ปัญญาประดิษฐ์กับการคุ้มครองข้อมูลส่วนบุคคลในทางการแพทย์ : กรณีศึกษาสาธารณรัฐประชาชนจีน

ที่มา: https://med-tech.world/news/china-worlds-first-ai-hospital-milestone-in-healthcare-innovation/

นโยบายและทิศทางการกำกับดูแลเกี่ยวกับการใช้ปัญญาประดิษฐ์ในทางการแพทย์ของประเทศจีน

๑. การพัฒนาทางนโยบายที่เกี่ยวข้องกับการใช้ปัญญาประดิษฐ์ในทางการแพทย์[๑]

จีนได้ริเริ่มนโยบายด้านปัญญาประดิษฐ์ตั้งแต่ปี ค.ศ. ๒๐๐๙ โดยแบ่งเป็นนโยบายหลักหกด้าน ได้แก่ ๑) “made in China[๒]” ๒) การพัฒนาเพื่อขับเคลื่อนด้านนวัตกรรม (innovation-driven development) ๓) IoT[๓] ๔) อินเทอร์เน็ต ๕) การจัดทำฐานข้อมูลขนาดใหญ่ (big data) และ ๖) การวิจัยและพัฒนาด้านวิทยาศาสตร์และเทคโนโลยี (scientific and technological R&D) ต่อมาในเดือนกรกฎาคม ค.ศ. ๒๐๑๕ คณะมุขมนตรี (The State Council) ซึ่งเป็นโครงสร้างหลักของรัฐบาลภายใต้พรรคคอมมิวนิสต์จีนได้เสนอแนวทางและข้อคิดเห็นในการพัฒนาการใช้อินเทอร์เน็ต “Guiding Opinions on Vigorously Advancing the “Internet+”Action” ซึ่งให้ความสำคัญกับปัญญาประดิษฐ์ในฐานะภารกิจหลักที่สำคัญประการหนึ่ง นอกจากนี้ ยังมีแผนงานด้านการพัฒนาระหว่างประเทศในด้านวิทยาศาสตร์ เทคโนโลยี และนวัตกรรม “The 13th Five-Year National Science and Technology Innovation Plan” ตลอดจนแผนงาน/โครงการขนาดใหญ่ด้านวิทยาศาสตร์ เทคโนโลยี และนวัตกรรม

---

[๑] Innovation Centre Denmark Ministry of Foreign Affairs of Denmark Report by Innovation Centre Denmark, “China AI healthcare”, 2020, หน้า ๔-๕, สืบค้นเมื่อ ๑๙ ธันวาคม ๒๕๖๗, จาก https://icdk.dk/-/media/websites/icdk/locations-reports/shanghai/2020_ai-healthcare-report.ashx

[๒] ยุทธศาสตร์ “Made in China 2025 (MIC 2025)” มีเป้าหมายเพื่อปรับเปลี่ยนแนวทางการผลิตของจีนเพื่อเป็น “แหล่งผลิตสินค้าอุตสาหกรรมที่มีการใช้เทคโนโลยีขั้นสูง”

[๓] คำว่า IoT หรืออินเทอร์เน็ตในทุกสิ่ง (Internet of Things) หมายถึง เครือข่ายรวมของอุปกรณ์ที่เชื่อมต่อถึงกันและเทคโนโลยีที่อำนวยความสะดวกในการสื่อสารระหว่างอุปกรณ์กับระบบคลาวด์ ตลอดจนระหว่างอุปกรณ์ด้วยกันเอง, https://aws.amazon.com/th/what-is/iot/

2030 “Mega projects for Science and Technology Innovation 2030” ซึ่งดำเนินการครอบคลุมทั้งเรื่องฐานข้อมูลขนาดใหญ่ อุตสาหกรรมที่เกี่ยวกับระบบอัจฉริยะ และหุ่นยนต์ด้วย

ในเดือนกรกฎาคม ค.ศ. ๒๐๑๗ คณะมุขมนตรีได้เผยแพร่แผนพัฒนายุคใหม่ในการใช้ปัญญาประดิษฐ์ “Development Plan on the New Generation of Artificial Intelligence” ซึ่งทำให้ปัญญาประดิษฐ์กลายเป็นยุทธศาสตร์ระดับชาติ และในเดือนพฤศจิกายนปีเดียวกัน กระทรวงวิทยาศาสตร์และเทคโนโลยีได้ยกระดับการพัฒนาเพื่อรองรับยุทธศาสตร์ดังกล่าวโดยการตั้งคณะกรรมการที่ปรึกษาซึ่งประกอบด้วยผู้เชี่ยวชาญด้านการศึกษาและภาคเอกชนที่มีชื่อเสียง เช่น Baidu Alibaba Tencent iFlytek Horizon Robotics และในเดือนธันวาคม กระทรวงอุตสาหกรรมและเทคโนโลยีสารสนเทศได้เผยแพร่แผนงาน “Three-Year Action Plan for Bolstering the Development of the Next-Generation Artificial Intelligent Industry” เพื่อส่งเสริมและสนับสนุนให้จีนเป็นผู้นำระดับโลกด้านอุตสาหกรรมเกี่ยวกับปัญญาประดิษฐ์ ต่อมาในเดือนเมษายน ค.ศ. ๒๐๑๘ สำนักงานกลางสภาแห่งรัฐของสาธารณรัฐประชาชนจีน (General Office of the State Council) ได้เสนอข้อคิดเห็นเพื่อสนับสนุนการพัฒนาอินเทอร์เน็ตเพื่อนำมาใช้กับการรักษาสุขภาพ “Internet plus Health Care” อีกทั้งยังมีข้อแนะนำต่าง ๆ เพื่อให้สถาบันด้านการแพทย์และสาธารณสุขนำไปใช้เพื่อช่วยยกระดับการใช้อินเทอร์เน็ตและเทคโนโลยีสารสนเทศเพื่อขยายการให้บริการด้านการแพทย์และสาธารณสุข รวมทั้งสร้างระบบการให้บริการโดยบูรณการทั้งการให้บริการแบบที่ต้องเชื่อมต่อกับเครือข่ายและที่ไม่ต้องเชื่อมต่อกับเครือข่าย (online/offline) ให้ครอบคลุมทุกกระบวนการด้านการแพทย์และสาธารณสุข นอกจากนี้ สถาบันด้านการแพทย์และสาธารณสุขยังสร้างความร่วมมือกับผู้ประกอบการอินเทอร์เน็ตเพื่อสร้างแหล่งข้อมูลด้านสุขภาพโดยใช้ฐานข้อมูลขนาดใหญ่ซึ่งใช้ในการคาดการณ์ข้อมูลทางระบาดวิทยา (epidemiological) และเพิ่มประสิทธิภาพมาตรการเฝ้าระวังโรคติดต่อ ตลอดจนการนำปัญญาประดิษฐ์มาใช้ในทางการแพทย์ เช่น การวิเคราะห์ข้อมูลคนไข้เบื้องต้น (intelligent medical image recognition) การจำแนกทางพยาธิวิทยาซึ่งรวมศาสตร์ต่าง ๆ เข้าด้วยกันเพื่อให้คำปรึกษาแก่ผู้ป่วย (pathological classification and multidisciplinary consultation) ด้วยการพัฒนาระบบ “Internet plus” เพื่อใช้ในการให้บริการทางการแพทย์และสาธารณสุข การพัฒนาโรงพยาบาลอินเทอร์เน็ต (Internet hospitals) ซึ่งอยู่ภายใต้สถาบันด้านการแพทย์และสาธารณสุขจึงถูกอนุญาตให้ดำเนินการได้ โดยสถาบันด้านการแพทย์และสาธารณสุขสามารถใช้ชื่อโรงพยาบาลอินเทอร์เน็ตเป็นชื่อที่สองได้ “second name” และในการให้การรักษาผู้ป่วย แม้จะเป็นการให้บริการโดยโรงพยาบาล (real hospital) แต่ก็สามารถรักษาโรคทั่วไป (chronic diseases) และโรคเรื้อรัง (chronic diseases) ผ่านทางออนไลน์ได้เช่นกัน

ในเดือนกันยายน ค.ศ. ๒๐๑๘ คณะกรรมการสุขภาพแห่งชาติ (the National Health Commission (NHC)) ได้กำหนดมาตรการการบริหารจัดการสำหรับการใช้อินเทอร์เน็ตในการตรวจวินิจฉัยและการรักษา (Measures for the Administration of Internet) มาตรการการบริหารจัดการโรงพยาบาลอินเทอร์เน็ต ข้อกำหนดการให้บริการการแพทย์ทางไกล ซึ่งทั้งสามมาตรการอยู่ในช่วงทดลองการใช้งาน (For Trial Implementation) และยังมีคำอธิบายเกี่ยวกับการใช้อินเทอร์เน็ตในการวินิจฉัยโรค และเพื่อที่จะยกระดับมาตรฐานการให้บริการด้วยระบบดิจิทัลโดยโรงพยาบาล ในเดือน

มีนาคม ค.ศ. ๒๐๑๙ จีนได้นำระบบการให้บริการทางการแพทย์อัจฉริยะ (a smart medical service grading system) มาใช้สำหรับการพัฒนาโรงพยาบาลอัจฉริยะ (smart hospitals) โรงพยาบาลอัจฉริยะดังกล่าวจะมีข้อมูลการให้บริการซึ่งรวมถึงข้อมูลทางการรักษาของผู้ป่วย ระบบการลงทะเบียน เป็นต้น ในภาพรวมการดำเนินการของประเทศ เมืองต่าง ๆ ในประเทศจีนได้ริเริ่มการพัฒนา รวมทั้งกำหนดนโยบายและแผนงานด้านปัญญาประดิษฐ์ของตนเอง เช่น เมืองปักกิ่งมีแผนงานที่พัฒนา “AI development park” รองรับบริษัทผู้ประกอบการด้านปัญญาประดิษฐ์ได้ถึง ๔๐๐ แห่ง เมืองเซี่ยงไฮ้มีนโยบายในการให้การอุดหนุนพิเศษ (a special fund) แก่กิจการปัญญาประดิษฐ์ เช่นเดียวกับเมืองหังโจวที่มีการพัฒนา “AI park” และมีการให้เงินอุดหนุน (fund)

นอกจากนี้ จีนยังมีนโยบายด้านสุขภาพ ที่เรียกว่า “Healthy China 2030”[๔] ซึ่งเป็นแผนระดับชาติระยะกลางและระยะยาวที่เป็นยุทธศาสตร์สำคัญของประเทศในด้านสุขภาพ อันเนื่องมาจากแนวคิดที่ว่า สุขภาพมีผลต่อปัจจัยหลายอย่างในวิถีชีวิตของผู้คน เช่น กรรมพันธุ์ (hereditary) สภาพแวดล้อม บริการทางการแพทย์ นโยบายดังกล่าวจึงประกอบไปด้วยวัตถุประสงค์หลักที่หวังผลระยะยาวในเป้าหมายด้านสุขภาพ (health) ความปลอดภัยด้านอาหาร (food safety) ตลอดจนแหล่งน้ำและสิ่งแวดล้อม ซึ่งเป้าหมายเหล่านี้จะต้องบรรลุภายในปี ค.ศ. ๒๐๓๐ โดยมียุทธศาสตร์และเป้าหมาย สรุปได้ดังนี้

(๑) การพัฒนาสุขภาพของประชาชนในประเทศอย่างต่อเนื่อง

(๒) ความเสี่ยงด้านสุขภาพในเรื่องต่าง ๆ จะต้องอยู่ในระดับที่สามารถควบคุมได้อย่างมีประสิทธิภาพ

(๓) เพิ่มศักยภาพด้านการให้บริการทางการแพทย์และสาธารณสุข (Healthcare service delivery)

(๔) การขยายตัวของอุตสาหกรรมด้านสุขภาพอย่างมีนัยสำคัญ

(๕) การพัฒนาการจัดโครงสร้างสถาบันเพื่อทำหน้าที่สนับสนุนด้านสุขภาพ

สำหรับแนวทางการดำเนินงานเพื่อเสริมสร้างให้ประชาชนในประเทศมีสุขภาพที่ดี ให้ดำเนินการตามแนวทางดังนี้

(๑) การรณรงค์ให้ประชาชนในประเทศมีความใส่ใจในสุขภาพ

(๒) การจัดการที่เข้มแข็งเกี่ยวกับปัญหาต่าง ๆ ที่ส่งผลกระทบต่อสุขภาพ

(๓) การทำให้เกิดความมั่นคงและความปลอดภัยทางอาหารและยา

(๔) การพัฒนาระบบความปลอดภัยสาธารณะ

นอกจากนี้ นโยบายดังกล่าวยังให้ความสำคัญกับการลดมลภาวะและการรักษาคุณภาพของสิ่งแวดล้อม การควบคุมการปล่อยของเสียของภาคอุตสาหกรรม การมีกลไกกำกับดูแลเรื่องสิ่งแวดล้อมควบคู่กับสุขภาพที่ดี และการจัดให้มีการสำรวจและประเมินความเสี่ยงด้านสิ่งแวดล้อม

---

[๔]FAOLEX Database Food and Agriculture Organization of the United Nation, “Outline of the Healthy China 2030 Plan”, สืบค้นเมื่อ ๑๙ ธันวาคม ๒๕๖๗, จาก https://www.fao.org/faolex/results/details/en/c/LEX-FAOC175038/

๒. ความสำคัญของข้อมูลส่วนบุคคลในทางการแพทย์และข้อพิจารณาเรื่องการให้ความคุ้มครอง[๕]

แนวคิดของความเป็นส่วนตัวหรือส่วนบุคคล (privacy) มีลักษณะที่ละเอียดอ่อนและขึ้นอยู่กับบริบทด้านวัฒนธรรม ดังนั้น จึงมีความจำเป็นที่จะต้องศึกษาถึงบรรทัดฐานและประวัติศาสตร์ของแต่ละประเทศเพื่อนำมาประกอบการพิจารณาและทำความเข้าใจเกี่ยวกับการจัดทำกฎหมายและการจัดการด้านข้อมูลทางการแพทย์และสาธารณสุข จีนเป็นประเทศที่ให้ความสำคัญกับการรวมกลุ่ม (collectivism) ในฐานะเป็นศูนย์รวมด้านคุณธรรม ทั้งยังให้ความสำคัญกับครอบครัวและชุมชน ซึ่งมีอิทธิพลมากยิ่งกว่าความเป็นปัจเจกบุคคล วัฒนธรรมดังกล่าวนี้ส่วนหนึ่งย่อมส่งผลให้คำอธิบายเกี่ยวกับสิทธิส่วนบุคคล (right to privacy) ในประเทศจีนมีมุมมองที่เป็นพลวัต (dynamic outlook) กล่าวคือ แม้จะให้ความเคารพต่อศักดิ์ศรีของความเป็นมนุษย์ในฐานะคุณค่าของปัจเจกบุคคล แต่ก็ต้องให้ความสำคัญกับผลประโยชน์หรือความต้องการของสังคมส่วนรวมด้วย สำหรับบริบทเรื่องการให้บริการด้านการแพทย์และสาธารณสุข แม้ประเทศจีนจะให้ความสำคัญกับข้อมูลส่วนบุคคลของผู้ป่วย แต่ก็ยังมีปัญหาและอุปสรรคใหญ่เรื่องความไม่สมดุลในการจัดสรรทรัพยากร (imbalance in resource allocation) และการขาดแคลนแพทย์ที่มีประสิทธิภาพ (a shortage of quality physicians) นอกจากนี้ ผู้ป่วยโดยส่วนใหญ่มักเลือกไปรักษาตัวที่โรงพยาบาลในตัวเมืองขนาดใหญ่ที่มีประสิทธิภาพสูง (high-level hospitals in big cities) ซึ่งเป็นโรงพยาบาลชั้นนำที่มีปริมาณผู้ป่วยหนาแน่น และไม่ถือว่าเป็นเรื่องที่ผิดปกติ หากจะพบเห็นผู้ป่วยสองถึงสามรายนั่งอยู่ด้วยกันในห้องตรวจขณะที่เข้าพบเพื่อขอคำปรึกษาและรับการรักษาจากแพทย์ ตัวอย่างที่กล่าวอ้างนี้มิได้หมายความว่า ผู้ป่วยในประเทศจีนไม่คำนึงถึงหรือไม่ให้ความสำคัญกับสิทธิความเป็นส่วนตัว แต่กลับแสดงให้เห็นว่าภายใต้สถานการณ์เช่นนั้น ผู้ป่วยจำเป็นต้องเลือกระหว่างการรักษาไว้ซึ่งความเป็นส่วนตัวกับการเข้าถึงบริการด้านการแพทย์และสาธารณสุขอย่างทันท่วงที (timely) ดังนั้น ประเด็นเรื่องการจัดสรรทรัพยากรที่เหมาะสม ตลอดจนการจัดการข้อมูลที่ใช้ในทางการแพทย์และสาธารณสุขที่จะต้องสร้างความสมดุลระหว่างการแบ่งปันข้อมูลด้านสุขภาพกับการให้ความคุ้มครองผลประโยชน์ขั้นพื้นฐานของปัจเจกบุคคลจึงเป็นความท้าทายในยุคแห่งการขับเคลื่อนด้วยข้อมูลด้านสุขภาพในประเทศจีน

จากสภาพปัญหาที่ต้องเผชิญในการเข้าถึงบริการด้านการแพทย์และสาธารณสุขและจำนวนประชากรของประเทศ ทำให้จีนมีความจำเป็นที่จะต้องนำนวัตกรรมต่าง ๆ มาใช้ในบริบทด้านการแพทย์และสาธารณสุข และจากความก้าวหน้าด้านเทคโนโลยีอินเทอร์เน็ต ทำให้จีนได้พัฒนานวัตกรรมด้านสุขภาพโดยการนำฐานข้อมูลขนาดใหญ่ด้านสุขภาพมาใช้เพื่อสร้างสรรค์ผลิตภัณฑ์สุขภาพรูปแบบใหม่ผ่านการให้บริการทางโทรศัพท์มือถือ “Mobile health (mHealth)” การให้บริการดังกล่าวเป็นตัวอย่างของการใช้นวัตกรรมดิจิทัลในทางการแพทย์และสาธารณสุข ซึ่งอาศัยก้าวหน้าทางเทคโนโลยีในการส่งผ่านข้อมูลทางไกล ทำให้ mHealth มีส่วนในการผลักดันให้การดูแลรักษาสุขภาพขยายวง

---

[๕] Sun, L. (2022). “ Health data governance in China: Emphasizing ‘sharing’ and ‘protection’ based on the right to health”, Medical Law International, 23(1) 26-43, หน้า ๑-๕, สืบค้นเมื่อ ๑๙ ธันวาคม ๒๕๖๗, จาก https://doi.org/10.1177/09685332221140416

กว้างขวางมากกว่าที่เคยเป็นมา และแม้ว่าความตื่นตัวด้านนวัตกรรมดิจิทัลจะได้รับผลตอบรับที่ดีทั้งจากภาครัฐและภาคเอกชน แต่ในอีกแง่มุมหนึ่ง กลับก่อให้เกิดข้อกังวลเกี่ยวกับข้อมูลส่วนบุคคลในทางการแพทย์ (medical privacy) และความชอบธรรมในการนำข้อมูลด้านสุขภาพไปใช้ เนื่องจากเรื่องดังกล่าวมีความเกี่ยวข้องกับผู้มีส่วนได้เสียหลายฝ่าย เช่น ผู้ป่วย หน่วยงานภาครัฐ บริษัทผู้ประกอบการด้านเทคโนโลยี และรัฐบาล จึงอาจกล่าวได้ว่า การนำข้อมูลไปใช้อีกครั้ง (reuse) และการแบ่งปันข้อมูล (sharing) ด้านสุขภาพทำให้ข้อมูลส่วนบุคคลถูกนำไปใช้ในทางที่ไม่ถูกต้อง (abuse of personal data) ด้วยเหตุนี้ จึงเป็นที่มาของการแสดงข้อคิดเห็นต่าง ๆ อันนำไปสู่การปรับปรุงแก้ไขกฎหมายเพื่อที่จะให้การนำข้อมูลด้านสุขภาพไปใช้เป็นไปโดยสะดวก มีความเหมาะสม ในขณะเดียวกันก็ต้องให้ความคุ้มครองแก่ปัจเจกบุคคลเพื่อป้องกันมิให้เกิดความเสี่ยงในการนำข้อมูลไปใช้ในทางที่ผิดหรือไม่เหมาะสม (the risk of data misuse) ข้อกังวลเกี่ยวกับการใช้ข้อมูลในทางที่ผิดหรือไม่เหมาะสมเป็นหัวข้อที่ได้รับความสนใจอย่างยิ่งในด้านการแพทย์และสาธารณสุขในประเทศจีน โดยเฉพาะอย่างยิ่งในช่วงเวลาที่มีการขยายตัวอย่างรวดเร็วของอุตสาหกรรม mHealth และโรงพยาบาลอินเทอร์เน็ต ในปี ค.ศ. ๒๐๒๑ อันมีเหตุผลสำคัญประการหนึ่งมาจากการแพร่ระบาดของโรคโควิด-๑๙ นอกจากนี้ บริษัทผู้ประกอบการด้านเทคโนโลยีขนาดใหญ่ยังเร่งขยายธุรกิจที่เกี่ยวข้องกับการให้บริการด้านสุขภาพผ่านระบบดิจิทัลโดยการสร้างผลิตภัณฑ์ใหม่ ๆ ซึ่งรวมถึงระบบให้บริการเบ็ดเสร็จจุดเดียวผ่านแพลตฟอร์มเสมือนจริง (one-stop virtual care platforms) ระบบจัดเก็บและรับส่งข้อมูลภาพทางการแพทย์บนคลาวด์ (cloud- based medical image diagnoses) และการใช้ปัญญาประดิษฐ์ในการคัดกรองผู้ป่วย (artificial intelligence-assisted screenings) อีกทั้งภาคธุรกิจยังเล็งเห็นประโยชน์ที่จะทำกำไรจากปริมาณข้อมูลจำนวนมากที่ได้รับจากการให้การบริการด้านสินค้าและบริการแก่ลูกค้าที่เข้าถึงการให้บริการผ่านระบบออนไลน์หรือระบบดิจิทัล ด้วยเหตุนี้ การปฏิบัติต่อข้อมูลทางการแพทย์และสาธารณสุขในลักษณะที่เป็นผลิตภัณฑ์หรือสินค้าที่นำมาซื้อขายกันได้ (a tradable commodity) จึงส่งผลให้เกิดความเหลื่อมล้ำ (disparities) และอีกนัยหนึ่งย่อมเป็นอุปสรรคในการเข้าถึงบริการด้านการแพทย์และสาธารณสุขอย่างเท่าเทียม และยังทำให้ข้อมูลส่วนบุคคลทางการแพทย์ของผู้ป่วยมีแนวโน้มที่จะถูกเข้าถึงและละเมิดได้โดยง่าย เนื่องจากประชาชนอยู่ในสถานะที่ด้อยกว่าและไม่มีอำนาจในการเจรจาต่อรองเมื่อเทียบกับผู้ให้บริการภาคเอกชน

องค์การอนามัยโลก (WHO) ให้ความสำคัญและมีมุมมองที่น่าสนใจเกี่ยวกับการใช้ปัญญาประดิษฐ์ว่าจะมีบทบาทสำคัญและมีศักยภาพสูงในการให้บริการทางการแพทย์และสาธารณสุข โดยปัญญาประดิษฐ์ถูกนำมาใช้ในทางการแพทย์ในหลายรูปแบบ เช่น การตรวจพบโรคและการวินิจฉัยโรค (disease detection and diagnosis) การสร้างภาพทางการแพทย์ (medical imaging) การรักษาทางการแพทย์และการให้ยาในปริมาณที่เหมาะสมแก่ผู้ป่วยแบบจำเพาะต่อบุคคล (personalized disease treatment) การพัฒนายา (drug development) และในส่วนระบาดวิทยา (epidemiological) และการสาธารณสุข ปัญญาประดิษฐ์ถูกนำมาใช้ในการเฝ้าระวังโรค (disease surveillance) การตอบสนองต่อการระบาดของโรค (outbreak response) และการบริหารจัดการระบบสาธารณสุข ในขณะเดียวกันการใช้ปัญญาประดิษฐ์ย่อมทำให้เกิดความเสี่ยงในมุมมองด้านสิทธิมนุษยชนและจริยธรรมวิชาชีพแพทย์ (medical ethics) เช่น การใช้ปัญญาประดิษฐ์ส่งผลให้สิทธิความเป็นส่วนตัวถูกคุกคาม กระทบต่อการตัดสินใจและศักดิ์ศรีความเป็นมนุษย์ อคติของปัญญาประดิษฐ์ (algorithmic

discrimination) เนื่องจากเป็นการพัฒนาจากการให้ข้อมูลของมนุษย์จึงก่อให้เกิดความไม่เท่าเทียมในด้านต่าง ๆ เช่น เชื้อชาติ อายุ เพศสภาพ ด้วยเหตุนี้ การนำปัญญาประดิษฐ์มาใช้ในทางการแพทย์จึงทำให้เกิดข้อกังวลและคำถามต่อแนวทางในการจัดการที่เหมาะสมเพื่อคุ้มครองสิทธิส่วนบุคคลของผู้ป่วย (the protection of patient privacy rights) เพราะหากสิทธิส่วนบุคคลของผู้ป่วยไม่ได้รับความคุ้มครองแล้ว ย่อมเกิดผลร้ายต่าง ๆ ตามมา เช่น การกีดกันในการจ้างงาน (employment discrimination) ค่าใช้จ่ายที่เพิ่มขึ้นสำหรับการรักษาในระยะยาว สำหรับในประเทศจีนการใช้ปัญญาประดิษฐ์ในทางการแพทย์มีความก้าวหน้าอย่างรวดเร็ว โดยตั้งแต่ช่วงปี ค.ศ. ๒๐๒๐ เป็นต้นมา ผลิตภัณฑ์ต่าง ๆ ที่พัฒนาขึ้นโดยอุตสาหกรรมปัญญาประดิษฐ์ในทางการแพทย์ของจีนได้รับการรับรองจากหน่วยงานภาครัฐที่เรียกว่า “National Medical Products Administration (NMPA)” ซึ่งภายใต้การรับรอง Class III classification ทำให้ผลิตภัณฑ์ต่าง ๆ ได้รับประโยชน์ เช่น ผลิตภัณฑ์ที่ใช้กับการศัลยกรรมกระดูก (orthopedics) จักษุวิทยา (ophthalmology) ระบบหัวใจและหลอดเลือด (cardiovascular system) และระบบทางเดินหายใจ (respiratory system) โดยมูลค่าทางการตลาดสำหรับการใช้ปัญญาประดิษฐ์ในทางการแพทย์ของจีนคาดการณ์ว่าจะมีมูลค่ามากกว่า 4.5 billion USD ในปี ค.ศ. ๒๐๒๕ ซึ่งการนำปัญญาประดิษฐ์มาใช้ในทางการแพทย์และสาธารณสุขถือเป็นนโยบายที่รัฐบาลจีนให้ความสำคัญเป็นอย่างยิ่ง ดังเช่นนโยบายที่เรียกว่า “Healthy China 2030” ซึ่งได้กล่าวไว้แล้วในหัวข้อข้างต้น โดยนโยบายดังกล่าววางเป้าหมายที่จะส่งเสริมและสนับสนุนการใช้เทคโนโลยีสารสนเทศและฐานข้อมูลขนาดใหญ่ในระบบสาธารณสุขของประเทศ ซึ่งการใช้ปัญญาประดิษฐ์ในทางการแพทย์ถือเป็นกลไกสำคัญประการหนึ่งในการขับเคลื่อนนโยบายดังกล่าว อย่างไรก็ดี เมื่อพิจารณามุมมองในด้านสิทธิส่วนบุคคลในประวัติศาสตร์ที่ผ่านมาของประเทศจีน ประเด็นดังกล่าวมักจะถูกละเลยหรือให้ความสำคัญน้อย (underrated) ส่งผลให้กฎหมาย ตลอดจนกฎระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับสิทธิส่วนบุคคลของประเทศจีนไม่เป็นไปในทิศทางเดียวกัน (fragmented) ขาดความชัดเจน (vague) และบังคับใช้ได้อย่างไม่มีประสิทธิภาพมากนัก (poorly enforced) และมักจะมีเหตุการณ์ที่มีการละเมิดสิทธิส่วนบุคคลเกิดขึ้นบ่อยครั้ง โดยเฉพาะการละเมิดในข้อมูลทางการแพทย์ซึ่งทำให้ผู้คนขาดความเชื่อมั่นต่อกระบวนการจัดการด้านข้อมูล สิ่งเหล่านี้ส่วนหนึ่งเป็นผลมาจากวัฒนธรรมของประเทศจีนเองที่ประเด็นเรื่องสิทธิส่วนบุคคลถูกให้ความสำคัญน้อยกว่าหรือต้องหลีกทางให้แก่ (subservient) เรื่องของส่วนรวม (social goals) และถือเป็นอุปสรรคสำคัญในการพัฒนาการใช้ปัญญาประดิษฐ์ในทางการแพทย์ของจีนอย่างยั่งยืน[๖]

[๖]Wang, C.; Zhang, J.; Lassi, N.; Zhang, X., “ Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective”, Healthcare 2022. 10. 1878, หน้า ๑-๒, สืบค้นเมื่อ ๑๙ ธันวาคม ๒๕๖๗, จาก https://doi.org/10.3390/healthcare10101878

๓. สถานการณ์ที่เกิดขึ้นกับข้อมูลทางการแพทย์และสาธารณสุขในประเทศจีนและการกำกับดูแล[๗]

นับแต่ศตวรรษที่ ๒๑ เป็นต้นมา การใช้ปัญญาประดิษฐ์ในประเทศจีนมีความก้าวหน้าเป็นอย่างมากโดยเฉพาะในวงการด้านการแพทย์และสาธารณสุข ซึ่งการนำปัญญาประดิษฐ์มาใช้เป็นระบบผู้ช่วยแพทย์ (The Clinical Decision Support System (CDSS)) ถือว่ามีการเติบโตมากที่สุด ในขณะเดียวกันการพัฒนาอย่างรวดเร็วของเทคโนโลยีทางการแพทย์ย่อมก่อให้เกิดความเสี่ยงต่อการนำข้อมูลทางสุขภาพต่าง ๆ มาใช้โดยไม่ชอบ โดยในปี ค.ศ. ๒๐๒๐ ได้มีการรายงานข้อมูลความปลอดภัยของการใช้อินเทอร์เน็ตในประเทศจีนโดย the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) จากรายงานดังกล่าวพบว่า ได้มีการส่งต่อการสร้างภาพทางการแพทย์ (medical imaging) มากกว่า ๔.๙๗ ล้านครั้งในปี ค.ศ. ๒๐๒๐ มีความเกี่ยวข้องกับบัญชีผู้ใช้ภายในประเทศ ๓,๓๔๗ บัญชี ทั้งนี้ การสร้างภาพทางการแพทย์มีไฟล์ขนาดใหญ่และเต็มไปด้วยข้อมูลส่วนบุคคลของผู้ป่วยซึ่งยังไม่ได้ดำเนินการเพื่อลด ปรับเปลี่ยน หรือซ่อนข้อมูลที่มีความละเอียดอ่อน (without desensitization) ทำให้ภาพของผู้ป่วยเกือบ ๔๐๐,๐๐๐ คน ถูกนำมาเผยแพร่ทั่วทั้งประเทศ การกระทำเหล่านี้เป็นการใช้ข้อมูลส่วนบุคคลโดยไม่ชอบและกระทบต่อสิทธิความเป็นส่วนตัวของบุคคล ทำให้จีนต้องเร่งดำเนินการโดยเร่งด่วนเพื่อพัฒนาให้มีระบบที่สร้างความมั่นคงและปลอดภัยในการคุ้มครองข้อมูลส่วนบุคคล

การกำกับดูแลข้อมูลส่วนบุคคลโดยส่วนใหญ่ในประเทศจีนจะอาศัยความร่วมมือจากหน่วยงานด้านกิจการทางอวกาศ (the Cyberspace Administration of China (CAC)) หน่วยงานด้านความมั่นคง (the Public Security Department) หน่วยงานด้านเทคโนโลยีสารสนเทศ (Industry and Information Department) เป็นต้น โดย CAC ร่วมกับ the China Cyberspace Security Association จะเป็นผู้รับผิดชอบดูแลแพลตฟอร์มเพื่อรับเรื่องร้องเรียนผ่านทางโทรศัพท์มือถือและระบบคอมพิวเตอร์เกี่ยวกับการใช้ข้อมูลส่วนบุคคล โดยเฉพาะในประเด็นที่มีการละเมิดต่อกฎหมาย กฎระเบียบ หรือข้อบังคับต่าง ๆ โดยในปี ค.ศ. ๒๐๒๑ มีการร้องเรียนเกี่ยวกับการใช้ข้อมูลส่วนบุคคลโดยไม่ชอบผ่านช่องทางต่าง ๆ มากกว่า ๒๐,๐๐๐ เรื่อง นอกจากนี้ ยังมีการร้องเรียนผ่านทางสื่อต่าง ๆ อีกมากมาย และภายในปีเดียวกัน “หน่วยงานด้านความมั่นคงของจีน (China’s public security authorities) ได้ปล่อยแคมเปญ “Clean Network 2021” เพื่อจัดการกับการละเมิดและการใช้ข้อมูลส่วนบุคคลโดยไม่ชอบเป็นการเฉพาะ ซึ่งในระยะแรก ถือว่าได้รับผลตอบรับที่ดีและข้อร้องเรียนมากกว่า ๙,๘๐๐ เรื่อง ได้รับการแก้ไข สำหรับคดีที่มีข้อพิพาทสู่ศาล ศาลฎีกาของจีน (China’s Supreme People’s Court) ได้รวบรวมและจัดทำข้อมูลรายงานประจำปีสรุปได้ว่า ในปี ค.ศ. ๒๐๒๑ มีคดีที่เกี่ยวข้องกับอาชญากรรมด้านข้อมูลส่วนบุคคล ๔,๐๙๘ คดี และมีปริมาณคดีเพิ่มมากขึ้นในแต่ละปีคิดเป็น ๖๐.๒ เปอร์เซ็นต์ อาชญากรรมเหล่านี้มีทั้งการขโมยและการขายบัตรประจำตัวประชาชน ทะเบียนบ้าน วีแชต แอคเคาท์ และข้อมูลของผู้ป่วย ส่วนคดีที่เกิดขึ้นทางออนไลน์ มีจำนวน ๑,๘๐๐ คดี ที่เกี่ยวข้องกับการ

---

[๗] Wang, C.; Zhang, J.; Lassi, N.; Zhang, X., “ Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective”, เพิ่งอ้าง, หน้า ๒, ๔–๖

ละเมิดสิทธิส่วนบุคคล โดยในจำนวนนี้ ๔๘ คดี เป็นข้อพิพาทเรื่องข้อมูลส่วนบุคคลที่มีการโต้แย้งกับโรงพยาบาล/สถาบันทางการแพทย์ซึ่งมีประเด็นข้อพิพาทคือ บุคลากรทางการแพทย์ (medical personnel) และโรงพยาบาล/สถาบันทางการแพทย์ ได้กระทำการเปิดเผยข้อมูลการรักษาพยาบาลที่ไม่ชอบด้วยกฎหมายหรือไม่ หรือเป็นการเปิดเผยโดยไม่ได้รับความยินยอมจากผู้ป่วย และแม้ว่าประเทศจีนจะมีการควบคุมเรื่องข้อมูลข่าวสารอย่างเคร่งครัด อย่างไรก็ดี สถิติข้อมูลด้านการละเมิดที่เกิดขึ้นในอุตสาหกรรมด้านสาธารณสุขในประเทศจีน โดยเฉพาะคดีต่าง ๆ กลับมีปริมาณและทวีความรุนแรงของปัญหาเพิ่มมากขึ้น ดังเช่นในเดือนสิงหาคม ค.ศ. ๒๐๒๒ มีคดีเกี่ยวกับการขายข้อมูลส่วนบุคคลและข้อมูลทางสาธารณสุขของผู้ใช้ประมาณ ๕๐ ล้านราย ซึ่งรั่วไหลจากระบบ “Shanghai’s compulsory COVID health code application” โดยตัวอย่างข้อมูลที่แฮกเกอร์ขโมยมาเพื่อขายให้แก่ผู้ซื้อนั้นมีทั้งชื่อของผู้ใช้ เลขประจำตัวประชาชน เบอร์โทรศัพท์ และข้อมูลว่าป่วยเป็นโรคโควิด-๑๙ หรือไม่ นอกจากนี้ยังปรากฏข้อมูลทางการแพทย์ในเมืองเซี่ยงไฮ้ที่รั่วไหล และในเดือนกรกฎาคม ค.ศ. ๒๐๒๒ มีการรั่วไหลของข้อมูลส่วนบุคคลจำนวนมหาศาลของประชาชนหนึ่งพันล้านคนจากฐานข้อมูลของตำรวจในเมืองเซี่ยงไฮ้ และยังมีการกล่าวอ้างว่า บริษัทผู้ประกอบการต่าง ๆ เช่น Sichuan Lianhao Technologies, an online Chinese medical company ทำให้ข้อมูลทางการแพทย์จำนวน ๒๔ ล้านรายการที่ถูกบันทึกไว้รั่วไหล ซึ่งข้อมูลดังกล่าวรวมถึงข้อมูลผู้ป่วย ชื่อของแพทย์ เลขบัตรประจำตัวประชาชน เบอร์โทรศัพท์มือถือ ข้อมูลด้านการรักษาพยาบาลผู้ป่วย ตลอดจนข้อมูลของผู้ป่วยที่มีการรายงานว่ารั่วไหลทั้งจากโรงพยาบาลและมหาวิทยาลัยอีกด้วย

ในปัจจุบันจีนมีกฎหมายที่วางกลไกในการคุ้มครองข้อมูลส่วนบุคคลในทางการแพทย์ที่ใช้ปัญญาประดิษฐ์ที่สำคัญ ได้แก่ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (the Personal Information Protection Law (PIPL)) ประมวลกฎหมายแพ่งและพาณิชย์ และมาตรฐานระดับชาติที่เกี่ยวข้อง โดยวางมาตรการในเรื่องต่าง ๆ เช่น การให้ความยินยอมของบุคคล การอนุญาตให้มีการจัดการข้อมูล นอกจากนี้ ยังต้องพิจารณาควบคู่กับกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security Law) และกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ Cybersecurity Law (CSL) อย่างไรก็ดี จีนยังไม่มีกฎหมายเฉพาะที่ตราขึ้นเพื่อกำกับดูแลเรื่องการใช้และการจัดการกับฐานข้อมูลขนาดใหญ่ที่ถูกนำมาใช้ในอุตสาหกรรมทางการแพทย์และสาธารณสุขโดยตรง (healthcare industry)

กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลกรณีการใช้ปัญญาประดิษฐ์ในทางการแพทย์ของประเทศจีน

ดังที่ได้กล่าวถึงภาพรวมของกฎหมายที่มีในประเทศจีนสำหรับการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลในทางการแพทย์ที่ใช้ปัญญาประดิษฐ์ในหัวข้อข้างต้นไว้บ้างแล้ว สำหรับหัวข้อนี้จะได้กล่าวถึงหลักการและสาระสำคัญของกฎหมายแต่ละฉบับในรายละเอียด ซึ่งสามารถสรุปได้ดังนี้

๑. The Personal Information Protection Law (PIPL)[๕]

๑.๑ หลักการและแนวคิด

PIPL เป็นกฎหมายฉบับแรกของจีนที่กำหนดหลักการเกี่ยวกับการจัดการข้อมูลส่วนบุคคลและการให้ความคุ้มครองสิทธิและผลประโยชน์ของปัจเจกบุคคลในส่วนที่เกี่ยวกับข้อมูลส่วนบุคคลโดยกฎหมายฉบับนี้มีผลใช้บังคับตั้งแต่วันที่ ๑ พฤศจิกายน ค.ศ. ๒๐๒๑ (พ.ศ. ๒๕๖๔) และมีหลักการและแนวคิดที่สำคัญครอบคลุมในเรื่องต่าง ๆ ได้แก่

(๑) การประมวลผลข้อมูลส่วนบุคคลต้องชอบด้วยกฎหมาย (legality) ยุติธรรม (justice) มีคุณธรรม (integrity) เป็นความจำเป็นขั้นต่ำ (minimum necessity) เปิดกว้างและมีความโปร่งใส (openness and transparency) โดยวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลต้องมีความชัดเจนและสมเหตุสมผล (explicit and reasonable)

(๒) บุคคลมีสิทธิเข้าถึง สำเนา แก้ไข และร้องขอให้ลบข้อมูลส่วนบุคคลจากผู้ดำเนินการข้อมูลส่วนบุคคล และมีสิทธิร้องขอให้ผู้ประมวลผลข้อมูลส่วนบุคคล (personal information processors) ดำเนินการโอนข้อมูลของตนไปยังผู้ประมวลผลข้อมูลส่วนบุคคลรายอื่นได้

(๓) การประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ที่มีอายุต่ำกว่า ๑๔ ปี ผู้ดำเนินการข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากผู้ปกครองหรือผู้ดูแลผู้เยาว์ และต้องปฏิบัติตามหลักเกณฑ์เฉพาะเรื่องที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

(๔) PIPL ห้ามมิให้มีการใช้การตัดสินใจโดยอัตโนมัติ (automated decision-making) ในส่วนที่เกี่ยวกับข้อมูลส่วนบุคคล อันจะส่งผลให้มีการปฏิบัติที่แตกต่างกันในทางการค้าอย่างไม่สมเหตุสมผล เช่น การเลือกปฏิบัติด้านราคาที่ไม่สมเหตุสมผลต่อลูกค้า นอกจากนี้ ในกรณีที่มีการใช้การตัดสินใจโดยอัตโนมัติเพื่อส่งข้อมูลหรือใช้ประโยชน์เชิงการตลาด ผู้ประมวลผลข้อมูลส่วนบุคคลต้องให้ทางเลือกแก่บุคคล ซึ่งทางเลือกที่ว่านั้นต้องไม่มีเป้าประสงค์ต่อลักษณะเฉพาะของบุคคล (personal characteristics) หรือต้องมีวิธีการที่สะดวกให้ถอนการให้ความยินยอมหรือการปฏิเสธไม่ให้มีการใช้ข้อมูลส่วนบุคคลได้ (opt-out)

(๕) ในกรณีผู้ประมวลผลข้อมูลส่วนบุคคลประสงค์ที่จะดำเนินการโอนข้อมูลส่วนบุคคลออกไปยังประเทศอื่น จะต้องได้รับความยินยอมต่างหากจากบุคคลนั้นและต้องปฏิบัติตามข้อกำหนดเฉพาะ เช่น ผ่านการประเมินความปลอดภัยที่ดำเนินการโดยหน่วยงานด้านกิจการอวกาศ (the national cyberspace authorities) หรือได้รับการรับรองจากสถาบันวิชาชีพที่เกี่ยวข้อง (from the relevant professional institutions) หรือทำสัญญามาตรฐานที่กำหนดโดยหน่วยงานด้านกิจการอวกาศ

---

[๕] Mainland's Personal Information Protection Law, สืบค้นเมื่อ ๒๐ มกราคม ๒๕๖๘, จาก https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/mainland_law.html

(๖) PIPL มีผลบังคับใช้ข้ามเขตแดนได้ (extraterritorial effect) หากองค์การระหว่างประเทศประมวลผลข้อมูลส่วนบุคคลของบุคคลในประเทศจีน โดยมีวัตถุประสงค์เพื่อเสนอผลิตภัณฑ์หรือการให้บริการ หรือเพื่อวิเคราะห์หรือประเมินพฤติกรรมของบุคคล องค์การระหว่างประเทศดังกล่าวจะต้องปฏิบัติตามข้อกำหนดต่าง ๆ ภายใต้ PIPL และต้องจัดตั้งหน่วยงานประจำหรือแต่งตั้งผู้แทนไว้ในประเทศจีนด้วย

(๗) หน่วยงานด้านกิจการอวกาศจะเป็นผู้รับผิดชอบในการประสานงานทั่วไปด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งการกำกับดูแลและการจัดการ และหน่วยงานที่เกี่ยวข้องภายใต้คณะมุขมนตรี (The relevant departments of the State Council) จะรับผิดชอบในการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนการกำกับดูแลและการจัดการที่เกี่ยวข้องภายในขอบเขตหน้าที่และอำนาจของตน

(๘) ผู้ประมวลผลข้อมูลส่วนบุคคลที่ละเมิดข้อกำหนดภายใต้ PIPL จะต้องรับผิดโดยมีค่าปรับสูงสุดจำนวนห้าสิบล้านหยวน หรือคิดเป็นจำนวนร้อยละ ๕ ของรายได้ต่อปีในปีก่อนหน้านี้ (5% of its annual turnover of the preceding year) และอาจถูกสั่งให้หยุดประกอบกิจการจนกว่าจะแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (to suspend its business operations for rectification) หรือถูกเพิกถอนใบอนุญาตประกอบธุรกิจ (business permits or licenses revoked)

๑.๒ สาระของกฎหมาย[๙]

(๑) PIPL มีวัตถุประสงค์เพื่อปกป้องสิทธิและผลประโยชน์ที่เกี่ยวกับข้อมูลส่วนบุคคล กำกับดูแลกิจกรรมการประมวลผลข้อมูลส่วนบุคคล และส่งเสริมให้มีการใช้ข้อมูลส่วนบุคคลอย่างสมเหตุสมผล

(๒) เป้าหมายของการกำกับดูแล PIPL เป็นกฎหมายที่ตราขึ้นเพื่อกำกับดูแลกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของบุคคลธรรมดา รวมถึงกิจกรรมการประมวลผลที่ดำเนินการโดยหน่วยงานของรัฐ โดยตามกฎหมายดังกล่าว ผู้ประมวลผลข้อมูลส่วนบุคคล หมายถึงองค์กรหรือบุคคลใด ๆ ที่กำหนดวัตถุประสงค์ วิธีการ ฯลฯ ของการประมวลผลข้อมูลส่วนบุคคล

(๓) การบังคับใช้นอกอาณาเขต (Extra-territorial Application) PIPL มีผลใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลที่เกิดขึ้นในต่างประเทศ ในกรณีดังต่อไปนี้

- การประมวลผลข้อมูลนั้นเป็นไปเพื่อนำเสนอสินค้าหรือบริการให้แก่ประชาชนในประเทศจีน
- การประมวลผลข้อมูลนั้นเป็นไปเพื่อวิเคราะห์หรือประเมินพฤติกรรมของประชาชนในประเทศจีน
- กรณีอื่น ๆ ตามที่กฎหมายหรือที่มีกฎระเบียบกำหนดไว้

---

[๙] English Translation: Personal Information Protection Law of the People's Republic of China, สืบค้นได้จาก http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559_3.htm

(๔) ความหมายของคำว่า "ข้อมูลส่วนบุคคล" (Personal Information) หมายถึง ข้อมูลต่าง ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่สามารถยืนยันหรือระบุตัวตนได้ ซึ่งบันทึกด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่น ๆ แต่ไม่รวมถึงข้อมูลนิรนาม (anonymized information)

(๕) ความหมายของคำว่า "ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน" (Sensitive Personal Information) หมายถึง ข้อมูลส่วนบุคคลที่หากรั่วไหลหรือถูกใช้โดยไม่ชอบด้วยกฎหมายอาจนำไปสู่การละเมิดศักดิ์ศรีของบุคคล หรืออาจทำให้เกิดความเสี่ยงต่อความปลอดภัยของบุคคลและทรัพย์สินอย่างร้ายแรง และให้หมายความรวมถึงข้อมูลที่เกี่ยวข้องกับเทคโนโลยีที่ใช้ระบุตัวตนและตรวจพิสูจน์ผู้ใช้ (biometrics) ความเชื่อทางศาสนา เอกลักษณ์เฉพาะตัว ข้อมูลทางการแพทย์และสาธารณสุข (medical care and health) บัญชีการเงิน ตำแหน่งที่อยู่ ฯลฯ รวมถึงข้อมูลส่วนบุคคลของผู้เยาว์ที่อายุต่ำกว่า ๑๔ ปี ด้วย[๑๐]

(๖) ความโปร่งใส (Transparency) หลักการเปิดเผยและความโปร่งใสต้องถูกนำมาบังคับใช้เมื่อมีการประมวลผลข้อมูลส่วนบุคคล. กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลต้องเปิดเผยต่อสาธารณชน ด้วยวัตถุประสงค์ วิธีการ และขอบเขตการประมวลผลที่เสนอให้เปิดเผยอย่างชัดเจน และก่อนที่จะประมวลผลข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งข้อมูลด้วยความซื่อสัตย์ถูกต้อง และครบถ้วนในลักษณะที่สามารถเห็นได้อย่างชัดเจนและด้วยภาษาที่เข้าใจได้ง่าย ในเรื่องดังนี้ ๑) ชื่อและข้อมูลติดต่อของผู้ประมวลผลข้อมูลส่วนบุคคล ๒) วัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล หมวดหมู่และระยะเวลาการเก็บรักษาของข้อมูลส่วนบุคคลที่จะประมวลผล และ ๓) วิธีและขั้นตอนการใช้สิทธิของบุคคล ฯลฯ

หากผู้ประมวลผลข้อมูลส่วนบุคคลต้องการบอกข้อมูลเกี่ยวกับกระบวนการประมวลผลข้อมูลให้เจ้าของข้อมูลทราบ จะต้องจัดทำกฎ/ข้อบังคับในการประมวลผลข้อมูลส่วนบุคคล กฎ/ข้อบังคับเหล่านี้ต้องเปิดเผยต่อสาธารณชนและสามารถเข้าถึงได้ง่าย รวมทั้งจัดเก็บกฎ/ข้อบังคับเหล่านี้ไว้เพื่อให้เจ้าของข้อมูลสามารถตรวจสอบได้ตลอดเวลา

หากผู้ประมวลผลข้อมูลส่วนบุคคลประสงค์จะโอนข้อมูลส่วนบุคคล เนื่องจากการควบรวม แยกบริษัท ยุบกิจการ ล้มละลาย หรือด้วยเหตุผลอื่น ต้องแจ้งรายชื่อและข้อมูลติดต่อของผู้รับข้อมูลให้เจ้าของข้อมูลส่วนบุคคลทราบด้วย

หากผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องให้ข้อมูลส่วนบุคคลที่ตนได้ประมวลผลแก่ผู้ประมวลผลรายอื่น ต้องแจ้งรายชื่อและข้อมูลติดต่อของผู้รับข้อมูล วัตถุประสงค์และวิธีการประมวลผล หมวดหมู่ของข้อมูลส่วนบุคคลที่จะประมวลผล และต้องได้รับความยินยอมแยกต่างหากจากเจ้าของข้อมูลส่วนบุคคลด้วย

---

[๑๐]Section 2: Rules for Handling Sensitive Personal Information

Article 28: Sensitive personal information is personal information that once leaked or illegally used can easily cause natural persons to suffer encroachments on their dignity or harms to their persons or property; including information such as on biometric identifiers, religious faith, particular identities, medical care and health, financial status, and location tracking, as well as the personal information of minors under the age of 14. etc.

(๗) การเก็บ การใช้ และการเปิดเผย ฯลฯ (Collection, Use and Disclosure, etc.) การประมวลผลข้อมูลส่วนบุคคล หมายถึงการเก็บรวบรวม เก็บรักษา การใช้ การประมวลผล การส่งผ่านข้อมูล การจัดหา การเปิดเผย และการลบข้อมูลส่วนบุคคล ฯลฯ โดยข้อมูลส่วนบุคคลจะต้องถูกประมวลผลโดยชอบด้วยกฎหมาย ยุติธรรม ตามความจำเป็น และมีคุณธรรม และต้องไม่ถูกประมวลผลโดยวิธีการที่เป็นการฉ้อโกง หลอกลวง หรือบีบบังคับ ฯลฯ

การประมวลผลข้อมูลส่วนบุคคลจะต้องมีวัตถุประสงค์ที่ชัดเจนและสมเหตุสมผล จำกัดเฉพาะวัตถุประสงค์ที่เกี่ยวข้องโดยตรงกับการประมวลผล และมีผลกระทบต่อสิทธิและผลประโยชน์ของบุคคลให้น้อยที่สุด การรวบรวมข้อมูลส่วนบุคคลจะต้องถูกจำกัดและต้องไม่เกินกว่าวัตถุประสงค์ของการประมวลผล

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องประมวลผลข้อมูลส่วนบุคคลเฉพาะภายใต้กรณีที่กำหนดไว้ใน PIPL กรณีดังกล่าวรวมถึง ๑) เมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแล้ว ๒) เมื่อจำเป็นต้องมีการจัดทำหรือดำเนินการตามสัญญา หรือการจัดการทรัพยากรมนุษย์ ๓) เมื่อจำเป็นต้องปฏิบัติตามหน้าที่ตามกฎหมายหรือข้อผูกพัน ๔) เมื่อจำเป็นต้องตอบสนองต่อสถานการณ์ฉุกเฉินด้านสาธารณสุข หรือเพื่อปกป้องชีวิต สุขภาพ และความปลอดภัยในทรัพย์สินของบุคคลในกรณีฉุกเฉิน ๕) เพื่อการประมวลผลข้อมูลส่วนบุคคลอย่างเหมาะสมในการรายงานข่าว การกำกับดูแลสื่อ และกิจกรรมอื่น ๆ ที่ดำเนินการเพื่อประโยชน์สาธารณะ ๖) เพื่อการประมวลผลข้อมูลส่วนบุคคลที่เปิดเผยต่อสาธารณชนโดยเจ้าของข้อมูลส่วนบุคคลนั้นเองหรือมีกฎหมายกำหนดให้ต้องเปิดเผย และ ๗) กรณีอื่น ๆ ตามกฎหมายหรือกฎ/ระเบียบต่าง ๆ กำหนดไว้ อย่างไรก็ดี กรณีตาม ๒) ถึง ๗) ถือเป็นข้อยกเว้นที่สามารถดำเนินการประเมินผลข้อมูลส่วนบุคคลโดยไม่ต้องได้รับความยินยอมได้ (Article 13[๑๑])

---

[๑๑]Article 13 A personal information processor can process personal information of an individual only if one of the following circumstances exists:

(1) the individual's consent has been obtained;

(2) the processing is necessary for the conclusion or performance of a contract in which the individual is a party, or necessary for human resources management in accordance with the labor rules and regulations established in accordance with the law and the collective contracts signed in accordance with the law;

(3) the processing is necessary for the performance of statutory duties or obligations;

(4) the processing is necessary for the response to public health emergencies, or for the protection of life, health, and property safety of natural persons in emergencies;

(5) the personal information is reasonably processed for news reporting, media supervision, and other activities conducted in the public interest;

(6) the personal information disclosed by the individual himself or other legally disclosed personal information of the individual is reasonably processed in accordance with this Law; and

(7) other circumstances as provided by laws or administrative regulations.

องค์กรหรือบุคคลใดจะรวบรวม ใช้ ประมวลผล ส่งผ่าน ซื้อขาย จัดหา หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลอื่นโดยผิดกฎหมายมิได้ และไม่อาจทำกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เป็นภัยต่อความมั่นคงของชาติหรือทำให้เป็นอันตรายต่อประโยชน์สาธารณะ

การติดตั้งอุปกรณ์รวบรวมภาพและระบุตัวตนในสถานที่สาธารณะจะต้องดำเนินการเมื่อมีความจำเป็นเพื่อรักษาความปลอดภัยสาธารณะ โดยมีป้ายเตือนให้เห็นชัดเจน ภาพส่วนบุคคลและข้อมูลการระบุตัวตนที่รวบรวมสามารถใช้ได้เฉพาะเพื่อวัตถุประสงค์ในการรักษาไว้ซึ่งความปลอดภัยสาธารณะ และหากไม่ได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง ต้องไม่ใช้เพื่อวัตถุประสงค์อื่น

PIPL จะไม่มีผลบังคับใช้ในกรณีที่บุคคลประมวลผลข้อมูลส่วนบุคคลเพื่อใช้ในเรื่องส่วนตัวหรือกิจการเกี่ยวกับครัวเรือน นอกจากนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลจะสามารถประมวลผลข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนได้เฉพาะในกรณีที่มีวัตถุประสงค์เฉพาะเจาะจงและมีความจำเป็นเท่านั้น ทั้งยังจะต้องมีมาตรการป้องกันที่เข้มงวด ทั้งนี้ ในการประมวลผลข้อมูลดังกล่าว ผู้ประมวลผลข้อมูลจะต้องได้รับความยินยอมแยกต่างหากจากเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องด้วย

ก่อนที่จะทำการประมวลผลข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการประเมินผลกระทบของการให้ความคุ้มครองข้อมูลส่วนบุคคล และจะต้องมีการรายงาน ตลอดจนบันทึกข้อมูลที่เกี่ยวข้องจะต้องถูกเก็บรักษาไว้อย่างน้อยสามปี โดยผู้ประมวลผลข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนจะต้องแจ้งให้บุคคลทราบถึงความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลดังกล่าว รวมทั้งแจ้งผลกระทบที่มีต่อสิทธิและผลประโยชน์ให้เจ้าของข้อมูลส่วนบุคคลนั้นทราบด้วย

ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการประมวลผลข้อมูลส่วนบุคคลของเยาวชนที่มีอายุต่ำกว่า ๑๔ ปี ผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะต้องกำหนดกระบวนการประมวลผลข้อมูลส่วนบุคคลขึ้นโดยเฉพาะสำหรับการประมวลผลดังกล่าว

(๘) ความยินยอม (Consent) การให้ความยินยอมของบุคคล หมายถึงความยินยอมที่ให้โดยสมัครใจและโดยชัดแจ้งโดยเจ้าของข้อมูลส่วนบุคคลที่ได้รับการแจ้งข้อมูลอย่างครบถ้วน หลักการเรื่องความยินยอมจะมีผลบังคับใช้เมื่อกฎหมาย กฎ ระเบียบ หรือข้อบังคับ กำหนดให้มีการให้ความยินยอมแยกต่างหากหรือต้องมีการให้ความยินยอมเป็นลายลักษณ์อักษร สำหรับการประมวลผลข้อมูลส่วนบุคคล การได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลถือเป็นกระบวนการสำคัญที่จะทำให้ข้อมูลส่วนบุคคลนั้นได้รับการประมวลผลโดยชอบด้วยกฎหมาย

ในกรณีที่วัตถุประสงค์หรือวิธีการประมวลผลข้อมูลส่วนบุคคลหรือประเภทข้อมูลส่วนบุคคลที่เกี่ยวข้องมีการเปลี่ยนแปลง จะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลใหม่อีกครั้งหนึ่ง

Individual consent shall be obtained for processing personal information if any other relevant provisions of this Law so provide, except under the circumstances specified in subparagraphs (2) to (7) of the preceding paragraph.

หากการประมวลผลข้อมูลที่มีการเปิดเผย มีผลกระทบอย่างมีนัยสำคัญต่อสิทธิและผลประโยชน์ของเจ้าของข้อมูลส่วนบุคคล จะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลด้วย

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมแยกต่างหากจากเจ้าของข้อมูลส่วนบุคคล ในกรณีดังต่อไปนี้

- มีการให้ข้อมูลส่วนบุคคลที่ตนประมวลผลไปยังผู้ประมวลผลข้อมูลส่วนบุคคลอื่น
- มีการเปิดเผยข้อมูลส่วนบุคคลที่ตนประมวลผล
- มีการประมวลผลข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน
- มีการใช้ภาพส่วนบุคคลและข้อมูลการระบุตัวตนที่รวบรวมในที่สาธารณะเพื่อวัตถุประสงค์อื่นนอกเหนือจากการรักษาความปลอดภัยสาธารณะ
- มีการโอนข้อมูลส่วนบุคคลออกนอกประเทศ

ในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคลของเยาวชนที่อายุต่ำกว่า ๑๔ ปี ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากผู้ปกครองหรือผู้ดูแลของเยาวชน

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องไม่ปฏิเสธที่จะให้ผลิตภัณฑ์หรือบริการแก่บุคคลเนื่องจากบุคคลปฏิเสธการให้ความยินยอม หรือเพิกถอนการให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคล เว้นแต่การประมวลผลข้อมูลส่วนบุคคลจะเป็นการจำเป็นเพื่อนำเสนอผลิตภัณฑ์หรือบริการ

ในกรณีที่การประมวลผลข้อมูลส่วนบุคคลขึ้นอยู่กับการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล บุคคลนั้นมีสิทธิที่จะถอนการให้ความยินยอมของตนได้ โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องมีวิธีการที่สะดวก เพื่อให้บุคคลสามารถถอนการให้ความยินยอมได้

(๙) ความถูกต้อง (Accuracy) เมื่อมีการประมวลผลข้อมูลส่วนบุคคล คุณภาพของข้อมูลส่วนบุคคลจะต้องได้รับการรับรองเพื่อหลีกเลี่ยงผลกระทบที่ไม่พึงประสงค์ต่อสิทธิและผลประโยชน์ของเจ้าของข้อมูลส่วนบุคคลอันเกิดจากข้อมูลส่วนบุคคลที่ไม่ถูกต้องหรือไม่สมบูรณ์

(๑๐) ความปลอดภัย (Security) ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องรับผิดชอบต่อการประมวลผลข้อมูลส่วนบุคคลของตน และใช้มาตรการที่จำเป็นเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่ประมวลผลนั้น

ผู้ประมวลผลข้อมูลส่วนบุคคลที่มอบหมายให้บุคคลที่สามทำการประมวลผลข้อมูลส่วนบุคคล จะต้องทำสัญญากับบุคคลที่สามโดยระบุวัตถุประสงค์ ระยะเวลา วิธีการประมวลผล ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง มาตรการป้องกัน และสิทธิและหน้าที่ของทั้งสองฝ่าย เป็นต้น โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องกำกับดูแลการประมวลผลที่ดำเนินการโดยผู้รับมอบหมาย

บุคคลที่ถูกมอบหมายให้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้มาตรการที่จำเป็นเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่ประมวลผลนั้น

(๑๑) ระยะเวลาในการเก็บรักษาข้อมูล (Retention Period) ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลจะต้องเป็นช่วงระยะเวลาที่สั้นที่สุด เท่าที่จำเป็นสำหรับการตอบสนองต่อวัตถุประสงค์ในการประมวลผล

ผู้ประมวลผลข้อมูลส่วนบุคคลไม่ว่าจะเป็นการริเริ่มด้วยตนเองหรือได้รับการร้องขอจากเจ้าของข้อมูลส่วนบุคคลก็ตาม จะต้องดำเนินการลบข้อมูลส่วนบุคคลตามที่ PIPL กำหนด เช่น เมื่อระยะเวลาในการเก็บรักษาข้อมูลสิ้นสุดลง เมื่อวัตถุประสงค์ในการประมวลผลสำเร็จลุล่วงหรือไม่สามารถสำเร็จลุล่วงได้หรือข้อมูลส่วนบุคคลนั้นไม่จำเป็นอีกต่อไป การให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคลได้ถูกเพิกถอน ผู้ประมวลผลข้อมูลส่วนบุคคลยุติการเสนอผลิตภัณฑ์หรือการให้บริการ

(๑๒) ความรับผิดชอบและการกำกับดูแล (Accountability and Governance) เมื่อพิจารณาวัตถุประสงค์และวิธีการประมวลผลข้อมูล ประเภทของข้อมูลส่วนบุคคล ผลกระทบต่อสิทธิและผลประโยชน์ของเจ้าของข้อมูลส่วนบุคคล และความเสี่ยงทางความปลอดภัยที่เป็นไปได้ (the potential security risks)[๑๒] แล้ว ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้มาตรการดังต่อไปนี้ เพื่อให้เกิดความมั่นใจว่าการประมวลผลข้อมูลส่วนบุคคลของตนเป็นไปตามกฎหมายและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การรั่วไหล การปลอมแปลง หรือการสูญเสียข้อมูลส่วนบุคคล

- กำหนดระบบการจัดการภายในและขั้นตอนการดำเนินงาน
- การจัดการและประมวลผลข้อมูลส่วนบุคคลโดยแยกประเภทหรือจำแนกข้อมูลออกเป็นระดับต่าง ๆ
- ใช้มาตรการทางเทคนิคความปลอดภัย เช่น การเข้ารหัสและการทำให้ข้อมูลเป็นนิรนาม

ผู้ประมวลผลข้อมูลส่วนบุคคลที่ประมวลผลข้อมูลส่วนบุคคลตามเกณฑ์ที่กำหนดโดยหน่วยงานด้านกิจการอวกาศ จะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่รับผิดชอบต่อการควบคุมดูแลกิจกรรมการประมวลผลข้อมูลส่วนบุคคลและการนำมาตรการป้องกันไปปฏิบัติ

ผู้ประมวลผลข้อมูลส่วนบุคคลจากภายนอกประเทศที่อยู่ภายใต้ PIPL จะต้องจัดตั้งหน่วยงานหรือแต่งตั้งตัวแทนในประเทศจีนเพื่อรับผิดชอบต่อการจัดการเรื่องการคุ้มครองข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการตรวจสอบความถูกต้องตามกฎหมายตลอดจนกฎ ระเบียบ และข้อบังคับต่าง ๆ ในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของตนอย่างสม่ำเสมอ

---

[๑๒]“ความเสี่ยงทางความปลอดภัยที่เป็นไปได้” หมายถึงความเสี่ยงที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคล ซึ่งอาจทำให้ข้อมูลส่วนบุคคลถูกเข้าถึงโดยไม่ได้รับอนุญาต มีการรั่วไหล การปลอมแปลง หรือการสูญหายของข้อมูล เป็นต้น

ตัวอย่างของความเสี่ยงทางความปลอดภัยที่เป็นไปได้ ได้แก่ : การโจมตีทางไซเบอร์ เช่น แฮกเกอร์ติดต่อเข้าถึงข้อมูลส่วนบุคคลอย่างผิดกฎหมาย การสูญหายของข้อมูลเนื่องจากความผิดพลาดทางเทคนิค การรั่วไหลของข้อมูลเนื่องจากความประมาทของพนักงาน การใช้ข้อมูลอย่างไม่ถูกต้องหรือโดยไม่ได้รับอนุญาต

การประเมินผลกระทบในการคุ้มครองข้อมูลส่วนบุคคลจะต้องดำเนินการในกรณีต่าง ๆ ดังต่อไปนี้

- การประมวลผลข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน
- การใช้ข้อมูลส่วนบุคคลในการตัดสินใจอัตโนมัติ
- การมอบหมายให้บุคคลอื่นประมวลผลข้อมูลส่วนบุคคล การให้ข้อมูลส่วนบุคคลแก่ผู้ประมวลผลข้อมูลส่วนบุคคลอื่น หรือการเปิดเผยข้อมูลส่วนบุคคล
- การโอนข้อมูลส่วนบุคคลออกนอกประเทศ
- การดำเนินกิจกรรมการประมวลผลที่มีผลกระทบอย่างมีนัยสำคัญต่อสิทธิและผลประโยชน์ของบุคคล

ทั้งนี้ รายงานและบันทึกที่เกี่ยวข้องจะต้องถูกเก็บรักษาไว้อย่างน้อยสามปี

(๑๓) ภาระหน้าที่ที่ผู้ให้บริการแพลตฟอร์มอินเทอร์เน็ตต้องปฏิบัติ (Obligations of Internet Platforms) ผู้ประมวลผลข้อมูลส่วนบุคคลที่ให้บริการแพลตฟอร์มอินเทอร์เน็ตที่สำคัญซึ่งมีผู้ใช้จำนวนมากและมีรูปแบบธุรกิจที่ซับซ้อน มีหน้าที่ที่ต้องปฏิบัติ ดังนี้

- การจัดตั้งระบบการปฏิบัติที่แข็งแกร่งสำหรับการคุ้มครองข้อมูลส่วนบุคคล และการจัดตั้งองค์กรอิสระที่ประกอบด้วยสมาชิกภายนอกเป็นหลัก เพื่อกำกับดูแลการประมวลผลข้อมูลส่วนบุคคล
- ปฏิบัติตามหลักการเปิดเผย ยุติธรรม และเป็นธรรม กำหนดกฎเกณฑ์ที่แพลตฟอร์มต้องปฏิบัติ ตลอดจนระบุวิธีปฏิบัติและภาระหน้าที่ของการประมวลผลข้อมูลส่วนบุคคลสำหรับผลิตภัณฑ์และผู้ให้บริการของแพลตฟอร์ม
- ระงับการให้บริการแก่ผลิตภัณฑ์หรือผู้ให้บริการที่ละเมิดกฎหมายและระเบียบข้อบังคับอย่างร้ายแรงในการประมวลผลข้อมูลส่วนบุคคล
- เผยแพร่รายงานความรับผิดชอบต่อสังคมเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลอย่างสม่ำเสมอ รวมทั้งพร้อมที่จะให้มีการกำกับดูแลจากสาธารณชน

(๑๔) การแจ้งเตือนการละเมิด (Breach Notification) เมื่อเกิดหรือมีแนวโน้มที่จะเกิดการรั่วไหล การปลอมแปลง หรือการสูญหายของข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการแก้ไขในทันที และแจ้งหน่วยงานคุ้มครองข้อมูลส่วนบุคคล รวมถึงบุคคลที่เกี่ยวข้องให้ทราบ การแจ้งเตือนนี้ต้องรวมถึง

- ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง สาเหตุของเหตุการณ์ และอันตรายที่คาดว่าจะเกิดขึ้น
- มาตรการแก้ไขที่ผู้ประมวลผลข้อมูลส่วนบุคคลได้ดำเนินการ และมาตรการลดผลกระทบที่เจ้าของข้อมูลส่วนบุคคลอาจดำเนินการ เป็นต้น

ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลพิจารณาว่ามาตรการที่ดำเนินการสามารถป้องกันอันตรายที่เกิดจากการรั่วไหล การแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือการสูญหายของข้อมูลได้อย่างมีประสิทธิภาพ อาจไม่จำเป็นต้องแจ้งบุคคลที่เกี่ยวข้อง อย่างไรก็ดี หากหน่วยงานคุ้มครองข้อมูลส่วนบุคคลพิจารณาว่าการรั่วไหลของข้อมูลส่วนบุคคลอาจส่งผลให้เกิดอันตรายต่อเจ้าของข้อมูลส่วนบุคคล หน่วยงานย่อมมีสิทธิในการร้องขอให้ผู้ประมวลผลข้อมูลส่วนบุคคลแจ้งให้บุคคลที่เกี่ยวข้องทราบ

(๑๕) การโอนข้อมูลข้ามพรมแดน (Cross-border Data Transfer) ผู้ประมวลผลข้อมูลส่วนบุคคลที่จำเป็นต้องโอนข้อมูลส่วนบุคคลออกนอกประเทศ เนื่องจากความต้องการทางธุรกิจจะต้องดำเนินการประเมินผลกระทบของการให้ความคุ้มครองข้อมูลส่วนบุคคลก่อน และเก็บรักษารายงานและบันทึกดังกล่าวไว้เป็นเวลาอย่างน้อยสามปี นอกจากนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมแยกต่างหากจากเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง และต้องดำเนินการให้เป็นไปตามเงื่อนไขต่อไปนี้

- ผ่านการประเมินความปลอดภัยที่ดำเนินการโดยหน่วยงานด้านกิจการอวกาศ
- ได้รับการรับรองการปกป้องข้อมูลส่วนบุคคลจากสถาบันวิชาชีพที่เกี่ยวข้องตามระเบียบของหน่วยงานด้านกิจการอวกาศ
- ทำสัญญากับผู้รับข้อมูลในต่างประเทศในการกำหนดสิทธิและหน้าที่ของทั้งสองฝ่ายตามสัญญามาตรฐานที่หน่วยงานด้านกิจการอวกาศกำหนด
- ปฏิบัติตามข้อกำหนดที่กำหนดในกฎหมายอื่น หรือระเบียบข้อบังคับที่กำหนดโดยหน่วยงานด้านกิจการอวกาศ

ในกรณีที่มีสนธิสัญญาหรือข้อตกลงระหว่างประเทศที่ประเทศจีนได้เข้าร่วมซึ่งมีข้อกำหนดเกี่ยวกับการโอนข้อมูลส่วนบุคคลออกนอกประเทศ ต้องปฏิบัติตามข้อกำหนดดังกล่าวด้วย

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้มาตรการที่จำเป็นเพื่อให้แน่ใจว่าการประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการโดยผู้รับในต่างประเทศมีความสอดคล้องกับมาตรฐานการให้ความคุ้มครองข้อมูลส่วนบุคคลที่กำหนดตาม PIPL นอกจากนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องแจ้งบุคคลที่เกี่ยวข้องให้ทราบถึงชื่อและข้อมูลติดต่อของผู้รับในต่างประเทศ วัตถุประสงค์และวิธีการในการประมวลผล ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง รวมตลอดทั้งวิธีการและขั้นตอนสำหรับเจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิตาม PIPL

ผู้ดำเนินโครงสร้างพื้นฐานข้อมูลที่สำคัญ (Critical information infrastructure operators) และผู้ประมวลผลข้อมูลส่วนบุคคลที่ประมวลผลข้อมูลตามเกณฑ์ที่กำหนดโดยหน่วยงานกิจการอวกาศ (เกณฑ์ในที่นี้ คือ ปริมาณข้อมูลที่กำหนดไว้) ต้องจัดเก็บข้อมูลที่รวบรวมและสร้างขึ้นในประเทศจีนไว้ในท้องถิ่น ในที่นี้คือจะต้องจัดเก็บข้อมูลส่วนบุคคลดังกล่าวในท้องถิ่น (in the Mainland locally) กล่าวคือ เก็บรักษาข้อมูลในเซิร์ฟเวอร์ที่ตั้งอยู่ภายในเขตแดนของจีน และหากจำเป็นต้องโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ต้องผ่านการประเมินความปลอดภัยที่ดำเนินการโดยหน่วยงานด้านกิจการอวกาศ เว้นแต่มีกฎหมาย ระเบียบ ข้อบังคับ หรือบทบัญญัติอื่นที่กำหนดว่าไม่จำเป็นต้องมีการดำเนินการประเมินความปลอดภัย

(๑๖) การตัดสินใจอัตโนมัติ (Automated decision-making) การตัดสินใจอัตโนมัติ หมายถึง กิจกรรมการวิเคราะห์และประเมินพฤติกรรมส่วนบุคคล งานอดิเรก หรือสถานะทางเศรษฐกิจ สุขภาพ และเครดิตทางการเงิน ฯลฯ โดยใช้โปรแกรมคอมพิวเตอร์ และทำการตัดสินใจ

ผู้ประมวลผลข้อมูลส่วนบุคคลที่ใช้ข้อมูลส่วนบุคคลในการตัดสินใจอัตโนมัติจะต้องรับประกันความโปร่งใสของการตัดสินใจ ตลอดจนความยุติธรรมและความเป็นกลางของผลลัพธ์ที่ได้มา และต้องไม่เกิดการปฏิบัติที่แตกต่างกันอย่างไม่สมเหตุสมผลต่อบุคคลในเรื่องของราคาและเงื่อนไขการซื้อขายอื่น

เจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกร้องให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดหาคำอธิบายและคัดค้านการตัดสินใจที่เกิดขึ้นจากการตัดสินใจโดยอัตโนมัติสำหรับการตัดสินใจอัตโนมัติที่มีผลกระทบอย่างมากต่อสิทธิและผลประโยชน์ของบุคคลได้

เมื่อมีการใช้การตัดสินใจอัตโนมัติในการแนะนำข้อมูลและทำการตลาดเชิงพาณิชย์ จะต้องให้ตัวเลือกที่ไม่ระบุลักษณะเฉพาะของบุคคลหรือวิธีการที่สะดวกในการถอนการให้ความยินยอมหรือการปฏิเสธไม่ให้มีการใช้ข้อมูลส่วนบุคคล (opt-out)

ก่อนที่จะดำเนินการใช้การตัดสินใจอัตโนมัติ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการประเมินผลกระทบของการให้ความคุ้มครองข้อมูลส่วนบุคคล และเก็บรักษารายงานและบันทึกที่เกี่ยวข้องเป็นเวลาอย่างน้อยสามปี

(๑๗) สิทธิในการเข้าถึงและแก้ไขข้อมูล (Rights of Data Access and Correction) เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงและสำเนาข้อมูลส่วนบุคคลของตนเองจากผู้ประมวลผลข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องให้ข้อมูลดังกล่าวในเวลาที่เหมาะสม และหากเจ้าของข้อมูลส่วนบุคคลพบว่าข้อมูลส่วนบุคคลของตนไม่ถูกต้องหรือไม่ครบถ้วน ย่อมมีสิทธิเรียกร้องให้ผู้ประมวลผลข้อมูลส่วนบุคคลแก้ไขและเพิ่มเติมข้อมูลที่เกี่ยวข้องได้ นอกจากนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องมีกลไกหรือระบบที่สะดวกสำหรับการรับและจัดการคำร้องจากเจ้าของข้อมูลส่วนบุคคลที่ต้องการใช้สิทธิของตน และหากผู้ประมวลผลข้อมูลส่วนบุคคลปฏิเสธการร้องขอใช้สิทธิ ผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะต้องให้เหตุผลในการปฏิเสธ ซึ่งเจ้าของข้อมูลส่วนบุคคลสามารถยื่นฟ้องศาลได้กรณีที่มีการปฏิเสธการร้องขอนั้น

(๑๘) การโอนข้อมูลส่วนบุคคล (Personal Information Portability) หากเจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ประมวลผลข้อมูลส่วนบุคคลโอนข้อมูลส่วนบุคคลของตนไปยังผู้ประมวลผลข้อมูลที่ระบุ และคำร้องเหล่านั้นเป็นไปตามข้อกำหนดที่กำหนดโดยหน่วยงานด้านกิจการอวกาศ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดหาวิธีการสำหรับการโอนข้อมูลดังกล่าว

(๑๙) สิทธิในการลบ จำกัด หรือปฏิเสธการประมวลผลข้อมูลส่วนบุคคล (Right to Erasure, Restrict or Refuse Personal Information Processing) ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องลบข้อมูลส่วนบุคคลในกรณีต่อไปนี้ ไม่ว่าจะโดยการริเริ่มของตนเองหรือเมื่อได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคล

- เมื่อวัตถุประสงค์ในการประมวลผลสำเร็จลุล่วงหรือไม่สามารถสำเร็จลุล่วงได้ หรือข้อมูลส่วนบุคคลนั้นไม่จำเป็นอีกต่อไป

- ผู้ประมวลผลข้อมูลส่วนบุคคลยุติการเสนอผลิตภัณฑ์หรือการให้บริการ

- ระยะเวลาในการเก็บรักษาข้อมูลสิ้นสุดลง

- เจ้าของข้อมูลส่วนบุคคลถอนการให้ความยินยอม

- ผู้ประมวลผลข้อมูลส่วนบุคคลได้ละเมิดกฎหมาย ระเบียบ ข้อบังคับ หรือข้อตกลงในขณะที่มีการประมวลผลข้อมูลส่วนบุคคล

- กรณีอื่นๆ ที่กฎหมาย หรือกฎ/ระเบียบ/ข้อบังคับ กำหนด

ในกรณีที่การลบข้อมูลส่วนบุคคลไม่อาจกระทำได้ด้วยเหตุทางเทคนิค ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องหยุดการประมวลผลข้อมูลส่วนบุคคล เว้นแต่เป็นการดำเนินการเพื่อการเก็บรักษาและดำเนินการมาตรการคุ้มครองความปลอดภัยที่จำเป็น

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะจำกัดหรือปฏิเสธการประมวลผลข้อมูลส่วนบุคคลโดยผู้อื่น เว้นแต่มีกฎหมายหรือกฎ/ระเบียบ/ข้อบังคับ/ข้อกำหนด กำหนดไว้เป็นอย่างอื่น

ญาติใกล้ชิดของเจ้าของข้อมูลส่วนบุคคลที่เสียชีวิตสามารถใช้สิทธิในการเข้าถึง สำเนา แก้ไข และลบข้อมูลส่วนบุคคลของผู้เสียชีวิตได้ หากมีเหตุผลและผลประโยชน์ที่ถูกต้องตามกฎหมายในการทำเช่นนั้น

(๒๐) สิทธิในการรับรู้ (Right to be Informed) เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการรับทราบและตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของตนเอง และมีสิทธิในการจำกัดหรือปฏิเสธการประมวลผลข้อมูลส่วนบุคคลโดยผู้อื่น เว้นแต่มีกฎหมายหรือกฎ/ระเบียบ/ข้อบังคับ/ข้อกำหนด กำหนดไว้เป็นอย่างอื่น

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอให้ผู้ประมวลผลข้อมูลส่วนบุคคลตีความกฎการประมวลผลข้อมูลส่วนบุคคลของตน

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องมีกลไกหรือระบบที่สะดวกสำหรับการรับและจัดการคำร้องจากเจ้าของข้อมูลส่วนบุคคลที่ต้องการใช้สิทธิของตน และหากผู้ประมวลผลข้อมูลส่วนบุคคลปฏิเสธการร้องขอใช้สิทธิ ผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะต้องให้เหตุผลในการปฏิเสธซึ่งเจ้าของข้อมูลส่วนบุคคลสามารถยื่นฟ้องศาลได้กรณีที่มีการปฏิเสธการร้องขอนั้น

(๒๑) บทกำหนดโทษ

ในกรณีที่การประมวลผลข้อมูลส่วนบุคคลดำเนินการโดยละเมิดข้อกำหนดภายใต้ PIPL หน่วยงานคุ้มครองข้อมูลส่วนบุคคลสามารถสั่งให้แก้ไข ออกคำเตือน และยึดผลประโยชน์ที่ได้มาโดยไม่ชอบด้วยกฎหมาย ผู้ที่ปฏิเสธการแก้ไขจะต้องรับผิดชอบโดยการจ่ายค่าปรับไม่เกินหนึ่งล้านหยวน บุคคลที่มีหน้าที่รับผิดชอบโดยตรงจะถูกปรับไม่น้อยกว่าหนึ่งหมื่นหยวน แต่ไม่เกินหนึ่งแสนหยวน ในกรณีเป็นการกระทำความผิดที่มีความร้ายแรง หน่วยงานคุ้มครองข้อมูลส่วนบุคคลที่มีอำนาจเหนือระดับจังหวัด (personal information protection authorities above the provincial level) สามารถสั่งให้แก้ไขหรือยึดผลประโยชน์ที่ได้มาโดยไม่ชอบด้วยกฎหมาย และกำหนดค่าปรับไม่เกินห้าสิบล้านหยวน หรือคิดเป็นจำนวนร้อยละ ๕ ของรายได้ต่อปีในปีก่อนหน้านี้ อีกทั้งหน่วยงานคุ้มครองข้อมูลส่วนบุคคล

ยังสามารถสั่งระงับการดำเนินธุรกิจที่เกี่ยวข้องหรือสั่งให้มีการแก้ไขให้ถูกต้อง รวมทั้งแจ้งหน่วยงานที่มีอำนาจเพื่อเพิกถอนใบอนุญาตหรือใบอนุญาตประกอบธุรกิจที่เกี่ยวข้อง

สำหรับกรณีความผิดที่ไม่มีความร้ายแรง บุคคลที่มีหน้าที่รับผิดชอบโดยตรงจะถูกปรับไม่น้อยกว่าไม่น้อยกว่าหนึ่งแสนหยวน แต่ไม่เกินหนึ่งล้านหยวน และอาจถูกห้ามทำหน้าที่เป็นกรรมการ ผู้ตรวจสอบ ผู้บริหารระดับสูง และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในบริษัทที่เกี่ยวข้องภายในระยะเวลาหนึ่ง และหากการละเมิดข้อกำหนดภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PIPL) ส่งผลถึงการละเมิดการจัดการความปลอดภัยสาธารณะ การกระทำนั้นจะต้องรับโทษตามระเบียบการจัดการความปลอดภัยสาธารณะ และถ้าการกระทำละเมิดนั้นถึงขนาดเป็นการกระทำผิดทางอาญา ผู้ที่กระทำผิดจะต้องรับโทษทางอาญาตามกฎหมาย

๒. Data Security Law (DSL)[๑๓]

DSL[๑๔] มีผลใช้บังคับตั้งแต่วันที่ ๑ กันยายน ค.ศ. ๒๐๒๑ (พ.ศ. ๒๕๖๔)

๒.๑ ขอบเขตการบังคับใช้และผลบังคับนอกอาณาเขต (Scope of Application and Extraterritorial Effect of DSL)

DSL (Data Security Law) มีผลบังคับใช้กับการควบคุมกิจกรรมการประมวลผลข้อมูลโดยองค์กรและบุคคล ตลอดจนกำกับดูแลความปลอดภัยของกิจกรรมเหล่านั้นภายในอาณาเขตของประเทศจีน และควบคุมกิจกรรมการประมวลผลข้อมูลที่ดำเนินการนอกประเทศหากกิจกรรมนั้นก่อให้เกิดอันตรายต่อความมั่นคงหรือผลประโยชน์สาธารณะของประเทศจีน หรือมีผลกระทบต่อการคุ้มครองสิทธิและผลประโยชน์ทางกฎหมายของบุคคลและองค์กรในประเทศ จึงอาจกล่าวได้ว่า DSL มีขอบเขตการบังคับใช้กว้างขวางและมีผลบังคับนอกอาณาเขตด้วย นอกจากนี้ DSL ยังกำหนดหน้าที่ให้องค์กรและบุคคลต้องปฏิบัติเกี่ยวกับการจัดประเภทและการแบ่งกลุ่มข้อมูล การควบคุมความเสี่ยงของข้อมูลและการประเมินความเสี่ยง การโอนข้อมูลข้ามพรมแดน และการควบคุมการส่งออกข้อมูล โดย DSL จะถูกนำบังคับใช้กับข้อมูลที่บันทึกในรูปแบบอิเล็กทรอนิกส์และรูปแบบอื่น ๆ รวมถึงข้อมูลดิจิทัลและข้อมูลด้านกิจกรรมอวกาศ (cyber information) และข้อมูลที่บันทึกในรูปแบบอื่น ๆ เช่น บันทึกลงบนกระดาษ กิจกรรมการประมวลผลข้อมูลที่ถูกควบคุมโดยกฎหมาย DSL รวมถึงการเก็บรวบรวม การจัดเก็บ การใช้ การประมวลผล การส่งผ่าน การให้บริการ หรือการเปิดเผยข้อมูลด้วย

๒.๒ การจัดประเภทและการจัดกลุ่มข้อมูล (Data Categorization and Classification Under DSL)

DSL จัดกลุ่มข้อมูลออกเป็นสองประเภทหลัก คือ ข้อมูลหลักของประเทศ (National Core Data) และข้อมูลสำคัญ (Important Data) โดย DSL จะกำหนดการควบคุมและการให้ความคุ้มครองที่เข้มงวดมากขึ้นสำหรับ “ข้อมูลหลักของประเทศ” ซึ่งครอบคลุมข้อมูลที่เกี่ยวข้องกับความมั่นคงของประเทศ ทิศทางสำคัญเศรษฐกิจของประเทศ (the lifeline of the national economy) และข้อมูล

---

[๑๓] “What is China’s Data Security Law?”, สืบค้นเมื่อ ๒๐ มกราคม ๒๕๖๘, จาก https://securiti.ai/china-data-security-law/, Published August 9, 2021/Updated December 13, 2023

[๑๔] English Translation: Data Security Law of the People's Republic of China, สืบค้นได้จาก http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html

ที่มีความสำคัญต่อความเป็นอยู่ของประชาชนและหรือที่จะกระทบต่อผลประโยชน์สาธารณะอย่างมีนัยสำคัญ อย่างไรก็ดี ภายใต้ DSL ยังไม่มีความชัดเจนว่าข้อมูลประเภทใดจะจัดอยู่ในกลุ่ม “ข้อมูลสำคัญ” คงมีเพียงการกำหนดเกณฑ์อย่างเป็นทางการสำหรับข้อมูลสำคัญเฉพาะที่ใช้ในภาคอุตสาหกรรม เพื่อป้องกันมิให้ผู้ประกอบธุรกิจมีดุลพินิจในการตัดสินใจขอบเขตของข้อมูลสำคัญได้ด้วยตนเอง และเกณฑ์ตามร่างแนวทางการบริหารความมั่นคงปลอดภัยของข้อมูล (Draft Data Security Administration Guidelines) ที่จัดทำโดย Cyberspace Administration of China (CAC) เพื่อเป็นข้อกำหนดเบื้องต้นที่ให้แนวทางเกี่ยวกับการจัดการและการคุ้มครองความมั่นคงปลอดภัยของข้อมูลในประเทศจีน ซึ่งกำหนดว่า “ข้อมูลสำคัญ” หมายถึง ข้อมูลที่อาจก่อให้เกิดอันตรายต่อความมั่นคงของชาติหรือผลประโยชน์สาธารณะ หากมีการแก้ไข ทำลาย รั่วไหล ถูกนำไปใช้ หรือถูกเข้าถึงโดยไม่ได้รับอนุญาตอย่างผิดกฎหมาย[๑๕]

ภายใต้มาตรา ๒๑[๑๖] แห่งกฎหมาย DSL รัฐบาลจีนจะจัดตั้งระบบการจัดการและการให้ความคุ้มครองข้อมูลตามลำดับชั้น โดยเน้นความสำคัญของประเภทข้อมูลต่าง ๆ ที่มีผลกระทบต่อเศรษฐกิจและความมั่นคงของชาติ ตลอดจนผลประโยชน์สาธารณะ โดยมีหน่วยงานที่เกี่ยวข้อง

---

[๑๕]China Releases Draft Regulations on Network Data Security 19 November 2021

Definitions of Terms

2. The Draft Regulations draw a threefold distinction of Data: “core data”, “important data” (“ID”) and “general data” – though these terms are also not entirely new to the existing cybersecurity framework. Briefly, “core data” refers to Data relevant to state security, key branches of the national economy, key areas of people’s livelihood and significant public interest. As for ID, the Draft Regulations define it much as other recent (draft) regulations do: Data that may endanger national security or public interests if tampered with, destroyed, leaked, illegally obtained or illegally used, including but not limited to: ect.

ดูรายละเอียดเพิ่มเติมได้จาก https://www.dahuilawyers.com/ media/documents/ DaHui_Newsletter_-_China_Releases_Draft_Regulations_on_Cyber_Data_Security.pdf?form=MG0AV3

[๑๖]**Article 21** The state shall establish a categorized and classified system and carry out data protection based on the importance of the data in economic and social development, as well as the extent of harm to national security, public interests, or the lawful rights and interests of individuals or organizations that will be caused once the data are altered, destroyed, leaked, or illegally obtained or used. The coordination mechanism for national data security shall coordinate the relevant departments to formulate a catalog of important data and strengthen protection of important data.

Data concerning national security, lifelines of the national economy, important aspects of people’s lives, major public interests, ect., are core data of the state, for which a stricter management system shall be implemented.

All localities and departments shall, in accordance with the categorized and classified data protection system, prepare specific catalogs of important data for their respective regions, departments, and relevant industries and sectors, and give priority to the data listed in the catalogs in terms of data protection.

ซึ่งรับผิดชอบในการพัฒนาการจัดประเภทข้อมูลตามลำดับชั้นและรักษาความมั่นคง ความปลอดภัยของข้อมูลตามลำดับชั้น ดังนี้

- การมีกลไกการประสานงานความมั่นคงปลอดภัยของข้อมูลระดับชาติเพื่อประสานงานกับหน่วยงานที่เกี่ยวข้อง โดยจะมีการสร้างแคตตาล็อกข้อมูลสำคัญในระดับชาติ (an important data catalogue at the national level) แต่ไม่รวมถึงข้อมูลหลักแห่งชาติ (core national data) ที่ถือเป็นหมวดหมู่ที่มีความสำคัญสูงสุดและแยกออกมาเป็นพิเศษ

- หน่วยงานระดับภูมิภาคจะต้องจัดทำแคตตาล็อกของข้อมูลสำคัญเฉพาะสำหรับภูมิภาค หน่วยงาน และภาคอุตสาหกรรมที่เกี่ยวข้องของตน ตามระบบการรักษาความมั่นคงปลอดภัยของข้อมูลตามการแบ่งประเภทและจัดกลุ่มข้อมูล และให้ความสำคัญเป็นลำดับแรกต่อข้อมูลที่ระบุในแคตตาล็อกในการรักษาความมั่นคงปลอดภัยของข้อมูลนั้น

๒.๓ การถ่ายโอนข้อมูลข้ามพรมแดนและการจัดที่ตั้งข้อมูล (Cross Border Data Transfers and Data Localization[๑๗])

โครงสร้างพื้นฐานที่สำคัญทางด้านข้อมูล (Critical Information Infrastructure “CII”) หมายถึง โครงสร้างพื้นฐานข้อมูลในอุตสาหกรรมและภาคส่วนที่สำคัญ (เช่น บริการด้านข้อมูล บริการสาธารณะ และรัฐบาลอิเล็กทรอนิกส์) และโครงสร้างพื้นฐานข้อมูลอื่น ๆ ซึ่งหากข้อมูลนั้นรั่วไหลออกไปอาจก่อให้เกิดความเสี่ยงอย่างร้ายแรงต่อความมั่นคงทางเศรษฐกิจของประเทศ ความเป็นอยู่ของประชาชนและผลประโยชน์สาธารณะ

DSL มีข้อกำหนดเกี่ยวกับการโอนข้อมูลข้ามพรมแดนที่แตกต่างกันสำหรับผู้ดำเนินการ CII และผู้ดำเนินการที่ไม่ใช่ CII โดยมาตรา ๓๑ แห่งกฎหมาย DSL[๑๘] กำหนดให้ผู้ดำเนินการ CII ต้องปฏิบัติตามมาตรการการจัดที่ตั้งข้อมูลและการโอนข้อมูลข้ามพรมแดนภายใต้กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Law, CSL) และมาตรการที่กำหนดขึ้นในภายหลัง. ภายใต้ CSL ผู้ดำเนินการ CII ต้องเก็บข้อมูลสำคัญที่รวบรวมหรือสร้างขึ้นในประเทศไว้ภายในประเทศจีน ผู้ดำเนินการ CII สามารถถ่ายโอนข้อมูลออกจากประเทศจีนได้เฉพาะในกรณีดังต่อไปนี้

---

[๑๗]การจัดที่ตั้งข้อมูล (Data Localization) หมายถึง การเก็บรักษาข้อมูลภายในเขตแดนของประเทศที่ข้อมูลนั้นถูกสร้างขึ้นหรือรวบรวม ซึ่งจะเป็นการป้องกันการถ่ายโอนหรือส่งข้อมูลออกนอกประเทศโดยไม่ได้รับการอนุญาต

[๑๘]**Article 31** The provisions of the Cyber Security Law of the People’s Republic of China shall apply to the outbound security management of the important data collected or produced by critical information infrastructure operators during their operation within the territory of the People’s Republic of China, and the measures for the outbound security management of the important data collected or produced by others data processors during their operation within the territory of the People’s Republic of China shall be formulated by the national cyberspace authority in conjunction with the relevant departments under the State Council.

- มีความจำเป็นทางธุรกิจอย่างแท้จริง

- ผู้ดำเนินการเครือข่ายได้ทำการประเมินความปลอดภัยตามมาตรการที่กำหนดร่วมกันโดยหน่วยงานด้านกิจการอวกาศ (Cyberspace Administration of China, CAC) และหน่วยงานที่เกี่ยวข้องภายใต้คณะมุขมนตรี (the State Council) และ

- ได้รับความยินยอมจากบุคคลที่เกี่ยวข้องในการโอนข้อมูลส่วนบุคคลออกนอกประเทศ (เว้นแต่การยินยอมนั้นถือว่าเป็นการให้ยินยอม เนื่องจากบุคคลนั้นเป็นผู้ส่งข้อมูลเอง)

กรณีที่ผู้ดำเนินการที่ไม่ใช่ CII จะโอน “ข้อมูลสำคัญ” ออกนอกประเทศจะต้องปฏิบัติตามกฎที่กำหนดโดย CAC และหน่วยงานที่เกี่ยวข้องภายใต้คณะมุขมนตรี

นอกจากนี้ DSL ได้กำหนดห้ามองค์กรและบุคคลให้ข้อมูลใด ๆ ที่ถูกเก็บไว้ในประเทศแก่หน่วยงานที่บังคับใช้กฎหมายต่างประเทศ (foreign law enforcement authorities) หรือหน่วยงานตุลาการของต่างประเทศ (other foreign judicial departments) โดยไม่ได้รับการอนุญาตล่วงหน้าจากรัฐบาลจีน

๒.๔ ระบบการจัดการความปลอดภัยของข้อมูล (Data Security Management System)

DSL กำหนดให้องค์กรต้องใช้มาตรการทางเทคนิค การจัดองค์กร และมาตรการคุ้มครองข้อมูลอื่น ๆ เพื่อปกป้องประเภทของข้อมูลที่ได้รับความคุ้มครอง เพื่อการนี้ องค์กรจะต้องจัดตั้งและดำเนินการระบบการจัดการความปลอดภัยของข้อมูล อีกทั้ง DSL ยังกำหนดบังคับให้องค์กรต้องจัดการฝึกอบรมด้านความปลอดภัยของข้อมูล และกำหนดบุคคลและแผนกที่รับผิดชอบด้านความปลอดภัยของข้อมูล ดังจะเห็นได้จากการที่มาตรา ๒๙[๑๙] แห่งกฎหมาย DSL กำหนดให้องค์กรควรเสริมสร้างมาตรการตรวจสอบความเสี่ยง และดำเนินมาตรการแก้ไขปัญหาในเวลาที่เหมาะสม หากพบข้อบกพร่องความเปราะบาง หรือความเสี่ยงอื่น ๆ นอกจากนี้ DSL ยังกำหนดให้องค์กรที่ดำเนินการด้านข้อมูลทางอินเทอร์เน็ตต้องปฏิบัติตามมาตรการคุ้มครองหลายระดับ “the Multi-level Protection Scheme” (MLPS) ซึ่งเป็นระบบการจำแนกระดับความปลอดภัยสำหรับบริษัทที่ตั้งอยู่ในประเทศจีนและนำมาใช้ภายใต้กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ (CSL) โดยภายใต้ MLPS องค์กรต้องดำเนินการดังนี้

- ปกป้องเครือข่ายของตนจากการรบกวน ความเสียหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต และ

- จัดประเภทรูปแบบโครงสร้างพื้นฐานและระบบแอพพลิเคชันของตน (application systems) เป็นห้าระดับการป้องกันที่แยกต่างหากจากกัน และปฏิบัติตามข้อผูกพันการป้องกัน (protection obligations) ตามที่ระบุไว้ในมาตรา ๒๗ แห่งกฎหมาย CSL เช่น บุคคลและองค์กรต้องไม่

---

[๑๙] **Article 29** Closer risk monitoring shall be applied in data processing. Where data security defects, bugs, or other risks are discovered, remedial measures shall be taken immediately. Where a data security incident occurs, measures shall be taken immediately to address it, and users shall be notified and reports made to relevant competent departments in a timely manner in accordance with relevant provisions.

เข้าถึงเครือข่ายของผู้อื่นโดยไม่ได้รับอนุญาต รบกวนการทำงานปกติของเครือข่ายของผู้อื่น ขโมยข้อมูลเครือข่าย หรือกระทำการอื่นใดที่เป็นภัยต่อความมั่นคงไซเบอร์

๒.๕ การประเมินความเสี่ยง (Risk Assessments)

ภายใต้ DSL ประเทศจีนจะจัดตั้งระบบการรายงานการประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลที่เป็นศูนย์รวมและเป็นมาตรฐานเดียวกัน โดยมาตรา ๓๐ แห่งกฎหมาย DSL กำหนดให้องค์กรทุกแห่งต้องดำเนินการประเมินความเสี่ยงเกี่ยวกับกิจกรรมการจัดการข้อมูลและการปฏิบัติในการจัดการกับ “ข้อมูลสำคัญ” อย่างสม่ำเสมอ โดยองค์กรยังต้องส่งรายงานการประเมินความเสี่ยงไปยังหน่วยงานกำกับดูแลที่เกี่ยวข้อง ซึ่งรายงานการประเมินความเสี่ยงจะมีข้อมูลดังต่อไปนี้

- ประเภทและปริมาณของข้อมูลสำคัญที่ถูกประมวลผล
- วิธีการที่ใช้การดำเนินกิจกรรมการประมวลผลข้อมูล และ
- ความเสี่ยงด้านความปลอดภัยของข้อมูลและกลไกการตอบสนองที่เกี่ยวข้อง

๒.๖ การตอบสนองต่อเหตุการณ์และการแจ้งเตือน (. Data Incident Response and Notifications)

คือ พันธกรณีหรือข้อกำหนดที่องค์กรต้องปฏิบัติตามเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความปลอดภัยของข้อมูล ซึ่ง DSL มีข้อกำหนดทำนองเดียวกับกฎหมายความมั่งคงปลอดภัยทางไซเบอร์ (CSL) กล่าวคือ องค์กรต้องมีแผนในการจัดการกับเหตุการณ์ที่เกิดขึ้นโดยไม่คาดคิด (incident) ซึ่งตามมาตรา ๒๙ แห่งกฎหมาย DSL กำหนดให้องค์กรมีหน้าที่ในการแก้ไขเหตุการณ์อย่างทันท่วงที แจ้งบุคคลที่เกี่ยวข้องโดยเร็ว และรายงานเหตุการณ์ความปลอดภัยของข้อมูลดังกล่าวต่อหน่วยงานกำกับดูแลที่เกี่ยวข้องตามที่กำหนด นอกจากนี้ ภายใต้มาตรา ๒๓[๒๐] แห่งกฎหมาย DSL รัฐบาลจีนจะจัดตั้งกลไกตอบสนองฉุกเฉินด้านความปลอดภัยของข้อมูลระดับชาติ ซึ่งกำหนดให้หน่วยงานกำกับดูแลเริ่มแผนการตอบสนองฉุกเฉินในกรณีเกิดเหตุการณ์ความไม่ปลอดภัยของข้อมูล

๒.๗ ภาระหน้าที่ของผู้ให้บริการกลางที่ให้บริการการค้าข้อมูล (Data Trading Intermediary Services Obligations)

DSL กำหนดให้องค์กรผู้ให้บริการกลางที่ให้บริการค้าข้อมูลจะต้องกำหนดให้ผู้ให้ข้อมูล (data provider) ปฏิบัติตามข้อกำหนดดังต่อไปนี้

- ชี้แจงแหล่งที่มาของข้อมูล
- ตรวจสอบตัวตนของฝ่ายที่ทำธุรกรรม และ
- เก็บบันทึกการตรวจสอบและบันทึกการทำธุรกรรมในขณะที่ให้บริการ

---

[๒๐] **Article 23** The state shall establish a data security emergency response mechanism. Where a data security incident occurs, the relevant competent departments shall initiate emergency response in accordance with the plan and the law, take corresponding measures to prevent further harm and eliminate security hazards, and send out warnings to the public by publishing information relevant thereto in a timely manner.

๒.๘ หน้าที่อื่น ๆ (Other General Obligations)

องค์กรและบุคคลผู้ที่มีส่วนเกี่ยวข้องกับการจัดการ การเก็บรวบรวม หรือการใช้ข้อมูลจำเป็นต้องใช้วิธีการที่ถูกต้องตามกฎหมายและชอบด้วยตามกฎหมายในการเก็บรวบรวมข้อมูลและไม่ควรขโมยหรือได้รับข้อมูลด้วยวิธีที่ผิดกฎหมาย

ในกรณีที่มีกฎหมาย กฎ ระเบียบ หรือข้อบังคับ ระบุวัตถุประสงค์และขอบเขตของการเก็บรวบรวมและการใช้ข้อมูล องค์กรต้องเก็บรวบรวมและใช้ข้อมูลภายใต้วัตถุประสงค์และขอบเขตที่กฎหมาย กฎ ระเบียบ หรือข้อบังคับนั้นกำหนด

๒.๙ บทกำหนดโทษ

หมวด ๖ แห่งกฎหมาย DSL กำหนดว่า หน่วยงานและบุคคลที่ไม่ปฏิบัติตามกฎหมายหรือข้อกำหนดภายใต้ DSL อาจได้รับคำสั่งจากหน่วยงานกำกับดูแลให้ดำเนินการแก้ไขการกระทำผิดหรือปฏิบัติตามข้อกำหนดที่ระบุในกฎหมาย ได้รับคำเตือน และมีค่าปรับสูงสุดถึงหนึ่งล้านหยวนในกรณีที่มีความรุนแรง รวมถึงบทลงโทษอื่นที่มีผลกระทบต่อการดำเนินงาน เช่น การระงับกิจการ นอกจากนี้บุคคลและหน่วยงานที่ไม่ปฏิบัติตามข้อกำหนดเกี่ยวกับการปกป้องข้อมูลภายใต้ DSL อาจได้รับคำสั่งให้แก้ไข ได้รับคำเตือน และ/หรือมีค่าปรับไม่ต่ำกว่าห้าหมื่นหยวน แต่ไม่เกินห้าแสนหยวน และหากการกระทำผิดละเมิดนั้นถึงระดับที่เป็นความผิดทางอาญา โทษทางอาญาดังกล่าวอาจรวมถึงบุคคลที่เกี่ยวข้องกับการดำเนินงานหรือการจัดการข้อมูลของหน่วยงานหรือองค์กร หรือผู้บริหารขององค์กรด้วย อีกทั้ง DSL ยังให้สิทธิแก่บุคคลในการร้องเรียนและฟ้องร้องทางแพ่งต่อการไม่ปฏิบัติตาม DSL ด้วย

๓. Cybersecurity Law (CSL)[๒๑]

ทั่วโลกเริ่มตระหนักถึงความสำคัญของการคุ้มครองข้อมูลอย่างแท้จริง โดยประเทศต่างๆ ได้เสนอกรอบหรือแนวทางด้านกฎหมายที่ครอบคลุมมากขึ้น เพื่อคุ้มครองข้อมูลส่วนบุคคลที่อยู่บนโลกออนไลน์ ดังจะเห็นได้จากการที่ประเทศสหรัฐอเมริกาที่มีการตราพระราชบัญญัติว่าด้วยความเป็นส่วนตัวผู้บริโภคของรัฐแคลิฟอร์เนีย (California Consumer Privacy Act - CCPA) และในเดือนมิถุนายน ค.ศ. ๒๐๑๗ สหภาพยุโรป (EU) ได้มีการวางกฎระเบียบการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation – GDPR) สำหรับประเทศจีนก็ได้มีการตรากฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์เพื่อปกป้องสิทธิในข้อมูลของผู้บริโภคในประเทศเช่นกัน โดยกฎหมายฉบับนี้ถูกกำหนดขึ้นโดยมีวัตถุประสงค์ดังนี้

(๑) ให้แนวทางเกี่ยวกับข้อกำหนดความปลอดภัยไซเบอร์เพื่อปกป้องกิจการอวกาศ (cyberspace) ของประเทศจีน

(๒) ปกป้องผลประโยชน์และสิทธิทางกฎหมายขององค์กรและบุคคลในประเทศจีน

---

[๒๑] “What is China’s Cybersecurity Law?”, สืบค้นเมื่อ ๒๐ มกราคม ๒๕๖๘, จาก https://securiti.ai/what-is-china-cybersecurity-law/, Published October 30, 2024

(๓) ส่งเสริมการพัฒนาเทคโนโลยีอย่างปลอดภัยและการปรับเปลี่ยนเป็นเศรษฐกิจดิจิทัลในประเทศจีน

CSL ให้สิทธิแก่ผู้ที่เกี่ยวข้องกับข้อมูล (data subjects)/ผู้บริโภค (data subjects/consumers (users) (ผู้ใช้งาน) ดังนี้

(๑) สิทธิในการรับรู้ข้อมูล (Right to information) ก่อนที่จะมีการรวบรวมหรือประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูล (ผู้ประกอบการเครือข่าย network operator) ผู้ใช้งานจะมีสิทธิทราบถึงวัตถุประสงค์ของการรวบรวมหรือประมวลผล วิธีที่ใช้ และขอบเขตของข้อมูลส่วนบุคคลของตน

(๒) สิทธิในการลบข้อมูล (Right to deletion) ผู้ใช้งานมีสิทธิที่จะขอให้ลบข้อมูลส่วนบุคคลของตนหากพบว่าการรวบรวมหรือการประมวลผลของผู้ประกอบการเครือข่ายนั้นเป็นการละเมิดข้อกำหนดตามกฎหมาย

(๓) สิทธิในการแก้ไขข้อมูล (Right to rectification) ผู้ใช้งานมีสิทธิที่จะขอให้ผู้ประกอบการเครือข่ายแก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้อง

(๔) สิทธิในการรับการแจ้งเตือน (Right to be notified) ผู้ใช้งานมีสิทธิที่จะรับการแจ้งเตือนจากผู้ประกอบการเครือข่ายหากข้อมูลของตนถูกแก้ไข เผยแพร่ ทำลาย หรือสูญหาย

๓.๑ โครงสร้างพื้นฐานข้อมูลที่สำคัญ (Critical-Information Infrastructure หรือ CII)

CSL ให้ความสำคัญกับโครงสร้างพื้นฐานข้อมูลที่สำคัญ (CII) เพื่อเป้าหมายในการปกป้องโครงสร้างพื้นฐานข้อมูลที่สำคัญจากภัยคุกคามทั้งภายในและภายนอกประเทศจีน โดยในเดือนกันยายน ปี ค.ศ. ๒๐๒๑ ได้มีการออก “Regulations on Critical Information Infrastructure Security Protections” ภายใต้ CSL เพื่อกำหนดขอบเขตความหมายของคำว่า “โครงสร้างพื้นฐานข้อมูลที่สำคัญ” ให้หมายความถึง บริการการสื่อสารและข้อมูลสาธารณะ พลังงาน การขนส่ง ระบบการจัดการน้ำ การเงิน บริการสาธารณะ การบริหารจัดการทางอิเล็กทรอนิกส์ อุตสาหกรรมเทคโนโลยีป้องกันประเทศและอุตสาหกรรมและภาคส่วนสำคัญอื่น ๆ รวมถึงเครือข่ายและระบบข้อมูลที่สำคัญอื่น ๆ ซึ่งหากถูกทำลาย สูญเสียการทำงาน หรือมีการรั่วไหลของข้อมูล อาจก่อให้เกิดอันตรายร้ายแรงต่อความมั่นคงของชาติ สวัสดิการแห่งรัฐ ชีวิตความเป็นอยู่ของประชาชน หรือผลประโยชน์สาธารณะ อีกทั้งโครงสร้างพื้นฐานเหล่านี้จะต้องได้รับการปกป้องตามระบบการป้องกันที่เป็นลำดับขั้นด้วย[๒๒]

---

[๒๒]Aynne Kokas, “China’s 2021 Data Security Law: Grand Data Strategy with Looming Implementation Challenges”, China Leadership Monitor, Winter 2021 Issue 70 Wednesday, December 1, 2021, หน้า ๗, สืบค้นเมื่อ ๒๐ มกราคม ๒๕๖๘, จาก https://www.prcleader.org/post/china-s-2021-data-security-law-grand-data-strategy-with-looming-implementation-challenges

๓.๒ หลักการในการประมวลผลข้อมูลส่วนบุคคลภายใต้กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ (CSL)

(๑) ข้อจำกัดวัตถุประสงค์ (Purpose limitation) ผู้ดำเนินการเครือข่ายต้องแจ้งให้ผู้บริโภคทราบถึงวัตถุประสงค์ในการเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคลของตน การประมวลผลข้อมูลส่วนบุคคลโดยผู้ดำเนินการเครือข่ายต้องไม่เกินวัตถุประสงค์ที่เก็บรวบรวมไว้ตั้งแต่แรกหรือต้องสมเหตุสมผล (มีเหตุผลเหมาะสมและเกี่ยวข้องกับวัตถุประสงค์เดิม) และหากต้องมีการประมวลผลเพิ่มเติม ผู้ดำเนินการเครือข่ายต้องได้รับความยินยอมเพิ่มเติมอย่างชัดเจนจากเจ้าของข้อมูลส่วนบุคคลนั้น

(๒) ความโปร่งใส (Transparency) ผู้ดำเนินการเครือข่ายต้องประกาศกฎเกณฑ์การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลของผู้บริโภค ต้องแจ้งให้ผู้บริโภคทราบถึงวัตถุประสงค์และขอบเขตในการเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคลของตน นอกจากนี้ ผู้บริโภคต้องได้รับการแจ้งวิธีการที่ใช้ในการเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคลของตนด้วย

(๓) ความยินยอม (Consent) ก่อนการเก็บรวบรวมหรือการใช้ข้อมูลส่วนบุคคล ผู้ดำเนินการเครือข่ายต้องได้รับความยินยอมอย่างชัดเจนจากเจ้าของข้อมูลส่วนบุคคลนั้น

(๔) ความถูกต้องตามกฎหมาย (Lawfulness) การเก็บรวบรวม การใช้ หรือการประมวลผลข้อมูลส่วนบุคคลต้องไม่ขัดแย้งกับระเบียบ ข้อบังคับ หรือข้อตกลงที่ทำไว้กับผู้ใช้

(๕) การลดขนาดข้อมูล (Data minimization) ผู้ดำเนินการเครือข่ายต้องปฏิบัติตามหลักการความจำเป็นในการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลของผู้ใช้ ซึ่งหมายความว่าผู้ดำเนินการต้องไม่เก็บรวบรวมข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้องกับบริการที่มอบให้แก่บุคคลนั้น

(๖) ความชอบธรรมและความลับ (Integrity and confidentiality) ผู้ดำเนินการเครือข่ายต้องรักษาข้อมูลส่วนบุคคลโดยใช้มาตรการทางเทคนิค ซึ่งรวมถึงมาตรการเพื่อป้องกันการรั่วไหล การทำลาย หรือทำให้เสียหาย โดยข้อมูลส่วนบุคคลจะต้องไม่ถูกเปิดเผยแก่บุคคลที่สามโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้น เว้นแต่จะมีข้อบังคับ/ข้อกำหนด ให้กระทำได้โดยไม่ต้องได้รับความยินยอม

(๗) ข้อจำกัดการเก็บรักษา (Storage limitation) ข้อมูลส่วนบุคคลจะถูกเก็บรักษาไว้เฉพาะในระยะเวลาขั้นต่ำที่จำเป็นในการบรรลุวัตถุประสงค์ที่เก็บรวบรวมไว้ หลังจากนั้นจะต้องถูกกำจัดโดยการลบหรือการไม่ระบุตัวตนอย่างเหมาะสม

๓.๓ บุคคลที่อยู่ภายใต้บังคับ CSL

CSL จะบังคับใช้กับเครือข่ายที่จัดตั้ง ดำเนินการ รักษา และใช้งานภายในอาณาเขตของสาธารณรัฐประชาชนจีน รวมถึงการควบคุมกำกับดูแลและการจัดการด้านความปลอดภัยทางเครือข่าย ซึ่งครอบคลุมทั้งหน่วยงานภาครัฐและเอกชน แต่ CSL ไม่ได้ระบุถึงขอบเขตการใช้บังคับนอกอาณาเขตอย่างชัดเจน อย่างไรก็ดี ได้มีการออกมาตรการการประเมินความปลอดภัยในการโอนย้ายข้อมูลส่วนบุคคลข้ามพรมแดน “Measures for Security Assessment of Cross-border Transfer of Personal Data” เพื่อกำหนดให้หน่วยงานต่างประเทศที่เก็บรวบรวมข้อมูลส่วนบุคคลภายในอาณาเขตของจีน ต้องมีตัวแทนหรือองค์กรในประเทศจีนเพื่อเป็นผู้รับผิดชอบในการปฏิบัติตามกฎ ระเบียบ และ

ข้อบังคับต่างๆ ที่ CSL กำหนดไว้ เช่น การเก็บรวบรวม การใช้ การประมวลผล การคุ้มครองข้อมูลส่วนบุคคล หน้าที่ของผู้ดำเนินการเครือข่าย

๓.๔ ข้อกำหนดด้านมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity requirements)

CSL กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์ที่สำคัญหลายประการต่อผู้ดำเนินการเครือข่าย สรุปได้ดังนี้

(๑) การปกป้องข้อมูลส่วนบุคคล (The protection of personal information) โดยเฉพาะการป้องกันข้อมูลส่วนบุคคลจากการเปิดเผย การปลอมแปลง การทำลาย และการสูญหาย

(๒) ดำเนินมาตรการทางการบริหารและเทคโนโลยีอย่างมีประสิทธิภาพเพื่อคุ้มครองและรักษาความปลอดภัยของข้อมูลส่วนบุคคล

(๓) การรักษาความปลอดภัยของระบบเครือข่ายและข้อมูลส่วนบุคคลให้มีความปลอดภัยอย่างต่อเนื่อง และแก้ไขข้อบกพร่องด้านความปลอดภัยให้เร็วที่สุด

(๔) การจัดทำแผนการตอบสนองฉุกเฉินสำหรับเหตุการณ์ความมั่นคงความปลอดภัยทางไซเบอร์ และปฏิบัติตามแผนเมื่อเกิดเหตุการณ์ รวมถึงการดำเนินมาตรการแก้ไขโดยทันที

(๕) ปฏิบัติตามระบบการป้องกันหลายระดับที่รัฐบาลจีนอนุมัติ (state-sanctioned multi-level protection systems หรือ MLPS) เพื่อปกป้องโครงสร้างพื้นฐานที่สำคัญและข้อมูลที่สำคัญจากภัยคุกคามทางไซเบอร์

(๖) ผู้ดำเนินการโครงสร้างพื้นฐานข้อมูลสำคัญที่กำหนดโดยคณะมุขมนตรี (the State Council) ต้องประเมินมาตรการความปลอดภัยทางไซเบอร์ของตนทุกปี และพยายามที่จะเพิ่มการปกป้องและการรักษาความปลอดภัยให้มากขึ้น

๓.๕ การโอนข้อมูลข้ามพรมแดน (Cross-border transfer)

ผู้ดำเนินการโครงสร้างพื้นฐานข้อมูลสำคัญต้องสร้างความมั่นใจให้เกิดขึ้นได้ว่าข้อมูลส่วนบุคคลของลูกค้าจะถูกเก็บรักษาไว้ภายในประเทศ หากมีความจำเป็นต้องโอนย้ายข้อมูลออกนอกประเทศเนื่องจากความจำเป็นทางธุรกิจ ผู้ดำเนินการเครือข่ายต้องดำเนินการประเมินความปลอดภัยตามมาตรการที่กำหนดร่วมกันโดยหน่วยงานด้านกิจการอวกาศ (China’s cyberspace administration bodies) และหน่วยงานที่เกี่ยวข้องภายใต้คณะมุขมนตรี

๓.๖ บทกำหนดโทษ[๒๓]

CSL กำหนดบทลงโทษหลายประการสำหรับผู้ดำเนินการเครือข่ายที่กระทำผิด ซึ่งโดยทั่วไปผู้กระทำผิดจะได้รับคำเตือนและคำสั่งให้แก้ไขปัญหา หากมีการกระทำผิดซ้ำ ๆ จะมีบทลงโทษดังนี้

(๑) ปรับตั้งแต่หนึ่งแสนหยวนถึงหนึ่งล้านหยวนสำหรับผู้ดำเนินการเครือข่าย

---

[๒๓]ศึกษาข้อมูลเพิ่มเติมเรื่องการเสนอให้มีการแก้ไขเพิ่มเติม CSL จาก https://www.china-briefing.com/news/china-cybersecurity law-cac-solicits-opinions-on-amendment/, สืบค้นเมื่อ ๖ กุมภาพันธ์ ๒๕๖๘

(๒) การปรับเงินส่วนบุคคลสำหรับเจ้าหน้าที่ที่รับผิดชอบในการดำเนินงานของผู้ดำเนินการเครือข่ายกรณีที่มีการละเมิดกฎหมาย CSLหรือไม่ปฏิบัติตามข้อกำหนดที่กฎหมายกำหนดไว้

(๓) ยึดรายได้ทางธุรกิจจากการกระทำที่ผิดกฎหมาย

(๔) จำกัดกิจกรรมทางธุรกิจ

(๕) ปิดเว็บไซต์

(๖) เพิกถอนหรือยกเลิกใบอนุญาตประกอบธุรกิจ (revocation of relevant operations permits, or the cancellation of business licenses)

ทั้งนี้ ผู้กระทำผิดอาจถูกตั้งข้อหาโทษทางอาญาตามความรุนแรงของการไม่ปฏิบัติตามข้อกำหนดหรือไม่ปฏิบัติตามกฎหมายด้วย

แนวทางการบังคับใช้กฎหมายและสภาพปัญหาเกี่ยวกับการให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลในทางการแพทย์ที่นำปัญญาประดิษฐ์มาใช้

๑. แนวทางการบังคับใช้กฎหมาย

ดังที่ได้กล่าวไว้แล้วว่า กฎหมายที่มีผลใช้บังคับแก่การคุ้มครองข้อมูลส่วนบุคคลในทางการแพทย์ที่นำปัญญาประดิษฐ์มาใช้ในประเทศจีนอยู่ภายใต้บังคับของกฎหมายฉบับหลักสามฉบับ ได้แก่ **Personal Information Protection Law (PIPL) Data Security Law (DSL)** และ **Cybersecurity Law (CSL)** โดย PIPL กำหนดให้ข้อมูลทางการแพทย์และสาธารณสุข (medical health status) จัดเป็นข้อมูลที่มีความละเอียดอ่อน ซึ่งจะต้องใช้มาตรการที่เข้มงวดในการประมวลผลข้อมูลเหล่านี้ภายใต้ PIPL[๒๔] (Article 28) เช่น ต้องมีวัตถุประสงค์เฉพาะเจาะจงในการประมวลผล ต้องมีเหตุจำเป็น ต้องใช้มาตรการคุ้มครองข้อมูลที่เข้มงวด รวมทั้งการได้รับความยินยอมต่างหากจากเจ้าของข้อมูลส่วนบุคคล (Article 29) กำหนดมาตรการที่มุ่งเน้นให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามหลักการรักษาความถูกต้องและความปลอดภัยของข้อมูลส่วนบุคคล การจำแนกข้อมูลเป็นส่วน ๆ ตามระดับความละเอียดอ่อน การได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลส่วนบุคคล รวมถึงการประเมินผลกระทบในการประมวลผลข้อมูลก่อนที่จะดำเนินการในข้อมูลที่มีความละเอียดอ่อน ส่วน DSL กำหนดหลักการครอบคลุมข้อมูลทั้งหมด ซึ่งรวมถึงข้อมูลส่วนบุคคลด้วย โดยมีการแบ่งประเภทของข้อมูลเป็นสองระดับ ได้แก่ ข้อมูลหลักแห่งชาติและข้อมูลสำคัญ กำหนดมาตรการควบคุมการส่งออกข้อมูลในบางหมวดหมู่เฉพาะ เพื่อป้องกันไม่ให้ข้อมูลสำคัญหรือข้อมูลที่มีความละเอียดอ่อนออกไปยังต่างประเทศโดยไม่ได้รับอนุญาต ตลอดจนการจำกัดการให้ข้อมูลแก่หน่วยงานต่างประเทศที่เข้มงวด ซึ่งหมายความว่าการให้ข้อมูลแก่หน่วยงานเหล่านี้ต้องเป็นไปตามกฎระเบียบและข้อกำหนดที่กำหนดโดย

---

[๒๔] Wang, C.; Zhang, J.; Lassi, N.; Zhang, X., “ Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective”, อ้างแล้ว เชิงอรรถที่ ๖, หน้า ๘-๙

รัฐบาลจีน[๒๕] สำหรับ CSL จะมุ่งเน้นการกำหนดมาตรการความปลอดภัยทางไซเบอร์สำหรับการดำเนินการกับข้อมูลส่วนบุคคล รวมถึงการกำกับดูแลข้อมูลที่สำคัญและกิจกรรมทางไซเบอร์เพื่อป้องกันการโจมตีทางไซเบอร์และการละเมิดข้อมูล รวมทั้งกำหนดมาตรการเพื่อป้องกันและการจัดการความเสี่ยงทางไซเบอร์ที่อาจเกิดขึ้นจากการใช้งานระบบที่ใช้ปัญญาประดิษฐ์ในทางการแพทย์ผ่านทางข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ การมีระบบการป้องกันหลายระดับ (Multi-Level Protection Scheme หรือ MLPS) ซึ่งจะมีบทบาทสำคัญในการปกป้องข้อมูลสุขภาพที่มีความละเอียดอ่อนและเป็นความลับ เช่น ข้อมูลสุขภาพของผู้ป่วย มีการจัดระดับความเสี่ยงและมาตรการความปลอดภัยที่เหมาะสมสำหรับข้อมูลสุขภาพ เพื่อป้องกันการรั่วไหลและการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ซึ่งการใช้ AI ในการวิเคราะห์และประมวลผลข้อมูลสุขภาพต้องปฏิบัติตามมาตรการความปลอดภัยที่กำหนด[๒๖]

๒. สภาพปัญหา

การกำกับดูแลด้านข้อมูลทางการแพทย์ในประเทศจีนกระจายอยู่ภายใต้กฎหมายระดับพระราชบัญญัติ ตลอดจนกฎ ระเบียบ และข้อคับ โดยกฎหมายระดับพระราชบัญญัติฯ จะมีหลักการที่เกี่ยวข้องกับสิทธิส่วนบุคคลและการให้ความคุ้มครองข้อมูลส่วนบุคคล เมื่อกล่าวถึง “สิทธิส่วนบุคคล” สิทธิดังกล่าวได้รับการรับรองไว้ในรัฐธรรมนูญของประเทศจีน ได้แก่ การรับรองศักดิ์ศรีความเป็นมนุษย์ “the right of personal dignity” สิทธิในที่อยู่อาศัย “the right of residence” และสิทธิในการติดต่อสื่อสาร “the right of the freedom of privacy in correspondence” และยังได้รับการรับรองภายใต้ประมวลกฎหมายแพ่งและพาณิชย์ในฐานะสิทธิในบุคลิกภาพ" (Right of Personality[๒๗]) ซึ่งสิทธิที่ได้รับการรับรองตามประมวลกฎหมายแพ่งและพาณิชย์ดังกล่าว ได้ถูกนำมาบัญญัติไว้ภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PIPL) เช่นกัน กล่าวคือ การกำหนดขอบเขตของคำว่า “ข้อมูลส่วนบุคคล” การกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลในการควบคุมและประมวลผลข้อมูลส่วนบุคคล และการกำหนดหน้าที่ความรับผิดชอบของผู้ประมวลผลข้อมูล จากแนวทางของกฎหมายข้างต้นเห็นได้ว่าประเทศจีนให้ความสำคัญและมีความพยายามอย่างต่อเนื่องในการปกป้องผลประโยชน์ส่วนบุคคล ข้อมูลสุขภาพก็เป็นข้อมูลหนึ่งที่ถูกควบคุมภายใต้กฎหมายเฉพาะ ระเบียบ ข้อบังคับ และนโยบายต่าง ๆ

---

[๒๕] Rogier Creemers, “ China’s emerging data protection framework”, Journal of cybersecurity, 2022, 1–12, หน้า ๗, สืบค้นเมื่อ ๑๒ ก.พ. ๖๘, จาก https:// academic.oup.com/ cybersecurity/ article/8/1/tyac011/6674794

[๒๖] Digital Health Laws and Regulations China 2024-2025, Chapter Content Free Access, สืบค้นเมื่อ ๑๒ ก.พ. ๖๘, จาก https://iclg.com/practice-areas/digital-health-laws-and-regulations/china#:~:text=Personal% 20information% 20protection% 2C%20data%20security ,most%20industries% 2C%20including%20digital%20health.

[๒๗] สิทธิที่บุคคลมีในการปกป้องและควบคุมเรื่องต่าง ๆ ที่เกี่ยวข้องกับความเป็นส่วนตัวของตนเอง เช่น สิทธิในการปกป้องข้อมูลส่วนตัว สิทธิในการปกป้องชื่อเสียงและภาพลักษณ์สิทธิในการไม่ถูกหมิ่นประมาทหรือดูหมิ่น

โดยหลักการสำคัญภายใต้ PIPL คือ การให้ความยินยอมในการแบ่งปันและการประมวลผลข้อมูลส่วนบุคคล หลักการนี้ทำให้ความเป็นส่วนตัวของผู้ป่วยจะได้รับการคุ้มครองผ่านข้อกำหนดในการรักษาความลับ อย่างไรก็ดี ปรากฏข้อยกเว้นตามกฎหมายบางประการที่ชี้ให้เห็นถึงการส่งเสริมการแบ่งปันข้อมูลสุขภาพระหว่างอุตสาหกรรมและสถาบันต่าง ๆ โดยข้อยกเว้นเหล่านี้อนุญาตให้ใช้ข้อมูลสุขภาพโดยชอบธรรมได้โดยไม่จำเป็นต้องได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง[๒๘] ซึ่งสามารถสรุปสภาพปัญหาของประเทศจีนในการบังคับใช้กฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลทางการแพทย์ที่นำปัญญาประดิษฐ์มาใช้ได้ดังนี้[๒๙]

(๑) PIPL กำหนดข้อยกเว้นในการประมวลผลข้อมูลส่วนบุคคลโดยไม่ต้องได้รับความยินยอมไว้ ๖ กรณี (Article 13[๓๐]) ได้แก่ ๑) เมื่อจำเป็นต้องมีการจัดทำหรือดำเนินการตามสัญญาหรือการจัดการทรัพยากรมนุษย์ ๒) เมื่อจำเป็นต้องปฏิบัติตามหน้าที่ตามกฎหมายหรือข้อผูกพัน ๓) เมื่อจำเป็นต้องตอบสนองต่อสถานการณ์ฉุกเฉินด้านสาธารณสุข หรือเพื่อปกป้องชีวิต สุขภาพและความปลอดภัยในทรัพย์สินของบุคคลในกรณีฉุกเฉิน ๔) เพื่อการประมวลผลข้อมูลส่วนบุคคลอย่างเหมาะสมในการรายงานข่าว การกำกับดูแลสื่อ และกิจกรรมอื่น ๆ ที่ดำเนินการเพื่อประโยชน์สาธารณะ ๕) เพื่อการประมวลผลข้อมูลส่วนบุคคลที่เปิดเผยต่อสาธารณชนโดยเจ้าของข้อมูลส่วนบุคคลนั้นเองหรือมีกฎหมายกำหนดให้ต้องเปิดเผย และ ๖) กรณีอื่น ๆ ตามกฎหมาย กฎ หรือระเบียบต่าง ๆ กำหนดไว้ การกำหนดข้อยกเว้นในลักษณะเช่นนี้ แม้จะสามารถนำมาบังคับใช้กับอุตสาหกรรมทางการแพทย์ได้ แต่ก็ยังขาดความชัดเจน กล่าวคือ การที่ข้อยกเว้นใน PIPL ใช้คำที่คลุมเครือ เช่น “สถานการณ์ฉุกเฉินด้านสาธารณสุข” และ “ภาวะฉุกเฉิน” จะทำให้การตีความและการนำไปใช้มีความยืดหยุ่นและไม่ชัดเจน อีกทั้ง PIPL ไม่ได้กำหนดรายละเอียดหรือกฎเกณฑ์ที่ชัดเจนในการประมวลผลข้อมูลในสถานการณ์ที่เป็นข้อยกเว้น นอกจากนี้ ยังขาดมาตรฐานสำหรับการปฏิบัติงานที่ชัดเจน เนื่องจากการที่ข้อยกเว้นใน PIPL ระบุว่า ขึ้นอยู่กับ “กรณีอื่นๆ ที่กำหนดโดยกฎหมาย กฎ หรือระเบียบต่าง ๆ ” ย่อมจะทำให้การประมวลผลข้อมูลในสถานการณ์ที่ยกเว้นอาจมีความไม่แน่นอนและขึ้นอยู่กับการตีความของเจ้าหน้าที่หรือหน่วยงาน

(๒) ระบบเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) ในประเทศจีนยังขาดความชัดเจนและไม่เข้มแข็ง เนื่องจาก

- ประเทศจีนไม่มีระบบเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่เฉพาะเจาะจงที่มีการกำหนดบทบาทและหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างชัดเจน

---

[๒๘] Sun, L. (2022). “ Health data governance in China: Emphasizing ‘sharing’ and ‘protection’ based on the right to health”, อ้างแล้ว เชิงอรรถที่ ๕, หน้า ๖

[๒๙] Wang, C.; Zhang, J.; Lassi, N.; Zhang, X., “ Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective”, อ้างแล้ว เชิงอรรถที่ ๖, หน้า ๙-๑๔

[๓๐] โปรดดูเชิงอรรถที่ ๑๑

- กฎหมายและระเบียบที่เกี่ยวข้องกับความปลอดภัยของเครือข่ายและการคุ้มครองข้อมูลส่วนบุคคลในประเทศจีนยังไม่เข้มงวดมากนัก เช่น กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ (CSL) มาตรา ๔๐ กำหนดให้ผู้ดำเนินการเครือข่ายต้องจัดการความปลอดภัยของเครือข่าย และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PIPL) มาตรา ๙ กำหนดให้หน่วยงานต้องจัดให้มีบุคคลทำหน้าที่เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล แต่ปรากฏว่ากฎเกณฑ์สำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลยังขาดความชัดเจน ทำให้การปฏิบัติงานและการดำเนินการของหน่วยงานต่างๆ ขาดความชัดเจนไปด้วย

- บทลงโทษสำหรับการไม่ปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลยังมีโทษค่อนข้างเบา (light)

(๓) การที่มาตรา ๒๘ แห่งกฎหมาย PIPL กำหนดว่า ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน คือ ข้อมูลส่วนบุคคลที่เมื่อรั่วไหลหรือถูกใช้อย่างผิดกฎหมาย อาจส่งผลกระทบต่อศักดิ์ศรีของบุคคลหรือทำให้เกิดอันตรายต่อความปลอดภัยหรือทรัพย์สินของบุคคล โดยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน รวมถึงข้อมูลชีวภาพ ความเชื่อทางศาสนา เอกลักษณ์เฉพาะตัว ข้อมูลทางการแพทย์และสาธารณสุข บัญชีการเงิน ที่อยู่ของบุคคล และข้อมูลส่วนบุคคลของผู้เยาว์อายุต่ำกว่า ๑๔ ปี กรณีจึงเห็นได้ว่า การที่ PIPL เพิ่มมาตรฐานการจำแนกประเภทข้อมูลส่วนบุคคลออกเป็นสองประเภท ได้แก่ ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Information) และข้อมูลส่วนบุคคลทั่วไป (General Personal Information) ทำให้เกิดปัญหาในการกำหนดความสัมพันธ์ระหว่างข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและข้อมูลส่วนบุคคลที่เป็นส่วนตัว และทำให้นักวิชาการมีความคิดเห็นที่ขัดแย้งกันในการพิจารณาว่าข้อมูลทั้งสองประเภทมีลักษณะที่เท่าเทียมกันหรือไม่

(๔) ความท้ายทายในการเก็บรวบรวมและการใช้ข้อมูล การรั่วไหลของข้อมูลส่วนบุคคล ซึ่งโดยส่วนใหญ่มักจะเกิดขึ้นในสามขั้นตอนในกระบวนการประมวลผลข้อมูลโดยใช้ปัญญาประดิษฐ์ ได้แก่ ๑) ขั้นตอนการเก็บข้อมูล ในขั้นตอนนี้ แพลตฟอร์มบริการข้อมูลอาจเก็บข้อมูลส่วนบุคคลเกินกว่าที่จำเป็นหรือเก็บข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนโดยที่บุคคลนั้นไม่ทราบ ซึ่งเป็นการละเมิดความเป็นส่วนตัวของบุคคล ๒) ขั้นตอนการใช้ข้อมูล ในขั้นตอนนี้ การใช้งานข้อมูลที่ไม่เหมาะสมหลังจากการเก็บข้อมูลหรือการแบ่งปันข้อมูลส่วนบุคคลของผู้ใช้ระหว่างแพลตฟอร์มต่าง ๆ โดยไม่แจ้งให้ผู้ใช้ทราบ เป็นสาเหตุที่ทำให้เกิดการรั่วไหลของความเป็นส่วนตัว และ ๓) ขั้นตอนการทำนายผลโดยใช้อัลกอริทึม ในขั้นตอนนี้ โปรแกรมคอมพิวเตอร์ขั้นสูงและเทคโนโลยีการวิเคราะห์ข้อมูลขนาดใหญ่ที่ใช้ปัญญาประดิษฐ์ (AI) ในการวิเคราะห์ข้อมูลส่วนบุคคลเพื่อค้นหาข้อมูลที่ซ่อนอยู่ กรณีนี้ความสำคัญมิได้อยู่ที่ตัวข้อมูล แต่กลับเป็นข้อมูลเพิ่มเติมที่มักจะถูกซ่อนอยู่ซึ่งได้รับมาจากการใช้อัลกอริทึม AI การใช้เทคโนโลยีอัลกอริทึมและความแม่นยำในการทำนายผล (prediction) ได้พัฒนาจนถึงระดับที่สามารถหลีกเลี่ยงการใช้ข้อมูลโดยตรงได้ ซึ่งสิ่งนี้จะก่อให้เกิดความเสี่ยงต่อการรั่วไหลของความเป็นส่วนตัวจากการทำนายผลโดยใช้อัลกอริทึม และการรั่วไหลดังกล่าวมักจะเกิดขึ้นกับการใช้เทคโนโลยีหรือเครื่องมือเสริมในการวินิจฉัยหรือรักษาผู้ป่วย (auxiliary diagnosis and treatment

scenarios) และแม้ว่า PIPL จะกำหนดมาตรการการแจ้งล่วงหน้า การขอความยินยอมจากบุคคล การห้ามเก็บข้อมูลเกินกว่าที่จำเป็น และการจัดการ (รวมถึงการเก็บ) ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนเฉพาะเมื่อมีวัตถุประสงค์เฉพาะ มีความจำเป็นเพียงพอ และมีมาตรการป้องกันอย่างเข้มงวดไว้แล้วก็ตาม แต่ด้วยการพัฒนาเทคโนโลยี AI ความเสี่ยงด้านความเป็นส่วนตัวย่อมมีแนวโน้มเพิ่มมากขึ้น ดังนั้น กฎหรือข้อบังคับเกี่ยวกับความยินยอมและการลบการระบุตัวตนของข้อมูลส่วนบุคคล (de-identification) ย่อมจะต้องเผชิญกับความท้าทายต่อไป

(๕) ความท้าทายเกี่ยวกับการให้ความยินยอม เทคโนโลยี AI มักประมวลผลข้อมูลจำนวนมากเพื่อทำนายผล โดยใช้การตัดสินใจและอัลกอริทึมที่ยากต่อการทำความเข้าใจและถอดรหัส (decipher) สำหรับโปรแกรมเมอร์คอมพิวเตอร์ ผู้เชี่ยวชาญด้านข้อมูล และผู้ที่เป็นเจ้าของข้อมูล สิ่งนี้เรียกว่า “black-box effect[๓๑]” ซึ่งเป็นความท้าทายอย่างมากในด้านการแพทย์ในการคุ้มครองความเป็นส่วนตัว แม้ว่าประมวลกฎหมายแพ่งและพาณิชย์ของจีน และ PIPL จะระบุวัตถุประสงค์ วิธีการ และขอบเขตของการประมวลผลข้อมูลส่วนบุคคลไว้แล้ว แต่บทบัญญัติเหล่านั้นยังคงมีความคลุมเครือและไม่ระบุชัดเจนว่ากฎการประมวลผลและเนื้อหาที่ต้องเปิดเผยคืออะไร เช่น โค้ด ข้อมูลพื้นฐาน หรือการตัดสินใจของอัลกอริทึม นอกจากนี้ การนำ AI มาใช้ในอุตสาหกรรมการแพทย์ โดยเฉพาะการใช้เทคโนโลยีการเรียนรู้เชิงลึกเพื่อช่วยในการวินิจฉัยหรือการคาดการณ์โรค จำเป็นต้องมีข้อมูลจำนวนมาก การทำให้มั่นใจว่ามีการขอความยินยอมจากบุคคลสำหรับข้อมูลทุกชิ้นในข้อมูลขนาดใหญ่จึงเป็นเรื่องที่ยุ่งยากและเป็นไปไม่ได้ในทางข้อเท็จจริง และทำให้เป็นอุปสรรคในการพัฒนาเทคโนโลยีและนวัตกรรมในด้านการแพทย์ หากการประมวลผลข้อมูลส่วนบุคคลแต่ละครั้งต้องได้รับความยินยอมและมีเอกสารจากผู้ป่วยหรือบุคคลที่เกี่ยวข้องทั้งหมด

(๖) การป้องกันการลบการระบุตัวตนอาจไม่สามารถปกป้องความเป็นส่วนตัวได้ (De-identification Protections May Not Protect Personal Privacy) PIPL ให้ความคุ้มครองเฉพาะข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ ซึ่งหมายความว่า การประมวลผลข้อมูลที่ไม่สามารถเชื่อมโยงกับบุคคลใด ๆ ได้หลังการลบการระบุตัวตน ไม่จำเป็นต้องขอความยินยอมจากบุคคลนั้น ดังนั้น ข้อมูลจำนวนมากจำเป็นต้องถูกลบการระบุตัวตนก่อนการประมวลผล อย่างไรก็ตาม ข้อมูลทางการแพทย์และสุขภาพในบางลักษณะไม่สามารถถูกลบการระบุตัวตนได้ มิฉะนั้นจะสูญเสียคุณค่าและความหมายเดิม นอกจากนี้ ผู้ป่วยรายบุคคลที่เป็นเป้าหมายเฉพาะในการวินิจฉัยทางการแพทย์ซึ่งมีการบันทึกและวิเคราะห์ข้อมูลสุขภาพ และมีผลการวินิจฉัยทางการแพทย์ เมื่อข้อมูลนี้ถูกลบการระบุตัวตน จะทำให้การให้ความช่วยเหลือเมื่อสุขภาพและชีวิตของเจ้าของข้อมูลตกอยู่ในอันตรายไม่อาจเกิดขึ้นได้อย่างทันท่วงที

---

[๓๑] **Black-box effect** หมายถึงปรากฏการณ์ที่เกิดขึ้นเมื่อการทำงานของโมเดล AI หรืออัลกอริทึมไม่สามารถถูกอธิบายหรือเข้าใจได้อย่างชัดเจน ทั้งนี้ เพราะขั้นตอนการทำงานภายในของอัลกอริทึมมีความซับซ้อนมาก ทำให้ยากต่อการถอดรหัสหรือการอธิบาย

อนึ่ง การลบการระบุตัวตนของข้อมูลส่วนบุคคลมีความสำคัญเมื่อมีการใช้ข้อมูลด้านสุขภาพในการวิจัยกลุ่มเป้าหมาย การพัฒนายา และด้านอื่นๆ และโดยทั่วไป โรงพยาบาลมักจะใช้มาตรการความปลอดภัยบางประการเมื่อใช้ข้อมูลทางการแพทย์และสุขภาพของผู้ป่วยในการวิจัย เช่น การให้ผู้ป่วยลงนามในข้อตกลงความลับ การป้องกันข้อมูลที่สำคัญหรือข้อมูลส่วนบุคคลจากการเปิดเผย โดยการแปลงข้อมูลนั้นให้อยู่ในรูปแบบที่ไม่สามารถระบุตัวตนได้โดยง่าย (data desensitization) เช่น การลดความละเอียดของข้อมูล การเข้ารหัส การใช้เทคนิคการลบการระบุตัวตน และการทำลายข้อมูลอย่างทันท่วงที อย่างไรก็ตาม ด้วยการพัฒนาทางเทคโนโลยี ข้อมูลที่ไม่สามารถระบุตัวตนได้อย่างสมบูรณ์อาจไม่มีอีกต่อไป การพัฒนาเทคโนโลยีการระบุตัวตนย้อนกลับได้เพิ่มความเสี่ยงในการระบุข้อมูลใหม่อีกทั้งมีความเสี่ยงสูงที่ข้อมูลส่วนบุคคลจะถูกระบุตัวตนได้ในโลกไซเบอร์ แม้ว่าข้อมูลนั้นจะถูกลบการระบุตัวตนแล้วก็ตาม (The high-risk nature of identifiability in cyberspace) ทำให้ยากต่อการบรรลุหลักการเรื่อง “ไม่ระบุตัวตน” อย่างสมบูรณ์ในโลกอินเทอร์เน็ต เนื่องจากข้อมูลเครือข่ายเกือบทั้งหมดสามารถเชื่อมโยงกับบุคคลที่สามารถระบุตัวตนได้ เพราะเหตุว่าข้อมูลที่ถูกลบการระบุตัวตนแล้วสามารถถูกรวมเข้ากับแหล่งข้อมูลส่วนบุคคลอื่น ๆ เพื่อประกอบเข้ากับข้อมูลเกี่ยวกับที่อยู่ ภูมิหลังทางสังคมและเศรษฐกิจ หรือแม้กระทั่งข้อมูลอัตลักษณ์ที่ครบถ้วนของบุคคล กล่าวโดยสรุป ความแตกต่างระหว่างข้อมูลส่วนบุคคลและข้อมูลที่ไม่ใช่ส่วนบุคคลมีความเปลี่ยนแปลงและการกำหนดขอบเขตระหว่างข้อมูลทั้งสองประเภทย่อมจะขึ้นอยู่กับการพัฒนาทางเทคโนโลยีที่รวดเร็ว ทำให้ยากต่อการใช้ “การระบุตัวตน” เป็นมาตรฐานสำหรับการคุ้มครองข้อมูลส่วนบุคคล

(๗) การส่งผ่านข้อมูลข้ามพรมแดน (Cross-Border Data Flow) ความพร้อมของการใช้งานและการส่งผ่านข้อมูลที่เสรีมักถูกพิจารณาว่าเป็นปัจจัยสำคัญในการพัฒนาเทคโนโลยี AI อย่างไรก็ตาม การส่งผ่านข้อมูลข้ามพรมแดนและการคุ้มครองความเป็นส่วนตัวย่อมมีความขัดแย้งกัน เนื่องจากแต่ละประเทศมีมาตรฐานความเป็นส่วนตัวและความปลอดภัย และแนวทางการส่งผ่านข้อมูลข้ามพรมแดนที่แตกต่างกัน สำหรับประเทศจีน การคุ้มครองข้อมูลมีความเกี่ยวโยงอย่างใกล้ชิดกับความมั่นคงของชาติและเกี่ยวข้องกับการรักษาอธิปไตยและความปลอดภัยสาธารณะ จีนจึงมักจะใช้ความระมัดระวังในการส่งผ่านข้อมูลข้ามพรมแดน และให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคลและอำนาจอธิปไตยแห่งชาติ โดยยอมเสียสละเสรีภาพบางประการในกระบวนการส่งข้อมูลข้ามพรมแดน เมื่อพิจารณาในบริบทของ PIPL ได้มีข้อกำหนดการตรวจสอบอย่างเข้มงวดสำหรับการส่งข้อมูลส่วนบุคคลข้ามพรมแดน โดยมาตรา ๓๘ กำหนดว่า การส่งผ่านข้อมูลส่วนบุคคลข้ามพรมแดนต้องได้รับการประเมินความปลอดภัยโดยหน่วยงานกิจการอากาศที่ได้รับการรับรองโดยสถาบันเฉพาะทางที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล หรือทำสัญญากับผู้รับข้อมูลในต่างประเทศตามสัญญามาตรฐานที่กำหนดโดยหน่วยงานกิจการอวกาศ (ระบุสิทธิและหน้าที่ของทุกฝ่าย) มาตรา ๓๙ กำหนดว่า การดำเนินการดังกล่าวต้องได้รับความยินยอมแยกต่างหากจากบุคคลที่เกี่ยวข้องทุกคน และมาตรา ๕๕ กำหนดให้ต้องมีการประเมินผลกระทบล่วงหน้าสำหรับการคุ้มครองข้อมูลส่วนบุคคล ส่วนในแง่ของกฎหมายระหว่างประเทศ จีนได้ลงนามในข้อตกลงการค้าเสรีกับประเทศอื่น ๆ ซึ่งข้อตกลงส่วนใหญ่ไม่ได้มีบทบัญญัติเรื่องการส่งผ่าน

ข้อมูลข้ามพรมแดน อย่างไรก็ดี ในปี ค.ศ. ๒๐๑๕ จีนได้ลงนามในข้อตกลงการค้าเสรีที่มีบทบัญญัติเรื่องการส่งผ่านข้อมูลข้ามพรมแดนกับประเทศเกาหลีใต้และออสเตรเลีย

ในบริบทของการพัฒนาฐานข้อมูลขนาดใหญ่ การส่งผ่านข้อมูลส่วนบุคคลข้ามพรมแดนเป็นช่องทางสำคัญสำหรับการพัฒนา AI ในทางการแพทย์ แต่การดำเนินการดังกล่าวก็อาจเข้าข่ายเป็นการละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล ด้วยเหตุนี้ การกำหนดแนวทางการส่งผ่านข้อมูลข้ามพรมแดนที่เหมาะสมจึงจำเป็นต้องพิจารณาทั้งเรื่องเศรษฐกิจและความเป็นส่วนตัว เพื่อสร้างสมดุลให้เกิดขึ้นในการพัฒนาเทคโนโลยีและเศรษฐกิจ ควบคู่กับการคุ้มครองความเป็นส่วนตัว

บทสรุปและข้อเสนอแนะ

๑. บทสรุป[๓๒]

ปัญญาประดิษฐ์ (AI) เป็นหนึ่งในหัวข้อที่น่าสนใจของการวิจัยในสาขาเทคโนโลยีทางการแพทย์สมัยใหม่ โดยได้มีการประยุกต์ใช้ในวงการแพทย์หลายด้าน รวมทั้งสถิติทางการแพทย์ การช่วยในการวินิจฉัยและการบำบัด การผ่าตัดโดยหุ่นยนต์ การถ่ายภาพทางการแพทย์ และการศึกษาชีววิทยาของมนุษย์ ปัจจุบันจีนประสบปัญหาการขาดแคลนทรัพยากรทางการแพทย์ในระบบบริการด้านสาธารณสุขของประเทศเป็นอย่างมาก อีกทั้งบริการทางการแพทย์ที่มีคุณภาพสูงมักจะมีเฉพาะในโรงพยาบาลขนาดใหญ่ ซึ่งผู้ป่วยจำนวนมากไม่สามารถเข้าถึงได้ ด้วยเหตุนี้ จึงทำให้เทคโนโลยี AI ที่มีการพัฒนาขึ้นตามลำดับ และสามารถเลียนแบบและแทนที่งานหลักของแพทย์ที่เป็นมนุษย์ และอาจถึงขั้นพัฒนาขีดความสามารถจนก้าวข้ามความสามารถของมนุษย์ได้ ถูกนำมาใช้ทดแทนการขาดแคลนแพทย์ผู้เชี่ยวชาญ อีกทั้งความก้าวหน้าทาง AI ในทางการแพทย์จะมีบทบาทสำคัญในการลดปัญหาที่ผู้ป่วยต้องเผชิญเมื่อพยายามเข้าถึงบริการทางการแพทย์ที่มีคุณภาพสูง ทำให้ผู้ป่วยสามารถได้รับบริการทางการแพทย์ที่มีคุณภาพสูงง่ายขึ้น และจะเป็นการกระจายการให้บริการทางการแพทย์ในประเทศจีนให้มีประสิทธิภาพมากยิ่งขึ้น ซึ่งการขาดแคลนทรัพยากรทางการแพทย์ โดยเฉพาะทรัพยากรคุณภาพสูงก่อให้เกิดความต้องการอย่างเร่งด่วนในการนำนวัตกรรมเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้ คุณประโยชน์ที่สำคัญที่สุดของการใช้ AI ในทางการแพทย์ ได้แก่ ความสามารถในการประหยัดเวลาและค่าใช้จ่าย การยกระดับการดูแลสุขภาพ และการกระจายทรัพยากรให้กว้างขวางยิ่งขึ้น การใช้ AI ในทางการแพทย์จึงควรขยายไปสู่การจัดการโรคที่มากขึ้น และควรมีความพยายามเพิ่มเติมในการสำรวจความเป็นไปได้ของการนำไปใช้ทางคลินิกในวงกว้างมากขึ้น การพัฒนาระบบ AI ที่ฉลาดกว่าและปลอดภัยกว่าถูกคาดว่าจะนำไปสู่การเปลี่ยนแปลงต่อระบบการดูแลสุขภาพทั่วทั้งประเทศ อีกทั้งการประยุกต์ใช้ AI

---

[๓๒] Li R, Yang Y, Wu S, Huang K, Chen W, Liu Y, Lin H., “ Using artificial intelligence to improve medical services in China”, Ann Transl Med 2020;8(11):711. doi: 10.21037/atm.2019.11.108, หน้า ๑-๔, สืบค้นเมื่อ ๑๒ ก.พ. ๖๘, จาก https://pmc.ncbi.nlm.nih.gov/articles/PMC7327308/#:~:text=Medical%20AI%20has%20been%20applied,achieve%20the%20intelligent%20medical%20care.

อย่างแพร่หลายย่อมจะเพิ่มระดับความแม่นยำในการให้บริการทางการแพทย์ในประเทศ อันนำไปสู่การปรับปรุงคุณภาพชีวิตของมนุษย์ให้ดียิ่งขึ้น

๒. ข้อเสนอแนะ

๒.๑ โดยที่เทคโนโลยี AI ในหลายเรื่องยังคงอยู่ในขั้นตอนการสำรวจ และยังมีข้อจำกัดต่าง ๆ ที่ต้องได้รับการแก้ไข ประการแรก คือ การประยุกต์ใช้ AI ทางคลินิกในสถานการณ์จริงมีน้อยมาก ความสำเร็จที่โดดเด่นของการใช้ AI ในทางการแพทย์ยังอยู่ในขั้นทดลองและต้องใช้ชุดข้อมูลเฉพาะที่มีคุณภาพสูง แต่ยังไม่สามารถนำมาใช้แทนที่ผลลัพธ์ในสถานการณ์จริงได้ นอกจากนี้ คุณภาพ ประสิทธิภาพ ความปลอดภัย และความน่าเชื่อถือของระบบ AI ยังต้องได้รับการรับรองโดยการกำหนดมาตรฐานและการทดลองทางคลินิกอย่างเข้มงวด ประการที่สอง คือ ในบริบทของการประยุกต์ใช้ AI ในทางการแพทย์ ข้อกำหนดทางกฎหมาย ระเบียบ ข้อบังคับ และแนวทางจริยธรรมที่เกี่ยวข้องยังคงเป็นสิ่งจำเป็นอย่างมาก เช่น การเปลี่ยนแปลงในวิธีการรวบรวม จัดเก็บ และใช้ข้อมูลทางการแพทย์ที่ใช้ AI อาจทำให้ต้องมีการทบทวนและปรับปรุงกฎหมายว่าด้วยการคุ้มครองข้อมูลต่าง ๆ ที่มีอยู่ให้ครอบคลุมทุกด้านและเพิ่มความมั่นใจในเรื่องความปลอดภัยและความเป็นส่วนตัวของข้อมูลทางการแพทย์มากยิ่งขึ้น ประการที่สาม ได้แก่ การใช้ AI อย่างแพร่หลายอาจส่งผลให้เกิดการเปลี่ยนแปลงในความสัมพันธ์ระหว่างแพทย์และผู้ป่วยแบบดั้งเดิม ซึ่งอาจส่งผลเสียต่อสภาพแวดล้อมในการดูแลสุขภาพ ปัญหาที่เกิดขึ้นจากการใช้ AI ในทางการแพทย์ควรจะต้องได้รับการแก้ไขด้วยการกำหนดแนวทางและระเบียบข้อบังคับใหม่ ๆ เพื่อให้เกิดความมั่นใจว่าการใช้ AI ในทางการแพทย์ในอนาคตจะมีความชาญฉลาดและน่าเชื่อถือมากยิ่งขึ้น[๓๓]

๒.๒ นโยบายส่วนใหญ่ของประเทศจีนในการลดความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลสุขภาพขนาดใหญ่ มุ่งเน้นไปที่การตั้งสมมติฐานความรับผิดชอบทางกฎหมายหลังจากที่เกิดเหตุการณ์แล้ว ในขณะที่ละเลยกลไกการป้องกันล่วงหน้า ซึ่งในความเป็นจริง เมื่อข้อมูลสุขภาพขนาดใหญ่รั่วไหลออกไป ย่อมจะทำให้เกิดความเสียหายอย่างมากต่อข้อมูลส่วนบุคคลและทรัพย์สินของผู้ป่วย ทำให้ถูกละเมิดความเป็นส่วนตัว ดังนั้น การสร้างกลไกการป้องกันล่วงหน้าเพื่อลดความเสี่ยงด้านความเป็นส่วนตัวจึงเป็นสิ่งสำคัญซึ่งกลไกดังกล่าวมีดังนี้[๓๔]

(๑) กลไกการประเมินผลกระทบต่อความเป็นส่วนตัว (Privacy Impact Assessment PIA) เป็นกระบวนการที่ใช้วิเคราะห์และประเมินผลกระทบเชิงลบที่อาจเกิดขึ้นจากการรวบรวม ใช้ แบ่งปัน และเก็บรักษาข้อมูลสุขภาพส่วนบุคคล ซึ่งมีจุดมุ่งหมายเพื่อระบุและลดความเสี่ยงที่อาจเกิดขึ้นต่อความเป็นส่วนตัวของบุคคล และภายหลังการประเมินผลกระทบนั้น จะต้องมีการเผยแพร่รายงาน PIA

---

[๓๓] Li R, Yang Y, Wu S, Huang K, Chen W, Liu Y, Lin H., “Using artificial intelligence to improve medical services in China”, เพิ่งอ้าง, หน้า ๓

[๓๔] Shi X (2024), “Reducing privacy risks of China’s healthcare big data through the policy framework”, Front Public Health 12:1414076.doi: 10.3389/fpubh.2024.1414076, หน้า ๕, สืบค้นเมื่อ ๑๒ ก.พ. ๖๘, จาก https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2024.1414076/full

และนโยบายการคุ้มครองความเป็นส่วนตัวที่เกี่ยวข้องของธุรกิจและองค์กรบนแพลตฟอร์มที่สาธารณชนสามารถเข้าถึงได้ เพื่อให้เกิดความโปร่งใสและความรับผิดชอบ

(๒) กลไกการพิจารณาด้านจริยธรรม (Ethics Review Mechanism) เทคโนโลยีเครือข่ายที่พัฒนาอย่างต่อเนื่องได้ก่อให้เกิดประเด็นด้านจริยธรรมของข้อมูล เช่น ความปลอดภัยของเครือข่ายและความเป็นส่วนตัวของบุคคล ซึ่งเป็นความท้าทายอย่างมากต่อสถานะและการตัดสินใจของบุคคล ด้วยเหตุนี้ การจัดตั้งหน่วยงานพิจารณาด้านจริยธรรมเฉพาะทางและการตรวจสอบผลกระทบของการใช้ข้อมูลสุขภาพขนาดใหญ่ต่อความเป็นส่วนตัวของบุคคล เป็นแนวทางหนึ่งที่จะสามารถควบคุมความเสี่ยงในการละเมิดความเป็นส่วนตัวได้ดีขึ้นตั้งแต่ต้นทาง

๒.๓ การปกป้องความเป็นส่วนตัวของข้อมูลขนาดใหญ่ทางการแพทย์ควรนำแนวคิด “สถานการณ์ที่จะเกิดขึ้น/ตามสถานการณ์ “scenario concept” มาปรับใช้ กล่าวคือ เปลี่ยนแปลงกรอบการทำงานแบบดั้งเดิมของหลัก “การยินยอมโดยได้รับการบอกกล่าว” (informed consent) และยอมรับว่ามาตรฐานการนำข้อมูลขนาดใหญ่ทางการแพทย์มาใช้อย่างเหมาะสม ขึ้นอยู่กับว่าการนำมาใช้ดังกล่าวตรงกับความคาดหวังด้านความเป็นส่วนตัวของบุคคลที่ใช้บริการหรือได้รับประโยชน์จากข้อมูลสุขภาพขนาดใหญ่หรือไม่ และสร้างความเสี่ยงด้านความเป็นส่วนตัวที่ไม่สมเหตุสมผลหรือไม่ แทนที่จะตรวจสอบอย่างเข้มงวดว่ามีการได้รับความยินยอมจากบุคคลที่เกี่ยวข้องแล้วหรือไม่ และในความเป็นจริงการนำแนวคิด“สถานการณ์ที่จะเกิดขึ้น” จำเป็นจะต้องพึ่งพากลไกการประเมินผลกระทบต่อความเป็นส่วนตัว (Privacy Impact Assessment หรือ PIA) โดยเฉพาะอย่างยิ่งเมื่อผลการประเมินปรากฏว่ามีผลกระทบต่อความเป็นส่วนตัวของบุคคลน้อยมาก ข้อมูลขนาดใหญ่ทางการแพทย์ของบุคคลย่อมสามารถประมวลผลได้โดยไม่ต้องได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูล ด้วยเหตุนี้ แนวคิด “สถานการณ์ที่จะเกิดขึ้น” ที่นำเสนอนี้จึงจะช่วยลดการพึ่งพาการให้ความยินยอมของผู้ใช้ (user consent) กล่าวคือ การใช้ข้อมูลสุขภาพขนาดใหญ่ที่ถูกต้องและเป็นไปตามกฎหมายสามารถกระทำได้โดยไม่ต้องพึ่งพาการขอความยินยอมจากผู้ใช้เสมอไป หากมีการใช้กระบวนการอื่น ๆ ที่ทำให้ข้อมูลนั้นถูกใช้อย่างปลอดภัยและถูกต้องตามกฎหมายอยู่แล้ว ในที่นี้ คือ การนำเรื่องการประเมินผลกระทบต่อความเป็นส่วนตัว (PIA) มาใช้ เพื่อเป็นข้อพิจารณาว่า การใช้ข้อมูลนั้นมีผลกระทบต่อความเป็นส่วนตัวของบุคคลมากน้อยเพียงใด ซึ่งจะช่วยสร้างสมดุลให้เกิดขึ้นระหว่างการส่งผ่านข้อมูล (the flow of data) และการปกป้องความเป็นส่วนตัว[๓๕]

---

[๓๕]Shi X (2024), “ Reducing privacy risks of China’s healthcare big data through the policy framework”, เพิ่งอ้าง, หน้า ๗-๘

ที่มา: https://www.tatlerasia.com/gen-t/leadership/chinese-startup-ai-healthcare

This three-metre-squared box, Dubbed One-minute Clinic, is part of a growing trend in China to use AI to accelerate healthcare and streamline the number of human medical professionals needed to serve the population.[๓๖]

---

[๓๖]Ping An Good Doctor เป็นแพลตฟอร์มบริการสุขภาพออนไลน์ในจีน ได้เปิดตัวคลินิก “One-minute Clinic” ที่ไม่มีพนักงานประจำ โดยใช้ AI ในการเชื่อมต่อผู้ป่วยกับทีมแพทย์ของบริษัท คลินิกเหล่านี้มีการให้บริการคำปรึกษาออนไลน์สำหรับโรคทั่วไปมากกว่า ๒,๐๐๐ ชนิด และสามารถตอบคำถามทางการแพทย์และสุขภาพได้ทันที, ศึกษาข้อมูลเพิ่มเติมได้จาก https://www.global-benefits-vision.com/ping-an-good-doctor-one-minute-clinics/?form=MG0AV3