลมีอำนาจออกคำสั่งดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลร่วมที่มีหน้าที่รับผิดชอบต่อการลบข้อมูลส่วนบุคคลนั้นด้วย[170]

---

[166] Ibid, มาตรา 100 (6) เฉพาะศาลสูง หรือศาลสูงในสก็อตแลนด์โดยศาลแพ่ง (Court of Session).

[167] Ibid, มาตรา 100 (2).

[168] Ibid, มาตรา 100 (3).

[169] Ibid, มาตรา 100 (4).

[170] Ibid, มาตรา 100 (5).

3.3.1.2 แนวปฏิบัติของของสำนักงานคณะกรรมการคุ้มครองข้อมูล

สำนักงานคณะกรรมการคุ้มครองข้อมูล (ICO) ได้จัดทำแนวปฏิบัติที่เกี่ยวข้องกับวิธีการลบข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นองค์กรสามารถยึดถือเป็นแนวทางในการปฏิบัติให้เป็นตามข้อกำหนดเรื่องการลบข้อมูลส่วนบุคคลได้[171] แนวทางดังกล่าวยังรวมไปถึงเรื่องการจัดเก็บข้อมูลส่วนบุคคลไว้ในคลังข้อมูลจดหมายเหตุ ซึ่งเป็นการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลข้อที่ 5 ที่กำหนดให้ข้อมูลส่วนบุคคลที่ถูกประมวลผลเพื่อวัตถุประสงค์ใดไม่จำต้องถูกเก็บรักษาไว้นานเกินกว่าที่จำเป็นเพื่อวัตถุประสงค์นั้น

(1) ลักษณะของการลบข้อมูล

แนวปฏิบัติฉบับดังกล่าวได้อธิบายคำว่า “Delete” หรือ “Deletion” ว่าหมายถึงการทำลาย (Destruction) โดยภายในประมวลว่าด้วยข้อมูลส่วนบุคคลออนไลน์ของ ICO ได้ระบุว่าถือเป็นการปฏิบัติที่ดีในการกำหนดให้ชัดเจนว่าจะเกิดอะไรขึ้นกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบ้างเมื่อเจ้าของข้อมูลได้ทำการเปิดบัญชีหากว่าข้อมูลส่วนบุคคลนั้นจะต้องถูกลบโดยไม่สามารถกู้คืนกลับมาได้ หรือเพียงยุติการใช้งาน (Deactivate) หรือจัดเก็บข้อมูลส่วนบุคคลไว้ในคลังข้อมูล (Archive) อย่างไรก็ตามแม้ว่าจะมีการจัดเก็บข้อมูลส่วนบุคคลไว้ในคลังข้อมูล (Archive) การจัดเก็บดังกล่าวยังคงต้องปฏิบัติให้เป็นไปตามกฎระเบียบด้านการคุ้มครองข้อมูลส่วนบุคคล รวมไปถึงการที่เจ้าของข้อมูลส่วนบุคคลยังคงมีสิทธิในการเข้าถึง

[171] ICO, ‘Deleting personal data’ (ICO, February 2014) <https ://ico.org.uk/media/for-organisations/documents/1475/deleting_ personal_data.pdf> accessed 3 October 2021.

ข้อมูลส่วนบุคคลนั้นได้อยู่ หากผู้ควบคุมข้อมูลส่วนบุคคลเสนอให้มีการลบข้อมูลที่สามารถระบุตัวตนได้ซึ่งเจ้าของข้อมูลได้ทำการอัพโหลดไว้ หากจะจัดให้มีการลบข้อมูลส่วนบุคคล ก็ต้องเป็นการลบข้อมูลส่วนบุคคลสามารถเกิดขึ้นได้จริงโดยที่เนื้อหานั้นไม่ควรต้องสามารถถูกกู้คืนกลับมาได้ (Recoverable) ไม่ว่ากรณีใดก็ตาม อย่างไรก็ตาม การทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจว่าการลบข้อมูลส่วนบุคคลนั้นเป็นการลบข้อมูลส่วนบุคคลทิ้งโดยสมบูรณ์ ในขณะที่ความเป็นจริงไม่เป็นเช่นนั้น กรณีดังกล่าวนี้จะถือว่าเป็นการปฏิบัติที่ไม่ดี[172]

แนวปฏิบัติฉบับนี้ระบุว่า ผู้ควบคุมข้อมูลควรจะต้องแจ้งต่อเจ้าของข้อมูลส่วนบุคคลให้ชัดแจ้งว่าการลบข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลนั้นหมายถึงอะไร และจะเกิดอะไรขึ้นเมื่อข้อมูลส่วนบุคคลนั้นได้ถูกลบออกไปแล้ว ทั้งนี้แนวปฏิบัติฯ ฉบับนี้มีจุดมุ่งหมายเพื่อแก้ไขปัญหาที่ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งต่อเจ้าของข้อมูลส่วนบุคคลว่า ข้อมูลส่วนบุคคลนั้นได้ถูกลบออกไปแล้ว ในขณะที่ความเป็นจริงแล้ว ข้อมูลส่วนบุคคลดังกล่าวยังคงถูกเก็บไว้ในคลังเก็บข้อมูลหรือเป็นสามารถถูกกู้คืนกลับมาได้อีกครั้ง (Re-Instate) โดยมุ่งเน้นให้ผู้ควบคุมข้อมูลส่วนบุคคลนั้นต้องจัดให้มีแนวทางการปกป้องข้อมูลส่วนบุคคลที่ถูกลบแต่ในความเป็นจริงแล้วข้อมูลส่วนบุคคลดังกล่าวยังคงอยู่ในความครอบครองของผู้ควบคุมข้อมูลส่วนบุคคลนั้นเอง โดยแนวปฏิบัติฉบับนี้[173]

การลบข้อมูลส่วนบุคคลโดยที่ไม่สามารถกู้คืนข้อมูลกลับมาได้ (Irretrievably) หรือการเก็บข้อมูลไว้ในคลังข้อมูลในลักษณะที่เป็นระบบ (Structure) และสามารถกู้คืนข้อมูลกลับมาได้ หรือการเก็บรักษาข้อมูลโดยทำให้เป็นข้อมูลประเภทอิสระ (Freedom) ไว้ในตะกร้าขยะอิเล็กทรอนิกส์ (Electronic Wastebasket) นั้นมีความแตกต่างกันโดยสิ้นเชิง

[172] Ibid, p. 3.

[173] Ibid, p. 4.

การเก็บในคลังข้อมูลต้องปฏิบัติให้เป็นไปตามกฎระเบียบเรื่องการคุ้มครองข้อมูลส่วนบุคคล โดยให้ถือว่าเป็นข้อมูลที่ยังมีความเคลื่อนไหวอยู่ ถึงแม้ว่าข้อมูลดังกล่าวแทบจะไม่มีความเคลื่อนไหวเลยก็ตาม และมีความเป็นไปได้ต่ำที่จะเกิดผลกระทบที่ไม่เป็นธรรมหรือเสียหายต่อเจ้าของข้อมูลส่วนบุคคล เมื่อเปรียบเทียบกับข้อมูลที่ยังคงมีความเคลื่อนไหวอยู่

อย่างไรก็ตาม ICO นั้นจะปรับใช้แนวทางการจัดการกับกรณีดังกล่าวโดยที่รับรู้ว่าการลบข้อมูลออกจากระบบนั้นไม่จำเป็นต้องเป็นการลบโดยตรงเสมอไป และอาจมีการทำให้ข้อมูลนั้นเป็นข้อมูลที่อยู่เหนือการใช้งาน (Put Beyond Use) โดยที่ต้องจัดให้มีแนวทางการคุ้มครองข้อมูลส่วนบุคคลด้วย เช่น

- กรณีที่ข้อมูลนั้นถูกลบโดยที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่มีเจตนาที่จะใช้ หรือเข้าถึงข้อมูลนั้นอีก แต่ข้อมูลยังคงมีอยู่ในระบบอิเล็กทรอนิกส์ เช่น ในกรณีที่เป็นข้อมูลที่รอการเขียนทับ (Over-Written) ด้วยข้อมูลอื่น ซึ่งในกรณีนี้ข้อมูลดังกล่าวไม่ถือว่ามีความเคลื่อนไหว (Live) อีกต่อไป ดังนั้น ปัญหาด้านการปฏิบัติให้เป็นไปตามการคุ้มครองข้อมูลส่วนบุคคลจึงหมดไป (ในกรณีที่คล้ายคลึงกันนี้อาจเป็นกรณีของถุงกระดาษขยะที่ถูกบดทำลาย แม้ว่ามีความเป็นไปได้ว่ากระดาษที่ถูกบดทำลายเป็นส่วน ๆ ไปแล้วนั้นจะสามารถถูกนำกลับมาเรียงต่อกันให้เป็นแผ่นกระดาษสมบูรณ์ดังเดิม (Re-Constitute) ได้ แต่เป็นกรณีที่เป็นได้ยากและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีเจตนาให้เป็นเช่นนั้น)

- กรณีที่ข้อมูลส่วนบุคคลควรจำต้องถูกลบทิ้งแต่ในความเป็นจริงแล้วข้อมูลนั้นถูกเก็บไว้ในระบบที่มีความเคลื่อนไหวอยู่ เนื่องจากเหตุผลทางเทคนิค และเป็นไปไม่ได้ที่จะลบข้อมูลนั้น

ทิ้งโดยไม่เป็นการลบข้อมูลอื่นที่ถูกบรรจุอยู่ในแหล่งเก็บเดียวกันทิ้งไปด้วย ซึ่งในกรณีดังกล่าวนี้อาจเป็นกรณีที่กฎหมายกำหนดอนุญาตเพียงให้สามารถใช้ข้อมูลนั้นในลักษณะเดียวกันกับการใช้ข้อมูลที่มีความเคลื่อนไหวอยู่ ซึ่งในกรณีดังกล่าวนี้อาจเกิดขึ้นเมื่อมีคำสั่งของศาลให้ดำเนินการลบข้อมูลที่เกี่ยวข้องกับบุคคลแต่ไม่สามารถลบข้อมูลที่เกี่ยวข้องกับบุคคลดังกล่าวโดยไม่เป็นการลบข้อมูลของบุคคลอื่นที่ถูกบรรจุอยู่ในแหล่งเก็บเดียวกันทิ้งไปด้วยได้

นอกจากกรณีของการลบข้อมูลส่วนบุคคลแล้ว ยังมีแนวทางอื่นการจัดการกับการลบข้อมูลในรูปแบบอื่นดังเช่นในการทำให้ข้อมูลอยู่เหนือการใช้งาน แนวปฏิบัติฉบับนี้ระบุให้การทำให้ข้อมูลอยู่เหนือการใช้งาน หากว่าข้อมูลดังกล่าวไม่ได้ถูกลบออกไปจริง และจำต้องเป็นกรณีที่ปรากฏด้วยว่าผู้ควบคุมข้อมูลส่วนบุคคลนั้นได้ปฏิบัติให้เป็นไปกรณีดังนี้[174]

- ไม่สามารถ หรือจะไม่พยายามใช้ข้อมูลส่วนบุคคลเพื่อแจ้งให้ทราบถึงการตัดสินใจใด ๆ ที่เกี่ยวข้องกับบุคคลใด ๆ หรือในลักษณะที่ส่งผลต่อบุคคลใด ๆ และไม่ว่าด้วยวิธีใดก็ตาม
- ไม่อนุญาตให้หน่วยงานอื่นใดสามารถเข้าถึงข้อมูลส่วนบุคคลนั้นได้
- จัดให้มีความมั่นคงปลอดภัยทางด้านเทคนิค และด้านการบริหารจัดการ และ
- ให้คำมั่นว่าจะลบข้อมูลนั้นทิ้งอย่างถาวร เมื่อหรือหากสามารถดำเนินการเช่นนั้นได้

[174] Ibid, p. 5.

ทั้งนี้ ICO จะไม่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลส่วนบุคคลของตนได้ หากว่าผู้ควบคุมข้อมูลส่วนบุคคลสามารถดำเนินการให้เป็นไปตามกรณีทั้ง 4 กรณีข้างต้น รวมถึงไม่ดำเนินการใด ๆ ต่อการปฏิบัติให้เป็นไปตามหลักการคุ้มครองข้อมูลส่วนบุคคลข้อที่ 5 อีกด้วยหากว่าผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิบัติให้เป็นไปตามกรณีข้างต้นทั้งหมดได้ อย่างไรก็ตามการทำให้ข้อมูลอยู่เหนือการใช้งานนั้น อาจเกิดกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลยังคงมีหน้าที่ที่ต้องปฏิบัติให้เป็นไปตามคำสั่งของศาล เมื่อศาลมีคำสั่งขอข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลใด ๆ ดังนั้นผู้ควบคุมข้อมูลส่วนบุคคลจึงควรต้องเสาะหาวิธีการทางเทคนิคที่จะช่วยป้องกันปัญหาเรื่องการลบข้อมูลที่อาจเกิดขึ้นในอนาคตอีกด้วย[175]

3.2.2 กรณีศึกษา

ในปี ค.ศ. 2018 ศาล CJEU ได้มีคำพิพากษาตัดสินในคดี *NT1 & NT2 v Google LLC* ที่ได้มีคำสั่งให้ Google นำข้อมูลเกี่ยวกับการได้รับโทษ (ที่สิ้นสุดแล้ว) ของนักธุรกิจรายหนึ่ง (NT2) ออกจากผลแสดงการสืบค้น แต่กลับปฏิเสธคำขอของนักธุรกิจอีกรายหนึ่ง (NT1)[176] NT1 และ NT2 เป็นบุคคลธรรมดาที่ไม่มีความเกี่ยวข้องเชื่อมโยงกันมาก่อน ทั้งสองได้นำคดีมาสู่ศาลโดยกล่าวหาว่า Google LLC นั้นปฏิเสธการลบข้อมูลที่ปรากฏบนผลแสดงการสืบค้นที่ Google LLC เป็นผู้ให้บริการอยู่ ซึ่งข้อมูลที่ปรากฏนั้นเป็นข้อมูลที่เกี่ยวข้องกับผู้ร้องทั้งสองเรื่องการต้องโทษจำคุกสืบเนื่องจาก

---

[175] Ibid.

[176] Global Freedom of Expression, 'NT1 and NT2 v. Google LLC' (Columbia University, April 2018) <https ://globalfreedomof expression.columbia.edu/cases/nt1-nt2-v-google-llc/> accessed 3 October 2021.

คำพิพากษาลงโทษในคดีอื่นซึ่งเกิดขึ้นเมื่อประมาณ ค.ศ. 1990 และประมาณ ค.ศ. 2001 NT2 ได้ถูกตัดสินว่ามีความผิดในคดีอาญาเกี่ยวกับธุรกิจของ NT2

ผู้ร้องทั้งสองได้ยื่นคำร้องไปยัง Google LLC เพื่อให้ทำการนำเอาลิงค์ที่มีข้อมูลการรายงานข่าวจากสื่อต่าง ๆ รวมถึงที่ถูกรายงานบนหนังสือพิมพ์ภายในประเทศถึงเรื่องคำพิพากษาของศาลในคดีก่อนนั้นออกจากผลแสดงการสืบค้นของ Google LLC ทั้งนี้ โดยอ้างว่าในข้อมูลที่ปรากฏบนผลการสืบค้นนั้นประกอบไปด้วยข้อมูลของบุคคลภายนอกที่มีลักษณะไม่ถูกต้องอีกด้วย[177] อย่างไรก็ตาม Google LLC กลับปฏิเสธคำร้องขอให้นำเอาลิงค์ดังกล่าวออกของผู้ร้องทั้งสอง ทำให้ผู้ร้องทั้งสองทำการยื่นเรื่องฟ้องร้องไปยังศาลภายใต้กฎหมาย Data Protection Act 1998 (DPA 1998) ในข้อหาใช้ข้อมูลส่วนบุคคลไปในทางที่ผิด (Misuse) เพื่อร้องขอให้ศาลมีคำสั่งไปยัง Google LLC ให้ทำการลบลิงค์ที่ปรากฏข้อมูลส่วนบุคคลของผู้ร้อง รวมไปถึงเรื่องค่าเสียหายต่อกรณีที่เกิดขึ้นนั้นด้วย

ศาลมีคำสั่งให้ Google LLC นำเอาข้อมูลเกี่ยวกับรับโทษของ NT2 ออกจากระบบการสืบค้นแต่ปฏิเสธคำขอให้นำข้อมูลของ NT1 ออกจากระบบการสืบค้น โดยทั้ง NT1 และ NT2 นั้น ต่างถูกลงโทษทางอาญาจากการกระทำความผิดเมื่อหลายปีก่อนแต่ข้อมูลเกี่ยวกับการถูกลงโทษนั้นยังถูกแสดงผ่านระบบการสืบค้นของ Google NT1 และ NT2 อ้างว่าการแสดงข้อมูลดังกล่าว “คลาดเคลื่อน (Inaccurate)” และ/หรือ “ล้าสมัย (Old)” “ไม่เกี่ยวข้อง (Irrelevant)” และ “ไม่ก่อประโยชน์สาธารณะ” อันใด หรือมิฉะนั้นก็เป็นการล่วงล้ำสิทธิของผู้ร้องโดยปราศจากความชอบธรรม ซึ่ง CJEU ได้วินิจฉัยคำร้องของ NT1 และ NT2 ดังนี้

[177] NT1 & NT2 v Google LLC, para 1 ถึง 2.

(1) ส่วนของ NT 1

ข้อมูลของ NT1 ที่เกี่ยวกับการกระทำความผิดอาญาและการได้รับการลงโทษนั้น ไม่ใช่ข้อมูลที่ลักษณะเป็นข้อมูลส่วนบุคคล เนื่องจากเป็นข้อมูลที่เกี่ยวข้องอาชญากรรมทางธุรกิจ อีกทั้งผู้ร้อง NT1 ยังคงจำกัดบทบาทหน้าที่ในชีวิตสาธารณะของตนทั้งไม่แสดงว่าข้อมูลเป็นข้อมูลที่ไม่ถูกต้องอย่างไร[178] แม้คำร้องของผู้ร้อง NT1 จะได้ระบุให้เห็นถึงเหตุผลอันชอบธรรมในการนำลิงค์ข้อมูลออกจากการแสดงผล แต่ผู้ร้อง NT1 ยังคงไม่สามารถแสดงหลักฐานที่สามารถพิสูจน์หักล้างเพื่อสนับสนุนเหตุผลอันชอบธรรมดังกล่าวได้ ซึ่งในคำร้องนั้นระบุเพียงความเสียหายที่เกี่ยวข้องกับธุรกิจเท่านั้น[179] และบางเหตุผลนั้นเป็นเรื่องที่เกิดขึ้นก่อนที่ผู้ร้อง NT1 จะมีสิทธิในการร้องเรียนโดยชอบธรรมเกี่ยวกับการประมวลผลข้อมูลของ Google LLC ได้ ซึ่งข้อมูลพิพาทนั้นเป็นข้อมูลเกี่ยวกับอาชญากรรมและการพิจารณาของศาล ซึ่งถูกเผยแพร่รายงานผ่านหนังสือพิมพ์ภายในประเทศ ข้อมูลพิพาทดังกล่าวถือเป็นเรื่องที่อาจคาดการณ์ถึงผลลัพธ์เรื่องพฤติกรรมที่เกี่ยวข้องกับอาชญากรรมของ NT1 ได้อยู่แล้ว ทั้งภายหลังจากพ้นโทษในคดีก่อน NT1 ยังคงกลับเข้ามาทำงานในแวดวงธุรกิจที่ NT1 เคยทำอยู่ก่อนหน้าที่ศาลจะพิพากษาให้ NT1 มีความผิดเกี่ยวกับธุรกิจของ NT1 ทำให้เห็นได้ว่าข้อมูลพิพาทดังกล่าวเป็นข้อมูลที่เป็นประโยชน์ต่อวัตถุประสงค์เพื่อลดความเสี่ยงที่ว่า ผู้ร้อง NT1 อาจยังคงไม่สำนักผิดและยังคงมีพฤติกรรมเดิมตามที่ผู้ร้อง NT1 เคยต้องโทษจากการกระทำนั้นในอดีต ประกอบกับการที่ผู้ร้องมีส่วนเกี่ยวข้องกับคดีแพ่งหลายคดี ศาลจึงพิจารณาว่ากรณีดังกล่าวนี้ข้อมูลที่ว่าผู้ร้อง NT1 เคยถูกพิพากษาให้ได้รับโทษนั้นยังมีความเกี่ยวพันกับชีวิตในการทำงานของผู้ร้อง[180] ดังนั้น ข้อมูลพิพาทดังกล่าวจึงควร

[178] Ibid, para 170.

[179] Ibid.

[180] Ibid.

จำต้องมีอยู่เพื่อประโยชน์สาธารณะ ด้วยเหตุนี้ ประโยชน์อันชอบธรรมของ Google LLC ในการประมวลผลข้อมูลส่วนบุคคลของผู้ร้อง NT1 จึงมีอยู่เหนือกว่าสิทธิที่จะถูกลืมของผู้ร้อง NT1

(2) ส่วนของ NT 2

ในขณะที่ข้อมูลพิพาทตามข้ออ้างเรื่องการนำข้อมูลออกจากการแสดงผลของ NT2 มีลักษณะที่เป็นข้อมูลอาชญากรรมและการลงโทษที่เกี่ยวข้องกับผู้ร้อง NT2 ซึ่งในระยะเวลาต่อมาได้กลายมาเป็นข้อมูลที่สิ้นอายุไม่เกี่ยวพัน และไม่มีเหตุผลอันชอบธรรมต่อผู้ใช้งานระบบการสืบค้นข้อมูลของ Google LLC ที่เพียงพอที่ทำให้การยังคงแสดงผลข้อมูลพิพาทดังกล่าวสามารถมีอยู่ได้ต่อไปโดยชอบด้วยกฎหมาย[181] การพิจารณาลงโทษของศาลนั้นย่อมสามารถคาดการณ์ได้ว่า NT2 จำต้องได้รับโทษอย่างแน่นอนและในความเป็นจริง NT2 ก็ได้รับโทษเช่นนั้นจริงใน ค.ศ. 2014 อีกทั้ง NT2 รับสารภาพว่าตนเป็นผู้กระทำความผิดและแสดงให้เห็นว่าตนสำนึกในการกระทำความผิดนั้นอย่างแท้จริง และมีข้อเท็จจริงว่าข้อมูลพิพาทนี้มีแนวโน้มที่จะส่งผลกระทบไปยังผู้เยาว์ซึ่งเป็นบุตรของ NT2 อีกด้วย ทำให้ไม่อาจมีความเสี่ยงในเรื่องการกระทำความผิดซ้ำได้อีก อีกทั้ง การประกอบธุรกิจของผู้ร้อง NT2 ในปัจจุบันอยู่ในประเภทธุรกิจที่ค่อนข้างแตกต่างไปจากธุรกิจเดิมที่ผู้ร้อง NT2 เคยต้องโทษว่ามีความผิดจากคดีก่อนทำให้ไม่มีความจำเป็นที่จำต้องเตือนให้บุคคลทั่วไปได้ทราบถึงกิจกรรมดังกล่าวของผู้ร้อง NT2[182]

ในการวินิจฉัยคำร้องของ NT1 และ NT2 นั้น CJEU ได้ตัดสินโดยใช้หลักการชั่งน้ำหนักระหว่างสิทธิความเป็นส่วนบุคคลกับสิทธิในการแสดงออก ศาลได้พิจารณาโดยใช้ปัจจัยที่ถือเป็นหลักการคุ้มครอง

[181] Ibid, para 223.

[182] Ibid.

ข้อมูลส่วนบุคคล อันได้แก่ ความถูกต้องของข้อมูล (Accuracy) ความเกี่ยวพันของข้อมูล (Relevance) และความอ่อนไหวของข้อมูล รวมไปถึงบทบาทหน้าที่ของผู้ร้องในชีวิตสาธารณะของผู้ร้อง[183] ที่ก่อให้ความเสียหายต่อผู้ร้องทั้งสอง หากว่าข้อมูลพิพาทนั้นยังคงถูกประมวลผลอยู่และตราบเท่าที่ข้อมูลพิพาทนั้นยังคงเป็นไปเพื่อประโยชน์สาธารณะ

เมื่อพิจารณาตัวบทกฎหมาย UK DPA 2018 แล้วจะเห็นได้ว่ากฎหมายของสหราชอาณาจักรนั้นไม่ได้รับรองถึงคำว่า “สิทธิที่จะถูกลืม” เอาไว้ดังเช่นมาตรา 17 ของ GDPR ซึ่งเป็นแนวทางที่คล้ายคลึงกับมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย อย่างไรก็ตาม มาตรา 47 (1) ของ UK DPA 2018 นั้น บัญญัติให้ผู้ควบคุมข้อมูลมีหน้าที่ต้องลบข้อมูล “โดยไม่ชักช้า (Undue Delay)” และบัญญัติรับรองสิทธิในการลบข้อมูลในมาตรฐานเดียวกับสิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล อย่างไรก็ตาม มาตรา 47 ของ UK DPA 2018 นี้มิได้บัญญัติถึงการปฏิเสธไม่ลบข้อมูลในกรณีจำเป็นต้องคุ้มครองเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลดังเช่นกรณีเดียวกับมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อย่างไรก็ตาม การคุ้มครองสิทธิในการลบข้อมูลส่วนบุคคลในสหราชอาณาจักรนั้น ถูกรับรองไว้ภายในแนวการปฏิบัติโดย ICO ซึ่งได้ออกแนวปฏิบัติที่เกี่ยวข้องกับวิธีการลบข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นองค์กรสามารถยึดถือเป็นแนวทางในการปฏิบัติให้เป็นตามข้อกำหนดเรื่องการลบข้อมูลส่วนบุคคลได้ นอกจากนี้ คดี *NT1 & NT2 v Google LLC* ยังแสดงให้เห็นว่าการพิจารณาว่าผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์นั้น อาจมีประโยชน์อันชอบธรรมของ Google LLC ในการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลได้ (ในส่วนของ NT1)

---

[183] Ibid, para 37.

3.4 ประเทศออสเตรเลีย

รัฐธรรมนูญของประเทศออสเตรเลีย ไม่ได้บัญญัติรับรองสิทธิในความเป็นส่วนตัวเอาไว้ในตัวบทกฎหมาย แต่ก็ไม่ได้หมายความว่าระบบกฎหมายของประเทศออสเตรเลียจะไม่คุ้มครองสิทธิในความเป็นส่วนตัวเสียทีเดียว[184] กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศออสเตรเลียนั้นถูกบัญญัติขึ้นครั้งแรกใน ค.ศ. 1988 โดยมีชื่อเรียกว่า Privacy Act 1988 (“AUS PA 1988”) หรือกฎหมายความเป็นส่วนบุคคลและหลักการความเป็นส่วนตัวออสเตรเลีย (Australian Privacy Principles : APP) โดยมี Australian Government Office of the Australian Information Commissioner (OAIC) ซึ่งเป็นคณะกรรมการที่มีอำนาจหน้าที่ในการกำกับดูแลเรื่องความเป็นส่วนบุคคลภายในประเทศออสเตรเลีย

3.4.1 ตัวบทกฎหมายและแนวปฏิบัติ

3.4.1.1 Privacy Act 1988

AUS PA 1988 กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการจัดการกับข้อมูลส่วนบุคคลที่มีความสอดคล้องกับ GDPR อยู่ส่วนหนึ่ง ซึ่งได้แก่ สิทธิที่จะได้รับการแจ้ง (Right to be Informed) สิทธิในการเข้าถึง (Right to Access) สิทธิในการแก้ไขให้ถูกต้อง (Right to Rectification) สิทธิในการคัดค้านหรือถอนความยินยอม (Right to Object/Opt Out) สิทธิในการโอนย้ายข้อมูล (Right to Data Portability) สิทธิในการร้องเรียน

[184] Parliament of Australia, ‘Do Australians have a legal right to privacy?’ (Department of Parliamentary Services, March 2005) <https ://parlinfo.aph.gov.au/parlInfo/download/library/prspub/CBHF6/upload_binary/cbhf64.pdf;fileType=application%2Fpdf#search=%22library/prspub/CBHF6%22> accessed 3 October 2021.

(Right to Complaint) สิทธิในการไม่ระบุตัวตน อย่างไรก็ตาม ไม่ปรากฏว่ากฎหมายบัญญัติถึงสิทธิที่จะถูกลืม (Right to be Forgotten) หรือสิทธิในการลบข้อมูล (Right to Erasure) เอาไว้

แม้ไม่ปรากฏว่าสิทธิที่จะถูกลืมหรือสิทธิในการลบข้อมูลได้ถูกกำหนดไว้ภายใต้ AUS PA 1988 แต่ตามกฎหมายฉบับนี้ก็ได้กำหนดหน้าที่แก่ผู้ควบคุมข้อมูลส่วนบุคคลให้ “ทำลาย” ข้อมูลส่วนบุคคลเอาไว้เป็นการเฉพาะ เช่น องค์กรที่ทำหน้าที่รายงานข้อมูลด้านเครดิต (Credit Reporting Entity) มีหน้าที่ในการทำลายข้อมูลการรายงานด้านเครดิตและให้แจ้งเจ้าของข้อมูลทราบถึงการทำลายอีกด้วย[185]

การทำลาย (Destroy) และการทำข้อมูลให้กลายเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตน (De-Identification) ได้ภายใต้ AUS PA 1988 นี้ จึงอาจสามารถเทียบเคียงได้กับกรณีการใช้สิทธิที่จะถูกลืมหรือสิทธิในการลบข้อมูลของเจ้าของข้อมูลส่วนบุคคลตามกรอบของ GDPR และ UK DPA 2018 (ตลอดจนมาตรา 33 และ 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

3.4.1.2 แนวทางการปฏิบัติเกี่ยวหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศออสเตรเลีย

OAIC ได้กล่าวถึงการทำลายและการทำให้ข้อมูลกลายเป็นข้อมูลที่บ่งชี้ตัวตนไม่ได้ว่าเป็นส่วนหนึ่งของมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Security of Personal Information) โดยระบุว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องใช้ความพยายามตามสมควรในการ

[185] Privacy Act 1988, มาตรา 20 Y (2) โดยกฎหมายใช้ถ้อยคำว่า “The credit reporting body must : (a) destroy the credit reporting information...”

ทำลายหรือทำให้ข้อมูลกลายเป็นข้อมูลที่บ่งชี้ตัวตนไม่ได้เมื่อหมดความจำเป็นที่จะต้องครอบครองข้อมูลนั้น[186]

(1) การทำลายข้อมูลส่วนบุคคล (Destroying Personal Information)

การทำลายข้อมูลส่วนบุคคลนั้น อาจกระทำได้เมื่อข้อมูลนั้นไม่มีความจำเป็นในการกู้คืนข้อมูลกลับมาอีกแล้ว (Retrieve) วิธีการทำลายข้อมูลส่วนบุคคลจะขึ้นอยู่กับรูปแบบของแหล่งเก็บข้อมูล ได้แก่ ข้อมูลที่ถูกเก็บไว้ในรูปแบบของกระดาษหรือเอกสาร (Hard Copy) การทิ้งลงถังขยะหรือรีไซเคิลเอกสารหรือกระดาษซึ่งมีข้อมูลส่วนบุคคลนั้น ไม่ถือเป็นการดำเนินการที่เหมาะสมในการทำลายข้อมูลส่วนบุคคล เว้นแต่ว่าข้อมูลส่วนบุคคลนั้นจะได้ถูกทำลายผ่านกระบวนการ เช่น การทำให้เป็นเยื่อกระดาษ (Pulping) การเผาทำลาย (Burning) การย่อยหรือการบด (Pulverizing) การทำให้สลายหรือละลาย (Disintegrating) หรือการบดทำลาย (Shredding)[187]

สำหรับข้อมูลที่ถูกเก็บไว้ในรูปแบบอิเล็กทรอนิกส์ การดำเนินการที่เหมาะสมจะขึ้นอยู่กับประเภทของฮาร์ดแวร์ที่ใช้เก็บรักษาข้อมูลส่วนบุคคลนั้น โดยในบางกรณีอาจใช้วิธีการ “ทำให้สะอาด (Sanitize)” ฮาร์ดแวร์ ด้วยการนำเอาข้อมูลส่วนบุคคลทั้งหมดออกจากฮาร์ดแวร์ หรือใช้วิธีการทำลายข้อมูลทิ้งโดยสิ้นเชิง หรือโดยที่ไม่สามารถกู้คืนกลับมาได้อีก อย่างไรก็ตาม หากว่าข้อมูลส่วนบุคคลนั้นไม่อาจถูกทำลายทิ้งโดยสิ้นเชิงโดยที่ไม่สามารถกู้คืนกลับมาได้อีก หน่วยงานหรือองค์กรอาจปฏิบัติตาม APP 11.2 โดยการดำเนินการให้เหมาะสมเพื่อทำให้ข้อมูลนั้นเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนแทนได้ หรือการทำให้ข้อมูลนั้นเป็นข้อมูลที่อยู่เหนือการใช้งาน (Putting Beyond Use)[188]

---

[186] Australian Privacy Principle (Chapter 11), para 11.3.

[187] Ibid, para 11.37.

[188] Ibid.

การทำให้ข้อมูลนั้นเป็นข้อมูลที่อยู่เหนือการใช้งานอาจทำได้เมื่อองค์กรธุรกิจไม่สามารถทำลายข้อมูลส่วนบุคคลที่ถูกเก็บไว้ในรูปแบบอิเล็กทรอนิกส์ โดยการทำให้ข้อมูลนั้นเป็นข้อมูลที่อยู่เหนือการใช้งานนี้ถือเป็นหนึ่งในการดำเนินการที่เหมาะสม อย่างไรก็ตาม องค์กรธุรกิจอาจพิจารณาทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้ หากว่าเป็นการเหมาะสมกว่า โดยกรณีที่จะถือว่าเป็นกรณี “เหนือการใช้งาน” อาจประกอบไปด้วยกรณีที่องค์กรธุรกิจไม่สามารถ และจะไม่พยายามใช้หรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่สามารถให้บุคคลใด ๆ เข้าถึงข้อมูลส่วนบุคคลได้ หรืออาจเป็นกรณีที่เป็นการจัดให้ข้อมูลส่วนบุคคลนั้นอยู่ในสภาพแวดล้อมที่เหมาะสม ทั้งที่เป็นการจัดให้ข้อมูลส่วนบุคคลนั้นอยู่ในสภาพความมั่นคงปลอดภัยทั้งทางเทคนิค กายภาพ และองค์กร ซึ่งอาจประกอบไปด้วยการควบคุมการเข้าถึง Log และ Audit Trails ทั้งนี้โดยที่องค์กรธุรกิจต้องให้คำมั่นในการที่จะดำเนินการให้เหมาะสมเพื่อทำลายข้อมูลส่วนบุคคลโดยไม่สามารถกู้คืนข้อมูลส่วนบุคคลนั้นกลับมาได้อีกหากองค์กรธุรกิจสามารถดำเนินการเช่นนั้นได้ ซึ่งกรณีการที่องค์กรธุรกิจไม่สามารถดำเนินการทำลายข้อมูลส่วนบุคคลที่ถูกเก็บไว้ในรูปแบบอิเล็กทรอนิกส์ได้ อาจเกิดขึ้นได้น้อยมาก เช่น ในกรณีสภาพทางเทคนิคไม่อาจดำเนินการทำลายข้อมูลส่วนบุคคลโดยไม่สามารถกู้คืนข้อมูลส่วนบุคคลนั้นกลับมาได้ เนื่องจากข้อมูลดังกล่าวปะปนอยู่กับข้อมูลส่วนบุคคลที่องค์กรนั้น ๆ จำเป็นต้องทำการเก็บรักษาไว้[189]

(2) การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้ (De-Identification)

ตาม AUS PA 1988 การทำให้ข้อมูลนั้นเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตน (De-Identification) อาจเป็นกรณีที่เหมาะสมกว่าการทำลายข้อมูล

[189] Ibid, para 11.40.

เนื่องจากข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้นั้น อาจสร้างประโยชน์หรือคุณค่าแก่หน่วยงานของรัฐหรือองค์กรเอกชนหรือบุคคลภายนอกได้ต่อไปอีก ยกตัวอย่างเช่น ในกรณีที่หน่วยงานหรือองค์กรแบ่งปันข้อมูลที่ไม่สามารถบ่งชี้ตัวตนต่อนักวิจัย หรือ ใช้ข้อมูลที่ไม่สามารถบ่งชี้ตัวตนเพื่อการพัฒนาผลิตภัณฑ์ใหม่[190] โดยแนวทางการปฏิบัติเกี่ยวหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศออสเตรเลียได้มีการกำหนดและชี้แนะแนวทางในการปฏิบัติต่อกรณีของการทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้ โดยที่ข้อมูลส่วนบุคคลจะถูกทำให้ไม่สามารถบ่งชี้ตัวตนได้เมื่อข้อมูลส่วนบุคคลนั้นไม่มีส่วนเกี่ยวข้องกับบุคคลที่สามารถบ่งชี้ตัวตนหรือบุคคลที่สามารถบ่งชี้ตัวตนอย่างสมเหตุสมผลได้ อย่างไรก็ตาม แนวทางปฏิบัติฉบับนี้ กล่าวไว้ว่าข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้นั้นไม่ใช่ข้อมูลส่วนบุคคล

โดยการทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตน คือ การกำจัดหรือเปลี่ยนแปลง (Alter) ข้อมูลที่บ่งชี้บุคคล หรือมีลักษณะที่อาจสามารถบ่งชี้ตัวตนได้ ทั้งนี้ ขั้นตอนในการทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้อาจประกอบไปด้วย 2 ขั้นตอน ดังต่อไปนี้

- ลบตัวบ่งชี้บุคคล (Personal Identifiers) เช่น ชื่อ ที่อยู่ วันเกิด หรือข้อมูลที่บ่งชี้ตัวตนอื่น ๆ ของบุคคล และ
- ลบหรือเปลี่ยนแปลงข้อมูลอื่นที่อาจเป็นการยอมให้บุคคลนั้นถูกบ่งชี้ตัวตน ยกตัวอย่างเช่น ลักษณะของบุคลิกภาพที่มีลักษณะพบเจอได้ยากหรือลักษณะของบุคลิกภาพที่เมื่อรวมกันแล้วมีลักษณะพิเศษ หรือมีลักษณะโดดเด่นที่ทำให้สามารถบ่งชี้หรือระบุตัวตนได้

[190] Ibid, para 11.41.

การทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนอาจไม่ได้เป็นการกำจัดความเสี่ยงที่ว่าบุคคลนั้นสามารถถูกบ่งชี้ตัวตนอีกครั้งโดยที่อาจมีความเป็นไปได้ว่าชุดข้อมูล (Dataset) หรือข้อมูลอื่นอาจไปสอดคล้องหรือตรงกับข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวตนได้ ทั้งนี้ ความเสี่ยงของกรณีการที่ข้อมูลสามารถถูกบ่งชี้ตัวตนได้อีกครั้ง จำต้องมีการประเมินและบริหารจัดการเพื่อลดความเสี่ยงอยู่เสมอ โดยที่ปัจจัยที่เกี่ยวข้องเมื่อต้องกำหนดว่าข้อมูลเหล่านี้ได้ถูกดำเนินการให้เป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้นั้นอาจเกี่ยวเนื่องไปถึงต้นทุน ความยากลำบาก การปฏิบัติได้จริง (Practicality) และความเป็นไปได้ในการที่ข้อมูลนั้นอาจถูกทำให้สามารถระบุตัวตนได้อีกครั้ง

3.4.2 กรณีศึกษา

ในเดือนกรกฎาคม ค.ศ. 2021 คณะกรรมการคุ้มครองข้อมูลและข้อมูลส่วนบุคคลของออสเตรเลีย (Australian Information Commissioner and Privacy Commissioner : AICPC) มีคำวินิจฉัยว่า Uber B.V. เข้าแทรกแซงความเป็นส่วนตัวของผู้ใช้งานราว 1.2 ล้านคน โดยมีเหตุผลสำคัญว่า Uber ฝ่าฝืน AUS PA 1988 เนื่องจากไม่ได้ใช้ความระมัดระวังตามสมควรในการคุ้มครองข้อมูลส่วนบุคคลของชาวออสเตรเลียจากการเข้าถึงโดยมิชอบด้วยกฎหมาย และทำลายหรือทำให้ข้อมูลส่วนบุคคลไม่อาจถูกระบุตัวตนได้ตามแนวทางการปฏิบัติเกี่ยวหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศออสเตรเลีย[191]

[191] OAIC, ‘Uber found to have interfered with privacy’ (OAIC, July 2021) < https ://www.oaic.gov.au/updates/news-and-media/uber-found-to-have-interfered-with-privacy/> accessed 3 October 2021.

AICPC มีคำสั่งให้ Uber ตระเตรียมและใช้งานนโยบายการเก็บรักษาและทำลายข้อมูลโปรแกรมตอบสนองต่อเหตุล่วงละเมิด ซึ่งจะช่วยให้บริษัทสามารถปฏิบัติตาม APP ได้ และให้แต่งตั้งผู้เชี่ยวชาญอิสระทำหน้าที่ในการตรวจสอบและรายงานนโยบายและโปรแกรมแก่ OAIC ตลอดจนดำเนินการแก้ไขแนะนำใด ๆ ที่จำเป็นในรายงาน[192]

เมื่อพิจารณาบทบัญญัติใน AUS PA 1988 ประกอบกับแนวทางการบังคับใช้กฎหมายโดย AICPC แล้ว สามารถกล่าวได้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศออสเตรเลียนั้น สามารถคุ้มครองสิทธิที่จะถูกลืมของเจ้าของข้อมูลส่วนบุคคลได้โดยผ่านหน้าที่ในการ “ทำลายหรือทำให้ข้อมูลส่วนบุคคลไม่อาจถูกระบุตัวตนได้” โดยที่กฎหมายไม่ต้องบัญญัติถึง “สิทธิที่จะถูกลืม” ในตัวบทกฎหมาย

มีข้อสังเกตว่า เพื่อให้การดำเนินการดังกล่าวเป็นไปได้ในทางปฏิบัติ AICPC จึงได้ออกแนวปฏิบัติและรายละเอียดเกี่ยวกับการทำลายและการทำให้ข้อมูลกลายเป็นข้อมูลที่บ่งชี้ตัวตนไม่ได้เป็นส่วนหนึ่งของมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลซึ่งทำให้เห็นได้ว่าการคุ้มครองสิทธิที่จะถูกลืมนั้น อาจถูกดำเนินการโดยผ่านการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลก็ได้

3.5 ประเทศญี่ปุ่น

รัฐธรรมนูญของประเทศญี่ปุ่นได้บัญญัติถึงสิทธิในชีวิตร่างกายของบุคคล โดยไม่ได้บัญญัติถึงสิทธิในความเป็นส่วนตัวเอาไว้โดยตรง[193] อย่างไรก็ตาม ในส่วนที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลนั้นได้มีการบังคับใช้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลมาตั้งแต่ พ.ศ. 2546

[192] Ibid.

[193] The Constitution of Japan, Seciton 13.

ชื่อว่า Act on Protection of Personal Information of Japan (“APPI”) โดยถือเป็นประเทศแรก ๆ ในทวีปเอเชียที่มีกฎหมายที่บังคับใช้ในความคุ้มครองในเรื่องข้อมูลส่วนบุคคล

3.5.1 ตัวบทกฎหมายและแนวปฏิบัติ

JAP APPI 2020 ได้บัญญัติให้สิทธิเจ้าของข้อมูลในการร้องขอให้ผู้ประกอบการที่จัดการกับข้อมูลส่วนบุคคลของตน ยุติการใช้ หรือลบข้อมูลส่วนบุคคลได้นับแต่มีการประกาศใช้ APPI เป็นครั้งแรก APPI (2003) ก่อนถูกแก้ไขในปี ค.ศ. 2020 (ในส่วนของสิทธิในการขอแก้ไข) ระบุถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลในการร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคล (องค์กรธุรกิจที่รับผิดชอบในการประมวลผลข้อมูล) ทำการลบข้อมูลตามที่ถูกร้องขอ[194] ต่อมาใน ค.ศ. 2020 ประเทศญี่ปุ่นได้มีการแก้ไขเพิ่มเติมกฎหมาย APPI เป็นครั้งที่สอง และได้มีการแก้ไขเพิ่มเติมบทบัญญัติที่เกี่ยวข้องกับสิทธิในการลบข้อมูลส่วนบุคคล โดยขยายสิทธิในการลบข้อมูลส่วนบุคคลเพื่อให้สามารถคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลให้ครอบคลุมมากขึ้น และมีการแก้ไขเพิ่มเติมสิทธิในการลบข้อมูลส่วนบุคคลในมาตรา 30 ของ JAP APPI 2020

JAP APPI 2020 รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลเพิ่มเติมสำหรับมีการใช้ข้อมูลส่วนบุคคลที่ไม่เหมาะสมตามมาตรา 16 มาตรา 16-2 และมาตรา 17 ซึ่งเป็นบทบัญญัติที่กำหนดลักษณะของการห้ามใช้งานข้อมูลส่วนบุคคลที่ไม่เหมาะสม หากว่าการใช้ข้อมูลส่วนบุคคลนั้นมีความเป็นได้ว่าจะก่อให้เกิดการกระทำที่ไม่ชอบด้วยกฎหมายหรือไม่เป็นธรรม[195]

---

[194] Act on the Protection of Personal Information Act No. 57 of (2003), Section 26.

[195] Act on the Protection of Personal Information (The amended Act fully put into effect on April 1, 2022), Section 30 (1).

เช่น กรณีข้อมูลส่วนบุคคลถูกใช้นอกเหนือจากวัตถุประสงค์เดิมที่ได้แจ้งไว้[196] เมื่อผู้ประกอบการได้รับข้อมูลส่วนบุคคลมาโดยการหลอกลวง หรือด้วยวิธีอื่นที่ไม่เหมาะสม[197] เมื่อข้อมูลส่วนบุคคลที่เก็บไว้นั้น ไม่จำเป็นต่อวัตถุประสงค์ในการใช้งานอีกต่อไป[198]

เมื่อผู้ประกอบการได้รับคำร้องขอใช้สิทธิในการยุติการใช้งานหรือลบข้อมูลส่วนบุคคลแล้ว และเป็นที่แน่ชัดแล้วว่ามีเหตุผลในการใช้สิทธิดังกล่าว ผู้ประกอบการต้องยุติการใช้งานหรือลบข้อมูลส่วนบุคคลโดยไม่ล่าช้า[199] ทั้งนี้ หากผู้ประกอบการประสงค์ที่จะปฏิเสธไม่ดำเนินการตามคำร้องขอดังกล่าว ผู้ประกอบการที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า[200]

เจ้าของข้อมูลส่วนบุคคลอาจใช้สิทธิร้องขอให้ผู้ประกอบการปฏิบัติการยุติการใช้งานข้อมูลส่วนบุคคลที่เก็บรักษาไว้หากเกิดกรณีตามมาตรา 22-2 (1) ซึ่งกำหนดให้ผู้ประกอบการมีหน้าที่ต้องรายงานต่อคณะกรรมการ Personal Information Protection Commission (PPC) เมื่อเกิดกรณีที่ข้อมูลส่วนบุคคลเกิดการรั่วไหว (Leakage) สูญเสีย หรือเสียหาย หรือเหตุการณ์อื่นใดที่เกี่ยวข้องกับการรับประกันความมั่นคงปลอดภัย (Insurance of Security) ของข้อมูลส่วนบุคคล หรือเกิดกรณีที่การจัดการกับข้อมูลส่วนบุคคลนั้นอาจกระทบกระเทือนต่อสิทธิหรือฐานประโยชน์อันชอบธรรมของเจ้าของข้อมูลส่วนบุคคล[201]

---

[196] Ibid, Section 16.

[197] Ibid, Section 17.

[198] Ibid, Section 19.

[199] Ibid, มาตรา 30 (2).

[200] Ibid, มาตรา 30 (7).

[201] Ibid, มาตรา 30 (5).

อย่างไรก็ตาม หากปรากฏว่าการยุติการใช้งานหรือการลบข้อมูลส่วนบุคคลนั้น จำต้องใช้ค่าใช้จ่ายจำนวนมากหรือเป็นการยากในการที่จะยุติการใช้งานหรือลบข้อมูลส่วนบุคคลนั้น และโดยที่ได้มีการดำเนินการตามทางเลือกใดแล้วเพื่อปกป้องสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลอาจปฏิเสธการร้องขอใช้สิทธิลบข้อมูลของเจ้าของข้อมูลส่วนบุคคลนั้นได้[202]

3.5.2 กรณีศึกษา

3.5.2.1 คดี Google ในศาลเขต

ใน ค.ศ. 2015 ศาลเขต Saitama (Saitama District Court) ในประเทศญี่ปุ่นได้มีการตัดสินเกี่ยวกับสิทธิที่จะถูกลืมเป็นครั้งแรก โดยคดีดังกล่าวเป็นคดีแพ่งที่ศาลได้ออกคำสั่งเป็นการชั่วคราว (Provisional Disposition) ที่อ้างอิงกฎหมายว่าด้วยการชดใช้เยียวยาชั่วคราว (Civil Provisional Remedies Act) เพื่อออกคำสั่งเกี่ยวกับการลบข้อมูลซึ่งแตกต่างไปจาก CJEU วินิจฉัยหน้าที่ของ Google ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลโดยตรง[203]

คำตัดสินของศาลในคดีดังกล่าวนี้ เป็นเรื่องที่เกี่ยวกับการคุ้มครองเกียรติยศและความเป็นส่วนตัวของเจ้าของข้อมูล และถือเป็นการรับรองถึงสิทธิในการลบในรูปแบบของคำสั่งคุ้มครองชั่วคราว (Injunctive Relief) เนื่องจากผู้ร้องในคดีนี้กล่าวอ้างว่าหากมีการพิมพ์ชื่อของผู้ร้องในระบบการสืบค้นพร้อมด้วยภูมิลำเนาของผู้ร้อง ผลการค้นหาจะแสดงให้เห็น URL

---

[202] Ibid.

[203] Frederike Zufall, 'Challenging the EU's 'Right to Be Forgotten'? Society's 'Right to Know' in Japan' (2019) EDPL 1 17, p. 18.

ซึ่งเชื่อมต่อไปยังเว็บไซต์ที่แสดงถึงประวัติการทำความผิดอาญาของผู้ร้อง ด้วยเหตุนี้ ผู้ใช้งานอินเทอร์เน็ตย่อมเข้าใจว่าผู้ร้องถูกจับกุมและเสียค่าปรับจำนวน 500,000 เยน จากการฝ่าฝืนกฎหมายว่าด้วยโสเภณีเด็ก ภาพอนาจารเด็ก และการคุ้มครองเด็ก เนื่องจากมีพฤติกรรม คือ การมีเพศสัมพันธ์กับเด็กที่มีอายุต่ำกว่า 18 ปี[204]

ศาลในคดีดังกล่าวได้มีคำสั่งให้ Google ทำการลบผลการค้นหาออกเป็นการชั่วคราว[205] โดยศาลมีคำวินิจฉัยว่าผลการค้นหานั้นได้สร้างความเสียหายให้แก่สิทธิในความเป็นส่วนตัวของผู้ร้องตามมาตรา 13 แห่งรัฐธรรมนูญของประเทศญี่ปุ่น ศาลเขต Saitama ระบุว่าแม้ลักษณะของกิจกรรมของ Google จะมีบทบาทสำคัญในการทำให้คนในสังคมสามารถเข้าถึงข้อมูลออนไลน์ได้ อย่างไรก็ตาม สิทธิของผู้ร้องในการที่จะสามารถฟื้นฟูนั้น ไม่ควรต้องถูกรบกวน (Undisturbed)[206] สิทธิในมาตรา 13 แห่งรัฐธรรมนูญของประเทศญี่ปุ่น ซึ่งได้รับรองถึง “สิทธิในการที่จะได้รับการเคารพในฐานะเป็นปัจเจกบุคคล (Right to be Respected as Individuals)” เพราะฉะนั้น การละเมิดสิทธิดังกล่าวจึงเป็นกรณีที่จะต้องคุ้มครองสิทธิในการลบข้อมูลขึ้นผ่านรูปแบบของคำสั่งคุ้มครองชั่วคราว[207]

3.5.2.2 คดี Google ในศาลฎีกา

ต่อมา Google ได้ยื่นคัดค้านคำสั่งของศาลเขต Saitama โดยให้เหตุผลว่ากิจกรรมที่ถูกดำเนินการผ่านโปรแกรมสืบค้นข้อมูลของ Google นั้นเป็นบทบาทที่สำคัญในเรื่องการมีเสรีภาพในการพูด (Freedom of Speech)

---

[204] Ibid, pp. 17-18.

[205] Ibid, p. 18.

[206] Ibid, p. 18.

[207] Ibid.

และการเข้าถึงข้อมูลของสาธารณะที่ให้สิทธิดังกล่าวไว้ในรัฐธรรมนูญของประเทศ แม้ต่อมา คำร้องคัดค้านของ Google ไม่ได้รับการพิจารณา Google ได้ยื่นอุทธรณ์ต่อศาลสูงโตเกียว (Tokyo High Court) และศาลสูงได้ตัดสินยกคำสั่งของศาลเขต Saitama ดังกล่าว โดย Google ให้ความเห็นว่าสิทธิในการรับรู้ (right to know) ของสังคมถือเป็นเรื่องสำคัญ

ศาลฎีกาของประเทศญี่ปุ่นได้วินิจฉัยใน ค.ศ. 2017 ว่า “ความชอบด้วยกฎหมาย” ของการแสดงผลข้อมูลนั้นจะต้องพิจารณาจากการชั่งน้ำหนักระหว่างประโยชน์ทางกฎหมาย (Legal Interest) ของการที่ข้อมูลส่วนบุคคลจะไม่ถูกเผยแพร่และสถานการณ์อื่น ๆ ที่เกี่ยวกับการแสดง URL จากการค้นหา ในคดีนี้ศาลเห็นว่าประโยชน์ทางกฎหมายของการไม่แสดงผลข้อมูลนั้นมีน้ำหนักมากกว่าประโยชน์ทางกฎหมายของการแสดงผลข้อมูล ดังนั้น เจ้าของข้อมูลส่วนบุคคลจึงมีสิทธิเรียกร้องให้ผู้ประกอบการลบ URL และรายการอื่น ๆ จากผลการค้นหาได้[208]

เมื่อพิจารณาบทบัญญัติในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น ประกอบกับแนวการบังคับใช้กฎหมายโดยศาลยุติธรรมแล้ว สามารถกล่าวได้ว่าสิทธิที่จะถูกลืมของในระบบกฎหมายของประเทศญี่ปุ่นนั้นมีพัฒนาการมาจากการเริ่มคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลในการร้องขอให้มีการ “แก้ไข” ข้อมูลส่วนบุคคล (ตามมาตรา 26 ของ Act on the Protection of Personal Information Act No. 57 of (2003)) ต่อมาใน ค.ศ. 2020 กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้บัญญัติถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลในการร้องขอให้ผู้ประกอบการหยุดการประมวลผลข้อมูลหรือลบข้อมูลส่วนบุคคล ซึ่งอาจกล่าวได้ว่าเป็นบทบัญญัติ

---

[208] Courts in Japan, ‘2016 (Kyo) 45’ (Courts in Japan, January 2017) <https ://www.courts.go.jp/app/hanrei_en/detail?id=1511> accessed 4 October 2021.

ที่มีความคล้ายคลึงกับมาตรา 47 ของ UK DPA 2018 ซึ่งเป็นบทบัญญัติรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลในการร้องขอให้ลบหรือจำกัดการประมวลผลข้อมูล (Right to Erasure or Restriction of Processing)[209] และสามารถเทียบเคียงได้กับสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลายตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้

การบังคับใช้สิทธิที่จะถูกลืมในประเทศญี่ปุ่นเผชิญกับความท้าทายจากความจำเป็นในการชั่งน้ำหนักระหว่างสิทธิในความเป็นส่วนตัวและสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเช่นเดียวกับกรณีศึกษาในสหภาพยุโรป (เช่น คดี *Plaintiff X v. PrimaDanoi*) โดยปรากฏตามคดี Google ซึ่งศาลฎีกาได้นำสิทธิในการรับรู้ (Right to Know) ของสังคมมาชั่งน้ำหนักกับสิทธิในความเป็นส่วนตัว ดังนั้น ในการตีความขอบเขตของสิทธิในการเข้าถึงข้อมูล (Right to Information) ซึ่งถือได้ว่าเป็นข้อจำกัดประการหนึ่งของสิทธิที่จะถูกลืมจึงอาจพิจารณาถึงสิทธิในการรับรู้ของสังคมด้วย

3.6 เขตปกครองพิเศษไต้หวัน

รัฐธรรมนูญของไต้หวัน (Constitution of the Republic of China (Taiwan)) ได้รับรองถึงสิทธิในความเป็นส่วนตัวของบุคคลเอาไว้อย่างชัดแจ้ง[210] นอกจากนี้ ไต้หวันมีการประกาศใช้ Personal Data Protection Act 2015 (“TW PDPA 2015”) และ Enforcement Rules of the Personal Data Protection Act (“TW PDPA Enforcement Rules”) รวมไปถึงคำสั่งต่าง ๆ เพื่อบังคับใช้กับการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศ กฎหมาย PDPA ได้ถูกประกาศใน พ.ศ. 2558 และมีผลใช้บังคับในอีกหนึ่งปีถัดมาจากวันที่

[209] โปรดดูรายละเอียดในหัวข้อ 3.3.1.1.

[210] Constitution of the Republic of China (Taiwan), Section 12.

ถูกประกาศ โดยหลังจากที่ GDPR ได้ถูกประกาศบังคับใช้อย่างเป็นทางการในสหภาพยุโรป ไต้หวันได้วางแผนในการแก้ไขกฎหมาย PDPA ของประเทศเพื่อให้เป็นไปตามมาตรฐานเรื่องการคุ้มครองข้อมูลส่วนบุคคลของกฎหมาย GDPR รวมไปถึงคำตัดสินต่าง ๆ จากสหภาพยุโรปด้วย ทำให้ต่อมาในพ.ศ. 2562 ไต้หวันได้มีการเปิดรับฟังความคิดเห็นของสาธารณะเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อแก้ไข TW PDPA 2015 ให้สอดคล้องกับมาตรฐาน GDPR โดยหลังจากการเปิดรับฟังความเห็นจากสาธารณะรัฐบาลไต้หวันได้มีการวางแผนนำบทบัญญัติที่เกี่ยวกับหน้าที่ในการแจ้งเหตุละเมิด และการจำกัดการโอนถ่ายข้อมูลส่วนบุคคลระหว่างประเทศของ GDPR มาปรับใช้กับ TW PDPA 2015 ภายในประเทศ รวมไปถึงการวางแผนในการจัดให้มีหน่วยงานคุ้มครองข้อมูลส่วนบุคคลที่เป็นอิสระอีกด้วย

3.6.1 ตัวบทกฎหมายและแนวปฏิบัติ

3.6.1.1 Personal Data Protection Act 2015

TW PDPA 2015 บัญญัติหน้าที่ต่าง ๆ ในการคุ้มครองข้อมูลส่วนบุคคลโดยระบุเจาะจงไปที่ “หน่วยงานของรัฐ (Government Agency)” และ “องค์กรนอกภาครัฐ (Non-Government Agency) โดยไม่ได้ใช้คำว่า “ผู้ควบคุมข้อมูลส่วนบุคคล” เหมือนดังกรณีของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หน่วยงานของรัฐ รวมไปถึงเจ้าหน้าที่ผู้ใช้อำนาจรัฐที่อยู่ในระดับรัฐบาลกลางและรัฐบาลท้องถิ่น[211] ส่วนองค์กรนอกภาครัฐนั้นได้แก่ บุคคลธรรมดา นิติบุคคล หรือกลุ่มของบุคคลที่มิได้มีสถานะเป็นหน่วยงานของรัฐ[212]

---

[211] Personal Data Protection Act (2015), Article 2 para 7.

[212] Ibid, Article 2 para 8.

ในส่วนของสิทธิที่จะถูกลืมนั้น มาตรา 3 วรรคหน้าของ TW PDPA 2015 ได้กำหนดให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิในการร้องขอให้ลบข้อมูลส่วนบุคคล (Right to Erase) ในขณะที่มาตรา 11 กำหนดให้หน้าที่หน่วยงานของรัฐและองค์กรนอกภาครัฐมีหน้าที่ “ลบ (Erase)” ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมที่ไม่มีความจำเป็นต้องถูกเก็บตามวัตถุประสงค์การประมวลผลอีกต่อไป หรือเมื่อเวลาในการเก็บรวบรวมนั้นได้หมดลง[213] หรือถูกเก็บรวบรวมหรือประมวลผลโดยฝ่าฝืนต่อ TW PDPA 2015[214] ทั้งนี้ ไม่ว่าจะเป็นกรณีที่ได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคลหรือเป็นกรณีที่หน่วยงานของรัฐและหน่วยที่ไม่ใช่องค์กรภาครัฐดำเนินการด้วยตนเอง

การลบข้อมูลประวัติอาชญากรรมเพื่อวัตถุประสงค์ด้วยการฟื้นฟูทางสังคมนั้น ไม่ได้ถูกบัญญัติเป็นสิทธิประเภทหนึ่งภายใต้ TW PDPA 2015 อย่างไรก็ตาม การใช้สิทธิในการลบข้อมูลประวัติอาชญากรรมในไต้หวันนั้นถูกกล่าวถึงในกฎหมายว่าด้วยการกระทำความผิดของผู้เยาว์ (Juvenile Delinquency Act) ในส่วนของ “Record Removal” ซึ่งกำหนดให้มีการลบประวัติอาชญากรรมของผู้เยาว์ออกหลังจากที่ถูกลงโทษเรียบร้อยแล้ว[215] นอกจากนี้ กฎหมายว่าด้วยการคุ้มครองเด็กและสวัสดิการสิทธิของผู้เยาว์ (Protection of Children and Youths Welfare and Rights Act) กำหนดห้ามมิให้วัตถุเพื่อส่งเสริมการขาย (Promotional Material) การตีพิมพ์ การกระจายเสียง โทรทัศน์ อินเทอร์เน็ต หรือสื่ออื่นรายงานถึงหรือเก็บข้อมูลเกี่ยวกับชื่อหรือข้อมูลอื่นใดที่จะทำให้สามารถระบุถึงตัวตนของเด็กและเยาวชนในกรณีเช่น การใช้ยาเสพติดหรือการถูกดำเนินคดีทางอาญา[216]

---

[213] Ibid, Article 11 para 3.

[214] Ibid, Article 11 para 4.

[215] Juvenile Delinquency Act, Article 83-1.

[216] Protection of Children and Youths Welfare and Rights Act 2021, Article 69 para 1.

เอกสารที่ถูกทำให้สาธารณชนเข้าถึงได้โดยหน่วยงานทางปกครองและองค์กรในฝ่ายตุลาการจะต้องไม่มีข้อมูลที่นำไปสู่การระบุตัวตนของเด็กและเยาวชนได้ (เว้นแต่กฎหมายจะกำหนดเป็นอย่างอื่น)[217]

3.6.1.2 Enforcement Rules of the Personal Data Protection Act

เพื่อให้ TW PDPA 2015 สามารถคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ ในทางปฏิบัติกระทรวงยุติธรรมของไต้หวันจึงได้ออกกฎเพื่อบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (Enforcement Rules of the Personal Data Protection Act) ที่ได้ถูกแก้ไขเพิ่มเติมใน พ.ศ. 2559 (TW PDPA Enforcement Rules) โดยอาศัยอำนาจตามมาตรา 55 ของ TW PDPA 2015 กฎดังกล่าวกำหนดศัพท์นิยามต่าง ๆ ที่บัญญัติอยู่ TW PDPA 2015 โดยเป็นการขยายความและวางหลักเกณฑ์ในรายละเอียดที่ TW PDPA 2015 มิได้บัญญัติไว้โดยตรง

(1) วัตถุประสงค์เฉพาะไม่มีอยู่อีกต่อไป

TW PDPA Enforcement Rules ได้ให้นิยามของคำว่า “เมื่อวัตถุประสงค์เฉพาะไม่มีอยู่อีกต่อไป” ตามมาตรา 11 วรรคสามของกฎหมาย กล่าวคือ[218]

1. เมื่อหน่วยงานของรัฐถูกยุบหรือถูกจัดระเบียบใหม่โดยไม่มีหน่วยงานอื่นรับหน้าที่เดิมของหน่วยงานนั้นต่อ

---

[217] Ibid, Article 69 para 2.

[218] Enforcement Rules of the Personal Data Protection Act (2016), Article 20.

2. เมื่อหน่วยงานที่มิใช่รัฐได้ยุติกิจการหรือเลิกกิจการโดยไม่มีองค์กรอื่นรับดำเนินกิจการต่อ หรือองค์กรนอกภาครัฐนั้นได้เปลี่ยนแปลงขอบเขตการดำเนินธุรกิจ โดยทำให้เกิดวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นไม่อาจใช้บังคับได้อีกต่อไป
3. เมื่อวัตถุประสงค์เฉพาะนั้นได้บรรลุวัตถุประสงค์แล้ว และทำให้ไม่มีความจำเป็นในการประมวลผลและใช้ข้อมูลส่วนบุคคลนั้นอีกต่อไป หรือ
4. เมื่อมีเหตุอื่นใดในลักษณะที่วัตถุประสงค์เฉพาะนั้นไม่สามารถทำให้บรรลุวัตถุประสงค์ได้อย่างชัดเจนหรือไม่มีวัตถุประสงค์นั้นอยู่อีกต่อไป

ดังนั้น เมื่อเกิดกรณีตามข้อหนึ่งข้อใดข้างต้นจึงเท่ากับว่าวัตถุประสงค์เฉพาะของการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นไม่มีอยู่อีกต่อไป ที่บัญญัติในมาตรา 11 วรรคสามแห่ง TW PDPA 2015 จึงส่งผลให้เจ้าของข้อมูลส่วนบุคคลอาจใช้สิทธิขอให้ลบข้อมูลส่วนบุคคลนั้น ๆ ของตนต่อผู้ที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลได้

(2) ความจำเป็นต่อการปฏิบัติหน้าที่ราชการหรือทางธุรกิจ

TW PDPA Enforcement Rules ยังได้ให้นิยามของคำว่า “ความจำเป็นต่อการปฏิบัติหน้าที่ราชการหรือทางธุรกิจ (Necessity for the Performance of an Official or Business Duty)” ตามที่บัญญัติไว้ในมาตรา 3 วรรคสามของ TW PDPA 2015 ซึ่งมีลักษณะเป็นการขยายความข้อยกเว้นของการปฏิบัติตามคำร้องขอใช้สิทธิลบข้อมูลส่วนบุคคลของเจ้าข้อมูลส่วนบุคคลไว้ดังนี้[219]

[219] Ibid, Article 21.

1. เมื่อระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลสิ้นสุดลงโดยกฎหมาย หรือกฎระเบียบ หรือตามที่ได้ตกลงไว้ภายใต้สัญญา
2. เมื่อมีเหตุผลที่เพียงพอจะเชื่อได้ว่าการลบข้อมูลส่วนบุคคลนั้นจะเป็นการละเมิดต่อสิทธิประโยชน์ของเจ้าของข้อมูลส่วนบุคคลที่เป็นเครื่องรับประกันความคุ้มครองในข้อมูลส่วนบุคคลของเขา
3. เมื่อมีเหตุผลอันชอบธรรม (Legitimate Reasons) ในการที่จะไม่ลบข้อมูลส่วนบุคคลนั้น

ดังนั้น เมื่อปรากฏกรณีใด ๆ ข้างต้นแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลทั้งที่เป็นหน่วยงานของรัฐและองค์กรนอกภาครัฐ อาจใช้กรณีดังกล่าวเป็นข้อยกเว้นในการไม่ปฏิบัติตามคำขอใช้สิทธิลบข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลได้

3.6.2 กรณีศึกษา

3.6.2.1 Supreme Administrative Court 106 Pan Zi No. 54

การใช้สิทธิที่จะถูกลืมในแง่มุมของสิทธิขอให้ลบข้อมูลส่วนบุคคลนั้นได้ปรากฏให้เห็นในคดีการยื่นฟ้องหน่วยงานประกันสุขภาพแห่งชาติ (National Health Insurance Administration : NHIA) โดยเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นบุคคลธรรมดา ที่มีความจำเป็นในการใช้ข้อมูลส่วนบุคคลในระดับทุติยภูมิ (Secondary Use) ที่ถูกเก็บรวบรวมบนฐานข้อมูลอาจแตกต่างไปจากที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไว้ จนอาจก่อให้เกิดสิทธิในการร้องขอให้ลบข้อมูลส่วนบุคคลได้เช่นเดียวกัน เจ้าของข้อมูลส่วนบุคคลในประเทศไต้หวันจำนวนหนึ่งได้ยื่นฟ้อง NHIA และร้องขอให้ยุติการประมวลผล

ข้อมูลส่วนบุคคลที่ใช้เพื่อการวิจัยทางการแพทย์ระดับทุติยภูมิและร้องขอให้ลบข้อมูลส่วนบุคคลดังกล่าวเหล่านั้นออกจากฐานข้อมูลการวิจัย

โดยตามข้อเท็จจริงนั้นปรากฏว่า NHIA ซึ่งเป็นองค์กรที่ทำหน้าที่เก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้สิทธิคุ้มครองด้านประกันสุขภาพแก่ประชาชนภายในประเทศ โดยมีอำนาจในการให้บริการด้านประกันสุขภาพและการเก็บรวบรวมข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดไว้เพื่อวัตถุประสงค์ในการอนุมัติการขอรับค่าสินไหมทดแทนจากประกันสุขภาพ ได้มีการแบ่งปันข้อมูลส่วนบุคคลที่เป็นข้อมูลสุขภาพของเจ้าของข้อมูลส่วนบุคคลไปยังกระทรวงสุขภาพและสวัสดิการแห่งรัฐ (Ministry of Health and Welfare : MHW) เพื่อสร้างฐานข้อมูลการวิจัย MHW ในขณะที่แม้ว่าข้อมูลการวิจัยของ NHI ที่ได้เปิดเผยให้กับ MHW เพื่อการเข้าถึงแบบสาธารณะนั้น เป็นข้อมูลส่วนบุคคลที่ไม่อาจระบุตัวตนได้โดยตรง แต่ข้อมูลสุขภาพที่อยู่ในฐานข้อมูลของ NHI นั้นยังคงสามารถถูกเชื่อมโยงไปยังชุดข้อมูลต่าง ๆ และชุดข้อมูลต่าง ๆ เหล่านั้นสามารถเข้าถึงได้โดยการใช้ข้อมูลบ่งชี้ตัวตนจำเพาะที่ใช้กันอย่างทั่วไป ซึ่งก็คือหมายเลขประจำตัวประชาชนนั้นเอง

ในคดีนี้ ศาลฎีกาได้ตัดสินว่าโจทก์ซึ่งเป็นบุคคลธรรมนั้น ไม่อาจใช้สิทธิในการร้องขอให้ทำการลบข้อมูลส่วนบุคคลได้ เนื่องจากการเก็บรวบรวมข้อมูลส่วนบุคคลเหล่านั้นได้ถูกเก็บรวบรวมโดยชอบด้วยกฎหมาย กล่าวคือกฎหมายได้ให้อำนาจให้การเก็บรวบรวมข้อมูลส่วนบุคคลเหล่านั้นโดยไม่อาศัยความยินยอมของเจ้าของข้อมูลส่วนบุคคล สิทธิในการเลือกที่จะไม่รับจะไม่สามารถใช้บังคับได้ หากว่าข้อมูลส่วนบุคคลนั้นถูกเก็บรวบรวมเพื่อวัตถุประสงค์ของการวิจัยทางการแพทย์ และโดยที่ข้อมูลส่วนบุคคลได้ถูกทำให้เป็นข้อมูลนิรนาม แม้จะไม่จำเป็นต้องทำให้เป็นข้อมูลนิรนามทั้งหมด[220]

[220] Supreme Administrative Court 106 Pan Zi No. 54.

ในคดีดังกล่าวนี้จึงเห็นได้ชัดว่า ความประสงค์ส่วนบุคคลนั้นได้ถูกจำกัดโดยประโยชน์สาธารณะเพื่อการวิจัยทางการแพทย์[221] นอกจากนี้ยังพบข้อสังเกตอีกว่า TW PDPA 2015 ไม่ได้ระบุชัดแจ้งถึงการถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล ที่อาจใช้เป็นฐานทางกฎหมายในการที่จะสามารถร้องขอให้ทำการลบข้อมูลส่วนบุคคลได้

อย่างไรก็ตาม โจทก์ได้ใช้สิทธิให้มีการดำเนินกระบวนการตีความรัฐธรรมนูญในกรณีดังกล่าวอีกด้วย โดยโจทก์ได้มีการตีความนำเอาเรื่องสิทธิส่วนบุคคลที่ซึ่งเป็นสิทธิขั้นพื้นฐานที่บัญญัติไว้ภายใต้รัฐธรรมนูญของประเทศ ยกขึ้นเป็นข้อกล่าวอ้างว่าการริดรอนสิทธิของบุคคลในการร้องขอให้ลบข้อมูลส่วนบุคคลนั้นมีค่าเท่ากับเป็นการบังคับให้เข้าร่วมการวิจัยและนำมาซึ่งการละเมิดสิทธิส่วนบุคคลตามรัฐธรรมนูญ

จะเห็นได้ว่าการคุ้มครองสิทธิความเป็นส่วนตัวในมิติของสิทธิที่จะถูกลืมของไต้หวันนี้ได้ถูกท้าทายโดยปัญหาการสร้างความสมดุลระหว่างประโยชน์สาธารณะและความเป็นส่วนตัวเช่นเดียวกับกรณีศึกษาที่เกิดในสหภาพยุโรป เช่น คดี *NT1 & NT2 v Google LLC* ก็มีปัญหาที่ศาลจะต้องพิจารณาชั่งน้ำหนักระหว่างการที่ข้อมูลยังคงถูกเข้าถึงได้โดยสาธารณะกับการคุ้มครองความเป็นส่วนตัวของบุคคล

3.6.2.2 Taiwan High Court 104 Shang Zi No. 389 (Civil Division)

กรอบทางกฎหมายในการคุ้มครองสิทธิที่จะถูกลืมในไต้หวันประสบปัญหาเกี่ยวกับการแสดงผลข้อมูลส่วนบุคคลจากระบบการค้นหา

[221] Wen-Tsong Chiou, ‘Commentary on The Right to be Forgotten : Forget about It? (Cons Judicial, July 2015) <https ://cons.j udicial. gov.tw/jcc/Uploads/files.pdf> accessed 5 August 2021.

ข้อมูลเช่นเดียวกับในสหภาพยุโรป โดยสิทธิที่จะถูกลืมในประเทศไต้หวันยังอาจถูกพิจารณาในแง่มุมของ “สิทธิในการนำออกจากการแสดงข้อมูลบนเว็บไซต์” ดังตัวอย่างของคดีใน พ.ศ. 2561 ที่ได้มีการยื่นฟ้องเป็นคดีแพ่ง โดยโจทก์ใช้ทางเลือกในการฟ้องร้องว่าได้มีกรณีการละเมิดตามประมวลกฎหมายแพ่งเกิดขึ้น ศาลเขตไทเป (Taipei District Court) ได้ตัดสินคดีที่เกี่ยวกับสิทธิที่จะถูกลืมเป็นครั้งแรก โจทก์ในคดีนี้เป็นอดีตเจ้าของทีมเบสบอลมืออาชีพได้ยื่นเรื่องฟ้องร้อง Google International LLC เป็นคดีละเมิด โดยร้องขอให้ Google นั้น ลบข้อมูลการรายงานข่าวในด้านลบที่เกี่ยวข้องกับคดีอาญาการโกงการแข่งขันทีมเบสบอลที่เชื่อมโยงมาถึงตัวโจทก์

แม้ว่าต่อมาศาลในคดีนั้นได้ตัดสินว่าโจทก์ไม่มีความผิด ศาลเขตได้มีคำพิพากษาตัดสินว่าแนวคิดเรื่องสิทธิที่จะถูกลืมไม่ได้ถูกบัญญัติรับรองไว้ภายใต้ประมวลกฎหมายแพ่งของประเทศไต้หวัน อีกทั้งตาม TW PDPA 2015 เจ้าของข้อมูลส่วนบุคคลมีสิทธิเพียงร้องขอให้ข้อมูลส่วนบุคคลของตนนั้นถูกลบออกเมื่อปรากฏว่าข้อส่วนบุคคลดังกล่าวไม่ถูกต้อง หรือวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลที่เฉพาะเจาะจงนั้นไม่มีอยู่ตามที่กฎหมายอนุญาตอีกต่อไป หรืออาจเป็นกรณีที่ข้อมูลส่วนบุคคลนั้นถูกประมวลผลหรือเก็บรวบรวมด้วยวิธีที่ไม่ชอบด้วยกฎหมายเท่านั้น ในคดีนี้ โจทก์ได้ยื่นอุทธรณ์คำตัดสินของศาลเขตไปยังศาลสูงไต้หวัน อย่างไรก็ตาม ศาลสูงในคดีละเมิดตัดสินว่า Google Inc. ซึ่งเป็นผู้ให้บริการโปรแกรมสืบค้นข้อมูลอย่างแท้จริงนั้นไม่ใช่นิติบุคคลเดียวกันกับ Google International LLC และ Google Inc. ไม่ถูกถือว่ามีความเป็นนิติบุคคลในประเทศไต้หวัน ทั้งนี้ไม่ปรากฏว่าคำตัดสินของศาลสูงดังกล่าวได้กล่าวถึงสิทธิที่จะถูกลืมไว้โดยตรงแต่อย่างใด[222]

[222] Taiwan High Court 104 Shang Zi No. 389 (Civil Division).

3.6.2.3 Taoyuan District Court 104 Su Zi No. 985 (Civil Division)

โจทก์ฟ้อง Google เป็นคดีหมิ่นประมาท (ความรับผิดฐานละเมิด) ร้องขอ Google ลบผลการค้นหาที่เป็นข้อมูลหมิ่นประมาทโจทก์ โดยศาลเขตได้ตัดสินให้มีการลบข้อมูลหมิ่นประมาทนั้นออกจากโดเมนของ Google.tw อย่างไรก็ตาม ศาลในคดีนี้ไม่ได้ตัดสินให้ Google ต้องเป็นผู้รับผิดชอบในการลบผลการค้นหาที่เป็นข้อมูลหมิ่นประมาทโจทก์ที่ถูกประมวลผลโดยบริษัทเซิฟเวอร์ประมวลผลข้อมูลอื่นที่ไม่ใช่สัญชาติไต้หวันด้วยแต่อย่างใด[223]

คำพิพากษานี้แสดงให้เห็นถึงข้อจำกัดในการคุ้มครองสิทธิที่จะถูกลืมโดยหน่วยงานรัฐของประเทศหนึ่งอันเป็นประเด็นที่ไม่ได้มีการตั้งข้อสังเกตเอาไว้ในคดี *Google LLC v CNIL* (ดังที่ได้กล่าวในหัวข้อ 3.2.2.4) ซึ่ง CJEU ได้วินิจฉัยว่า การคุ้มครองสิทธิในความส่วนตัวในมิติของการร้องขอให้นำข้อมูลออกจากระบบนั้นจะต้องคำนึงถึงกรอบทางกฎหมายและระดับการคุ้มครองสิทธินี้ในแต่ละประเทศอีกด้วย

เมื่อพิจารณาบทบัญญัติใน TW PDPA 2015 สามารถเห็นได้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของไต้หวันนั้น คุ้มครองสิทธิที่จะถูกลืมโดยผ่านการ “ลบ” ข้อมูลส่วนบุคคลซึ่งเป็นทั้งสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 3 ของ TW PDPA 2015 และเป็นหน้าที่ของผู้ควบคุมข้อมูลตามมาตรา 11 วรรคสามและวรรคสี่ของ TW PDPA 2015 หน้าที่ในการลบดังกล่าวนี้มีได้แม้ว่าจะไม่มีการร้องขอของเจ้าของข้อมูลส่วนบุคคลซึ่งมีลักษณะคล้ายคลึงกับการบัญญัติสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย

[223] Taoyuan District Court 104 Su Zi No. 985 (Civil Division).

การที่กระทรวงยุติธรรมของไต้หวันออก TW PDPA Enforcement Rules เพื่อขยายรายละเอียดเกี่ยวกับความหมายของถ้อยคำต่าง ๆ ใน TW PDPA 2015 ซึ่งรวมถึงรายละเอียดและลักษณะของคำว่า “เมื่อวัตถุประสงค์เฉพาะไม่มีอยู่อีกต่อไป” และ “ความจำเป็นต่อการปฏิบัติหน้าที่ราชการหรือทางธุรกิจ” ซึ่งเงื่อนไขสำคัญในการคุ้มครองสิทธิที่จะถูกลืมตามกฎหมายแสดงให้เห็นว่าการออกกฎเกณฑ์เพื่อขยายรายละเอียดของกฎหมายแม่บท (TW PDPA 2015) เป็นเรื่องที่มีความจำเป็นเพื่อการคุ้มครองสิทธิในทางปฏิบัติ

ในขณะเดียวกันความท้าทายในการคุ้มครองสิทธิที่จะถูกลืมซึ่งปรากฏในประเทศอื่น เช่น การชั่งน้ำหนักระหว่างความสมดุลระหว่างประโยชน์สาธารณะและความเป็นส่วนตัว (*Supreme Administrative Court 106 Pan Zi No. 54*) และขอบเขตการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับตัวผู้ให้บริการระบบสืบค้นออนไลน์ซึ่งตั้งอยู่ต่างประเทศ (Taiwan High Court 104 Shang Zi No. 389 (Civil Division)) และการแสดงผลการค้นหาซึ่งอาจไม่ตกอยู่ในบังคับของกฎหมายของไต้หวัน (*Taoyuan District Court 104 Su Zi No. 985 (Civil Division)*)

3.7 เขตปกครองพิเศษฮ่องกง

เขตปกครองพิเศษฮ่องกงได้ตรากฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นครั้งแรกเมื่อ พ.ศ. 2538 โดยเรียกกฎหมายฉบับดังกล่าวว่า Personal Data (Privacy) Ordinance 1996 (“HK PDPO 1996”)[224] โดยที่ HK PDPO 1996 เป็นกฎหมายที่บังคับใช้กับทั้งภาครัฐและภาคเอกชนที่บัญญัติถึงข้อกำหนดต่าง ๆ สำหรับทั้งผู้ใช้ข้อมูลส่วนบุคคลและกำหนดสิทธิให้กับเจ้าของข้อมูลส่วนบุคคลด้วย สิทธิที่จะถูกลืมในฮ่องกงนั้นถูกพิจารณา

[224] Personal Data (Privacy) Ordinance (Cap. 486).

ในลักษณะเป็นข้อกำหนดเกี่ยวกับการลบข้อมูล (Erasure of Data) และการนำข้อมูลออกจากการแสดงผล ซึ่งสามารถอธิบายได้ดังนี้

3.7.1 ตัวบทกฎหมายและแนวปฏิบัติ

3.7.1.1 Personal Data (Privacy) Ordinance

HK PDPO 1996 รับรองถึงสิทธิที่จะถูกลืมในลักษณะเป็นการกำหนดหน้าที่ให้กับผู้ใช้งานข้อมูลส่วนบุคคล (Data User) มากกว่าจะกำหนดให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลโดยตรง[225] โดยหน้าที่อันเกี่ยวกับการลบข้อมูลส่วนบุคคลนั้น ผู้ใช้งานข้อมูลส่วนบุคคลมีหน้าที่ต้องดำเนินการใด ๆ ที่อาจกระทำได้ทั้งหมดเพื่อ “ลบ” ข้อมูลส่วนบุคคลที่ผู้ใช้ข้อมูลส่วนบุคคลมีอยู่ หากว่าข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็นต่อวัตถุประสงค์ในการใช้งานอีกต่อไป (เว้นแต่ว่าการลบข้อมูลส่วนบุคคลนั้นไม่อาจกระทำได้ตามกฎหมายหรือหากการลบข้อมูลส่วนบุคคลจะกระทบต่อประโยชน์สาธารณะหรือประโยชน์ทางประวัติศาสตร์)[226]

โดย HK PDPO 1996 ยังกำหนดให้ผู้ที่ใช้งานข้อมูลส่วนบุคคลอื่นใดที่ควบคุมการประมวลผลข้อมูลส่วนบุคคลนั้นอยู่มีหน้าที่ในการลบข้อมูลส่วนบุคคลออกเช่นเดียวกัน และกำหนดให้เป็นความรับผิดชอบของผู้ที่ใช้งานข้อมูลส่วนบุคคลอื่นที่มีหน้าที่ควบคุมการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับความเสียหายต่าง ๆ ที่เกิดกับการลบข้อมูลส่วนบุคคลนั้น[227]

---

[225] โดยกฎหมายใช้ถ้อยคำว่า “A data user must take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose…”

[226] Personal Data (Privacy) Ordinance (1996), Section 26 (1).

[227] Ibid, Section 26 (2).

นอกจากนี้ ยังมีหลักการการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Principle) ที่ถูกบัญญัติไว้ท้าย HK PDPO 1996 ที่กำหนดหลักการไว้ 4 ประเภท โดยหนึ่งในหลักการดังกล่าวมีการบัญญัติเรื่องที่เกี่ยวกับการลบข้อมูลส่วนบุคคลไว้ในหลักที่ 2 ความถูกต้องและระยะเวลาเก็บรักษาข้อมูลส่วนบุคคล (DPP2) หลักเกณฑ์ในการก่อให้เกิดหน้าที่ในลบข้อมูลส่วนบุคคลนั้นอาจพิจารณาได้จาก “ความถูกต้อง” และ “วัตถุประสงค์” ของการใช้ข้อมูลส่วนบุคคล ซึ่งหากพิจารณาตาม DPP2 (2) ซึ่งกำหนดให้เกิดหน้าที่ในการลบข้อมูลส่วนบุคคลได้ต่อเมื่อ “วัตถุประสงค์” ในการใช้งานข้อมูลส่วนบุคคลนั้น ๆ ไม่มีอยู่อีกต่อไป[228]

อย่างไรก็ตาม ในส่วนของการนำข้อมูลออกจากการแสดงผลการค้นหานั้น สำนักงานคณะกรรมการความเป็นส่วนบุคคลของข้อมูลส่วนบุคคล (Office of the Privacy Commissioner for Personal Data (Hong Kong) : HK PCPD) ได้ให้ความเห็นต่อสิทธิที่จะถูกลืมไว้ว่า สิทธิดังกล่าวยังคงมีกรอบแนวคิดที่ยังไม่แน่นอน แต่พัฒนาการของสิทธินี้อาจเกิดขึ้นอย่างรวดเร็วได้ โดย HK PCPD ไม่ถือว่าสิทธิส่วนบุคคลนั้นเป็นสิทธิเด็ดขาด จึงทำให้ต้องมีการชั่งน้ำหนักและสร้างความสมดุลระหว่างสิทธิส่วนบุคคลและสิทธิอื่น ประโยชน์ต่าง ๆ รวมไปถึงเสรีภาพในการแสดงออกและเข้าถึงข้อมูลข่าวสาร

3.7.1.2 Guidance on Personal Data Erasure and Anonymization

สำนักงาน HK PCPD ได้มีการออกแนวปฏิบัติในการลบข้อมูลส่วนบุคคลและการทำข้อมูลนิรนาม[229] โดยมีสาระสำคัญเพื่อให้ผู้ควบคุม

---

[228] Ibid, Section 26 (1) (a) & (b).

[229] PCPD, ‘Guidance on Personal Data Erasure and Anonymization’ (PCPD,

ข้อมูลส่วนบุคคลสามารถปฏิบัติตามมาตรา 26 ของ HK PDPO 1996 โดย HK PDPC อธิบายว่าแนวทางในการ “ลบ” ข้อมูลส่วนบุคคลที่หมดความจำเป็นในการประมวลผลแล้วนั้น หมายถึงการทำให้ข้อมูลถูกลบหรือทำลายโดยไม่อาจกลับคืนมาได้อีก (Irreversibly) ทั้งนี้ โดยพิจารณาจากลักษณะและการเก็บรักษาข้อมูลด้วย[230] โดยได้ตั้งข้อสังเกตว่าการลบทำลายข้อมูลอิเล็กทรอนิกส์โดยทางกายภาพนั้นสามารถเป็นไปได้ เช่น การเจาะทำลายอุปกรณ์หรือแถบแม่เหล็ก[231]

ในกรณีที่ข้อมูลส่วนบุคคลจะต้องถูกลบตามมาตรา 26 และ DPP2 (2) สำเนาของข้อมูลส่วนบุคคลทุกประเภทไม่ว่าจะอยู่ในรูปของการถ่ายเอกสาร การสำรองข้อมูล หรือสำเนาอิเล็กทรอนิกส์ของข้อมูลส่วนบุคคลจะต้องถูกทำลายทั้งสิ้น ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องเก็บรักษาข้อมูลส่วนบุคคลบางประเภทไว้นานกว่าข้อมูลส่วนบุคคลอื่น นโยบายการลบและเก็บรักษาข้อมูลควรจะอธิบายถึงแนวทางการบริหารจัดการ และแนวทางการปฏิบัติ[232]

3.7.2 กรณีศึกษา

3.7.2.1 David Webb Case

คำวินิจฉัยในกรณีนี้แสดงให้เห็นถึงความท้าทายในการคุ้มครองสิทธิที่จะถูกลืมอันเนื่องจากการต้องชั่งน้ำหนักระหว่างเสรีภาพของสื่อ

April 2014) <https ://www.pcpd.org.hk/english/ publications/files/erasure_e.pdf> accessed 4 October 2021.

[230] Ibid, หน้า 2.

[231] Ibid, หน้า 3.

[232] Ibid.

และการแสดงความคิดเห็นของผู้ให้บริการข้อมูลออนไลน์กับสิทธิในความส่วนตัวของเจ้าของข้อมูลส่วนบุคคล กรณีนี้มีจุดเริ่มต้นจากผู้ร้องและอดีตสามีซึ่งเป็นคู่ความในคดีเกี่ยวกับการสมรสและเป็นบุคคลตามคำพิพากษาที่ศาลมีคำพิพากษาใน ค.ศ. 2000 ถึง 2002 ต่อมาใน ค.ศ. 2010 และ 2012 ผู้ร้องมีคำขอให้ศาลแทนที่ชื่อจริงของผู้ร้องด้วยอักษรย่อในคำพิพากษาซึ่งปรากฏในระบบอ้างอิงเกี่ยวกับข้อมูลทางกฎหมาย (Legal Reference System) และเว็บไซต์ของศาล[233]

ต่อมาผู้ร้องพบชื่อของผู้ร้องซึ่งถูกเปิดเผยโดยไฮเปอร์ลิงค์ (ตัวเชื่อมโยงกับอินเทอร์เน็ต) ที่แสดงข้อความว่า “Who’s Who’s” ที่ถูกแสดงบนเว็บไซต์ชื่อ “Webb-site” ซึ่งเป็นเว็บไซต์ที่ถูกก่อตั้งขึ้นโดย David Webb โดยเมื่อผู้ใช้งานเว็บไซต์ใส่ชื่อของผู้ร้องเข้าไปในกล่องการค้นหาผู้คน (“Search People”) เว็บไซต์ได้นำผู้ใช้งานไปยังหน้า Who’s Who และไฮเปอร์ลิงค์ถูกฝังเอาไว้ในรายการ “Articles” และหากผู้ใช้งานกดเข้าไปที่ Articles และไฮเปอร์ลิงค์ดังกล่าว ผู้ใช้งานจะถูกนำไปยังคำพิพากษาที่ไม่มีการระบุตัวตนของบุคคล (Anonymised Judgments) ในระบบอ้างอิงเกี่ยวกับข้อมูลทางกฎหมาย (Legal Reference System) และเว็บไซต์ของศาล[234]

เว็บไซต์ชื่อ “Webb-site” นั้น มีวัตถุประสงค์ที่เกี่ยวกับคำชี้แจง (Commentary) เกี่ยวกับองค์กรธุรกิจ เศรษฐกิจ ธรรมาภิบาล ธุรกิจ การเงิน และการควบคุมกำกับในฮ่องกง อย่างไรก็ตาม ผู้ร้องเห็นว่าตนได้รับความเสียหายและยื่นคำร้องไปยัง HK PDPC (เพื่อให้มีการดำเนินการ David Webb)[235]

---

[233] PDPC, ‘Media Statement : ‘PCPD Welcomes Administrative Appeals Board’s Decision on Dismissing David Webb’s Appeal Case’ (PDPC, October 2015) <https ://www.pcpd.org.hk/english/news_events/media_statements/press_20151029.html> accessed 17 November 2021.

[234] Ibid.

[235] Ibid.

HK PDPC วินิจฉัยว่า David Webb ฝ่าฝืนต่อหลักการคุ้มครองข้อมูลส่วนบุคคลข้อ 3 (DPP 3) เรื่องการใช้ข้อมูลเนื่องจากเผยแพร่ตัวไฮเปอร์ลิงค์ซึ่งทำให้มีการเปิดเผยถึงตัวตนของผู้ร้องตามคำพิพากษา และมีคำสั่งให้ David Webb ลบไฮเปอร์ลิงค์ดังกล่าวออกจากเว็บไซต์ของตน เนื่องจากคำพิพากษาในกรณีนี้เป็นเรื่องเกี่ยวกับการสมรส กระทบต่อชีวิตส่วนตัว มิใช่หน้าที่สาธารณะ[236]

อย่างไรก็ตาม David Webb ไม่เห็นด้วยกับคำวินิจฉัยของ HK PDPC จึงยื่นคำร้องต่อคณะกรรมการพิจารณาอุทธรณ์ทางปกครอง (Administrative Appeals Board : AAB) เพื่อให้พิจารณาคำวินิจฉัยของ HK PDPC ใน ค.ศ. 2015 ต่อมา AAB จึงได้มีคำสั่งยืนตามคำวินิจฉัยของ HK PDPC และเห็นว่าคำสั่งของ HK PDPC ที่กำหนดให้ David Webb ลบไฮเปอร์ลิงค์และวินิจฉัยว่าการกระทำของ David Webb นั้น ฝ่าฝืนต่อหลักการคุ้มครองข้อมูลส่วนบุคคล เป็นการฝ่าฝืนต่อหลักการดังกล่าวจริง AAB ให้เหตุผลของการพิจารณาคำร้องอุทธรณ์ดังกล่าวโดยวิเคราะห์ถึงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลของศาลและของ David Webb ซึ่งมีความแตกต่างกัน วัตถุประสงค์ของศาลในการเก็บรวบรวมข้อมูลโดยศาลนั้นมีเหตุผลเพื่อให้คำพิพากษาสามารถใช้อ้างอิงในเชิงการเป็นบรรทัดฐานอันเป็นประโยชน์ต่อการทำงานของศาลและประโยชน์สาธารณะ ในขณะที่วัตถุประสงค์ในการเก็บรวบรวมและใช้ข้อมูลของ David Webb นั้นเป็นไปเพื่อการรายงานข้อมูลทั่วไป มิได้เป็นวัตถุประสงค์เดียวกันกับวัตถุประสงค์ของศาล[237]

---

[236] Ibid.

[237] Ibid.

3.7.2.2 X v Privacy Commissioner for Personal Data (Administistrative Appeal No. 15/2019)

คำวินิจฉัยในกรณีนี้มีมูลเหตุจากการที่ข้อมูลส่วนบุคคล (ชื่อ) ของบุคคลที่ถูกจับกุมในการชุมนุมโดยไม่ชอบด้วยกฎหมายและการขัดขวางการปฏิบัติหน้าที่ของเจ้าหน้าที่ใน ค.ศ. 2014 ได้ถูกเผยแพร่ในข่าวและบทความอย่างกว้างขวางโดยรวมไปถึงการเผยแพร่ผ่านระบบออนไลน์[238] ผู้ร้องอธิบายว่าหากผู้ใช้งานพิมพ์ชื่อของผู้ร้องเข้าไปในระบบสืบค้นออนไลน์ (Google) ผลแสดงการค้นหาจะนำผู้ใช้งานไปยังลิงค์ข่าว บทความ และสื่ออิเล็กทรอนิกส์[239] ต่อมาใน ค.ศ. 2017 ผู้ร้องมีคำขอให้ Google LLC ลบผลการค้นหา (Delist)ลิงค์จากหน้าแสดงผลการค้นหาจากระบบการค้นหาของ Google โดยให้เหตุผลว่าข้อมูลที่ถูกแสดงผลทำให้ผู้ร้องเสียชื่อเสียงไม่เป็นความจริง และไม่ได้มีหลักฐานสนับสนุนอย่างเพียงพอ[240] อย่างไรก็ตาม Google LLC ปฏิเสธที่จะดำเนินการตามคำขอของผู้ร้อง[241]

AAB ปฏิเสธที่จะใช้อำนาจสั่งให้ Google LLC ดำเนินการตามคำร้องเนื่องจากข้อจำกัดในเรื่องขอบเขตการใช้บังคับของ HK PDPO 1996 โดย AAB วางหลักว่ากฎหมายของประเทศหนึ่งย่อมไม่มีผลบังคับนอกดินแดนของตนเอง (No Extra-Territorial Effect) และ HK PDPO 1996 นั้นย่อมไม่มีผลบังคับกับบุคคลที่อยู่นอกเขตปกครองพิเศษฮ่องกงในเรื่องที่เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล[242] หรือกล่าวอีกนัยหนึ่ง คือ HK PDPO 1996 มีผลใช้บังคับกับผู้ใช้ข้อมูลซึ่งมีการดำเนินการในเขตแดนของฮ่องกงเท่านั้น[243]

---

[238] X v Privacy Commissioner for Personal Data (Administistrative Appeal No. 15/2019), para 2.

[239] Ibid, para 4.

[240] Ibid, para 5

[241] Ibid, para 6.

[242] Ibid, para 64.

[243] Ibid, para 66.

อย่างไรก็ตาม AAB ได้ตั้งข้อสังเกตเกี่ยวกับเนื้อหาของสิทธิที่จะถูกลืมใน HK PDPO 1996 ว่า “สิทธิที่จะถูกลืม (Right to be Forgotten)” นั้นยังไม่ถูกยอมรับใน HK PDPO 1996 แม้ว่ามาตรา 26 จะกล่าวถึงการลบข้อมูล แต่สิทธิในการขอให้มีการลบข้อมูลเป็นคนละสิทธิกับสิทธิที่จะถูกลืมและมีความเป็นอิสระจากกัน และในปัจจุบันยังไม่มีสิทธิที่จะถูกลืมในฮ่องกง[244]

โดยสรุป เมื่อพิจารณาตัวบทกฎหมายของ HK PDPO 1996 แล้ว สามารถกล่าวได้ว่าการคุ้มครองสิทธิที่จะถูกลืมของฮ่องนั้นมีลักษณะคล้ายคลึงกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอื่น ๆ กล่าวคือ การทำให้มีการ “ลบ” ข้อมูลส่วนบุคคลเมื่อหมดความจำเป็นที่จะต้องประมวลผลตามวัตถุประสงค์ อย่างไรก็ตาม ตัวบทกฎหมายของ HK PDPO 1996 นั้นมิได้กำหนดไว้เพียงหน้าที่ในการลบข้อมูลส่วนบุคคลเท่านั้น หากแต่กำหนดให้ผู้ใช้ข้อมูลต้องดำเนินการใด ๆ ตามที่จำเป็นเพื่อลบข้อมูลส่วนบุคคล ซึ่งแสดงให้เห็นว่าการลบข้อมูลส่วนบุคคลนั้นมีลักษณะเป็นกระบวนการที่จำเป็นต้องอาศัยขั้นตอนในทางปฏิบัติหลายขั้นตอน เพื่อให้การดำเนินเกี่ยวกับการลบข้อมูลมีความเป็นไปได้ HK PDPC จึงได้ออกแนวปฏิบัติในการลบข้อมูลส่วนบุคคลและการทำข้อมูลนิรนามโดยขยายรายละเอียดต่าง ๆ เช่น แนวทางในการลบข้อมูลทั้งในเชิงอิเล็กทรอนิกส์และเชิงกายภาพ

ความท้าทายในการคุ้มครองสิทธิที่จะถูกลืมในฮ่องกงนั้นถูกแสดงอย่างชัดเจนใน David Webb Case และ X v Privacy Commissioner for Personal Data (Administistrative Appeal No. 15/2019) จะเห็นได้ว่าเหตุผลในการปฏิเสธไม่ลบข้อมูลระหว่างตัวเจ้าของฐานข้อมูลและผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์นั้นอาจมีความแตกต่างกัน ศาลอาจมีเหตุผลในการไม่ลบข้อมูลเพื่อประโยชน์ในการอ้างอิงบรรทัดฐานคำวินิจฉัย ในขณะที่ผู้ให้บริการเว็บไซต์ไม่อาจอ้างเหตุดังกล่าวได้ (David Webb case) ในขณะที่

[244] Ibid, para 91.

X v Privacy Commissioner for Personal Data (Administistrative Appeal No. 15/2019 แสดงให้เห็นว่าผู้ให้บริการระบบสืบค้นออนไลน์อาจไม่ตกอยู่ในบังคับของการถูกสั่งให้ลบข้อมูลตามกฎหมายของประเทศหนึ่งได้เนื่องจากข้อจำกัดของขอบเขตการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

3.8 ประเทศฟิลิปปินส์

ในประเทศฟิลิปปินส์มีการบัญญัติกฎหมายความเป็นส่วนบุคคลของข้อมูล (Data Privacy Act 2012 : PH PDA 2012) โดยมีโครงสร้างและลักษณะของข้อกำหนดภายในถูกออกแบบให้เป็นตาม Data Protection Directive (95/46/EC) ของสหภาพยุโรป นอกจากนี้ ยังได้มีการตรา Implementing Rules and Regulations of the Data Privacy Act of 2012 (“PH IRR”) ซึ่งเป็นกฎหมายลำดับรองของ PH DPA 2012 ที่ได้ให้รายละเอียดเกี่ยวกับการลบ (Erasure) การทำลาย (Destruction) และขัดขวาง (Block) ตามกฎหมาย PH DPA 2012 อีกด้วย[245]

3.8.1 ตัวบทกฎหมายและแนวปฏิบัติ

3.8.1.1 Data Privacy Act 2012

PH PDA 2012 กำหนดหลักการของความเป็นส่วนตัวของข้อมูลส่วนบุคคลเอาไว้ประการหนึ่งว่า ข้อมูลส่วนบุคคลนั้นจะต้องมีความถูกต้อง มีความเกี่ยวข้อง มีความเป็นปัจจุบัน (ในกรณีที่จะมีการประมวลผลข้อมูลส่วนบุคคลนั้น) โดยที่ข้อมูลส่วนบุคคลที่คลาดเคลื่อนหรือไม่สมบูรณ์จะต้องถูกแก้ไขหรือทำลาย หรือจำกัดการประมวลผล[246] โดย PH PDA 2012 กำหนดให้สิทธิเจ้าของข้อมูลส่วนบุคคลในการลบ (Erasure) หรือ บล็อก (Block)

[245] Data Privacy Act 2012 (DPA) : RA No. 10173), Section 2 (j).

[246] Ibid, Section 11 (c).

ข้อมูลส่วนบุคคลต่อผู้ควบคุมข้อมูลส่วนบุคคลได้ โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิในการขอให้หยุดชั่วคราว (Suspend) ถอน (Withdraw) หรือสั่งให้มีการขัดขวาง (Block) ลบ (Removal) หรือทำลาย (Destruction) ข้อมูลส่วนบุคคลของตนจากระบบการจัดเก็บไฟล์ (Filing System) ของผู้ควบคุมข้อมูลส่วนบุคคลได้[247]

3.8.1.2 Implementing Rules and Regulations of the Data Privacy Act of 2012

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะหยุด ถอน ขัดขวาง เพิกถอน หรือทำลายข้อมูลส่วนบุคคลของตนจากระบบของผู้ควบคุมข้อมูลส่วนบุคคล หากพบและมีหลักฐานอันควรเชื่อว่า (1) ข้อมูลส่วนบุคคลไม่สมบูรณ์ ไม่เป็นปัจจุบัน ผิด หรือได้รับมาโดยไม่ชอบด้วยกฎหมาย (2) ข้อมูลถูกใช้ไปเพื่อวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลไม่ได้อนุญาต (3) ข้อมูลส่วนบุคคลนั้นไม่จำเป็นต่อวัตถุประสงค์ที่ข้อมูลนั้นถูกเก็บรวบรวมไว้อีกต่อไป (4) เจ้าของข้อมูลส่วนบุคคลประสงค์จะทำการถอนความยินยอม หรือคัดค้านการประมวลผล และไม่ปรากฏว่ามีหลักฐานทางกฎหมายอื่น ๆ หรือประโยชน์อันชอบธรรมที่เหนือกว่าเพื่อให้สามารถประมวลผลต่อไปได้ (5) ข้อมูลนั้นส่งผลร้ายต่อเจ้าของข้อมูลส่วนบุคคล เว้นแต่ว่าเป็นข้อมูลที่ถูกต้องตามเสรีภาพในการพูดแสดงออก หรือในการได้รับข้อมูลข่าวสาร หรือสิทธิเสรีภาพหรือที่ศาลได้อนุญาตไว้ (6) การประมวลผลข้อมูลนั้นไม่ชอบด้วยกฎหมาย และ (7) ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นฝ่าฝืนสิทธิของเจ้าของข้อมูลส่วนบุคคล[248] อย่างไรก็ตาม ไม่ปรากฏว่าทั้ง PH DPA 2012 และ PH IRR ได้มีการขยายความคำว่า “การขอให้หยุดชั่วคราว ถอน หรือสั่งให้มีการขัดขวาง ลบ หรือทำลาย” ว่ามีความแตกต่างกันอย่างไร

---

[247] Ibid, Section 16 (e).

[248] Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 34 (e).

PH IRR กำหนดให้เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติให้เป็นไปตามแนวทาง (Guideline) โดยต้องจัดให้มีนโยบายและกระบวนการเกี่ยวกับการโอน กำจัด (Removal) ทำลาย (Disposal) สื่ออิเล็กทรอนิกส์ และการนำสื่ออิเล็กทรอนิกส์กลับมาใช้ใหม่ ทั้งนี้ เพื่อให้มั่นใจได้ว่ามีการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม[249] รวมไปถึงนโยบายและกระบวนการเกี่ยวกับการป้องกันการทำลายทางเครื่องจักรกล (Mechanical Destruction) ของไฟล์ข้อมูลและเครื่องมืออีกด้วย[250] ซึ่งถือเป็นมาตรการทางความปลอดภัยในการปกป้องคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 25 ที่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการด้านการรักษาความมั่นคงความปลอดภัยที่มีวัตถุประสงค์เพื่อการรักษาไว้ซึ่งความพร้อมใช้งาน (Availability) ความถูกต้อง (Integrity) และการรักษาความลับ (Confidentiality) ของข้อมูลส่วนบุคคลเอาไว้เพื่อป้องกันการทำลายข้อมูลที่เกิดจากอุบัติเหตุหรือการทำลายข้อมูลที่มิชอบด้วยกฎหมาย ซึ่งการทำลายข้อมูลที่มิชอบด้วยกฎหมาย ถือเป็นหนึ่งในเหตุละเมิดข้อมูลส่วนบุคคลด้วยเช่นเดียวกัน[251] และเมื่อมีการเก็บข้อมูลส่วนบุคคลก็ต้องจัดให้มีการทำบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities) โดยบันทึกการเคลื่อนย้าย (Flow) ของข้อมูลภายในหน่วยงาน (Organization) นับตั้งแต่การเริ่มการเก็บรวบรวม ไปจนถึงการประมวลผล และการเก็บรักษาข้อมูล และต้องบันทึกระยะเวลาสำหรับการทำลาย (Disposal) หรือการลบ (Erasure) ข้อมูลส่วนบุคคลนั้นด้วย[252]

---

[249] Ibid, Section 27 (d).

[250] Ibid, Seciton 27 (e).

[251] Ibid, Section 3 (k).

[252] Ibid, Section 26 (c).

3.8.2 กรณีศึกษาของสิทธิที่จะถูกลืมในประเทศฟิลิปปินส์

คดี Vivares v. St. Theresa's College

คดีนี้เป็นคดีเกี่ยวกับสิทธิในความเป็นส่วนบุคคลที่ศาลฎีกาฟิลิปปินส์ตัดสินให้ผู้ร้องแพ้คดีในคดีที่ผู้ร้องได้ยื่นคำร้องว่าสิทธิส่วนบุคคลของผู้ร้องถูกละเมิด เนื่องมาจากภาพถ่ายที่ถูกถ่ายในขณะที่ผู้ร้องนั้นเป็นผู้เยาว์สวมชุดชั้นในขณะกำลังเปลี่ยนเป็นชุดว่ายน้ำในงานเลี้ยงริมชายหาด โดยผู้ร้องทั้งสองได้ถ่ายรูปตนเองในชุดดังกล่าวและต่อมารูปดังกล่าวนั้นได้ถูกอัพโหลดลงบนโปรไฟล์ของบัญชีเฟสบุ๊คที่ชื่อ Angela Lindsay Tan (Angela) ต่อมารูปถ่ายดังกล่าวได้ถูกตรวจพบโดยครูภายในโรงเรียนที่ผู้ร้องทั้งสองกำลังศึกษาอยู่ในขณะนั้น โดยครูคนดังกล่าวได้ทราบเรื่องราวเกี่ยวกับรูปถ่ายของผู้ร้องในขณะสวมใส่ชุดที่ไม่เหมาะสมจากนักเรียนคนอื่นภายในโรงเรียน เนื่องจากมีนักเรียนกลุ่มหนึ่งใช้บัญชีเฟสบุ๊คของตนเข้าไปยังรูปถ่ายนั้นและแสดงรูปถ่ายให้ครูคนดังกล่าวเห็น ทั้งยังมีรูปถ่ายที่ปรากฏรูปผู้ร้องทั้งสองดื่มสุราและสูบบุหรี่ และผู้ร้องทั้งสองอยู่ในลักษณะที่เห็นแต่เพียงชุดชั้นในเท่านั้น ทำให้ครูคนดังกล่าวรายงานเรื่องพฤติกรรมของผู้ร้องทั้งสองไปยังครูที่ทำหน้าที่คุมประพฤตินักเรียนภายในโรงเรียน ทำให้ต่อมาผู้ร้องทั้งสองถูกลงโทษโดยการไม่ให้เข้าร่วมงานพิธีจบการศึกษาของโรงเรียนเนื่องจากมีพฤติกรรมที่ไม่เหมาะสม[253]

---

[253] LawPhil, 'Vivares v. St. Theresa's College GR No. 202666' (LawPhil, September 2014) <https ://lawphil.net/judjuris/juri2014/ sep2014/ gr_202666_2014.html#fnt3> accessed 4 October 2021.

ด้วยเหตุนี้ ผู้ร้องได้ยื่นคำร้องไปยังศาลเพื่อเรียกร้องการชดใช้เยียวยา (Issuance of a Writ of Habeas Data) โดยอ้างว่าการตั้งค่าความเป็นส่วนบุคคลของบัญชีเฟสบุ๊คของนักเรียนนั้นถูกตั้งค่าให้เป็น “เฉพาะเพื่อน” (Friends Only) เท่านั้น ดังนั้น จึงถือได้ว่ายังมีความคาดหวังที่เหมาะสมถึงความต้องการความเป็นส่วนบุคคลอยู่ ความเป็นส่วนบุคคลดังกล่าวจึงควรจำต้องถูกเคารพ อีกทั้งรูปถ่ายที่สามารถเข้าถึงได้นั้นเป็นของผู้ร้องทั้งสอง ดังนั้น จึงไม่สามารถถูกใช้หรือทำซ้ำโดยไม่ได้รับความยินยอมจากผู้ร้อง การที่ครูที่ได้ตรวจพบรูปภาพดังกล่าวในตอนแรกนั้นแล้วทำการบันทึกรูปถ่ายที่ปรากฏผู้ร้องทั้งสองเป็นสำเนาดิจิทัลนั้น เป็นการฝ่าฝืนสิทธิของผู้ร้องทั้งสอง อีกทั้งต่อมายังนำเอารูปถ่ายดังกล่าวไปแสดงต่อบุคคลอื่นได้รับรู้ และรูปถ่ายดังกล่าวยังได้ถูกทำซ้ำและเผยแพร่อย่างชัดแจ้งโดยผู้ถูกร้องไปทั่วในโรงเรียนที่ผู้ร้องทั้งสองศึกษาอยู่[254]

อย่างไรก็ตาม ศาลในคดีนี้ได้ตัดสินว่าผู้ร้องทั้งสองไม่สามารถแสดงให้เห็นถึงการมีอยู่ของการฝ่าฝืนโดยแท้จริงหรือการฝ่าฝืนที่ถูกคุกคามของสิทธิในความเป็นส่วนบุคคลของผู้เยาว์แต่อย่างใด ซึ่งถือเป็นหนึ่งในเงื่อนไขของการชดใช้ เยียวความเสียหายที่เกิดขึ้น อีกทั้ง การที่รูปถ่ายนั้นได้ถูกอัพโหลดลงบนเฟสบุ๊คโดยปราศจากการจำกัดบุคคลที่อาจมองเห็นรูปถ่ายได้มีลักษณะของการที่ความส่วนเป็นส่วนบุคคลนั้นไม่มีอยู่อีกต่อไปแล้ว อีกทั้งการที่โรงเรียนทำการรวบรวมและเผยแพร่รูปถ่ายดังกล่าวเป็นไปเพื่อการปฏิบัติตามนโยบายและกฎระเบียบภายในโรงเรียน และได้ตัดสินว่าผู้ใช้งานอินเทอร์เน็ตจำต้องทำการตรวจสอบกิจกรรมออนไลน์ของตนเองและต้องไม่ละเลยในการปกป้องสิทธิของตนเอง โดยศาลระบุว่าความยุติธรรมนั้นย่อมสนับสนุน

[254] Ibid.

ผู้ที่รอบคอบเสมอ “Equity Serves the Vigilant” และกำหนดให้ผู้ร้องต้องดำเนินการเพื่อปกป้องสิทธิที่ผู้ร้องอ้างว่าได้ถูกละเมิด โดยการปกป้องคุ้มครองจะไม่สามารถเกิดขึ้นได้หากว่าบุคคลไม่ดำเนินการใด ๆ เพื่อขอบเขตความเป็นส่วนบุคคลของตน

คำพิพากษาจากคดีดังกล่าวแม้จะไม่ได้เกี่ยวข้องกับสิทธิที่จะถูกลืมโดยตรง แต่เกี่ยวข้องโดยตรงกับสิทธิความเป็นส่วนบุคคลและสิทธิในการควบคุมข้อมูลส่วนบุคคลที่ถูกเข้าถึงได้ผ่านอินเทอร์เน็ต โดยศาลฎีกาของประเทศฟิลิปปินส์ได้ระบุในคำวินิจฉัยว่า *“เนื่องจากการมีอยู่ของวิธีการในการรวมและแบ่งปันข้อมูล ความเสี่ยงที่ระบบจะถูกล่วงละเมิด จึงมีเหตุผลที่ปัจเจกบุคคลควรจะมีสิทธิในการควบคุมการไหลเวียนของข้อมูล และตัวเจ้าของข้อมูลส่วนบุคคลควรจะสามารถคาดหมายถึงความเป็นส่วนตัวในโลกไซเบอร์”*[255]

โดยสรุป การคุ้มครองสิทธิที่จะถูกลืมในประเทศฟิลิปปินส์นั้นเป็นไปโดยผ่านสิทธิในการขอให้ “ลบ” ข้อมูลส่วนบุคคลตาม PH PDA 2012 อย่างไรก็ตาม กรณีมีข้อสังเกตว่ากฎหมายของประเทศฟิลิปปินส์นั้นมีรายละเอียดเกี่ยวกับสิ่งที่เจ้าของข้อมูลส่วนบุคคลจะมีคำขอได้ กล่าวคือ ขอให้ผู้ควบคุมข้อมูล พักใช้ ถอน หรือสั่งให้มีการขัดขวาง ลบ หรือทำลายข้อมูลส่วนบุคคลของตนจากระบบการจัดเก็บไฟล์ของผู้ควบคุมข้อมูลส่วนบุคคลได้ และเพื่อให้การดำเนินการเป็นไปได้ในทางปฏิบัติ รายละเอียดเกี่ยวกับการลบทำลายข้อมูลจึงถูกกำหนดเอาไว้ใน Implementing Rules and Regulations of the Data Privacy Act of 2012

---

[255] Robert Walters and Marko Novak, Cyber Security, Artificial Intelligence, Data Protection and the Law (Springer Nature Singapore, 2021) p. 204.

3.9 ประเทศสิงคโปร์

ประเทศสิงคโปร์มีกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่ชื่อว่า Personal Data Protection Act 2012 (“SG PDPA 2012”) ซึ่งถูกประกาศใช้เมื่อ ค.ศ. 2012 อย่างไรก็ตาม SG PDPA 2012 มิได้มีการบัญญัติถึงสิทธิที่จะถูกลืมหรือสิทธิที่จะขอให้ลบข้อมูลไว้แต่อย่างใด หากแต่ได้ระบุถึงหน้าที่อันเป็นข้อจำกัดเกี่ยวกับระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล (Rentention Limitation Obligation) เอาไว้ตามมาตรา 25 ของ SG PDPA 2012 โดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ (Personal Data Protection Commission (Singapore) : SG PDPC) ได้ออกแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลโดยให้รายละเอียดเกี่ยวกับระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลซึ่งอาจถูกใช้เพื่อเทียบเคียงกับหน้าที่ในการยุติการประมวลผลข้อมูล

3.9.1 ตัวบทกฎหมายและแนวปฏิบัติ

3.9.1.1 Personal Data Protection Act 2012

SG PDPA 2012 บัญญัติถึง “ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล” โดยระบุว่าองค์กร (ไม่ว่าบุคคลธรรมดาหรือนิติบุคคล)[256] มีหน้าที่ต้อง “หยุดที่จะเก็บรักษา” เอกสารที่มีข้อมูลส่วนบุคคล หรือ “กำจัด (Remove)” ช่องทางที่จะดำเนินการใดต่อข้อมูลส่วนบุคคลโดยไม่ชักช้า เมื่อ (a) วัตถุประสงค์ที่ข้อมูลส่วนบุคคลถูกเก็บรวบรวมหมดลง และ (b) การเก็บรักษาข้อมูลนั้นหมดความจำเป็นเพื่อวัตถุประสงค์ทางกฎหมายหรือธุรกิจอีก[257] โดยมีข้อสังเกต

[256] Personal Data Protection Act 2012, Section 2.

[257] Ibid, Section 25.

ว่าหน้าที่ที่เกี่ยวกับระยะเวลาการเก็บรักษาข้อมูลภายใต้กฎหมาย SG PDPA 2012 นั้น หากเปรียบเทียบกับมาตรา 17 แห่ง GDPR แล้วค่อนข้างมีการบังคับใช้ที่จำกัด[258]

อย่างไรก็ตาม SG PDPA 2012 ไม่ได้กำหนดระยะเวลาในการเก็บข้อมูลส่วนบุคคลไว้อย่างชัดเจน แต่หน่วยงานอาจยึดถือระยะเวลาการเก็บรักษาข้อมูลตามมาตรฐานที่กำหนดโดยกฎหมายที่เกี่ยวข้องกับธุรกิจของหน่วยงานเหล่านั้น ส่วนรายละเอียดเกี่ยวกับข้อจำกัดด้านระยะเวลาการเก็บรักษาข้อมูลนั้นจะเป็นไปตามแนวปฏิบัติที่ออกโดย SG PDPC

3.9.1.2 แนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคล

แนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคล (Advisory Guidelines on Key Concepts in the PDPA) ระบุว่า ระยะเวลาในการเก็บข้อมูลส่วนบุคคลตาม SG PDPA 2012 ขึ้นอยู่กับปัจจัย ดังต่อไปนี้ **ประการที่หนึ่ง** วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล ได้แก่ (1) ข้อมูลส่วนบุคคลนั้นได้ถูกเก็บรักษาไว้ตราบเท่าที่วัตถุประสงค์ของการเก็บข้อมูลทั้งหมดหรือบางส่วนยังคงมีอยู่ และ (2) ข้อมูลส่วนบุคคลจำต้องไม่ถูกเก็บรักษาไว้ในลักษณะ “เผื่อว่า” จำต้องใช้ข้อมูลส่วนบุคคลเหล่านั้นเพื่อวัตถุประสงค์อื่น ๆ ที่ไม่ได้แจ้งต่อเจ้าของข้อมูลส่วนบุคคล[259]

---

[258] Nadia Yeo, op. cit., p. 106.

[259] Personal Data Protection Commission (Singapore), ‘Advisory Guidelines on Key Concepts in the PDPA’ (PDPC, 24 September 2013) <https ://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2013/09/advisory-guidelines-on-key-concepts-in-the-pdpa-24-sept.pdf> accessed 4 October 2021, para 16.4.

ประการที่สอง การเก็บรักษาข้อมูลส่วนบุคคลโดยหน่วยงานถือเป็นเรื่องจำเป็นต่อวัตถุประสงค์ทางกฎหมายหรือวัตถุประสงค์ธุรกิจอื่น ๆ รวมไปถึงกรณีที่ (1) ข้อมูลส่วนบุคคลนั้นจำเป็นต่อการฟ้องร้องดำเนินคดี (Legal Action) ที่เกี่ยวข้องกับหน่วยงานที่กำลังดำเนินอยู่ (2) การเก็บข้อมูลส่วนบุคคลนั้นจำเป็นเพื่อปฏิบัติหน้าที่ตามกฎหมายที่ใช้บังคับ กฎระเบียบ มาตรฐานเรื่องการเก็บรักษาข้อมูลส่วนบุคคลระหว่างประเทศ ภูมิภาค หรือความตกลง (Bilateral) อื่น ๆ ที่หน่วยงานมีหน้าที่ต้องปฏิบัติตาม และ (3) ข้อมูลส่วนบุคคลที่หน่วยงานจำต้องใช้เพื่อการปฏิบัติงานด้านธุรกิจ เช่น การจัดทำรายงานประจำปี หรือแผนคาดการณ์การดำเนินงาน[260]

โดยที่หน่วยงานอาจมีการจัดทำหรือกำหนดกรอบเวลาในการเก็บรักษาข้อมูลภายในหน่วยงานของตนได้ แต่ต้องเป็นระยะเวลาที่สอดคล้องกับระยะเวลาที่ควรเก็บรักษาข้อมูลส่วนบุคคลด้วย ทั้งนี้ หน่วยงานอาจใช้นโยบายด้านระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลกับประเภทหรือกลุ่มของข้อมูลส่วนบุคคลบางประเภทได้ด้วย โดยหน่วยงานอาจยุติการเก็บรักษาเอกสารที่มีข้อมูลส่วนบุคคลเมื่อหน่วยงาน หรือตัวแทนหรือตัวกลางด้านข้อมูล (Data Intermediaries) ของหน่วยงานนั้น ไม่อาจเข้าถึงข้อมูลส่วนบุคคลที่ตัวแทนหรือตัวกลางมีอยู่อีกต่อไปด้วยวิธีการตามกรณีตัวอย่าง ดังนี้ (1) อาจคืนเอกสารที่มีข้อมูลส่วนบุคคลกลับไปยังเจ้าของข้อมูลส่วนบุคคล (2) ส่งเอกสารนั้นไปยังบุคคลอื่นตามคำสั่งของเจ้าของข้อมูลส่วนบุคคล (3) ทำลายเอกสาร เช่น โดยการใช้เครื่องทำลายเอกสาร หรือทำลายทิ้งด้วยวิธีการที่เหมาะสม หรือ (4) ทำให้ข้อมูลส่วนบุคคลนั้น ๆ เป็นนิรนาม[261]

---

[260] Ibid.

[261] Ibid, para 16.10.

3.9.2 กรณีศึกษา

SG PDPC มีโอกาสได้ใช้ SG PDPA 2012 เป็นฐานในคุ้มครองสิทธิที่จะถูกลืมโดยอาศัยข้อจำกัดในเรื่องระยะเวลาการเก็บรักษาข้อมูล ในกรณี *Re Credit Bureau (Singapore) Pte Ltd* ซึ่งเป็นกรณีที่สถาบันการเงินแห่งหนึ่งได้เผยแพร่ข้อมูลเกี่ยวกับการล้มละลายของผู้ร้อง ซึ่งรวมถึงข้อมูลเกี่ยวกับ “HX” Ratings เป็นเวลาห้าปีในส่วนที่เป็นรายงานเกี่ยวกับเครดิตของผู้บริโภคซึ่งผู้ร้องโต้แย้งว่าข้อมูลที่ถูกเผยแพร่ดังกล่าวไม่เกี่ยวข้องกับตนอีกแล้วและไม่ความจำเป็นที่จะต้องเก็บรวบรวมข้อมูลอีกต่อไป[262]

อย่างไรก็ตาม SG PDPC พบว่าระยะเวลาห้าปีนั้นสอดคล้องกับระยะเวลาการแสดงข้อมูลเกี่ยวกับการล้มละลายตามหน่วยงานรัฐด้านการล้มละลาย SG PDPC มองว่าระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลเป็นเวลาห้าปีนั้น สามารถช่วยให้สถาบันการเงินมีข้อมูลเกี่ยวกับประวัติด้านเครดิตของบุคคลซึ่งอาจเป็นผู้กู้ที่เป็นประโยชน์ต่อการพิจารณาให้สินเชื่อ และการเก็บรักษาข้อมูลเกี่ยวกับการล้มละลายนั้นยังมีความสมเหตุสมผลด้านธุรกิจ[263]

โดยสรุป SG PDPA 2012 ไม่ได้บัญญัติถึงสิทธิที่จะถูกลืมโดยชัดแจ้ง แต่บัญญัติถึงการลบข้อมูลเมื่อพ้นระยะเวลาการเก็บรักษาข้อมูล โดยแนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคล (Advisory Guidelines on Key Concepts in the PDPA) ได้กำหนดปัจจัยที่ใช้ในการพิจารณาว่าเวลาในการเก็บรักษาข้อมูลส่วนบุคคลนั้นจะหมดลงเมื่อใด ความสำคัญของการพิจารณาระยะเวลานั้นถูกแสดงให้เห็นในกรณี *Re Credit Bureau (Singapore) Pte Ltd* กล่าวคือ หากยังปรากฏประโยชน์และความจำเป็นในการเก็บข้อมูลส่วนบุคคลเอาไว้ (เช่น เพื่อประโยชน์ด้านการพิจารณาสินเชื่อ) ผู้ควบคุมข้อมูลส่วนบุคคลย่อมอาศัยเหตุดังกล่าวเพื่อเก็บข้อมูลส่วนบุคคลเอาไว้ได้

---

[262] Nadia Yeo, op. cit., p. 107.

[263] Ibid.

บทสรุป

การศึกษาตัวบทกฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายลำดับรอง แนวปฏิบัติ คำวินิจฉัย และคำพิพากษาของศาลทั้งในประเทศไทยและต่างประเทศดังที่กล่าวในหัวข้อ 3.1 ถึง 3.9 ในบทที่ 3 นี้แสดงให้เห็นถึงสาระสำคัญของกฎหมายซึ่งมีภารกิจในการคุ้มครองสิทธิที่จะถูกลืมอยู่สี่ประการ ได้แก่ (1) การกำหนดตัวผู้ทรงสิทธิ (2) การกำหนดผู้มีหน้าที่คุ้มครองสิทธิ (3) การกำหนดเนื้อหาของสิทธิที่จะถูกลืม และ (4) การกำหนดข้อจำกัดของสิทธิที่จะถูกลืม

ประการแรก กฎหมายคุ้มครองข้อมูลส่วนบุคคลระบุถึงตัวผู้ทรงสิทธิกล่าวคือตอบคำถามที่ว่า “ใคร” เป็นผู้ทรงสิทธิที่จะสามารถเรียกร้องให้มีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้ กฎหมายของทุกประเทศระบุว่าผู้ทรงสิทธิได้แก่ “เจ้าของข้อมูลส่วนบุคคล” โดยมีข้อสังเกตว่าสิทธิดังกล่าวถูกบัญญัติให้ตัวเจ้าของข้อมูลส่วนบุคคลมีสิทธิ “เรียกร้อง” ให้มีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคล โดยมีเพียงมาตรา 17 ของ GDPR เท่านั้นที่บัญญัติเจาะจงถึง “สิทธิที่จะถูกลืม (Right to be Forgotten)” ส่วนกฎหมายของประเทศอื่น ๆ (รวมถึงของประเทศไทย) ไม่ได้เรียกสิทธิในการขอให้มีลบข้อมูลว่า “สิทธิที่จะถูกลืม”

ประการที่สอง กฎหมายคุ้มครองข้อมูลส่วนบุคคลระบุถึงผู้มีหน้าที่ดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลซึ่งไม่ได้ถูกเรียกว่าผู้ควบคุมข้อมูลส่วนบุคคลในทุก ๆ กรณี กฎหมายของประเทศไทย GDPR UK DPA PH DPA 2012 กำหนดหน้าที่ลบข้อมูลตามคำขอแก่ “ผู้ควบคุมข้อมูลส่วนบุคคล” ในขณะที่ AUS PA 2018 ระบุถึงหน้าที่ผู้รายงานด้านเครดิต ส่วน JAP APPI 2020 กำหนดหน้าที่ให้แก่ผู้ใช้งานข้อมูลส่วนบุคคล (Personal Information Handling Business Operator) TW PDPA 2015 กำหนดหน้าที่ให้แก่

“หน่วยงานของรัฐ (Government Agency)” และ “องค์กรนอกภาครัฐ (Non-Government Agency) HK PDPO 1996 กำหนดหน้าที่ให้แก่ “ผู้ใช้ข้อมูล” และ SG PDPA 2012 กำหนดหน้าที่ให้แก่ “องค์กร” ที่ทำการประมวลผลข้อมูล

ประการที่สาม ในส่วนเนื้อหาของสิทธิที่จะถูกลืมนั้นกฎหมายของทุกประเทศให้ความสำคัญกับการลบข้อมูลส่วนบุคคล (โดยไม่เน้นที่การถูกลืม) เพื่อประโยชน์ในการดำเนินการของบุคคลที่เกี่ยวข้อง จึงมีการออกแนวปฏิบัติที่เกี่ยวข้องกับการลบข้อมูลส่วนบุคคล กล่าวคือ แนวปฏิบัติที่เกี่ยวกับประเภทหรือลักษณะของสิทธิที่จะถูกลืมที่อยู่บนโปรแกรมสืบค้นข้อมูลของสหภาพยุโรป โดย EDPB แนวปฏิบัติที่เกี่ยวข้องกับวิธีการลบข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคล (ในส่วนของการลบข้อมูล) ของสหราชอาณาจักร โดย ICO แนวทางการปฏิบัติเกี่ยวหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศออสเตรเลีย กฎเพื่อบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของไต้หวัน แนวปฏิบัติในการลบข้อมูลส่วนบุคคลและการทำข้อมูลนิรนามของฮ่องกง และแนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ อย่างไรก็ตาม กรณีศึกษาและคำวินิจฉัยต่าง ๆ แสดงให้เห็นว่าการลบผลการค้นหานั้นอาจไม่ได้ทำให้มีการลบข้อมูลโดยผู้เผยแพร่ข้อมูลอื่น

ประการที่สี่ สิทธิที่จะถูกลืมถูกจำกัดได้โดยความจำเป็นที่บุคคลอื่นมีสิทธิในการเข้าถึงข้อมูลและเสรีภาพในการแสดงความคิดเห็น ประโยชน์สาธารณะอื่นอันเกิดจากการที่ข้อมูลไม่ถูกลบ และข้อจำกัดของกฎหมายที่ไม่อาจมีผลบังคับในต่างประเทศไทย จากองค์ประกอบทั้งสี่ข้อนี้ มีความจำเป็นต้องวิเคราะห์ต่อไปว่ามาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น สามารถคุ้มครองสิทธิที่จะถูกลืมได้เพียงใดและมีข้อจำกัดประการใดหรือไม่หากเปรียบเทียบกับกฎหมายของต่างประเทศ

บทที่ 4
วิเคราะห์มาตรการทางกฎหมายของประเทศไทยเกี่ยวกับสิทธิที่จะถูกลืมและแนวทางแก้ไข

งานวิจัยนี้มีวัตถุประสงค์ประการสำคัญ คือ เพื่อศึกษาการบัญญัติเกี่ยวกับสิทธิที่จะถูกลืมในกฎหมายไทยว่ามีความครอบคลุมเพียงใด และมีหลักเกณฑ์ตลอดจนแนวทางในการบังคับใช้อย่างไร ด้วยเหตุนี้ จึงมีความจำเป็นที่จะต้องทำการ “ประเมิน” ตัวบทกฎหมายตามมาตรา 33 และ 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ว่ามี “ความครอบคลุม” เพียงใด การศึกษาในบทที่ 2 และบทที่ 3 แสดงให้เห็นว่า กฎหมายที่จะทำหน้าที่คุ้มครองสิทธิที่จะถูกลืมนั้นมีเนื้อหาและองค์ประกอบหลายประการ อีกทั้งยังต้องมีความพร้อมที่จะเผชิญกับลักษณะของการแสดงผลและการเข้าถึงข้อมูลในปัจจุบันโดยเฉพาะอย่างยิ่งการเข้าถึงและการแสดงผลข้อมูลผ่านระบบออนไลน์และสื่ออิเล็กทรอนิกส์ต่าง ๆ ซึ่งงานวิจัยนี้เลือกที่จะทำการประเมินดังกล่าวโดยอาศัยวิธีการศึกษาและวิเคราะห์กฎหมายในเชิงเปรียบเทียบ กล่าวคือ

การวิเคราะห์และเปรียบเทียบมาตรา 33 และ 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับกฎหมายที่มีภารกิจในการคุ้มครองสิทธิที่จะถูกลืมในต่างประเทศ (ตามที่ได้อธิบายในบทที่ 3) เพื่อให้เกิดความเข้าใจถึงความคล้ายคลึงและแตกต่างของกฎหมายไทยและต่างประเทศ[264] และท้ายที่สุดเพื่อเผยให้เห็นถึงข้อจำกัดของกฎหมายไทยเพื่อประโยชน์ในการพัฒนาบทบัญญัติอันจะได้นำเสนอในบทที่ 5 ต่อไป

การเปรียบเทียบตัวบทกฎหมาย (และข้อเท็จจริงในสังคมโดยผ่านคำวินิจฉัยของศาลและหน่วยงานของรัฐ) ในบทที่ 4 นี้ เป็นไปโดยยึดโยงกับองค์ประกอบอันเป็นสาระสำคัญของกฎหมายซึ่งมีภารกิจในการคุ้มครองสิทธิที่จะถูกลืม ดังที่ได้สรุปในบทที่ 3 ได้แก่ (4.1) ผู้ทรงสิทธิที่จะถูกลืม (4.2) ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม (4.3) รายละเอียดการคุ้มครองสิทธิที่จะถูกลืม และ (4.4) ข้อจำกัดของสิทธิที่จะถูกลืม

4.1 การบัญญัติถึงตัวผู้ทรงสิทธิที่จะถูกลืม

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติให้ “เจ้าของข้อมูลส่วนบุคคล” มีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ การบัญญัติให้เจ้าของข้อมูลส่วนบุคคลเป็นผู้ทรงสิทธิ อันเป็นแนวทางการบัญญัติกฎหมายที่สอดคล้องกับมาตรา 17 ของ GDPR มาตรา 47 ของ UK DPA 2018 มาตรา 3 ของ TW PDPA 2015 มาตรา 26 ของ HK PDPO 1996 และมาตรา 16 ของ PH PDA 2012[265] ซึ่งสามารถกล่าวได้ว่าการที่กฎหมายจะคุ้มครองสิทธิที่จะถูกลืมได้นั้นมีจุดเริ่มต้นจากการที่กฎหมายกำหนดตัวผู้ทรงสิทธิเสียก่อน

---

[264] Edward J. Eberle, op. cit., p. 452.

[265] โปรดดูข้อเปรียบเทียบเรื่องผู้ทรงสิทธิที่จะถูกลืม ในเอกสารหมายเลข 1 ในภาคผนวก.

4.1.1 เจ้าของข้อมูลส่วนบุคคล (Data Subject)

มาตรา 17 ของ GDPR บัญญัติให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบหรือทำลายข้อมูลส่วนบุคคล และได้ให้นิยามคำว่า “เจ้าของข้อมูลส่วนบุคคล” ตามมาตรา 4 (1) เอาไว้ว่า เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง บุคคลที่สามารถถูกระบุอัตลักษณ์ได้ ไม่ว่าจะโดยตรงหรือโดยอ้อม โดยเฉพาะอย่างยิ่งด้วยการอ้างอิงจากสิ่งระบุอัตลักษณ์เป็นการเฉพาะ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลสถานที่ สิ่งระบุอัตลักษณ์ออนไลน์ หรือปัจจัยอย่างหนึ่งหรือมากกว่าที่เจาะจงไปยังอัตลักษณ์ทางกายภาพ กายวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคลธรรมดานั้น ในทำนองเดียวกัน UK DPA 2018 ก็บัญญัติรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลให้สามารถร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบหรือทำลายข้อมูลส่วนบุคคลได้ตามตามมาตรา 47 โดยที่ UK DPA 2018 ได้ให้นิยามว่าเจ้าของข้อมูลส่วนบุคคลเอาไว้ตามนิยามของเจ้าของข้อมูลส่วนบุคคลที่กำหนดไว้ใน GDPR

เช่นเดียวกับแนวทางที่ปรากฏในสหภาพยุโรป กฎหมายคุ้มครองข้อมูลส่วนบุคคลในทวีปเอเชีย เช่น เขตปกครองพิเศษไต้หวันและประเทศฟิลิปินส์ มาตรา 3 ของ TW PDPA 2015 กำหนดให้สิทธิเจ้าของข้อมูลส่วนบุคคลมีสิทธิในการลบข้อมูลส่วนบุคคลเช่นเดียวกัน โดยให้นิยามคำว่า “เจ้าของข้อมูลส่วนบุคคล (Data Subject)” ว่าหมายถึง บุคคลธรรมดาที่เป็นเจ้าของข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม ประมวลผลและใช้งาน มาตรา 16 (e) ของ PH PDPA 2012 กำหนดให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) มีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบหรือทำลายข้อมูลส่วนบุคคล โดยได้ให้นิยามว่า เจ้าของข้อมูลส่วนบุคคล หมายถึง บุคคลธรรมดาซึ่งข้อมูลส่วนบุคคลของบุคคลคนนั้นถูกประมวลผล

ในขณะที่ มาตรา 2 ของ HK PDPO นั้น ได้กำหนดนิยามของเจ้าของข้อมูลส่วนบุคคล (Data Subject) เอาไว้ว่าเป็นปัจเจกบุคคล (Individual) ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตาม มีข้อสังเกตว่า มาตรา 26 ของ HK PDPO 1996 นั้น มิได้บัญญัติโดยรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลที่จะร้องขอให้มีการลบทำลายข้อมูลส่วนบุคคลโดยตรง หากแต่บัญญัติให้ตัวผู้ใช้ข้อมูล (Data User) ซึ่งได้แก่ บุคคลที่มีอำนาจในการเก็บรวบรวม ถือครอง ประมวลผล และใช้ข้อมูลส่วนบุคคล[266] มีหน้าที่ในการลบทำลายข้อมูลส่วนบุคคลที่หมดความจำเป็นที่จะต้องถูกประมวลผลตามวัตถุประสงค์อีกต่อไป จึงอาจกล่าวได้ว่ามาตรา 26 ของ HK PDPO 1996 นี้ มีลักษณะที่สอดคล้องกับหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มากกว่าจะเป็นบทบัญญัติในส่วนของสิทธิที่ของเจ้าของข้อมูลส่วนบุคคลมาตรา 33 โดยตรง

4.1.2 ปัจเจกบุคคล (Individual)

อย่างไรก็ตาม การกำหนดถึงตัวบุคคลผู้ทรงสิทธิที่จะถูกลืมนั้นมิได้ถูกดำเนินการผ่านคำว่าผู้ทรงสิทธิเท่านั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลอาจใช้ถ้อยคำอื่นในการกำหนดตัวผู้ทรงสิทธิได้ เช่น AUS PA 1988 กำหนดให้ผู้ทรงสิทธิที่ข้อมูลส่วนบุคคลของบุคคลคนนั้นจะถูกทำลายได้แก่ “ปัจเจกบุคคล (Individual)” ซึ่งหมายรวมถึงบุคคลธรรมดา โดยกฎหมายของประเทศออสเตรเลียได้บัญญัตินิยามของคำว่า Individual เอาไว้ว่า “บุคคลธรรมดา”

มาตรา 25 ของ SG PDPA 2012 บัญญัติให้มีการยุติการเก็บและลบทางเชื่อมต่อกับข้อมูลส่วนบุคคลเมื่อหมดเวลาของการเก็บรักษาข้อมูลส่วนบุคคล โดยไม่ได้บัญญัติรับรองว่าตัวเจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอ

[266] Personal Data (Privacy) Ordinance (1996), Section 2.

ให้มีการลบทำลายข้อมูลส่วนบุคคลโดยตรงซึ่งอาจกล่าวได้ว่าเป็นแนวทางที่สอดคล้องกับมาตรา 26 ของ HK PDPO 1996 ในเชิงของเนื้อหานั้น SG PDPA 2012 ไม่ได้บัญญัติถึงคำว่าเจ้าของของข้อมูลส่วนบุคคลโดยตรง หากแต่ได้บัญญัติถึง “ปัจเจกบุคคล (Individual)” โดยได้ระบุเอาไว้ในนิยามของข้อมูลส่วนบุคคล (ข้อมูลที่ทำให้ระบุถึงตัวตนของปัจเจกบุคคลได้[267])

4.1.3 ตัวการ (Principal)

นอกเหนือจากการคุ้มครองสิทธิที่จะถูกลืมของตัวเจ้าของข้อมูลส่วนบุคคล (Data Subject) และตัวปัจเจกบุคคล (Individual) การบัญญัติถึงตัวบุคคลที่กฎหมายจะคุ้มครองนั้นยังสามารถใช้ถ้อยคำอื่นตามแนวทางของ JP APPI 2020 ได้อีกด้วย JP APPI 2020 นั้น ก็ไม่ได้บัญญัติถึง “เจ้าของข้อมูลส่วนบุคคล” ดังกรณีของมาตรา 17 ของ GDPR มาตรา 47 ของ UK DPA 2018 มาตรา 3 ของ TW PDPA 2015 มาตรา 26 ของ HK PDPO 1996 และมาตรา 16 ของ PH PDA 2012 หากแต่บัญญัติให้ “ตัวการ (Principal)” มีสิทธิร้องขอให้ผู้ทำการประมวลผลข้อมูลส่วนบุคคลหยุดการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 30 โดยได้บัญญัตินิยามของตัวการว่าหมายถึงปัจเจกบุคคลใด ๆ ที่ถูกเผยให้เห็นถึงตัวตนได้โดยข้อมูลส่วนบุคคล[268]

การบัญญัติกฎหมายของประเทศญี่ปุ่นเป็นแนวทางที่คล้ายคลึงกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศออสเตรเลีย (AUS PA 1988) และประเทศสิงคโปร์ (SG PDPA 2012) ซึ่งระบุถึงผู้ทรงสิทธิที่จะถูกลืมโดยอาศัยคำว่าปัจเจกบุคคลซึ่งแตกต่างไปจากแนวทางการบัญญัติกฎหมายตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

---

[267] Personal Data Protection Act 2012, Section 2.

[268] Act on the Protection of Personal Information (The amended Act fully put into effect on April 1, 2022), Section 2 (8).

4.2 การบัญญัติถึงตัวผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม

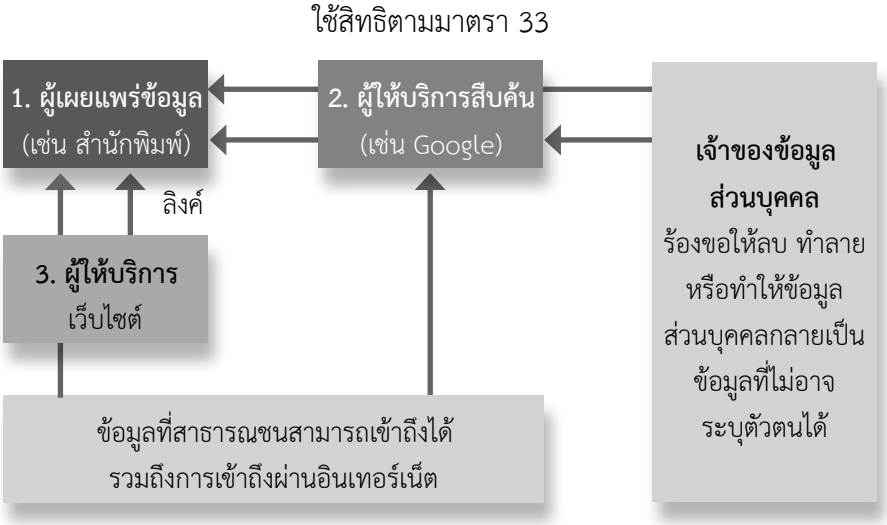
เมื่อมีผู้ทรงสิทธิก็ย่อมหลีกเลี่ยงไม่ได้ที่จะต้องมีผู้มีหน้าที่ต้องคุ้มครองสิทธิที่จะถูกลืมหรือกล่าวอีกนัยหนึ่งก็คือต้องมีการระบุถึงตัวผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม ถ้อยคำที่ถูกใช้เพื่อกำหนดหน้าที่ดังกล่าวตามในกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้แก่ ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) (ตามกฎหมายของประเทศไทย GDPR UK DPA 2018 PH PDPA 2012) ผู้ใช้ข้อมูล (Data User) (ตาม HK PDPO 1996) ผู้ประกอบธุรกิจที่ประมวลผลข้อมูลส่วนบุคคล (Personal Information Handling Business Operator) (ตาม JAP APPI 2020) ในขณะที่ TW PDPA 2015 บัญญัติหน้าที่ในการคุ้มครองสิทธิที่จะถูกลืมให้กับหน่วยงานของรัฐและองค์กรนอกภาครัฐ แม้ว่าการใช้ถ้อยคำจะมีความแตกต่างกัน แต่อย่างไรก็ตาม กฎหมายคุ้มครองข้อมูลส่วนบุคคลของทุกประเทศมีสาระสำคัญต้องตรงกันคือกำหนดหน้าที่ให้กับผู้ที่มีอำนาจตัดสินใจในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

4.2.1 ผู้ให้บริการระบบสืบค้นออนไลน์

4.2.1.1 การแยกความแตกต่างระหว่างผู้ให้บริการระบบสืบค้นออนไลน์กับผู้ควบคุมข้อมูลส่วนบุคคลอื่น

กฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ได้บัญญัติถึง “ผู้ให้บริการระบบสืบค้นออนไลน์” โดยตรง แต่คำวินิจฉัยและคำพิพากษาของศาลในต่างประเทศได้เผยให้เห็นว่า การคุ้มครองสิทธิที่จะถูกลืมนั้นมีความจำเป็นที่จะต้องครอบคลุมไปถึงผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์นอกเหนือไปจากตัวผู้ทำการเผยแพร่ข้อมูลดั้งเดิม เช่น สำนักพิมพ์หรือหน่วยงานรัฐที่ทำหน้าที่เผยแพร่ข้อมูลตามขอบเขตแห่งอำนาจหน้าที่ของตนซึ่งสามารถแสดงได้ตามแผนภาพที่ 4-1 ดังนี้

แผนภาพที่ 4-1 : บุคคลที่มีหน้าที่คุ้มครองข้อมูลส่วนบุคคล



ตามแผนภาพที่ 4-1 ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลอาจถูกเผยแพร่โดยผู้เผยแพร่ข้อมูล เช่น สำนักพิมพ์ซึ่งทำการตีพิมพ์เผยแพร่ข่าวสารผ่านเว็บไซต์ของตน เช่น สำนักพิมพ์ La Vanguardia ซึ่งตีพิมพ์ข้อมูลเกี่ยวกับถูกบังคับคดีของ Mario Costeja González ในคดี *Google Spain v AEPD and Mario Costeja González* กระทรวงยุติธรรมซึ่งเผยแพร่ข้อมูลเกี่ยวกับคำพิพากษาของศาลในกรณี David Webb Case ผู้ใช้งานอินเทอร์เน็ตสามารถเข้าถึงข้อมูลส่วนบุคคลที่ถูกเผยแพร่โดยอาศัยผลการแสดงการค้นหาที่แสดงผลโดยผู้ให้บริการสืบค้นเช่น Google นอกจากนี้ผลแสดงการค้นหาที่ Google แสดงนั้นยังทำให้ผู้ใช้งานอินเทอร์เน็ตเข้าถึงข้อมูลที่ผู้เผยแพร่ข้อมูลทำการเผยแพร่โดยผ่านเว็บไซต์ของบุคคลอื่น ดังเช่นเว็บไซต์ของ David Webb ในกรณี David Webb Case ซึ่งผู้ใช้งานอินเทอร์เน็ตสามารถเข้าถึงคำพิพากษาโดยผ่านเว็บไซต์ของ David Webb

ฐานทางกฎหมายในการคงผลการค้นหาของบุคคลดังกล่าวนี้อาจมีความแตกต่างกันและต้องพิจารณาเป็นรายกรณี จากกรณี David Webb Case กระทรวงยุติธรรมยังคงมีเหตุผลที่จะแสดงคำพิพากษาซึ่งมีข้อมูลส่วนบุคคลของปัจเจกบุคคลตราบเท่าที่มีความจำเป็นในการใช้ข้อมูลนี้เพื่อประโยชน์ในการอ้างอิงและเพื่อประโยชน์สาธารณะ ในขณะที่ David Webb ไม่อาจอ้างอิงเหตุผลเช่นเดียวกับการกระทรวงยุติธรรมได้ เนื่องจากเว็บไซต์นี้มีวัตถุประสงค์เพียงการให้ข้อมูลทั่วไปแก่สาธารณะ ในทำนองเดียวกันผลการค้นหาของ Google ซึ่งนำผู้ใช้งานอินเทอร์เน็ตไปยังเว็บไซต์ของ David Webb ก็ไม่อาจอ้างเหตุผลที่กระทรวงยุติธรรมอ้างได้เช่นกัน

หากพิจารณาจากมุมมองของ “ตัวบทกฎหมาย” การกำหนดหน้าที่ให้กับ “ผู้ควบคุมข้อมูลส่วนบุคคล” (หรือถ้อยคำอื่น ๆ ไม่ว่าจะเป็นผู้ใช้ข้อมูลหรือผู้ประกอบธุรกิจที่ประมวลผลข้อมูลส่วนบุคคล) ไม่ได้ก่อปัญหาว่าผู้มีอำนาจตัดสินใจในการประมวลผลข้อมูลบางรายจะไม่อยู่ในคำนิยาม ไม่ว่าจะเป็นสำนักพิมพ์หรือหน่วยงานรัฐซึ่งเป็นผู้เผยแพร่ข้อมูลส่วนบุคคลตั้งแต่แรก ผู้ให้บริการเว็บไซต์หรือผู้ให้บริการสืบค้นข้อมูลส่วนบุคคลล้วนมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หากปรากฏข้อเท็จจริงว่ามีอำนาจตัดสินใจว่าจะประมวลผลข้อมูลส่วนบุคคลในลักษณะใด

4.2.1.2 ผู้ให้บริการระบบสืบค้นออนไลน์ซึ่งตั้งอยู่ต่างประเทศ

ข้อจำกัดในการกำหนดหน้าที่แก่ผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์ เช่น Google นั้นไม่เกิดตัวบทกฎหมายที่กำหนดหน้าที่ แต่เป็นข้อจำกัดของการที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศหนึ่งย่อมไม่มีผลบังคับถึงบุคคลซึ่งทำการประมวลผลข้อมูลจากต่างประเทศ

(Extra-Territorial Effect) ในคดี *Google Spain v AEPD and Mario Costeja González* ศาลวินิจฉัยว่าเพื่อให้สิทธิร้องขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลนั้นถูกคุ้มครองอย่างแท้จริง CJEU ได้วินิจฉัยว่าการจำกัดให้การดังกล่าวถูกใช้ได้เฉพาะกับโดเมนในสหภาพยุโรปนั้น ส่งผลให้การคุ้มครองไม่อาจเกิดขึ้นอย่างเพียงพอได้ ในทางปฏิบัติ สิทธิในการขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลควรครอบคลุมถึงโดเมนที่เกี่ยวทุกโดเมนรวมไปถึงโดเมน “.com” ด้วย

นอกจากนี้ ในคดี *Google LLC v CNIL* ศาลมีคำวินิจฉัยเกี่ยวกับขอบเขตการใช้บังคับในทางพื้นที่ของกฎหมายว่า คำสั่งให้นำข้อมูลออกจากระบบการสืบค้นนั้นจะมีผลบังคับในประเทศใดบ้าง แม้การนำข้อมูลออกจากระบบ “ควร” จะถูกคุ้มครองในทุกประเทศสมาชิก อย่างไรก็ตาม การคุ้มครองสิทธินี้ก็ยังไม่ได้เป็นอันหนึ่งอันเดียวกันในทุกประเทศ[269] ทำนองเดียวกับ CJEU

โดยสอดคล้องกับคำวินิจฉัยของ CJEU ในคดี *Google Spain v AEPD and Mario Costeja González* และคดี *Google LLC v CNIL* ศาลของประเทศในทวีปเชียก็ได้แสดงให้เห็นถึงข้อจำกัดในการบังคับใช้กฎหมายในต่างประเทศ เช่น ศาลของไต้หวันในคดี *Taoyuan District Court 104 Su Zi No. 985 (Civil Division)* ซึ่งวินิจฉัยว่า Google ไม่ต้องเป็นผู้รับผิดชอบในการลบผลการค้นหาที่เป็นข้อมูลหมิ่นประมาทโจทก์ที่ถูกประมวลผลโดยบริษัทเซิฟเวอร์ประมวลผลข้อมูลอื่นที่ไม่ใช่สัญชาติไต้หวันด้วยแต่อย่างใด หรือคำวินิจฉัยของ AAB ในกรณี *X v Privacy Commissioner for Personal Data (Administistrative Appeal No. 15/2019)* ซึ่ง AAB ปฏิเสธที่จะใช้

---

[269] Global Freedom of Expression, ‘Google LLC v. National Commission on Informatics and Liberty (CNIL)’ (Columbia University, September 2019) <https://globalfreedomofexpression.columbia.edu/cases/google-llc-v-national-commission-on-informatics-and-liberty-cnil/> accessed 3 October 2021.

อำนาจสั่งให้ Google LLC ดำเนินการตามคำร้อง เนื่องจากข้อจำกัดในเรื่องขอบเขตการใช้บังคับของ HK PDPO 1996 โดย AAB วางหลักว่ากฎหมายของประเทศหนึ่งย่อมไม่มีผลบังคับนอกดินแดนของตนเอง (No Extra-Territorial Effect)

ปัญหาเกี่ยวกับการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับบุคคลซึ่งอยู่ต่างประเทศนั้น เป็นประเด็นที่จะต้องวิเคราะห์ถึงขอบเขตการบังคับใช้ในเชิงพื้นที่ (Territorial Scope) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยบัญญัติเอาไว้ว่า “ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร โดยการดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เมื่อเป็นการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร” ตามมาตรา 5 (2) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ดังนั้น ในกรณีที่การแสดงผลข้อมูลตามระบบการสืบค้นออนไลน์ผ่านอินเทอร์เน็ตมีลักษณะ เช่น เป็นการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรแม้ว่าผู้ให้บริการระบบสืบค้นข้อมูลจะทำการประมวลผลข้อมูลนอกราชอาณาจักรก็ตาม อย่างไรก็ตาม ผลการบังคับใช้กฎหมายไทยแก่บุคคลที่อยู่นอกราชอาณาจักรนั้นจะเผชิญกับความท้าทายในการบังคับใช้ในทางปฏิบัติดังที่ได้ถูกแสดงผ่านกรณีศึกษา เช่น คดี *Google Spain v AEPD and Mario Costeja González* และคดี *Google LLC v CNIL*

4.2.2 หน่วยงานของรัฐ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติเอาไว้ว่ากฎหมายบังคับกับหน่วยงานของรัฐด้วย เว้นแต่หน่วยงานของรัฐในบางกรณี เช่น การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์[270] โดยไม่ได้บัญญัติหน้าที่ของหน่วยงานรัฐเกี่ยวกับลบหรือทำลายข้อมูลเป็นการเฉพาะ หน่วยงานรัฐที่ไม่ได้รับการยกเว้นตามมาตรา 4 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ย่อมตกอยู่ในบังคับของมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

อย่างไรก็ตาม อาจกล่าวได้ว่า TW PDPA 2015 นั้นมีรายละเอียดเกี่ยวกับหน่วยงานของรัฐที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลเอาไว้มากกว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดย TW PDPA 2015 บัญญัติกำหนดหน้าที่ให้กับหน่วยงานของรัฐให้ทำการลบข้อมูลส่วนบุคคลโดยเฉพาะ โดยกฎหมายได้บัญญัติหลักเกณฑ์ในการลบข้อมูลส่วนบุคคลไว้โดยให้หน่วยงานของรัฐในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลทำการลบข้อมูลส่วนบุคคลออกหากว่าเจ้าของข้อมูลส่วนบุคคลร้องขอ เช่นเดียวกันกับ PH DPA 2012 ของฟิลิปปินส์ที่ให้หน่วยงานรัฐมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ภายใต้บังคับของกฎหมายฉบับดังกล่าวด้วย และจำต้องปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลเมื่อมีการร้องขอใช้สิทธิที่จะถูกลืม

---

[270] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4 วรรคหนึ่ง (2).

HK PDPO 1996 ของฮ่องกงก็บัญญัติไว้ในทำนองเดียวกัน ให้ ‘Data User’ ที่หมายความรวมถึงหน่วยงานของรัฐ มีหน้าที่ต้องลบข้อมูลส่วนบุคคลของปัจเจกบุคคลออกเมื่อสิ้นระยะเวลาที่ควรจำต้องเก็บรักษาข้อมูลไว้ และตาม AUS PA 1988 ก็ได้บัญญัติไว้อย่างชัดเจนว่า ‘Agency’ ซึ่งหมายความถึง รัฐมนตรี กระทรวง และหน่วยงานรัฐบางประเภทที่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการตามสมควรทุกประการเพื่อทำการลบข้อมูลส่วนบุคคลออกเมื่อไม่มีความจำเป็นต่อวัตถุประสงค์ในการเก็บรวบรวมข้อมูลนั้นอีก[271]

4.3 การบัญญัติถึงเนื้อหาการคุ้มครองสิทธิที่จะถูกลืม

การศึกษาตัวบทกฎหมาย แนวปฏิบัติ คำวินิจฉัยของหน่วยงานของรัฐ และคำพิพากษาของศาลในต่างประเทศทำให้เห็นว่ากฎหมายจำเป็นที่จะต้องระบุถึงรายละเอียดเกี่ยวกับการคุ้มครองสิทธิที่จะถูกลืมโดยมีประเด็นที่ต้องพิจารณาความครอบคลุมของกฎหมายในประเด็น ได้แก่

(4.3.1) การร้องขอผู้ทรงสิทธิและหน้าที่ดำเนินการโดยผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม

(4.3.2) ข้อจำกัดการคุ้มครองจากการไม่มีคำว่าสิทธิที่จะถูกลืม

(4.3.3) การลบหรือทำลายข้อมูลเมื่อข้อมูลส่วนบุคคลหมดความจำเป็นที่จะต้องถูกประมวลผลตามวัตถุประสงค์

(4.3.4) การกำหนดรายละเอียดเกี่ยวกับการลบทำลายและทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และ

(4.3.5) การบัญญัติถึงข้อจำกัดการใช้สิทธิที่จะถูกลืม

---

[271] โปรดดู ข้อเปรียบเทียบ เรื่อง ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืมในเอกสารหมายเลข 2 ของภาคผนวก

4.3.1 การร้องขอผู้ทรงสิทธิและหน้าที่ดำเนินการโดยผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม โดยปราศจากการร้องขอของเจ้าของข้อมูลส่วนบุคคล

มาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ การบัญญัติกฎหมายในลักษณะดังกล่าวทำให้เข้าใจไปว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการลบทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้เมื่อมีการ “ร้องขอ” โดยเจ้าของข้อมูลส่วนบุคคลเท่านั้น (ซึ่งสอดคล้องกับการใช้สิทธิที่จะถูกลืมตามมาตรา 17 ของ GDPR มาตรา 29 ของ JAP APPI 2020 มาตรา 3 ของ TW PDPA 2015 มาตรา 26 ของ PH DPA 2012)

อย่างไรก็ตาม หน้าที่ในการลบ ทำลายข้อมูลส่วนบุคคลโดยปราศจากการร้องขอของเจ้าของข้อมูลส่วนบุคคลก็ถูกบัญญัติเอาไว้เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังกล่าวนั้น สามารถเทียบได้กับการกำหนด “หน้าที่” ให้กับผู้ควบคุมข้อมูลส่วนบุคคลของต่างประเทศ[272] ได้แก่ มาตรา 47 (1) ของ UK DPA 2018 *“ผู้ควบคุมข้อมูลส่วนบุคคล “จะต้องลบข้อมูลส่วนบุคคล (Must Erase Personal Data)” โดยไม่ชักช้าในกรณี ...”*[273] ตามมาตรา 26 (1) ของ

---

[272] โปรดดู ข้อเปรียบเทียบ เรื่อง หน้าที่ในการลบ ทำลายหรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในเอกสารหมายเลข 3 ของภาคผนวก

[273] Privacy Data Protection Act 2018, Section 47 (1).

HK PDPO 1996 ของฮ่องกง ผู้ควบคุมข้อมูลส่วนบุคคล *"จะต้องทำการใด ๆ ที่ส่งผลในทางปฏิบัติเพื่อลบข้อมูลส่วนบุคคลซึ่งไม่มีความจำเป็นจะต้องใช้ตามวัตถุประสงค์อีกต่อไป"*[274] และตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ ตามมาตรา 25 ของ SG PDPA 2012 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล *"จำต้องยุติการเก็บรักษาเอกสารที่มีข้อมูลส่วนบุคคลหรือกำจัดวัตถุใด ๆ ที่มีข้อมูลส่วนบุคคลที่เกี่ยวข้องกับปัจเจกบุคคลใด ๆ รวมอยู่"*[275] ทำให้อาจพิจารณาได้ว่า การลบข้อมูลส่วนบุคคลอาจเกิดขึ้นได้โดยไม่จำต้องรอให้เจ้าของข้อมูลส่วนบุคคลร้องขอ อีกทั้งในมาตรา 11 ของ TW PDPA 2015 ของไต้หวัน ได้กำหนดให้องค์ภาครัฐและองค์กรที่มิได้เป็นหน่วยงานของรัฐสามารถพิจารณาลบข้อมูลส่วนบุคคลนั้น ๆ ได้เอง[276] หากเห็นควรให้มีการลบได้ตามที่กฎหมายกำหนด โดยไม่จำต้องรอให้เจ้าของข้อมูลส่วนบุคคลร้องขอ อีกทั้งในหลักการความเป็นส่วนตัวออสเตรเลียในข้อที่ 11.2 ได้ระบุในทำนองเดียวกัน *"ต้องดำเนินขั้นตอนที่เหมาะสมตามแต่ละกรณี เพื่อทำลายข้อมูลหรือทำให้มั่นใจว่าข้อมูลได้ถูกทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้"*[277]

ด้วยเหตุนี้ จึงสามารถกล่าวได้ว่ามาตรา 33 ประกอบมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีความครอบคลุมถึงการคุ้มครองตามแนวทางของกฎหมายในต่างประเทศ ทั้งในมิติที่รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลในการ "ร้องขอ" และในมิติของการกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล "ดำเนินการ" ลบหรือทำลายข้อมูลโดยปราศจากการร้องขอ

---

[274] Personal Data (Privacy) Ordinance (1996), Section 26 (1).

[275] Singapore PDPA 2012, Section 25.

[276] TW PDPA 2015, Section 11 para 3.

[277] AUS PA 1988 & APPI ข้อ 11.2.

4.3.2 ข้อจำกัดการคุ้มครองจากการไม่มีคำว่าสิทธิที่จะถูกลืม

คดี *Google Spain v AEPD and Mario Costeja González* ประกอบกับความเห็นของคณะมนตรียุโรป No 6/2016 (2016/c 159/02) แสดงให้เห็นว่าการนำข้อมูลออกจากการแสดงผลการค้นหานั้น อาจไม่ส่งผลให้มีการ “ลบ” ข้อมูลซึ่งถูกเผยแพร่โดยผู้ควบคุมข้อมูลส่วนบุคคลอื่น (เช่น สำนักพิมพ์) ทั้งนี้ เพื่อรองรับบริบทของโลกในยุคดิจิทัล (Digital Context)[278] ด้วยเหตุนี้ มาตรา 17 ของ GDPR จึงได้เพิ่มถ้อยคำ คือ “ (Right to be Forgotten)” เอาไว้ควบคู่กับ “Right to Erasure”

มาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้ถ้อยคำ ได้แก่ *“ลบหรือทำลายข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้”* โดยไม่ปรากฏคำว่า “สิทธิที่จะถูกลืม” เอาไว้เช่นเดียวกับมาตรา 17 ของ GDPR และหากพิจารณาประเภทของสิทธิที่จะถูกลืมตามที่อธิบายในหัวข้อ 2.1.2 (ในบทที่ 2) แล้วจะเห็นได้ว่าการรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายในปัจจุบันบัญญัติตัวอย่างของสิทธิที่จะถูกลืม เช่น การลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ โดยไม่ได้บัญญัติถ้อยคำว่าที่แสดงถึงเนื้อหาของสิทธิที่จะถูกลืมอันเป็นคำที่สามารถครอบคลุมสิทธิที่จะถูกลืมประเภทต่าง ๆ

การบัญญัติกฎหมายในลักษณะดังกล่าวโดยไม่ได้บัญญัติคำว่า *“สิทธิที่จะถูกลืม”* เอาไว้ในตัวบทกฎหมาย อาจก่อให้เกิดปัญหาว่าหากผู้ให้บริการสืบค้นข้อมูลออนไลน์ซึ่งถูกเจ้าของข้อมูลส่วนบุคคลเรียกร้องให้ดำเนินการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุ

---

[278] Statement of the Council’s reasons : Position (EU) No 6/2016 (2016/c 159/02), para 4.6.

ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว หากผู้ให้บริการดำเนินการเพียงลบ Link ในหน้าแสดงผลโดยไม่ได้ลบข้อมูลส่วนบุคคลที่ครอบครอง โดยผู้ควบคุมข้อมูลส่วนบุคคลอื่นจะถือว่าเป็นการปฏิบัติหน้าที่โดยชอบด้วยกฎหมายแล้วหรือไม่ หากถือว่ายังไม่ได้ปฏิบัติตามกฎหมายตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด ผู้ให้บริการสืบค้นข้อมูลออนไลน์ซึ่งเป็นผู้ควบคุมข้อมูลอาจมีความเสี่ยงที่จะต้องรับผิดทางแพ่ง ชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคลในกรณีที่เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลได้[279]

ส่วนมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการ “ลบหรือทำลายข้อมูลส่วนบุคคล” ในทำนองเดียวกับปัญหาของมาตรา 33 บทบัญญัตินี้ก็ไม่ได้ปรากฏถ้อยคำว่า “สิทธิที่จะถูกลืม” ในตัวบทกฎหมาย โดยบัญญัติเพียงตัวอย่างของสิทธิที่จะถูกลืม คือ “การลบ ทำลายข้อมูลส่วนบุคคล” เท่านั้น หากผู้ให้บริการสืบค้นข้อมูลออนไลน์ดำเนินการเพียงลบ Link ในหน้าแสดงผลโดยไม่ได้ลบข้อมูลส่วนบุคคลที่ครอบครองโดยผู้ควบคุมข้อมูลส่วนบุคคลอื่นจะถือว่าเป็นการปฏิบัติหน้าที่โดยชอบด้วยกฎหมายแล้วหรือไม่ หากผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 37 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท[280]

---

[279] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 77.

[280] Ibid, มาตรา 83.

4.3.3 การลบหรือทำลายข้อมูลเมื่อข้อมูลส่วนบุคคลหมดความจำเป็นที่จะต้องถูกประมวลผลตามวัตถุประสงค์

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศนั้น บัญญัติให้มีการลบ ทำลาย หรือทำให้ข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในกรณีที่ข้อมูลส่วนบุคคล “หมดความจำเป็น” ที่จะต้องถูกใช้ตามวัตถุประสงค์ของการเก็บรวบรวม เช่น GDPR ซึ่งใช้ถ้อยคำว่า *“เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นเพื่อการประมวลผลข้อมูลอีกต่อไป”*[281] HK PDPO 1996 ที่ใช้ถ้อยคำว่า *“เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นสำหรับวัตถุประสงค์ของการใช้ข้อมูล”*[282] TW PDPA 2015 ซึ่งบัญญัติว่า *“เมื่อวัตถุประสงค์ของการเก็บรวบรวมข้อมูลหมดลง ซึ่งอาจเป็นผลจากการพ้นผ่านไปของเวลา หน่วยงานรัฐหรือองค์กรนอกภาครัฐจะต้องลบหรือหยุดประมวลผลข้อมูล”*[283] ซึ่งสอดคล้องกับตัวบทกฎหมายของมาตรา 33 และมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างไรก็ตาม กรณีนี้มีข้อสังเกตว่าตัวบทกฎหมายเหล่านี้ถูกบัญญัติขึ้นโดยใช้ถ้อยคำที่มีความยืดหยุ่นและเปิดโอกาสให้มีการปรับใช้กฎหมายให้เหมาะสมกับกรณี ด้วยเหตุนี้ การปรับใช้กฎหมายจึงมิอาจหลีกเลี่ยงการพิจารณาข้อเท็จจริงเป็นรายกรณี ซึ่งสามารถแสดงได้ตามตัวอย่าง ดังต่อไปนี้

4.3.3.1 การพิจารณาข้อเท็จจริงในเรื่องเวลาพ้นผ่านไป

การพิจารณาว่า “ข้อมูลส่วนบุคคลหมดความจำเป็นหรือไม่และเมื่อใด” นั้น เป็นข้อพิจารณาสำคัญในการคุ้มครองสิทธิที่จะถูกลืม เช่น คดี *Hurbain v. Belgium* แสดงให้เห็นว่าสำนักพิมพ์ (Le Soir) นั้น

---

[281] GDPR, Article 17 วรรค 1 (a).

[282] Personal Data (Privacy) Ordinance (1996), Section 26 (1).

[283] Personal Data Protection Act 2015, Article 11.

มีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล เนื่องจากเป็นผู้ทำการเผยแพร่ข้อมูลส่วนบุคคลของคนขับรถซึ่งเป็นต้นเหตุให้เกิดอุบัติเหตุที่ทำให้มีคนเสียชีวิต ศาลได้ทำการวินิจฉัยถึงระยะเวลาได้พ้นผ่านไปนับจากวันที่ได้มีการเผยแพร่ข้อมูลครั้งแรก (โดยศาลได้พิจารณาและชั่งน้ำหนักถึงเสรีภาพในการแสดงความคิดเห็นของหนังสือพิมพ์ด้วย) โดยในคดีนี้ศาลได้สรุปว่า เวลานับจากวันเกิดอุบัติเหตุได้ผ่านมานานแล้ว และผู้ก่อเหตุก็ไม่ได้เป็นบุคคลสาธารณะ กรณีไม่ปรากฏคุณค่าของการที่ยังคงมีชื่อและสกุลของบุคคลที่ก่อเหตุในข่าวการเกิดสถิติของอุบัติเหตุบนท้องถนนนั้น ยังคงทำได้โดยไม่ต้องมีชื่อของบุคคลอยู่

4.3.3.2 การสิ้นสุดของเวลา

สื่อมวลชนย่อมมีเสรีภาพในการนำเสนอข้อมูลข่าวสารต่าง ๆ ข้อมูลที่สื่อมวลชน เช่น สำนักข่าวนำเสนอโดยผ่านฐานหนังสือพิมพ์ออนไลน์ อาจถูกค้นหาและเข้าถึงโดยบุคคลทั่วไปในสังคม ศาลในคดี *Plaintiff X v. PrimaDanoi* ยอมรับถึงความสำคัญของสิทธิในการรายงานข้อมูล แต่ก็ได้วินิจฉัยว่า “ข้อมูลที่มีความอ่อนไหว (Sensitive Information) และข้อมูลส่วนตัว (Private Information) ไม่ควรจะถูกทำให้เข้าถึงได้โดยสาธารณชนโดยปราศจากการจำกัดเวลา (เว้นแต่สำนักพิมพ์จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล)

การบัญญัติโดยใช้ถ้อยคำที่ยืดหยุ่น เช่น “เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล” ตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ย่อมเปิดโอกาสให้บุคคลที่เกี่ยวข้องสามารถใช้ดุลพินิจให้เหมาะกับกรณี และช่วยเปิดโอกาสให้มีการชั่งน้ำหนักประโยชน์ต่าง ๆ ที่เกี่ยวข้องและอาจขัดแย้งกันในบางกรณี

อย่างไรก็ตาม ในบางกรณีภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลอาจไม่ได้ระบุว่าหากสิ้นสุดระยะเวลาลง ข้อมูลส่วนบุคคลจำต้องถูกทำลายหรือลบทิ้งไปไว้อย่างชัดเจน แต่เป็นการบัญญัติในทำนองให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามกฎหมายอื่นที่ไม่ใช่กฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น ตามหลักการความเป็นส่วนตัวออสเตรเลีย ในข้อที่ 11.2 (d) ที่ให้ APP entity อาจทำการทำลายหรือทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ต่อเมื่อไม่มีกฎหมาย หรือคำสั่งของศาลหรือองค์คณะไกล่เกลี่ย (Tribunal) ให้จำต้องเก็บรักษาข้อมูลนั้นไว้[284] อย่างกรณีของบทบัญญัติภายใต้กฎหมายโทรคมนาคมที่กำหนดระยะเวลาสิ้นสุดของการเก็บรักษาข้อมูลไว้อย่างชัดแจ้ง นอกจากบทบัญญัติของกฎหมายยังมีคำสั่งศาล หรือคำสั่งขององค์คณะไกล่เกลี่ยที่มีอำนาจ อาจสั่งให้ทำการเก็บข้อมูลนั้นไว้ตามระยะเวลาที่กำหนด และเมื่อสิ้นระยะเวลาการเก็บรักษาข้อมูลที่กำหนดก็ต้องทำการทำลายข้อมูลนั้น[285] โดยจะมีบทบัญญัติเฉพาะที่กำหนดไว้ว่าข้อมูลส่วนบุคคลแต่ละประเภทจำต้องถูกเก็บไว้ตามระยะเวลาที่กำหนด โดยบทบัญญัติดังกล่าวอาจเป็นบทบัญญัติที่เป็นการสั่งให้ APP entity โดยเฉพาะที่เป็น Agency ทำการทำลายข้อมูลส่วนบุคคลตามที่กำหนดได้[286]

เช่นเดียวกัน กรณีตามมาตรา 25 ของ SG PDPA 2012 ก็ได้บัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลยุติการเก็บรักษาเอกสารที่มีข้อมูลส่วนบุคคลหรือกำจัดวัตถุใด ๆ ที่มีข้อมูลส่วนบุคคลที่เกี่ยวข้องกับปัจเจกบุคคลใด ๆ รวมอยู่ เมื่อวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นไม่มีประโยชน์ต่อการเก็บรักษาข้อมูลส่วนบุคคลอีกต่อไป และการเก็บรักษาข้อมูลนั้น

---

[284] Privacy Act 1988 & APPI Clause 11.2 (c).

[285] Destruction or de-identification that is 'lawful', Australian Privacy Principles Guidelines Privacy Act 1988, Australian Government Office of the Australian Information Commissioner.

[286] Archives Act 1983, Section 24.

ไม่มีความจำเป็นต่อวัตถุประสงค์ด้านกฎหมายหรือธุรกิจอีก แม้กฎหมายฉบับดังกล่าวไม่ได้กำหนดระยะเวลาในการเก็บข้อมูลส่วนบุคคลไว้อย่างชัดเจน แต่ผู้ควบคุมข้อมูลส่วนบุคคลอาจยึดถือระยะเวลาการเก็บรักษาข้อมูลตามมาตรฐานที่กำหนดโดยกฎหมายที่เกี่ยวข้องกับธุรกิจของผู้ควบคุมข้อมูลส่วนบุคคล หรืออาจกำหนดระยะเวลาการสิ้นสุดของการเก็บรักษาข้อมูลนั้นเองโดยพิจารณาจากปัจจัยที่กำหนด[287]

อีกทั้งในมาตรา 5 (1) (e) ของ GDPR ที่เป็นหนึ่งในหลักการคุ้มครองข้อมูลส่วนบุคคลไว้ว่าข้อมูลส่วนบุคคลจำต้องเก็บไว้ไม่เกินกว่าที่จำเป็นเพื่อวัตถุประสงค์ในการเก็บรวบรวม โดยเรียกเงื่อนไขตามบทบัญญัติข้อนี้ว่าเป็น “ข้อจำกัดของการเก็บ (Storage Limitation)” โดยไม่ได้กำหนดระยะเวลาในการเก็บว่าควรจำต้องเก็บไว้นานเพียงใดแต่เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่อาจกำหนดระยะเวลาการสิ้นสุดของการเก็บข้อมูลส่วนบุคคลไว้เอง

4.3.4 การกำหนดรายละเอียดเกี่ยวกับการลบ ทำลายและทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

มาตรา 33 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติเนื้อหาของสิทธิที่จะถูกลืมเอาไว้ ได้แก่ การลบ ทำลาย หรือทำให้ข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ โดยไม่ได้บัญญัติรายละเอียดของการดำเนินการเอาไว้ว่าในการลบหรือทำลายข้อมูลส่วนบุคคลนั้นจะต้องดำเนินการอย่างไร ซึ่งเป็นแนวทางที่สอดคล้องกับแนวทางของ GDPR UK DPA 2018 AUS PA 1988 JAP APPI 2020 TW PDPA 2015

[287] Personal Data Protection Act 2012, Section 25.

HK PDPO 1996 PH DPA 2012 และ SG PDPA 2012[288] อย่างไรก็ตาม การที่ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืมนั้น ไม่ทราบถึงรายละเอียดการดำเนินการย่อมส่งผลให้เกิดปัญหาการปฏิบัติตามกฎหมายในทางปฏิบัติได้ เช่น อาจมีคำถามขึ้นได้ว่าการดำเนินการใดที่จะถือได้ว่าผู้ควบคุมข้อมูลส่วนบุคคลได้ดำเนินตามกฎหมายเพื่อคุ้มครองสิทธิที่จะถูกลืมแล้ว เพื่อแก้ปัญหาดังกล่าว หน่วยงานคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศมิได้ดำเนินการแก้ไขบทบัญญัติในกฎหมายคุ้มครองข้อมูลส่วนบุคคล หากแต่ได้ออกแนวปฏิบัติหรือกฎหมายลำดับรองเพื่อขยายความและให้รายละเอียดเกี่ยวกับการลบหรือทำลายข้อมูลส่วนบุคคล

4.3.4.1 การบัญญัติถ้อยคำในเรื่องการลบ ทำลายข้อมูลส่วนบุคคล

UK DPA 2018 ไม่ได้บัญญัตินิยามของการลบ ทำลายข้อมูลส่วนบุคคลเอาไว้ แต่ ICO ได้ให้คำอธิบายว่าข้อมูลส่วนบุคคลนั้นจะต้องถูกลบโดยไม่สามารถกู้คืนกลับมาได้ นอกจากกรณีของการลบข้อมูลส่วนบุคคลแล้ว ยังมีแนวทางอื่นที่เป็นการจัดการกับการลบข้อมูลในรูปแบบอื่น ดังเช่น ในการทำให้ข้อมูลอยู่เหนือการใช้งาน แนวปฏิบัติฉบับนี้ระบุให้การทำให้ข้อมูลอยู่เหนือการใช้งาน หากปรากฏว่าข้อมูลดังกล่าวไม่ได้ถูกลบออกไปจริง จำต้องเป็นกรณีที่ปรากฏด้วยว่าผู้ควบคุมข้อมูลส่วนบุคคลนั้นได้ปฏิบัติให้เป็นไปกรณีดังนี้ (1) ไม่สามารถหรือจะไม่พยายามใช้ข้อมูลส่วนบุคคลเพื่อแจ้งให้ทราบถึงการตัดสินใจใด ๆ ที่เกี่ยวข้องกับบุคคลใด ๆ หรือในลักษณะที่ส่งผลต่อบุคคลใด ๆ และไม่ว่าด้วยวิธีใดก็ตาม (2) ไม่อนุญาตให้หน่วยงานอื่นใดสามารถเข้าถึงข้อมูลส่วนบุคคลนั้นได้ (3) จัดให้มีความมั่นคงปลอดภัย

[288] โปรดดู ข้อเปรียบเทียบใน เรื่อง การลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในเอกสารหมาย 5 ในภาคผนวก

ทางด้านเทคนิคและด้านการบริหารจัดการ และ (4) ให้คำมั่นว่าจะลบข้อมูลนั้นทิ้งอย่างถาวร เมื่อหรือหากสามารถดำเนินการเช่นนั้นได้[289]

AUS PA 1988 ไม่ได้บัญญัติถึงแนวปฏิบัติในเรื่องการลบ ทำลายข้อมูลส่วนบุคคล แนวการปฏิบัติจะออกโดย OAIC ซึ่งได้กล่าวถึงการทำลายและการทำให้ข้อมูลกลายเป็นข้อมูลที่บ่งชี้ตัวตนไม่ได้เป็นส่วนหนึ่งของมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยระบุว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องใช้ความพยายามตามสมควรในการทำลายหรือทำให้ข้อมูลกลายเป็นข้อมูลที่บ่งชี้ตัวตนไม่ได้เมื่อหมดความจำเป็นที่จะต้องครอบครองข้อมูลนั้น

HK PDPO 1996 ไม่ได้บัญญัตินิยามของการลบ ทำลายข้อมูลส่วนบุคคลเอาไว้ แต่อย่างไรก็ตาม สำนักงานคณะกรรมการความเป็นส่วนบุคคลของข้อมูลส่วนบุคคลได้อธิบายว่า แนวทางในการ “ลบ” ข้อมูลส่วนบุคคลที่หมดความจำเป็นในการประมวลผลแล้วนั้น หมายถึง การทำให้ข้อมูลถูกลบหรือทำลายโดยไม่อาจกลับคืนมาได้อีก ทั้งนี้ โดยพิจารณาจากลักษณะและการเก็บรักษาข้อมูลด้วย โดยได้ตั้งข้อสังเกตว่าการลบ ทำลายข้อมูลอิเล็กทรอนิกส์โดยทางกายภาพนั้นสามารถเป็นไปได้ เช่น การเจาะทำลายอุปกรณ์หรือแถบแม่เหล็ก PH IRR ซึ่งเป็นกฎหมายลำดับรองของ PH DPA 2012 ของประเทศฟิลิปปินส์ ไม่เพียงแต่บัญญัติให้สามารถลบทำลายได้เท่านั้น หากแต่ยังได้บัญญัติเพิ่มเติมว่าอาจเป็นกรณี การขอให้หยุดชั่วคราว ถอน หรือสั่งให้มีการขัดขวาง กำจัด หรือทำลาย[290]

---

[289] ICO, ‘Deleting personal data’ (ICO, February 2014) <https ://ico.org.uk/media/for-organisations/documents/1475/deleting_ personal_data.pdf> accessed 3 October 2021, p. 5.

[290] Data Privacy Act 2012, Section 16 (e) & Implementing Rules and Regulations (IRR) of the Data Privacy Act of 2012, Section 34 (e).

แนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคล (Advisory Guidelines on Key Concepts in the PDPA) ของประเทศสิงคโปร์ ระบุว่า ในการยุติการเก็บรักษาข้อมูลส่วนบุคคลนั้น ผู้ที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลอาจพิจารณาให้ดำเนินการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนาม (Anonymization) ซึ่งถือเป็นกระบวนหนึ่งในการกำจัด (Remove) ข้อมูลที่สามารถระบุตัวบุคคลได้

เมื่อเปรียบเทียบบทบัญญัติตามมาตรา 33 และมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศเหล่านี้แล้ว สามารถกล่าวได้ว่า การที่กฎหมายไม่ได้บัญญัติถึงรายละเอียดของการลบหรือทำลายข้อมูลส่วนบุคคลเอาไว้ในกฎหมายระดับพระราชบัญญัตินั้น ไม่อาจถือได้ว่ากฎหมายไทยขาดความครอบคลุมในส่วนการคุ้มครองสิทธิที่จะถูกลืม เนื่องจาก การดำเนินการลบ ทำลาย หรือทำให้ข้อมูลไม่อาจระบุตัวตนได้นั้น เกี่ยวข้องรายละเอียดทางเทคนิค ซึ่งสามารถให้รายละเอียดได้โดยผ่านการออกแนวปฏิบัติหรือกฎหมายลำดับรองที่เกี่ยวข้องต่อไป

4.3.4.2 ปัญหาการลบ ทำลายข้อมูลส่วนบุคคลโดยผู้ให้บริการสืบค้นข้อมูลออนไลน์

มาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้” ในขณะที่มาตรา 37 (3) บัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล ในกรณีที่ผู้ให้บริการระบบ

สืบค้นข้อมูลออนไลน์เป็นผู้ควบคุมข้อมูลส่วนบุคคลซึ่งได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคลหรือเป็นกรณีที่มีหน้าที่จัดให้มีระบบการลบหรือทำลายข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าวย่อมสามารถทำได้เพียงการลบลิงค์หรือข้อมูลที่ทำให้ผู้ใช้งานอินเทอร์เน็ตเข้าถึงข้อมูลส่วนบุคคลเท่านั้น โดยอาจไม่สามารถลบข้อมูลจากฐานข้อมูลต้นทางที่ถูกเผยแพร่โดยบุคคลอื่น เช่น สำนักพิมพ์ (ตามแผนภาพที่ 4-1)

ในคดี *Google Spain v AEPD and Mario Costeja González* ข้อมูลการขายทรัพย์สินทอดตลาดอันเป็นข้อมูลส่วนบุคคลของ Mario Costeja González นั้น ปรากฏอยู่ในโปรแกรมสืบค้นข้อมูลของ Google ที่เป็นผู้ให้บริการโปรแกรมสืบค้นข้อมูลที่ถูกใช้งานทั่วโลก ซึ่งระบบการสืบค้นของ Google ถูกสร้างขึ้นเพื่อเป็นเครื่องมือเพื่อการเข้าถึงเท่านั้น Google เพียงแต่ทำให้ข้อมูลดังกล่าวที่ถูกประกาศโดยบุคคลอื่น สามารถเข้าถึงได้อย่างรวดเร็วมากขึ้นเท่านั้น มิได้เป็นผู้เผยแพร่ข้อมูลโดยดั้งเดิม หากผู้เผยแพร่ข้อมูลตัดสินใจที่จะลบข้อมูลดังกล่าวออกจากเว็บไซต์ของตน ข้อมูลส่วนบุคคลของ Mario Costeja González ก็ย่อมถูกลบออกจากรายการข้อมูลของ Google และไม่สามารถปรากฏบนผลแสดงการค้นหาได้ด้วยเช่นกัน

CJEU สั่งให้ Google ดำเนินการลบ “ลิงค์” ในส่วนของ “ชื่อ” เท่านั้น อย่างไรก็ตาม ข้อมูลที่ถูกเผยแพร่เดิมยังคงถูกเข้าถึงได้โดยการอาศัยคำค้นหาอื่น ๆ หรือการเข้าถึงจากฐานข้อมูลของผู้เผยแพร่โดยตรง โดยมีข้อสังเกตว่าตัวเจ้าของข้อมูลส่วนบุคคลนั้นไม่ได้มีหน้าที่ต้องติดต่อกับผู้เผยแพร่ข้อมูลเดิมผ่านระบบสืบค้น จากคำวินิจฉัยดังกล่าวแสดงให้เห็นว่าสิ่งที่ Google สามารถดำเนินการได้เพื่อ “ลืม” ข้อมูลส่วนบุคคลของ Mario Costeja González นั้นมีเพียงการลบลิงค์เท่านั้น มิอาจลบหรือทำลายข้อมูลส่วนบุคคลที่ถูกเผยแพร่โดยผู้ควบคุมข้อมูลส่วนบุคคลอื่นได้ ดังนั้น หากตีความกฎหมายว่าผู้ให้บริการ

ระบบสืบค้นข้อมูลออนไลน์เป็นผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบหรือทำลายข้อมูลซึ่งถูกเผยแพร่โดยผู้ควบคุมข้อมูลส่วนบุคคลอื่น เช่น สำนักพิมพ์ แล้วผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์ย่อมไม่สามารถปฏิบัติหน้าที่ตามกฎหมายได้เนื่องจากเป็นกรณีที่เกินความสามารถที่ตนจะกระทำได้

4.4 การบัญญัติถึงข้อจำกัดการใช้สิทธิที่จะถูกลืม

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศนั้น แสดงให้เห็นอย่างชัดเจนว่าสิทธิที่จะถูกลืมนั้นมิใช่เด็ดขาด หากแต่ถูกจำกัดด้วยเงื่อนไขตามที่กฎหมายบัญญัติได้ในหลายประการ ดังนั้น ตัวบทกฎหมายที่จะถูกใช้เพื่อคุ้มครองสิทธิที่จะถูกลืมย่อมจะต้องบัญญัติถึงข้อจำกัดดังกล่าวด้วยเหตุปฏิเสธการใช้สิทธิที่จะถูกลืมตามมาตรา 33 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น มีแนวทางที่สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ โดยข้อจำกัดประการสำคัญ ได้แก่ ความจำเป็นในการคุ้มครองเสรีภาพในการเข้าถึงข้อมูลและการแสดงความคิดเห็น ซึ่งปรากฏอย่างชัดเจนในตัวบทกฎหมาย เช่น มาตรา 17 วรรคสาม ของ GDPR และการคุ้มครองประโยชน์สาธารณะ เช่น มาตรา 26 ของ HK PDPO 1996[291]

4.4.1 การสร้างความสมดุลระหว่างสิทธิในความเป็นส่วนตัวกับเสรีภาพในการเข้าถึงข้อมูลและการแสดงออก

การบัญญัติข้อจำกัดของสิทธิที่จะถูกลืมโดยใช้ถ้อยคำว่า *“ความในวรรคหนึ่ง (ของมาตรา 33) มิให้นำมาใช้บังคับกับการเก็บรักษาไว้*

[291] โปรดดูข้อเปรียบเทียบเกี่ยวกับข้อยกเว้นในการใช้สิทธิที่จะถูกลืม ในเอกสารหมายเลข 6 และหมายเลข 7 ของภาคผนวก.

เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น”[292] นั้น เป็นแนวทางการบัญญัติกฎหมายโดยอาศัยถ้อยคำที่มีความยืดหยุ่น เช่นเดียวกับการบัญญัติถึงเงื่อนไขในการลบหรือทำลายข้อมูล กล่าวคือ *“เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล”*[293] การบัญญัติกฎหมายโดยอาศัยถ้อยคำที่ยืดหยุ่นดังกล่าว ไม่ได้เป็นปัญหาเนื่องจากกระบวนการนิติบัญญัติ หากแต่เป็นกรณีที่กฎหมายจำเป็นที่ต้องมีความยืดหยุ่นเพื่อตอบสนองต่อพัฒนาการของสังคมและลักษณะการเข้าถึงข้อมูลอันมีลักษณะเป็นพลวัติ

อย่างไรก็ตาม ปัญหาการจำกัดสิทธิที่จะถูกลืมโดยอาศัยฐานของเสรีภาพในการแสดงความคิดเห็นดังกล่าว ได้ถูกสะท้อนอย่างชัดเจนในข้อพิพาทซึ่งเป็นปัญหาที่เกิดขึ้นจริงในสังคมในกรณีต่าง ๆ ซึ่งหน่วยงานที่เกี่ยวข้องมีความจำเป็นจะต้อง “ชั่งน้ำหนัก” ระหว่างสิทธิในความเป็นส่วนตัวและเสรีภาพในการเข้าถึงข้อมูลและการแสดงออก โดยสามารถสรุปได้ดังต่อไปนี้

4.4.1.1 ประโยชน์ในการเข้าถึงข้อมูลอาจหมดลงได้เมื่อเวลาพ้นผ่านไป

CJEU ในคดี *Hurbain v. Belgium* ได้แสดงให้เห็นว่าเสรีภาพในการแสดงความเห็นของหนังสือพิมพ์ (Freedom of Expression of the Newspaper) นั้น ส่งผลกระทบต่อสิทธิในความส่วนตัวของผู้ขับรถที่ก่อให้เกิดอุบัติเหตุ ศาลได้สรุปว่าเวลานับจากวันเกิดอุบัติเหตุได้ผ่านมานานแล้ว (Substantial Period had Elapsed) และผู้ก่อเหตุก็ไม่ได้เป็นบุคคลสาธารณะ

---

[292] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 33 วรรคสอง.

[293] Ibid, มาตรา 33 วรรคหนึ่ง (1).

กรณีไม่ปรากฏคุณค่าของการที่ยังคงมีชื่อและสกุลของบุคคลที่ก่อเหตุในข่าว การเกิดสถิติของอุบัติเหตุบนท้องถนนนั้น ยังคงทำได้โดยไม่ต้องมีชื่อของบุคคลอยู่

CJEU ในคดี *Plaintiff X v. PrimaDanoi* ต่อไป ศาลฎีกาของประเทศอิตาลีวินิจฉัยว่าแม้บทความดังกล่าวจะถูกเผยแพร่โดยชอบด้วยกฎหมายและเคยมีประโยชน์สาธารณะ แต่การที่ยังทำให้บทความนี้สามารถเข้าถึงได้อย่างไม่ได้สัดส่วน ก่อให้เกิดผลกระทบต่อสิทธิในความเป็นอยู่ส่วนตัวของบุคคล จึงต้องมีการลบข้อมูลที่ถูกเผยแพร่

CJEU ในคดี *Segerstedt-Wiberg and Others v. Sweden* วินิจฉัยว่าการที่ตำรวจยังคงทำการเก็บรวบรวมข้อมูลซึ่งเป็นประวัติการกระทำความผิดของผู้ร้องรายดังกล่าวเอาไว้ ซึ่งเป็นประวัติการกระทำความผิดที่กล่าวหาว่าผู้ร้องได้กระทำการอันเป็นปรปักษ์ร้ายแรงต่อการควบคุมของเจ้าหน้าที่ตำรวจระหว่างการเดินขบวนใน ค.ศ. 1969 การเก็บข้อมูลดังกล่าวแม้ว่าจะเป็นการเก็บรักษาข้อมูลที่มีความเกี่ยวข้อง อย่างไรก็ตาม การเก็บรักษาข้อมูลดังกล่าวเอาไว้ เป็นการแทรกแซงสิทธิในความเป็นส่วนตัวมากเกินสัดส่วน

คดี *Hurbain v. Belgium* คดี *Plaintiff X v. PrimaDanoi* และคดี *Segerstedt-Wiberg and Others v. Sweden* แสดงให้เห็นว่า “เวลาที่พ้นผ่านไป” นั้น ส่งผลให้น้ำหนักของการที่ข้อมูลส่วนบุคคลยังคงถูกเข้าถึงได้นั้นมีน้ำหนักลดลง แม้ว่า ณ จุดเริ่มต้น (ในอดีต) การเผยแพร่ข้อมูลจะเป็นไปโดยชอบ แต่ความจำเป็นที่สาธารณชนจะเข้าถึงข้อมูลส่วนบุคคลก็อาจลดลงตามกาลเวลา และส่งผลให้การไม่ลบหรือทำลายข้อมูลส่วนบุคคลนั้นไม่ได้สัดส่วนกับความเป็นส่วนตัวที่เสียไป

4.4.1.2 ประโยชน์ในการเข้าถึงยังอาจมีอยู่หากการเข้าถึงยังคงมีประโยชน์

อย่างไรก็ตาม มีข้อสังเกตว่าข้อมูลที่ถูกเผยแพร่นั้นอาจจำเป็นที่จะต้องถูกคงให้สามารถเข้าถึงได้ในช่วงเวลาหนึ่งไม่ได้หมายความว่าเมื่อเวลาพ้นผ่านไปแล้วจะต้องมีการลบหรือทำลายข้อมูลส่วนบุคคลในทันที CJEU ในคดี *Camera di Commercio di Lecce v. Manni* แสดงให้เห็นถึงความท้าทายในทางปฏิบัติของข้อมูลที่ถูกเก็บรวบรวมโดยทะเบียนสาธารณะของบริษัทซึ่งเป็นข้อมูลที่ถูกเก็บรวบรวมอยู่ในฐานข้อมูลของรัฐเพื่อประโยชน์สาธารณะ เช่น เพื่อให้บุคคลภายนอกที่จะทำธุรกรรมกับบริษัทสามารถตรวจสอบสถานะและข้อมูลของบริษัทได้ ในกรณีนี้ประโยชน์สาธารณะมีน้ำหนักมากกว่าความเป็นส่วนตัวโดยมิได้เป็นกรณีของการแทรกแซงที่ไม่ได้สัดส่วน

ในกรณี Re Credit Bureau (Singapore) Pte Ltd PDPC ของประเทศสิงคโปร์ พบว่า ระยะเวลาห้าปีนั้นสอดคล้องกับระยะเวลาการแสดงข้อมูลเกี่ยวกับการล้มละลายตามหน่วยงานรัฐด้านการล้มละลาย SG PDPC มองว่า ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลเป็นเวลาห้าปีนั้นสามารถช่วยให้สถาบันการเงินมีข้อมูลเกี่ยวกับประวัติด้านเครดิตของบุคคลซึ่งอาจเป็นผู้กู้ที่เป็นประโยชน์ต่อการพิจารณาให้สินเชื่อ และการเก็บรักษาข้อมูลเกี่ยวกับการล้มละลายนั้นยังมีความสมเหตุสมผลด้านธุรกิจ

คดี *Camera di Commercio di Lecce v. Manni* และกรณี *Re Credit Bureau (Singapore) Pte Ltd* เป็นตัวอย่างที่แสดงให้เห็นว่าข้อมูลส่วนบุคคลที่เป็น “ประโยชน์ต่อการสอบตรวจสอบ” เพื่อประโยชน์ในการทำธุรกรรมของบุคคลทั่วไปหรือการตรวจสอบเครดิตทางการเงินนั้นอาจมีน้ำหนักมากกว่าการคุ้มครองสิทธิในความเป็นส่วนตัวได้ กล่าวคือ

สิทธิในความเป็นส่วนตัวนั้นได้ถูกล่วงล้ำ แต่การล่วงล้ำนั้นยังมีความได้สัดส่วน กล่าวคือประโยชน์ที่บุคคลอื่นได้รับนั้นมีน้ำหนักมากกว่าความเป็นส่วนตัวที่เสียไป

4.4.2 การสร้างสมดุลระหว่างความเป็นส่วนตัวและสิทธิในการได้รับการฟื้นฟูกับประโยชน์สาธารณะ

สิทธิที่จะถูกลืมนั้นมีรากฐานประการหนึ่งจากสิทธิในการฟื้นฟูสภาพที่รับรองถึงสิทธิของเจ้าของข้อมูลในการร้องขอให้มีการลบประวัติที่ปรากฏในฐานข้อมูลตำรวจแห่งชาติที่ไม่ได้ถูกตัดสินว่ามีความผิด หรือเป็นประวัติที่เป็นเพียงการกล่าวหาเนื่องจากมีเหตุต้องสงสัยว่าบุคคลดังกล่าวได้กระทำผิดเท่านั้น[294] อย่างไรก็ตาม เมื่อสิทธิที่จะถูกลืมนั้นถูกจำกัดได้ด้วยประโยชน์สาธารณะ (ดังที่มาตรา 33 วรรคสองของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่าความใน (มาตรา 33) วรรคหนึ่งมิให้นำมาใช้บังคับกับการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นในกรณีเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล[295] ด้วยเหตุนี้ จึงเกิดความท้าทายว่าการสร้างความสมดุลระหว่างสิทธิในความเป็นส่วนตัวและประโยชน์สาธารณะนั้นจะเกิดในทางปฏิบัติได้อย่างไร

---

[294] โปรดดูรายละเอียดในหัวข้อ 2.1.2.1 ในบทที่ 2.

[295] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 วรรคสอง ประกอบมาตรา 24 (4).

4.4.2.1 สิทธิในการได้รับการฟื้นฟูและความเป็นส่วนตัวมีน้ำหนักมากกว่า

CJEU ในคดี *Hurbain v. Belgium* มีคำวินิจฉัยว่าบุคคลย่อมมีสิทธิที่จะสามารถกลับคืนสู่สังคมโดยไม่ต้องถูกรบกวนจากความผิดพลาดในอดีตหลังจากที่ได้รับการลงโทษเรียบร้อยแล้ว การรบกวนสิทธิได้รับการฟื้นฟูนั้นอาจเกิดขึ้นในลักษณะ เช่น การที่การกระทำความผิดยังคงถูกแสดงผลในรายการสืบค้นข้อมูลออนไลน์ กล่าวคือ การเก็บรวบรวมข้อมูลในระบบดิจิทัลนั้นอาจเกี่ยวข้องกับการกระทำความผิดอาญาได้ แต่การเก็บรวบรวมข้อมูลดังกล่าวนั้นจะต้องไม่เป็นไปในลักษณะของการทำหน้าที่เป็นระบบการเก็บประวัติอาชญากรรมแบบเสมือน (Virtual Criminal Record)

4.4.2.2 ประโยชน์สาธารณะมีน้ำหนักมากกว่าความเป็นส่วนตัว

ในคดี *NT1 & NT2 v Google LLC* ภายหลังจากพ้นโทษในคดีก่อน NT1 ยังคงกลับเข้ามาทำงานในแวดวงธุรกิจที่ NT1 เคยทำอยู่ก่อนหน้าที่ศาลจะพิพากษาให้ NT1 มีความผิดเกี่ยวกับธุรกิจของ NT1 ทำให้เห็นได้ว่า ข้อมูลพิพาทดังกล่าวเป็นข้อมูลที่เป็นประโยชน์ต่อวัตถุประสงค์ในด้านการลดความเสี่ยง (Risk Minimizing) ที่ว่าผู้ร้อง NT1 อาจยังคงไม่สำนึกผิดและยังคงมีพฤติกรรมเดิมตามที่ผู้ร้อง NT1 เคยต้องโทษจากการกระทำนั้นในอดีต ประกอบกับการที่ผู้ร้องมีส่วนเกี่ยวข้องกับคดีแพ่งหลายคดี ศาลจึงพิจารณาว่ากรณีดังกล่าวนี้ข้อมูลที่ว่าผู้ร้อง NT1 เคยถูกพิพากษาให้ได้รับโทษนั้นยังมีความเกี่ยวพันกับชีวิตในการทำงานของผู้ร้อง ดังนั้น ข้อมูลพิพาทดังกล่าวจึงควรจำต้องมีอยู่เพื่อประโยชน์สาธารณะด้วยเหตุนี้ ประโยชน์อันชอบธรรมของ Google LLC ในการประมวลผลข้อมูลส่วนบุคคลของผู้ร้อง NT1 จึงมีอยู่เหนือกว่าสิทธิในการจะถูกลืมของผู้ร้อง NT1

เมื่อเปรียบเทียบคดี *Melvin v. Reid* และคดี *NT1 & NT2 v Google LLC* แล้วจะเห็นได้ว่าการพิจารณาความสมดุลระหว่างความเป็นส่วนตัวและประโยชน์อันเกิดจากการที่สาธารณะยังคงสามารถเข้าถึงข้อมูลส่วนบุคคลได้นั้น เป็นเรื่องที่จะต้องพิจารณาเป็นรายกรณี (เช่นเดียวกับกรณีการชั่งน้ำหนักระหว่างสิทธิในความเป็นส่วนตัวกับเสรีภาพในการเข้าถึงข้อมูลและการแสดงออกตามที่กล่าวในหัวข้อ 4.4.1) คดี Hurbain v. Belgium ได้ให้น้ำหนักกับความเป็นส่วนตัวและสิทธิในการได้รับการฟื้นฟูและความเป็นส่วนตัวของบุคคลมากกว่าเสรีภาพในการแสดงออกของสำนักพิมพ์ ในขณะที่ในคดี *NT1 & NT2 v Google LLC* นั้น ข้อมูลเกี่ยวกับการรับโทษของเจ้าของข้อมูลส่วนบุคคลยังคงจำเป็นต่อสาธารณชน เนื่องจากการรับโทษในอดีตนั้นยังมีความเกี่ยวพันกับชีวิตในการทำงานของเจ้าของข้อมูลส่วนบุคคลในปัจจุบัน

บทสรุป

การประเมินความครอบคลุมของการคุ้มครองสิทธิที่จะถูกลืมนั้นสามารถเริ่มประเมินได้จากการพิจารณากฎหมายคุ้มครอง “ใคร” จากการศึกษาและวิเคราะห์กฎหมายในเชิงเปรียบเทียบจะเห็นได้ว่ามาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น มีศักยภาพที่จะคุ้มครองบุคคลที่ข้อมูลส่วนบุคคลของตนถูกประมวลผลโดยรับรองผ่านการระบุตัวผู้ทรงสิทธิโดยถ้อยคำ ได้แก่ “เจ้าของข้อมูลส่วนบุคคล (Data Subject)” ซึ่งเป็นแนวทางที่สอดคล้องกับกฎหมายของสหภาพยุโรป สหราชอาณาจักร เขตปกครองพิเศษไต้หวัน และเขตปกครองพิเศษฮ่องกง การบัญญัติถึงตัวผู้ทรงสิทธิตามกฎหมายไทยแตกต่างจากการบัญญัติถึงตัวผู้ทรงสิทธิของประเทศออสเตรเลีย ประเทศสิงคโปร์ และประเทศญี่ปุ่นนั้น

คุ้มครอง “ปัจเจกบุคคล” และ “ตัวการ” แต่ถึงแม้ว่ากฎหมายจะใช้ถ้อยคำที่แตกต่าง บุคคลที่ถูกคุ้มครองสิทธิที่จะถูกลืมตามกฎหมายไทยนั้นมีสารัตถะเช่นเดียวกับตัวบุคคลที่ถูกคุ้มครองตามกฎหมายประเทศออสเตรเลีย ประเทศสิงคโปร์ และประเทศญี่ปุ่น เนื่องจาการบัญญัติโดยใช้คำว่า “เจ้าของข้อมูลส่วนบุคคล” นั้น ก็สามารถครอบคลุมตัวปัจเจกบุคคลและตัวการได้เช่นกัน เนื่องจากโดยสาระแล้วบุคคลที่ถูกคุ้มครอง ได้แก่ บุคคลธรรมดาใด ๆ ที่ข้อมูลส่วนบุคคลของตนถูกประมวลผลโดยบุคคลอื่น

ในส่วนของผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืมนั้น การกำหนดหน้าที่ให้กับ “ผู้ควบคุมข้อมูลส่วนบุคคล” ตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลไม่ได้ก่อปัญหาว่าผู้มีอำนาจตัดสินใจในการประมวลผลข้อมูลบางรายจะไม่อยู่ในคำนิยาม ไม่ว่าจะสำนักพิมพ์หรือหน่วยงานของรัฐซึ่งเป็นผู้เผยแพร่ข้อมูลส่วนบุคคลตั้งแต่แรก ผู้ให้บริการเว็บไซต์ หรือผู้ให้บริการสืบค้นข้อมูลส่วนบุคคลล้วนมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หากปรากฏข้อเท็จจริงว่ามีอำนาจตัดสินใจว่าจะประมวลผลข้อมูลส่วนบุคคลในลักษณะใด ข้อจำกัดในการกำหนดหน้าที่แก่ผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์ เช่น Google นั้น ไม่เกิดตัวบทกฎหมายที่กำหนดหน้าที่ หากแต่เป็นข้อจำกัดของการที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศหนึ่งย่อมไม่มีผลบังคับถึงบุคคลซึ่งทำการประมวลผลข้อมูลจากต่างประเทศ

ในการคุ้มครองสิทธิที่จะถูกลืมนั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลจะต้องบัญญัติถึงการร้องขอผู้ทรงสิทธิและหน้าที่ดำเนินการโดยผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม การลบหรือทำลายข้อมูลเมื่อข้อมูลส่วนบุคคลหมดความจำเป็นที่จะต้องถูกประมวลผลตามวัตถุประสงค์ การกำหนดรายละเอียดเกี่ยวกับการลบ ทำลายและทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

และการบัญญัติถึงข้อจำกัดการใช้สิทธิที่จะถูกลืม ซึ่งสามารถกล่าวสรุปได้ว่า มาตรา 33 ประกอบมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นมีบทบัญญัติที่สอดคล้องกับกฎหมายของต่างประเทศและครอบคลุมรายละเอียดต่าง ๆ ที่จำเป็นต่อการคุ้มครองสิทธิที่จะถูกลืม

มีข้อสังเกตในส่วนของถ้อยคำในตัวบทกฎหมายได้แก่ “เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์” และ “การลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล” ถ้อยคำดังกล่าวเป็นถ้อยคำที่มีความยืดหยุ่นและจำเป็นที่จะต้องอาศัยการตีความและการพัฒนารายละเอียดต่อไป การที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้บัญญัติโดยถ้อยคำที่ยืดหยุ่นและถ้อยคำที่ต้องการรายละเอียดเพิ่มเติมต่อไปนั้น ไม่ได้เป็นกรณีที่กฎหมายไทยมีลักษณะที่ไม่ครอบคลุมแต่ประการใด เนื่องจากเป็นทางที่สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศซึ่งสามารถถูกพัฒนารายละเอียดและแนวปฏิบัติได้ต่อไป

ในส่วนของข้อจำกัดการคุ้มครองสิทธิที่จะถูกลืมนั้น การบัญญัติข้อยกเว้นตามข้อ 33 วรรคสองของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นเป็นไปโดยสอดคล้องกับแนวทางของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ ทั้งกฎหมายไทยและต่างประเทศต่างต้องเผชิญกับปัญหาการต้องสร้างความสมดุลระหว่างสิทธิในความเป็นส่วนตัวกับเสรีภาพในการเข้าถึงข้อมูลและการแสดงออกหรือการสร้างสมดุลระหว่างความเป็นส่วนตัวและสิทธิในการได้รับการฟื้นฟูกับประโยชน์สาธารณะ ซึ่งกฎหมายเปิดช่องให้หน่วยงานของรัฐ เช่น ศาล ทำหน้าที่พิจารณาข้อเท็จจริงเป็นรายกรณี

แม้ว่ามาตรา 33 และมาตรา 37 (2) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีลักษณะที่สอดคล้องกับกฎหมายคุ้มครองสิทธิที่จะถูกลืมของต่างประเทศ แต่อย่างไรก็ตาม มีข้อสังเกตว่าตัวบทกฎหมายมิได้ระบุถึง “สิทธิที่จะถูกลืม” โดยชัดแจ้งดังเช่นกรณีของมาตรา 17 ของ GDPR ซึ่งหากพิจารณาตามข้อสังเกตของ AAB ในฮ่องกงแล้ว สิทธิที่จะถูกลืมนั้นมีข้อความคิดเป็นของตัวเองและสามารถแยกออกจากสิทธิในการขอให้ลบข้อมูลตามมาตรา 26 ของ HK PDPO 1996 ได้ และประเทศไทยยังขาดรายละเอียดเกี่ยวกับข้อปฏิบัติในการลบ ทำลาย หรือทำให้ข้อมูลระบุตัวตนของบุคคลมิได้ นอกจากนี้ ยังปรากฏความท้าทายที่ว่า ผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์นั้น อาจไม่สามารถดำเนินการลบหรือทำลายข้อมูลที่ถูกเผยแพร่โดยผู้ควบคุมข้อมูลส่วนบุคคลอื่น ข้อจำกัดเหล่านี้จะได้มีการนำเสนอแนวทางการพัฒนาต่อไปในบทที่ 5

บทที่ 5
บทสรุปและข้อเสนอแนะ

แม้ว่าจะไม่ได้บัญญัติถึงสิทธิที่จะถูกลืมเอาไว้โดยชัดแจ้งในตัวบทกฎหมาย สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีส่วนในการคุ้มครองสิทธิที่จะถูกลืมในมิติของการลบ ทำลายหรือทำให้ข้อมูลระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ อย่างไรก็ตาม งานวิจัยนี้เสนอให้มีการพัฒนาตัวบทกฎหมายโดยมีการเพิ่มคำว่า “สิทธิที่จะถูกลืม” เข้าไปในมาตรา 33 และมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และบัญญัติรายละเอียดเกี่ยวกับการนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์สามารถปฏิบัติตามกฎหมายได้ และควรมีการออกกฎหมายลำดับรองหรือออกแนวปฏิบัติซึ่งกำหนดรายละเอียดการลบ ทำลายข้อมูลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลที่มีหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถปฏิบัติตามกฎหมายได้

5.1 บทสรุป

สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 33 ประกอบมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น มีคุณสมบัติที่จะเรียกได้ว่า “สิทธิที่จะถูกลืม” ตามฐานทางทฤษฎีและมาตรฐานของกฎหมายในระดับสากล อย่างไรก็ตาม มิได้บัญญัติโดยใช้ถ้อยคำว่า “สิทธิที่จะถูกลืม” เอาไว้ในตัวกฎหมาย โดยบัญญัติเพียงตัวอย่างของการใช้สิทธิที่จะถูกลืมเอาไว้ กล่าวคือ การลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้ การบัญญัติกฎหมายในลักษณะดังกล่าวแตกต่างไปจากถ้อยคำที่ปรากฏในมาตรา 17 ของ GDPR ที่มีคำว่า “Right to be Forgotten” ควบคู่ไปกับ “Right to Erasure”

5.1.1 การลบทำลายและทำให้ข้อมูลกลายเป็นข้อมูลที่ระบุตัวตนไม่ได้

เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นบุคคลธรรมดา สามารถอาศัยสิทธิตามมาตรา 33 ดังกล่าวในการเรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งหมายรวมถึงทั้งผู้ทำการเก็บรวบรวมและเผยแพร่ข้อมูลส่วนบุคคล (เช่น สำนักพิมพ์) และผู้ให้บริการสืบค้นข้อมูลออนไลน์ (เช่น Google) ทำการ “ลบ” “ทำลาย” หรือ “ทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้” อันเป็นสาระสำคัญของสิทธิที่จะถูกลืม จะเห็นได้ว่าสิทธิตามมาตรา 33 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นรวมไปถึงสิทธิในการทำให้ข้อมูลส่วนบุคคลนั้นกลายเป็นข้อมูลที่ไม่อาจถูกระบุตัวตนได้โดยอาจไม่ได้เป็นการลบหรือทำลายข้อมูลส่วนบุคคล อันเป็นการดำเนินการคุ้มครองสิทธิที่จะถูกลืม โดยเป็นฐานทางกฎหมายให้มีการกำหนดหน้าที่หรือสั่งให้สำนักพิมพ์ทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้

อย่างไรก็ตาม การใช้ถ้อยคำที่ยืดหยุ่นว่าเป็นกรณีที่ “หมดความจำเป็น” โดยไม่ได้บัญญัตินิยามและรายละเอียดเอาไว้ดังเช่นกฎหมายของต่างประเทศนั้น[296] ถือได้ว่ามีความเหมาะสมแล้ว เนื่องจากการหมดความจำเป็นในการเผยแพร่และเข้าถึงข้อมูลของสาธารณชนนั้นจะต้องพิจารณาเป็นรายกรณี

5.1.2 การนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลที่ถูกแสดงบนอินเทอร์เน็ต

ในกรณีที่เป็นการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้ โดยผู้ให้บริการสืบค้นข้อมูล เช่น Google นั้น กรณีนี้มีประเด็นต้องพิจารณาต่อไปว่า ในกรณีที่ผู้ให้บริการสิทธินำออกจากการแสดงข้อมูลบนเว็บไซต์ (Delisting/Delinking) สิทธินี้มิใช่การลบข้อมูลส่วนบุคคลออกไปโดยสิ้นเชิง ข้อมูลส่วนบุคคลดังกล่าวจะยังคงแสดงหรือปรากฏอยู่บนหน้าเว็บเพจหรือเว็บไซต์ที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลเดิม (Original Controller)[297] นั้น เป็นการดำเนินการตามที่มาตรา 33 และมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่

สิทธิในการขอให้นำข้อมูลออกจากโปรแกรมสืบค้นข้อมูลนั้นมีผลเฉพาะต่อ “ผลลัพธ์” ในส่วนของ “ชื่อ” ที่ปรากฏจากการสืบค้นเท่านั้น และไม่ส่งผลให้ต้องมีการลบลิงค์จากดัชนีแสดงผลการค้นหาของระบบสืบค้นทั้งหมด ส่งผลให้ข้อมูลที่ถูกเผยแพร่เดิมยังคงถูกเข้าถึงได้โดยการอาศัยคำค้นหาอื่น ๆ หรือการเข้าถึงจากฐานข้อมูลของผู้เผยแพร่โดยตรง

---

[296] โปรดดู ข้อเปรียบเทียบ เรื่อง การพิจารณาการหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลในเอกสารหมายเลข 4 ตามภาคผนวก 1.

[297] โปรดดู หัวข้อ 2.1.2.3 ในบทที่ 2.

ดังนั้น ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นผู้ให้บริการสืบค้นข้อมูลส่วนบุคคล เช่น Google อาจดำเนินการเพียงการนำข้อมูลออกจากผลการค้นหาก็ถือได้ว่าเป็นการดำเนินการเพื่อความคุ้มครองความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลแล้ว โดยไม่ต้องทำการลบหรือทำลายข้อมูลส่วนบุคคลซึ่งอาจเป็นข้อมูลที่ถูกเผยแพร่โดยบุคคลอีกคนหนึ่ง เช่น สำนักพิมพ์ เป็นต้น

5.1.3 ผู้ควบคุมข้อมูลซึ่งมิได้อยู่ในราชอาณาจักรไทย

การคุ้มครองสิทธิที่จะถูกลืมนี้ ไม่ได้เป็นอันหนึ่งอันเดียวกันในทุกประเทศ ด้วยเหตุนี้ การคุ้มครองสิทธิในความเป็นส่วนตัวในมิติของการร้องขอให้นำข้อมูลออกจากระบบนั้น จะต้องคำนึงถึงกรอบทางกฎหมายและระดับการคุ้มครองสิทธินี้ในแต่ละประเทศอีกด้วย กรณีศึกษาซึ่งได้แสดงในบทที่ 3 และบทวิเคราะห์ในบทที่ 4 ได้แสดงให้เห็นว่าข้อมูลส่วนบุคคลซึ่งถูกแสดงผ่านระบบการสืบค้นข้อมูลและสามารถเข้าถึงได้โดยผ่านระบบอินเทอร์เน็ตนั้น มีข้อจำกัดในการจะถูกลืม เนื่องจากตัวผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์นั้นตั้งอยู่ในประเทศที่เป็นคนละประเทศกับเจ้าของข้อมูลส่วนบุคคล และอาจเป็นไปได้ที่กฎหมายในประเทศที่ผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์นั้น ไม่ได้รับรองและคุ้มครองสิทธิที่จะถูกลืมในระดับที่เท่าเทียมกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศที่เจ้าของข้อมูลส่วนบุคคลอยู่

ดังที่ได้วิเคราะห์ในบทที่ 4 หากผู้ให้บริการระบบสืบค้นข้อมูลออนไลน์เฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรและแสดงผลเกี่ยวกับพฤติกรรมดังกล่าว ผู้ให้บริการระบบสืบค้นข้อมูลดังกล่าวย่อมตกอยู่ในบังคับของมาตรา 33 และมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตัวบทกฎหมายในปัจจุบันจึงไม่ได้มีปัญหาที่ว่าไม่อาจครอบคลุมการดำเนินกิจกรรมของผู้ให้บริการระบบ

สืบค้นข้อมูลออนไลน์ที่ตั้งในต่างประเทศได้ อย่างไรก็ตาม ความท้าทายของกฎหมายจะเป็นประเด็นเรื่องการบังคับใช้กฎหมายไทยในทางต่างประเทศ

5.2 ข้อเสนอแนะ

ผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 33 และมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นย่อมหมายรวมถึงบุคคลที่เผยแพร่ข้อมูลผ่านอินเทอร์เน็ตโดยตรง เช่น สำนักพิมพ์ และผู้ให้บริการสืบค้นข้อมูลออนไลน์ เช่น Google อีกด้วย สิ่งที่ผู้ให้บริการสืบค้นข้อมูลออนไลน์ดำเนินการเพื่อคุ้มครองสิทธิที่จะถูกลืมได้ อาจมีขอบเขตจำกัดเพียงการนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลบนเว็บไซต์เท่านั้น มิได้รวมไปถึงการลบ ทำลายข้อมูลส่วนบุคคลซึ่งถูกเผยแพร่หรือครอบครองโดยผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น นอกจากนี้ ยังมีความท้าทายที่จะต้องมีการกำหนดถึงหลักเกณฑ์และรายละเอียดเกี่ยวกับการ “ลบ” “ทำลาย” หรือ “ทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่ไม่อาจระบุตัวตนได้” อีกด้วย

5.2.1 เพิ่มคำว่า “สิทธิที่จะถูกลืม” ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เพื่อให้เกิดความชัดเจนเกี่ยวกับการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งในกรณีของผู้ให้บริการสืบค้นข้อมูลออนไลน์ ทั้งนี้ เพื่อรองรับข้อเท็จจริงที่ว่าการสื่อสารแลกเปลี่ยนความคิดของคนในสังคมนั้นเกิดขึ้นในโลกดิจิทัลมากขึ้น จึงควรเพิ่มเติมคำว่า “สิทธิที่จะถูกลืม” ในมาตรา 33 และมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 33 เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะถูกลืม โดยดำเนินการขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูล แล้วแต่กรณี ในกรณีดังต่อไปนี้

...

มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

...

(3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินเพื่อคุ้มครองสิทธิที่จะถูกลืมโดยดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลหรือนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูล แล้วแต่กรณี เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมายหรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความในมาตรา 33 วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

การแก้ไขกฎหมายโดยเพิ่มเติมคำว่า “สิทธิที่จะถูกลืม” ในมาตรา 33 และมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะช่วยให้เกิดความชัดเจนว่าหากผู้ให้บริการสืบค้นข้อมูลได้ดำเนินการนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลแล้วก็ย่อมถือได้ว่าปฏิบัติหน้าที่ตามกฎหมายแล้ว โดยไม่ต้องดำเนินการเพื่อลบหรือทำลายข้อมูล

ในทำนองเดียวกับมาตรา 17 วรรคสองของ GDPR มาตรา 33 วรรคสาม ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลบัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องเป็นผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำขอนั้น โดยแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ เพื่อให้ได้รับคำตอบในการดำเนินการให้เป็นไปตามคำขอ ซึ่งมีผลเสมือนเป็นการได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคลโดยตรงเพื่อให้กระบวนการยื่นคำร้องต่อผู้ควบคุมข้อมูลทั้งหมดมีผล ด้วยการยื่นคำร้องเพียงฉบับเดียว หน้าที่ในการแจ้งไปยังผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าวย่อมมีส่วนช่วยคุ้มครองสิทธิที่จะถูกลืมของเจ้าของข้อมูลส่วนบุคคลต่อไป[298]

5.2.2 การออกประกาศหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้ ตามมาตรา 33 วรรคท้ายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การออกกฎหมายลำดับรอง (หรือแนวปฏิบัติ) ดังกล่าวอาจดำเนินการโดยอาศัยแนวปฏิบัติของต่างประเทศตามที่ได้กล่าวในบทที่ 4 มาเป็นฐานในการดำเนินการ โดยครอบคลุมประเด็นต่าง ๆ ดังต่อไปนี้

---

[298] อรรถกร สุขปุณพันธ์ (อ้างแล้ว เชิงอรรถที่ 35), หน้า 16.

5.2.2.1 การลบ ทำลายข้อมูลส่วนบุคคล

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลควรกำหนด “ลักษณะ” ของการดำเนินการที่ถือได้ว่าเป็นการ “ลบ” หรือ “ทำลาย” ข้อมูลส่วนบุคคล โดยคำนึงถึงหลักเกณฑ์ เช่น การทำให้ข้อมูลส่วนบุคคลที่หมดความจำเป็นในการประมวลผลแล้วนั้น หมายถึง การทำให้ข้อมูลถูกลบหรือทำลายโดยไม่อาจกลับคืนมาได้อีก ซึ่งสอดคล้องกับแนวปฏิบัติของสหราชอาณาจักรและฮ่องกง

หลักเกณฑ์ที่ถูกประกาศนั้น ควรยอมรับ “วิธีการ” ที่หลากหลายและสอดคล้องกับลักษณะของข้อมูลตามแนวทางของประเทศออสเตรเลีย ซึ่งกำหนดวิธีการทำลายข้อมูลส่วนบุคคลจะขึ้นอยู่กับรูปแบบของแหล่งเก็บข้อมูล ได้แก่ ข้อมูลที่ถูกเก็บไว้ในรูปแบบของกระดาษ ทิ้งลงถังขยะหรือรีไซเคิลเอกสาร หรือกระดาษซึ่งมีข้อมูลส่วนบุคคลนั้น ไม่ถือเป็นการดำเนินการที่เหมาะสมในการทำลายข้อมูลส่วนบุคคล เว้นแต่ว่าข้อมูลส่วนบุคคลนั้นจะได้ถูกทำลายผ่านกระบวนการ เช่น การทำให้เป็นเยื่อกระดาษ การเผาทำลาย การย่อยหรือการบด การทำให้สลายหรือละลาย หรือการบดทำลาย เป็นต้น

5.2.2.2 การทำให้ข้อมูลอยู่เหนือการใช้งาน

นอกจากกรณีของการลบข้อมูลส่วนบุคคลแล้ว ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ยังอาจจะรับรองแนวทางอื่นเพื่อการจัดการกับการลบข้อมูลในรูปแบบอื่น ดังเช่น ในการทำให้ข้อมูลอยู่เหนือการใช้งาน โดยถือว่าเป็นการลบข้อมูลตามกฎหมาย ซึ่ง ICO ได้ออกแนวปฏิบัติระบุให้การทำให้ข้อมูลอยู่เหนือการใช้งาน หากว่าข้อมูลดังกล่าวไม่ได้ถูกลบออกไปจริง แต่ปรากฏด้วยว่าผู้ควบคุมข้อมูลส่วนบุคคลนั้นได้ปฏิบัติให้เป็นไปกรณีดังนี้ (1) ไม่สามารถ หรือจะไม่พยายามใช้ข้อมูลส่วนบุคคลเพื่อแจ้งให้ทราบถึงการตัดสินใจใด ๆ ที่เกี่ยวข้องกับบุคคลใด ๆ หรือในลักษณะที่ส่งผล

ต่อบุคคลใด ๆ และไม่ว่าด้วยวิธีใดก็ตาม (2) ไม่อนุญาตให้หน่วยงานอื่นใดสามารถเข้าถึงข้อมูลส่วนบุคคลนั้นได้ (3) จัดให้มีความมั่นคงปลอดภัยทางด้านเทคนิคและด้านการบริหารจัดการ และ (4) ให้คำมั่นว่าจะลบข้อมูลนั้นทิ้งอย่างถาวร เมื่อหรือหากสามารถดำเนินการเช่นนั้นได้

5.2.2.3 การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ควรกำหนดหลักเกณฑ์และวิธีการในการทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้ โดยอาจกำหนดให้มี คือ การกำจัดหรือเปลี่ยนให้ข้อมูลที่บ่งชี้บุคคลหรือมีลักษณะที่อาจสามารถบ่งชี้ตัวตนได้ ทั้งนี้ ขั้นตอนในการทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้ อาจประกอบไปด้วย 2 ขั้นตอน ดังต่อไปนี้ (1) ลบตัวบ่งชี้บุคคล (Personal Identifiers) เช่น ชื่อ ที่อยู่ วันเกิด หรือข้อมูลที่บ่งชี้ตัวตนอื่น ๆ ของบุคคล และ (2) ลบหรือเปลี่ยนแปลงข้อมูลอื่นที่อาจเป็นการยอมให้บุคคลนั้นถูกบ่งชี้ตัวตน เช่น ลักษณะของบุคลิกภาพที่มีลักษณะพบเจอได้ยาก หรือลักษณะของบุคลิกภาพที่เมื่อรวมกันแล้วมีลักษณะพิเศษ หรือมีลักษณะโดดเด่นที่ทำให้สามารถบ่งชี้หรือระบุตัวตนได้

การทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้ อาจไม่ได้เป็นการกำจัดความเสี่ยงที่ว่าบุคคลนั้นสามารถถูกบ่งชี้ตัวตนอีกครั้ง โดยที่อาจมีความเป็นไปได้ว่าชุดข้อมูลหรือข้อมูลอื่นอาจไปสอดคล้องหรือตรงกับข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวตนได้ ทั้งนี้ ความเสี่ยงของการกรณีการที่ข้อมูลสามารถถูกบ่งชี้ตัวตนได้อีกครั้ง จำต้องมีการประเมินและบริหารจัดการเพื่อลดความเสี่ยงอยู่เสมอ โดยที่ปัจจัยที่เกี่ยวข้องเมื่อต้องกำหนดว่าข้อมูลเหล่านี้ได้ถูกดำเนินการให้เป็นข้อมูลที่ไม่สามารถบ่งชี้ตัวตนได้นั้น อาจเกี่ยวเนื่องไปถึงต้นทุน ความยากลำบาก การปฏิบัติได้จริง และความเป็นไปได้ในการที่ข้อมูลนั้นอาจถูกทำให้สามารถระบุตัวตนได้อีกครั้ง

5.2.2.4 การนำข้อมูลส่วนบุคคลออกจากการแสดงผล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยุโรป ได้อธิบายสิทธิที่จะถูกลืมในแง่มุมของสิทธิในการร้องขอให้นำออกจากโปรแกรมสืบค้นข้อมูลนั้นว่ามิใช่สิ่งเดียวกับการลบข้อมูลส่วนบุคคล โดยระบุว่ากิจกรรมการประมวลผลข้อมูลของโปรแกรมสืบค้นข้อมูลนั้น ควรต้องถูกนิยามให้แตกต่างจากการประมวลผลข้อมูลที่ดำเนินการโดยผู้เผยแพร่ข้อมูลที่เป็นบุคคลภายนอก เช่น สื่อต่าง ๆ ที่ให้ข้อมูลข่าวสารออนไลน์

การกำหนดหลักเกณฑ์และวิธีการในการนำข้อมูลส่วนบุคคลออกจากการแสดงผลตามประกาศคณะกรรมคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 33 วรรคท้ายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ควรจะมีหลักเกณฑ์โดยรับรู้ว่า (1) การใช้สิทธินำออกจากโปรแกรมสืบค้นข้อมูลโดยผู้ให้บริการระบบสืบค้นออนไลน์ไม่ได้เป็นการใช้สิทธิที่สามารถร้องขอให้ข้อมูลส่วนบุคคลนั้นถูกลบออกไปจากระบบอินเทอร์เน็ตโดยสิ้นเชิง และ (2) ข้อมูลส่วนบุคคลจะยังคงไม่ถูกลบออกจากแหล่งข้อมูลทั้งที่เป็นเว็บไซต์และการแสดงผลและหน่วยความจำขนาดเล็กที่มีความเร็วสูงซึ่งเก็บข้อมูลหรือคำสั่งที่ถูกเรียกใช้หรือเรียกใช้บ่อย ๆ (Cache) ของผู้ให้บริการโปรแกรมสืบค้นข้อมูล แต่เป็นเพียงการนำผลแสดงการค้นหาออกจากการแสดงการค้นหาบนหน้าโปรแกรมสืบค้นข้อมูลเท่านั้น

บทสรุป

การแก้ไขกฎหมายโดยเพิ่มเติมคำว่า “สิทธิที่จะถูกลืม” ในมาตรา 33 และมาตรา 37 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะช่วยให้เกิดความชัดเจนว่ากฎหมายนั้นรับรู้ว่าสิทธิที่จะถูกลืมมีขอบเขตที่สามารถถูกพัฒนาไปได้ไกลกว่าการลบหรือทำลายข้อมูลส่วนบุคคล โดยรับรู้ว่าการถูกลืมนั้นอาจเกิดขึ้นจากการลบหรือทำลายข้อมูลในเชิงกายภาพหากข้อมูลนั้นเป็นวัตถุที่จับต้องได้ และขณะเดียวกันก็รับรู้ว่าการลบสิ่งที่ระบบสืบค้นข้อมูลออนไลน์แสดงผลผ่านอินเทอร์เน็ตก็นับได้กว่าเป็นการคุ้มครองสิทธิที่จะถูกลืมได้เช่นกัน แม้ว่าข้อมูลส่วนบุคคลนั้นอาจจะยังไม่ถูกลบหรือทำลายในฐานข้อมูลหรือระบบของผู้เผยแพร่ข้อมูลรายอื่น เช่น สำนักพิมพ์หรือหน่วยงานของรัฐ กล่าวได้ว่า การพัฒนากฎหมายเพื่อคุ้มครองสิทธิที่จะถูกลืมนั้นจะต้องเป็นได้โดยสอดคล้องและพร้อมที่จะตอบสนองต่อสภาพของข้อเท็จจริงในสังคม โดยเฉพาะยิ่งความก้าวหน้าในการสื่อสารและระบบฐานข้อมูลอิเล็กทรอนิกส์ในโลกยุคดิจิทัล

การแก้ไขกฎหมายตามข้อเสนอในบทที่ 5 นี้จะช่วยสร้างความชัดเจนว่าผู้ให้บริการสืบค้นข้อมูลออนไลน์ซึ่งมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายสามารถมีส่วนคุ้มครองสิทธิที่จะถูกลืมของเจ้าของข้อมูลส่วนบุคคลได้ โดยการนำเอาผลการแสดงการค้นหาออกจากระบบการสืบค้นในลักษณะ de-listing โดยไม่จำเป็นต้องมีการลบข้อมูลในฐานะข้อมูลซึ่งถูกเผยแพร่โดยบุคคลอื่น และเมื่อผู้ให้บริการสืบค้นข้อมูลได้ดำเนินการนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลแล้ว ก็ย่อมถือได้ว่าปฏิบัติหน้าที่ตามกฎหมายแล้วโดยไม่ต้องกังวลว่าจะมีความรับผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากการฝ่าฝืนกฎหมาย

นอกจากนี้ เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมายและเป็นไปได้ในทางปฏิบัติ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลควรอาศัยอำนาจตามมาตรา 33 วรรคท้าย ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ออกประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล โดยควรมีรายละเอียดและแนวการปฏิบัติเกี่ยวกับนำข้อมูลส่วนบุคคลออกจากการแสดงข้อมูลอีกด้วย นอกจากการออกกฎหมายลำดับรองแล้ว คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังสามารถออกแนวการปฏิบัติในลักษณะเป็นข้อแนะนำ หรือแนวการปฏิบัติที่ดีเพื่อสนับสนุนการให้มีการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เหมาะสมกับลักษณะของข้อมูลส่วนบุคคลได้อีกด้วย

ภาคผนวก

หมายเลข 1 : ข้อเปรียบเทียบ เรื่อง ผู้ทรงสิทธิที่จะถูกลืม

ข้อเปรียบเทียบ เรื่อง ผู้ทรงสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 33)	เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้	บุคคลธรรมดา
GDPR (มาตรา 17)	“The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay…”	Data subject หมายถึง เจ้าของข้อมูลส่วนบุคคล หมายถึง บุคคลที่สามารถถูกระบุอัตลักษณ์ได้ ไม่ว่าจะโดยตรงหรือโดยอ้อม โดยเฉพาะอย่างยิ่งด้วยการอ้างอิงจากสิ่งระบุอัตลักษณ์เป็นการเฉพาะ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลสถานที่

ข้อเปรียบเทียบ เรื่อง ผู้ทรงสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
		สิ่งระบุอัตลักษณ์ออนไลน์หรือปัจจัยอย่างหนึ่งหรือมากกว่าที่เจาะจงไปยังอัตลักษณ์ทางกายภาพ กายวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคลธรรมดา นั้น
UK DPA 2018	บังคับใช้เช่นเดียวกัน GDPR	บังคับใช้เช่นเดียวกัน GDPR
TW PDPA 2015 (มาตรา 11 วรรคสามและมาตรา 2 (9))	A data subject shall be able to exercise the following rights with regard to his/her personal data and such rights shall not be waived or limited contractually in advance ...5. the right to erase his/her personal data.”	Data subject หมายถึงบุคคลธรรมดาที่เป็นเจ้าของข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม ประมวลผลและใช้งาน

ข้อเปรียบเทียบ เรื่อง ผู้ทรงสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
AUS PA 1988 (มาตรา 20 Y และมาตรา 6)	“ (2) The credit reporting body must : (a) destroy the credit reporting information… (i) give the individual a written notice that states that the information has been destroyed…”	Individual หมายถึง บุคคลธรรมดา
JP APPI 2020 (มาตรา 30 และมาตรา 2 (8))	“A principal may…demand of a personal information handling business operator a utilization cease or deletion…of the retained personal data…”	Principal หมายถึง ปัจเจกบุคคลเฉพาะที่สามารถถูกบ่งชี้ตัวตนได้โดยข้อมูลส่วนบุคคล
HK PDPO 1996 (มาตรา 27)	(Erasure of personal data no longer required)	Data user หมายถึง บุคคลธรรมดาที่เป็นเจ้าของข้อมูลส่วนบุคคล

ข้อเปรียบเทียบ เรื่อง ผู้ทรงสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
	(1) A data user must take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose (including any directly related purpose) for which the data was used unless—…"	
PH DPA 2012 (มาตรา 16 และมาตรา 3)	*"Rights of the Data Subject.* – The data subject is entitled to… (e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system…"	Data subject หมายถึง ปัจเจกบุคคล ที่เป็นเจ้าของข้อมูลส่วนบุคคลที่ถูกประมวลผล

ข้อเปรียบเทียบ เรื่อง ผู้ทรงสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
SG PDPA 2012	"An organization shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals..."	Individual หมายถึง บุคคลธรรมดาทั้งที่มีชีวิตอยู่และที่เสียชีวิตแล้ว

หมายเลข 2 : ข้อเปรียบเทียบ เรื่อง ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม

ข้อเปรียบเทียบ เรื่อง ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (มาตรา 33) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม (มาตรา 37)	ผู้ควบคุมข้อมูลส่วนบุคคลรวมถึงหน่วยงานของรัฐ (โดยมีข้อยกเว้นในบางกรณี) แต่ไม่ได้บัญญัติหน้าที่ให้กับหน่วยงานของรัฐเอาไว้เป็นการเฉพาะ (เทียบกับ TW PDPA 2015)

ข้อเปรียบเทียบ เรื่อง ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
GDPR (มาตรา 4 (7))	ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการลบข้อมูลส่วนบุคคลโดยไม่ล่าช้าหากไม่มีเหตุอันควร	ผู้ควบคุมข้อมูลส่วนบุคคล หมายถึง บุคคลธรรมดาหรือนิติบุคคล หน่วยงาน สาธารณะที่มีอำนาจ หรือองค์กรใดที่กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล ไม่ว่าโดยลำพังหรือร่วมกัน โดยที่วัตถุประสงค์และวิธีการในการประมวลผลดังกล่าวถูกกำหนดโดยกฎหมายของสหภาพหรือรัฐสมาชิก ผู้ควบคุมข้อมูลส่วนบุคคลหรือเกณฑ์เฉพาะสำหรับการแต่งตั้งตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลอาจถูกกำหนดไว้โดยกฎหมายของสหภาพหรือรัฐสมาชิก

ข้อเปรียบเทียบ เรื่อง ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
UK DPA 2018 (มาตรา 32)	"...In this Part, "controller" means the competent authority which, alone or jointly with others..."	UK DPA 2018 มีการใช้นิยามของคำว่าผู้ควบคุมข้อมูลส่วนบุคคลตาม GDPR และได้บัญญัติเพิ่มเติมใน UK DPA 2018 ให้ผู้ควบคุมข้อมูลส่วนบุคคล หมายความรวมถึงหน่วยงานของรัฐผู้มีอำนาจ
TW PDPA 2015 (มาตรา 11 มาตรา 2 (7) และ (8))	"...When the specific purpose of data collection no longer exists, or upon expiration of the relevant time period, **the government or non-government agency shall, on its own initiative or upon the request of the data subject, erase** or cease processing or using the personal data..."	หน่วยงานของรัฐ หมายถึง หน่วยงานของรัฐบาลกลางหรือท้องถิ่น หรือหน่วยงานทางปกครอง (Administrative Entity) ที่ใช้อำนาจของรัฐ (Public Authority) องค์กรนอกภาครัฐ หมายถึง บุคคลธรรมดา นิติบุคคล หรือกลุ่มบุคคล นอกเหนือจากที่ระบุไว้ข้างต้นซึ่งเป็นหน่วยงานภาคเอกชน บุคคลธรรมดาทั่วไป และหน่วยงานที่รัฐไม่ได้เป็นเจ้าของ

ข้อเปรียบเทียบ เรื่อง ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง	คำอธิบาย
AUS PA 1988 (มาตรา 6)	"... (a) **an APP entity** holds personal information...the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is deidentified."	APP entity หมายถึง หน่วยงานของรัฐ (Agencies) [299] หรือองค์กรเอกชน (Organization)

[299] Agency หมายถึง รัฐมนตรี กระทรวง หน่วยงานหรือองค์คณะไกล่เกลี่ย (Tribunal) จัดตั้งขึ้นหรือได้รับมอบหมายเพื่อวัตถุประสงค์สาธารณะภายใต้กฎหมาย หน่วยงานหรือองค์คณะไกล่เกลี่ย (tribunal) จัดตั้งขึ้นหรือได้รับมอบหมายเพื่อวัตถุประสงค์สาธารณะภายใต้กฎหมายของรัฐหรืออาณาเขตปกครองตนเองที่มีอำนาจอยู่ใน (as in force) อาณาเขตปกครองตนเองภายนอก (external Territory) หน่วยงานที่ได้รับมอบหมายหรือแต่งตั้งจาก Governor General หรือจากรัฐมนตรีภายใต้กฎหมาย Commonwealth รวมไปถึงบุคคลที่มีหน้าที่หรือปฏิบัติหน้าที่อยู่ในตำแหน่งที่จัดตั้งขึ้นตามกฎหมาย Commonwealth นอกเหนือจากเลขาธิการกระทรวง หรือของรัฐหรือเขตดินแดนของออสเตรเลียที่มีอำนาจอยู่ในเขตดินแดนภายนอก (external territory) ศาลกลาง (federal court) สำนักงานตำรวจกลาง (Australian Federal Police) ศาลแห่งเกาะนอร์ฟอล์ค ผู้ให้บริการด้านหู คอ จมูก (eligible hearing service provider) ผู้ให้บริการด้านสุขภาพภายใต้ Healthcare Identifiers Act 2010 Organization หมายถึง บุคคล ธรรมดา นิติบุคคล ห้างหุ้นส่วน นิติบุคคลอื่น ๆ ที่ไม่ได้จดทะเบียน ทรัสต์ (โดยที่ไม่ใช่ผู้ประกอบธุรกิจขนาดเล็ก พรรคการเมืองจดทะเบียน หน่วยงานของรัฐ รัฐ หรือเขตแดน (territory) หรือ หน่วยงานที่จัดตั้งขึ้นโดยรัฐหรือเขตแดน (territory) และดำเนินการเพื่อประโยชน์สาธารณะ รวมไปถึงหน่วยงานสื่อที่มีกิจกรรมเกี่ยวกับวารสารศาสตร์ (journalism)) เฉพาะในกรณีที่หน่วยงานนั้นได้ให้คำมั่นต่อสาธารณะต่อมาตรฐานการเผยแพร่ความเป็นส่วนบุคคล)

ข้อเปรียบเทียบ เรื่อง ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
JP APPI 2020 (มาตรา 30 และมาตรา 5)	“A principal may…demand of a personal information handling business operator a utilization cease or deletion…of the retained personal data…”	ผู้ประกอบกิจการที่จัดการกับข้อมูลส่วนบุคคล โดยไม่รวมถึงองค์กรรัฐบาลกลาง รัฐบาลท้องถิ่น หน่วยงานทางปกครองที่จดทะเบียน หน่วยงานทางปกครองจดทะเบียนท้องถิ่น
HK PDPO 1996 (มาตรา 26)	“ (1) A data user must take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose (including any directly related purpose) for which the data was used unless—…”	ผู้ใช้ข้อมูล หมายถึง บุคคลไม่ว่าโดยลำพังหรือร่วมกับบุคคลอื่น ควบคุมการเก็บรวบรวม การมีไว้ในครอบครอง การประมวลผลหรือการใช้ข้อมูล โดยไม่ปรากฏว่า PDPO ได้กำหนดยกเว้นผู้ใช้งานที่เป็นหน่วยงานรัฐแต่อย่างใด

ข้อเปรียบเทียบ เรื่อง ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
	"Rights of the Data Subject. – The data subject is entitled to... (e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system..."	ผู้ควบคุมข้อมูลส่วนบุคคล (Personal Information Controller) หมายถึง บุคคลหรือหน่วยงานที่ควบคุมการเก็บรวบรวม การมีไว้ในครอบครอง การประมวลผล และการใช้ข้อมูลส่วนบุคคล รวมไปถึงบุคคลหรือหน่วยงานที่สั่งการบุคคลหรือหน่วยงานอื่นในการเก็บรวบรวม มีไว้ในครอบครอง ประมวลผล ใช้ โอนย้าย หรือเปิดเผยข้อมูลส่วนบุคคลในนามตน รวมไปถึง หน่วยงานของรัฐ แต่ไม่รวมถึงบุคคล หรือหน่วยงานที่ปฏิบัติงานตามหน้าที่ที่ได้รับคำสั่งโดยบุคคลอื่นหรือหน่วยงานอื่น และ บุคคลธรรมดาที่เก็บรวบรวม มีไว้ในครอบครองหรือใช้ข้อมูลส่วนบุคคลในลักษณะเพื่อวัตถุประสงค์ส่วนตน ครอบครัว หรือเพื่องานภายในบ้าน

ข้อเปรียบเทียบ เรื่อง ผู้มีหน้าที่คุ้มครองสิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
SG PDPA 2012 (มาตรา 25)	“An organization shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals…”	หน่วยงาน หมายรวมถึง บุคคลธรรมดา บริษัท สมาคม หรือองค์กรธุรกิจทั้งที่จดทะเบียนหรือไม่จดทะเบียน ที่ไม่ว่าจะถูกจัดตั้งขึ้น หรือถูกยอมรับภายใต้กฎหมายสิงคโปร์ หรือเป็นผู้พักอาศัย หรือมีสถานที่ธุรกิจในประเทศสิงคโปร์

หมายเลข 3 : ข้อเปรียบเทียบ เรื่อง หน้าที่ในการลบทำลายหรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

หน้าที่ในการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (มาตรา 33) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม (มาตรา 37)	ตามมาตรา 33 จะต้องมีการร้องขอให้ดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้โดยเจ้าของข้อมูลส่วนบุคคลก่อน อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลก็มีหน้าที่ในการลบหรือทำลายข้อมูลส่วนบุคคลตามมาตรา 37 (3) อีกด้วย

หน้าที่ในการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
GDPR (มาตรา 17)	Art. 17 GDPR Right to erasure ('right to be forgotten') the controller shall have the obligation to erase personal data without undue delay	ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ลบข้อมูลส่วนบุคคลโดยไม่ชักช้า (ภายใต้หัวข้อสิทธิที่จะถูกลืม)
UK DPA 2018 (มาตรา 47)	"... (1)The controller must erase personal data without undue delay where..."	ผู้ควบคุมข้อมูลส่วนบุคคลต้องลบข้อมูลส่วนบุคคลโดยไม่ล่าช้า
AUS PA 1988 (APP 11.2)	"...the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is deidentified."	Entity (หรือ APP entity) ต้องดำเนินขั้นตอนที่เหมาะสมตามแต่ละกรณีเพื่อทำลายข้อมูลหรือทำให้มั่นใจว่าข้อมูลได้ถูกทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
HK PDPO 1996 (มาตรา 26 (1))	(1) A data user must take all practicable steps to erase personal data held by the data user..."	Data user ต้องทำการใด ๆ ที่ส่งผลในทางปฏิบัติ (All Practical Steps) เพื่อลบข้อมูลส่วนบุคคล

หน้าที่ในการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
PH PDA 2012 (มาตรา 16 (e))	The data subject is entitled to (e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information ; and	กำหนดให้สิทธิเจ้าของข้อมูลส่วนบุคคลมีสิทธิในการลบหรือ บล็อกข้อมูลส่วนบุคคลต่อผู้ควบคุมข้อมูลส่วนบุคคลได้ โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิในการขอให้หยุดชั่วคราว ถอน หรือสั่งให้มีการขัดขวาง ลบ หรือทำลายข้อมูลส่วนบุคคลของตนจากระบบการจัดเก็บไฟล์ของผู้ควบคุมข้อมูลส่วนบุคคลได้

หน้าที่ในการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
SG PDPA 2012 (มาตรา 25)	"An organization shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals..."	หน่วยงาน จำต้องยุติการเก็บรักษาเอกสารที่มีข้อมูลส่วนบุคคล หรือกำจัดวัตถุใด ๆ ที่มีข้อมูลส่วนบุคคล (ไม่ได้บัญญัติหน้าที่ในการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้โดยตรง แต่เป็นหน้าที่เกี่ยวกับข้อจำกัดในระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลเมื่อหมดความจำเป็น

หมายเลข 4 : ข้อเปรียบเทียบ เรื่อง การพิจารณาการหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล

ข้อเปรียบเทียบ เรื่อง การพิจารณาการหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 33 (1))	(1) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	การพิจารณาความจำเป็นจะต้องพิจารณาเป็นรายกรณี โดยไม่ได้มีการบัญญัติหลักเกณฑ์เอาไว้อย่างชัดเจน
GDPR (มาตรา 17 (1) (a))	“... (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed...”	ไม่มีความจำเป็น หรือหมดความจำเป็นต่อวัตถุประสงค์ของการเก็บรวบรวม หรือประมวลผลต่อข้อมูลส่วนบุคคลนั้น หมายถึงกรณีที่การเก็บและการประมวลผลข้อมูลส่วนบุคคลนั้นได้บรรลุวัตถุประสงค์แล้ว

ข้อเปรียบเทียบ เรื่อง การพิจารณาการหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
UK DPA 2018	บังคับใช้เช่นเดียวกัน GDPR	อาจพิจารณาได้ว่า “ไม่เกินกว่าที่จำเป็น” สามารถเป็นกรณีที่ “ไม่เกินกว่าระยะเวลาการเก็บข้อมูลที่จำเป็นที่กำหนดไว้” ได้ ดังที่ ICO ได้ระบุไว้ตามคำแนะนำในเรื่องข้อจำกัดในการเก็บที่กล่าวว่าผู้ควบคุมข้อมูลส่วนบุคคลอาจจัดให้มีนโยบายการเก็บรักษาข้อมูล (Retention Policy) พร้อมระบุระยะเวลาที่จะจัดเก็บ ดังนั้น เมื่อสิ้นระยะเวลานั้นแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลก็อาจพิจารณาลบหรือทำลายข้อมูลส่วนบุคคลนั้นได้

ข้อเปรียบเทียบ เรื่อง การพิจารณาการหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
TW PDPA 2015 (มาตรา 11 วรรคสาม)	"...When the specific purpose of data collection no longer exists..."	เมื่อการสิ้นสุดของระยะเวลาที่เกี่ยวข้องกับการเก็บรวบรวมข้อมูลนั้น ต้องดำเนินการลบหรือยุติการประมวลผลหรือใช้ข้อมูลส่วนบุคคลนั้น โดยกฎหมายไม่ได้ระบุว่าระยะเวลาดังกล่าวจะสิ้นสุดลงเมื่อใด แต่ให้ดำเนินการตามกฎหมายเฉพาะที่บังคับใช้กับของผู้ควบคุมข้อมูลส่วนบุคคลแต่ละประเภทธุรกิจ
HK PDPO 1996	"...where the data is no longer required for the purpose (including any directly related purpose) for which the data was used..."	เมื่อข้อมูลไม่จำเป็นต่อวัตถุประสงค์ (รวมไปถึงวัตถุประสงค์ที่เกี่ยวข้องโดยตรง) ที่ข้อมูลนั้นถูกใช้เพื่อวัตถุประสงค์นั้น

ข้อเปรียบเทียบ เรื่อง การพิจารณาการหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
JAP APPI 2020 (มาตรา 30)	"...and to delete the personal data without delay when such utilization has become unnecessary."	ลบข้อมูลส่วนบุคคลโดยไม่ล่าช้าเมื่อการใช้งานข้อมูลส่วนบุคคลหมดความจำเป็น
PH DPA 2012 (มาตรา 34 (e))	"... (c) The personal data is no longer necessary for the purposes for which they were collected..."	เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นต่อวัตถุประสงค์ในการเก็บรวบรวม

ข้อเปรียบเทียบ เรื่อง การพิจารณาการหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
SG PDPA 2012 (มาตรา 25 (a))	An organization shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that — (a) the purpose for which that personal data was collected is no longer being served by retention of the personal data	ให้หน่วยงานหยุดการเก็บรักษาข้อมูลเมื่อ “วัตถุประสงค์ในการเก็บรวบรวมข้อมูลนั้นหมดลง”

หมายเลข 5 : ข้อเปรียบเทียบ เรื่อง การลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

ข้อเปรียบเทียบ เรื่อง การลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง	คำอธิบาย
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้	กำหนดเป็นทางเลือกโดยให้เลือกทำการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
GDPR (มาตรา 17)	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies :	สิทธิที่เจ้าของข้อมูลส่วนบุคคลอาจร้องขอให้ผู้ให้บริการเครื่องมือสืบค้นข้อมูลทำการนำเอาลิงค์ที่ปรากฏข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลออกจากหน้าผลการสืบค้นข้อมูลเท่านั้น อย่างไรก็ตามสิทธิ Delisting ดังกล่าวยังไม่ทำให้ข้อมูลส่วนบุคคลถูกลบออกจากระบบออนไลน์แต่อย่างใด ข้อมูลส่วนบุคคลดังกล่าวอาจยังคง

ข้อเปรียบเทียบ เรื่อง การลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคล เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
		ปรากฏอยู่บนเว็บเพจที่เป็นของผู้เผยแพร่ข้อมูลส่วนบุคคลนั้นอยู่ เพื่อไม่ให้กระทบกระเทือนต่อประโยชน์ของผู้ใช้บริการอินเทอร์เน็ตบุคคลอื่นในการที่จะสามารถเข้าถึงข้อมูลต่าง ๆ ซึ่งถือเป็นสิทธิและเสรีภาพในการแสดงออกและเข้าถึงข้อมูลข่าวสาร (Right to Freedom of Expression and Information) และเป็นหนึ่งในสิทธิมนุษยชน กรณีดังกล่าว จึงทำให้เกิดความสมดุลระหว่างสิทธิ Delisting ซึ่งเป็นสิทธิส่วนบุคคล และสิทธิในการเข้าถึงข้อมูลข่าวสารของผู้ใช้บริการอินเทอร์เน็ตทั่วไปได้
UK DPA 2018 (มาตรา 32)	“... (1) The controller must erase personal data without undue delay...”	วิธีการในการลบนั้นอาจหมายรวมถึงการทำให้ข้อมูลอยู่เหนือการใช้งานได้

ข้อเปรียบเทียบ เรื่อง การลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
TW PDPA 2015 (มาตรา 11)	"...When the specific purpose of data collection no longer exists, or upon expiration of the relevant time period, the government or non-government agency shall, on its own initiative or upon the request of the data subject, erase or cease processing or using the personal data..."	ในไต้หวันไม่มีการจัดทำแนวปฏิบัติในเรื่องการลบ ทำลายข้อมูล อย่างไรก็ตาม ผู้ที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล ทั้งที่เป็นหน่วยงานของรัฐและที่ไม่ใช่หน่วยงานของรัฐต้องจัดทำนโยบายในการลบ ทำลาย เพื่อบังคับใช้ภายในองค์กรเอง
AUS PA 1988 (APPI ข้อ 11.2)	"... (a) an APP entity holds personal information...the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is deidentified."	บัญญัติให้ทางเลือกแก่ผู้ที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลว่าสามารถทำลายหรือทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (DeIdentified) ดังเช่นเดียวกับบทบัญญัติของประเทศไทย

ข้อเปรียบเทียบ เรื่อง การลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคล เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้		
กฎหมาย คุ้มครองข้อมูล ส่วนบุคคล	**เนื้อหาจากบทบัญญัติ ที่เกี่ยวข้อง**	**คำอธิบาย**
JP APPI 2020 (มาตรา 30)	“A principal may…demand of a personal information handling business operator a utilization cease or deletion …of the retained personal data…”	บัญญัติให้มีการลบ และอนุญาตให้มีการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนามได้
HK PDPO 1996 (Advisory Guidelines on Key Concepts in the Personal Data Protec-tion Act)	“ (1) A data user must take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose (including any directly related purpose) for which the data was used unless—…”	อาจเลือกดำเนินการลบ หรือการทำให้เป็นข้อมูลนิรนามก็ได้

ข้อเปรียบเทียบ เรื่อง การลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
PH DPA 2012 (มาตรา 34)	"The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system..."	ในมาตราที่บัญญัติเรื่องสิทธิในการลบและขัดขวาง (Right to Erasure or Blocking) บัญญัติให้สามารถทำการขอให้หยุดชั่วคราว ถอน หรือสั่งให้มีการขัดขวาง กำจัด หรือทำลาย
SG PDPA 2012 (มาตรา 25)	"An organization shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals..."	แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลระบุให้สามารถมีการทำให้ข้อมูลส่วนบุคคลเป็นนิรนามได้

หมายเลข 6 : ข้อเปรียบเทียบเกี่ยวกับข้อยกเว้นในการใช้สิทธิที่จะถูกลืม

ข้อเปรียบเทียบเกี่ยวกับข้อยกเว้นในการใช้สิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	(ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย	-
GDPR (มาตรา 17)	(e) การก่อตั้ง ใช้ และปกป้องสิทธิเรียกร้องทางกฎหมาย (หากการประมวลผลข้อมูลส่วนบุคคลเป็นไปเพื่อวัตถุประสงค์ในการก่อตั้ง ใช้ และปกป้องสิทธิเรียกร้องทางกฎหมาย จึงถือว่าเป็นข้อยกเว้นอย่างหนึ่งที่อนุญาตให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถประมวลผลข้อมูลอ่อนไหวต่อไปได้ แต่ต้องเป็นการประมวลผลข้อมูลอ่อนไหวที่เป็นไปตามเพื่อวัตถุประสงค์ดังกล่าวเท่านั้น ดังนั้น แม้เจ้าของ	ยกตัวอย่างเช่น ใน Recital 52 แห่ง GDPR ที่ได้กล่าวถึงข้อยกเว้นเรื่องข้อห้ามการประมวลผลข้อมูลอ่อนไหว (Special Categories on Personal Data) ไว้ว่า ข้อยกเว้นดังกล่าวควรต้องอนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลที่จำเป็นต่อการก่อตั้ง ใช้ และปกป้องสิทธิเรียกร้องตามกฎหมายได้ ไม่ว่าจะเป็นกระบวนการพิจารณาภายในศาลหรือกระบวนการ

ข้อเปรียบเทียบเกี่ยวกับข้อยกเว้นในการใช้สิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง	คำอธิบาย
	ข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไหวตามเงื่อนไขใน Recital 52 นี้แล้ว ผู้ควบคุมข้อมูลส่วนบุคคลก็สามารถอ้างข้อยกเว้นข้างต้นนี้เพื่อปฏิเสธการใช้สิทธิขอให้ลบข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลได้	ด้าน Administrative Procedure หรือกระบวนการภายนอกศาล (Out-of-Court Procedure)
UK DPA 2018	บังคับใช้ตาม GDPR	บังคับใช้ตาม GDPR
AUS PA 1988	"...When the specific purpose of data collection no longer exists, or upon expiration of the relevant time period, the government or non-government agency shall, on its own initiative or upon the request of the data subject, erase or cease processing or using the personal data..."	ในไต้หวันไม่มีการจัดทำแนวปฏิบัติในเรื่องการลบ ทำลายข้อมูล อย่างไรก็ตาม ผู้ที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลทั้งที่เป็นหน่วยงานของรัฐ และที่ไม่ใช่หน่วยงานของรัฐ ต้องจัดทำนโยบายในการลบ ทำลาย เพื่อบังคับใช้ภายในองค์กรเอง

ข้อเปรียบเทียบเกี่ยวกับข้อยกเว้นในการใช้สิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
JP APPI 2020	"...This, however, shall not apply in cases where a utilization cease etc. of the said retained personal data requires a large amount of expenses or other cases where it is difficult to fulfil a utilization cease etc. and when necessary alternative action is taken to protect a principal's rights and interests..." (มาตรา 30 (2))	เมื่อปรากฏว่าการใช้สิทธินั้นจำต้องใช้ค่าใช้จ่ายจำนวนมากในการลบข้อมูลส่วนบุคคลออก หรือเป็นการยากในการปฏิบัติการดังกล่าว แต่ต้องเป็นกรณีที่การปฏิบัติการตามทางเลือก (Alterative Actions) อื่น ๆ ได้ถูกนำมาปรับใช้เพื่อคุ้มครองสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
	"... (3) The provisions under the preceding two paragraphs shall not apply to those cases set forth in the following ... (i) cases based on laws and regulations..." (มาตรา 16 (3))	เป็นกรณีการใช้ข้อมูลส่วนบุคคล (Utilization) เพื่อวัตถุประสงค์ที่มีกฎหมายหรือระเบียบกำหนดให้ไม่จำต้องปฏิบัติตาม มาตรา 16 (1) และ (2) จึงทำให้ผู้ประกอบกิจการที่จัดการกับข้อมูลส่วนบุคคลนั้นสามารถปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลได้

ข้อเปรียบเทียบเกี่ยวกับข้อยกเว้นในการใช้สิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง	คำอธิบาย
	"... (ii) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent..." (มาตรา 16 (3))	เป็นกรณีการใช้ข้อมูลส่วนบุคคลที่จำต้องปกป้องชีวิต ร่างกาย ทรัพย์สิน เมื่อเป็นการยากที่จะขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้
	"... (iii) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent..."	เป็นกรณีการใช้ข้อมูลส่วนบุคคลที่จำเป็นพิเศษเพื่อการพัฒนาสุขอนามัยสาธารณะ หรือเพื่อสนับสนุนการเลี้ยงดูเด็กเล็กให้มีสุขภาพดี และเป็นการยากที่จะขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้
	"... (iv) cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws	เป็นกรณีการใช้ข้อมูลส่วนบุคคลที่จำเป็นเพื่อร่วมมือกับองค์กรรัฐบาลกลาง หรือท้องถิ่น หรือบุคคลที่มีอำนาจในการดำเนินการโดยกฎหมาย และการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคลอาจเป็นการกระทบต่อ

ข้อเปรียบเทียบเกี่ยวกับข้อยกเว้นในการใช้สิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
	and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs" (มาตรา 16 (3))	การดำเนินการตามหน้าที่ดังกล่าว
	"A period prescribed by cabinet order under Article 2, paragraph (7) of the Act shall be six months."	เมื่อข้อมูลส่วนบุคคลดังกล่าวจะถูกลบออกภายใน 6 เดือน หลังจากถูกเก็บรวบรวมอยู่แล้ว ดังนั้น เจ้าของข้อมูลส่วนบุคคลจึงไม่สามารถสั่งการให้มีการลบข้อมูลส่วนบุคคลของตนก่อนสิ้นสุดระยะเวลาดังกล่าวได้
TW PDPA 2015 (มาตรา 11 วรรคสาม)	"...the government or non-government agency shall, on its own initiative or upon the request of the data subject, erase or cease processing or using the personal data,	กรณีที่หน่วยงานของรัฐมีหน้าที่ต้องปฏิบัติหน้าที่ตามกฎหมาย เป็นข้อยกเว้นการใช้สิทธิในการลบทำลายข้อมูลได้

ข้อเปรียบเทียบเกี่ยวกับข้อยกเว้นในการใช้สิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง	คำอธิบาย
	unless the processing or use is either necessary for the performance of an official or business duty, or has been agreed to by the data subject in writing...” The “necessity for the performance of an official or business duty”...shall mean any of the following circumstances : 1. where a retention period is prescribed by laws or regulations, or agreed upon under a contract; 2. where there are sufficient reasons to believe that the deletion of the personal data will infringe upon the data subject’s interests that warrant protection; or	มาตรา 21 แห่งระเบียบข้อบังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ Enforcement Rules of the Personal Data Protection Act ได้ขยายความคำนิยามของคำว่า “ความจำเป็นต่อการปฏิบัติหน้าที่ราชการหรือทางธุรกิจ”

ข้อเปรียบเทียบเกี่ยวกับข้อยกเว้นในการใช้สิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
	3. where there are other legitimate reasons for not erasing the personal data.	
PH DPA 2012	"Rights of the Data Subject. – The data subject is entitled to... (e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system..."	ไม่ปรากฏเหตุในการปฏิเสธ

ข้อเปรียบเทียบเกี่ยวกับข้อยกเว้นในการใช้สิทธิที่จะถูกลืม		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**เนื้อหาจากบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
SG PDPA 2012	(1) A data user must take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose (including any directly related purpose) for which the data was used unless— (a) any such erasure is prohibited under any law; or (b) it is in the public interest (including historical interest) for the data not to be erased...	ไม่ปรากฏเหตุในการปฏิเสธ

หมายเลข 7 : ข้อเปรียบเทียบในการชั่งน้ำหนักเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลกับสิทธิในความเป็นส่วนตัว

ข้อเปรียบเทียบในการชั่งน้ำหนักเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลกับสิทธิในความเป็นส่วนตัว		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ความในวรรคหนึ่งมิให้นำมาใช้บังคับกับการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือ มาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย	รับรองการชั่งน้ำหนักเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลกับสิทธิในความเป็นส่วนตัว

ข้อเปรียบเทียบในการชั่งน้ำหนักเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลกับสิทธิในความเป็นส่วนตัว		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
GDPR	(a) การประมวลผลข้อมูลส่วนบุคคลจำเป็นต่อการใช้สิทธิในการแสดงออกและเข้าถึงข้อมูลข่าวสาร (Right of Freedom of Expression and Information)	ต้องปรากฏว่าการประมวลผลข้อมูลส่วนบุคคลเป็นประโยชน์ต่อสิทธิในการแสดงออก และเข้าถึงข้อมูลข่าวสารของสาธารณะมากกว่าสิทธิในการลบข้อมูลส่วนบุคคลของเจ้าของข้อมูล
UK DPA 2018	บังคับใช้เช่นเดียวกับ GDPR	บังคับใช้เช่นเดียวกับ GDPR
AUS PA 1988	ไม่ปรากฏเรื่องการชั่งน้ำหนักในกฎหมาย	-
JP APPI 2020	ไม่ปรากฏเรื่องการชั่งน้ำหนักในกฎหมาย	แต่มีการชั่งน้ำหนักในทางปฏิบัติ ศาลฎีกาของประเทศญี่ปุ่นได้วินิจฉัยใน ค.ศ. 2017 ว่า “ความชอบด้วยกฎหมาย” ของการแสดงผลข้อมูลนั้นจะต้องพิจารณาจากการชั่งน้ำหนักระหว่างประโยชน์ทางกฎหมาย (Legal Interest) ของการที่

ข้อเปรียบเทียบในการชั่งน้ำหนักเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลกับสิทธิในความเป็นส่วนตัว		
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	**ถ้อยคำตามบทบัญญัติที่เกี่ยวข้อง**	**คำอธิบาย**
		ข้อมูลส่วนบุคคลจะไม่ถูกเผยแพร่ และสถานการณ์อื่น ๆ ที่เกี่ยวกับการแสดง URL จากการค้นหา ในคดีนี้ศาลเห็นว่าประโยชน์ทางกฎหมายของการไม่แสดงผลข้อมูลนั้นมีน้ำหนักมากกว่าประโยชน์ทางกฎหมายของการแสดงผลข้อมูล ดังนั้นเจ้าของข้อมูลส่วนบุคคลจึงมีสิทธิเรียกร้องให้ผู้ประกอบธุรกิจลบ URL และรายการอื่น ๆ จากผลการค้นหา
TW PDPA 2015	ไม่ปรากฏเรื่องการชั่งน้ำหนักในกฎหมาย	-
PH DPA 2012	ไม่ปรากฏเรื่องการชั่งน้ำหนักในกฎหมาย	-
SG PDPA 2012	ไม่ปรากฏเรื่องการชั่งน้ำหนักในกฎหมาย	-

บรรณานุกรม

กฎหมาย

Act on Protection of Personal Information (revised 2020) (Japan) [https ://www.ppc.go.jp/ files/pdf/APPI_english.pdf]

Archives Act 1983 (Australia) [https ://www.legislation.gov.au/ Details/C2016C00772]

Constitution of Japan [https ://japan.kantei.go.jp/ constitution_ and_government_of _japan/ constitution_e.html]

Constitution of the Republic of China (Taiwan) [https ://law.moj. gov.tw/ENG/LawClass/ LawAll.aspx?pcode=A0000001]

Data Privacy Act 2012 (DPA) : RA No. 10173) (Philippines) [https ://www.privacy.gov.ph/data-privacy-act/]

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 [https ://eur-lex.europa.eu/ legal-content/EN/TXT/HTML/?uri=CELEX :32015L1535& from=EN]

Enforcement Rules of the Personal Data Protection Act 2016 (Taiwan) [https ://law. moj.gov.tw/ENG/LawClass/LawAll. aspx?pcode=I0050022]

EU Charter of Fundamental Rights [https ://eur-lex.europa.eu/legal-content/EN/TXT/HTML /?uri=CELEX :12012P/TXT&from=EN]

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [https ://eur-lex.europa.eu/legal-content/EN/TXT/ HTML/?uri=CELEX :31995L0046&from=EN]

EU General Data Protection Regulation (GDPR) [https ://eur-lex.europa.eu/legal-content/ EN/TXT/HTML/?uri=CELEX :32016R0679&from=EN]

Implementing Rules and Regulations of the Data Privacy Act of 2012 (Philippines) [https ://www.privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/]

Personal Data (Privacy) Ordinance (Cap. 486) (Hong Kong) [https ://www.elegislation. gov.hk/hk/cap486]

Personal Data Protection Act 2012 (Singapore) [https ://sso.agc. gov.sg/Act/PDPA2012]

Personal Data Protection Act 2015 (Taiwan) [https ://law.moj. gov.tw/ENG/LawClass/LawAll.

spx?pcode=I0050021# :~ :text=The%20Personal%20Data%20Protection%20Act,proper%20use%20of%20personal%20data.&text=%22data%20subject%22%20refers%20to%20an,is%20collected%2C%20processed%20or%20used.]

Rehabilitation of Offenders Act 1974 (UK) [https ://www.legislation.gov.uk/ukpga/1974/53]

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 [https ://www.krisdika.go.th/librarian/ get?sysid=302231&ext=htm]

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [https ://www.krisdika.go.th/librarian/ get?sysid=834296&ext=htm]

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 [https ://www.krisdika.go.th/librarian/ get?sysid=774606&ext=htm]

ปฏิญญา

Universal Declaration of Human Rights [https ://www.un.org/sites/un2.un.org/files/udhr. pdf]

คำวินิจฉัยของศาล

Hurbain v. Belgium – 57292/16 (European Court of Human Rights) June 2021 [https ://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-13318%22]}]

Judgment of the Court C-131/12 (CJEU) [https ://curia.europa.eu/juris/document/ document.jsf;jsessionid=0536322C65BBCB9D3FF36B8118F4C272?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=53081]

Judgment of the Court C-507/17 (CJEU) [https ://curia.europa.eu/juris/document/ document.jsf?text=&docid=218105&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=53228]

Judgment of the Court Case C-398/15 (CJEU) [https ://curia.europa.eu/juris/document/ document.jsf?docid=188750&doclang=EN]

Saitama District Court, Decision of 25 June 2015 (Japan) [http ://blog.renforce.eu/ index.php/en/2017/02/07/a-right-to-be-forgotten-case-before-the-japanese-supreme-court/]

Segerstedt-Wiberg and Others v. Sweden (application no. 62332/00) [file :///C :/Users/ admin/Downloads/003-1688388-1769677%20 (2).pdf]

Supreme Administrative Court 106 Pan Zi No. 54 (Taiwan) [https ://cons.judicial.gov.tw/jcc/ Uploads/files/%E7%AC%AC%E4%B8%89%E5%A0%B4%E7%A0%94%E8%A8%8E%E6%9C%83%E8%88%87%E8%AB%87%E4%BA%BA%E9%82%B1%E6%96%87%E8%81%B0%E5%89%AF%E7%A0%94%E7%A9%B6%E5%93%A1.pdf]

Taiwan High Court 102 Shang Zi No. 915 (Civil Division) (Taiwan) [https ://cons.judicial.gov. tw/jcc/Uploads/files/%E7%AC%AC%E4%B8%89%E5%A0%B4%E7%A0%94%E8%A8%8E%E6%9C%83%E8%88%87%E8%AB%87%E4%BA%BA%E9%82%B1%E6%96%87%E8%81%B0%E5%89%AF%E7%A0%94%E7%A9%B6%E5%93%A1.pdf]

Taiwan High Court 104 Shang Zi No. 389 (Civil Division) (Taiwan) [https ://cons.judicial.gov. tw/jcc/Uploads/files/%E7%AC%AC%E4%B8%89%E5%A0%B4%E7%A0%94%E8%A8%8E%E6%9C%83%E8%88%87%E8%AB%87%E4%BA%BA%E9%82%B1%E6%96%87%E8%81%B0%E5%89%AF%E7%A0%94%E7%A9%B6%E5%93%A1.pdf]

Taoyuan District Court 104 Su Zi No. 985 (Civil Division) (Taiwan) [https ://cons.judicial.gov. tw/jcc/Uploads/files/%E7%AC%AC%E4%B8%89%E5%A0%B4%E7%A0%94%E8%A8%8E%E6%9C%83%E8%88%87%E8%AB%87%E4%BA%BA%E9%82%B1%E6%96%87%E8%81%B0%E5%89%AF%E7%A0%94%E7%A9%B6%E5%93%A1.pdf]

U.S. Department of Justice v. Reporters Committee [https :// supreme.justia.com/cases/ federal/us/489/749/]

คำพิพากษาศาลฎีกาที่ 4893/2558 [https ://deka.in.th/view-585752. html]

คำแปลกฎหมาย

นคร เสรีรักษ์ ณรงค์ ใจหาญ ประสิทธิ์ ปิวาวัฒนพานิช ศุภเกียรติ ศุภศักดิ์-ศึกษากร และนิชานันท์ นันทศิริศรณ์, GDPR ฉบับภาษาไทย (บริษัท พี.เพรส จำกัด, ธันวาคม 2562)

แนวปฏิบัติและเอกสารอื่น

Advisory Guidelines on Key Concepts in the PDPA (Singapore) [https ://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Oct-2021.pdf?la=en]

Australian Privacy Principle (Chapter 11) [https ://www.oaic.gov.au/__data/assets/pdf_file/ 0018/1287/app-guidelines-chapter-11-v1.2.pdf]

Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines case under the GDPR [https ://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf]

Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (GDPR) [https ://ec.europa.eu/newsroom/article29/items/611237]

ICO Guide to the General Data Protection Regulation (GDPR) [https ://ico.org.uk/media/ for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf]

Statement of the Council’s reasons : Position (EU) No 6/2016 (2016/c 159/02) [https ://op. europa.eu/en/publication-detail/-/publication/8263b3d6-10f6-11e6-ba9a-01aa75ed71a1]

บทความ

Adian Forde, ‘Implication of the Right to Be Forgotten’ (2015) Tulane Journal of Technology and Intellectual Property 18 83

Alexandra Rengel, ‘Privacy as an International Human Right and the Right to Obscurity in Cyberspace’ (2014) Groningen Journal of International Law 2 (2) 33

Anita L. Allen, ‘Privacy-as-Data Control : Conceptual, Practical, and Moral Limits of the Paradigm’ (2000) Connecticut Law Review 32 861

Antoon De Baets, ‘A historian’s view on the right to be forgotten’ (2016) International Review of Law, Computers & Technology 30 (1) 57

Christopher Kotfila, ‘This Message Will Self-Destruct : The Growing Role ofObscurity and Self-Destructing Data in Digital Communication’ (2014) Bulletin of the Association for Information Science and Technology 40 (2) 12

David Erdos, ‘The ‘right to be forgotten’ beyond the EU : an analysis of wider G20 regulatory action and potential next steps’ (2021) Journal of Media Law 13 (1) 1

David J. Stute, ‘Privacy Almighty? The CJEU’s Judgment in Google Spain SL v. AEPD’ (2015) Michigan Journal of International Law 36 (4) 649

Edward J. Eberle, 'The Method and Role of Comparative Law' (2009) Washington University Global Studies Law Review 8 (3) 451, 452.

Frederike Zufall, 'Challenging the EU's 'Right to Be Forgotten'? Society's 'Right to Know' in Japan' (2019) EDPL 1 17

Hunter Criscione, 'Forgetting the Right to Be Forgotten : The Everlasting Negative Implications of a Right to Be Deferrenced on Global Freedom in the Wake of Google v. CNIL' (2020) Pace International Law Review 32 (2) 315

Jed Rubemfeld, 'The Right of Privacy' (1989) Harvard Law Review 102 (4) 737

Jongwon Lee, 'What the Right to be Forgotten Means to Companies : Threat or Opportunities?' (2016) Procedia Computer Science 91 542

Kamrul Faisal, 'Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions' (2021) Security Privacy 4

Maja Ovcak Kos, 'The Right to be Forgotten and the Media' (2019) LeXonomica 11 (2) 195

Marko Milosavljevic, Melita Poler, and Rok Ceferin, 'In the Name of the Right to be Forgotten : New Legal and Policy Issues and Practices regarding Unpublishing Requests in Slovenian Online News Media' (2020) Digital Journalism 8 (6) 780

Michael J. Kelly and David Satola, 'The Right to be Forgotten' (2017) University of Illinois Law Review 1

Patrick C. File, 'A History of Practical Obscurity : Clarifying and Contemplating the Twentieth Century Roots of a Digital Age : Concept of Privacy' (2017) UB Journal of Media Law & Ethics 6 (1/2) 1

Rolf H. Weber, 'The Right to Be Forgotten More Than a Pandora's Box?' (2011) Journal of Intellectual Property, Information Technology and E-Commerce 2 (2) 120

Shaniqua Singleton, 'Balancing Right to Be Forgotten with A Right to Freedom of Expression in the Wake of Google vs AEPD' (2015) Georgia Journal of International and Comparative Law (44) 165

Woodrow Hartzog and Evan Selinger, 'Surveillance as Loss of Obscurity' (2015) Washington and Law Law Review 72 (3) 1343

ยุกต์กฤต กัณฑมณี, "การคุ้มครองสิทธิที่จะถูกลืม" (2019) สุทธิปริทัศน์ 33 (108) 14

หนังสือ

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)

Ralf Michaels, “The Functional Method of Comparative Law,” in The Oxford Handbook of Comparative Law eds. Mathias Reimann and Reinhard Zimmermann (New York : Oxford University Press, 2006)

Robert Walters and Marko Novak, Cyber Security, Artificial Intelligence, Data Protection and the Law (Springer Nature Singapore, 2021)

แหล่งข้อมูลอิเล็กทรอนิกส์

Article 19, ‘The “Right to be Forgotten” : Remembering Freedom of Expression’ (Article 19, 2016) <https ://www.article19. org/data/files/The_right_to_be_forgotten_A5_EHH _HYPERลิงค์. pdf> accessed 5 August 2021

Article 29 Data Protection Working Party, ‘Guidelines on the Implementation of the Court of Justice of the European Union Judgment on “Google Spain and Inc v. Agencia Espanola De Proteccion De Datos (AEPD) and Mario Costeja Gonzalez C-131/12’ (Article 29 Data Protection Working Party, November 2014) <file :///C :/Users/User/Downloads/wp225_en_ 6F61B70D-A130-F778-619246F5CE8DE165_64437. pdf> accessed 5 August 2021

Cécile de Terwangne, ‘The Right to be Forgotten and the Informational Autonomy in the Digital Environment’ (EU Commission, 2013) <file :///C :/Users/admin/ Downloads/jrc 86750_cecile_fv.pdf> accessed 2 October 2021

Charamaine Koo and Eliza Siew, 'Territorial limitation of data protection law and the "right to be forgotten" in Hong Kong - A landmark decision by the Administrative Appeals Board' (Deacons, February 2021) <https ://www.deacons.com/news-and-insights/publications/ territorial-limitation-of-data-protection-law-and-the-"right-to-be-forgotten". html> accessed 6 August 2021.

Courts in Japan, '2016 (Kyo) 45' (Courts in Japan, January 2017) <https ://www.courts. go.jp/app/hanrei_en/detail?id=1511> accessed 4 October 2021

Global Freedom of Expression, 'Google LLC v. National Commission on Informatics and Liberty (CNIL)' (Columbia University, September 2019) <https ://globalfreedomof expression. columbia.edu/cases/google-llc-v-national-commission-on-informatics-and-liberty-cnil/> accessed 3 October 2021

Global Freedom of Expression, 'NT1 and NT2 v. Google LLC' (Columbia University, April 2018) <https ://globalfreedomof expression.columbia.edu/cases/nt1-nt2-v-google-llc/> accessed 3 October 2021

Global Freedom of Expression, 'Plaintiff X v. PrimaDaNoi' (Columbia University, 2015) <https ://globalfreedomofexpression. columbia.edu/cases/plaintiff-x-v-primadanoi/> accessed 1 October 2021

ICO, 'An Overview of Data Protection Act 2018, Part 2, Data Protection Act – General processing' (ICO, 2018) <https ://ico.org.uk/ media/for-organisations/documents/2614158/ico-introduction-to-the-data-protection-bill.pdf> accessed 3 October 2021

ICO, 'Deleting personal data' (ICO, February 2014) <https ://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf> accessed 3 October 2021

Jeffrey Rosen, 'The Right to Be Forgotten' (Standford Law Review (Online) 2012) <https ://www.Stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/> accessed 30 September 2021

KOD Lyons, 'Strengthening the Right to be Forgotten : The Implications of Hurbain v. Belgium' (KOD Lyons, 2021) <https :// kodlyons.ie/strengthening-the-right-to-be-forgotten-the-implications-of-hurbain-v-belgium/> accessed 2 October 2021

LawPhil, 'Vivares v. St. Theresa's College GR No. 202666' (LawPhil, September 2014) <https ://lawphil.net/judjuris/juri2014/sep2014/gr_202666_2014.html#fnt3> accessed 4 October 2021

Melanie Dulong de Rosnay and Andres Guadamuz, 'Memory Hole or Right to Delist? Implications of the Right to be Forgotten for Web Archiving' (RESET, 19 April 2019) <file :///F :/reset-807.pdf> accessed 2 October 2021

OAIC, 'Uber found to have interfered with privacy' (OAIC, July 2021) <https ://www.oaic. gov.au/updates/news-and-media/uber-found-to-have-interfered-with-privacy/> accessed 3 October 2021.

Parliament of Australia, 'Do Australians have a legal right to privacy?' (Department of Parliamentary Services, March 2005) <https ://parlinfo.aph.gov.au/parlInfo/ download/ library/prspub/CBHF6/upload_binary/cbhf64.pdf;fileType=application%2Fpdf#search=%22library/prspub/CBHF6%22> accessed 3 October 2021

PCPD, 'Guidance on Personal Data Erasure and Anonymization' (PCPD, April 2014) <https :// www.pcpd.org.hk/english/publications/files/erasure_e.pdf> accessed 4 October 2021

Privacy Commission, 'Examples' (Privacy Commission, 2021) <https ://www.privacy.gov. ph/know-your-rights/> accessed 4 October 2021.

Stephen Wong (Privacy Commissioner for Personal Data), 'Recent Developments of Hong Kong Personal Data Privacy Protection' (PCPD) <https ://www.pcpd.org.hk/english/news_ events/whatison/files/PCPD_AmCham_9Dec2015.pdf> accessed 6 August 2021

Wen-Tsong Chiou, 'Commentary on The Right to be Forgotten : Forget about It? (Cons Judicial, July 2015) <https ://cons.judicial. gov.tw/jcc/Uploads/files.pdf> accessed 5 August 2021.

อรรถกร สุขปุณพันธ์, “สิทธิที่จะถูกกลืม (Right to be forgotten) : จากคำวินิจนิจฉัยสู่มิติใหม่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป” (Krisdika) <https ://www.krisdika.go.th/data/activity/act352.pdf> สืบค้นเมื่อ 6 ตุลาคม 2564