# ภาระรับผิดทางกฎหมายของตัวกลาง ตามระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป
# Intermediary liability under General Data Protection Regulation

**Received: 12 มกราคม 2563**
**Revised: 8 มีนาคม 2563**
**Accepted: 10 มีนาคม 2563**

ผู้ช่วยศาสตราจารย์ ดร. อรอมล อาระพล*
Assistant Professor Dr. Ornamol Arapol **

## บทคัดย่อ

ระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป หรือ General Data Protection Regulation: GDPR ได้กำหนดหลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นสิทธิมนุษยชนขั้นพื้นฐานของประชาชน ทุกคน หนึ่งในหลักการสำคัญคือการให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการที่จะแก้ไขข้อมูลให้มีความทันสมัยและเป็นปัจจุบัน หรือการลบหรือการนำข้อมูลออกจากระบบ หากข้อมูลนั้นอาจเป็นการก่อให้เกิดความเสียหายหรือกระทบต่อชื่อเสียงของเจ้าของข้อมูลส่วนบุคคลนั้น ซึ่ง GDPR กำหนดให้เป็นภาระของตัวกลาง หรือผู้ให้บริการเว็บไซต์ที่จะต้องมีภาระในการดำเนินการ แก้ไข เปลี่ยนแปลง หรือนำข้อมูลส่วนบุคคลออกจากเว็บไซต์ของตนตามหลักการในเรื่องสิทธิที่จะถูกลืม มิเช่นนั้นจะถือว่าไม่กระทำตามข้อกำหนดภายใต้ GDPR และจะต้องมีความรับผิดตามกฎหมาย

**คำสำคัญ:** ความรับผิดตัวกลาง, คุ้มครองข้อมูลส่วนบุคคล, สหภาพยุโรป

## Abstract

General Data Protection Regulation has imposed a principle to protect personal data which is the fundamental right of a human. One of the basic principles is to allow owner of personal data to correct, update or remove their data from the website, especially data that may cause defamation of the owner. GDPR imposes the obligation to online service providers to process in correcting or removing personal data out of their websites under the Right to be forgotten principle.

**Keywords:** Intermediary Liability, Data Protection, European Union

* รองคณบดีฝ่ายบริหาร คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย Ornamol@gmail.co

** Associate Dean of Administrative Affair, School of Law, The University of the Thai Chamber of Commerce. ornamol@gmail.com

## 1. บทนำ

ในปัจจุบัน Online Service Provider (OSP) หรือ ผู้ให้บริการเว็บไซต์ออนไลน์บนอินเทอร์เนต มีบทบาทมากขึ้นในการเสนอบริการในรูปแบบที่หลากหลาย จากแต่เดิมที่เคยเป็นลักษณะของการให้บริการเพียงการให้บริการที่อนุญาตให้ผู้ใช้บริการสามารถนำเว็บเพจของตนเองเพื่อออนไลน์บนอินเตอร์เน็ต (web hosting)[1] และอาจมีการนำรูปภาพเพียงเล็กน้อยขึ้นออนไลน์บนอินเทอร์เนต ส่งผลให้ในขณะนั้น OSP จึงยังไม่ถูกมุ่งประเด็นในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลมากนัก แต่ในปัจจุบันการเสนอรูปแบบของการให้บริการของ OSP มีรูปแบบที่หลากหลายมากยิ่งขึ้นในการที่จะให้ผู้ใช้บริการสามารถนำข้อมูลของตนเองขึ้นสู่โลกออนไลน์ OSP หลายรายได้พัฒนารูปแบบธุรกิจของตนเองเพื่อตอบสนองความต้องการของผู้บริโภคในหลายๆรูปแบบ เช่น การให้บริการโปรแกรมค้นหา (Google, Yahoo) การให้บริการแพลตฟอร์มเพื่อการติดต่อสื่อสาร (Facebook, Twitter) การให้บริการการจัดเก็บข้อมูลบนระบบคลาวน์ (Dropbox, Google Drive) การทำพาณิชยกรรมอิเล็กทรอนิกส์ (e-Bay, Amazon) การชำระเงินทางอินเทอร์เนต (Paypal) ซึ่งการให้บริการในรูปแบบที่มีความทันสมัยเหล่านี้ล้วนแล้วแต่เป็นการขับเคลื่อนธุรกิจโดยใช้ข้อมูลเป็นหลัก ซึ่งเจ้าของข้อมูล (Data Subject) เป็นผู้ใช้บริการของ OSP โดยระบบปฏิบัติงานของผู้ให้บริการจะทำการประมวลผลข้อมูลต่างๆของเจ้าของข้อมูล กรณีนี้จึงควรพิจารณาถึงขอบเขตการให้บริการของ OSP และอำนาจในการประมวลผลข้อมูลส่วนบุคคลของ OSP ว่ามีขอบเขตเพียงใด หรือการกระทำในลักษณะใดของ OSP ในการประมวลผลข้อมูลส่วนบุคคลของผู้ใช้บริการที่เป็นเจ้าของข้อมูลส่วนบุคคลจะต้องมีความรับผิดตามกฎหมาย[2] โดยเฉพาะอย่างยิ่งภายใต้กฎหมายฉบับใหม่ของสหภาพยุโรป General Data Protection Regulation : GDPR ที่มีผลใช้บังคับ โดยมีหลักการพื้นฐานที่ต้องการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิมนุษยชนขั้นพื้นฐานของประชาชนชาวยุโรปและทั่วโลก ซึ่งถ้าหากผู้ให้บริการ OSP ได้ดำเนินการในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ก็จะต้องมีภาระในการปฏิบัติการประมวลผลข้อมูลของเจ้าของข้อมูลส่วนบุคคลภายใต้หลักการของบทบัญญัติ GDPR

---

[1] เว็บโฮสติ้ง (Web Hosting) คืออะไร, https://www.ic-myhost.com/web-hosting-articles/web-hosting-%E0%B8%84%E0%B8%B7%E0%B8%AD.html. (เข้าถึงเมื่อ 11 มกราคม 2563).

[2] Giovanni De Gregorio, European University Institute Working Papers. The E-Commerce Directive and GDPR Convergence of Legal Regimes in the Algorithmic Society?. https://cadmus.eui.eu/bitstream/handle/1814/63044/RSCAS%202019_36.pdf?sequence=1&isAllowed=y. (last visited 11 January 11, 2020).

## 2. เนื้อหา

### 2.1 General Data Protection Regulation (GDPR): หลักการทั่วไป

สหภาพยุโรปได้ออกกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เรียกว่าระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป (General Data Protection Regulation : GDPR) ซึ่งนำมาใช้แทน แนวปฏิบัติคุ้มครองข้อมูล (Data Protection Directive) 95/46/EC มีวัตถุประสงค์เพื่อคุ้มครองสิทธิขั้นพื้นฐานของมนุษย์ในการที่จะรักษาความเป็นส่วนตัวในข้อมูลของตนเอง ในขณะเดียวกันก็สนับสนุนให้มีการเคลื่อนย้ายข้อมูลภายในประเทศสมาชิกสหภาพยุโรปได้อย่างอิสระเพื่อวัตถุประสงค์ในการขับเคลื่อนเศรษฐกิจในสหภาพยุโรปให้เป็นตลาดการค้าตลาดเดียวกันทั้งภูมิภาคตามนโยบาย Digital Single Market โดยการกำหนดเงื่อนไขต่างๆ ให้ผู้ประกอบการและภาคส่วนต่างๆ ต้องปฏิบัติตาม โดย GDPR จะมีสถานะเป็นกฎหมายฉบับเดียวที่ประเทศสมาชิกสหภาพยุโรปจะต้องปฏิบัติตามโดยปราศจากข้อขัดแย้งในเรื่องระบบกฎหมายภายในประเทศสมาชิกที่มีความแตกต่างกัน หรือภาระทางด้านการดำเนินการเพื่อให้เป็นไปตามกฎหมาย GDPR ซึ่งมีผลบังคับใช้แก่ประเทศสมาชิกเมื่อวันที่ 26 พฤษภาคม 2516 และบังคับใช้ในทางปฏิบัติเมื่อวันที่ 28 พฤษภาคม 2018[3] โดยกฎหมายฉบับใหม่นี้ส่งผลกระทบต่อ OSP ทั้งที่มีสาขาอยู่ในประเทศสมาชิกสหภาพยุโรปและที่มีสาขาอยู่นอกประเทศที่เป็นสมาชิกสหภาพยุโรปแต่ได้มีการเก็บรวบรวมข้อมูลของประชากรชาวยุโรปมาประมวลผล ในการที่จะต้องมีภาระในการปฏิบัติตามกฎหมายฉบับนี้ที่จะต้องแจ้งให้แก่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงวัตถุประสงค์ของการจัดเก็บ และนำข้อมูลส่วนบุคคลไปใช้ภายใต้วัตถุประสงค์ อีกทั้งต้องสร้างระบบของการให้ความยินยอม และมีภาระในการจัดหาบุคลากรมาทำหน้าที่ตามกฎหมายในฐานะ data protection officer (DPO)[4] หากผู้ที่มีส่วนเกี่ยวข้องไม่ปฏิบัติตามกฎหมายฉบับนี้จะต้องรับบทลงโทษที่ร้ายแรง โดยคิดเป็นค่าปรับจำนวนร้อยละ 4 ของผลประกอบการทั่วโลกในปีนั้นๆหรือเป็นจำนวนเงิน 20 ล้านยูโร[5]

---

[3] European Commission, Data Protection in the EU. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en#fundamental-rights. Last visited 11 January 11, 2020.

[4] Data Protection Officer หรือเจ้าหน้าที่คุ้มครองข้อมูลประจำองค์กร ทำหน้าที่ในการบริหารจัดการการประมวลผลข้อมูลของพนักงานประจำองค์กร ข้อมูลลูกค้า ผู้ให้บริการ หรือปัจเจกชนใดที่มีสถานะเป็นเจ้าของข้อมูลส่วนบุคคลให้เป็นไปตามหลักการของการคุ้มครองข้อมูลส่วนบุคคล ซึ่ง GDPR ได้กำหนดให้องค์กรตามที่กฎหมายกำหนด จะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลประจำองค์กร ที่มา Data Protection Officer (DPO) https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

[5] Daphne Keller, “The Right Tools: Europe’s Intermediary Liability Laws and the EU 2016 General Data Protection”. Berkeley Technology Law Journal Vol.33:287. (2018). 318. https://btlj.org/data/articles2018/vol33/33_1/Keller_Web.pdf. Last visited 11 January 11, 2020.

หลักการต่างๆใน GDPR ประกอบด้วยหลักการพื้นฐานในเรื่องสิทธิความเป็นส่วนตัวของมนุษย์ในการรักษาไว้ซึ่งข้อมูลส่วนบุคคล ซึ่งประกอบด้วย

1) การกำหนดว่าข้อมูลประเภทไหนที่ผู้ประเมินผลข้อมูลสามารถที่จะนำไปประมวลผลได้เพื่อให้เป็นไปตามวัตถุประสงค์ที่ได้แจ้งแก่เจ้าของข้อมูล และการประมวลผลข้อมูลจะต้องมีความโปร่งใส

2) การแจ้งวัตถุประสงค์ของการนำข้อมูลไปประมวลผลต่อเจ้าของข้อมูลและจะต้องใช้ข้อมูลตามวัตถุประสงค์ที่ได้แจ้งไว้เท่านั้น โดยจะต้องได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูล

3) การกำหนดให้มีภาระในการคุ้มครองข้อมูลของเจ้าของข้อมูลไม่ให้มีการรั่วไหล เสียหายหรือสูญหายของข้อมูล ประกอบด้วยกระบวนการในประประมวลผลข้อมูลที่มีความปลอดภัยและมีมาตรการทางเทคนิคที่มีความเหมาะสม การป้องกันการเข้าถึงข้อมูลจากผู้ที่ไม่มีอำนาจ

4) การกำหนดปริมาณของข้อมูลที่รวบรวมจากปัจเจกบุคคลที่สามารถนำไปประมวลผลได้โดยจะต้องเป็นไปตามวัตถุประสงค์ที่ได้แจ้งแก่เจ้าของข้อมูลไว้

5) ระยะเวลาในการเก็บข้อมูลให้เป็นไปเท่าที่มีความจำเป็นที่จะต้องใช้ข้อมูลในการประมวลผลข้อมูลนั้นและเป็นไปตามวัตถุประสงค์ที่ได้แจ้งแก่เจ้าของข้อมูลไว้

6) การแก้ไขข้อมูลให้มีความทันสมัยและเป็นปัจจุบัน หรือการลบหรือการนำข้อมูลออกจากระบบหรือการแก้ไขข้อมูลให้ถูกต้อง ภายใต้เงื่อนไขที่กำหนดตามกฎหมายฉบับนี้[6]

**2.2 การกำหนดสถานะทางกฎหมายของตัวกลาง หรือ ผู้ให้บริการ OSP ภายใต้ GDPR**

ความหมายของคำว่าตัวกลาง (intermediary) จะอาศัยหลักการตามที่ปรากฏใน E-Commerce Directive 2000/31/EC ซึ่งได้นิยามความหมายของตัวกลางว่าเป็นตัวกลางระหว่างเจ้าของสิทธิกับบุคคลที่สามหรือกล่าวอีกนัยหนึ่งตัวกลางจะทำหน้าที่ในการเข้าถึงเนื้อหาหรือข้อมูลในอินเทอร์เนต ตัวกลางจะถูกนิยามว่าเป็นผู้ให้บริการในการจัดการ แก้ไข โฆษณา ตรวจสอบ เนื้อหาที่จะถูกบรรจุขึ้นหรือถูกส่งผ่านโดยบริการของตัวกลาง[7] โดยหลักการในเรื่องความรับผิดตัวกลางต้องการที่จะจำกัดความรับผิดของ Online Service Provider (OSP) ซึ่งได้แก่ ผู้ให้บริการ web hosting เช่นเว็บไซต์ที่ให้บริการเครือข่ายสังคมต่างๆที่รวบรวมข้อมูลของผู้ใช้บริการไว้เป็นจำนวนมาก[8] การให้บริการโปรแกรมค้นหา (Google, Yahoo) การให้บริการแพลตฟอร์มเพื่อการติดต่อสื่อสาร (Facebook, Twitter) การ

---

[6] Guide to the General Data Protection Regulation (GDPR)The principles. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ last visited 11 January 11, 2020.

[7] Antti Lankinen, Intermediary Liability for Copyright Infringements: Striking a Fair Balance the Right to Intellectual Property and Other Fundamental Rights of the Charter of Fundamental Rights of the European Union, (Master of Laws, School of Law, Orebro Universitet), http://www.diva-portal.org/smash/get/diva2:1233315/FULLTEXT01.pdf. last visited 11 January 11, 2020.

[8] Ibid. p.17.

ให้บริการการจัดเก็บข้อมูลบนระบบคลาวน์ (Dropbox, Google Drive) การทำพาณิชยกรรมอิเล็กทรอนิกส์ (e-Bay, Amazon) การชำระเงินทางอินเทอร์เนต (Paypal) เป็นต้น[9]

การกำหนดความรับผิดตามกฎหมายของตัวกลางปรากฏอยู่ใน E-Commerce Directive[10] ของสหภาพยุโรป โดยได้จำกัดความรับผิดของตัวกลาง ซึ่งประกอบด้วยผู้ให้บริการเคเบิ้ล ผู้ให้บริการการ

---

[9] Giovanni De Gregorio, European University Institute Working Papers. The E-Commerce Directive and GDPR Convergence of Legal Regimes in the Algorithmic Society?. https://cadmus.eui.eu/bitstream/handle/1814/63044/RSCAS%202019_36.pdf?sequence=1&isAllowed=y.

last visited 11 January 11, 2020.

[10] Article 12 of DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

"Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; and

(c) does not select or modify the information contained in the transmission.

Article 13 of DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

"Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

(a) the provider does not modify the information;

(b) the provider complies with conditions on access to the information;

(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

เข้าถึงอินเทอร์เนตเคลื่อนที่ ผู้ให้บริการที่มีระบบของการเก็บข้อมูลที่ถูกเก็บซ้ำไว้ในคอมพิวเตอร์ ผู้ให้บริการจัดเก็บข้อมูล ไม่ให้ต้องรับผิดสำหรับเนื้อหาต่างๆที่เกิดจากการที่ผู้บริโภคหรือลูกค้ากลุ่มเป้าหมายผลิตเนื้อหาด้วยตัวเอง กฎหมายฉบับดังกล่าวให้ความคุ้มครอง OSP ที่ได้ทำตามมาตรฐานทางเทคนิคในฐานะผู้ให้บริการ โดยอาจมีบางกรณีที่ OSP จะต้องรับผิดตามกฎหมายหากเจตนาที่จะเข้าไปมีส่วนเกี่ยวข้องกับเนื้อหา หรือในกรณีที่ OSP เป็นผู้ผลิตเนื้อหาด้วยตนเอง หรือในกรณีที่มีส่วนรู้เห็นหรือควรจะรู้เห็นเกี่ยวกับเนื้อหาที่ผิดกฎหมาย[11] อย่างไรก็ดี E-commerce directive มิได้พิจารณาในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล

ดังนั้นการพิจารณาความรับผิดของผู้ให้บริการ OSP ตามหลักการของการคุ้มครองข้อมูลส่วนบุคคล ภายใต้ GDPR จึงมีความจำเป็นต้องกำหนดสถานะของ OSP ให้ชัดเจน ซึ่งหากการพิจารณาสถานะของผู้ให้บริการ OSP ถูกจัดให้อยู่ในฐานะของการเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือผู้ประมวลข้อมูล (Data Processor) ตามนิยามที่กำหนดใน GDPR จะทำให้ผู้ให้บริการ OSP ต้องมีภาระที่จะต้องดำเนินภายใต้ GDPR ซึ่งผู้ให้บริการ OSP อาจอยู่ในสถานะของ Data Controller หรือ Data Processor หรืออยู่ในทั้งสองสถานะก็ได้ โดยผู้ให้บริการ OSP จะถูกจัดอยู่ในสถานะของ Data Controller ก็ต่อเมื่อมีความรับผิดชอบในการกำหนดวัตถุประสงค์และวิธีการในการจัดเก็บข้อมูลส่วนบุคคล โดย Data Controller จะต้องปฏิบัติตามมาตรการในการจัดเก็บและรักษาข้อมูล กำหนดวัตถุประสงค์ของการนำข้อมูลนั้นไปใช้ และกำหนดระยะเวลาในการจัดเก็บตามความจำเป็น และจะต้องมีวิธีการในการให้ประชาชนสามารถเข้าถึงข้อมูลส่วนตัวของเขา นอกจากนั้นผู้ให้บริการ OSP ในฐานะของการเป็น Data Controller จะต้องทำสัญญากับ Data Processor ในการที่จะทำให้เป็นที่มั่นใจได้ว่า Data Processor มีมาตรการในการประมวลผลข้อมูลที่มีความปลอดภัยและถูกต้องตามกฎหมาย ในส่วนของการพิจารณาว่าผู้ให้บริการ OSP มีสถานะเป็น Data Processor หรือไม่จะพิจารณาจากการทำหน้าที่ในการประมวลผลข้อมูลแทน Data Controller ซึ่งภายใต้ GDPR Data Processor จะต้องมีภาระในการประมวลผลข้อมูลด้วยมาตรการที่มีความปลอดภัยและถูกต้องตามกฎหมาย กรณีศึกษา Facebook ทำหน้าที่ในฐานะผู้ประมวลข้อมูล ในกรณีดังต่อไปนี้

---

(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

[11] Daphne Keller, “The Right Tools: Europe’s Intermediary Liability Laws and the EU 2016 General Data Protection”. Berkeley Technology Law Journal Vol.33:287. (2018). 295. https://btlj.org/data/articles2018/vol33/33_1/Keller_Web.pdf. Last visited 11 January 11, 2020.

- Facebook ใช้ข้อมูลของระบบลูกค้าสัมพันธ์ในการหาความสัมพันธ์ของบุคคลกับการทำการตลาดในการโฆษณา[12]

- Facebook ประมวลผลข้อมูลในนามของผู้โฆษณา เพื่อที่จะวัดพฤติการณ์ของประชาชนและรายงานกลับไปยังผู้โฆษณาว่าประชาชนให้ความสนใจและปฏิกิริยาต่อโฆษณาหรือไม่[13]

อย่างไรก็ดี เงื่อนไขของการประมวลผลข้อมูลส่วนบุคคลภายใต้ GDPR ถูกกำหนดภายใต้ Article 6[14] ที่ได้กำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องกระทำภายใต้ความยินยอม (consent) ของเจ้าของข้อมูล (Data Subject) โดยมีการกำหนดข้อยกเว้นในกรณีที่การประมวลผลข้อมูลไม่จำต้องขอความยินยอมจากเจ้าของข้อมูลในกรณีดังต่อไปนี้ คือ

- การประมวลผลข้อมูลกระทำไปเพื่อการปฏิบัติตามสัญญา เช่น การประมวลผลข้อมูลธุรกรรมเพื่อคำนวณดอกเบี้ยธนาคาร หรือ เว็บไซต์ขายของออนไลน์ เก็บรวบรวมข้อมูลที่อยู่ของลูกค้า

---

[12] https://www.facebook.com/business/gdpr#Facebook-as-the-data-controller-vs-Facebook-as-the-data-processor

[13] https://www.facebook.com/business/gdpr#Facebook-as-the-data-controller-vs-Facebook-as-the-data-processor

[14] Article 6 of General Data Protection Regulation Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks

เพื่อส่งต่อให้ร้านค้าสำหรับการจัดส่งสินค้าให้แก่ลูกค้า อย่างไรก็ดีควรระมัดระวังให้การประมวลผลข้อมูลตามความจำเป็นเพื่อการปฏิบัติตามสัญญาเท่านั้น เช่น ไม่นำข้อมูลเกี่ยวกับพฤติกรรมของลูกค้าที่ได้จากเว็บไซต์ขายของออนไลน์ไปทำการประมวลผลเพื่อประโยชน์ในการโฆษณาเสนอขายสินค้า

- การประมวลผลข้อมูลสำหรับการปฏิบัติเพื่อให้เป็นไปตามกฎหมาย โดยผู้ควบคุมข้อมูลจะต้องระบุให้ชัดเจนว่าปฏิบัติตามกฎหมายฉบับใด หรือตามคำสั่งของหน่วยงานรัฐที่มีอำนาจ เช่น การดำเนินการประมวลผลข้อมูลตามคำสั่งศาล

- การประมวลผลข้อมูลเนื่องจากความจำเป็นต่อชีวิตของบุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้อง ซึ่งอาจเกิดขึ้นในกรณีที่เจ้าของข้อมูลไม่อยู่สภาวะที่สามารถให้ความยินยอมได้ เช่น โรงพยาบาลเปิดเผยข้อมูลการรักษาพยาบาลที่ผู้ป่วยเคยรักษาที่โรงพยาบาลนั้นแก่อีกโรงพยาบาลหนึ่งที่ผู้ป่วยเข้ารับการรักษาในกรณีฉุกเฉิน

- การประมวลผลข้อมูลที่จำเป็นต่อการดำเนินการตามภารกิจของรัฐเพื่อประโยชน์สาธารณะ โดยผู้ประมวลผลข้อมูลในกรณีนี้จะเป็นเจ้าหน้าที่หรือองค์กรของรัฐ เช่น สำนักงานศาลยุติธรรม หรือเจ้าหน้าที่ของกระทรวงต่างๆที่ปฏิบัติตามกฎหมาย เช่น การให้บริการการสอบใบอนุญาตขับขี่รถยนต์

- การประมวลผลข้อมูลเพื่อประโยชน์โดยชอบธรรมของผู้ควบคุมข้อมูล โดยไม่เกินขอบเขตอันจำเป็น ซึ่งอาจมีการตีความอย่างกว้าง จึงจำเป็นที่ผู้ควบคุมข้อมูลต้องพิจารณาอย่างระมัดระวังเพื่อไม่ให้การประมวลผลข้อมูลขัดต่อสิทธิอันชอบธรรมของเจ้าของข้อมูล เช่น การที่โรงแรมเก็บข้อมูลการเข้าออกห้องพักของลูกค้าและพนักงานผ่านการใช้คีย์การ์ด เพื่อการบริหารจัดการหากเกิดกรณีที่มีข้อพิพาทหรือมีการสอบสวนพนักงาน โดยการเก็บข้อมูลนี้จะกระทำเป็นการชั่วคราวในระยะเวลาที่เหมาะสม และจะถูกลบออก 30 วัน ข้อมูลนี้อาจนำไปใช้เพื่อปรับปรุงการให้บริการในอนาคต[15]

**2.3 ความเชื่อมโยงของความรับผิดตัวกลางตาม GDPR**

การพิจารณากรอบกฎหมายในเรื่องความรับผิดของตัวกลางบนอินเทอร์เนตกับการคุ้มครองข้อมูลส่วนบุคคลมีแง่มุมในการพิจารณาที่แตกต่างกัน ความรับผิดของตัวกลางจะมุ่งเน้นในประเด็นที่เกี่ยวข้องกับความรับผิดของผู้ให้บริการเว็บไซต์บนอินเทอร์เนตหากมีกรณีที่บุคคลที่สามกระทำการ ผิดกฎหมายในระหว่างที่อยู่ในขอบเขตของการบริการของเว็บไซต์ของผู้ให้บริการ ในขณะที่การคุ้มครองข้อมูลส่วนบุคคลมุ่งเน้นที่ประเด็นของการกำกับดูแลกระบวนการประมวลผลข้อมูลส่วนบุคคล อย่างไรก็ดีหลักการในเรื่องดังกล่าวได้ถูกพิจารณาควบคู่กันตามหลักการที่ถูกบัญญัติภายใต้ GDPR[16]

---

[15] ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

[16] Giovanni De Gregorio, European University Institute Working Papers. The E-Commerce Directive and GDPR Convergence of Legal Regimes in the Algorithmic Society?. p.1 https://cadmus.eui.eu/bitstream/handle/1814/63044/RSCAS%202019_36.pdf?sequence=1&isAllowed=y. (last visited 11 January 11, 2020).

ประเด็นในเรื่องการพิจารณาเรื่องความรับผิดตัวกลาง (intermediary liability) ได้ถูกหยิบยกขึ้นสืบเนื่องจากการเข้าถึงข้อมูลส่วนบุคคลส่วนใหญ่ในโลกยุคปัจจุบันเกิดขึ้นผ่านช่องทางของการใช้อินเทอร์เนตที่มีการแสดงความคิดเห็นได้อย่างเสรี ในขณะเดียวกันก็อาจก่อให้เกิดภัยคุกคามต่อความเป็นส่วนตัวของปัจเจกชน กรณีศึกษาที่สำคัญได้แก่ คดีขึ้นสู่ศาลยุติธรรมสหภาพยุโรป โดยชายชาวสเปนได้ทำการฟ้องร้องต่อบริษัท Google ของ Google Spain โดยมีชายชาวสเปนรายหนึ่ง (Mario Costeja Gonzalez) แพ้คดีที่ศาลได้ทำการตัดสิน และบ้านของเขาได้ถูกประกาศขายทอดตลาดเพื่อนำเงินมาชำระหนี้แล้วในปี 1998 และได้มีการประกาศการขายทอดตลาดในหนังสือพิมพ์โดยมีชื่อของ Mr. Costeja ในหนังสือพิมพ์ เป็นผลให้คดีเป็นที่ยุติ อย่างไรก็ดี สิบปีต่อมาหนังสือพิมพ์ฉบับดังกล่าวได้ถูกทำออกในรูปแบบดิจิทัลเพื่อเผยแพร่ทางออนไลน์ ประชาชนทั่วไปสามารถค้นหาชื่อของ Mr. Costeja และพบว่าเขาเคยมีคดีความที่เกี่ยวกับสภาพทางการเงิน ทำให้เขาได้รับความเสียหาย Mr. Costeja จึงได้ร้องไปที่ Data Protection Authority ในประเทศสเปนเพื่อให้บริษัท Google นำผลของการค้นหาชื่อของเขาใน google ออกจากโปรแกรมการค้นหา (search engine) ของ Google ซึ่งศาลยุติธรรมสหภาพยุโรป Court of Justice of the European Union (CJEU) ได้ตัดสินให้บริษัท Google ดำเนินการลบข้อมูลของผู้ร้องออกจากโปรแกรมค้นหา โดยพิจารณาบนพื้นฐานที่ว่า Google อยู่ในฐานะของการเป็นผู้ควบคุมข้อมูล (data controller) ศาล CJEU ยังได้ให้เหตุผลเพิ่มเติมว่าข้อมูลที่ถูกนำออกจากระบบเป็นข้อมูลที่ไม่ถูกต้อง หรือ ไม่มีความเกี่ยวข้อง หรือเกินความจำเป็นกับวัตถุประสงค์ของการประมวลผลข้อมูล[17] อย่างไรก็ดีการพิจารณาการลบข้อมูลออกจากโปรแกรมค้นหาตามคำขอของผู้ร้องจะต้องพิจารณาถึงการค้นหาข้อมูลทั่วๆไปที่อยู่บนโลกออนไลน์ จึงต้องทำการพิจารณาเป็นกรณีๆไป ซึ่งศาลยุติธรรมสหภาพยุโรปได้บัญญัติหลักการดังกล่าวว่า สิทธิที่จะถูกลืม หรือ “Right to be forgotten”[18]

คำตัดสินของศาลยุติธรรมสหภาพยุโรปในกรณีของ Google Spain ถือได้ว่าเป็นจุดเริ่มต้นของความเชื่อมโยงกันระหว่างการคุ้มครองข้อมูลส่วนบุคคลและความรับผิดของตัวกลาง ซึ่งความรับผิดของตัวกลางตาม E-Commerce Directive กำหนดแต่เพียงหน้าที่ในการเฝ้าระวังในการสังเกตถึงข้อมูลที่ผิดกฎหมายและแจ้งเตือนไปยังผู้ใช้บริการ แต่ไม่ได้กำหนดหน้าที่ในการวิเคราะห์ว่าข้อมูลดังกล่าวเป็นข้อมูลส่วนบุคคลที่อาจมีผลกระทบต่อความเป็นส่วนตัวหรือก่อให้เกิดความเสียหายต่อชื่อเสียงของเจ้าของข้อมูลเมื่อข้อมูลนั้นได้ถูกเผยแพร่บนโปรแกรมค้นหา หรือกล่าวอีกนัยหนึ่งคือผู้ให้บริการโปรแกรมค้นหา (google) ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ตามหลักการของ GDPR ซึ่งได้กำหนดหน้าที่และความรับผิดไว้ในกรณีที่ไม่ปฏิบัติตามหลักการต่างๆที่ได้กำหนดไว้ใน GDPR ซึ่งรวมถึงสิทธิในการที่จะต้องแก้ไขข้อมูลให้มีความทันสมัยและเป็นปัจจุบัน หรือการลบหรือการนำข้อมูลออกจากระบบหรือการแก้ไขข้อมูลให้ถูกต้อง (Right to be forgotten) ภายใต้เงื่อนไขที่กำหนด

---

[17] Daphne Keller, “The Right Tools: Europe’s Intermediary Liability Laws and the EU 2016 General Data Protection”. Berkeley Technology Law Journal Vol.33:287. (2018). 313-314. https://btlj.org/data/articles2018/vol33/33_1/Keller_Web.pdf. (Last visited 11 January 11, 2020).

[18] Ibid. p. 290.

ตามกฎหมายฉบับนี้ ผลของการกำหนดหลักการ Right to be forgotten ภายใต้ GDPR ซึ่งมีผลใช้บังคับเมื่อพฤษภาคม 2018 ส่งผลให้ OSP จะต้องมีภาระหน้าที่ในการนำผลการค้นหาออกจากโปรแกรมค้นหาเมื่อมีเงื่อนไขที่กระทบต่อความเป็นส่วนตัวของบุคคลนอกเหนือจากภาระหน้าที่ที่จะต้องทำการเฝ้าระวังข้อมูลที่มีลักษณะขัดต่อกฎหมายไม่ให้มีการเผยแพร่บนเว็บไซต์ของ OSP จึงถือได้ว่า GDPR ได้ทำการยกระดับในการคุ้มครองของการคุ้มครองสิทธิขั้นพื้นฐานของบุคคลให้เพิ่มมากยิ่งขึ้น[19]

อย่างไรก็ดีในบางกรณีเจ้าของข้อมูลอาจไม่สามารถขอลบข้อมูลส่วนบุคคลของตนได้ เช่น กรณีที่มีการดำเนินการประมวลข้อมูลบนการดำเนินการของรัฐ ซึ่งจะต้องมีการระบุไว้โดยชัดแจ้ง และไม่สามารถนำข้อมูลส่วนบุคคลของเจ้าของข้อมูลไปดำเนินการประมวลผลโดยอาศัยข้อยกเว้นในกรณีอื่น เช่น การดำเนินการเพื่อเก็บข้อมูลจราจร (traffic data) จะต้องทำการเก็บข้อมูลตามระยะเวลาที่กฎหมาย (พระราชบัญญัติ คอมพิวเตอร์) กำหนด หรือกรณีของการดำเนินประมวลผลข้อมูลเพื่อปฏิบัติตามสัญญา ผู้เป็นเจ้าของข้อมูลส่วนบุคคล (Data Subject) จะดำเนินการขอลบข้อมูลส่วนบุคคลได้ในกรณีมีเงื่อนไขตามสัญญาให้ลบได้เท่านั้น

กล่าวโดยสรุปคือ หลักการในเรื่อง Right to be forgotten ได้ถูกกำหนดเป็นภาระหน้าที่ของ OSP ที่จะต้องมีหน้าที่ในการดำเนินการตามที่กำหนดไว้ภายใต้ GDPR ซึ่งถ้าหาก OSP ถูกพิจารณาว่าเป็น Data Controller ที่มีวัตถุประสงค์ในการรวบรวมข้อมูลส่วนบุคคลและนำข้อมูลนั้นไปประมวลผล แต่หากการประมวลผลข้อมูลนั้นเกินไปจากขอบวัตถุประสงค์ที่ได้แจ้งไว้ในการให้บริการ และไม่เข้ากรณีข้อยกเว้นตามที่กำหนดไว้ใน Article 6 ของ GDPR ผู้ให้บริการ OSP ก็จะต้องมีภาระในการนำข้อมูลนั้นออกจากระบบการให้บริการของ OSP

## 3. บทสรุป

นับตั้งแต่คำตัดสินของศาลยุติธรรมสหภาพยุโรปในคดี Google Spain ถือได้ว่าเป็นจุดเริ่มต้นของความเชื่อมโยงระหว่างหลักการของการคุ้มครองข้อมูลส่วนบุคคลกับความรับผิดของตัวกลาง โดยหลักการ Right to be forgotten ที่ศาลยุติธรรมสหภาพยุโรปได้ใช้เป็นหลักในการตัดสินคดีดังกล่าว ได้ถูกนำมาบัญญัติเป็นหลักการสำคัญของการคุ้มครองข้อมูลภายใต้ GDPR เนื่องด้วยเหตุผลที่ว่าในอนาคตพัฒนาการของเทคโนโลยีจะก่อให้เกิดการประมวลผลข้อมูลส่วนบุคคลโดยระบบอัตโนมัติ โดยเฉพาะอย่างยิ่งผู้ให้บริการเว็บไซต์ต่างๆ ที่มีการเก็บรวมรวมและประมวลผลข้อมูลส่วนบุคคลของผู้ใช้บริการ (OSP) ซึ่งจะก่อให้เกิดประเด็นโต้แย้งขึ้นว่าระบบที่ทำการประมวลผลดังกล่าวมีขอบเขต หน้าที่ เพียงใด และระบบอัตโนมัติที่ประมวลผลข้อมูลดังกล่าวจะถูกพิจารณาว่าเป็น Data Controller ตาม GDPR ซึ่งจะต้องมีหน้าที่ในการจัดการข้อมูลส่วนบุคคลภายใต้ข้อกำหนดที่บัญญัติไว้ตาม GDPR

[19] Giovanni De Gregorio, European University Institute Working Papers. The E-Commerce Directive and GDPR Convergence of Legal Regimes in the Algorithmic Society?. P. 7-9. https://cadmus.eui.eu/bitstream/handle/1814/63044/RSCAS%202019_36.pdf?sequence=1&isAllowed=y. (last visited 11 January 11, 2020).

## บรรณานุกรม


เว็บโฮสติ้ง (Web Hosting) คืออะไร, https://www.ic-myhost.com/web-hosting-articles/web-hosting-%E0%B8%84%E0%B8%B7%E0%B8%AD.html. (เข้าถึงเมื่อ 11 มกราคม 2563).

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

European Commission, Data Protection in the EU. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en#fundamental-rights. (Last visited 11 January 11, 2020).

Gregorio, Giovanni De, European University Institute Working Papers. The E-Commerce Directive and GDPR Convergence of Legal Regimes in the Algorithmic Society?. https://cadmus.eui.eu/bitstream/handle/1814/63044/RSCAS%202019_36.pdf?sequence=1&isAllowed=y. (last visited 11 January 11, 2020).

Guide to the General Data Protection Regulation (GDPR) The principles. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/. (last visited 11 January 11, 2020).

Keller, Daphne "The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection". Berkeley Technology Law Journal Vol.33:287. (2018). https://btlj.org/data/articles2018/vol33/33_1/Keller_Web.pdf. (Last visited 11 January 11, 2020).

Lankinen, Antti, Intermediary Liability for Copyright Infringements: Striking a Fair Balance the Right to Intellectual Property and Other Fundamental Rights of the Charter of Fundamental Rights of the European Union, (Master of Laws, School of Law, Orebro Universitet), http://www.diva-portal.org/smash/get/diva2:1233315/FULLTEXT01.pdf