ระบบประมวลผลแบบคลาวด์ (Cloud Computing) : ข้อเสนอแนะเพื่อการยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย

CLOUD COMPUTING : RECOMMENDATIONS FOR THAI PERSONAL DATA PROTECTION ACT

เบญญาภา ช่างประดิษฐ์

Benyapa Changpradit

นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต สาขากฎหมายการค้าระหว่างประเทศ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ : benyapa.chang@gmail.com

Graduate student of Master of Laws Program in International Trade Regulation, Faculty of Law, Thammasat University. Email address : benyapa.chang@gmail.com

Received : August 9, 2018
Revised : June 10, 2019
Accepted : June 26, 2019

บทคัดย่อ

ระบบการประมวลผลแบบคลาวด์เป็นเทคโนโลยีที่มีความสำคัญต่อทั้งผู้ประกอบการและบุคคลทั่วไปและเป็นเทคโนโลยีที่มีความเกี่ยวข้องกับข้อมูลจำนวนมากโดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคล ดังนั้น องค์การระหว่างประเทศและนานาประเทศจึงปรับปรุงหรือออกกฎหมายใหม่ที่เกี่ยวเนื่องกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้กฎหมายดังกล่าวสามารถนำไปบังคับใช้กับระบบการประมวลผลแบบคลาวด์ได้ ยกตัวอย่างเช่น สหภาพยุโรปออกกฎหมายฉบับใหม่ที่มีชื่อว่า “General Data Protection Regulation : GDPR” เป็นต้น สำหรับประเทศไทยแม้จะมีพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เป็นกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลในขณะนี้ แต่ก็ไม่สามารถใช้บังคับกับข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ที่ให้บริการโดยภาคเอกชนได้ เพราะพระราชบัญญัติดังกล่าวมีผลใช้บังคับกับหน่วยงานของรัฐเท่านั้น นอกจากนี้ ประเทศไทยยังมีร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่ยังไม่มีผลใช้บังคับอีกหลายฉบับ โดยฉบับล่าสุด คือ ฉบับที่คณะรัฐมนตรีอนุมัติหลักการเมื่อวันที่ 22 พ.ค. 2561 และเมื่อวันที่ 27 พฤษภาคม 2562 ประเทศไทยได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกที่มีชื่อว่า “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” อย่างไรก็ตาม พระราชบัญญัติดังกล่าวยังไม่เหมาะสมที่จะบังคับใช้กับข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ และจำเป็นต้องได้รับการแก้ไขในประเด็นต่าง ๆ เพิ่มเติม

คำสำคัญ

ข้อมูลส่วนบุคคล, ระบบการประมวลผลแบบคลาวด์, การคุ้มครองข้อมูลส่วนบุคคล, ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

ABSTRACT

Cloud Computing is a valuable technology for both business operators and individuals as it assists the businesses in IT cost reduction as well as facilitates individuals to access and manage data over the Internet everywhere. Cloud computing is also relevant to personal data due to the fact that there are a great number of personal data stored in cloud computing and, as a consequence, there is possibility and risk of cloud data leaks. To deal with this issue, various

international organizations and many countries have legislated personal data protection laws and enforced such laws and regulations with cloud computing services. In Thailand, there has been only one effective data protection law so far which is “the Official Information Act 1997” applied with data in possession of the government sector. For private sector, there have been a number of drafted personal data protection laws over a long period of time. However, the lasts drafted personal data protection of Thailand is not consistent with international standard guideline and in appropriate to apply with the context of cloud computing.

Keywords

Personal Data, Cloud Computing, Data Protection, Draft Personal Data Protection Act

บทนำ

ในปัจจุบันประเทศไทยกำลังเข้าสู่รูปแบบของการพัฒนาประเทศที่เรียกว่า “ประเทศไทย 4.0” ซึ่งจำเป็นต้องอาศัยเทคโนโลยีเพื่อรองรับการประกอบกิจการและรองรับการบริโภคของผู้บริโภคทั่วไป ดังจะเห็นได้จากการที่ผู้ประกอบการและผู้บริโภคหลายรายหันมาให้ความสนใจเทคโนโลยีด้านไอทีต่าง ๆ โดยเฉพาะอย่างยิ่งระบบการประมวลผลแบบคลาวด์ ซึ่งสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology หรือ NIST ของประเทศสหรัฐอเมริกาได้ให้คำจำกัดความของระบบการประมวลผลแบบคลาวด์ไว้ว่าเป็นรูปแบบของการบริการที่ช่วยเพิ่มความสะดวกสบายและความสามารถในการเข้าถึงเครือข่ายของทรัพยากรที่ใช้ในระบบการประมวลผลร่วมกัน ซึ่งเป็นทรัพยากรที่สามารถปรับแต่งได้ (เช่น เครือข่าย เซิร์ฟเวอร์ ที่จัดเก็บข้อมูล แอพพลิเคชั่น และบริการต่าง ๆ) โดยผู้ใช้งานสามารถเรียกใช้งานเครือข่ายดังกล่าวได้ตามความต้องการของผู้ใช้งานผ่านช่องทางต่าง ๆ ที่หลากหลาย และสามารถเพิ่ม หรือลดทรัพยากรที่ต้องการใช้งานได้อย่างสะดวกรวดเร็วไม่ก่อให้เกิดความยุ่งยากในการบริหารจัดการหรือการติดต่อกับผู้ให้บริการ[1]

แม้ว่าระบบการประมวลผลแบบคลาวด์จะได้รับความสนใจจากทั้งผู้ประกอบการและผู้บริโภคเป็นอย่างมาก แต่เมื่อพิจารณาถึงลักษณะของการให้บริการระบบการประมวลผลแบบคลาวด์ในประเทศไทยในระหว่างปี พ.ศ. 2559 – พ.ศ. 2560 ที่ผ่านมา จะพบว่าประเทศไทยยังขาดความพร้อมและระบบจัดการของการให้บริการระบบการประมวลผลแบบคลาวด์ที่ดี หากเปรียบเทียบกับประเทศอื่น ๆ ดังจะสังเกตได้จากผลการประเมินความพร้อม และระบบจัดการของภาครัฐในการส่งเสริมให้เกิดการให้บริการระบบการประมวลผลแบบคลาวด์ (Asia Cloud Computing Association ประเภท Asia Cloud Computing Readiness) ซึ่งประเมินโดยกลุ่มพันธมิตรธุรกิจซอฟต์แวร์ (Business Software Alliance) หรือ “บีเอสเอ” โดยประเทศไทยได้รับการจัดอันดับอยู่ในอันดับที่ 21 ในปี 2559[2] และอันดับที่ 19 ในปี 2561 จากทั้งหมด 24 ประเทศ ซึ่งคำนวณเป็น 80% ของตลาดไอทีโลก ทั้งนี้ ผลการประเมินดังกล่าวระบุไว้ว่าประเทศไทยสอบตกในประเด็นเรื่องความเป็นส่วนตัวของข้อมูล เนื่องจากประเทศไทยไม่มีกฎหมายหรือข้อบังคับเกี่ยวกับเรื่องการเก็บ ใช้ หรือดำเนินการต่าง ๆ กับข้อมูลส่วนบุคคลที่สอดคล้องกับหลักการคุ้มครองความเป็นส่วนตัวตามข้อบังคับด้านการคุ้มครองข้อมูลของสหภาพยุโรปและตามกรอบการคุ้มครองความเป็นส่วนตัวของเอเปค นอกจากนี้ประเทศไทยยังไม่มีกฎหมายที่กำหนดถึงการแจ้งให้เจ้าของข้อมูลทราบในกรณีที่เกิดการละเมิดข้อมูล รวมทั้งไม่มีกฎหมายหรือมาตรการรองรับสิทธิส่วนบุคคลในการดำเนินการในกรณีที่เกิดการละเมิดความเป็นส่วนตัวของข้อมูลอย่างชัดเจนอีกด้วย ซึ่งจุดนี้ถือเป็นจุดอ่อนที่สำคัญของประเทศไทย และส่งผลกระทบโดยตรงต่อความเชื่อมั่นในการใช้บริการระบบการประมวลผลแบบคลาวด์ภายในประเทศไทยและส่งผลทางโดยอ้อมต่อเศรษฐกิจ การลงทุนและการค้าระหว่างประเทศ

จากกรณีดังกล่าวข้างต้น ผู้เขียนขอสรุปปัญหาของประเทศไทยเกี่ยวกับการคุ้มครองข้อมูลบุคคลที่ถูกจัดเก็บอยู่ในระบบการประมวลผลแบบคลาวด์ออกเป็น 3 ระยะ ดังนี้

<u>ระยะที่ 1</u> ประเทศไทยกำลังประสบปัญหาการขาดแคลนกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่จะบังคับใช้กับระบบการประมวลผลแบบคลาวด์ เพราะแม้ว่าประเทศไทยจะมีพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แต่พระราชบัญญัติดังกล่าวก็ใช้บังคับเฉพาะกรณีที่หน่วยงานของรัฐเป็นผู้จัดเก็บข้อมูลเท่านั้น ซึ่งในทางปฏิบัติของการให้บริการระบบการประมวลผลแบบคลาวด์ ผู้ให้บริการส่วนใหญ่ล้วนเป็นภาคเอกชนทั้งสิ้น ประกอบกับแม้ประเทศไทยจะมีกฎหมายเฉพาะเรื่องบัญญัติให้ความคุ้มครองข้อมูลส่วนบุคคล เช่น พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 พระราชบัญญัติ

[1] ชินดนัย สังคะคุณ, “การจัดเก็บภาษีเงินได้นิติบุคคลจากการให้บริการของบริษัทต่างประเทศ : กรณีการให้บริการประมวลผลแบบคลาวด์,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558), น.14-15.

[2] BSA and Galexia, “ผลการประเมินความพร้อมของประเทศต่าง ๆ ทั่วโลก สำหรับเทคโลโยลีคลาวด์คอมพิวติ้ง โดยบีเอสเอ (BSA) ประจำปี พ.ศ. 2559 : การเผชิญหน้ากับความท้าทายใหม่,” สืบค้นเมื่อวันที่ 10 ตุลาคม 2559, จาก http://cloudscorecard.bsa.org/2016/Pdf/BSA_2016_Global_Cloud_Scorecard_th.pdf

การทะเบียนราษฎร พ.ศ. 2534 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 เป็นต้น ก็ตาม แต่พระราชบัญญัติดังกล่าวก็ไม่สามารถใช้บังคับกับข้อมูลส่วนบุคคลที่จัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์เช่นกัน

<u>ระยะที่ 2</u> หากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) (“ร่างพระราชบัญญัติฯ”) ที่กำลังอยู่ในการพิจารณามีผลใช้บังคับแล้ว ร่างพระราชบัญญัติฯ ดังกล่าวก็ยังขาดหลักการสำคัญหลายประการเพื่อให้สอดรับกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลระดับสากลโดยเฉพาะอย่างยิ่ง กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปหรือ General Data Protection Regulation (GDPR) ซึ่งกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลซึ่งถือเป็นมาตรฐานการคุ้มครองสูงสุด ณ ขณะนี้ และไม่สอดคล้องกับรูปแบบธุรกิจหรือรูปแบบการให้บริการระบบการประมวลผลแบบคลาวด์อีกด้วย ทั้งนี้ ความไม่สอดคล้องกับหลักการสากลและความไม่เหมาะสมกับรูปแบบธุรกิจของการให้บริการของระบบการประมวลผลแบบคลาวด์สามารถสรุปได้ดังนี้

(1) ขอบเขตของข้อมูลที่จะตกอยู่ภายใต้บังคับของร่างพระราชบัญญัติฯ

แต่เดิมกฎหมายคุ้มครองข้อมูลส่วนบุคคลของนานาประเทศและร่างพระราชบัญญัติของประเทศไทยเอง ต่างกำหนดให้กฎหมายของตนมีผลใช้บังคับเฉพาะกับข้อมูลที่เข้าลักษณะเป็นข้อมูลส่วนบุคคลเท่านั้น นั่นหมายความว่าหากข้อมูลใดไม่เข้าลักษณะหรือคำจำกัดความของข้อมูลส่วนบุคคล ข้อมูลนั้นจะไม่ตกอยู่ภายใต้บังคับของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ตัวอย่างข้อมูลที่ไม่เข้าลักษณะเป็นข้อมูลส่วนบุคคล คือ ข้อมูลที่สามารถเชื่อมโยงถึงตัวบุคคลซึ่งเป็นเจ้าของข้อมูลได้นั่นเอง

การกำหนดขอบเขตการบังคับใช้เช่นนี้อาจก่อให้เกิดปัญหาในการบังคับใช้กฎหมายในปัจจุบัน เนื่องจากเทคโนโลยีการป้องกันการเข้าถึงข้อมูลส่วนบุคคล เพื่อป้องกันไม่ให้ข้อมูลส่วนบุคคลหรือข้อมูลทางธุรกิจที่สำคัญรั่วไหล ทำให้เกิดกระบวนการทำให้ข้อมูลส่วนบุคคลสูญเสียสิ่งเชื่อมโยงตัวบุคคลไป ดังนั้น ผู้ที่ได้รับข้อมูลดังกล่าวจะไม่สามารถเชื่อมโยงถึงตัวบุคคลที่เป็นเจ้าของข้อมูลได้ไม่ว่าชั่วคราวหรือถาวร ซึ่งกระบวนดังกล่าวประกอบไปด้วยกระบวนการ Anonymization[3] กระบวนการ Pseudonymous[4] และกระบวนการ Encryption[5] เป็นต้น กรณีจึงเกิดปัญหาในทางปฏิบัติว่าข้อมูลที่ผ่านกระบวนการเหล่านี้จะยังมีลักษณะเป็นข้อมูลส่วนบุคคลที่ยังตกอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่

ด้วยเหตุนี้ หลายประเทศจึงปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคลของตนเอง เพื่อให้เกิดความชัดเจนว่าข้อมูลเหล่านี้จะอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของตนหรือไม่ อาทิ GDPR กำหนดให้ไม่มีผลใช้บังคับกับข้อมูลส่วนบุคคลที่ได้ผ่านกระบวนการ Anonymization แต่สำหรับข้อมูลที่ผ่านกระบวนการ Pseudonymous นั้น GDPR บังคับให้ข้อมูลดังกล่าวยังอยู่ภายใต้บังคับของ GDPR เนื่องจากข้อมูลที่ผ่าน

---

[3] กระบวนการแปลงข้อมูลนิรนาม (Anonymization) หมายถึง วิธีการใด ๆ ที่จะทำให้ข้อมูลส่วนบุคคลในชุดข้อมูลของเจ้าของข้อมูลได้รับความคุ้มครองก่อนที่จะมีการส่งต่อไปยังบุคคลที่สาม ทำให้บุคคลที่สามซึ่งเป็นผู้รับข้อมูลมีโอกาสน้อยที่สุดที่จะนำข้อมูลดังกล่าวไปใช้ในการวิเคราะห์ที่ทำให้รู้ตัวเจ้าของข้อมูลส่วนบุคคลได้

[4] กระบวนการแปลงข้อมูลแฝง (Pseudonumous) เป็นกระบวนการที่มีลักษณะคล้ายคลึงกับกระบวนการแปลงข้อมูลนิรนาม (Anonymization) โดยหมายถึง กระบวนการประมวลผลข้อมูลส่วนบุคคลในทางที่ข้อมูลส่วนบุคคลไม่สามารถพิจารณาได้ว่าเป็นข้อมูลของเจ้าของข้อมูลส่วนบุคคลคนใดโดยเฉพาะหากไม่มีการนำข้อมูลส่วนอื่น ๆ ที่ถูกจัดเก็บไว้แยกต่างหากและมีมาตรฐานการจัดการองค์กรหรือมาตรฐานทางเทคนิคป้องกันไว้มาประกอบหรือมาเชื่อมโยงไม่ว่าโดยทางตรงหรือทางอ้อม

[5] กระบวนการเข้ารหัสข้อมูล (Encryption) เป็นกระบวนการรักษาความปลอดภัยให้แก่ข้อมูลส่วนบุคคลวิธีการหนึ่งที่ได้รับความนิยมเป็นอย่างมาก โดยมีลักษณะเป็นการเข้ารหัสหรือการแปลงข้อมูลให้เป็นรหัสลับเพื่อไม่ให้ข้อมูลถูกอ่านได้โดยบุคคลที่ไม่ได้รับอนุญาตผ่านทางการนำข้อมูลเดิมที่บุคคลใด ๆ ก็สามารถอ่านได้ในรูปแบบที่เรียกว่า “Plain Text” หรือ “Clear Text” มาทำการเข้ารหัสก่อนเพื่อเปลี่ยนแปลงข้อมูลเดิมให้เป็นข้อความที่เราเข้ารหัส (Ciphertext) และเมื่อข้อมูลถูกส่งไปยังบุคคลที่ได้รับอนุญาตให้เข้าถึงแล้วก็จะเข้าสู่กระบวนการที่เรียกว่า Decryption หรือกระบวนการถอดรหัสข้อมูล

กระบวนการ Pseudonymous เป็นข้อมูลที่ไม่ได้สูญเสียสิ่งเชื่อมโยงตัวบุคคลเป็นการถาวรเหมือนดังเช่นข้อมูลที่ผ่านกระบวนการ Anonymization อย่างไรก็ตาม GDPR ยังไม่บัญญัติครอบคลุมถึงข้อมูลที่ผ่านกระบวนการ Encryption เช่นเดิม

สำหรับประเทศไทย เมื่อพิจารณาร่างพระราชบัญญัติฯ จะพบว่าร่างพระราชบัญญัติดังกล่าวไม่ได้บัญญัติถึงข้อมูลที่ผ่านกระบวนการ Anonymization กระบวนการ Pseudonymous และกระบวนการ Encryption แต่อย่างใด ในประเด็นนี้ผู้เขียนมีความเห็นว่า ร่างพระราชบัญญัติควรกำหนดให้ข้อมูลที่ผ่านกระบวนการ Anonymization ไม่ต้องตกอยู่ภายใต้ร่างพระราชบัญญัติฯ ดังกล่าวแต่ข้อมูลที่ผ่านกระบวนการ Pseudonymous และกระบวนการ Encryption ยังคงต้องอยู่ภายใต้บังคับ ทั้งนี้ เนื่องจากข้อมูลทั้งสองประเภท มีลักษณะเป็นข้อมูลที่สูญเสียสิ่งเชื่อมโยงบุคคลเป็นการชั่วคราวเท่านั้น ข้อมูลดังกล่าวจึงยังควรได้รับความคุ้มครองภายใต้ร่างพระราชบัญญัติฉบับนี้ ดังนั้น ผู้เขียนจึงเสนอแนะให้เพิ่มอนุมาตรา (6) ในมาตรา 4 เพื่อระบุว่าข้อมูลส่วนบุคคลที่ถูกลบสิ่งเชื่อมโยงตัวบุคคลออกอย่างถาวรไม่อยู่ภายใต้บังคับของร่างพระราชบัญญัติฯ นี้

(2) การขาดหลักการเรื่องผู้ควบคุมข้อมูลร่วมกัน (Joint Controller)

ผู้ควบคุมข้อมูลร่วมกัน หมายถึง บุคคลธรรมดาหรือนิติบุคคลแยกต่างหากจากผู้ควบคุมข้อมูลและผู้ควบคุมข้อมูลร่วมกันดังกล่าวจะเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคลดังกล่าวร่วมกันกับผู้ควบคุมข้อมูล ซึ่งเมื่อพิจารณาร่างพระราชบัญญัติฯ เทียบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปทั้งฉบับเดิมและฉบับใหม่จะพบว่า ร่างพระราชบัญญัติของไทยไม่รองรับหลักการว่าด้วยผู้ควบคุมข้อมูลร่วมกัน ทั้งที่หลักการของผู้ควบคุมข้อมูลร่วมกันเป็นหลักการที่สำคัญที่จะช่วยรองรับการคุ้มครองข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ เพราะในการให้บริการระบบการประมวลผลแบบคลาวด์นั้น ผู้ให้บริการและผู้ใช้บริการอาจอยู่ในสถานะของผู้ควบคุมข้อมูลร่วมกันได้ ดังเช่นกรณีที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศสมีความเห็นว่าผู้ใช้บริการและผู้ให้บริการระบบการประมวลผลแบบคลาวด์ประเภท Public SaaS[6] และ Public PaaS[7] มีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน ด้วยเหตุนี้ ผู้เขียนจึงเสนอให้เพิ่มหลักการของผู้ควบคุมข้อมูลร่วมกันเข้าไปในร่างพระราชบัญญัติฯ โดยการกำหนดบทนิยามของผู้ควบคุมข้อมูลร่วมกันในมาตรา 6 และเพิ่มหน้าที่ของผู้ควบคุมข้อมูลร่วมกันเป็นมาตราใหม่ในร่างพระราชบัญญัติฯ[8]

(3) การกำหนดหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลไม่ครบถ้วนและไม่สอดคล้องกับทางปฏิบัติ

ผู้ประมวลผลข้อมูลส่วนบุคคลถือเป็นบุคคลสำคัญในการให้บริการระบบการประมวลผลแบบคลาวด์ เนื่องจากคณะทำงานของการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 29 (Article 29 Data Protection Working Party) พิจารณาว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์อยู่ในสถานะของผู้ประมวลผลข้อมูลส่วนบุคคล และเมื่อพิจารณาร่างพระราชบัญญัติฯ จะพบว่าร่างพระราชบัญญัติฯฉบับนี้ได้รองรับหลักการเรื่องผู้ประมวลผลข้อมูลส่วนบุคคลเอาไว้แล้ว แต่อย่างไรก็ตาม เมื่อพิจารณารายละเอียดบทบัญญัติเรื่องผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติฯ จะพบว่า บทบัญญัติเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติ ฯ

---

[6] ระบบการประมวลแบบคลาวด์ประเภท Public SaaS หมายถึง การให้บริการที่นำเอาแอพพลิเคชั่นหรือซอฟต์แวร์บางส่วนของผู้ให้บริการออกให้บริการแก่ผู้ใช้บริการทั่วไปโดยไม่จำกัดเฉพาะกลุ่มใดกลุ่มหนึ่ง โดยผู้ใช้บริการสามารถเข้าถึงบริการได้โดยอาศัยระบบอินเทอร์เน็ตของตน และผู้ให้บริการจะเป็นผู้รับผิดชอบในการดูแลและอัพเดตซอฟต์แวร์แทนผู้ใช้บริการ

[7] ระบบการประมวลแบบคลาวด์ประเภท Public PaaS หมายถึง การให้บริการที่ผู้ให้บริการนำเสนอแพลตฟอร์มสำหรับการดำเนินงานระบบต่าง ๆ เพื่อให้ผู้ใช้บริการซึ่งก็คือผู้พัฒนาชุดคำสั่งงานสามารถเข้าถึงและใช้ประโยชน์แบบออนไลน์ได้เป็นการทั่วไปไม่ได้จำกัดเฉพาะกลุ่มใดกลุ่มหนึ่ง

[8] Commission Nationale De I'informatique et des libertés, "Recommendations for companies planning to use Cloud Computing services," Retirevd on April 17, 2561, from https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf.

ดังกล่าวยังไม่ครอบคลุมเมื่อเทียบกับหลักเกณฑ์ในระดับสากล ดังนั้น ผู้เขียนจึงเสนอแนะให้กำหนดหน้าที่ให้แก่ผู้ประมวลผลข้อมูลส่วนบุคคลเพิ่มเติมดังนี้

- แจ้งคำสั่งที่ขัดหรือแย้งกับกฎหมายให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยทันที
- ไม่แต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคลหากไม่ได้รับความยินยอม
- แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลไปยังคณะกรรมการโดยไม่ชักช้า
- ปฏิบัติตามบทบทบัญญัติว่าด้วยการโอนหรือส่งข้อมูลส่วนบุคคล

(4) การขาดการรับรองสิทธิในการขอสำเนาและโอนย้ายข้อมูลส่วนบุคคลของเจ้าของข้อมูล (Data Portability)

สิทธิในการโอนย้ายข้อมูลส่วนบุคคลเป็นสิทธิที่กำหนดถึงการทำสำเนาของผู้ควบคุมข้อมูลหรือผู้ประมวลผลและส่งมอบให้แก่เจ้าของข้อมูล รวมถึงสิทธิในการโอนย้ายข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลรายหนึ่งไปยังผู้ควบคุมข้อมูลอีกรายหนึ่ง หรือผู้ประมวลรายหนึ่งไปยังผู้ประมวลผลอีกรายหนึ่ง ซึ่งจะสอดคล้องกับการใช้บริการระบบการประมวลผลแบบคลาวด์ที่อาจเปลี่ยนไปใช้บริการของผู้ให้บริการรายอื่นได้ ดังนั้น การขาดสิทธิดังกล่าวย่อมก่อให้เกิดความไม่ต่อเนื่องจากในการใช้บริการระบบการประมวลผลแบบคลาวด์และก่อให้เกิดความยุ่งยากและความไม่คล่องตัวแก่เจ้าของข้อมูล ซึ่งจะเป็นผลกระทบต่อการแข่งขันภายในตลาดเทคโนโลยี ดังนั้น ผู้เขียนจึงเสนอแนะให้เพิ่มบทบัญญัติใหม่เพื่อรองรับสิทธิประเภทนี้ของเจ้าของข้อมูลส่วนบุคคล ในขณะเดียวกันก็แก้ไขมาตรา 29 และมาตรา 30 เพื่อเพิ่มหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติตามสิทธิของเจ้าของข้อมูล

(5) ข้อยกเว้นเรื่องการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศยังไม่สอดรับกับรูปแบบธุรกิจของการให้บริการระบบการประมวลผลแบบคลาวด์

ข้อยกเว้นเกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศตามร่างพระราชบัญญัติฯ ยังไม่เพียงพอกับการให้บริการระบบการประมวลผลแบบคลาวด์ ทั้งนี้ เนื่องจากในทางปฏิบัติของระบบการประมวลผลแบบคลาวด์ซึ่งผู้ให้บริการหลายรายมีบริษัทในเครือจำนวนมากเพื่อถือครองดาต้าเซ็นเตอร์หลายแห่งทั่วโลก ทำให้ต้องมีการส่งหรือโอนข้อมูลระหว่างกันจำนวนมาก ดังนั้น ผู้เขียนจึงเสนอแนะให้แก้ไขมาตรา 25 เพื่อเพิ่มข้อยกเว้นให้รองรับการโอนข้อมูลส่วนบุคคลระหว่างบริษัทในเครือในลักษณะเดียวกับ GDPR โดยการกำหนดให้การโอนข้อมูลส่วนบุคคลสามารถกระทำได้โดยไม่ต้องเป็นไปตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด หากเป็นการโอนข้อมูลส่วนบุคคลระหว่างบริษัทในเครือซึ่งมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรที่ได้รับอนุมัติจากคณะกรรมการ

(6) ความไม่เหมาะสมของบทกำหนดโทษภายใต้ร่างพระราชบัญญัติฯ

ความรับผิดทางแพ่ง : ร่างพระราชบัญญัตินี้กำหนดให้เฉพาะผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้นที่ต้องรับผิดทางแพ่ง แต่ในทางปฏิบัติย่อมมีโอกาสที่ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลจนก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลได้ ด้วยเหตุนี้ ผู้เขียนจึงเสนอแนะให้แก้ไขมาตรา 64 โดยเพิ่มให้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับผิดทางแพ่งด้วย

โทษอาญา : การกำหนดให้กรรมการต้องรับผิดกรณีที่ผู้กระทำความผิดเป็นนิติบุคคลไม่ช่วยให้ผู้ประกอบการเกิดความตระหนักในการให้ความคุ้มครองข้อมูลและในการปฏิบัติตามกฎหมาย ด้วยเหตุนี้ ผู้เขียนจึงเสนอแนะให้ตัดมาตรา 67 ซึ่งกำหนดโทษของกรรมการออกจากร่างพระราชบัญญัติฯ และเพิ่มโทษทางปกครองแทน

โทษปรับทางปกครอง : จำนวนโทษปรับทางปกครองยังไม่เพียงพอที่จะทำให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลเกิดความเกรงกลัวและปฏิบัติตามบทบัญญัติแห่งกฎหมายนี้อย่างเคร่งครัด ด้วยเหตุนี้ ผู้เขียนเสนอแนะให้เพิ่มจำนวนโทษปรับทางปกครองโดยพิจารณาตามความร้ายแรง เช่น 100,000 บาทเป็น 2 ล้านบาทหรือ 1% ของรายได้ของบริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย เป็นต้น

(7) การกำหนดบทเฉพาะกาลเกี่ยวกับการมีผลใช้บังคับของร่างพระราชบัญญัติฯ ยังไม่เหมาะสม

การที่ร่างพระราชบัญญัตินี้กำหนดให้ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลต่อไปได้ตามวัตถุประสงค์เดิม โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่ายนั้น ก่อให้เกิดช่องว่างในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์ เพราะข้อมูลส่วนบุคคลโดยส่วนใหญ่มีกฎหมายเฉพาะที่กำหนดบทบัญญัติให้ผู้ที่เกี่ยวข้องต้องปฏิบัติตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับหลักการสากลอยู่แล้ว ในขณะที่ข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์ไม่มีกฎหมายใดให้ความคุ้มครองไว้โดยเฉพาะ การกำหนดให้ข้อมูลส่วนบุคคลทุกประเภทที่ผู้ควบคุมข้อมูลเก็บไว้ก่อนร่างพระราชบัญญัตินี้มีผลใช้บังคับสามารถเก็บรวบรวมและใช้ต่อไปได้ จึงไม่เป็นธรรม นอกจากนี้ในทางปฏิบัติบุคคลทีเก็บรวบรวมข้อมูลไม่ได้จำกัดเฉพาะผู้ควบคุมข้อมูลส่วนบุคคล แต่ยังรวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลด้วย ด้วยเหตุนี้ ผู้เขียนจึงเสนอแนะให้แก้ไขมาตรา 83 โดยกำหนดให้

- ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลเก็บรวบรวมไว้โดยปฏิบัติตามบทบัญญัติแห่งกฎหมายเฉพาะว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแล้วก่อนวันที่ร่างพระราชบัญญัติฯ มีผลใช้บังคับสามารถเก็บรวบรวมและใช้ต่อไปได้ แต่ต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์จะให้เก็บรวบรวมและใช้สามารถยกเลิกความยินยอมได้โดยง่าย ส่วนการเปิดเผยและการดำเนินการอื่นที่มิใช่การใช้และการเก็บรวบรวมให้ปฏิบัติตามร่างพระราชบัญญัติฯ นี้ใหม่

- ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลเก็บรวบรวมไว้โดยไม่ได้ปฏิบัติตามบทบัญญัติแห่งกฎหมายเฉพาะว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแล้วก่อนวันที่ร่างพระราชบัญญัติฯ มีผลใช้บังคับไม่ว่าจะดำเนินการใด ๆ ให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามร่างพระราชบัญญัติฯ นี้ใหม่ทุกกรณี

<u>ระยะที่ 3</u> แม้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก้ไขประเด็นความไม่สอดคล้องกับหลักการสากลและความไม่เหมาะสมกับรูปแบบธุรกิจบางส่วนดังต่อไปนี้

(1) บัญญัติรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลในการขอสำเนาและโอนย้ายข้อมูลส่วนบุคคล (Data Portability) โดยกำหนดไว้ในมาตรา 31 ของพระราชบัญญัติฯ

(2) บัญญัติข้อยกเว้นเรื่องการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเพิ่มเติมซึ่งสอดรับกับรูปแบบธุรกิจของการให้บริการระบบการประมวลผลแบบคลาวด์มากยิ่งขึ้น เช่น บัญญัติให้การโอนข้อมูลส่วนระหว่างบริษัทในเครือสามารถทำได้โดยอิสระหากมีการกำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงาน ตามที่กำหนดไว้ในมาตรา 29 เป็นต้น

(3) บัญญัติให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีความรับผิดทางแพ่งเช่นเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลในมาตรา 77 และบัญญัติเพิ่มโทษปรับทางปกครองเพิ่มขึ้นจากเดิม โดยกำหนดสูงสุดถึง 5 ล้านบาทในมาตรา 84 และมาตรา 87

ประเทศไทยก็ยังคงประสบปัญหาความไม่สอดคล้องกับหลักการสากลและความไม่เหมาะสมกับรูปแบบธุรกิจเช่นเดิม เนื่องจากพระราชบัญญัติฉบับนี้ยังไม่ได้แก้ไขประเด็นความไม่สอดคล้องกับหลักการสากลและความไม่เหมาะสมกับรูปแบบธุรกิจทั้งหมด ดังนั้น จึงต้องพิจารณาต่อไปว่าในอนาคตจะมีการแก้ไขพระราชบัญญัติฉบับนี้อีกหรือไม่เพื่อให้สอดรับกับหลักกฎหมายสากลและรูปแบบธุรกิจโดยเฉพาะธุรกิจการให้บริการระบบการประมวลผลแบบคลาวด์

บทสรุป

กล่าวโดยสรุปแม้ประเทศไทยจะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่จะใช้บังคับกับข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์แล้ว แต่ก็ยังไม่สอดคล้องกับ GDPR ถือเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานในการคุ้มครองสูงสุดทั้งหมด ดังนั้น ผู้ที่เกี่ยวข้องกับพระราชบัญญัติฯ ฉบับนี้จึงควรพิจารณาหลักการสำคัญ

ของ GDPR ในส่วนที่กฎหมายฉบับนี้ยังไม่ครบถ้วนและควรให้ความสำคัญกับข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์ด้วยโดยพิจารณาแก้ไขความไม่เหมาะสมหลายประการที่ยังคงไม่ได้รับการแก้ไขเพื่อให้พระราชบัญญัติฯ ฉบับนี้มีความสมบูรณ์และสามารถให้ความคุ้มครองผู้ใช้บริการระบบการประมวลผลแบบคลาวด์ได้อย่างเต็มที่และเป็นธรรม

บรรณานุกรม

หนังสือ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. คู่มือการเลือกใช้บริการ Cloud Computing. กรุงเทพมหานคร: กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2556.

นคร เสรีรักษ์. การคุ้มครองข้อมูลส่วนบุคคล : ข้อเสนอสำหรับประเทศไทย. กรุงเทพมหานคร : บริษัท พี.เพรส จำกัด, 2559.

บทความ

จันทจิรา เอี่ยมมยุรา. “การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย.” วารสารนิติศาสตร์ ปีที่ 34. ฉบับที่ 4. (ธันวาคม 2547). น.627.

_____. “แนวคิดและหลักการยกร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย.” วารสารนิติศาสตร์ ปีที่ 34. ฉบับที่ 4, (ธันวาคม 2547). น.653.

เพลินตา ตันรังสรรค์. “โครงการเสวนาให้ความเห็นต่อร่างกฎหมาย เรื่อง “ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .....” จุลนิติ 73. ฉบับที่ 5. ปีที่ 7. (กันยายน – ตุลาคม 2553). น.77.

ลันตา อุตมะโภคิน. “ร่างกฎหมายที่น่าสนใจ : ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .....” จุลนิติ. ฉบับที่ 3. ปีที่ 11. (พฤษภาคม – มิถุนายน 2557). น.75.

ประสิทธิ์ ปิวาวัฒนพาณิช. “กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย.” วารสารนิติศาสตร์ ปีที่ 34. ฉบับที่ 4. (ธันวาคม 2547). น.535.

วิทยานิพนธ์

ชินดนัย สังคะคุณ. “การจัดเก็บภาษีเงินได้นิติบุคคลจากการให้บริการของบริษัทต่างประเทศ : กรณีการให้บริการประมวลผลแบบคลาวด์.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558.

นัทรี เกตุแก้ว. “ความรับผิดทางแพ่งของผู้ให้บริการ Cloud Computing.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2557.

สื่ออิเล็กทรอนิกส์

BSA and Galexia. “ผลการประเมินความพร้อมของประเทศต่าง ๆ ทั่วโลก สำหรับเทคโลโยลีคลาวด์คอมพิวติ้ง โดย บีเอสเอ (BSA) ประจำปี พ.ศ. 2559 : การเผชิญหน้ากับความท้าทายใหม่.” http://cloudscorecard.bsa.org/2016/Pdf/BSA_2016_Global_Cloud_Score card_th.pdf, 10 ตุลาคม 2559.

BOOKS

Buyya, Rajkumar, Broberg, James Goscinski and Andrzej. Cloud computing : principles and paradigms. Hoboken, NJ : Wiley, 2011.

Chris Reed. Computer Law. Seventh Edition. New York, Oxford University Press Inc., 2011.

Christopher Kuner. European Data Privacy Law and Online Business. New York : Oxford University Press Inc., 2003.

ARTICLES

Romansky, Radi. "Cloud Services : Challenges for personal data protection." International Journal on Information Technologies & Security. Vol. 4. Issue 3. 2012.

ELECTRONIC MEDIAS

BSA. "2018 BSA Global Cloud Computing Scorecard Powering a Bright Future." http://cloudscore card.bsa.org/2018/, February 2, 2018.

European Data Protection Supervisor. "The History of the General Data Protection Regulation." https: / / edps. europa. eu/ data-protection/ data-protection/ legislation/ history-general-data-protection-regulation_en, February 24, 2018.