



กฎหมายว่าด้วยถิ่นที่อยู่ของข้อมูล (Data residency laws) ^๑

ปิยะขวัญ ชมชื่น^๒

การระบาดของ COVID-19 เป็นปัจจัยเร่งให้เกิดการใช้งานระบบออนไลน์ในทุกภาคส่วน ทั้งการบริการภาครัฐ ภาคการศึกษา และการดำเนินธุรกิจ โดยเฉพาะตลาด E-commerce ธุรกิจหนึ่งที่มีความโดดเด่นในขณะนี้ คือ ธุรกิจ Cloud Computing หรือ การบริการที่ใช้กำลังประมวลผล หน่วยจัดเก็บข้อมูลและระบบออนไลน์ที่จะช่วยลดความยุ่งยากในการติดตั้ง ดูแลระบบ ลดต้นทุนในการสร้างระบบคอมพิวเตอร์และเครือข่ายด้วยตนเอง^๓ โดยระหว่างปี พ.ศ. ๒๕๕๑ – ๒๕๖๓ มูลค่าตลาดของธุรกิจ Cloud Computing ทั่วโลกพุ่งสูงขึ้น ๔๔ เท่า และคาดว่าในปี พ.ศ. ๒๕๖๒ - ๒๕๖๕ ตลาด Cloud Computing จะเติบโตขึ้นโดยเฉลี่ยร้อยละ ๒๘^๔ นอกจากนี้ วิกฤต COVID -19 ยังแสดงให้เห็นถึงความสำคัญของการทำธุรกรรมออนไลน์ระหว่างประเทศและกฎเกณฑ์ที่ใช้ในการปกป้องคุ้มครองข้อมูลของแต่ละประเทศ จึงนำมาสู่การกล่าวถึงกฎหมายว่าด้วยถิ่นที่อยู่ของข้อมูล (Data residency law) ในวงกว้าง ซึ่งกฎหมายดังกล่าวจะเป็นอุปสรรคในการดำเนินกิจการของบริษัทที่ใช้ข้อมูลเป็นตัวขับเคลื่อนธุรกิจ บทความนี้จึงขอแนะนำข้อมูลจากเว็บไซต์ World Economic Forum ที่แสดงข้อมูลที่น่าสนใจเกี่ยวกับกฎหมายว่าด้วยถิ่นที่อยู่ของข้อมูล (Data residency laws) ไว้ดังนี้

๑. ความเข้าใจเกี่ยวกับกฎหมายถิ่นที่อยู่ของข้อมูล (Data residency laws) โดยทั่วไป

กฎหมายถิ่นที่อยู่ของข้อมูล หรือ “Data residency laws” เป็นคำที่ค่อนข้างใหม่ และถูกเรียกในชื่อที่หลากหลาย เช่น "Data sovereignty" หรือ "Data localization" ในอดีตการกำหนดข้อจำกัดเรื่องถิ่นที่อยู่ของข้อมูลจะเป็นไปตามกฎหมายที่ตราขึ้นสำหรับยุคที่มีการบันทึกข้อมูลโดยกระดาษ ซึ่งแต่ละ

^๑ บทความนี้เผยแพร่เมื่อวันที่ ๓๐ พฤศจิกายน พ.ศ. ๒๕๖๓ โดยสรุปข้อมูลจากบทความ How data residency laws can harm privacy, commerce and innovation and do little for national security จากเว็บไซต์ World Economic Forum สามารถเข้าถึงได้ที่นี้

<https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/>

^๒ บุคลากรจัดทำข้อมูลกฎหมาย ฝ่ายค้นคว้าและเปรียบเทียบกฎหมาย กองกฎหมายต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

^๓ “Cloud Computing คืออะไร?” กลุ่มภาระงานด้านเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์มหาวิทยาลัยขอนแก่น <http://sc2.kku.ac.th/office/sci-it/index.php/29-cloud-computing.html>

^๔ “จับตาธุรกิจ Cloud Computing รับเทรนด์ดิจิทัล Big Data เติบโต” ไทยรัฐออนไลน์ <https://www.thairath.co.th/news/business/stocks-gold/1941460>



บริษัทจะถูกตรวจสอบข้อมูลดังกล่าวเพื่อให้หน่วยงานด้านภาษีของรัฐใช้ประโยชน์จากข้อมูลชุดนี้ ขณะที่ปัจจุบันเป็นยุคของเทคโนโลยีดิจิทัลที่ข้อมูลจะถูกใช้เป็นตัวจักรสำคัญในการขับเคลื่อนเศรษฐกิจและสังคม

หลักการของกฎหมายถิ่นที่อยู่ของข้อมูล (Data residency laws) คือ การที่รัฐบาลกำหนดให้บริษัทต่าง ๆ ต้องจัดเก็บข้อมูลไว้ในดินแดนของประเทศนั้น ซึ่งโดยทั่วไปกฎหมายเกี่ยวกับถิ่นที่อยู่ของข้อมูลมุ่งเน้นไปที่ข้อมูลส่วนบุคคล (personal data) และอาจรวมถึงข้อมูลทางภูมิศาสตร์ของผู้ใช้คอมพิวเตอร์หรือเครื่องคอมพิวเตอร์ ซึ่งข้อมูลทั้งหมดดังกล่าวเป็นข้อมูลหลักสำหรับการดำเนินธุรกิจ (business needs)

ภายใต้หลักของกฎหมายถิ่นที่อยู่ของข้อมูล บริษัทต่าง ๆ จะต้องประมวลผลและจัดเก็บข้อมูลภายในอาณาเขตของดินแดนของรัฐนั้น ๆ และสามารถถ่ายโอนสำเนาของข้อมูลไปยังต่างประเทศได้ เฉพาะกรณีที่ได้ทำสำเนาเก็บไว้ในพื้นที่ที่รัฐนั้น ๆ สามารถตรวจสอบได้ หลักการดังกล่าวทำให้เกิดข้อห่วงกังวลประเด็นการละเมิดข้อมูลและความปลอดภัยในโลกไซเบอร์ ซึ่งแต่ละประเทศต้องการที่จะรักษาความปลอดภัยในการเข้าถึงข้อมูลในพื้นที่และการจำกัดการถ่ายโอนข้อมูลระหว่างประเทศ และโดยที่กฎหมายคุ้มครองความเป็นส่วนตัวของข้อมูลโดยทั่วไป (Data protection and privacy laws) กำหนดข้อจำกัดในการถ่ายโอนข้อมูล แต่ไม่ครอบคลุมถึงการกำหนดสถานที่เก็บรักษาข้อมูลเป็นการเฉพาะ โดยทั่วไปกำหนดให้บริษัทที่ครอบครองข้อมูลไม่จำเป็นต้องเก็บสำเนาข้อมูลและห้ามถ่ายโอนข้อมูลไปยังประเทศอื่น เว้นแต่จะพิสูจน์ได้ว่าตนมีความสามารถในการป้องกันและรับรองความปลอดภัยของข้อมูลที่จะถ่ายโอนได้อย่างเพียงพอ สิ่งดังกล่าวสะท้อนได้ว่าในความเป็นจริงนั้นกฎหมายคุ้มครองความเป็นส่วนตัวมีวัตถุประสงค์ที่ไม่ต้องการให้มีการเก็บสำเนาไว้ ณ ที่ใด

๒. ผลกระทบและข้อสังเกตจากกฎหมายถิ่นที่อยู่ของข้อมูล (Data residency law)

กฎหมายถิ่นที่อยู่ของข้อมูลอาจมีผลกระทบอย่างกว้างขวางในประเด็นต่าง ๆ ทั้งความเป็นส่วนตัว (privacy) ความมั่นคงปลอดภัยของรัฐ (national security) และในทางการค้า (commerce) ดังนี้

ประการแรก ประเด็นความเป็นส่วนตัว (privacy) และความปลอดภัยของข้อมูล (Data Security) ข้อมูลจากเว็บไซต์ World Economic Forum ได้ให้ข้อสังเกตว่ามาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลของแต่ละประเทศไม่ได้มีวัตถุประสงค์ในการกำหนดถิ่นที่อยู่ของข้อมูล ในขณะเดียวกัน ปริมาณข้อมูลที่ถูกจัดเก็บจำนวนมาก อาจทำให้เป็นช่องทางเข้าถึงและใช้ประโยชน์จากข้อมูลในระดับประเทศได้ ซึ่งจะเป็นการขัดขวางความเป็นส่วนตัวโดยแท้จริง เช่น หน่วยงานของรัฐอาจมีอำนาจในการบังคับให้บุคคลใดจัดเก็บหรือแสดงข้อมูลในพื้นที่ของตน นอกจากนี้ สำหรับประเทศที่เทคโนโลยียังไม่ก้าวหน้าอาจไม่สามารถปกป้องข้อมูลที่จัดเก็บไว้ในประเทศจากการคุกคามทางทหารและอาชญากรรมข้ามชาติได้ หรืออาจกล่าวได้ว่ากฎหมายถิ่นที่อยู่ของข้อมูลขัดแย้งกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล



ประการที่สอง ประเด็นความมั่นคงของชาติ (national security) บางประเทศได้พยายามจัดให้มีการตรวจสอบให้แน่ใจว่าการจัดเก็บข้อมูลต่าง ๆ ได้มีการระบุพิกัด (geolocation) ของสถานที่จัดเก็บข้อมูลไว้ภายในประเทศ เพื่อประโยชน์ด้านความมั่นคงของชาติ และลดความกังวลเรื่องความสามารถในการเข้าถึงข้อมูลที่แตกต่างที่อาจนำไปสู่ความขัดแย้ง

ประการที่สาม ประเด็นด้านการค้า (Commerce) มีข้อสังเกตว่าโดยพื้นฐานแล้ว กฎหมายถิ่นที่อยู่ของข้อมูลจะกระทบโดยตรงต่อการค้าระหว่างประเทศซึ่งเป็นผลมาจากการให้สิทธิแก่บริษัทท้องถิ่นมากกว่าบริษัทคู่แข่งจากต่างประเทศ บริษัทท้องถิ่นสามารถปฏิบัติตามข้อกำหนดเกี่ยวกับถิ่นที่อยู่ของข้อมูลได้โดยง่ายกว่าคู่แข่งจากต่างประเทศที่มักจะเก็บข้อมูลไว้ที่สำนักงานใหญ่ที่มีสถานที่ที่แตกต่างกัน ซึ่งในระยะสั้นข้อกำหนดในลักษณะนี้จะเป็นประโยชน์ต่อการคุ้มครองข้อมูลและเป็นการอำนวยความสะดวกแก่บริษัทท้องถิ่น แต่ในระยะยาวอาจกระทบต่อความสามารถในการแข่งขันของบริษัทที่มีความต้องการที่จะแข่งขันในระดับระหว่างประเทศ นอกจากนี้ หากมีการใช้บังคับกฎหมายว่าด้วยถิ่นที่อยู่ของข้อมูลอย่างเข้มข้นอาจเป็นอุปสรรคต่อการเข้าสู่ตลาดของธุรกิจต่างชาติที่ต้องการหลีกเลี่ยงภาษีและค่าใช้จ่ายการดำเนินการเกี่ยวกับถิ่นที่อยู่ของข้อมูลซึ่งเป็นผลมาจากการใช้บังคับกฎหมายว่าด้วยถิ่นที่อยู่ของข้อมูลของประเทศคู่ค้าได้

นอกจากนั้น มีข้อสังเกตว่าการตรากฎหมายถิ่นที่อยู่ของข้อมูลอาจกำหนดให้บริษัทข้ามชาติต้องลงทุนจัดตั้งศูนย์ข้อมูลในพื้นที่ท้องถิ่นของประเทศนั้น ๆ ซึ่งอาจนำมาสู่ความเสี่ยงที่เกี่ยวข้องกับการทุจริตภาครัฐ

ประการสุดท้าย โดยทั่วไปแล้ว ข้อมูลส่วนบุคคลที่บริษัทได้เก็บรวบรวมไว้เพื่อใช้ประโยชน์ในทางการค้า ไม่มีไว้เพื่อวัตถุประสงค์ด้านความมั่นคงของรัฐ ซึ่งการดำเนินการในเรื่องดังกล่าวจะต้องคำนึงถึงการเคารพสิทธิความเป็นส่วนตัวและเสรีภาพของประชาชน จึงนำมาสู่ข้อคิดเห็นที่ว่า การดำเนินการเกี่ยวกับเรื่องดังกล่าวของรัฐควรกำหนดให้บริษัทที่ใช้ข้อมูลในการดำเนินกิจการจะต้องรับรองความปลอดภัยในการเข้าถึงข้อมูลจากระยะไกล (ไม่ว่าจะจัดเก็บไว้ที่ใด) หรือเก็บสำเนาสำรองไว้ในรัฐนั้น ๆ เพื่อวัตถุประสงค์ในการตรวจสอบและการรักษาความปลอดภัยในการเข้าถึงข้อมูลโดยรัฐ โดยเฉพาะประเทศที่มีความจำเป็นที่ต้องสนับสนุนอุตสาหกรรมดิจิทัล และต้องการดึงดูดการลงทุนโดยตรงจากต่างประเทศ จะต้องพิจารณาการใช้บังคับกฎหมายว่าด้วยถิ่นที่อยู่ของข้อมูลอย่างเหมาะสมเพื่อให้เกิดประโยชน์แก่ประชาชนของประเทศตนในทุกมิติ
